Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

"Cyber Risk Assessment Box"

Γεώργιος Παπαμιχαήλ

Επιβλέπων Καθηγητής

Δρ. Σιαηλής Σταύρος

Δεκέμβριος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

"Cyber Risk Assessment Box"

Γεώργιος Παπαμιχαήλ

Επιβλέπων Καθηγητής

Δρ. Σιαηλής Σταύρος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2020

Περίληψη

Η μεταπτυχιακή διατριβή έχει ως στόχο την υλοποίηση εκτίμησης του ρίσκου σε μια οντότητα και επομένως την δημιουργία του «Cyber Risk Assessment Box». Σύμφωνα και με την βιβλιογραφική επισκόπηση, η μεθοδολογία έχει χωριστεί σε 3 μέρη βάση των οποίων πραγματοποιείται η εκτίμηση του ρίσκου. Επομένως, η μεθοδολογία βασίζεται σε παράγοντες που επηρεάζουν το μέγεθος του ρίσκου, δηλαδή i) Ανθρώπινους Παράγοντες, ii) Ανάλυση της Ανθρώπινης Συμπεριφοράς και iii) Εντοπισμός Ευπαθειών στα Πληροφοριακά Συστήματα.

Η μεθοδολογία βασίζεται σε μια προσέγγιση όπου i) οι Ανθρώπινοι Παράγοντες, ii) η Ανάλυση της Ανθρώπινης Συμπεριφοράς και iii) ο Εντοπισμός Ευπαθειών στα Πληροφοριακά Συστήματα συνδυάζονται κατάλληλα βάση της μαθηματικής σχέσης: ρίσκο = επίδραση x πιθανότητα. Συνεπώς, γίνεται η εκτίμηση του συνολικού ρίσκου βάση των παραγόντων που έχουν επιλεγεί. Το τελικό αποτέλεσμα παρουσιάζει μια ενιαία τιμή του ρίσκου σε ποσοστό (%).

Επιπλέων, γίνεται χρήση μιας διαμορφωμένης μεθοδολογίας «Weighted Factor Analysis» όπου οι ανθρώπινοι παράγοντες χωρίζονται σε ανθρώπινα χαρακτηριστικά: i) Χρόνια Εργασίας, ii) Επίπεδο Πρόσβασης Πληροφοριών και iii) Επίπεδο Γνώσεων. Παράλληλα, γίνεται χρήση κριτηρίων βαρύτητας που υπογραμμίζουν τα είδη των επιπτώσεων που μπορεί να πλήξουν μια οντότητα. Δηλαδή, οικονομικές και νομικές επιπτώσεις, καθώς και επιπτώσεις στην φήμη.

Για την ανάπτυξη της συγκεκριμένης προσέγγισης, έχουν αξιοποιηθεί λογισμικά και εργαλεία όπως το «Spyder». Μέσω του «Spyder», έγινε η σύνταξη και η μετατροπή της προσέγγισης σε κώδικα, στην γλώσσα προγραμματισμού «Python», με σκοπό την επεξεργασία των δεδομένων της μεθοδολογίας. Επίσης, η «Python» βοήθησε στην υλοποίηση μαθηματικών πράξεων και την παρουσίαση των αποτελεσμάτων. Επιπλέων, με την χρήση της εικονικής μηχανής «Metasploitable», έγινε η δημιουργία ενός ευπαθές δικτύου για την προσομοίωση ενός δικτύου σε ένα οργανισμό με ευπάθειες. Το εργαλείο «OpenVAS» βοήθησε στον εντοπισμό ευπαθειών στο δίκτυο που δημιουργήθηκε. Παράλληλα, τα αποτελέσματα του εργαλείου αξιοποιήθηκαν κατάλληλα στην μεθοδολογία για τον υπολογισμό του συνολικού ρίσκου.

Τα αποτελέσματα της μεταπτυχιακής διατριβής, μετά από τις δοκιμές που πραγματοποιήθηκαν, τονίζουν ότι το ρίσκο αυξάνεται i) όταν το μέγεθος της αρνητικής επίδρασης των παραγόντων μεγαλώνει και ii) όταν οι πιθανότητες υλοποίησης μιας απειλής αυξάνονται. Τα αποτελέσματα συμφωνούν και με τα δεδομένα των συγγραφέων από την βιβλιογραφική επισκόπηση.

Summary

The goal of the postgraduate thesis is to perform a risk assessment in an entity and thus the creation of the "Cyber Risk Assessment Box". Based on the literature review, the methodology has been divided into 3 sections that were used to calculate risk. Therefore, the methodology is based on certain factors that affect the risk assessment. These factors are: i) Human Factors, ii) Human Behaviour Analysis and iii) Vulnerability Assessment in Information Systems.

The methodology is based on an approach where the: i) Human Factors, ii) Human Behaviour Analysis and iii) Vulnerability Assessment in Information Systems are appropriately combined according to the mathematical relationship: risk = impact x probability. As a result, the total risk is being calculated, based on the factors that were selected. The final result represents a unified value of the risk as a percentage value (%).

Furthermore, the methodology "Weighted Factor Analysis" has been used but in a modified version, where the human factors are divided into human characteristics: i) Years Worked, ii) Data Access Level and iii) Proficiency/Knowledge Level. Additionally, the methodology uses criteria weights which underline the types of impacts an entity could be faced with. For example, financial and legal impacts, as well as reputational impact.

In order to develop and translate this particular approach, certain tools and software have been utilised such as the software tool "Spyder". The use of "Spyder" has allowed the development and the conversion of the approach into a script of the programming language "Python" to process the necessary data. Additionally, "Python" has helped to perform mathematical calculations and to provide the final output for the risk assessment. Furthermore, the installation of the virtual machine "Metasploitable" has allowed the creation of a vulnerable network, thus simulating a network in an organization with vulnerabilities. The software tool "OpenVAS" was used for the identification of vulnerabilities in the network that has been created. In addition, the output data of the tool has been used in the methodology appropriately in order to provide the final risk assessment output.

The results of the postgraduate thesis, based on the tests that have been carried out, emphasize that risk increases i) when the negative impact of the selected factors increases and ii) when the probabilities of a threat to realize increase. The results align with the data that the authors have presented in the literature review.

Ευχαριστίες

Ιδιαίτερες ευχαριστίες προς τον επιβλέποντα της μεταπτυχιακής διατριβής Δρ. Σιαηλή Σταύρο, όπου με την καθοδήγησή του έχει ολοκληρωθεί με επιτυχία η επίτευξη των στόχων της μεταπτυχιακής Διατριβής.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Το Κεφάλαιο 1 παρουσιάζει συνοπτικά το θέμα της μεταπτυχιακής διατριβής ως προς τους στόχους που έχουν τεθεί και την σημαντικότητα της έρευνας. Επίσης, γίνεται αναφορά στην δομή της μεταπτυχιακής διατριβής. Ακόμη, γίνεται μια καταγραφή των εργαλείων και λογισμικών που έχουν χρησιμοποιηθεί για την ολοκλήρωση της έρευνας.

1.1 Θέμα, Στόχοι και Σημαντικότητα της Έρευνας

Το θέμα της μεταπτυχιακής διατριβής είναι η ανάπτυξη ενός προγράμματος στον υπολογιστή για την εκτίμηση του ρίσκου σε μια οντότητα. Δηλαδή, τον υπολογισμό του μεγέθους του ρίσκου σε ένα οργανισμό, βάση των διάφορων απειλών που αντιμετωπίζει. Επομένως, η μεταπτυχιακή διατριβή θα ασχοληθεί με απειλές που προέρχονται από ανθρώπινους παράγοντες, από κακόβουλα λογισμικά, καθώς και με απειλές που δημιουργούνται από την συμπεριφορά και την δραστηριότητα των ανθρώπων («Behavioural Analysis»). Έτσι, θα γίνει χρήση διαδικτυακών βάσεων δεδομένων με κακόβουλες ενέργειες χρηστών, με σκοπό την ανάλυση των συγκεκριμένων δεδομένων. Επίσης, το συγκεκριμένο πρόγραμμα θα αναπτυχθεί στην γλώσσα προγραμματισμού «Python» σε περιβάλλον Kali Linux. Με αυτό τον τρόπο θα δημιουργηθεί ένα πρόγραμμα ή αλλιώς «κουτί» που θα μπορεί να υπολογίσει το μέγεθος του ρίσκου σε μια οντότητα. Αυτό είναι το «Cyber Risk Assessment Box».

Επομένως, οι βασικοί στόχοι της μεταπτυχιακής διατριβής είναι η δημιουργία κώδικα για την ανάπτυξη του «Cyber Risk Assessment Box» και ο υπολογισμός του ρίσκου που θα αντιπροσωπεύει σε ένα μεγάλο βαθμό την πραγματικότητα. Επίσης, είναι αναγκαίο το τελικό αποτέλεσμα του ρίσκου να είναι ένας αριθμός σε ποσοστό (%) που θα συμπεριλαμβάνει στους υπολογισμούς του, τους πιο κάτω παράγοντες:

1. Ανθρώπινοι Παράγοντες, όπως: Εργασιακή Εμπειρία (Χρόνια Εργασίας), Επίπεδο Πρόσβασης σε Πληροφορίες και Επίπεδο Γνώσεων.

2. Ανθρώπινη Συμπεριφορά.

3. Ευπάθειες Πληροφοριακών Συστημάτων.

Ακόμη, κάποια άλλοι στόχοι της μεταπτυχιακής διατριβής που θα πρέπει να επιτευχθούν είναι η επιλογή μιας μεθοδολογίας για την εκτίμηση του ρίσκου βάση των ανθρωπίνων παραγόντων, ο τρόπος που θα υλοποιείται η ανάλυση της ανθρώπινης συμπεριφοράς καθώς και η δημιουργία ενός δικτύου με ευπάθειες.

Συμπερασματικά, μέσω της έρευνας και της μεταπτυχιακής διατριβής, παρουσιάζεται μια πρωτότυπη ιδέα για τον υπολογισμό του ρίσκου συμπεριλαμβανομένων διάφορων σημαντικών παραγόντων. Το «Cyber Risk Assessment Box» παρουσιάζει μια ξεχωριστή προσέγγιση για τον υπολογισμό του ρίσκου όπου θα μπορεί να αξιοποιηθεί σε διάφορους οργανισμούς ως εργαλείο για την δημιουργία της πολιτικής ασφαλείας και στην ενίσχυση της ασφάλειας των πληροφοριακών δεδομένων.

1.2 Δομή Μεταπτυχιακής Διατριβής

Αρχικά, όπως έχει ήδη αναφερθεί, το Κεφάλαιο 1 παρουσιάζει μια σφαιρική εικόνα της μεταπτυχιακής διατριβής. Στην συνέχεια, το Κεφάλαιο 2 αναφέρεται στην έρευνα που πραγματοποιήθηκε μετά από την ανασκόπηση σε βιβλιογραφικές αναφορές. Στο συγκεκριμένο κεφάλαιο αναφέρονται απόψεις, ορισμοί και συμπεράσματα από συγγραφείς σχετικά με το ρίσκο και τις διάφορες προσεγγίσεις εκτίμησης κινδύνων.

Μετά, το Κεφάλαιο 3 παρουσιάζει την δημιουργία και την εγκατάσταση του δικτύου με ευπάθειες. Η δημιουργία του δικτύου με ευπάθειες αποτελεί σημαντικό σημείο στην μεταπτυχιακή διατριβή. Ο στόχος είναι ο εντοπισμός των ευπαθειών μέσω των αναφορών σάρωσης και την μετέπειτα χρήση τους στον κώδικα της μεθοδολογίας. Επίσης, υπογραμμίζεται η συσχέτιση μεταξύ του ευπαθές δικτύου και διαδικτυακών βάσεων δεδομένων που παρουσιάζουν ενδεικτικές κακόβουλες ενέργειες χρηστών σε ένα οργανισμό.

Έπειτα, στο Κεφάλαιο 4 γίνεται μια περιγραφή των κύριων εργαλείων που έχουν χρησιμοποιηθεί στην μεθοδολογία για εύρεση ευπαθειών: i) «OpenVAS» και ii) «Spyder». Επίσης, παρουσιάζεται μια περιγραφή της εγκατάστασης και της χρήσης των συγκεκριμένων εργαλείων.

Συνεχίζοντας, στο Κεφάλαιο 5 γίνεται μια περιγραφή της μεθοδολογίας που έχει αναπτυχθεί στην μεταπτυχιακή διατριβή καθώς δίνεται και επεξήγηση της μετατροπής της προσέγγισης στην γλώσσα προγραμματισμού «Python». Με αυτόν τον τρόπο δημιουργείται το «Cyber Risk Assessment Box». Ακολούθως, το Κεφάλαιο 6 παρουσιάζει τις δοκιμές που έγιναν στο «Cyber Risk Assessment Box» αλλά και τα αποτελέσματα που έχουν αποκτηθεί.

Τέλος, στο Κεφάλαιο 7 πραγματοποιείται συζήτηση των αποτελεσμάτων, ενώ το Κεφάλαιο 8 παρουσιάζει μια σύνοψη των κύριων σημείων της μεταπτυχιακής διατριβής.

1.3 Εργαλεία και Λογισμικά που Χρησιμοποιήθηκαν

Τα εργαλεία και τα λογισμικά που χρησιμοποιήθηκαν στην μεταπτυχιακή διατριβή είναι:

i. Oracle VM Virtual Box 6.0
ii. Ubuntu Linux - 64
iii. Kali Linux 2020.1 – amd64
iv. OpenVAS
v. Spyder (Python 3.7)
vi. Metasploitable Virtual Machine
vii. Nmap (Kali Linux Environment)

Κεφάλαιο 2

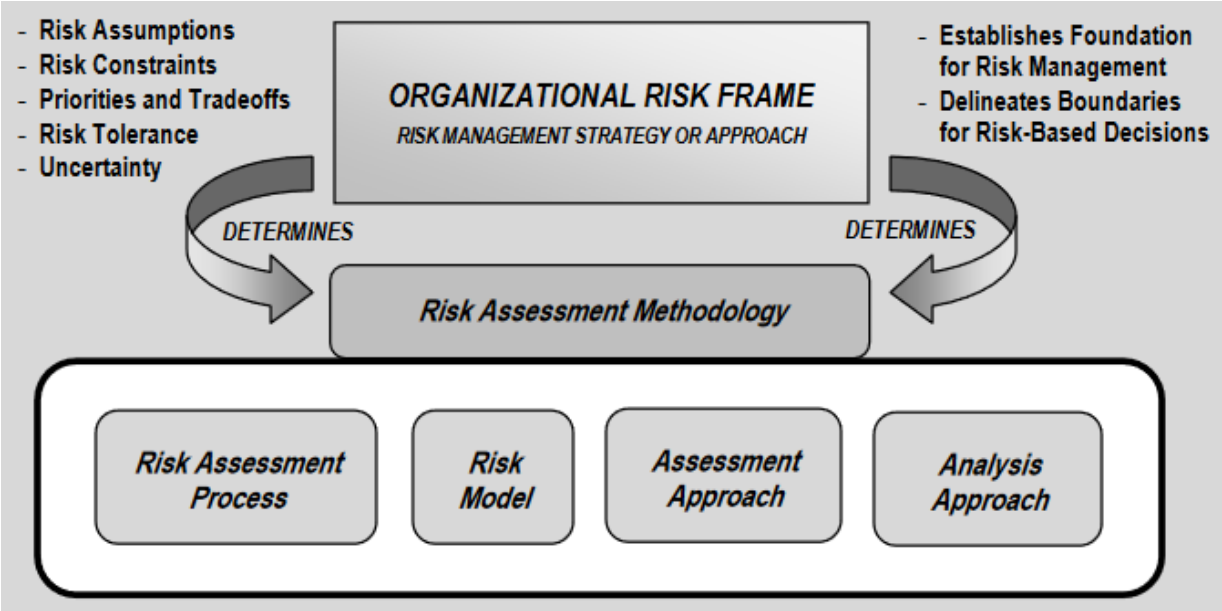
Βιβλιογραφική Επισκόπηση

Σύμφωνα με το πρότυπο NIST (National Institute of Standards and Technology), το ρίσκο είναι μια μονάδα μέτρησης για τον υπολογισμό του βαθμού της απειλής που δέχεται μια οντότητα [11]. Ο βαθμός της απειλής καθορίζεται από δύο παράγοντες: i) το μέγεθος της ζημιάς που μπορεί να προκαλέσει μια συγκεκριμένη απειλή (επίδραση) και ii) οι πιθανότητες αυτής της απειλής να πραγματοποιηθεί. Δηλαδή, το ρίσκο μπορεί να αποτυπωθεί με την εξίσωση: Risk = Impact x Probability (ρίσκο = επίδραση x πιθανότητα).

Επομένως, είναι αναγκαία η διαχείριση του ρίσκου σε ένα οργανισμό έτσι ώστε να μειωθεί ο κίνδυνος υλοποίησης απειλών που θα οδηγήσουν σε προβλήματα και αρνητικά αποτελέσματα. Δηλαδή, να μειωθεί το μέγεθος της απειλής, ή αλλιώς η επίδραση της απειλής και οι πιθανότητες υλοποίησης της απειλής. Ο Ευρωπαϊκός Οργανισμός ENISA (European Union Agency for Cyber Security) υπογραμμίζει ότι η διαχείριση του ρίσκου είναι μια διαδικασία εντοπισμού, ποσοτικού προσδιορισμού και διαχείρισης των ρίσκων (κινδύνων) που αντιμετωπίζει μια οντότητα [09].

Συνεχίζοντας με το πρότυπο NIST [18], όπως φαίνεται και στην πιο κάτω εικόνα 2.1, για να επιτευχθεί μια αποτελεσματική διαχείριση του ρίσκου, θα πρέπει να δημιουργηθεί μια μεθοδολογία αναθεώρησης των ρίσκων όπου θα συμπεριλαμβάνει:

i. Μια κατάλληλη προσέγγιση της διαδικασίας αναθεώρησης των ρίσκων.
ii. Την διαδικασία αναθεώρησης και καταγραφή των ρίσκων.
iii. Ένα μοντέλο για την αποτίμηση των κινδύνων.
iv. Ανάλυση των αποτελεσμάτων.



Εικόνα 2.1: Προσέγγιση Διαχείρισης Ρίσκων [18].

Επομένως, είναι αναγκαία η εφαρμογή μιας κατάλληλης μεθοδολογίας για την διαδικασία διαχείρισης και αναθεώρησης των ρίσκων. Το πρότυπο NIST τονίζει ότι δεν υπάρχει μια συγκεκριμένη μεθοδολογία που ακολουθείται, αφού αυτή πρέπει να είναι κατάλληλη βάση τις ανάγκες του κάθε οργανισμού και οντότητας. Αυτό βρίσκει σύμφωνους και τους Wan Husin κ. ά. [23], που τονίζουν ότι μια κατάλληλη στρατηγική για την διαχείριση των ρίσκων θα οδηγήσει σε θετικά αποτελέσματα. Άρα, είναι αναγκαία μια συστηματική προσέγγιση για την διαχείριση των κινδύνων με σκοπό να απομακρυνθούν οι πιθανότητες υλοποίησης των απειλών [17].

Στον χώρο της ασφάλειας πληροφοριακών συστημάτων, οι συγγραφείς Diesch κ. ά. [08] τονίζουν ότι τα στοιχεία που μπορεί να αποτελέσουν μια απειλή στον οργανισμό δεν είναι μόνο τεχνικά και επομένως χρειάζεται μια πιο ολοκληρωμένη προσέγγιση σχετικά με την υιοθέτηση μιας αποτελεσματικής στρατηγικής. Για την εφαρμογή μιας σωστής στρατηγικής για την διαχείριση των ρίσκων θα πρέπει πρώτα να καταγραφούν τα αγαθά μιας οντότητας/οργανισμού που θα πρέπει να προστατευτούν. Ακολούθως, οι πιθανές απειλές και οι ευπάθειες που αποτελούν το σημείο εκμετάλλευσης. Τέλος, είναι αναγκαίο να σημειωθούν τα μέτρα αντιμετώπισης των απειλών [22]. Σύμφωνα με τους συγγραφείς Saleh και Alfantookh [22], ένα αγαθό ορίζεται οτιδήποτε έχει αξία στην συγκεκριμένη οντότητα. Τα αγαθά κατηγοριοποιούνται σε χειροπιαστά (tangible) και άυλα (intangible) όπως φαίνεται και στην εικόνα 2.2. Οι συγγραφείς στηρίζουν τις απόψεις τους βάση του Διεθνή Οργανισμού Τυποποίησης (International Organization for Standardization, ISO) που αναπτύσσει πρότυπα για την διασφάλιση της ποιότητας και της ασφάλειας των προϊόντων, υπηρεσιών και των συστημάτων [02].

Assets main groups	
Tangible (*Examples*)	Intangible
Information: (*Policy document*)	– Goodwill
Information: (*Data files*)	– Service to clients
IT services: (*Messaging-active directory*)	– Public confidence
Software: System (*Solaris*), Application (*Oracle*),	– Public trust
Utilities (management tools)	– Competitive advantage
Hardware: Hosts (*Servers*) other (*Printers*)	– Image of the organization
Communication: Network (*Routers*), (*Cable*)	– Reputation
Documents: (*Management commitment*)	– Trust in services
Agreements: (*Confidentiality-third party*)	– Employee moral
Information: (*Research*)	– Productivity
Other: (*User manuals-training material*)	– Loyalty
IT staff: (*IT security manager*)	– Ethics
Employee: (*Senior management*)	
Users: (*Inside/Outside*)	
Contractors:(*Consultants*)	
Owners:(*Stakeholders*)	
Services: (*Heating-lighting-power-AC*)	
Equipment: (*Desks-Fax machines-Cables*)	
Physical (infrastructure): (*Offices-facilities*)	

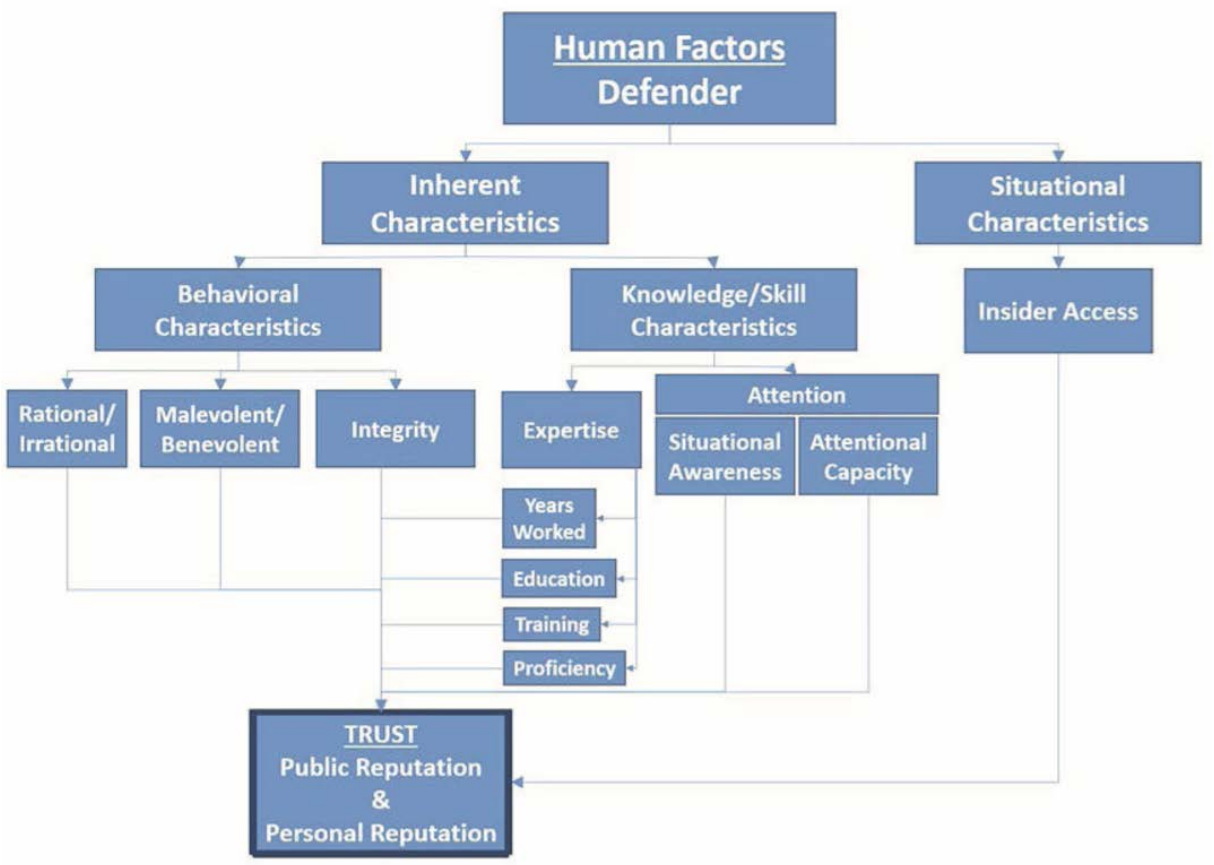
Εικόνα 2.2: Κατηγορίες Αγαθών [22].

Βάση της εικόνας 2.2, εκτός από τα εμφανή αγαθά που φαίνεται να επηρεάζουν ένα οργανισμό, όπως τα δεδομένα, οι υπηρεσίες, τα λογισμικά, ο εξοπλισμός, τα έγγραφα, οι υπάλληλοι, υπάρχουν και σημαντικά αγαθά όπως καλή θέληση, ηθική, φήμη, εμπιστοσύνη, παραγωγικότητα. Επομένως, μια αποτελεσματική στρατηγική διαχείρισης των ρίσκων θα πρέπει να λάβει υπόψη και τον ανθρώπινο παράγοντα. Δηλαδή, την ψυχολογία και την συμπεριφορά του ανθρώπου που επηρεάζει άμεσα την παραγωγικότητα και την εμπιστοσύνη σε ένα οργανισμό. Επίσης, οι υπηρεσίες ενός οργανισμού μπορεί να επηρεαστούν αρνητικά αν τα ανθρώπινα χαρακτηριστικά που παρουσιάζει ένας χρήστης δεν είναι τα επιθυμητά. Ακόμη, αυτό ίσως αποτελέσει και αρνητικό αντίκτυπο στην εικόνα του οργανισμού. Επιπλέων, ηθικοί παράγοντες μπορεί να οδηγήσουν και σε διάφορες νομικές επιπτώσεις, για παράδειγμα, διαρροή προσωπικών δεδομένων πελατών ενός οργανισμού. Οι συγγραφείς Diesch, Pfaff και Krcmar [08] αναφέρουν ότι ένας οργανισμός μπορεί να έχει οικονομικές και νομικές επιπτώσεις, καθώς και επιπτώσεις στην εικόνα του.

Σύμφωνα με τους συγγραφείς Oltramari κ. ά. [19], οι ενέργειες ενός ανθρώπου καθορίζονται από τα περιστασιακά χαρακτηριστικά του, το επίπεδο της γνώσης του, τις ικανότητές του, καθώς και την συμπεριφορά του. Έτσι, οι συγγραφείς στηρίζουν την ιδέα τους για την δημιουργία ενός μοντέλου για την εκτίμηση κινδύνων και μείωση των ρίσκων, βάση του στοιχείου της εμπιστοσύνης. Επομένως, όταν μια οντότητα δείχνει εμπιστοσύνη σε ένα αγαθό (ανθρώπινο

παράγοντα) σημαίνει ότι τα χαρακτηριστικά του, η γνώση του, οι ικανότητες του και η συμπεριφορά του είναι στα ιδανικά επίπεδα για να μειωθεί το ρίσκο υλοποίησης μιας απειλής. Αυτό φαίνεται να στηρίζεται και από την εικόνα 2.2, όπου διακρίνεται ο παράγοντας της εμπιστοσύνης στα άυλα αγαθά. Άρα, τονίζεται η κρισιμότητα του ανθρώπινου παράγοντα σε μια στρατηγική εκτίμησης των κινδύνων.

Οι συγγραφείς Henshel κ. ά. [14] υπογραμμίζουν ότι τα ανθρώπινα χαρακτηριστικά είναι πολύ σημαντικά στοιχεία στην διαδικασία εκτίμησης κινδύνων. Επίσης, τονίζουν ότι καταλήγουν στον παράγοντα της εμπιστοσύνης όπως έχουν αναφέρει και οι συγγραφείς Oltramari κ. ά. [19]. Η άποψη των συγγραφέων Henshel κ. ά. [14] αποτυπώνεται στο σχεδιάγραμμα που δημιουργήσαν στην εικόνα 2.3. Στην συγκεκριμένη εικόνα διακρίνονται τα κύρια ανθρώπινα χαρακτηριστικά που έχουν την δυνατότητα να επηρεάσουν το μέγεθος του ρίσκου σε ένα οργανισμό.



Εικόνα 2.3: Ανθρώπινοι Παράγοντες και Ανθρώπινα Χαρακτηριστικά [14].

Επιπλέων, όπως φαίνεται και στην πιο πάνω εικόνα 2.3, τονίζεται και το στοιχείο της συμπεριφοράς του ανθρώπου. Ένα στοιχείο όπου δείχνει στο τέλος να επηρεάζει και την

εμπιστοσύνη που επικρατεί σε ένα οργανισμό. Η ιδέα αυτή ενισχύεται και στην δημοσίευση του ENISA «White Paper» [10], όπου υπογραμμίζεται ότι η συμπεριφορά του κάθε ανθρώπου αποτελεί ένα σημαντικό παράγοντα που επηρεάζει τον οργανισμό και ιδιαίτερα το κομμάτι της ασφάλειας των υπολογιστικών συστημάτων. Για παράδειγμα, το κίνητρο είναι ένα στοιχείο που επηρεάζει την συμπεριφορά ενός ανθρώπου. Επομένως, ένας εργαζόμενος χωρίς κάποιο κίνητρο να είναι ιδιαίτερα παραγωγικός, έχει ως συνέπεια την μείωση των επιπέδων παραγωγικότητας στον οργανισμό όπου ανήκει. Επίσης, διατηρώντας τα επίπεδα του κίνητρου σε υψηλά επίπεδα, ο εργαζόμενος θα νοιάζεται περισσότερο για τον οργανισμό. Αυτό θα έχει σαν αποτέλεσμα να είναι πιο προσεκτικός ώστε να μειωθούν οι πιθανότητες υλοποίησης μιας επιτυχημένης επίθεσης στον οργανισμό.

Σύμφωνα με το ENISA «White Paper» [10], κάποιες πιθανές κακόβουλες επιθέσεις είναι το «phishing» και το «social engineering». Οι συγκεκριμένες επιθέσεις στοχεύουν στην αδυναμία του ανθρώπου να εντοπίσει τις συγκεκριμένες απειλές λόγω μη επαρκής εμπειρίας, εκπαίδευσης ή γνώσεων. Επομένως, τονίζεται ότι τα ανθρώπινα χαρακτηριστικά όπως παρουσιάζονται και στην εικόνα 2.3, μπορεί να αποτελέσουν σημαντικό παράγοντα στην αποτροπή ή υλοποίηση κακόβουλων επιθέσεων.

Ακόμη, τονίζεται ότι δεν είναι αρκετό να «διορθωθεί ένας άνθρωπος», αν δεν διορθωθεί το σύστημα [10]. Επομένως, είναι εμφανές ότι το στοιχείο της ανθρώπινης συμπεριφοράς είναι αναγκαίο να συμπεριληφθεί στον υπολογισμό του ρίσκου.

Συνεχίζοντας στο κομμάτι της ανθρώπινης συμπεριφοράς και σύμφωνα με τους Greitzer και Hohimer [12] τα πιο κάτω αποτελούν κάποια από τα «σήματα» για τον εντοπισμό απειλών από το εσωτερικό περιβάλλον ενός οργανισμού:

i. Ερωτήματα σε διαδικτυακές μηχανές αναζητήσεων (Search engine queries).
ii. Πρόσβαση σε ιστοσελίδες (Internet sites accessed).
iii. Αρχεία καταγραφής συμβάντων (Firewall logs, host event logs, network print logs).
iv. Υπογραφές γνωστών λογισμικών (Known software signature).
v. Πρόσβαση σε λογαριασμούς (Access to account).
vi. Εγκατάσταση εφαρμογών (Applications installed).
vii. Τοπικά αποθηκευμένα ή προσωρινά αποθηκευμένα αρχεία (Local stored or cached files).

Όπως φαίνεται πιο πάνω, τα συγκεκριμένα στοιχεία τα οποία αναφέρουν οι συγγραφείς τονίζουν την αναγκαιότητα της χρήσης ειδικών συστημάτων παρακολούθησης για τον εντοπισμό εσωτερικών απειλών. Οι συγγραφείς εξηγούν ότι η συλλογή δεδομένων οδηγεί στην παρατήρηση κάποιων μοτίβων που με την σειρά τους αποτελούν ενδείξεις. Αυτό χαρακτηρίζει την συμπεριφορά ενός ανθρώπου που ίσως οδηγήσει στην εκμετάλλευση των ευπαθειών για υλοποίηση μιας επιτυχημένης επίθεσης.

Η κρισιμότητα του ανθρώπινου παράγοντα σε μια στρατηγική εκτίμησης των κινδύνων φαίνεται και στον πιο κάτω πίνακα 2.1, ο οποίος απεικονίζει τις πιθανές απειλές και ευπάθειες σε ένα οργανισμό, τις οποίες αναφέρουν και οι συγγραφείς Saleh και Alfantookh [22]. Είναι εμφανές λοιπόν ότι κάποιες από τις κύριες απειλές στον χώρο της ασφάλειας πληροφοριακών συστημάτων είναι οι εσωτερικές απειλές από υπαλλήλους και το σαμποτάζ. Επομένως, τονίζεται η ανάγκη της εκτίμησης των ρίσκων συμπεριλαμβανομένου και του ανθρώπινου παράγοντα.

Απειλές	**Ευπάθειες**
Κακόβουλα Λογισμικά	- Όχι συχνή αναβάθμιση των συστημάτων και λογισμικών. - Απουσία λογισμικών anti-virus.
Προβλήματα στον Εξοπλισμό	- Ανεπαρκές «Patching».
Λάθος Διαδικασίες και Σχεδιασμός	- Απουσία εγγράφων και καταγραφή γεγονότων.
Ανεπαρκείς Πολιτικές Ασφαλείας	- Απουσία εγγράφων και αναβάθμιση της πολιτικής ασφαλείας.
Εσωτερικές Απειλές από Υπαλλήλους και Σαμποτάζ	- Ανεπαρκής εκπαίδευση προσωπικού και χαμηλό ηθικό υπαλλήλων.

Εξωτερικές Απειλές (Hackers)	- Ανεπαρκής εκπαίδευση προσωπικού και μη επαρκή συστήματα ασφαλείας (Firewall, IDS).
Φυσικές Απειλές	- Μη ύπαρξη σχεδίου «Disaster Recovery Plan» για φυσικές καταστροφές. - Απουσία φρουρών και καμερών ασφαλείας για παράνομη πρόσβαση στις εγκαταστάσεις ενός οργανισμού.

Πίνακας 2.1: Απειλές και Ευπάθειες στον Χώρο της Ασφάλειας Πληροφοριακών Συστημάτων.

Επιπλέων, οι συγγραφείς Saleh και Alfantookh [22], παρουσιάζουν στην εικόνα 2.4, έξι μεθοδολογίες που μπορούν να υιοθετηθούν με σκοπό την διαχείριση των ρίσκων και την μείωση του μεγέθους της ζημιάς ή/και την πιθανότητα υλοποίησης των πιο πάνω απειλών.

	AS/NZS: 4360	ISO/IEC TR 13335-3	NIST 800-30	OCTAVE	CRAMM	Microsoft
Define	Communicate and consult	Risk analysis	System characterizations	Knowledge of management–operational area–staff	Asset identification	
	Establish the context			Create threat profile		
Measure	Identify risks		Threat identification	Identify key components	Asset valuation	
			Vulnerability identification	Evaluate selected components	Threat and vulnerability assessment	
Analyze	Analyze risk		Control analysis			Assessing risk
			Likelihood determination			
	Evaluate risk		Impact analysis			
			Risk determination			
Improve	Treat risk	Safeguards selection	Recommended controls	Develop protection strategy	Countermeasure selection and recommendation	Conducting decision support
		Policy and plan implementation	Risk assessment report			
			Cost-benefit analysis and selection of controls			Implement controls
			Implementation			
Control	Monitor and review	Follow-up	Test and evaluate			Measuring risk management program effectiveness

Εικόνα 2.4: Μεθοδολογίες για την Διαχείριση των Ρίσκων και Εκτίμηση των Κινδύνων [22].

Συνεχίζοντας, οι συγγραφείς Radanliev, P. et al. [20], προσθέτουν τις ακόλουθες μεθοδολογίες για την εκτίμηση των κινδύνων οι οποίες μπορούν να χρησιμοποιηθούν σαν βάση στην στρατηγική που ακολουθεί μια οντότητα για την μείωση των απειλών:

i. Return on Investment (ROI)
ii. Net Present Value (NPV)
iii. Strength Weaknesses Opportunities Threats (SWOT) Analysis
iv. Threat Agent Risk Assessment (TARA)
v. Common Vulnerability Scoring System (CVSS)
vi. Capability Maturity Model Integration (CMMI)
vii. Factor Analysis of Information Risk (FAIR)
viii. Cyber Value at Risk (CyVaR) Model – Monte Carlo Simulations

Επομένως, βάση των πιο πάνω πληροφοριών, έχει διατυπωθεί μια νέα προσέγγιση για τον υπολογισμό του ρίσκου. Έτσι, το «Cyber Risk Assessment Box» πραγματοποιεί τον υπολογισμό του ρίσκου σε μια οντότητα λαμβάνοντας υπόψη όχι μόνο τις ευπάθειες στα πληροφοριακά συστήματα αλλά και τον πολύπλευρο ανθρώπινο παράγοντα. Δηλαδή, τα ανθρώπινα χαρακτηριστικά και την ανθρώπινη συμπεριφορά.

Κεφάλαιο 3

Δίκτυο με Ευπάθειες και Διαδικτυακές Βάσεις Δεδομένων

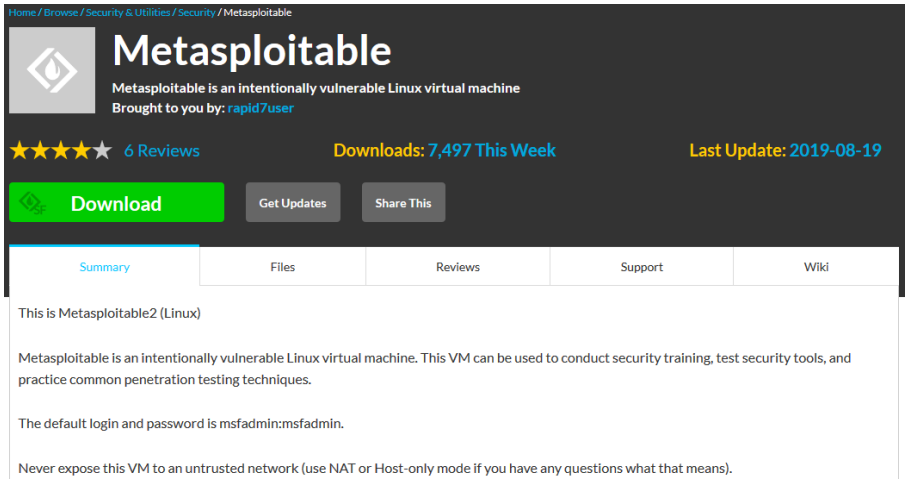
Στο Κεφάλαιο 3 πραγματοποιείται η περιγραφή της δημιουργίας του δικτύου με ευπάθειες. Όπως έχει αναφερθεί, το ευπαθές δίκτυο αποτελεί σημαντικό σημείο στην μεθοδολογία της μεταπτυχιακής διατριβής. Επομένως, γίνεται αναφορά στον σκοπό της δημιουργίας του αλλά και τα βήματα που πραγματοποιήθηκαν για την σωστή λειτουργία του στην μεθοδολογία. Ακολούθως, παρουσιάζεται η συσχέτιση μεταξύ του δικτύου με ευπάθειες και διαδικτυακών βάσεων δεδομένων που έχουν συμπεριληφθεί στην μεθοδολογία με σκοπό να προσομοιάζουν ένα σύνολο δεδομένων με κακόβουλες ενέργειες χρηστών σε ένα οργανισμό.

3.1 Σκοπός Δημιουργίας Δικτύου με Ευπάθειες

Το συγκεκριμένο δίκτυο έχει δημιουργηθεί έτσι ώστε να προσομοιάζει ένα δίκτυο σε ένα οργανισμό με διάφορες ευπάθειες. Ο σκοπός είναι η παραγωγή μιας αναφοράς με ευπάθειες μετά από την χρήση του εργαλείου OpenVAS για σάρωση ευπαθειών. Επομένως, παρουσιάζεται μια διαδικασία για εντοπισμών ευπαθειών που μπορεί να υιοθετήσει ένας οργανισμός ως μέτρο πρόληψης στο πλαίσιο της πολιτικής ασφαλείας που ακολουθά.

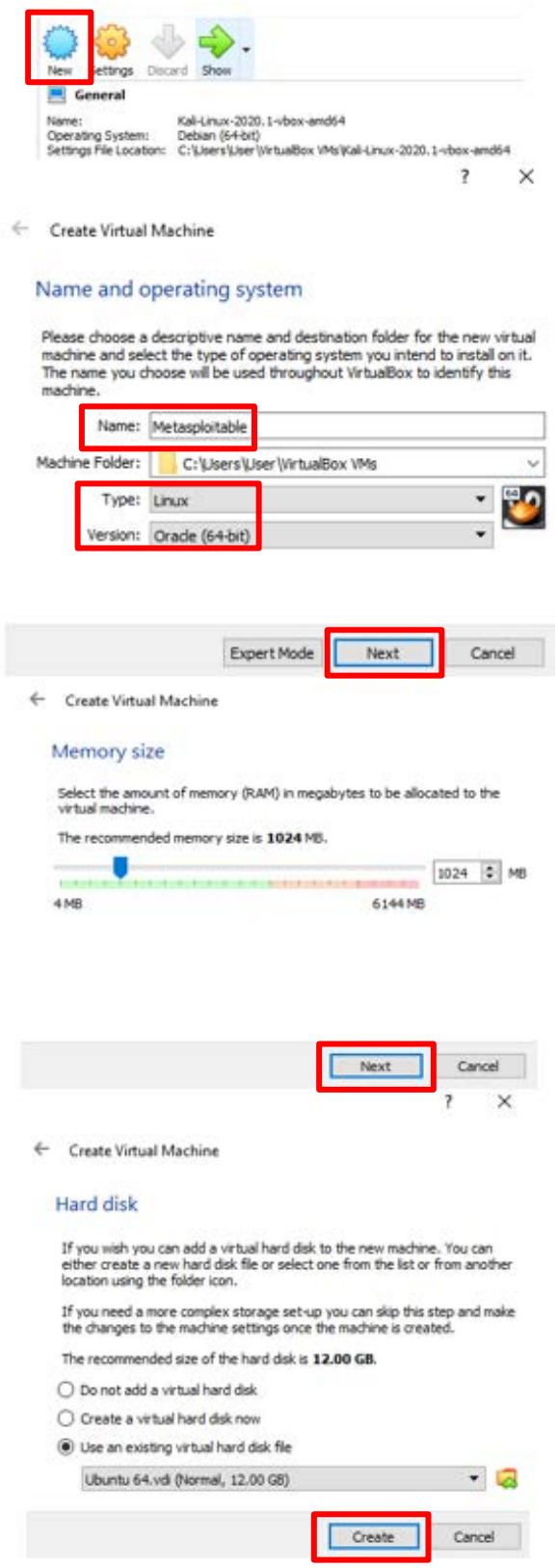
3.2 Εγκατάσταση και Λειτουργία Εικονικής Μηχανής «Metasploitable».

Πρώτα, ακολουθώντας τον σύνδεσμο της ιστοσελίδας «sourceforge.net» [03] γίνεται η λήψη της εικονικής μηχανής «Metasploitable» για το λογισμικό Kali-Linux (Εικόνα 3.1). Η συγκεκριμένη εικονική μηχανή περιέχει ευπάθειες για σκοπούς εκπαίδευσης.



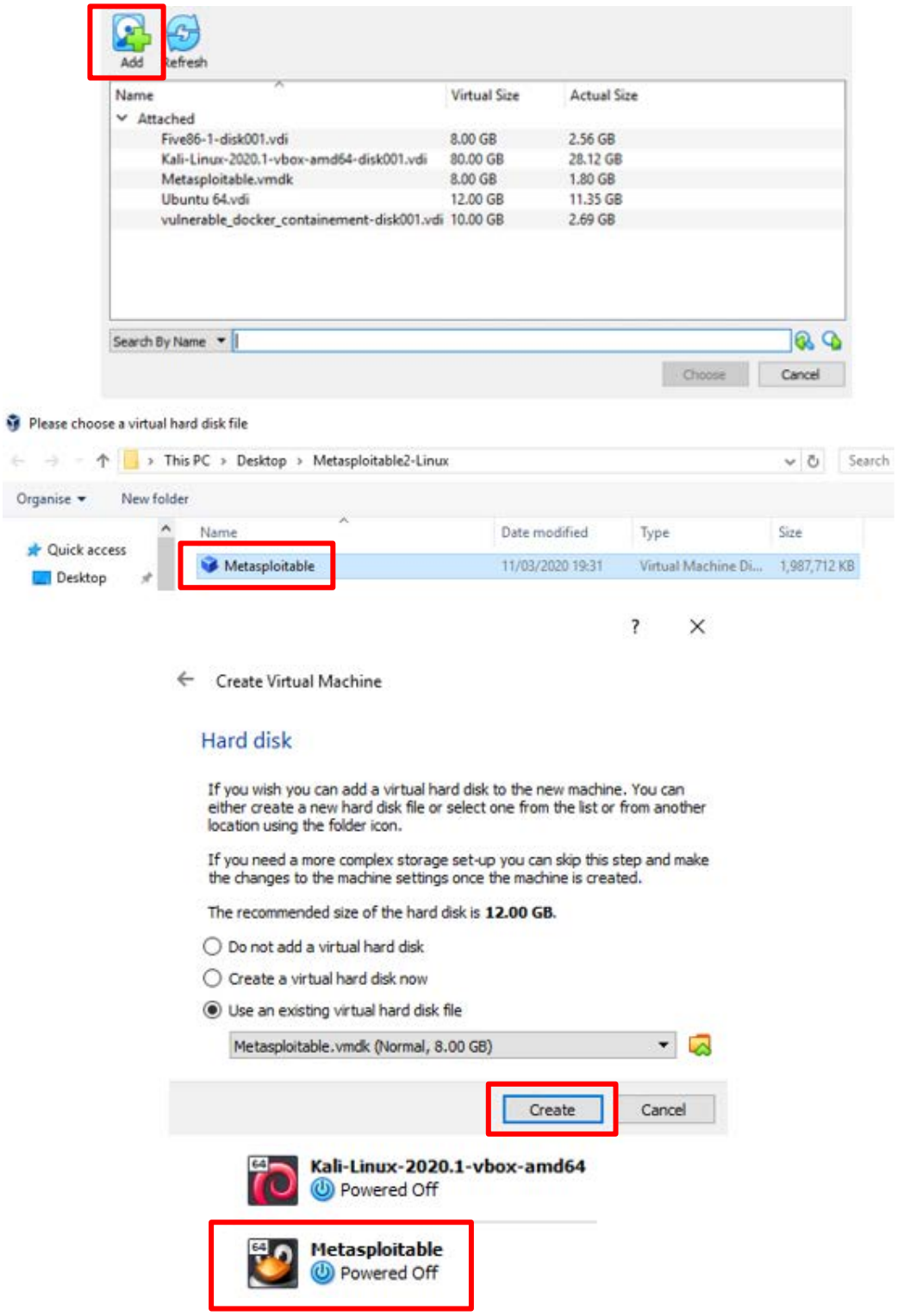
Εικόνα 3.1: Λήψη της Εικονικής Μηχανής «Metasploitable» [03].

Στην συνέχεια, σύμφωνα με τα βήματα που διακρίνονται στην εικόνα 3.2, γίνεται δημιουργία του λειτουργικού λογισμικού για την εικονική μηχανή «Metasploitable» στο Oracle VM Virtual Box. Το περιβάλλον που έχει δημιουργηθεί για την εικονική μηχανή είναι Ubuntu – Linux.



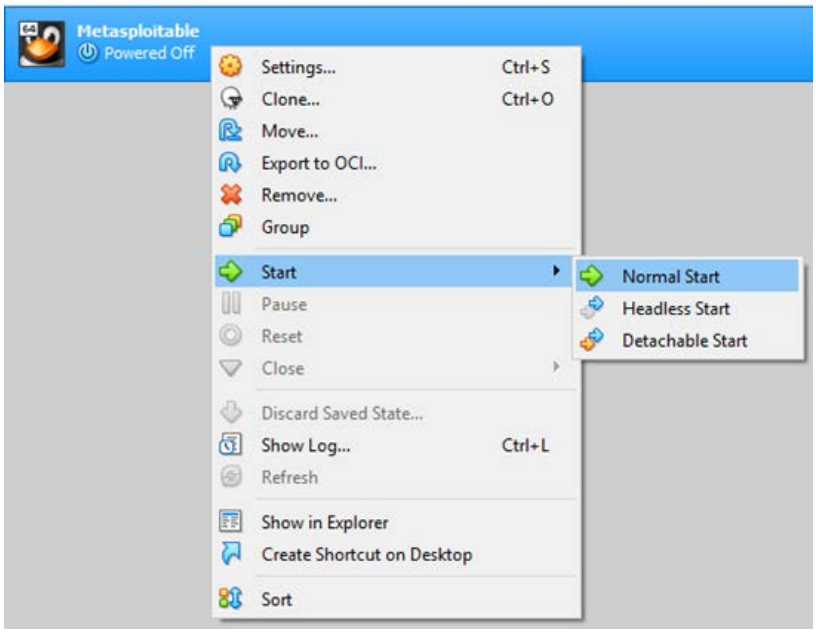
Εικόνα 3.2: Δημιουργία Λειτουργικού Λογισμικού Ubuntu - Linux για το Metasploitable στο Oracle VM Virtual Box.

Ακολούθως, γίνεται η εγκατάσταση της εικονικής μηχανής «Metasploitable» στο περιβάλλον που έχει δημιουργηθεί (Ubuntu - Linux). Η εικόνα 3.3 παρουσιάζει τα βήματα για την εγκατάσταση της εικονικής μηχανής.



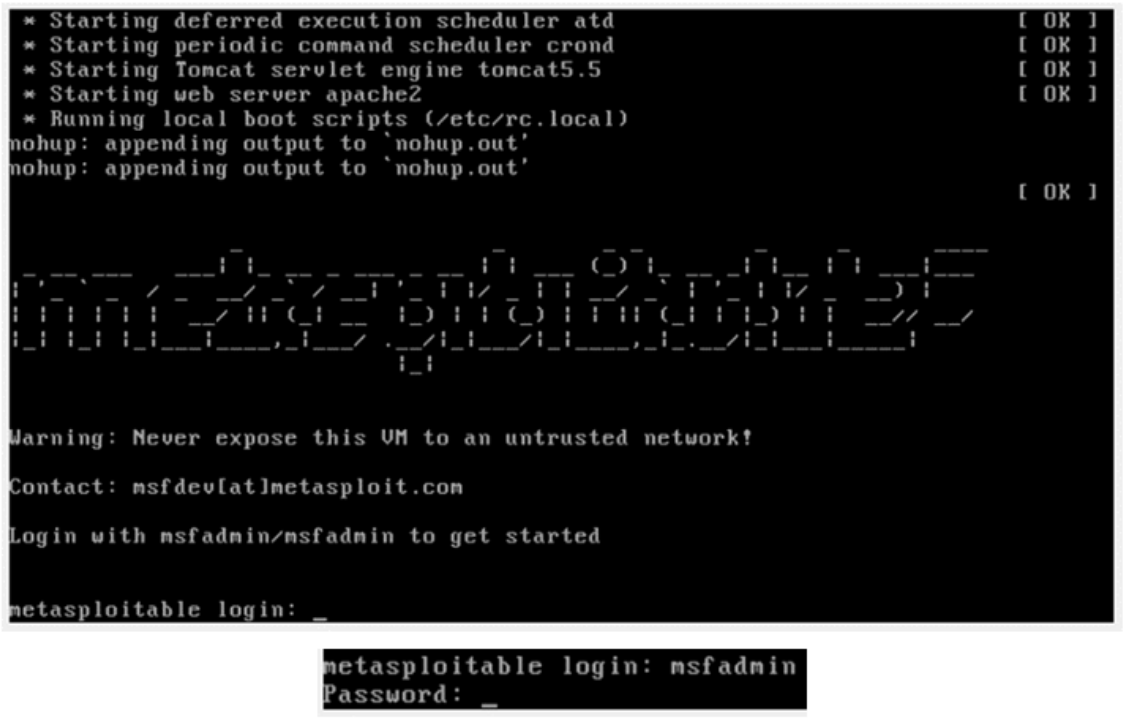
Εικόνα 3.3: Δημιουργία Λειτουργικού Λογισμικού Linux για το Metasploitable στο Oracle VM Virtual Box.

Στην συνέχεια, όπως φαίνεται και στην εικόνα 3.4, γίνεται εκκίνηση της εικονικής μηχανής «Metasploitable».



Εικόνα 3.4: Εκκίνηση της Εικονικής Μηχανής Metasploitable.

Έπειτα, για την λειτουργία της εικονικής μηχανής «Metasploitable», γίνεται η τοποθέτηση του ονόματος και του κωδικού χρήστη: **msfadmin,** όπως φαίνεται και στην εικόνα 3.5.

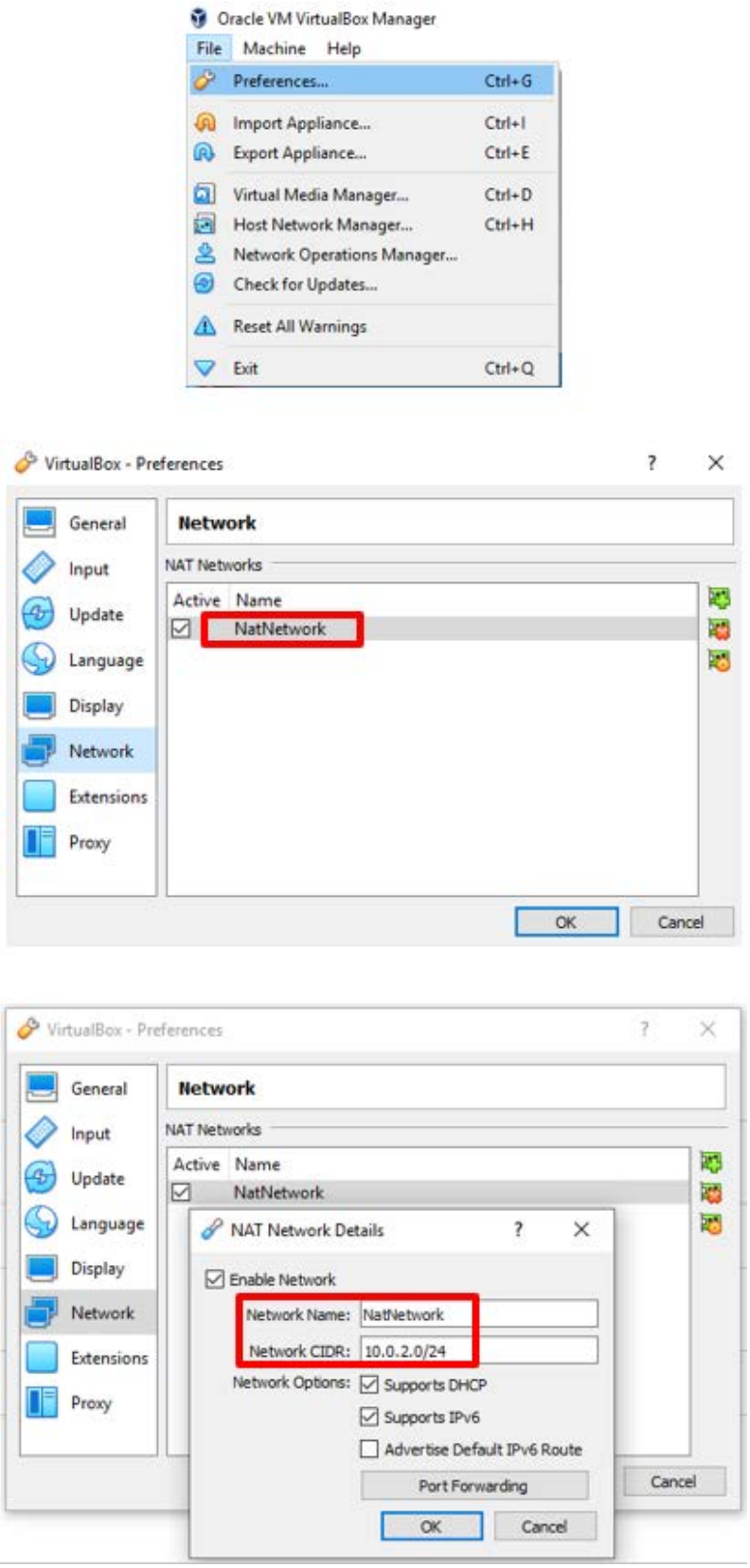


Εικόνα 3.5: Τοποθέτηση του Ονόματος και του Κωδικού Χρήστη στην Εικονική Μηχανή Metasploitable.

3.3 Δημιουργία Δικτύου με Ευπάθειες και Σύνδεση Εικονικών Μηχανών

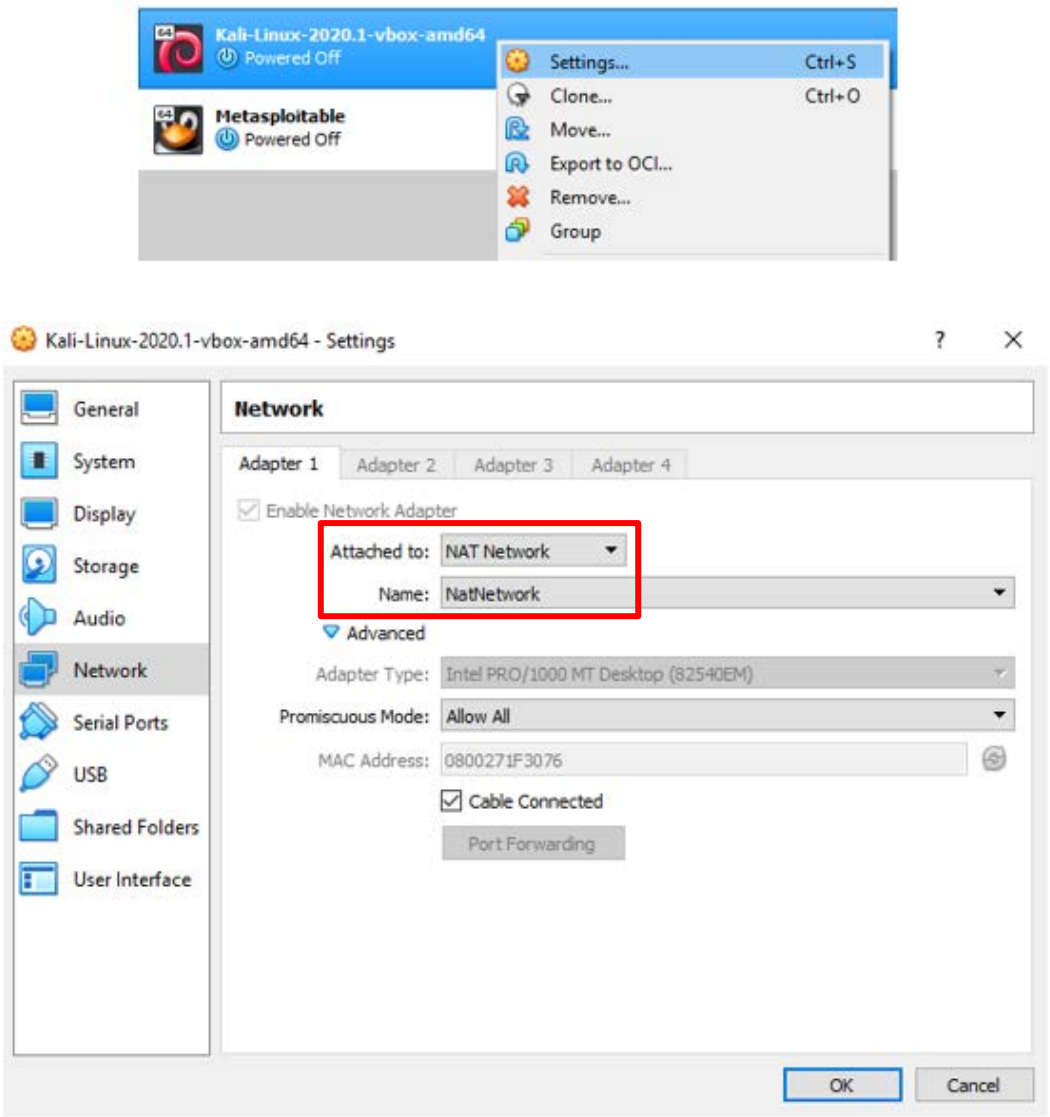
Για την δημιουργία ενός κοινού δικτύου με ευπάθειες είναι αναγκαία η παράλληλη λειτουργία της εικονικής μηχανής «Metasploitable» με το λειτουργικό λογισμικό Kali-Linux, στο οποίο είναι εγκατεστημένο το εργαλείο «OpenVAS». Αυτό θα επιτρέπει την σάρωση ευπαθειών στο ίδιο δίκτυο. Επίσης, είναι αναγκαία η ρύθμιση των δύο αυτών εικονικών μηχανών που θα τρέχουν παράλληλα έτσι ώστε να βρίσκονται στο ίδιο εύρος IP διευθύνσεων.

Η εικόνα 3.6 παρουσιάζει τα βήματα στις ρυθμίσεις του «Oracle VM Virtual Box» για την δημιουργία ενός δικτύου με ευπάθειες. Το συγκεκριμένο δίκτυο έχει ονομαστεί «NatNetwork» και θα καλύπτει το εύρος των IP διευθύνσεων **10.0.2.0/24.**



Εικόνα 3.6: Δημιουργία Δικτύου με Ευπάθειες στο Oracle VM Virtual Box.

Τέλος, βάση της εικόνας 3.7, οι δύο εικονικές μηχανές Kali-Linux και «Metasploitable» συνδέονται μεταξύ τους, τοποθετώντας στις ρυθμίσεις τους το δίκτυο που έχει δημιουργηθεί: **NatNetwork**. Με αυτό τον τρόπο έχει δημιουργηθεί ένα δίκτυο με ευπάθειες στο οποίο οι δύο εικονικές μηχανές επικοινωνούν μεταξύ τους.



Εικόνα 3.7: Σύνδεση Εικονικών Μηχανών στο Ευπαθές Δίκτυο.

3.4 Σάρωση Δικτύου και Εύρεση Ευπαθειών

Για να διεκπεραιωθεί ο στόχος της συγκεκριμένης ενότητας και για την σωστή λειτουργία του εργαλείου «OpenVAS», θα πρέπει να γίνει ξανά ενημέρωση σχετικά με τις τελευταίες ευπάθειες που έχουν εντοπιστεί και έχουν προστεθεί στις βάσεις δεδομένων του εργαλείου. Επομένως, γίνεται χρήση της εντολής **sudo openvas-setup** στο τερματικό του λογισμικού Kali-Linux.

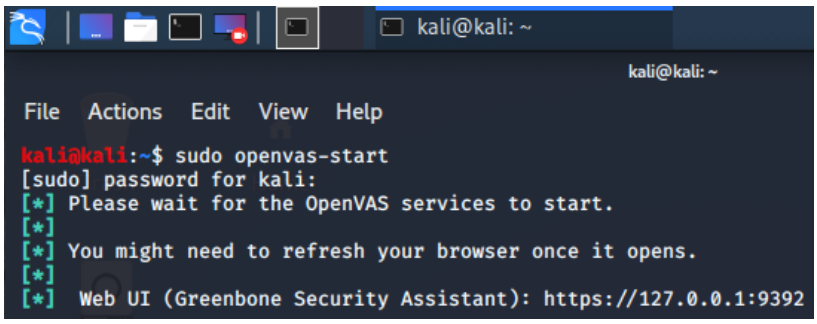
Ακολούθως, γίνεται χρήση του NMAP, ένα εργαλείο το οποίο είναι δωρεάν και ανοικτού κώδικα στα λογισμικά Kali-Linux [05]. Το συγκεκριμένο εργαλείο επιτρέπει στον χρήστη, μέσω εντολών από το τερματικό, να πραγματοποιεί σάρωση δικτύου για εντοπισμό ενεργών IP διευθύνσεων.

Επομένως, χρησιμοποιώντας την εντολή **nmap -sn -Oa nmap 10.0.2.0/24** όπως φαίνεται και στην εικόνα 3.8, γίνεται σάρωση του δικτύου που έχει δημιουργηθεί στην Ενότητα 3.3 για εντοπισμό IP διευθύνσεων των εξυπηρετητών (IP Hosts).

```
kali@kali:~$ nmap -sn -oA nmap 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-11 10:00 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00052s latency).
Nmap scan report for 10.0.2.5
Host is up (0.00060s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00010s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.66 seconds
```

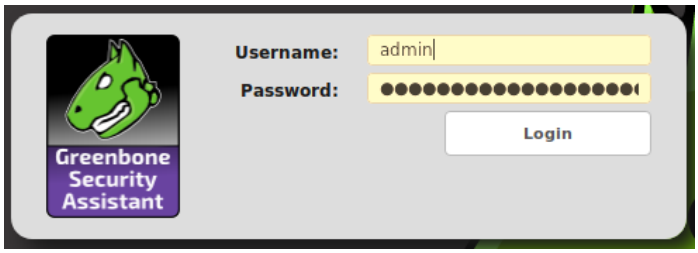
Εικόνα 3.8: Σάρωση Δικτύου 10.0.2.0/24 για Εντοπισμό Διευθύνσεων Εξυπηρετητών (IP Hosts).

Στην συνέχεια, χρησιμοποιώντας την εντολή **sudo openvas-start** γίνεται η εκκίνηση του εργαλείου «OpenVAS». Επίσης είναι αναγκαία η εισαγωγή του κωδικού «sudo». Αυτό φαίνεται στην πιο κάτω εικόνα 3.9.



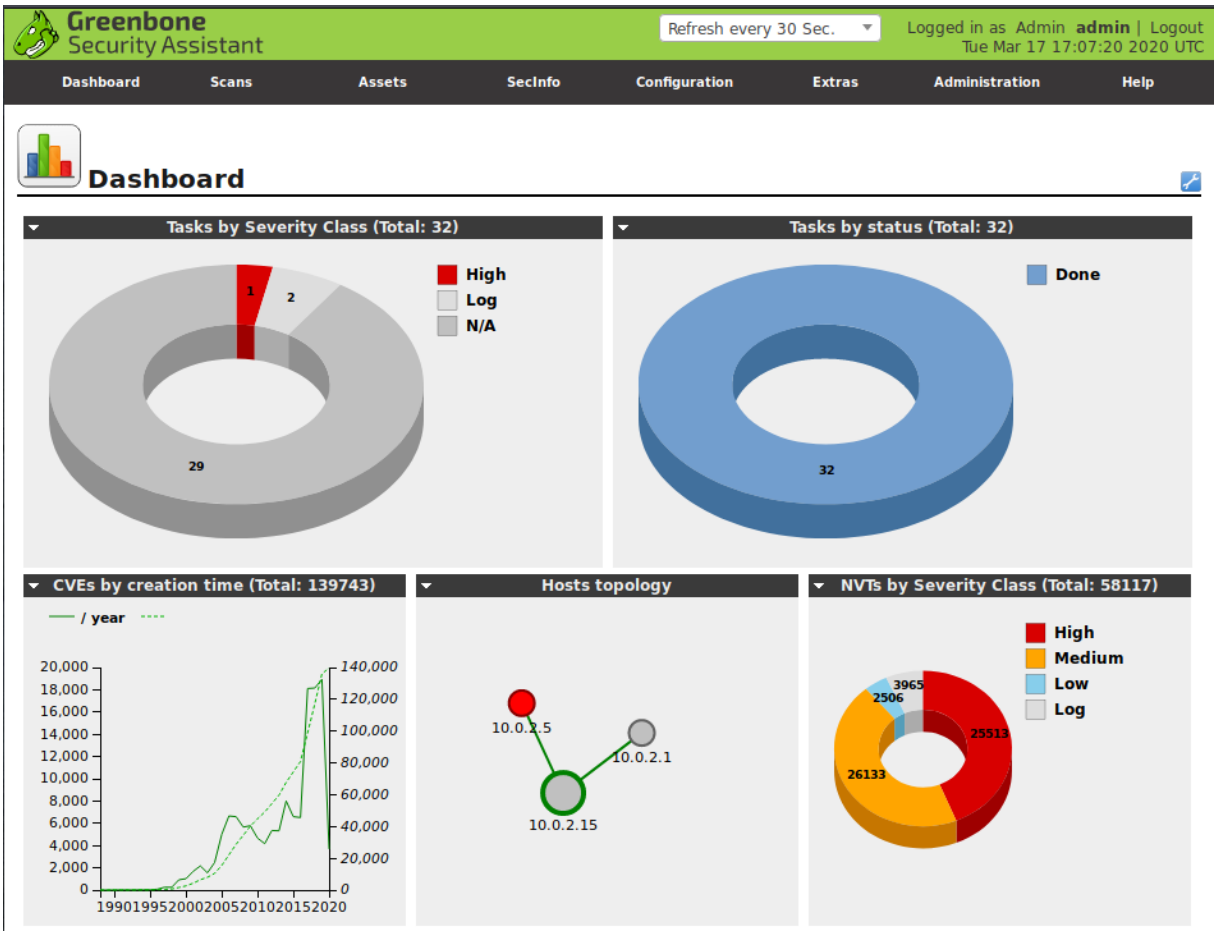
Εικόνα 3.9: Εντολή Εκκίνησης του Εργαλείου OpenVAS.

Όπως φαίνεται και στην πιο πάνω εικόνα 3.9, το εργαλείο μας οδηγεί στην ιστοσελίδα **https://127.0.0.1:9392**. Επομένως, η πρόσβαση και η χρήση του εργαλείου πραγματοποιείται από την συγκεκριμένη διαδικτυακή πύλη. Η εικόνα 3.10 παρουσιάζει το παράθυρο τοποθέτησης των στοιχείων του χρήστη.



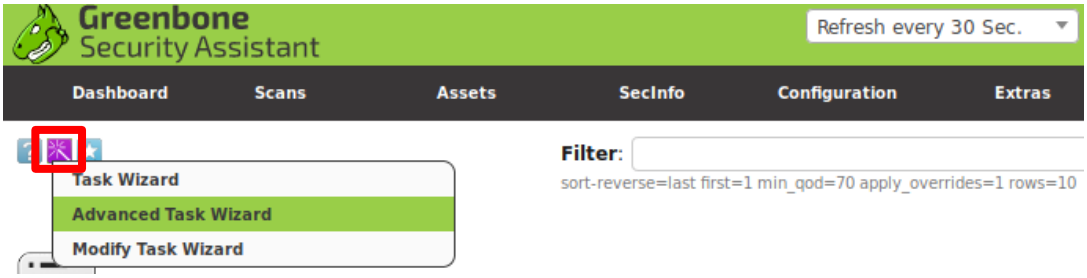
Εικόνα 3.10: Παράθυρο Τοποθέτησης των Στοιχείων του Χρήστη στην Διαδικτυακή Πύλη του OpenVAS.

Συνεχίζοντας, ο χρήστης αποκτά πρόσβαση στον αρχικό πίνακα λειτουργιών του «OpenVAS» (Εικόνα 3.11).



Εικόνα 3.11: Αρχικός Πίνακας Λειτουργιών του OpenVAS.

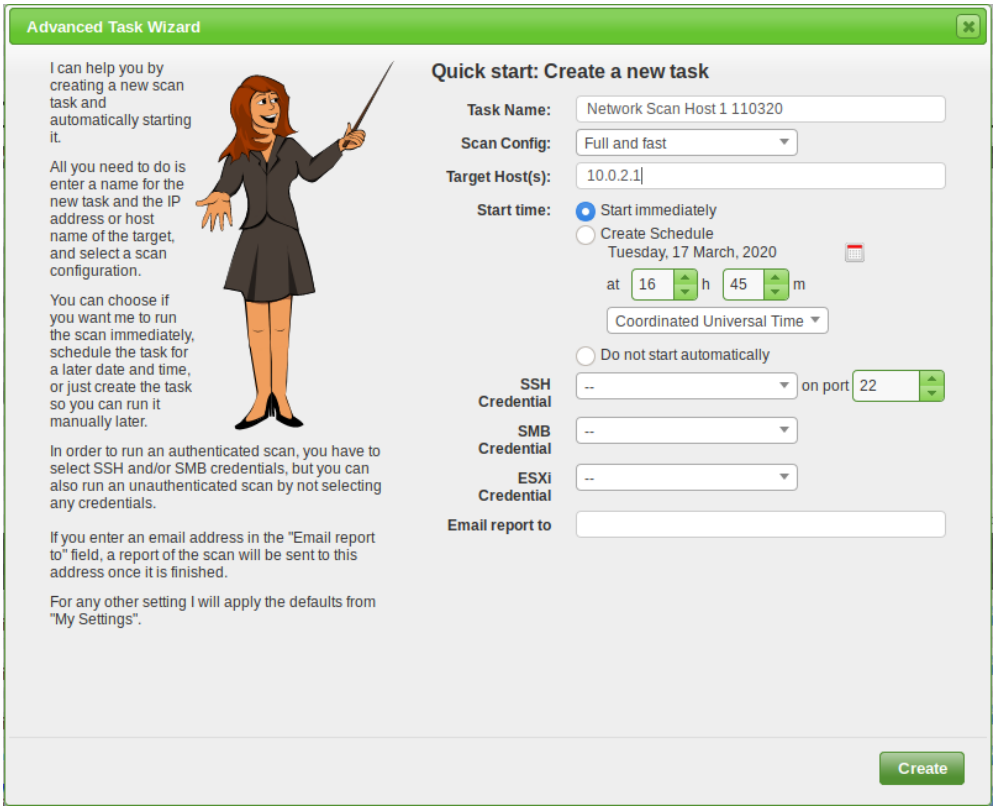
Ακολούθως, όπως διακρίνεται και στην πιο κάτω εικόνα 3.12, παρουσιάζεται η επιλογή στο εργαλείο «OpenVAS» που οδηγεί στην σάρωση ευπαθειών στο δίκτυο που έχει δημιουργηθεί.



Εικόνα 3.12: Αρχικός Πίνακας Λειτουργιών. Επιλογή Advanced Task Wizard.

Επίσης, όπως διακρίνεται και στην πιο κάτω εικόνα 3.13, γίνεται η τοποθέτηση των IP διευθύνσεων για την σάρωση εξυπηρετητών στο σημείο **Target Host(s)**. Βάση των αποτελεσμάτων από την χρήση του εργαλείου «NMAP», γίνεται τοποθέτηση των IP διευθύνσεων του δικτύου που έχει δημιουργηθεί με την σειρά: **10.0.2.1**, **10.0.2.5** και **10.0.2.15**.

Ακόμη, για κάθε διαφορετική IP διεύθυνση γίνεται εισαγωγή ονόματος της σάρωσης (Task Name) και επιλογή ρυθμίσεων της σάρωσης (Scan Config). Τέλος, γίνεται η επιλογή **Create** για να πραγματοποιηθεί η σάρωση.



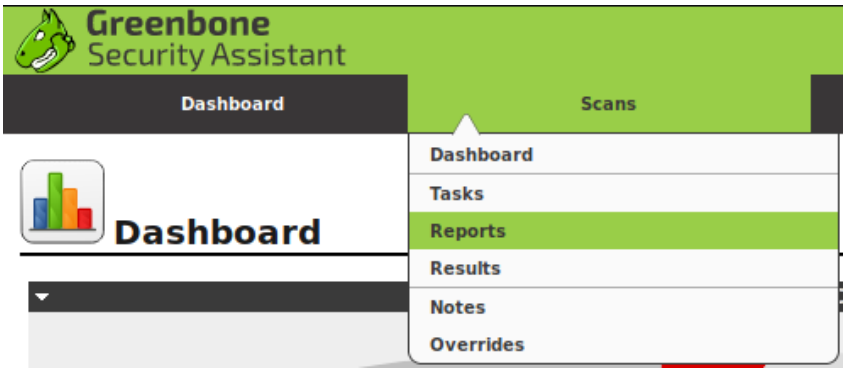
Εικόνα 3.13: Advanced Task Wizard για Σάρωση Δικτύου.

Επίσης, πρέπει να σημειωθεί ότι η διαδικασία τοποθέτησης των κάθε IP διευθύνσεων ξεχωριστά έγινε για πιο ξεκάθαρη ανάλυση των αποτελεσμάτων και για την δημιουργία μιας αναφοράς που θα περιλαμβάνει σημαντικές ευπάθειες για τους σκοπούς της μεταπτυχιακής διατριβής. Όπως φαίνεται και στην πιο κάτω εικόνα 3.14, μετά την σάρωση των IP διευθύνσεων, το εργαλείο «OpenVAS» έχει εντοπίσει ευπάθειες από τον εξυπηρετητή με την IP διεύθυνση **10.0.2.5** και την ονομασία **Network Scan Host 2 110320**. Ο συγκεκριμένος εξυπηρετητής είναι η εικονική μηχανή που έχει εγκατασταθεί στην ενότητα 3.2 για την δημιουργία του δικτύου με ευπάθειες στο εύρος των IP διευθύνσεων 10.0.2.0/24.

Name	Status	Reports		Severity
		Total	Last	
Network Scan Host 3 110320 (Automatically generated by wizard)	Done	1 (1)	Mar 11 2020	0.0 (Log)
Network Scan Host 1 110320 (Automatically generated by wizard)	Done	1 (1)	Mar 11 2020	0.0 (Log)
Network Scan Host 2 110320 (Automatically generated by wizard)	Done	1 (1)	Mar 11 2020	10.0 (High)

Εικόνα 3.14: Ολοκληρωμένες Σαρώσεις Εξυπηρετητών.

Στην συνέχεια, για την δημιουργία των αναφορών γίνεται η επιλογή **Scans, Reports** (εικόνα 3.15) από τον Αρχικό Πίνακα Λειτουργιών του «OpenVAS».



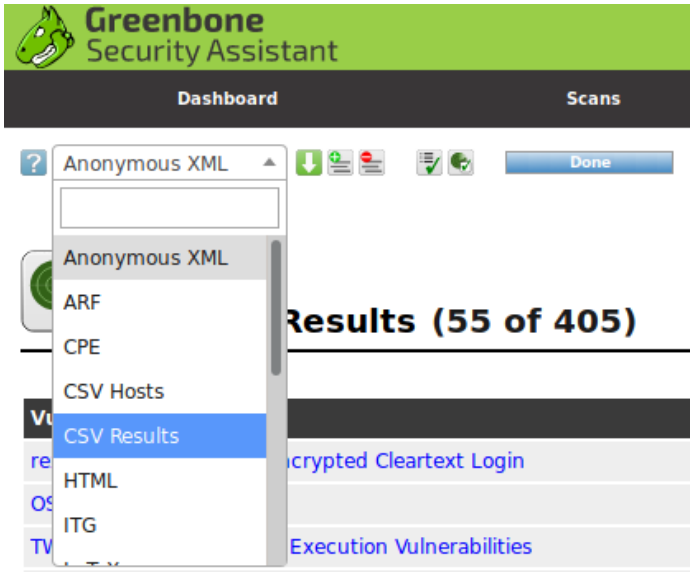
Εικόνα 3.15: Δημιουργία Αναφορών.

Οι αναφορές που έχουν δημιουργηθεί παρουσιάζονται όπως φαίνεται και στην πιο κάτω εικόνα 3.16.

Date	Status	Task	Severity
Wed Mar 11 16:50:17 2020	Done	Network Scan Host 3 110320	0.0 (Log)
Wed Mar 11 16:43:52 2020	Done	Network Scan Host 1 110320	0.0 (Log)
Wed Mar 11 16:12:26 2020	Done	Network Scan Host 2 110320	10.0 (High)

Εικόνα 3.16: Αναφορές από τις Σαρώσεις.

Έπειτα, ο χρήστης έχει την δυνατότητα να διαλέξει τον τύπο της αναφοράς με τα αποτελέσματα (Εικόνα 3.17). Στην συγκεκριμένη μεταπτυχιακή διατριβή, γίνεται η επιλογή **CSV Results** για την παρουσίαση των αποτελεσμάτων της σάρωσης σε τύπο **.csv**.



Εικόνα 3.17: Τύποι Αναφορών.

Το Παράρτημα Α παρουσιάζει όλες τις ευπάθειες που έχουν εντοπιστεί από την σάρωση του δικτύου. Σύμφωνα με ένα δείγμα στην εικόνα 3.18, τα αποτελέσματα της αναφοράς με τις διάφορες ευπάθειες που έχουν εντοπιστεί, χωρίζονται σε κατηγορίες (στήλες):

i. IP
ii. Port
iii. Protocol
iv. CVSS
v. Severity
vi. Solution Type
vii. NVT Name
viii. Summary

Η μεταπτυχιακή διατριβή θα επικεντρωθεί στην κατηγορία **CVSS**. Το CVSS (Common Vulnerability Scoring System) είναι μια τιμή σε κλίμακα 1-10 που αποτυπώνει το μέγεθος της σοβαρότητας μια συγκεκριμένης ευπάθειας [01]. Επομένως, η σοβαρότητα μιας συγκεκριμένης ευπάθειας τονίζει το μέγεθος της επίδρασης της. Έτσι, όταν η τιμή CVSS αυξάνεται, τότε αυξάνεται και το μέγεθος της επίδρασης μιας συγκεκριμένης ευπάθειας. Ακολούθως, αυξάνεται και η τιμή του ρίσκου που παρουσιάζει η συγκεκριμένη ευπάθεια, σε περίπτωση εκμετάλλευσής της.

IP	Port	Port Protocol	CVSS	Severity	Solution Type	NVT Name	Summary
10.0.2.5	512	tcp	10	High	Mitigation	rexec Passwordless / Unencrypted Cleartext Login	This remote host is running a rexec service.
10.0.2.5			10	High	Mitigation	OS End Of Life Detection	OS End Of Life Detection.
10.0.2.5	80	tcp	10	High	VendorFix	TWiki XSS and Command Execution Vulnerabilities	The host is running TWiki and is prone to Cross-Site Scripting
10.0.2.5	8787	tcp	10	High	Mitigation	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6
10.0.2.5	1524	tcp	10	High	Workaround	Possible Backdoor: Ingreslock	A backdoor is installed on the remote host.
10.0.2.5	3632	tcp	9.3	High	VendorFix	DistCC Remote Code Execution Vulnerability	DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict
10.0.2.5	3306	tcp	9	High	Mitigation	MySQL / MariaDB weak password	It was possible to login into the remote MySQL as
10.0.2.5	5900	tcp	9	High	Mitigation	VNC Brute Force Login	Try to log in with given passwords via VNC protocol.
10.0.2.5	5432	tcp	9	High	Mitigation	PostgreSQL weak password	It was possible to login into the remote PostgreSQL as user
10.0.2.5	8009	tcp	7.5	High	VendorFix	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Apache Tomcat is prone to a remote code execution vulnerability in the AJP
10.0.2.5	514	tcp	7.5	High	Mitigation	rsh Unencrypted Cleartext Login	This remote host is running a rsh service.
10.0.2.5	80	tcp	7.5	High	Workaround	phpinfo() output Reporting	Many PHP installation tutorials instruct the user to create
10.0.2.5	513	tcp	7.5	High	Mitigation	rlogin Passwordless / Unencrypted Cleartext Login	This remote host is running a rlogin service.
10.0.2.5	80	tcp	7.5	High	VendorFix	PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	PHP is prone to an information-disclosure vulnerability.
10.0.2.5	80	tcp	7.5	High	Mitigation	Test HTTP dangerous methods	Misconfigured web servers allows remote clients to perform
10.0.2.5	6667	tcp	7.5	High	VendorFix	Check for Backdoor in UnrealIRCd	Detection of backdoor in UnrealIRCd.
10.0.2.5	6200	tcp	7.5	High	VendorFix	vsftpd Compromised Source Packages Backdoor Vulnerability	vsftpd is prone to a backdoor vulnerability.
10.0.2.5	21	tcp	7.5	High	VendorFix	vsftpd Compromised Source Packages Backdoor Vulnerability	vsftpd is prone to a backdoor vulnerability.
10.0.2.5	22	tcp	7.5	High	Mitigation	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.
10.0.2.5	21	tcp	7.5	High	Mitigation	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials.

Εικόνα 3.18: Αναφορά Ευπαθειών σε Τύπο **.csv**.

3.5 Διαδικτυακές Βάσεις Δεδομένων, «Insider Data Threats»

Στην μεταπτυχιακή διατριβή έχει πραγματοποιηθεί χρήση διαδικτυακών δεδομένων που αποτελούν παραδείγματα από κακόβουλες ενέργειες χρηστών σε ένα οργανισμό [15]. Οι συγκεκριμένες βάσεις δεδομένων έχουν χρησιμοποιηθεί στην μεθοδολογία για την δημιουργία του «Cyber Risk Assessment Box» με αποτέλεσμα την εκτίμηση του ρίσκου σε μια οντότητα. Τα «Insider Data Threats» αποτελούν παραδείγματα από αρχεία καταγραφής συμβάντων βασισμένα σε ενέργειες χρηστών που έχουν καταχωρηθεί και πιθανόν να εντοπιστούν σε μια διαδικασία ανάλυσης της ανθρώπινης συμπεριφοράς.

Οι συγκεκριμένες κακόβουλες ενέργειες από τους χρήστες μπορεί να οδηγήσουν στην εκμετάλλευση ευπαθειών στα πληροφοριακά συστήματα, όπως για παράδειγμα των ευπαθειών που εντοπίστηκαν από την σάρωση του εργαλείου «OpenVAS» στο ευπαθές δίκτυο που δημιουργήθηκε. Στην πιο πάνω εικόνα 3.18 αλλά και στο Παράρτημα Α, η τοποθέτηση ενός αδύνατου κωδικού πρόσβασης σε μια βάση δεδομένων, μπορεί να οδηγήσει στην παράνομη πρόσβαση από ένα εργαζόμενο και υποκλοπή στοιχείων. Έπειτα, αυτό μπορεί να προκαλέσει οικονομικές και νομικές συνέπειες. Επομένως, βάση του «OpenVAS», η συγκεκριμένη ευπάθεια έχει τιμή «CVSS» ίση με 9 που τονίζει την σοβαρότητα της σε περίπτωση εκμετάλλευσής της.

Συνεχίζοντας, σύμφωνα με τις βάσεις δεδομένων [15] και όπως φαίνεται και στο παράδειγμα στην εικόνα 3.19, υπάρχει πιθανότητα ένας υπάλληλος σε ένα οργανισμό να μην είναι ευχαριστημένος με το εργασιακό του περιβάλλον. Στο συγκεκριμένο παράδειγμα, οι εργαζόμενοι ενημερώνουν μέσω ηλεκτρονικού ταχυδρομείου ότι η εργασία τους δεν εκτιμάται και δεν υπάρχει σεβασμός. Αυτό, μπορεί να έχει αρνητικές συνέπειες στην παραγωγικότητα καθώς και στην συμπεριφορά τους. Επίσης, αυτό μπορεί να οδηγήσει σε κακόβουλες ενέργειες από τους υπαλλήλους και να προκαλέσουν ζημιά στον οργανισμό. Έτσι, ο οργανισμός μπορεί να υποστεί οικονομικές επιπτώσεις καθώς και αρνητικά σχόλια που μπορεί να πλήξουν την εικόνα του οργανισμού.

email	PC-9776	Tatiana.Indira.Hanson@dtaa.com	Kyle.Tanner.Whitaker@dtaa.com					my work not appreciated i work weekends fed up my work not appreciated	
email	PC-7309	Daniel.Kibo.Bruce@dtaa.com	Berk.Griffin.Cooley@dtaa.com	Send	39869		AA First Email To Supervisor	my work not appreciated no gratitude	
email	PC-7309	Daniel.Kibo.Bruce@dtaa.com	Berk.Griffin.Cooley@dtaa.com	Send	21118		AA Second Email To Supervisor	angry take me seriously exacerbated i will leave bad things	

Εικόνα 3.19: Παράδειγμα Δυσαρέσκειας Υπαλλήλων στο Εργασιακό Περιβάλλον [15].

Επομένως, στο συγκεκριμένο γεγονός, ένας δυσαρεστημένος εργαζόμενος θα μπορούσε να πραγματοποιήσει μια κακόβουλη ενέργεια, μαντεύοντας τον εύκολο κωδικό πρόσβασης της βάσης δεδομένων για παράνομη υποκλοπή στοιχείων, όπως φαίνεται και στην αναφορά του εργαλείου «OpenVAS» (Εικόνα 3.18). Με αυτό τον τρόπο τονίζεται η συσχέτιση των διαδικτυακών βάσεων δεδομένων με τις ευπάθειες που μπορεί να εντοπιστούν σε ένα δίκτυο όπως αυτό που δημιουργήθηκε. Έτσι, η μεταπτυχιακή διατριβή θα βασιστεί σε αυτή την σύνδεση για την εκτίμηση της τελικής τιμής του ρίσκου.

Συνεχίζοντας, η χαμηλή παραγωγικότητα και η συμπεριφορά των υπαλλήλων ως προς την διάθεση που παρουσιάζουν για εργασία, φαίνεται και στο παράδειγμα τις εικόνας 3.20, όπου διάφοροι υπάλληλοι εισέρχονται σε ιστοσελίδες που δεν αφορούν τον οργανισμό [15].

{D9J5-F0DR67XQ-6676RTUB}	01/18/2010 15:55:27	DTAA/BTW0973	PC-4462	http://netflix.com
{Q4U2-X6JO59DT-7377MVIX}	01/18/2010 16:03:44	DTAA/RAA0594	PC-1665	http://netflix.com
{H3S1-X7JD84WC-8143VOJR}	01/18/2010 16:18:02	DTAA/KSP0927	PC-2221	http://netflix.com
{H1E8-V8LN79SZ-9056HAMY}	01/18/2010 16:25:11	DTAA/AJB0370	PC-0054	http://netflix.com
{N3I0-J9AN26KF-7058TJGR}	01/18/2010 16:42:00	DTAA/ABS0726	PC-3698	http://netflix.com
{P3K1-M7NI28ZP-0608NTKV}	01/19/2010 06:39:47	DTAA/CLB0995	PC-1731	http://netflix.com
{Y2D5-F1ZM10UV-6537QRXV}	01/19/2010 17:14:57	DTAA/ASS0824	PC-4842	http://netflix.com
{M7B8-D5GA43FK-0394CKNE}	01/20/2010 08:20:07	DTAA/CAO0951	PC-2846	http://netflix.com
{U1V5-U8BD18VL-6964RBSS}	01/20/2010 08:28:56	DTAA/BCM0558	PC-3916	http://netflix.com
{Y5I8-U2HY28GN-7144QGXI}	01/20/2010 10:49:47	DTAA/AJA0220	PC-3872	http://netflix.com
{L6G3-C8EX35NT-3098HTVB}	01/25/2010 20:15:40	DTAA/ARG0405	PC-3289	http://netflix.com
{E1O6-O1HO26TW-5824XQCG}	01/26/2010 13:05:00	DTAA/BCJ0800	PC-2703	http://netflix.com
{O1C8-O6LX96UY-2190HJMW}	01/26/2010 13:19:53	DTAA/AAK0924	PC-4772	http://netflix.com
{R3E2-H1FM06ZU-9098BHDT}	01/26/2010 13:37:39	DTAA/LBC0422	PC-1535	http://netflix.com
{U7G1-H7LB92SX-9883BZOK}	02/01/2010 09:30	DTAA/ATJ0284	PC-4337	http://netflix.com
{B8U4-K4KI09HE-3951ZCME}	02/01/2010 10:03	DTAA/BFV0911	PC-1532	http://netflix.com
{H7X5-V1IW99OI-3414EQNX}	02/01/2010 13:28	DTAA/BCM0558	PC-3916	http://netflix.com
{V8M5-Y2EV71GF-5540NOPO}	02/01/2010 16:19	DTAA/BML0618	PC-0659	http://netflix.com
{P1X1-B2UJ07AU-4972ZFSK}	02/01/2010 16:23	DTAA/ABS0726	PC-3698	http://netflix.com
{S8G3-D5YX95VZ-2313HXIO}	02/02/2010 09:11	DTAA/MJM0469	PC-1592	http://netflix.com
{U3U0-T2FO36JM-4618WJNT}	02/02/2010 09:16	DTAA/CDS0300	PC-2678	http://netflix.com

{S3Z0-P9UG02AS-5790DTJF}	10/27/2010 16:07:33	DTAA/RRF0245	PC-0019	http://youtube.com
{R2F4-E6WV56BR-5518JNQW}	10/27/2010 16:42:19	DTAA/AKS0283	PC-3049	http://youtube.com
{I1K1-V8DV93EN-9242FATI}	10/29/2010 07:41:56	DTAA/JFA0081	PC-4328	http://youtube.com
{F8T5-C8FN18IT-7675MEBZ}	10/29/2010 07:41:57	DTAA/AJS0917	PC-2082	http://youtube.com
{Y2B1-X4HB14PR-6724HUSB}	10/29/2010 07:45:52	DTAA/AJS0917	PC-2082	http://youtube.com
{V8V5-V6IS56SV-2068IAJD}	10/29/2010 08:50:30	DTAA/AKM0969	PC-0691	http://youtube.com
{K3P0-P9OK64NL-0457MJVJ}	10/29/2010 09:58:36	DTAA/AJS0917	PC-2082	http://youtube.com
{T3W9-A6GP19AV-6836QJGF}	10/29/2010 11:09:21	DTAA/AJS0978	PC-1738	http://youtube.com
{E3G3-X1QR98DN-6375HZVA}	10/29/2010 11:46:02	DTAA/ECG0753	PC-1669	http://youtube.com
{H9D5-L3TM79QG-1290MVGJ}	10/29/2010 11:58:42	DTAA/AEC0750	PC-2926	http://youtube.com
{G9R7-A0NL93IJ-0230LYIH}	11/01/2010 07:42	DTAA/ASC0132	PC-2960	http://youtube.com
{Y3D0-P4IQ76FO-1733ZRGM}	11/01/2010 08:37	DTAA/AKW0582	PC-0891	http://youtube.com
{Z9P4-Q2MZ49ZD-9217XOME}	11/01/2010 08:41	DTAA/AFG0122	PC-4492	http://youtube.com
{R8E5-K0BT74NB-4143AUQX}	11/01/2010 08:52	DTAA/ACL0865	PC-0124	http://youtube.com

{F4Y2-O8QD88ZL-9676VSPK}	03/31/2010 16:56:04	DTAA/AAR0508	PC-1469	http://facebook.com
{F6Z0-M8LB37UE-1891SNEN}	03/31/2010 17:00:58	DTAA/BCH0912	PC-2485	http://facebook.com
{U5Z5-H2VJ45NW-1365PFSF}	03/31/2010 17:11:49	DTAA/AAK0924	PC-4772	http://facebook.com
{V8T3-V0ZU93AT-5964QYES}	03/31/2010 17:21:28	DTAA/ACL0865	PC-0124	http://facebook.com
{X1B9-C8SY04NN-1835FMMI}	04/01/2010 07:15	DTAA/AKA0033	PC-2020	http://facebook.com
{Y3D9-B4HU12JA-4953FFBN}	04/01/2010 07:18	DTAA/BFO0438	PC-4057	http://facebook.com
{Q3P2-I2UR04IJ-7173AVNG}	04/01/2010 07:32	DTAA/ACD0647	PC-3117	http://facebook.com
{V7N3-M4KK33MV-3393GBFU}	04/01/2010 07:39	DTAA/AJA0220	PC-3872	http://facebook.com
{Q8Z7-I2KP84IM-4293JULF}	04/01/2010 07:39	DTAA/ACH0803	PC-4334	http://facebook.com

Εικόνα 3.20: Παράδειγμα Πρόσβασης σε Ιστοσελίδες που Δεν Αφορούν τον Οργανισμό [15].

Ακόμη, σύμφωνα με το επαγγελματικό επίπεδο του ανθρώπινου δυναμικού, το επίπεδο γνώσεων, καθώς και την εργασιακή εμπειρία, το ρίσκο για πρόκληση ζημιάς σε μια οντότητα είναι μεγαλύτερο σε περίπτωση κακόβουλης ενέργειας. Στην πιο κάτω εικόνα 3.21, παρουσιάζονται παραδείγματα από την βάση δεδομένων, όπου φαίνεται να γίνεται χρήση κακόβουλου λογισμικού «keylogger» με πιθανό σκοπό την παρακολούθηση και την παράνομη απόκτηση δεδομένων [07]. Επομένως, υπάρχει πιθανότητα να διαρρεύσουν πληροφορίες που κάνουν μια οντότητα πετυχημένη όταν υπάρχουν τεχνικές γνώσεις και εμπειρία για χρήση κακόβουλων λογισμικών όπως το «keylogger». Αυτό μπορεί να οδηγήσει ένα οργανισμό σε οικονομικές συνέπειες.

http	{Z8O8-G2UI61TW-7042FUSY}	PC-9776	http://download.cnet.com/Refog-Free-Keylogger/Climate_of_Ohio/snowiest/NNXrlybttre1252221508.aspx

surveillance monitor program file free keyboard free stealth program hidden

device	PC-7309	R:\;R:\BGC0686;R:\24h64f6
file	PC-7309	R:\keylogger.exe
device	PC-7309	
logon	PC-2403	Logon
device	PC-2403	R:\;R:\BGC0686;R:\24h64f6
file	PC-2403	R:\keylogger.exe
device	PC-2403	
logon	PC-2403	Logoff
logon	PC-2403	Logon
logon	PC-2403	Logoff

Εικόνα 3.21: Παράδειγμα Χρήσης Κακόβουλου Λογισμικού «keylogger» [15].

Επιπλέων, το επίπεδο πρόσβασης που αποκτά το ανθρώπινο δυναμικό μπορεί να καθορίσει το μέγεθος της ζημιάς που μπορεί να προκαλέσει μια κακόβουλη ενέργεια. Επομένως, το ρίσκο σε ένα οργανισμό είναι μεγαλύτερο όταν το επίπεδο πρόσβασης που καθορίζεται είναι μεγαλύτερο. Η εικόνα 3.22 παρουσιάζει ένα συγκεκριμένο παράδειγμα όπου ο χρήστης με την μηχανή PC-3585 φαίνεται να πραγματοποιεί κακόβουλες ενέργειες, ανεβάζοντας αρχεία και πληροφορίες στην γνωστή ιστοσελίδα διαρροής δεδομένων «wikileaks.org» [15]. Στην περίπτωση μιας τέτοιας κακόβουλης ενέργειας από ένα εργαζόμενο είναι πιθανόν να οδηγήσει σε διαρροή ευαίσθητων πληροφοριών και ιδιωτικών δεδομένων. Έτσι, οργανισμός μπορεί να έχει νομικές και οικονομικές επιπτώσεις, καθώς και αρνητικές συνέπειες στην εικόνα του οργανισμού.

logon	{G2H1-V3LL26UJ-4609MBGD}	03/06/2010 01:41	ONS0995	PC-3585	Logon
device	{Y6I8-I2LO77NI-8263FFFU}	03/06/2010 01:47	ONS0995	PC-3585	Insert
http	{C5O3-K3KK36TF-3444YDYN}	03/06/2010 01:47	ONS0995	PC-3585	http://wikileaks.org
device	{R6O4-Q6TK19WO-2378PYOS}	03/06/2010 01:48	ONS0995	PC-3585	Remove
logon	{I9P2-Z8JX07HI-2460KGXN}	03/06/2010 02:40	ONS0995	PC-3585	Logoff
logon	{X6F2-G7RK34PF-6119MNWN}	03/09/2010 12:04	ONS0995	PC-3585	Logon
device	{T6M6-V7HH64YF-6253NFTK}	03/09/2010 12:57	ONS0995	PC-3585	Insert
device	{J6N9-T3AN23NV-9781KHHG}	03/09/2010 02:10	ONS0995	PC-3585	Remove
logon	{C0Q0-Q7NF61RO-0237KQXF}	03/09/2010 02:32	ONS0995	PC-3585	Logoff
logon	{Q1W9-X7EB31VJ-6835VJPN}	03/12/2010 03:03	ONS0995	PC-3585	Logon
device	{E4Z3-J3YP97FO-3445TUDC}	03/12/2010 03:12	ONS0995	PC-3585	Insert
device	{F5E3-U9QK34HM-3404OFAO}	03/12/2010 03:22	ONS0995	PC-3585	Remove
logon	{T7Y9-Q2LD36CL-0630ZOMX}	03/12/2010 03:29	ONS0995	PC-3585	Logoff
logon	{I9Q8-A6SN35RS-7732TJRL}	3/16/2010 5:31:57	ONS0995	PC-3585	Logon
device	{O6Y7-Y5BO88JF-0919JXJK}	3/16/2010 5:52:24	ONS0995	PC-3585	Insert
device	{N2K1-W2HW73KA-9256IDLX}	3/16/2010 5:58:31	ONS0995	PC-3585	Remove
logon	{K8V2-C7RN96HD-2871XQZF}	3/16/2010 6:06:30	ONS0995	PC-3585	Logoff
logon	{H9A7-G9XK94ZM-6166AIOL}	3/19/2010 6:46:47	ONS0995	PC-3585	Logon
device	{I8G0-X2DD58JN-6372VACI}	3/19/2010 6:49:14	ONS0995	PC-3585	Insert
device	{P9A9-G3BE85UM-3445XJCZ}	3/19/2010 6:54:17	ONS0995	PC-3585	Remove
logon	{B2Z8-D2NX57XP-5870ZDFI}	3/19/2010 6:55:32	ONS0995	PC-3585	Logoff
logon	{I7P3-B2NK51OW-1892ESZM}	3/19/2010 22:04:38	ONS0995	PC-3585	Logon
device	{Q4E5-V8XA18EF-0280QQZJ}	3/20/2010 1:47:28	ONS0995	PC-3585	Insert
http	{N5X1-H1SK37SS-9208ENYS}	3/20/2010 01:59:32	ONS0995	PC-3585	http://wikileaks.org
device	{Y2H2-W4AE27KN-4301QKDP}	3/20/2010 5:38:08	ONS0995	PC-3585	Remove
logon	{K6D9-V5LZ17OM-8387EOQC}	3/20/2010 8:10:12	ONS0995	PC-3585	Logoff

Εικόνα 3.22: Παράδειγμα Κακόβουλων Ενεργειών και Διαρροής Δεδομένων [15].

Συμπερασματικά λοιπόν, υπογραμμίζεται το γεγονός ότι οι ανθρώπινοι παράγοντες και ιδιαίτερα τα ανθρώπινα χαρακτηριστικά μπορεί να οδηγήσουν σε κακόβουλες ενέργειες όπως παρουσιάζουν οι διαδικτυακές βάσεις δεδομένων («Insider Data Threats»). Έπειτα, οι συγκεκριμένες κακόβουλες ενέργειες μπορεί να οδηγήσουν στην εκμετάλλευση των ευπαθειών των πληροφοριακών συστημάτων, όπως φαίνεται μετά την σάρωση του εργαλείου «OpenVAS» στο ευπαθές δίκτυο που δημιουργήθηκε.

Κεφάλαιο 4

Εγκατάσταση Εργαλείων

Το Κεφάλαιο 4 παρουσιάζει τα εργαλεία που χρησιμοποιήθηκαν στην μεταπτυχιακή διατριβή για εύρεση ευπαθειών και μετατροπή της μεθοδολογίας στην γλώσσα προγραμματισμού «Python» . Επίσης, επεξηγεί βήμα προς βήμα τις ενέργειες που πραγματοποιήθηκαν για την σωστή χρήση τους.

4.1 Εργαλείο OpenVAS

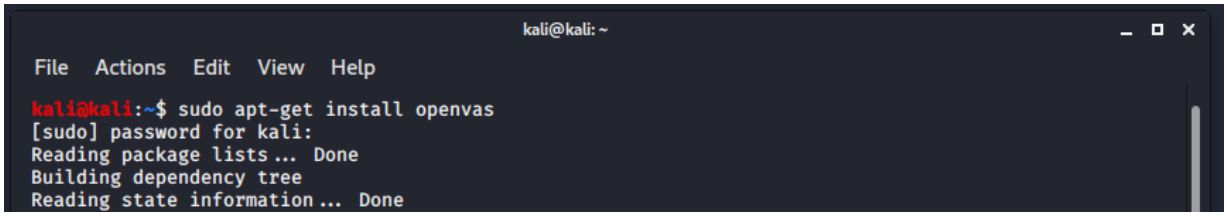
Η συγκεκριμένη ενότητα αναφέρεται στο εργαλείο «OpenVAS». Πραγματοποιείται μια εισαγωγή στο εργαλείο και ακολούθως παρουσιάζονται πληροφορίες σχετικά με την εγκατάσταση, ρύθμιση και λειτουργία του εργαλείου.

4.1.1 Εισαγωγή στο Εργαλείο OpenVAS

Το εργαλείο «OpenVAS» είναι ένα εργαλείο ανοικτού κώδικα για την σάρωση και τον εντοπισμό ευπαθειών στα δίκτυα υπολογιστών και πληροφοριακών συστημάτων [06]. Η λειτουργία του συγκεκριμένου εργαλείου γίνεται διαδικτυακά. Επίσης, η εγκατάσταση του «OpenVAS» πραγματοποιείται στο λογισμικό λειτουργικών συστημάτων «Kali - Linux».

4.1.2 Εγκατάσταση OpenVAS

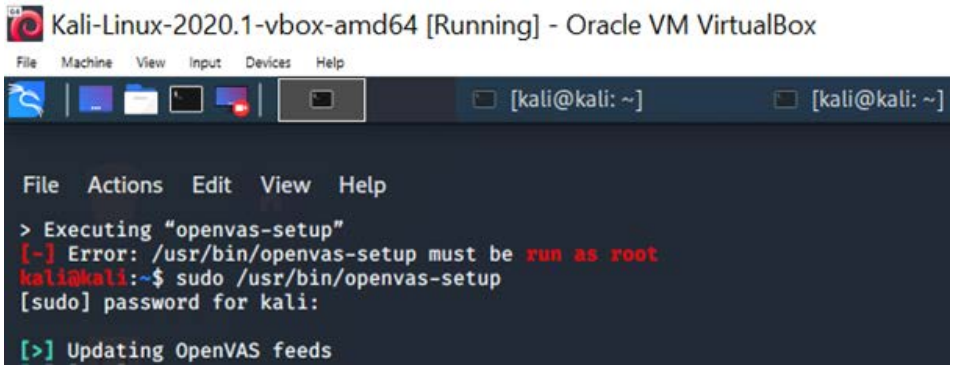
Όπως φαίνεται και στην εικόνα 4.1, η εγκατάσταση του εργαλείου «OpenVAS» γίνεται με την χρήση της εντολής **sudo apt-get install openvas** στο τερματικό (terminal) των Kali – Linux.



Εικόνα 4.1: Εντολή για την Εγκατάσταση του «OpenVAS».

4.1.3 Ρύθμιση OpenVAS

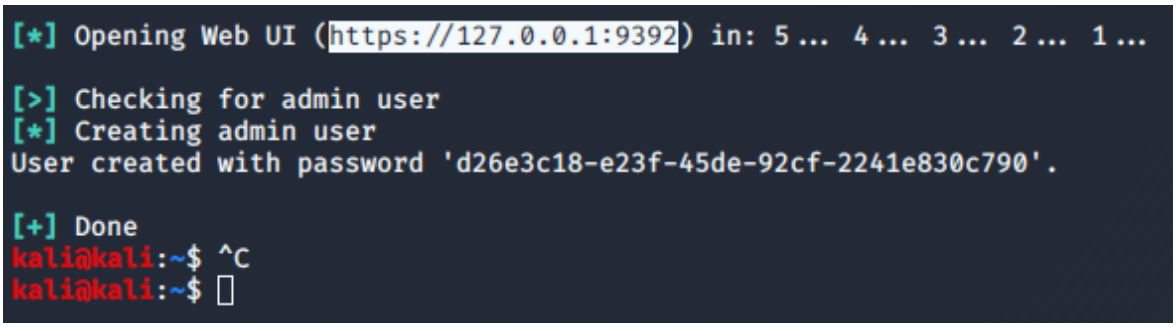
Όπως διακρίνεται και στην εικόνα 4.2, η ρύθμιση του εργαλείου είναι αναγκαία πριν από την χρήση του. Επομένως, γίνεται η χρήση της εντολής **sudo /usr/bin/openvas-setup** που οδηγεί και σε αναβάθμιση του εργαλείου με τις τελευταίες ευπάθειες που έχουν δημοσιευτεί. Επίσης, ο χρήστης έχει την δυνατότητα αναβάθμισης της βάσης δεδομένων με τις ευπάθειες όποτε αυτός το επιθυμεί χρησιμοποιώντας την εντολή **sudo openvas-setup.**



Εικόνα 4.2: Ρύθμιση του OpenVAS.

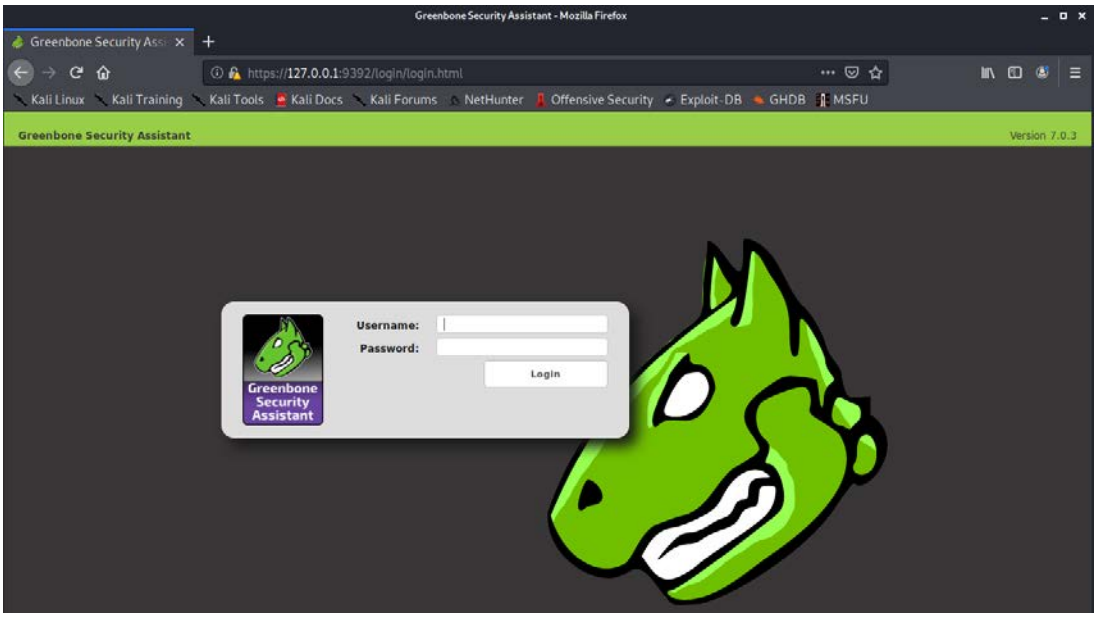
4.1.4 Λειτουργία OpenVAS

Συνεχίζοντας, όταν γίνεται για πρώτη φορά η ρύθμιση και η χρήση του εργαλείου, δίνεται ένας κωδικός που θα χρησιμοποιηθεί για την είσοδο στην διαδικτυακή πλατφόρμα του OpenVAS. Η εικόνα 4.3 παρουσιάζει την ηλεκτρονική διεύθυνση στην οποία θα εκτελείται η λειτουργία του OpenVAS, καθώς και ο κωδικός εισόδου. Ακόμη, το όνομα του χρήστη είναι **admin.**



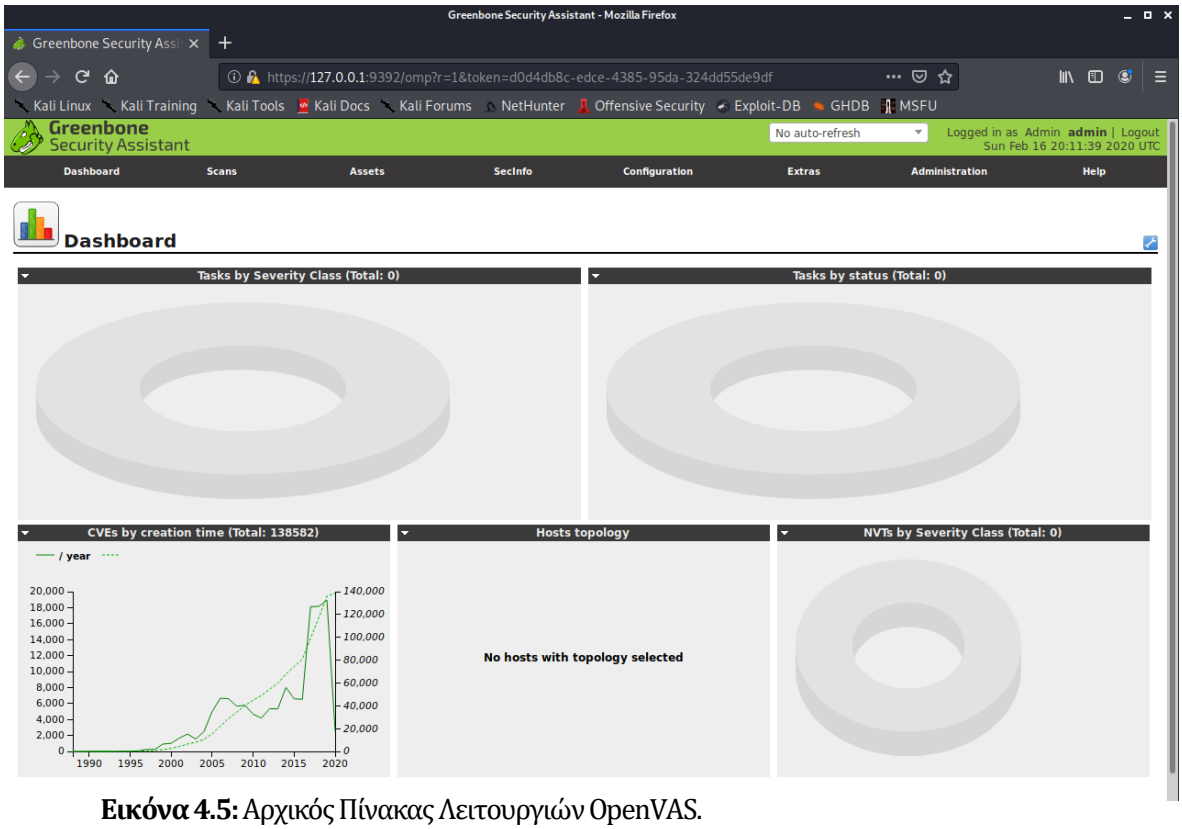
Εικόνα 4.3: Στοιχεία Εισόδου στο Εργαλείο OpenVAS: i) Ηλεκτρονική Διεύθυνση, ii) Κωδικός Εισόδου .

Ακολούθως, βάση της εικόνας 4.4, γίνεται αυτόματη ανακατεύθυνση στην συγκεκριμένη ηλεκτρονική διεύθυνση και ζητείται η τοποθέτηση του ονόματος χρήστη και του κωδικού εισόδου.



Εικόνα 4.4: Παράθυρο Εισόδου στο εργαλείο OpenVAS.

Τέλος, η εικόνα 4.5 παρουσιάζει τον αρχικό πίνακα λειτουργιών (dashboard) του OpenVAS μετά την επιτυχή πρόσβαση του χρήστη.



Εικόνα 4.5: Αρχικός Πίνακας Λειτουργιών OpenVAS.

4.2 Εργαλείο Spyder

Η συγκεκριμένη ενότητα αναφέρεται στο εργαλείο «Spyder3». Πραγματοποιείται μια εισαγωγή στο εργαλείο και ακολούθως παρουσιάζονται πληροφορίες σχετικά με την εγκατάσταση, ρύθμιση και λειτουργία του εργαλείου.

4.2.1 Εισαγωγή στο Εργαλείο Spyder

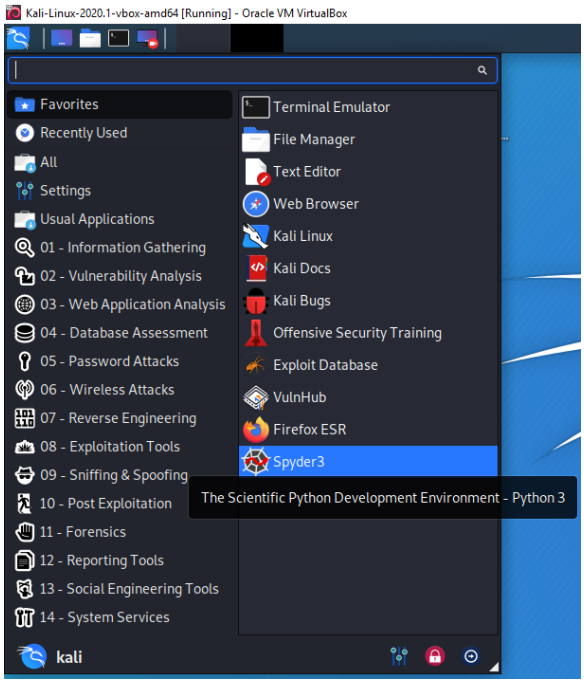
Το εργαλείο «Spyder» επιτρέπει στον χρήστη την δημιουργία και την επεξεργασία κώδικα σε γλώσσα προγραμματισμού «Python» [21]. Επίσης, επιτρέπει την αλληλεπίδραση με τον χρήστη, αφού ο χρήστης μπορεί να τοποθετήσει τιμές σε ένα παράθυρο αλληλεπίδρασης με τον κώδικα.

4.2.2 Εγκατάσταση Spyder

Η εγκατάσταση του «Spyder» έγινε στο λογισμικό λειτουργικών συστημάτων «Kali - Linux», με το τρέξιμο της εντολής **sudo apt-get install spyder3** στο τερματικό.

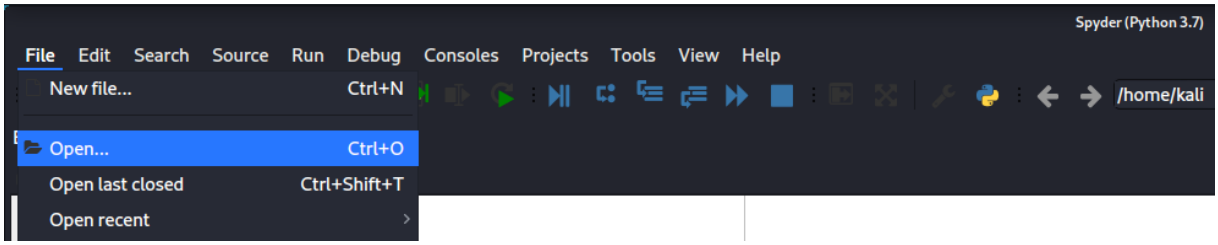
4.2.3 Είσοδος και Λειτουργία Spyder

Η είσοδος στο «Spyder» γίνεται με το τρέξιμο της εφαρμογής, όπως φαίνεται και στην εικόνα 4.6 πιο κάτω.



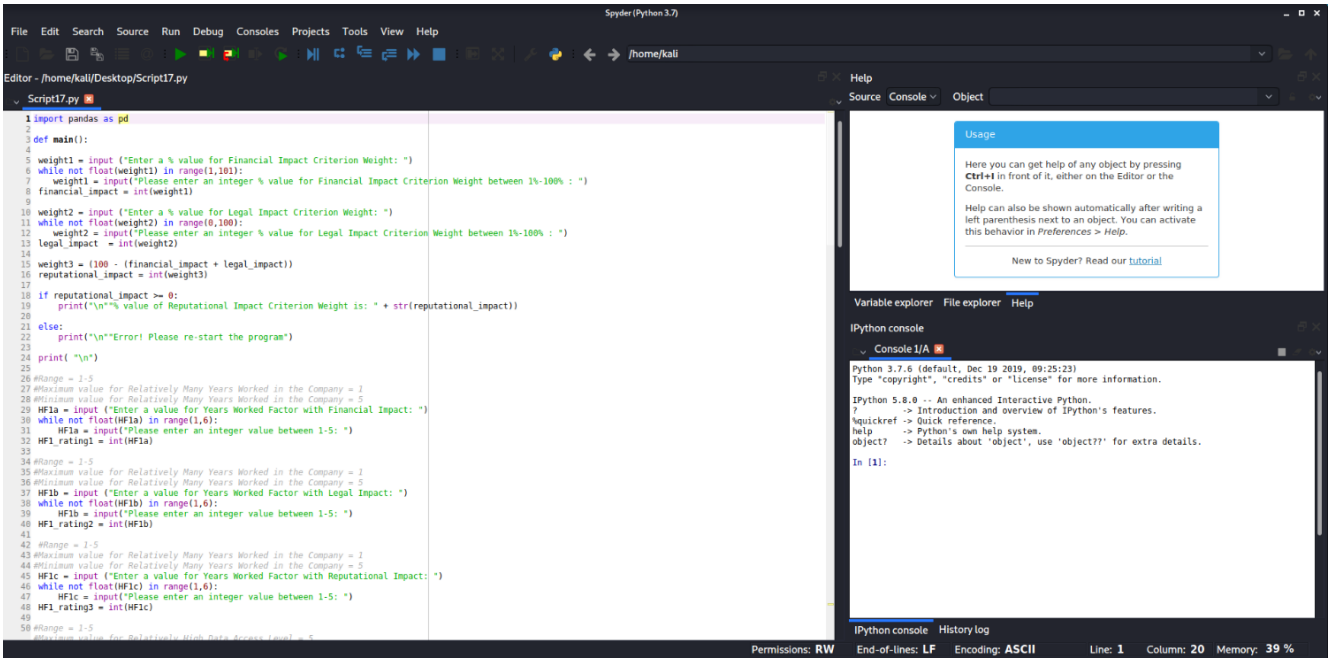
Εικόνα 4.6: Εφαρμογή Spyder3.

Στην συνέχεια, όπως φαίνεται και στην εικόνα 4.7, ο χρήστης καλείται να δημιουργήσει ή να ανοίξει ένα αρχείο με κώδικα «Python».



Εικόνα 4.7: Δημιουργία ή Άνοιγμα Αρχείου με Κώδικα Python.

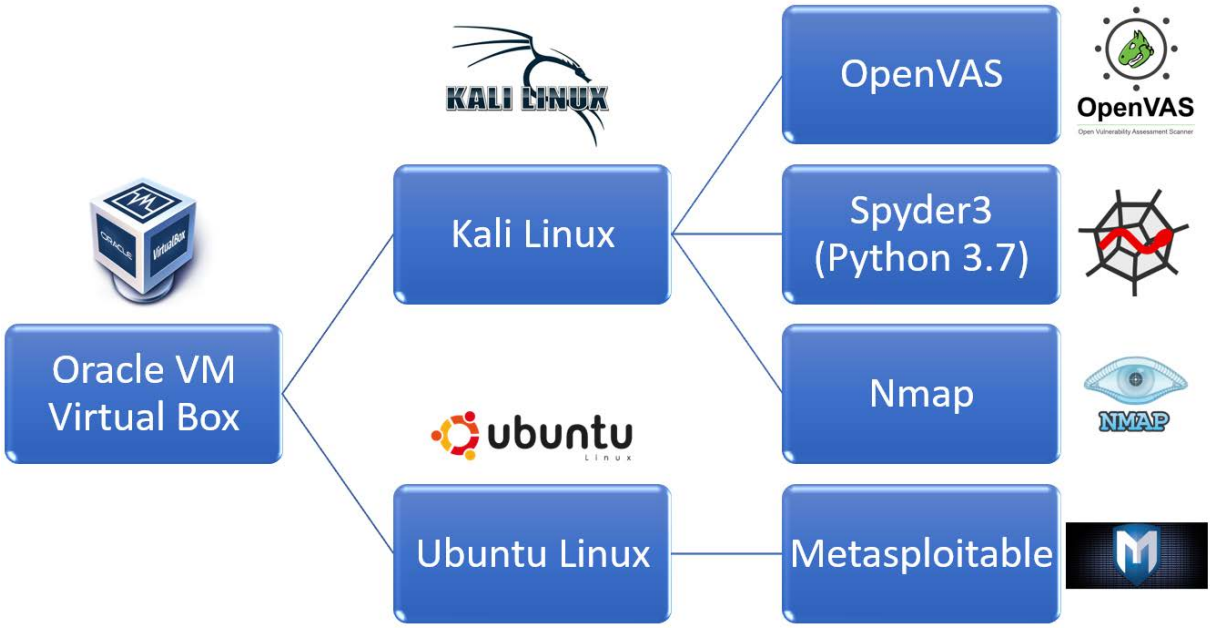
Επιπλέον, στην εικόνα 4.8, διακρίνεται στα αριστερά το κύριο παράθυρο επεξεργασίας κώδικα Python, ενώ κάτω-δεξιά φαίνεται το παράθυρο αλληλεπίδρασης με τον χρήστη.



Εικόνα 4.8: Παράθυρα Λειτουργιών του εργαλείου Spyder3.

4.3 Σφαιρική Εικόνα των Εργαλείων

Η συγκεκριμένη ενότητα παρουσιάζει την σύνδεση μεταξύ των εργαλείων στην μεταπτυχιακή διατριβή, όπως χρησιμοποιήθηκαν για την υλοποίηση του «Cyber Risk Assessment Box» και την εκτίμηση του ρίσκου. Επομένως, η εικόνα 4.9 παρουσιάζει την σφαιρική εικόνα των εργαλείων και των μηχανών που χρησιμοποιήθηκαν.



Εικόνα 4.9: Σφαιρική Εικόνα των Εργαλείων και Μηχανών που Χρησιμοποιήθηκαν.

Κεφάλαιο 5

Μεθοδολογία

Το κεφάλαιο 5 περιγράφει την μεθοδολογία και την προσέγγιση της μεταπτυχιακής διατριβής για την εκτίμηση του ρίσκου σε μια οντότητα, λαμβάνοντας υπόψη τους 3 σημαντικούς παράγοντες που έχουν επιλεγεί βάση και της βιβλιογραφικής επισκόπησης που έγινε στο Κεφάλαιο 2:

i. Ανθρώπινοι Παράγοντες.
ii. Ανάλυση Συμπεριφοράς (Behavioural Analysis).
iii. Εντοπισμός Ευπαθειών στα Πληροφοριακά Συστήματα.

Επομένως, ήταν αναγκαίο να βρεθεί μια χρυσή τομή όπου θα συνδύαζε τους 3 πιο πάνω παράγοντες, έτσι ώστε να δημιουργηθεί ένα πρόγραμμα ή διαφορετικά το «Cyber Risk Assessment Box». Επίσης, για την εκτίμηση του ρίσκου, οι υπολογισμοί έχουν υλοποιηθεί στην γλώσσα προγραμματισμού «Python» με την χρήση του εργαλείου «Spyder 3», σε περιβάλλον «Kali-Linux». Επιπλέων, έγινε χρήση δεδομένων από διαδικτυακές βάσεις που περιέχουν κακόβουλες ενέργειες χρηστών έτσι ώστε να προσομοιάζει ένα περιβάλλον οργανισμού με πιθανές απειλές από το «εσωτερικό» [15].

5.1 Εισαγωγή στην Μεθοδολογία

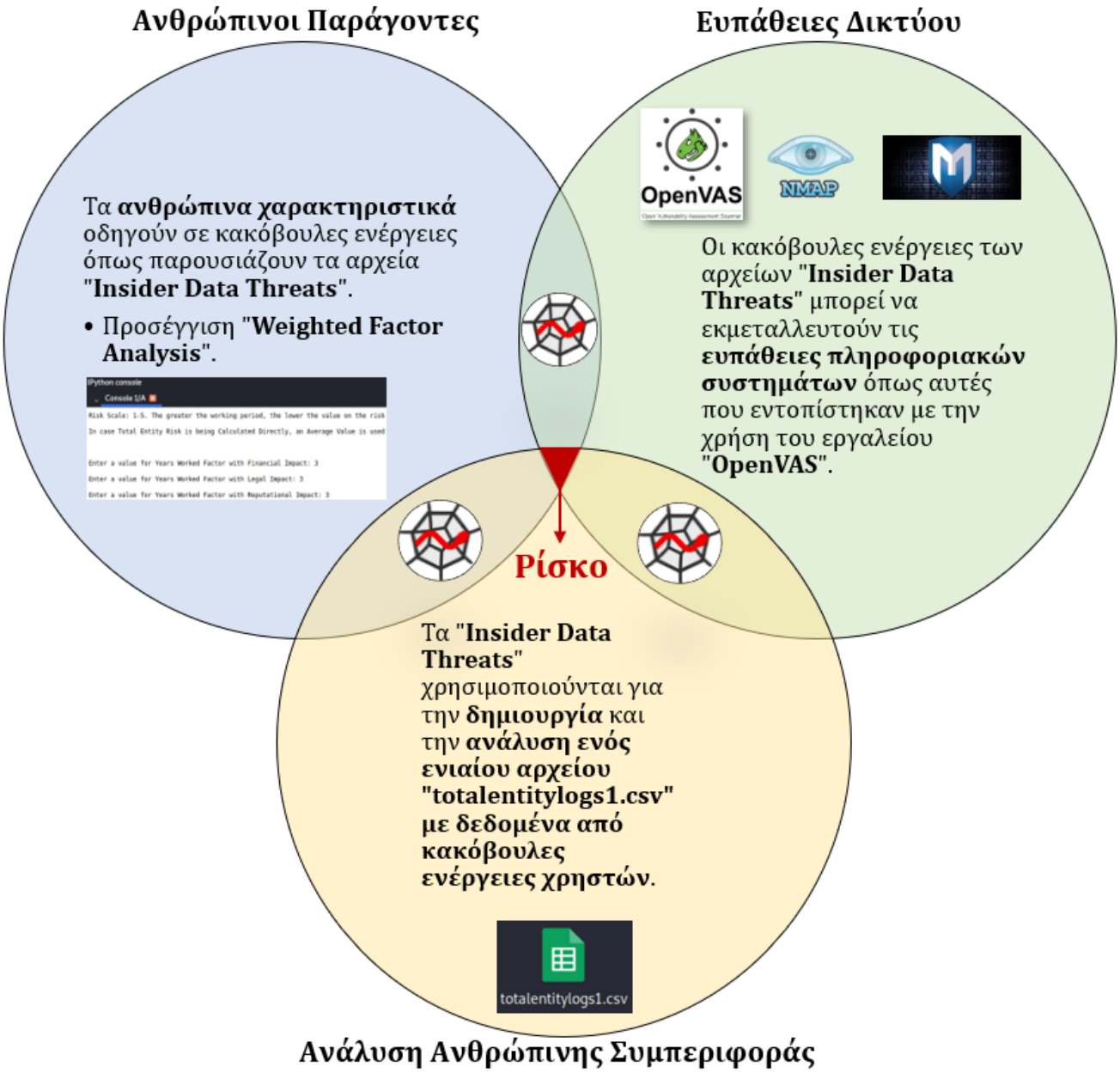
Σύμφωνα με το NIST [18] και τις πληροφορίες που αναφέρονται στο Κεφάλαιο 2, η προσέγγιση της μεταπτυχιακής διατριβής για τον υπολογισμό του ρίσκου βασίζεται στην μαθηματική εξίσωση Risk = Impact x Probability. Συνεπώς, η μεθοδολογία που ακολουθείται θα έχει ως βάση το Μέγεθος της Επίδρασης της Απειλής (Impact) και τις Πιθανότητες Υλοποίησης της (Probability).

Προσθέτοντας στα πιο πάνω, για να μπορέσει επιτυχώς η μεταπτυχιακή διατριβή να συνδυάσει σωστά τους πιο πάνω παράγοντες, θα πρέπει ο κάθε παράγοντας ξεχωριστά να έχει σαν «μονάδα μέτρησης» το μέγεθος της απειλής ή/και τις πιθανότητες υλοποίησης της. Έτσι, ο συνδυασμός των 3 παραγόντων θα έχει ένα κοινό «έδαφος» στο οποίο θα στηρίζεται η μεθοδολογία της μεταπτυχιακής διατριβής και τον επιτυχή υπολογισμό του ρίσκου σε μια οντότητα. Επίσης, η χρήση των «Insider Data Threats» ήταν σημαντική για την ανάλυση δεδομένων από κακόβουλες ενέργειες χρηστών [15].

Σύμφωνα με τα πιο πάνω, ο υπολογισμός του ρίσκου βάση των ανθρώπινων παραγόντων επικεντρώνεται περισσότερο στις πιθανότητες υλοποίησης μιας απειλής. Παράλληλα, ο υπολογισμός του ρίσκου βάση της ανάλυσης της συμπεριφοράς δίνει σημασία στο μέγεθος της ζημιάς αλλά και στις πιθανότητες υλοποίησης της. Τέλος, η εκτίμηση του ρίσκου βάση του εντοπισμού ευπαθειών σε πληροφοριακά συστήματα, έχει ως βασικό γνώμονα το μέγεθος της ζημιάς που θα προκαλέσει μια συγκεκριμένη ευπάθεια.

Συμπερασματικά λοιπόν, οι τελικές τιμές των 3 παραγόντων θα προστεθούν με μαθηματική πράξη και το τελικό αποτέλεσμα για την εκτίμηση του ρίσκου θα παρουσιαστεί σαν ποσοστό (%). Επιπλέων, υπογραμμίζεται το γεγονός ότι το συγκεκριμένο πρόγραμμα προσαρμόζεται με ιδιαίτερη ευκολία στις ανάγκες της κάθε οντότητας. Για παράδειγμα, το συγκεκριμένο πρόγραμμα έχει αναπτυχθεί με τρόπο ώστε να μπορεί να υπολογίσει το ρίσκο σε ένα οργανισμό, σε ένα τμήμα ή ακόμη στον κάθε χρήστη ξεχωριστά. Ακόμη, έχουν συμπεριληφθεί διάφορες βαρύτητες (weights) στους υπολογισμούς έτσι ώστε να είναι εφικτή η τροποποίηση του προγράμματος στα σημεία όπου η συγκεκριμένη οντότητα θεωρεί πιο σημαντικά.

Η εικόνα 5.1 παρουσιάζει την βασική ιδέα της μεθοδολογίας και την προσέγγισης της μεταπτυχιακής διατριβής. Επομένως, φαίνεται ο συσχέτιση των παραγόντων που έχουν επιλεγεί για την δημιουργία του «Cyber Risk Assessment Box» και την εκτίμηση του ρίσκου. Επίσης, παρουσιάζονται τα εργαλεία και οι μηχανές που χρησιμοποιήθηκαν στο κάθε τμήμα.



Εικόνα 5.1: Γενική Εικόνα της Μεθοδολογίας.

Όπως φαίνεται και στην πιο πάνω εικόνα 5.1, τα «Insider Data Threats» παρουσιάζουν παραδείγματα από κακόβουλες ενέργειες. Χρησιμοποιήθηκαν με σκοπό την ανάλυση των δεδομένων στα αρχεία καταγραφής συμβάντων και τον εντοπισμό κακόβουλων ενέργειων [15].

Λόγω των ανθρώπινων παραγόντων, οι κακόβουλες ενέργειες που παρουσιάζουν τα «Insider Data Threats» μπορούν να οδηγήσουν σε εκμετάλλευση ευπαθειών στα πληροφοριακά συστήματα. Έπειτα, αυτό μπορεί να οδηγήσει σε οικονομικές και νομικές επιπτώσεις καθώς και επιπτώσεις στην φήμη ενός οργανισμού.

Τα αρχεία «Insider Data Threats» δεν περιέχουν τις ευπάθειες των πληροφοριακών συστημάτων που αποτελούν τα ευάλωτα σημεία για την επιτυχής διεκπεραίωση των κακόβουλων ενεργειών που περιέχουν. Επομένως, η δημιουργία του δικτύου με τις ευπάθειες ήταν αναγκαία με σκοπό την προσομοίωση ενός οργανισμού με ευπάθειες. Έτσι, υπογραμμίζεται ότι η χρήση του «Cyber Risk Assessment Box» σε ένα αληθινό παράδειγμα ενός οργανισμού θα οδηγήσει σε πιο ακριβή αποτελέσματα. Η σάρωση των ευπαθειών θα πραγματοποιηθεί στο ίδιο περιβάλλον όπου γίνεται και η ανάλυση της ανθρώπινης συμπεριφοράς από τα αρχεία καταγραφής συμβάντων. Επομένως, θα υπάρχει αντιστοιχία των δύο παραγόντων για την υλοποίηση της εκτίμησης της τελικής τιμής του ρίσκου.

Επιπλέων, είναι σημαντικό να σημειωθεί ότι τα αρχεία «Insider Data Threats» περιέχουν μόνο κακόβουλες ενέργειες χρηστών χωρίς να γίνεται αναφορά αν η υλοποίηση των συγκεκριμένων απειλών ήταν επιτυχής, προκαλώντας ζημιά. Ακόμη, δεν αναφέρουν τις πιθανότητες υλοποίησης μιας κακόβουλης ενέργειας. Έτσι, ήταν σημαντική η χρήση τους στο πρόγραμμα «Cyber Risk Assessment Box» αφού μέσω της ανάλυσης συμπεριφοράς που πραγματοποιήθηκε, έγινε η εκτίμηση του ρίσκου λαμβάνοντας υπόψη το μέγεθος της επίπτωσης (Impact) και τις πιθανότητες υλοποίησης της απειλής (Probability).

Συνεχίζοντας, ο πίνακας 5.1 παρουσιάζει ευπάθειες που εντοπίστηκαν από το εργαλείο «OpenVAS» στο δίκτυο που δημιουργήθηκε και την πιθανή αντιστοιχία τους με τις κακόβουλες ενέργειες που έχουν καταγραφεί στα «Insider Data Threats». Στην στήλη «Insider Data Threats Activity - Threat», παρουσιάζονται οι κακόβουλες ενέργειες ή απειλές προς τον οργανισμό που θα μπορούσαν να εκμεταλλευτούν τις ευπάθειες που εντοπίστηκαν στο ευπαθές δίκτυο και να προκαλέσουν ζημιά, αυξάνοντας το ρίσκο. Οι συγκεκριμένες κακόβουλες ενέργειες έχουν χρησιμοποιηθεί στην αναζήτηση λέξεων-κλειδιά στο κομμάτι της ανάλυσης της ανθρώπινης συμπεριφοράς.

Ευπάθειες από το Δίκτυο που Δημιουργήθηκε					Διαδικτυακές Βάσεις Δεδομένων – «Insider Data Threats»		
Port on Host IP 10.0.2.5	**CVSS**	**Severity**	**NVT Name**	**Summary**	**Insider Data Threats Activity - Threat**	**Insider Data Threats User**	**Insider Data Threats Detected Device**
1524	10	High	Possible Backdoor : Ingreslock	A backdoor is installed on the remote host.	Possible malicious installation/execution of **R:\keylogger.exe.** High level of technical knowledge might increase the risk of this attack being successful.	• BGC0686	• PC-7309 • PC-2403
						• KTW0365	• PC-9776
3306	9	High	MySQL / MariaDB weak password	It was possible to login into the remote MySQL as root using weak credentials.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929	• PC-4442
						• ACM2278	• PC-8431
5432	9	High	PostgreSQL weak password	It was possible to login into the remote PostgreSQL as user postgres using weak credentials.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929	• PC-4442
						• ACM2278	• PC-8431
6667	7.5	High	Check for Backdoor in UnrealIRCd	Detection of backdoor in UnrealIRCd.	Possible malicious installation/execution of **R:\keylogger.exe.** High level of technical knowledge might increase the risk of this attack being successful.	• BGC0686	• PC-7309 • PC-2403
						• KTW0365	• PC-9776
6200	7.5	High	vsftpd Compromised Source Packages Backdoor Vulnerability	vsftpd is prone to a backdoor vulnerability.	Possible malicious installation/execution of **R:\keylogger.exe.** High level of technical knowledge might increase the risk of this attack being successful.	• BGC0686	• PC-7309 • PC-2403
						• KTW0365	• PC-9776
21	7.5	High	vsftpd Compromised	vsftpd is prone to a backdoor vulnerability.	Possible malicious installation/execution of **R:\keylogger.exe.**	• BGC0686	• PC-7309 • PC-2403

			Source Packages Backdoor Vulnerability		High level of technical knowledge might increase the risk of this attack being successful.	• KTW0365	• PC-9776
21	7.5	High	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials. As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929	• PC-4442
						• ACM2278	• PC-8431
25	5	Medium	SSL/TLS: Certificate Expired	The remote server's SSL/TLS certificate has already expired.	Possible man-in-the-middle attack for malicious access of data and leakage into the website: http://wikileaks.org. High level of technical knowledge increases the risk of this attack being successful.	• CSF0929	• PC-4442
						• ACM2278	• PC-8431
5432	5	Medium	SSL/TLS: Certificate Expired	The remote server's SSL/TLS certificate has already expired.	Possible man-in-the-middle attack for malicious access of data and leakage into the website: http://wikileaks.org. High level of technical knowledge increases the risk of this attack being successful.	• CSF0929	• PC-4442
						• ACM2278	• PC-8431

80	4.8	Medium	Cleartext Transmission of Sensitive Information via HTTP	The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929 • ACM2278	• PC-4442 • PC-8431
5432	4.3	Medium	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	This host is prone to an information disclosure vulnerability.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929 • ACM2278	• PC-4442 • PC-8431
25	4.3	Medium	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	This host is prone to an information disclosure vulnerability.	Possible malicious access of data and leakage into the website: **http://wikileaks.org** due to employee dissatisfaction or low morale.	• CSF0929 • ACM2278	• PC-4442 • PC-8431

Πίνακας 5.1: Πιθανή Αντιστοιχία Ευπαθειών του Δικτύου με τις Κακόβουλες Ενέργειες στα αρχεία «Insider Data Threats».

Στην συνέχεια, όπως φαίνεται και στην εικόνα 5.1, γίνεται η ανάλυση και η επεξήγηση των 3 παραγόντων που έχουν επιλεγεί για την μεθοδολογία και την προσέγγιση της μεταπτυχιακής διατριβής. Επίσης, παρουσιάζεται η μετατροπή της μεθοδολογίας στην γλώσσα προγραμματισμού «Python» για την δημιουργία του «Cyber Risk Assessment Box». Τέλος, δίνεται η επεξήγηση για τον υπολογισμό της τελικής τιμής του ρίσκου.

5.2 Ανθρώπινοι Παράγοντες

Το πρώτο κομμάτι του προγράμματος αφορά τους ανθρώπινους παράγοντες. Όπως έχει αναφερθεί στο Κεφάλαιο 2, αποτελούν σημαντικό ρόλο στην λειτουργία ενός συστήματος, όπως για παράδειγμα σε ένα οργανισμό.

5.2.1 Μεθοδολογία «Weighted Factor Analysis»

Βάση του NIST [11, 18], έχει γίνει χρήση μιας διαμορφωμένης μεθοδολογίας στηριζόμενη στην μεθοδολογία για εκτίμηση των κινδύνων «Weighted Factor Analysis». Επίσης, η μεθοδολογία της μεταπτυχιακής διατριβής είναι στηριζόμενη στις πληροφορίες από διαδικτυακές βάσεις δεδομένων [15] όπου ανθρώπινες ενέργειες και χαρακτηριστικά είναι πιθανόν να παρουσιάσουν απειλές προς τον οργανισμό. Επομένως, το ρίσκο για πρόκλησης ζημιάς είναι μεγαλύτερο.

Συνεχίζοντας, σύμφωνα με την εικόνα 2.3 στο Κεφάλαιο 2, οι συγγραφείς Henshel κ. ά. [14] τονίζουν ότι το κλίμα εμπιστοσύνης σε ένα οργανισμό και επομένως η σωστή λειτουργία του οργανισμού στηρίζεται σε 2 βασικούς πυλώνες: i) Στα έμφυτα χαρακτηριστικά του ανθρώπου και ii) στα περιστασιακά χαρακτηριστικά. Τα έμφυτα χαρακτηριστικά του ανθρώπου μετά χωρίζονται σε 2 κατηγορίες: i) την ανθρώπινη συμπεριφορά και ii) το επίπεδο γνώσεων. Παράλληλα, τα περιστασιακά χαρακτηριστικά επηρεάζονται από το επίπεδο πρόσβασης που αποκτά ένας χρήστης σε ένα οργανισμό, δηλαδή τις συνθήκες που επικρατούν γύρω του. Οι συγγραφείς αναφέρουν ότι το επίπεδο πρόσβασης μπορεί να περιοριστεί με πολιτική ασφαλείας. Συνεπώς, το επίπεδο πρόσβασης σε ένα οργανισμό μπορεί να αποτελέσει σημαντικό ρόλο στην επιρροή που μπορεί να έχει ένας χρήστης στον οργανισμό αφού οι συνθήκες γύρω του και τα περιστασιακά χαρακτηριστικά πιθανόν να μην του το επιτρέπουν.

Επομένως, η μεταπτυχιακή διατριβή θα επικεντρωθεί στις 3 κύριες κατηγορίες που αφορούν τον ανθρώπινο παράγοντα για την εκτίμηση του ρίσκου:

i) Την ανθρώπινη συμπεριφορά.
ii) Το επίπεδο γνώσεων.
iii) Το επίπεδο πρόσβασης.

Στην συγκεκριμένη ενότητα, θα γίνει αναφορά στο επίπεδο των γνώσεων και το επίπεδο πρόσβασης, ενώ για την ανθρώπινη συμπεριφορά θα γίνει αποκλειστική αναφορά στην Ενότητα 5.3.

Συνεχίζοντας, εκτός από τις πιο πάνω κατηγορίες και βάση της εικόνας 2.2, οι συγγραφείς Diesch, Pfaff και Krcmar [08] υπογραμμίζουν ότι ένα από τα σημαντικά άυλα αγαθά είναι το χαρακτηριστικό της αφοσίωσης που μπορεί να επιδεικνύει ένας εργαζόμενος σε ένα οργανισμό. Ένα στοιχείο που χαρακτηρίζει την αφοσίωση είναι τα χρόνια που ένας εργαζόμενος αποτελεί κομμάτι του οργανισμού. Επομένως, η μεταπτυχιακή διατριβή θα υπολογίσει και το στοιχείο της αφοσίωσης για την εκτίμηση των ρίσκων αφού όσο η αφοσίωση σε ένα οργανισμό μεγαλώνει από ένα εργαζόμενο, το ρίσκο για πρόκληση κακόβουλης ζημιάς μειώνεται. Άρα, η περίοδος εργασίας ενός εργαζομένου σε ένα συγκεκριμένο οργανισμό υποδεικνύει το επίπεδο της αφοσίωσης στον οργανισμό. Επομένως, τα χρόνια εργασίας σε ένα οργανισμό θα συμπεριληφθούν στους υπολογισμούς για την εκτίμηση του ρίσκου.

Συμπερασματικά λοιπόν, η διαμορφωμένη μεθοδολογία του «Weighted Factor Analysis» έχει λάβει υπόψη τους ανθρώπινους παράγοντες που πιθανόν να προκαλέσουν αρνητικά αποτελέσματα σε μια οντότητα. Έτσι, έγινε η επιλογή των πιο κάτω ανθρώπινων χαρακτηριστικών:

i. Χρόνια Εργασίας στον Οργανισμό (Years Worked)
ii. Επίπεδο Πρόσβασης στις Πληροφορίες (Data Access Level)
iii. Επαγγελματικό Επίπεδο – Επίπεδο Γνώσεων (Proficiency/Knowledge Level)

Η συγκεκριμένη μεθοδολογία που έχει αναπτυχθεί για της ανάγκες της μεταπτυχιακής διατριβής, φαίνεται και πιο κάτω στον πίνακα 5.2 με ενδεικτικές τιμές για λόγους επεξήγησης.

	Επιλογή Κριτηρίου 1: **Οικονομική Επίπτωση (Financial Impact)**	Επιλογή Κριτηρίου 2: **Νομική Επίπτωση (Legal Impact)**	Επιλογή Κριτηρίου 3: **Επίπτωση στην Φήμη (Reputational Impact)**	**Συνολικός Συντελεστής**
Συντελεστής Βαρύτητας (%)	40	30	30	
Παράγοντας 1: **Χρόνια Εργασίας στον Οργανισμό (Years Worked)**	5	5	5	**5**
Παράγοντας 2: **Επίπεδο Πρόσβασης στις Πληροφορίες (Data Access Level)**	4	4	4	**4**
Παράγοντας 3: **Επαγγελματικό Επίπεδο – Επίπεδο Γνώσεων (Proficiency/Knowledge**	4	4	4	**4**
Συνολικός Συντελεστής Ρίσκου (Risk Rating)				**13.0**

Πίνακας 5.2: Διαμορφωμένη Μεθοδολογία «Weighted Factor Analysis» για την Διαχείριση των Ρίσκων και Εκτίμηση των Κινδύνων.

Σύμφωνα με την βιβλιογραφία και τις διάφορες μεθοδολογίες που χρησιμοποιούνται για την εκτίμηση των κινδύνων, καθώς και με βάση τον γνώμονα ότι η μεθοδολογία θα συμπεριλαμβάνει και τον ανθρώπινο παράγοντα, το πρώτο βήμα είναι η επιλογή παραγόντων επιρροής. Οι συγκεκριμένοι παράγοντες, όπως έχει αναφερθεί στην βιβλιογραφία, είναι ανθρώπινα χαρακτηριστικά που επηρεάζουν μια οντότητα/οργανισμό και επομένως, είναι αναγκαίο να συμπεριληφθούν στην διαδικασία εκτίμησης των κινδύνων. Επίσης, όπως φαίνεται και στον πίνακα 5.2, οι τιμές που δίνονται στον κάθε παράγοντα αντιπροσωπεύουν το μέγεθος του ρίσκου που θα αποτελέσει ένας παράγοντας στον οργανισμό. Δηλαδή, σε μια κλίμακα **1-5**, δίνεται η τιμή **5** για το **μεγαλύτερο ρίσκο** που θα αποτελέσει στον οργανισμό, ενώ δίνεται η τιμή **1** για το **μικρότερο ρίσκο** που θα αποτελέσει στον οργανισμό. Επιπλέων, βάση των πληροφοριών που έχουν ήδη παρουσιαστεί στο Κεφάλαιο 5, η κλίμακα όχι μόνο δηλώνει το μέγεθος του ρίσκου, αλλά παρουσιάζει και τον βαθμό των πιθανοτήτων που κάθε παράγοντας μπορεί να επηρεάσει τον οργανισμό.

Επίσης, πρέπει να σημειωθεί ότι στην προσπάθεια διαμόρφωσης μιας ποσοτικής μεθοδολογίας για την εκτίμηση των κινδύνων, ο χρήστης θα κληθεί να τοποθετήσει τιμές αποτυπώνοντας σε ποσοτικές μονάδες ποιοτικά δεδομένα. Ακόμη, όπως έχει ήδη αναφερθεί, το ρίσκο είναι ίσο με το μέγεθος της ζημιάς και τις πιθανότητες υλοποίησης μιας απειλής (Risk = Impact x Probability). Επομένως, η συγκεκριμένη μεθοδολογία στηρίζεται σε αυτή την μαθηματική σχέση, όπου όσο αυξάνονται οι πιθανότητες υλοποίησης ζημιάς στον οργανισμό, το ρίσκο στην κλίμακα 1-5 αυξάνεται. Επιπλέων, είναι αναγκαίο να σημειωθεί ότι σε περίπτωση υπολογισμού συνολικού ρίσκου σε ένα οργανισμό και όχι ατομικού για κάθε χρήστη, τότε οι μέσες τιμές θα χρησιμοποιηθούν στην κλίμακα του ρίσκου 1-5.

5.2.2 Επιλογή Ανθρώπινων Παραγόντων

Στην συγκεκριμένη υπό-ενότητα δίνεται επεξήγηση για την επιλογή των συγκεκριμένων ανθρώπινων παραγόντων και πως χρησιμοποιούνται στην συγκεκριμένη μεθοδολογία:

i. **Χρόνια Εργασίας στον Οργανισμό (Years Worked)**

   Όσα περισσότερα χρόνια έχει εργαστεί ένας χρήστης σε ένα οργανισμό, τόσο λιγότερες είναι οι πιθανότητες να προκαλέσει ζημιά στον οργανισμό, επειδή θα είναι εκτεθειμένος περισσότερο χρόνο στο περιβάλλον της εργασίας του και οι πιθανότητες εντοπισμού ύποπτων ενεργειών θα είναι αυξημένες. Επομένως, το ρίσκο που παρουσιάζει ο

συγκεκριμένος χρήστης θα κυμαίνεται σε χαμηλά επίπεδα. Παράλληλα, τα στοιχεία της αφοσίωσης και της εμπιστοσύνης στον οργανισμό ενισχύονται. Συνεπώς, ένας εργαζόμενος με αρκετά χρόνια υπηρεσίας σε ένα οργανισμό παρουσιάζει λιγότερες πιθανότητες υλοποίησης μιας κακόβουλης ενέργειας συγκριτικά με ένα εργαζόμενο με λιγότερα χρόνια εργασίας στον οργανισμό.

Στην συγκεκριμένη μεθοδολογία δίνεται τιμή 5 (μεγαλύτερο ρίσκο/πιθανότητες ζημιάς) αν ένας υπάλληλος έχει εργαστεί σχετικά λίγα χρόνια στον οργανισμό, ενώ δίνεται η τιμή 1 (ελάχιστο ρίσκο/πιθανότητες ζημιάς) αν έχει εργαστεί σχετικά αρκετά χρόνια στον οργανισμό. Οι τιμές 2,3,4 δίνονται αναλόγως με τα σχετικά χρόνια εργασίας στον οργανισμό.

ii. Επίπεδο Πρόσβασης στις Πληροφορίες (Data Access Level)

Το ρίσκο είναι μεγαλύτερο όταν το επίπεδο πρόσβασης στις πληροφορίες ενός οργανισμού δεν είναι αρκετά περιορισμένο βάση και των πολιτικών ασφαλείας. Πιθανές κακόβουλες ενέργειες είναι η διαρροή, τροποποίηση ή διαγραφή πληροφοριών και ευαίσθητων δεδομένων.

Δηλαδή, στην περίπτωση που η πρόσβαση σε κρίσιμες/ευαίσθητες πληροφορίες του οργανισμού δεν είναι περιορισμένη ή ελεγχόμενη, τότε οι πιθανότητες υλοποίησης μιας κακόβουλης ενέργειας είναι περισσότερες. Άρα, η τιμή για το ρίσκο είναι η μεγαλύτερη, δηλαδή 5 στην κλίμακα της μεθοδολογίας.

iii. Επαγγελματικό Επίπεδο – Επίπεδο Γνώσεων (Proficiency/Knowledge Level)

Το επαγγελματικό επίπεδο και το επίπεδο γνώσεων μπορεί να καθορίσουν αν ένας χρήστης είναι σε θέση να πραγματοποιήσει μια επιτυχημένη επίθεση σε ένα οργανισμό και να προκαλέσει ζημιά. Ένας χρήστης με υψηλό επίπεδο γνώσεων στην πληροφορική και στην ασφάλεια υπολογιστών και δικτύων μπορεί να έχει τις απαραίτητες γνώσεις που χρειάζεται για να προκαλέσει ζημιά στον οργανισμό. Για παράδειγμα, χρησιμοποιώντας κακόβουλα λογισμικά όπως το «keylogger», ο χρήστης θα μπορεί να παρακολουθεί ενέργειες άλλων χρηστών που πιθανόν να οδηγήσει και σε διαρροή πληροφοριών [07].

Επομένως, όσο μεγαλύτερο είναι το επαγγελματικό επίπεδο και το επίπεδο γνώσεων, τόσες μεγαλύτερες είναι οι πιθανότητες πρόκλησης ζημιάς. Συνεπώς, το ρίσκο και η τιμή στην κλίμακα της μεθοδολογίας πλησιάζει τον βαθμό 5.

5.2.3 Κριτήρια Βαρύτητας

Στην συγκεκριμένη μεθοδολογία έχουν επιλεγεί 3 κριτήρια τα οποία υπογραμμίζουν την επίδραση που μπορεί να παρουσιάσουν σε ένα οργανισμό. Οι συγγραφείς Haaker κ. ά. [13] περιγράφουν ότι για την δημιουργία ενός επιτυχημένου επιχειρηματικού σχεδίου είναι αναγκαίο να ληφθεί υπόψη: i) τα έσοδα της επιχείρησης, ii) η ασφάλεια που θα παρέχουν οι συνεταίροι στην επιχείρηση, καθώς και iii) οι σχέσεις με τους πελάτες. Επομένως, τονίζεται η ανάγκη για προστασία της επιχείρησης από οικονομικές και νομικές επιπτώσεις. Επίσης, ένα σημαντικό στοιχείο για την διατήρηση καλών σχέσεων με τους πελάτες και η επιτυχής προσέγγιση νέων πελατών είναι η εικόνα της επιχείρησης. Συνεπώς, η «φήμη» της επιχείρησης διαδραματίζει σημαντικό ρόλο για την επιτυχία των υπηρεσιών που προσφέρει.

Αυτό οδηγεί στην επιλογή των πιο κάτω κριτηρίων που επηρεάζουν άμεσα ένα οργανισμό. Όμως, πρέπει να σημειωθεί ότι η βαρύτητα που αναλογεί σε κάθε κριτήριο αλλάζει, σύμφωνα πάντα με το επιχειρηματικό σχέδιο που ακολουθεί ο κάθε οργανισμός. Τα κριτήρια που έχουν επιλεγεί είναι:

i. Οικονομική Επίπτωση (Financial Impact)
ii. Νομική Επίπτωση (Legal Impact)
iii. Επίπτωση στην Φήμη (Reputational Impact)

Επομένως, γίνεται χρήση **συντελεστής βαρύτητας (%)**. Έτσι, οι παράγοντες που έχουν επιλεγεί θα πολλαπλασιάζονται με την σειρά με τον συντελεστή βαρύτητας του κάθε κριτηρίου και θα παρουσιάζουν στο τέλος ένα συνολικό συντελεστή. Με αυτό τον τρόπο παρουσιάζεται η επίδραση του κάθε παράγοντα στο κάθε κριτήριο. Όπως φαίνεται και στον πίνακα 5.2, έχουν δοθεί οι τιμές 40% για τις οικονομικές επιπτώσεις, 30% για τις νομικές επιπτώσεις και 30% για τις επιπτώσεις στην φήμη του οργανισμού. Η συγκεκριμένες βαρύτητες που έχουν επιλεγεί μπορούν να κυμανθούν σε διάφορα επίπεδα ανάλογος με το επιχειρηματικό πλάνο και τους στόχους του οργανισμού. Σε ένα οργανισμό όπου δίνεται ιδιαίτερη σημασία στις οικονομικές επιπτώσεις που μπορεί να προκληθούν, τότε ο συντελεστής βαρύτητας μπορεί να έχει την τιμή 50%. Ακόμη,

μπορεί να γίνει χρήση και άλλων κριτηρίων, όπως για παράδειγμα επιπτώσεις σε μελλοντικούς στόχους που θέτει ο οργανισμός.

5.2.4 Υπολογισμός Συνολικού Συντελεστή Ρίσκου

Στην συνέχεια, υπολογίζεται ο συνολικός συντελεστής για τον παράγοντα 1 (Χρόνια Εργασίας στον Οργανισμό). Γίνεται η μαθηματική πράξη πολλαπλασιασμού μεταξύ των τιμών του ρίσκου που τοποθετήσαμε στον παράγοντα 1 με την βαρύτητα του κάθε κριτηρίου ξεχωριστά. Δηλαδή, γίνεται η πράξη (5x40%)+(5x30%)+(5x30%) = **5**. Το αποτέλεσμα (5) είναι ο συνολικός συντελεστής για τον παράγοντα 1 (Χρόνια Εργασίας). Με αυτό τον τρόπο υπολογίζονται οι συνολικοί συντελεστές για όλους τους παράγοντες. Για τον παράγοντα 2 (Επίπεδο Πρόσβασης Πληροφοριών), γίνεται η πράξη (4x40%)+(4x30%)+(4x30%) = **4**, ενώ για τον παράγοντα 3 (Επίπεδο Γνώσεων), γίνεται η πράξη (4x40%)+(4x30%)+(4x30%) = **4.** Ακολούθως, γίνεται η πρόσθεση όλων των συντελεστών των παραγόντων για να αποκτήσουμε τον τελικό συντελεστή ρίσκου. Δηλαδή, γίνεται η πρόσθεση **5+4+4= 13**. Ο συνολικός συντελεστής ρίσκου (risk rating) είναι ίσο με **13** ο οποίος υποδεικνύει το «risk rating» για ένα συγκεκριμένο χρήστη.

Όμως, είναι σημαντικό να σημειωθεί ότι σε περίπτωση που πραγματοποιείται εκτίμηση του ρίσκου σε ένα ολόκληρο οργανισμό τότε είναι αναγκαίο να γίνει χρήση μέσων τιμών για κάθε παράγοντα, έτσι ώστε το αποτέλεσμα του «risk rating» να αντιπροσωπεύει όλο τον οργανισμό. Επομένως, τονίζεται η ευελιξία της μεθοδολογίας αφού έχει την δυνατότητα να πραγματοποιεί εκτίμηση του ρίσκου i) για κάθε χρήστη ξεχωριστά αλλά και ii) σε ένα ολόκληρο οργανισμό, βάση των ανθρώπινων παραγόντων και της διαμορφωμένης μεθοδολογίας «Weighted Factor Analysis».

5.2.5 Μετατροπή Μεθοδολογίας στην Γλώσσα Προγραμματισμού «Python» στο εργαλείο «Spyder3».

Αρχικά ο χρήστης του προγράμματος επιλέγει την ανάλογη βαρύτητα για τους παράγοντες που έχουν επιλεγεί. Η βαρύτητα είναι σε ποσοστό και το άθροισμά τους είναι ίσο με 100% (Εικόνα 5.2).

i. **riskr_weight**
   Βαρύτητα για τον υπολογισμό του ρίσκου βάση των ανθρώπινων παραγόντων.

ii. **ba_weight**
   Βαρύτητα για τον υπολογισμό του ρίσκου βάση της ανάλυσης της ανθρώπινης συμπεριφοράς.

iii. **va_weight**
   Βαρύτητα για τον υπολογισμό του ρίσκου βάση τον εντοπισμό ευπαθειών στα πληροφοριακά συστήματα.

```
riskr_weight = 25 #Section 1, Risk Rating Weight in Percentage.
ba_weight = 50    #Section 2, Behavioural Analysis Weight in Percentage.
va_weight = 25    #Section 3, Vulnerability Assessment Weight in Percentage.
```

Εικόνα 5.2: Βαρύτητα Παραγόντων Μεθοδολογίας.

Μετά, ο χρήστης του προγράμματος καλείται να τοποθετήσει τιμές για τα 2 πρώτα κριτήρια **«weight1»** και **«weight2»** στο παράθυρο αλληλεπίδρασης με τον χρήστη, ενώ ο υπολογισμός του **«weight3»** γίνεται αυτόματα αφού το σύνολο των 3 κριτηρίων είναι ίσο με 100% (Εικόνα 5.3).

Όπως φαίνεται και στην εικόνα 5.3, ο κώδικας αναφέρεται στα 3 κριτήρια που έχουν επιλεγεί:

i. weight1 = Βαρύτητα για την Οικονομική Επίπτωση (Financial Impact)
ii. weight2 = Βαρύτητα για την Νομική Επίπτωση (Legal Impact)
iii. weight3 = Βαρύτητα για την Επίπτωση στην Φήμη (Reputational Impact)

Επίσης, για σκοπούς ευχρηστίας είναι αποδεκτή μόνο η τοποθέτηση ακέραιων αριθμών και τιμών μεγαλύτερων ή ίσο με το 0.

```
#SECTION 1: Risk Rating#

#The first section of the program covers manual user input.
#It is based on the Risk Management Methodology: Weighted Factor Analysis.
#User defines the Weight of each of the 3 selected Citeria: Financial Impact, Legal Impact and Reputational Impac
#The weight values of these criteria depend on decision-making by the entity and the importance it perceives each

#Financial Impact Criterion Weight
weight1 = input ("Enter a % value for Financial Impact Criterion Weight between 1%-100%: ") #Program asks for an
while not float(weight1) in range(1,101): #Input value should be in the range 0% - 100%.
   weight1 = input("Please enter an integer % value for Financial Impact Criterion Weight between 1%-100%: ") #In
financial_impact = int(weight1) #Input value should is an integer.

#Legal Impact Criterion Weight
weight2 = input ("Enter a % value for Legal Impact Criterion Weight between 1%-100%: ") #Program asks for an inpu
while not float(weight2) in range(0,100): #Input value should be in the range 0% - 100%.
   weight2 = input("Please enter an integer % value for Legal Impact Criterion Weight between 1%-100%: ") #In cas
legal_impact  = int(weight2) #Input value should is an integer.

#Reputational Impact Criterion Weight
weight3 = (100 - (financial_impact + legal_impact)) #Automatic calculation of the final criterion, Reputational I
reputational_impact = int(weight3) #The value for the Reputational Impact Criterion is an integer value.

#Checking that the values for the 3 Criteria add up to 100%.
if reputational_impact >= 0:
    print("\n""% value of Reputational Impact Criterion Weight is: " + str(reputational_impact))

else:
    print("\n""Error! Please re-start the program") #In case the values for the 3 Criteria do not add up to 100%,
```

Εικόνα 5.3: Καθορισμός των 3 Κριτηρίων «weight1», «weight2» και «weight3».

Συνεχίζοντας, η εικόνα 5.4 παρουσιάζει ένα μέρος του κώδικα όπου ο χρήστης καλείται να τοποθετήσει τιμές στο παράθυρο αλληλεπίδρασης για τις πιθανότητες που παρουσιάζει ο κάθε ανθρώπινος παράγοντας για να προκαλέσει ζημιά στον οργανισμό. Δηλαδή, το ρίσκο που αντιμετωπίζει το κάθε κριτήριο από κάθε ανθρώπινο παράγοντα ξεχωριστά. Οι τιμές που χρησιμοποιούνται είναι βάση της κλίμακας που έχει ήδη αναφερθεί στο Κεφάλαιο 5, ενώ για σκοπούς ευχρηστίας η τιμή είναι ένας ακέραιος αριθμός μεταξύ 1-5.

Ακόμη, πρέπει να σημειωθεί ότι το συγκεκριμένο μέρος του κώδικα επαναλαμβάνεται 3 φορές για να καλύψει όλους τους παράγοντες. Η εικόνα 5.4 παρουσιάζει την τοποθέτηση τιμής για το ρίσκο του ανθρώπινου παράγοντα «Χρόνια Εργασίας στον Οργανισμό (Years Worked)» που παρουσιάζεται ως προς το κριτήριο «Οικονομική Επίπτωση (Financial Impact)».
Επομένως, η τιμή που τοποθετείται από τον χρήστη ταυτίζεται με την ονομασία στον κώδικα «HF1_rating1». Για την επιρροή του παράγοντα «Χρόνια Εργασίας στον Οργανισμό (Years Worked)» στο Νομικό Πλαίσιο , η ονομασία στον κώδικα είναι «HF1_rating2». Έτσι, η επιρροή του συγκεκριμένου παράγοντα στην Φήμη του οργανισμού, έχει την ονομασία «HF1_rating3».

Με την ίδια προσέγγιση, ο παράγοντας του Επιπέδου Πρόσβασης έχει την ονομασία «HF2_ratingX» στον κώδικα, ενώ ο παράγοντας του Επιπέδου Γνώσεων έχει την ονομασία «HF3_ratingX».

```
#Impact of Years Worked Factor on the Financial Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
HF1a = input ("Enter a value for Years Worked Factor with Financial Impact: ")
while not float(HF1a) in range(1,6):
    HF1a = input("Please enter an integer value between 1-5: ") #Error Message displayed
HF1_rating1 = int(HF1a)

#Impact of Years Worked Factor on the Legal Criterion.
#Range = 1-5.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
HF1b = input ("Enter a value for Years Worked Factor with Legal Impact: ")
while not float(HF1b) in range(1,6):
    HF1b = input("Please enter an integer value between 1-5: ") #Error Message displayed
HF1_rating2 = int(HF1b)

#Impact of Years Worked Factor on the Reputational Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
HF1c = input ("Enter a value for Years Worked Factor with Reputational Impact: ")
while not float(HF1c) in range(1,6):
    HF1c = input("Please enter an integer value between 1-5: ") #Error Message displayed
HF1_rating3 = int(HF1c)
```

Εικόνα 5.4: Τοποθέτηση τιμών για τις πιθανότητες ζημιάς από τον κάθε παράγοντα.

Έπειτα, όπως παρουσιάζεται και στην εικόνα 5.5, γίνεται ο υπολογισμός του Συνολικού Συντελεστή Ρίσκου (Risk Rating) για τους ανθρώπινους παράγοντες. Πρώτα όμως, υπολογίζονται ξεχωριστά οι συντελεστές του ρίσκου που παρουσιάζει ο κάθε ανθρώπινος παράγοντας: i) risk_HF1, ii) risk_HF2, iii) risk_HF3. Μετά, γίνεται η πρόσθεση των συντελεστών του ρίσκου για να υπολογιστεί ο συνολικός συντελεστής του ρίσκου.

```
#Risk Rating Calculation based on the user input values regarding Criteria Weights and Impact Factors.
#Mathematical multiplication is being carried out between the above human factors and the criteria weights.
risk_HF1 = (HF1_rating1*(financial_impact/100)) + (HF1_rating2*(legal_impact/100)) + (HF1_rating3*(reputational_impact/100))
risk_HF2 = (HF2_rating1*(financial_impact/100)) + (HF2_rating2*(legal_impact/100)) + (HF2_rating3*(reputational_impact/100))
risk_HF3 = (HF3_rating1*(financial_impact/100)) + (HF3_rating2*(legal_impact/100)) + (HF3_rating3*(reputational_impact/100))

#Mathematical addition provides a sum of the risk of the above human factors.
#The result is named as risk rating.
risk_rating = risk_HF1 + risk_HF2 + risk_HF3

print("\n")

#Value of Risk Rating for Section 1.

print("\n""Value for Risk Rating: ")
print(risk_rating)
```

Εικόνα 5.5: Υπολογισμός Συνολικού Συντελεστή Ρίσκου από τους Ανθρώπινους Παράγοντες.

Τέλος, βάση της εικόνας 5.6, το αποτέλεσμα του συνολικού ρίσκου από τους ανθρώπινους παράγοντες παρουσιάζεται στο παράθυρο αλληλεπίδρασης του χρήστη ως ποσοστό (%). Αυτό είναι ίσο με τον πολλαπλασιασμό του συνολικού συντελεστή ρίσκου, **risk_rating** και της βαρύτητας, **riskr_weight** και την διαίρεση με την τιμή **15**. Η τιμή 15 λειτουργεί σαν βάση στους υπολογισμούς αφού είναι το μέγιστο πιθανόν αποτέλεσμα που μπορεί να έχει ο συνολικός συντελεστής ρίσκου.

```
#Value of Risk Rating for Section 1 in Percentage, taking into account that maximum risk rating value is equal to 15.
risk_rating_perc = (risk_rating*riskr_weight)/15

print("\n")

print("Risk Rating in %: " + str(risk_rating_perc))

print("\n")
```

Εικόνα 5.6: Υπολογισμός του Ρίσκου από τους Ανθρώπινους Παράγοντες.

5.3 Ανάλυση Ανθρώπινης Συμπεριφοράς (Behavioural Analysis)

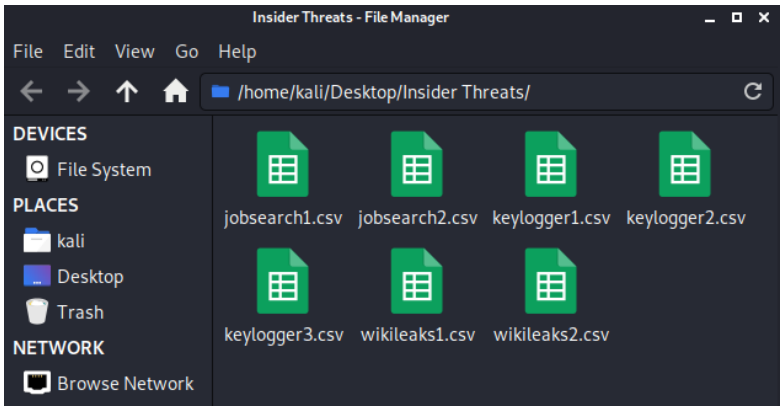
Η ενότητα παρουσιάζει την προσέγγιση της μεταπτυχιακής διατριβής ως προς τον υπολογισμό του ρίσκου βάση της ανθρώπινης συμπεριφοράς. Για να γίνει αυτό εφικτό, ήταν αναγκαίο να χρησιμοποιηθεί η γλώσσα προγραμματισμού «Python» στο εργαλείο «Spyder3», αφού επιτρέπει στον χρήστη να πραγματοποιήσει δύσκολες μαθηματικές πράξεις. Επίσης, με το κάλεσμα διάφορων βιβλιοθηκών, ο χρήστης έχει στα χέρια του εργαλεία που του παρέχουν περισσότερες δυνατότητες για την υλοποίηση πιο περίπλοκων ενεργειών.

Ακόμη, για τους σκοπούς της ανάλυσης της συμπεριφοράς, έχουν χρησιμοποιηθεί τα παραδείγματα των αρχείων καταγραφής δεδομένων από εσωτερικές απειλές [15]. Επομένως, τα αρχεία αυτά σε τύπο **.csv**, αντιπροσωπεύουν πιθανά σενάρια όπου η ανάλυση της συμπεριφοράς θα ήταν απαραίτητη. Η εικόνα 5.7 παρουσιάζει ένα παράδειγμα αρχείου καταγραφής δεδομένων, όπου οι διάφορες πληροφορίες έχουν κατηγοριοποιηθεί. Στο συγκεκριμένο παράδειγμα, ο χρήστης BGC0686 φαίνεται να κατεβάζει ένα κακόβουλο λογισμικό «keylogger» στους υπολογιστές PC-7309 και PC-2403 και ακολούθως να τρέχει το συγκεκριμένο κακόβουλο λογισμικό. Πιθανόν για παράνομη παρακολούθηση χρηστών.

	A	B	C	D	E	F	G	H	I
1	Action	Number	Timestamp	User	Device	Activity			
2	http	{D5T6-M5VT84TZ-2060CMUL}	11/11/2010 15:26	BGC0686	PC-7309	http://www.relytec.com/Climate_of_Florida,			
3	device	{I7N3-C6FQ76CA-8308ILFR}	11/11/2010 15:37	BGC0686	PC-7309	R:\;R:\BGC0686;R:\24h64f6			
4	file	{H2Q6-Q8BN31JU-1543XFZN}	11/11/2010 15:41	BGC0686	PC-7309	R:\keylogger.exe			
5	logon	{R7E5-S2JM42GS-7498OOCE}	11/11/2010 19:30	BGC0686	PC-2403	Logon			
6	device	{P5H6-P3MD58MX-6958TXCW}	11/11/2010 19:33	BGC0686	PC-2403	R:\;R:\BGC0686;R:\24h64f6			
7	file	{N8F5-R2LW02MY-3271EKFS}	11/11/2010 19:35	BGC0686	PC-2403	R:\keylogger.exe			
8	logon	{Z5L0-D9QV40MP-8876JIMI}	11/11/2010 19:39	BGC0686	PC-2403	Logoff			
9	logon	{M9I7-X7DG75MJ-7915BAHF}	11/12/2010 19:08	BGC0686	PC-2403	Logon			
10	logon	{X7T4-H2BI85LN-2210PAMF}	11/12/2010 19:22	BGC0686	PC-2403	Logoff			
11	logon	{T7Y4-B3HS66WG-3205FOAI}	11/12/2010 19:29	DKB0259	PC-2403	Logon			

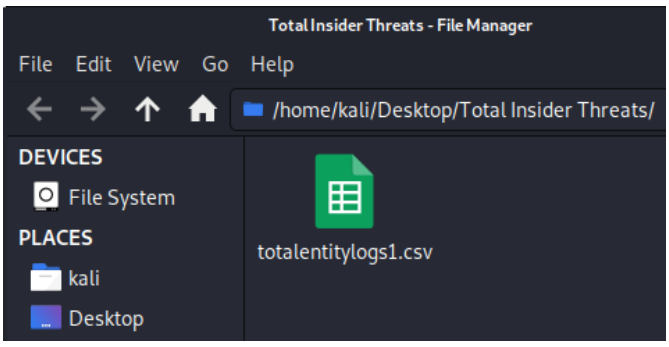
Εικόνα 5.7: Παράδειγμα Αρχείου Καταγραφής Δεδομένων [15].

Όπως φαίνεται και στην πιο κάτω εικόνα 5.8, τα αρχεία καταγραφής δεδομένων έχουν αποθηκευτεί από την συγκεκριμένη πηγή σε τύπο **.csv**, έτσι ώστε να μπορούν να αξιοποιηθούν κατάλληλα από το πρόγραμμα στην γλώσσα παραγραμματισμού «Python» για τους σκοπούς της ανάλυσης της ανθρώπινης συμπεριφοράς.



Εικόνα 5.8: Αρχεία Καταγραφής Δεδομένων σε τύπο .csv [15].

Συνεχίζοντας, όπως παρουσιάζει και η πιο πάνω εικόνα 5.8, το κάθε αρχείο **.csv** περιέχει κακόβουλες ενέργειες των χρηστών σε ένα οργανισμό όπου υπάρχει μια ενδεικτική ονομασία του κάθε αρχείου με την κύρια απειλή. Ακολούθως, όπως φαίνεται και στην εικόνα 5.9, οι ενέργειες των χρηστών από τα παραδείγματα των αρχείων καταγραφής συμβάντων, έχουν ενοποιηθεί σε ένα νέο αρχείο **«totalentitylogs1.csv»**. Δηλαδή, τα δεδομένα των αρχείων της εικόνας 5.8 έχουν τοποθετηθεί μαζί στο ίδιο αρχείο όπως δείχνει η εικόνα 5.9. Το συγκεκριμένο αρχείο χρησιμοποιείται στην μεταπτυχιακή διατριβή για τους σκοπούς της εκτίμησης του ρίσκου σε ένα οργανισμό βάση της ανάλυσης της ανθρώπινης συμπεριφοράς.



Εικόνα 5.9: Νέο Αρχείο Καταγραφής Δεδομένων «totalentitylogs1.csv».

Η εικόνα 5.10 παρουσιάζει ένα μέρος με τα περιεχόμενα του συγκεκριμένου αρχείου καταγραφής δεδομένων, ενώ ολόκληρο το αρχείο παρουσιάζεται στο Παράρτημα Β.

	A	B	C	D	E	F
1	Action	Number	Timestamp	User	Device	Activity
2	email	{B1Y9-Z7AR66CW-9353ONTE}	11/11/2010 10:21	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com
3	email	{A5Q3-L7MS05UI-3620UQII}	11/11/2010 10:22	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
4	email	{B2P6-F0ST65UC-0302NJJA}	11/11/2010 13:03	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
5	email	{T1C8-Q7CC58LS-7289GJFY}	11/11/2010 13:04	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com
6	email	{Z5M1-A0TV56TL-3102CFDH}	11/11/2010 13:39	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com
7	email	{K6C7-X6NX01ET-4527SHPO}	11/11/2010 13:40	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
8	email	{M4V2-C8ZS86KH-5652MPGJ}	11/11/2010 13:46	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
9	email	{B4Q0-W5QX16RW-7102LCFN}	11/11/2010 13:47	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com
10	http	{D5T6-M5VT84TZ-2060CMUL}	11/11/2010 15:26	BGC0686	PC-7309	http://www.relytec.com/Climate_of_Florida/suniest/NNXrlybttre1893061997.aspx
11	device	{I7N3-C6FQ76CA-8308ILFR}	11/11/2010 15:37	BGC0686	PC-7309	R:\;R:\BGC0686;R:\24h64f6
12	file	{H2Q6-Q8BN31JU-1543XFZN}	11/11/2010 15:41	BGC0686	PC-7309	R:\keylogger.exe
13	logon	{R7E5-S2JM42GS-7498OOCE}	11/11/2010 19:30	BGC0686	PC-2403	Logon
14	device	{P5H6-P3MD58MX-6958TXCW}	11/11/2010 19:33	BGC0686	PC-2403	R:\;R:\BGC0686;R:\24h64f6
15	file	{N8F5-R2LW02MY-3271EKFS}	11/11/2010 19:35	BGC0686	PC-2403	R:\keylogger.exe
16	logon	{Z5L0-D9QV40MP-8876JIMI}	11/11/2010 19:39	BGC0686	PC-2403	Logoff
17	logon	{M9I7-X7DG75MJ-7915BAHF}	11/12/2010 19:08	BGC0686	PC-2403	Logon
18	logon	{X7T4-H2BI85LN-2210PAMF}	11/12/2010 19:22	BGC0686	PC-2403	Logoff
19	logon	{T7Y4-B3HS66WG-3205FOAI}	11/12/2010 19:29	DKB0259	PC-2403	Logon
20	email	{B5N4-C7IX58TM-0955XNDA}	11/12/2010 19:37	DKB0259	PC-2403	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;
21	logon	{N8N4-X0WB23KK-1872ALNE}	11/12/2010 19:44	DKB0259	PC-2403	Logoff
22	email	{L0A1-W9AB34GS-6692RUSO}	11/15/2010 07:31:00	MAH0683	PC-4972	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;
23	email	{Q7J8-Z5HV63PJ-8605VMZP}	11/15/2010 07:41:00	RNW0269	PC-0978	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;

Εικόνα 5.10: Περιεχόμενα Αρχείου Καταγραφής Δεδομένων «totalentitylogs1.csv.

Συνεχίζοντας με το πρόγραμμα, καλείτε η βιβλιοθήκη **«panda as pd»**. Η συγκεκριμένη βιβλιοθήκη επιτρέπει στον χρήστη να εκτελέσει εντολές για να διαβαστεί και να επεξεργαστεί ένα αρχείο **.csv**. Επομένως, χρησιμοποιείται η εντολή **import pandas as pd.**

Όπως έχει ήδη αναφερθεί πιο πάνω και όπως φαίνεται στην εικόνα 5.11, για να είναι εφικτό το διάβασμα του αρχείου καταγραφής δεδομένων «**totalentitylogs1.csv**» γίνεται η χρήση της εντολής **df=pd.read_csv("totalentitylogs1.csv")**.

```
#The program reads the report containing the activity of users.
df = pd.read_csv("totalentitylogs1.csv")
```

Εικόνα 5.11: Εντολή για Διάβασμα του Αρχείου Καταγραφής Δεδομένων «**totalentitylogs1.csv**».

Στην συνέχεια, βάση της εικόνας 5.12, γίνεται σάρωση από το πρόγραμμα στο συγκεκριμένο αρχείο για εντοπισμό συγκεκριμένων λέξεων-κλειδιά που έχουν ήδη καταχωρηθεί με την εντολή **df[df.Activity.str.contains('wikileaks', na=False) | df.Activity.str.contains('keylogger', na=False) | df.Activity.str.contains('Keylogger', na=False)] = 1**. Η συγκεκριμένη εντολή πραγματοποιεί αναζήτηση των λέξεων «wikileaks», «keylogger» και «Keylogger» στην κατηγορία «Activity» και σε περίπτωση εντοπισμού των συγκεκριμένων λέξεων, γίνεται άμεση αντικατάσταση με τον αριθμό 1. Στην αντίθετη περίπτωση γίνεται αντικατάσταση των υπόλοιπων λέξεων με τον αριθμό 0, χρησιμοποιώντας την εντολή **df.loc[df["Activity"] != 1, "Activity"] = 0**.

Η αναζήτηση της λέξης «wikileaks» πραγματοποιείται για τον εντοπισμό κακόβουλων ενεργειών στην γνωστή ιστοσελίδα διαρροής δεδομένων «wikileaks.org». Σε περίπτωση μιας τέτοιας κακόβουλης ενέργειας από ένα εργαζόμενο, πιθανόν να οδηγήσει σε διαρροή ευαίσθητων πληροφοριών και ιδιωτικών δεδομένων του οργανισμού. Συνεπώς, ο οργανισμός μπορεί να έχει νομικές και οικονομικές επιπτώσεις, καθώς και αρνητικές συνέπειες στην εικόνα του οργανισμού. Επίσης, οι λέξεις-κλειδιά που χρησιμοποιούνται «keylogger» και «Keylogger», εντοπίζουν κακόβουλες ενέργειες από την χρήση του συγκεκριμένου κακόβουλου λογισμικού με σκοπό την παράνομη παρακολούθηση κάποιου χρήστη [07]. Το συγκεκριμένο λογισμικό, καταγράφει και παρακολουθεί τις πληκτρολογήσεις που πραγματοποιούνται στο πληκτρολόγιο του υπολογιστή κάποιου χρήστη. Συνεπώς, το ρίσκο από μια τέτοια κακόβουλη ενέργεια αυξάνεται.

```
#Keywords were selected to be identified in the Behavioural Analysis procedure, by reading the activity report.
#In the instance that a keyword is being matched in the activity report, then the numerical value 1 replaces the particular word in the report.
#The remaining words in the activity report that are not matched, are replaced with the numerical value 0.
df[df.Activity.str.contains('wikileaks', na=False) | df.Activity.str.contains('keylogger', na=False) | df.Activity.str.contains('Keylogger', na=False) ] = 1
df.loc[df["Activity"] != 1, "Activity" ] = 0
```

Εικόνα 5.12: Εντολή για Εντοπισμό Λέξεων-Κλειδιά.

Έπειτα, με την εντολή **df.to_csv("HighRisk.csv", index=False)**, δημιουργείται ένα καινούργιο αρχείο, «HighRisk.csv» περιέχοντας τους αριθμούς 1 και 0 στην κατηγορία «Activity» που έχουν αντικατασταθεί με την προηγούμενη εντολή (Εικόνα 5.13). Συνεπώς, το συγκεκριμένο αρχείο περιέχει ενδείξεις για ενέργειες που μπορεί να προκαλέσουν σοβαρές ζημιές στον οργανισμό. Έτσι, γίνεται εντοπισμός ενεργειών όπου το μέγεθος της ζημιάς που πιθανόν να προκαλέσουν είναι μεγάλο.

```
#New report is being generated, named as High Risk report
df.to_csv("HighRisk.csv", index=False)
```

Εικόνα 5.13: Εντολή για Δημιουργία Αρχείου «HighRisk.csv».

Ακολούθως, με την εντολή **high_risk_activity_values = pd.read_csv("HighRisk.csv", usecols = ["Activity"])**, το πρόγραμμα διαβάζει την κατηγορία «Activity» από το καινούργιο αρχείο που έχει δημιουργηθεί, «HighRisk.csv», περιέχοντας τους αριθμούς 1 και 0 (Εικόνα 5.14).

```
#The program now reads the Activity column of the newly generated High Risk report.
#The numerical value 1 is an indication of a high risk incident.
high_risk_activity_values = pd.read_csv("HighRisk.csv", usecols = ["Activity"])
print("\n", high_risk_activity_values)
```

Εικόνα 5.14: Εντολή για Διάβασμα Αρχείου «HighRisk.csv».

Στην συνέχεια, όπως φαίνεται και στην εικόνα 5.15, πραγματοποιείται μαθηματική πρόσθεση των ενδείξεων που έχουν καταγραφεί με την ονομασία **high_risk_activity_values** (ενέργειες «υψηλής» σοβαρότητας). Δηλαδή, άθροισμα των τιμών 1 που έχουν αντικαταστήσει τις λέξεις-κλειδιά στο αρχείο «HighRisk.csv». Η εντολή που χρησιμοποιείται είναι **print(high_risk_activity_values["Activity"].sum())**.

```
#The program sums up the numerical values in the Activity column and prints out the result.
#The result represents a total idication of High Risk User Activity.
print("\n""Total Indications from High Risk User Activity: ")
print(high_risk_activity_values["Activity"].sum())
```

Εικόνα 5.15: Εντολή για Πρόσθεση των Τιμών για Ενέργειες «Υψηλής» Σοβαρότητας.

Επίσης, πρέπει να σημειωθεί ότι το αποτέλεσμα παρουσιάζει στον χρήστη: i) ενδείξεις για την επίδραση που παρουσιάζει μια απειλή (Impact), εφόσον εντοπιστούν οι λέξεις-κλειδιά, αλλά και ii) τις πιθανότητες υλοποίησης μιας επιτυχημένης κακόβουλης επίθεσης, αφού η ίδια κακόβουλη ενέργεια μπορεί να εντοπιστεί παραπάνω από 1 φορά. Άρα, οι πιθανότητες για την υλοποίηση της συγκεκριμένης κακόβουλης ενέργειας αυξάνονται. Επομένως, το ρίσκο είναι μεγαλύτερο.

Ακολούθως, η συγκεκριμένη προσέγγιση στον κώδικα επαναλαμβάνεται για τον εντοπισμό i) ενεργειών «μεσαίας» σοβαρότητας, **medium_risk_activity_values** και ii) ενεργειών «χαμηλής» σοβαρότητας, **low_risk_activity_values**. Οι λέξεις-κλειδιά που συμπεριλαμβάνονται για εντοπισμό ενεργειών «μεσαίας» σοβαρότητας (medium_risk_activity_values) μπορεί να είναι αναζήτηση ιστοσελίδων όπως «jobhunter» και «careerbuilder» αφού υποδεικνύει ότι ο συγκεκριμένος χρήστης αφιερώνει χρόνο εργασίας σε άλλα θέματα, ενώ πιθανόν να γίνεται και αναζήτηση για εργασία σε άλλο οργανισμό. Αυτές οι ενέργειες ίσως παρουσιάσουν κάποιο ρίσκο στον οργανισμό και ένα οικονομικό αντίκτυπο. Παράλληλα, οι λέξεις-κλειδιά που συμπεριλαμβάνονται για εντοπισμό ενεργειών «χαμηλής» σοβαρότητας (low_risk_activity_values) μπορεί να αποτελέσουν οι λέξεις «Logon» και «Logoff». Οι συγκεκριμένες ενέργειες υπογραμμίζουν την συχνότητα που ο χρήστης αποκτά πρόσβαση στον λογαριασμό του οργανισμού του και επομένως τον βαθμό της ενασχόλησης του. Ο εντοπισμός των συγκεκριμένων ενεργειών σε μεγάλο βαθμό, σημαίνει ότι υπάρχει μια μεγάλη πιθανότητα ο χρήστης να μην αξιοποιεί τον χρόνο εργασίας του όπως προβλέπεται. Αυτό, πιθανόν να οδηγήσει σε οικονομικές συνέπειες. Επομένως, το ρίσκο στον οργανισμό αυξάνεται.

Συνεχίζοντας, γίνεται χρήση βαρύτητας σε κάθε υπολογισμό των πιο πάνω ενεργειών: i) **high_risk_activity_values,** ii) **medium_risk_activity_values** και iii) **low_risk_activity_values**. Αυτό γίνεται για να δοθεί περισσότερη σημασία στις ενέργειες που χρίζουν ιδιαίτερης προσοχής και αποφυγή σοβαρών επιπτώσεων στον οργανισμό. Η εικόνα 5.16 παρουσιάζει ενδεικτικές τιμές βαρύτητας:

i. BA_weight_high - Βαρύτητα για ενέργειες «υψηλής» σοβαρότητας.
ii. BA_weight_medium - Βαρύτητα για ενέργειες «μεσαίας» σοβαρότητας.
iii. BA_weight_low - Βαρύτητα για ενέργειες «χαμηλής» σοβαρότητας.

```
#Behavioural Activity Weight.

#In this part, a weight value is assigned
#The particular weight values emphasize th
BA_weight_high = 5
BA_weight_medium = 2
BA_weight_low = 1
```

Εικόνα 5.16: Χρήση Βαρύτητας στις Κατηγορίες των Ενεργειών.

Έπειτα, όπως παρουσιάζεται και στην εικόνα 5.17, πραγματοποιείται το συνολικό άθροισμα των ενδείξεων για τις πιο πάνω ενέργειες, συμπεριλαμβανομένου και των τιμών βαρύτητας. Η εντολή που χρησιμοποιείται είναι:

Behavioural_Activity=(high_risk_activity_values["Activity"].sum()*BA_weight_high)+(medium_risk_activity_values["Activity"].sum()*BA_weight_medium)+(low_risk_activity_values["Activity"].sum()*BA_weight_low).

```
#Behavioural activity is being calculated by the mathematical addition of the total high, medium and low incidents, taking ir
Behavioural_Activity = (high_risk_activity_values["Activity"].sum()*BA_weight_high)
+(medium_risk_activity_values["Activity"].sum()*BA_weight_medium)+(low_risk_activity_values["Activity"].sum()*BA_weight_low)
```

Εικόνα 5.17: Συνολικό Άθροισμα των Ενδείξεων.

Τέλος, σύμφωνα με την εικόνα 5.18, πραγματοποιείται ο υπολογισμός του συνολικού ρίσκου από την ανάλυση της ανθρώπινης συμπεριφοράς σε ποσοστό (%). Η εντολή που χρησιμοποιείται είναι:

BA_perc_calc = (Behavioural_Activity*ba_weight)/Policy_Level.

Όπως παρουσιάζεται στην εικόνα 5.18, γίνεται χρήση τριών πολιτικών λειτουργίας (Policy_Level) με ενδεικτικές τιμές:

i. strict_mode = 10
ii. default_mode = 40
iii. light_mode = 80

Οι συγκεκριμένες πολιτικές λειτουργίας αλλάζουν την βάση με την οποία υπολογίζεται το ρίσκο. Επομένως, όσο πιο υψηλή είναι η τιμή της βάσης, τόσο πιο χαμηλό είναι το συνολικό ρίσκο. Η επιλογή αυτή προσομοιάζει την αυστηρότητα της πολιτικής ασφαλείας που μπορεί να ακολουθεί κάποιος οργανισμός.

Επίσης, ο υπολογισμός του συνολικού ρίσκου από την ανάλυση της ανθρώπινης συμπεριφοράς, συμπεριλαμβάνει και την βαρύτητα «ba_weight», όπως έχει ήδη επεξηγηθεί στο Κεφάλαιο 5. Επιπλέων, σε περίπτωση που ο τελικός υπολογισμός του ρίσκου είναι ίσος ή μεγαλύτερος από την τιμή που έχει δοθεί για το «ba_weight», τότε η τελική τιμή του ρίσκου έχει την ίδια τιμή με το «ba_weight» (Εικόνα 5.18).

Συμπερασματικά λοιπόν, για τον υπολογισμό του ρίσκου από την ανάλυση της ανθρώπινης συμπεριφοράς, πραγματοποιείται ο πολλαπλασιασμός μεταξύ του αθροίσματος των ενδείξεων, **Behavioural_Activity** και της βαρύτητας **ba_weight** και ακολούθως διαίρεσης με την πολιτική λειτουργίας, **Policy_Level**.

```
#strict_mode = 10
default_mode = 40
#light_mode = 80

Policy_Level = default_mode

#Calculation of Behavioural Analysis Value in percentage.
#Behavioural Activity value is multiplied by the Behavioural Analysis Weight
BA_perc_calc = (Behavioural_Activity*ba_weight)/Policy_Level

#An if statement is used in case the Behavioural Activity result exceeds the
#If the result is greater than or equal to the behavioural Activity percenta
if BA_perc_calc >= ba_weight:
    BA_perc = ba_weight

#Otherwise, the Behavioural Activity result is given out as the calculated p
else:
    BA_perc = BA_perc_calc

#The result of Behavioural Analysis value in percentage is printed out.
print("\n""Total Behavioural Analysis Value in %: " + str(BA_perc))
```

Εικόνα 5.18: Υπολογισμός Ρίσκου από την Ανάλυση της Ανθρώπινης Συμπεριφοράς (%).

5.4 Εντοπισμός Ευπαθειών στα Πληροφοριακά Συστήματα

Η ενότητα περιγράφει τον υπολογισμό του ρίσκου βάση τον εντοπισμό ευπαθειών στα πληροφοριακά συστήματα ενός οργανισμού. Σύμφωνα με το Κεφάλαιο 4, η χρήση του εργαλείου «OpenVAS» είναι αναγκαία για την δημιουργία αναφοράς σε τύπο **.csv** για την καταγραφή των ευπαθειών που έχουν εντοπιστεί στο ευπαθές δίκτυο που έχει δημιουργηθεί. Το συγκεκριμένο δίκτυο προσομοιάζει μια κατάσταση όπου το δίκτυο ενός οργανισμού είναι μολυσμένο με διάφορες ευπάθειες. Το πρόγραμμα χρησιμοποιεί τις τιμές CVSS (Common Vulnerability Scoring System) από την αναφορά του εργαλείου «OpenVAS» με ονομασία «report.csv». Σύμφωνα με τον οργανισμό FIRST (Forum of Incident Response and Security Teams), οι τιμές CVSS παρουσιάζουν την σοβαρότητα της κάθε ευπάθειας [01]. Επομένως, η μεταπτυχιακή διατριβή θα χρησιμοποιήσει τον μέσο όρο των τιμών «CVSS» για να παρουσιάσει την συνολική επίδραση που παρουσιάζουν οι ευπάθειες στον οργανισμό. Αυτό θα αποτελέσει και την τιμή του ρίσκου από την διαδικασία του εντοπισμού ευπαθειών σύμφωνα με την μαθηματική σχέση: ρίσκο = επίδραση x πιθανότητα. Υποθέτουμε ότι οι πιθανότητες παραμένουν αμετάβλητες και δεν επηρεάζουν το αποτέλεσμα.

Βάση της εικόνας 5.19, η εντολή **cvss_values = pd.read_csv("report.csv", usecols = ["CVSS"])**, επιτρέπει στο πρόγραμμα να διαβάσει το αρχείο «report.csv» και συγκεκριμένα την στήλη «CVSS». Έπειτα, υπολογίζεται ο μέσος όρος των τιμών «CVSS» και δίνεται η ονομασία **cvss_average**. Μετά, υπολογίζεται η τιμή του ρίσκου (%) με τον πολλαπλασιασμό του **cvss_average** και της βαρύτητας **va_weight** και ακολούθως της διαίρεσης με την τιμή 10 που είναι η μέγιστη πιθανή τιμή του **cvss_average.**

```
#SECTION 3: Vulnerability Assessment#

#The program uses the vulnerability assessment report generated by the OpenVAS tool.
#The program reads the CVSS column of the report and prints out the CVSS values.
print("CVSS Records of Vulnerability Assessment Scanning Report: ")
cvss_values = pd.read_csv("report.csv", usecols = ["CVSS"])
print("\n", cvss_values)

#A mean value of the CVSS values is being calculated which represents the average severity
print("\n""Average Value from CVSS Records: ")
print(cvss_values["CVSS"].mean())
cvss_average = cvss_values["CVSS"].mean()

#The maximum CVSS value is 10, thus the base value used in calculating the average cvss val
#The average CVSS value is being multiplied by the vulnerability assessment weight set in t
cvss_average_perc = (cvss_average*va_weight)/10

#The average CVSS value in percentage is printed out.
print("\n""% Value for CVSS Records: ")
print(cvss_average_perc)
```

Εικόνα 5.19: Υπολογισμός Ρίσκου από τον Εντοπισμό Ευπαθειών στα Πληροφοριακά Συστήματα.

5.5 Υπολογισμός Συνολικού Ρίσκου

Η συγκεκριμένη ενότητα παρουσιάζει την τελική μαθηματική πράξη στην γλώσσα προγραμματισμού «Python» για την εκτίμηση του Συνολικού Ρίσκου σε μια οντότητα, σύμφωνα με:

i. Τους Ανθρώπινους Παράγοντες που έχουν επιλεγεί.

ii. Την Ανάλυση της Ανθρώπινης Συμπεριφοράς.

iii. Τον Εντοπισμό Ευπαθειών στα Πληροφοριακά Συστήματα.

Όπως φαίνεται στην εικόνα 5.20, το συνολικό ρίσκο, **risk** είναι ίσο με το άθροισμα των: i) **risk_rating_perc** (ρίσκο ανθρώπινων παραγόντων), ii) **BA_perc** (ρίσκο ανάλυσης συμπεριφοράς) και iii) **cvss_average_perc** (ρίσκο ευπαθειών). Το τελικό αποτέλεσμα παρουσιάζεται στο παράθυρο αλληλεπίδρασης με τον χρήστη.

```
#Calculation of the Total Risk#

#The Total Risk, named as Risk in the program, is being calculated
risk = risk_rating_perc + BA_perc + cvss_average_perc
print("\n""Risk in %: " + str(risk))
```

Εικόνα 5.20: Υπολογισμός Συνολικού Ρίσκου.

Κεφάλαιο 6

Αποτελέσματα

Το Κεφάλαιο 6 περιγράφει τα αποτελέσματα από τις δοκιμές που έγιναν στο «Cyber Risk Assessment Box» με σκοπό την εκτίμηση του συνολικού ρίσκου σε μια οντότητα. Η εκτέλεση της συγκεκριμένης προσέγγισης για τον υπολογισμό του ρίσκου έχει δώσει ιδιαίτερη σημασία στον υπολογισμό του ρίσκου σε ένα οργανισμό. Επίσης, όπως φαίνεται και στον πίνακα 6.2, η συγκεκριμένη προσέγγιση έχει πραγματοποιήσει εκτίμηση του ρίσκου και σε ατομικό επίπεδο για να τονίσει την ευελιξία του προγράμματος. Το Παράρτημα Γ παρουσιάζει ολόκληρο των κώδικα που έχει αναπτυχθεί για την δημιουργία του «Cyber Risk Assessment Box» με σχολιασμό.

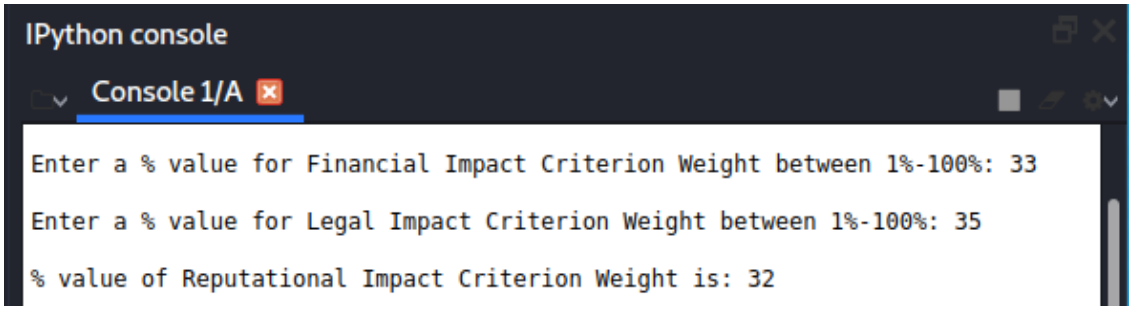
6.1 Εκτίμηση Ρίσκου σε Οργανισμό – Υψηλή Τιμή Ρίσκου

Αρχικά, οι ενδεικτικές τιμές για το ρίσκο που παρουσιάζουν οι ανθρώπινοι παράγοντες αλλά και οι ενδεικτικές τιμές των κριτηρίων (Πίνακας 6.1), τοποθετούνται στο παράθυρο αλληλεπίδρασης με τον κώδικα του εργαλείου «Spyder» (Εικόνα 6.1). Επίσης, πρέπει να σημειωθεί ότι στην περίπτωση που πραγματοποιείται ο υπολογισμός του ρίσκου σε ολόκληρο τον οργανισμό, τότε χρησιμοποιείται ο μέσος όρος τιμών στην κλίμακα του ρίσκου, αφού γίνεται αναφορά σε όλους τους εργαζόμενους του οργανισμού. Επομένως, η τιμή 3 παρουσιάζει τον μέσο όρο όλων των εργαζόμενων στον οργανισμό, για κάθε ανθρώπινο παράγοντα. Στην περίπτωση που η εκτίμηση ρίσκου απευθυνόταν για ένα εργαζόμενο ατομικά, τότε οι τιμές στην κλίμακα του ρίσκου θα ήταν διαφορετικές.

	Επιλογή Κριτηρίου 1: **Οικονομική Επίπτωση (Financial Impact)**	Επιλογή Κριτηρίου 2: **Νομική Επίπτωση (Legal Impact)**	Επιλογή Κριτηρίου 3: **Επίπτωση στην Φήμη (Reputational Impact)**	**Συνολικός Συντελεστής**
Συντελεστής Βαρύτητας (%)	33	35	32	
Παράγοντας 1: **Χρόνια Εργασίας στον Οργανισμό (Years Worked)**	3	3	3	**3**
Παράγοντας 2: **Επίπεδο Πρόσβασης στις Πληροφορίες (Data Access Level)**	3	3	3	**3**
Παράγοντας 3: **Επαγγελματικό Επίπεδο – Επίπεδο Γνώσεων (Proficiency/Knowledge Level)**	3	3	3	**3**
Συνολικός Συντελεστής Ρίσκου (Risk Rating)				**9**

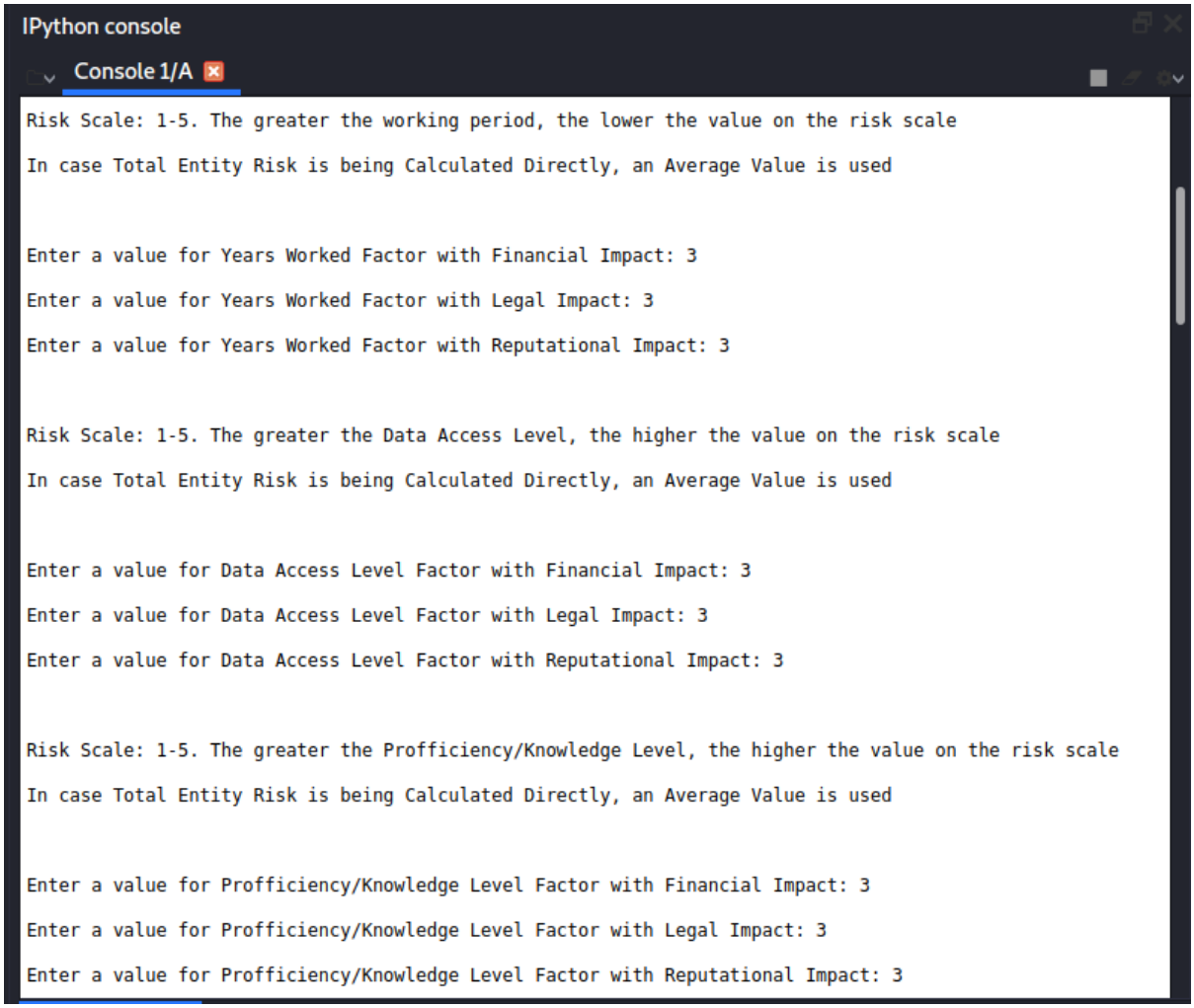
Πίνακας 6.1: Τιμές για τον Υπολογισμό του Συνολικού Συντελεστή Ρίσκου σε ένα Οργανισμό.

Συνεχίζοντας, στην εικόνα 6.1 διακρίνεται το παράθυρο αλληλεπίδρασης με τον κώδικα όπου ο χρήστης καλείται να τοποθετήσει τις πιο πάνω τιμές βαρύτητας για τα 3 κριτήρια.



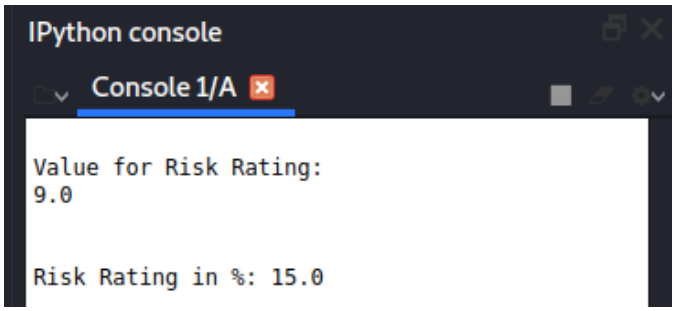
Εικόνα 6.1: Τιμές Βαρύτητας για τα 3 κριτήρια: «Financial Impact», «Legal Impact», «Reputational Impact».

Ακολούθως, ο χρήστης τοποθετεί τις τιμές στην κλίμακα του ρίσκου για τους ανθρώπινους παράγοντες, όπως διακρίνεται και στην εικόνα 6.2.



Εικόνα 6.2: Τιμές για το Ρίσκο που Παρουσιάζουν οι Ανθρώπινοι Παράγοντες.

Μετά, όπως φαίνεται και στην εικόνα 6.3, γίνεται ο υπολογισμός του συνολικού συντελεστή ρίσκου, «Risk Rating» που είναι ίσο με **9** όπως έχει εκτιμηθεί και από τον πίνακα 6.1. Επίσης, γίνεται ο υπολογισμός του συντελεστή ρίσκου σε ποσοστό που είναι ίσο με **15%**.



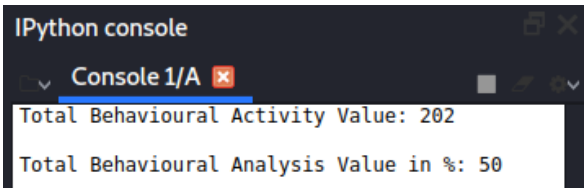
Εικόνα 6.3: Τιμές για τον Υπολογισμό του Συνολικού Συντελεστή Ρίσκου.

Συνεχίζοντας, παρουσιάζεται μια ανάλυση της ανθρώπινης συμπεριφοράς στο παράθυρο αλληλεπίδρασης με τον κώδικα. Η εικόνα 6.4 παρουσιάζει τα συνολικά περιστατικά που εντοπίστηκαν για ενέργειες «υψηλού», «μεσαίου» και «χαμηλού» κινδύνου. Στο συγκεκριμένο παράδειγμα, εντοπίστηκαν **16** περιστατικά «υψηλού» κινδύνου, **52** περιστατικά «μεσαίου» κινδύνου και **18** περιστατικά «χαμηλού» κινδύνου.

```
Insider Activity of Behavioural Log Analysis:

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
689          1
690          1
691          1
692          1
693          1

[694 rows x 1 columns]

Total Indications from High Risk User Activity: 16

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
689          0
690          0
691          0
692          0
693          0

[694 rows x 1 columns]

Total Indications from Medium Risk User Activity: 52

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
689          0
690          0
691          0
692          0
693          0

[694 rows x 1 columns]

Total Indications from Low Risk User Activity: 18
```

Εικόνα 6.4: Ανάλυση της Ανθρώπινης Συμπεριφοράς.

Έπειτα, γίνεται ο υπολογισμός των συνολικών περιστατικών κινδύνου που είναι ίσος με 202, βάση και των παραγόντων βαρύτητας που αναλογούν σε κάθε κατηγορία περιστατικού. Δηλαδή, (**5**x16) + (**2**x52) + (**1**x18) = **202**. Επίσης, υπολογίζεται και το ποσοστό του ρίσκου που αναλογεί στην συγκεκριμένη τιμή, **50%** (Εικόνα 6.5).



Εικόνα 6.5: Συνολικά Περιστατικά Κινδύνου και το Ανάλογο Ποσοστό του Ρίσκου.

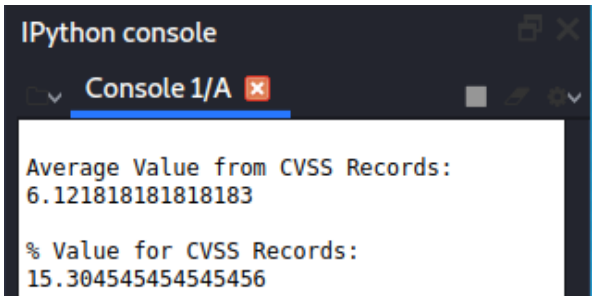
Στην συνέχεια, η εικόνα 6.6 παρουσιάζει τις τιμές «CVSS» για την σοβαρότητα των ευπαθειών στα πληροφοριακά συστήματα που έχουν αποκτηθεί από την αναφορά «report.csv» του εργαλείου «OpenVAS».

CVSS Records of Vulnerability Assessment Scanning Report:

	CVSS
0	10.0
1	10.0
2	10.0
3	10.0
4	10.0
5	9.3
6	9.0
7	9.0
8	9.0
9	7.5
10	7.5
11	7.5
12	7.5
13	7.5
14	7.5
15	7.5
16	7.5
17	7.5
18	7.5
19	7.5
20	6.8
21	6.8
22	6.8
23	6.4
24	6.0
25	6.0
26	5.8
27	5.8
28	5.0
29	5.0
30	5.0
31	5.0
32	5.0
33	4.8
34	4.8
35	4.8
36	4.8
37	4.8
38	4.3
39	4.3
40	4.3
41	4.3
42	4.3
43	4.3
44	4.3
45	4.3
46	4.3
47	4.3
48	4.3
49	4.0
50	4.0
51	4.0
52	4.0
53	2.6
54	2.6

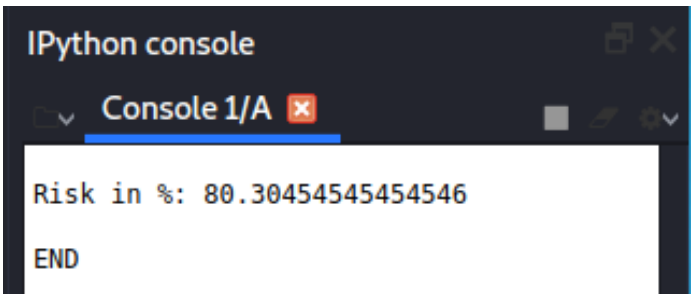
Εικόνα 6.6: Τιμές CVSS από το εργαλείο OpenVAS.

Έπειτα, γίνεται ο υπολογισμός για την μέση τιμή των CVSS που είναι ≃ **6.12** και ποσοστό ≃ **15.3%** (Εικόνα 6.7). Αυτό αναλογεί στην μέση τιμή σοβαρότητας των ευπαθειών που έχουν εντοπιστεί. Έτσι παρουσιάζεται η επίδραση (Impact) των ευπαθειών που εντοπίστηκαν σε περίπτωση εκμετάλλευσης τους. Επομένως, όπως φαίνεται και στην εικόνα 6.7, γίνεται ο υπολογισμός του ρίσκου σε ποσοστό, βάση των ευπαθειών που εντοπίστηκαν.



Εικόνα 6.7: Μέση Τιμή Σοβαρότητας Ευπαθειών και Υπολογισμός του Ρίσκου (%).

Τέλος, γίνεται ο υπολογισμός του συνολικού ρίσκου για τον οργανισμό με την πρόσθεση των ποσοστών ρίσκου που υπολογίστηκαν και αφορούν i) τους ανθρώπινους παράγοντες, ii) την ανθρώπινη συμπεριφορά και iii) τον εντοπισμό ευπαθειών στα πληροφοριακά συστήματα. Επομένως, γίνεται η πράξη **15%** + **50%** + **15.3%** = **80.3%** (Εικόνα 6.8).



Εικόνα 6.8: Υπολογισμός Συνολικού Ρίσκου του Οργανισμού.

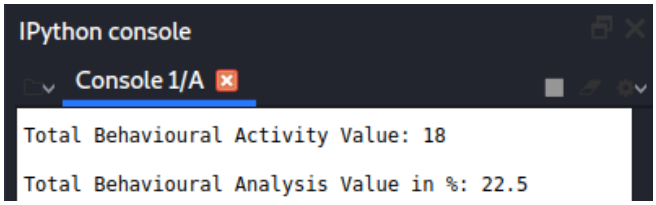
6.2 Εκτίμηση Ρίσκου σε Οργανισμό – Χαμηλή Τιμή Ρίσκου

Η διαδικασία της Ενότητας 6.1 επαναλαμβάνεται, χρησιμοποιώντας όμως ένα αρχείο καταγραφής δεδομένων με λιγότερα περιστατικά κινδύνου για την ανάλυση της ανθρώπινης συμπεριφοράς. Οι υπόλοιποι παράγοντας διατηρούν τις ίδιες τιμές. Η εικόνα 6.9 παρουσιάζει τις καινούργιες τιμές για τις κατηγορίες των κινδύνων που έχουν εντοπιστεί. Όπως φαίνεται, έχουν εντοπιστεί 0 περιστατικά «υψηλού» κινδύνου, 4 περιστατικά «μεσαίου» κινδύνου και 10 περιστατικά «χαμηλού» κινδύνου.

```
Insider Activity of Behavioural Log Analysis:

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
227          0
228          0
229          0
230          0
231          0

[232 rows x 1 columns]

Total Indications from High Risk User Activity: 0

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
227          0
228          0
229          0
230          0
231          0

[232 rows x 1 columns]

Total Indications from Medium Risk User Activity: 4

      Activity
0            0
1            0
2            0
3            0
4            0
..         ...
227          0
228          0
229          0
230          0
231          0

[232 rows x 1 columns]

Total Indications from Low Risk User Activity: 10
```

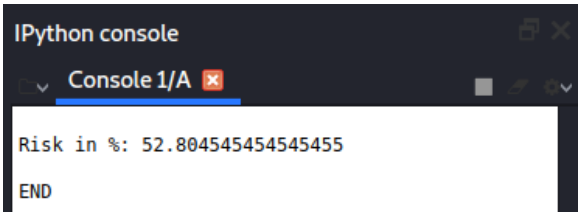
Εικόνα 6.9: Ανάλυση της Ανθρώπινης Συμπεριφοράς.

Έπειτα, γίνεται ο υπολογισμός των συνολικών περιστατικών κινδύνου που είναι ίσος με 18, βάση και των παραγόντων βαρύτητας που αναλογούν σε κάθε κατηγορία περιστατικού. Δηλαδή, (**5**x0) + (**2**x4) + (**1**x10) = **18**. Επίσης, υπολογίζεται και το ποσοστό ρίσκου που αναλογεί στην συγκεκριμένη τιμή και είναι ίσο με **22.5%** (Εικόνα 6.10).



Εικόνα 6.10: Συνολικά Περιστατικά Κινδύνου.

Τέλος, βάση του ότι οι υπόλοιποι παράγοντες διατήρησαν τις ίδιες τιμές όπως στο παράδειγμα της Ενότητας 6.1, το αποτέλεσμα για την συνολική τιμή του ρίσκου είναι ≃ **52.8 %** (Εικόνα 6.11). Δηλαδή, έγινε η μαθηματική πράξη **15%** + **22.5%** + **15.3%** = **52.8%**.



Εικόνα 6.11: Υπολογισμός του Συνολικού Ρίσκου.

Συμπερασματικά λοιπόν, το παράδειγμα της Ενότητας 6.2 παρουσιάζει πιο χαμηλό ρίσκο για τον οργανισμό σε σύγκριση με το παράδειγμα της Ενότητας 6.1. Ο κύριος λόγος είναι ο εντοπισμός πιο χαμηλού αριθμού περιστατικών κινδύνου από την ανάλυση της ανθρώπινης συμπεριφοράς.

Στην συνέχεια, πραγματοποιήθηκαν περισσότερες δοκιμές τις οποίες αποτυπώνει ο πίνακας 6.2. Ο στόχος των δοκιμών ήταν οι αλλαγές στους διάφορους παράγοντες του προγράμματος που επηρεάζουν το τελικό αποτέλεσμα της εκτίμησης του ρίσκου όπως οι διάφορες τιμές βαρύτητας και το επίπεδο πολιτικής ασφάλειας. Επίσης, οι δοκιμές Ε και ΣΤ αναφέρονται στην εκτίμηση του ρίσκου σε ατομικό επίπεδο χρησιμοποιώντας μια παραλλαγή του αρχείου «totalentitylogs1.csv» με μειωμένες κακόβουλες ενέργειες. Όπως φαίνεται στον πίνακα δοκιμών 6.2, το ρίσκο αυξάνεται όταν ο αριθμός ενδείξεων από την ανάλυση συμπεριφοράς μεγαλώνει και όταν ο μέσος όρος σοβαρότητας των ευπαθειών μεγαλώνει. Επιπλέων, το ρίσκο μεγαλώνει όταν οι πιθανότητες πρόκλησης κακόβουλης ενέργειας από ανθρώπινους παράγοντες αυξάνονται.

Πίνακας Δοκιμών	Δοκιμή Α	Δοκιμή Β	Δοκιμή Γ	Δοκιμή Δ	Δοκιμή Ε	Δοκιμή ΣΤ
Οργανισμός/Ατομική Εκτίμηση	Οργανισμός	Οργανισμός	Οργανισμός	Οργανισμός	Ατομική	Ατομική
Βαρύτητα Ανθρώπινων Παραγόντων (riskr_weight, %)	25	25	10	10	25	25
Βαρύτητα Ανάλυσης Ανθρώπινης Συμπεριφοράς (ba_weight, %)	50	50	60	70	50	50
Βαρύτητα Εντοπισμό Ευπαθειών (va_weight, %)	25	25	30	20	25	25
Συντελεστής – Years Worked Factor	3	3	3	3	2	4
Συντελεστής – Data Access Level Factor	3	3	3	3	2	2
Συντελεστής – Proficiency/Knowledge Level	3	3	3	3	3	2
Βαρύτητα Κριτηρίων (Financial Impact – FI, Legal Impact - LI, Reputational Impact - RI in %)	• FI = 33 • LI = 35 • RI = 32	• FI = 33 • LI = 35 • RI = 32	• FI = 40 • LI = 35 • RI = 25	• FI = 40 • LI = 35 • RI = 25	• FI = 35 • LI = 35 • RI = 30	• FI = 40 • LI = 35 • RI = 25
Βαρύτητα Κατηγοριών Κινδύνου (BA_weight_high, BA_weight_medium, BA_weight_low)	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1	• BA_weight_high = 5 • BA_weight_medium = 2 • BA_weight_low = 1
Επίπεδο Πολιτικής Ασφαλείας (Policy Level)	default_mode = 40	default_mode = 40	default_mode = 40	strict_mode = 10	strict_mode = 10	light_mode = 80
Ρίσκο Ανθρώπινων Παραγόντων (%)	15	15	6	6	11.7	13.3
Ρίσκο Ανάλυσης Συμπεριφοράς (%)	50	22.5	60	70	50	16.9
Ρίσκο Ευπαθειών (%)	15.3	15.3	18.4	12.2	15.3	15.3
Συνολικό Ρίσκο – Risk (%)	80.3	52.08	84.4	88.2	77.0	45.5

Πίνακας 6.2: Πίνακας Δοκιμών Εκτίμησης Ρίσκου.

Κεφάλαιο 7

Συζήτηση των Αποτελεσμάτων

Το κεφάλαιο περιγράφει τον συσχετισμό των αποτελεσμάτων με τα στοιχεία που εντοπίστηκαν από την θεωρητική έρευνα καθώς και την αξιολόγηση της μεθοδολογίας που έχει ακολουθήσει η μεταπτυχιακή διατριβή. Επίσης, παρουσιάζεται η επίδραση και οι περιορισμοί της έρευνας στην επιστημονική περιοχή της εκτίμησης του ρίσκου.

7.1 Συζήτηση

Το πρώτο κομμάτι της μεθοδολογίας αναφέρεται στην συμβολή των ανθρώπινων παραγόντων για την εκτίμηση του ρίσκου. Οι παράγοντες όπως τα χρόνια εργασίας σε ένα οργανισμό, η πρόσβαση στα δεδομένα και το επίπεδο των γνώσεων αποτελούν ανθρώπινα χαρακτηριστικά που επηρεάζουν το κλίμα εμπιστοσύνης σε ένα οργανισμό όπως στηρίζουν και οι συγγραφείς Henshel κ. ά. [14]. Αυτό με την σειρά ίσως να αποτελέσει ένα ρίσκο ως προς την υλοποίηση των στόχων του οργανισμού σύμφωνα με τους Oltramari κ. ά. [19] που παρουσιάζουν μια προσέγγιση για την εκτίμηση κινδύνων βάση του παράγοντα της εμπιστοσύνης. Επομένως, η μεταπτυχιακή διατριβή παρουσίασε μια ποσοτική ένδειξη για το μέγεθος των πιθανοτήτων και επομένως του ρίσκου που παρουσιάζει ο κάθε ανθρώπινος παράγοντας ξεχωριστά. Τα αποτελέσματα δείχνουν ότι όσο οι τιμές στην κλίμακα του ρίσκου/πιθανοτήτων αυξάνονται τότε αυξάνεται και το ρίσκο που υπολογίζεται από τους ανθρώπινους παράγοντες.

Στην συνέχεια, χρησιμοποιώντας παραδείγματα από τις διαδικτυακές βάσεις δεδομένων [15], η μεταπτυχιακή διατριβή κατάφερε να παρουσιάσει κακόβουλες ενέργειες από διάφορους χρήστες, μέσα από τα αρχεία καταγραφής συμβάντων. Ο σκοπός της συγκεκριμένης προσέγγισης ήταν η ανάλυση της ανθρώπινης συμπεριφοράς χρησιμοποιώντας μια διαδικασία για εντοπισμό λέξεων-κλειδιά. Οι λέξεις-κλειδιά προσομοίωναν ύποπτες και κακόβουλες ενέργειες από τους χρήστες σε ένα οργανισμό. Όπως αναφέρεται και στο ENISA «White Paper» [10], η συμπεριφορά του κάθε ανθρώπου έχει αντίκτυπο στον οργανισμό και ιδιαίτερα στο κομμάτι της ασφάλειας των

πληροφοριακών συστημάτων. Επομένως, σύμφωνα και με τους Greitzer και Hohimer [12], οι συγκεκριμένες λέξεις-κλειδιά που έχουν επιλεγεί, ανήκουν στις κατηγορίες που αναλύουν οι συγγραφείς ότι αποτελούν ενδείξεις για τον εντοπισμό εσωτερικών απειλών. Έτσι, η διαδικασία εκτίμησης του ρίσκου έλαβε υπόψη τον παράγοντα της ανθρώπινης συμπεριφοράς. Τα αποτελέσματα δείχνουν ότι το μέγεθος της ζημιάς και επομένως το ρίσκο αυξάνεται με τον εντοπισμό των εσωτερικών απειλών. Επίσης, ο αριθμός των ενδείξεων που παρουσίασε η μεταπτυχιακή διατριβή για την κάθε κατηγορία απειλής, τονίζουν το μέγεθος των πιθανοτήτων για την πραγματοποίηση της κάθε απειλής. Αυτό παρουσιάζουν και τα αποτελέσματα όπου η τιμή του ρίσκου από την ανθρώπινη συμπεριφορά μεγαλώνει όσο ο αριθμός των ενδείξεων για κακόβουλες ενέργειες (λέξεις-κλειδιά) μεγαλώνει. Επίσης, η τιμή του ρίσκου από την ανθρώπινη συμπεριφορά μεγαλώνει όσο ο εντοπισμός των ενδείξεων για ενέργειες υψηλού κινδύνου μεγαλώνει. Ο πίνακας των αποτελεσμάτων εξηγεί ότι όσο αυξάνεται η τιμή του ρίσκου από την ανθρώπινη συμπεριφορά, η τιμή του συνολικού ρίσκου αυξάνεται αναλογικά.

Έπειτα, η μεταπτυχιακή διατριβή συμπεριέλαβε τον εντοπισμό ευπαθειών στα πληροφοριακά συστήματα στην διαδικασία εκτίμησης του συνολικού ρίσκου. Όπως αναφέρεται και στην βιβλιογραφική επισκόπηση, οι συγγραφείς Saleh και Alfantookh [22] υπογραμμίζουν τις διάφορες ευπάθειες που εντοπίζονται στα πληροφοριακά συστήματα. Τονίζουν ότι η πιθανή εκμετάλλευση των ευπαθειών από εσωτερικές απειλές αυξάνει το ρίσκο και το μέγεθος της ζημιάς σε μια οντότητα. Έτσι, έγινε η χρήση του εργαλείου «OpenVAS» για εντοπισμό ευπαθειών σε ένα δίκτυο που δημιουργήθηκε ώστε να προσομοιάζει ένα οργανισμό με ευπαθές δίκτυο. Οι ευπάθειες που εντοπίστηκαν από την σάρωση του δικτύου με το εργαλείο, αντιστοιχούν σε τιμές «CVSS» οι οποίες παρουσιάζουν την σοβαρότητα της κάθε ευπάθειας. Στην συνέχεια, ο μέσος όρος των τιμών «CVSS» που χρησιμοποιήθηκε για την εκτίμηση του συνολικού ρίσκου, παρουσιάζει τον μέσο όρο σοβαρότητας όλων των ευπαθειών που εντοπίστηκαν. Τα αποτελέσματα παρουσιάζουν μια σταθερή τιμή στο ρίσκο που υπολογίστηκε από τον εντοπισμό ευπαθειών λόγο του ότι έχει δημιουργηθεί μόνο ένα ευπαθές δίκτυο. Παρόλα αυτά, η διαδικασία για εντοπισμό ευπαθειών σε διάφορα δίκτυα, παραμένει η ίδια.

Συμπερασματικά λοιπόν και σύμφωνα με τα πιο πάνω, τα αποτελέσματα της μεταπτυχιακής διατριβής επιβεβαιώνουν τις αναφορές που πραγματοποιήθηκαν στην βιβλιογραφική επισκόπηση αφού τα ευρήματα συμφωνούν με τα συμπεράσματα και τα αποτελέσματα των συγγραφέων. Δηλαδή, η τελική τιμή του ρίσκου επηρεάζεται από ένα σύνολο παραγόντων που συμπεριλαμβάνει ανθρώπινους παράγοντες, την ανθρώπινη συμπεριφορά αλλά και τις ευπάθειες στα πληροφοριακά συστήματα . Επιπλέων, η μεθοδολογία που έχει αναπτυχθεί, εμπλουτίζει τον

επιστημονικό χώρο που ασχολείται με την εκτίμηση του ρίσκου. Η μεταπτυχιακή διατριβή έχει καταφέρει να παρουσιάσει μια ξεχωριστή προσέγγιση για την εκτίμηση του ρίσκου, συνδυάζοντας διαφορετικά είδη παραγόντων ως προς τον υπολογισμό του ρίσκου. Έτσι, ήταν αναγκαία η ανεύρεση μιας κοινής βάσης με στόχο τον συνδυασμό των διάφορων παραγόντων. Επομένως, ο βασικός στόχος της μεταπτυχιακής διατριβής έχει ολοκληρωθεί αφού επιτρέπει στον χρήστη τον υπολογισμό μιας τελικής τιμής του συνολικού ρίσκου λαμβάνοντας υπόψη τους ανθρώπινους παράγοντες, την ανθρώπινη συμπεριφορά και τις ευπάθειες στα πληροφοριακά συστήματα.

7.2 Επίδραση

Τονίζεται η μοναδικότητα της συγκεκριμένης μεθοδολογίας μετά και την βιβλιογραφική επισκόπηση που έχει πραγματοποιηθεί. Επομένως, επισημαίνεται η σημαντικότητα της μεθοδολογίας που έχει αναπτυχθεί καθώς μπορεί να δώσει το έναυσμα για περαιτέρω επιστημονικές έρευνες με παρόμοιες προσεγγίσεις στον επιστημονικό χώρο της εκτίμησης του ρίσκου. Ακόμη, λόγο της προσαρμοστικότητας του προγράμματος «Cyber Risk Assessment Box», υπάρχει η δυνατότητα για πρόσθεση περισσότερων παραγόντων για τον υπολογισμό του συνολικού ρίσκου, έτσι ώστε τα αποτελέσματα να είναι πιο κοντά στην πραγματικότητα. Επίσης, η ιδέα που παρουσιάζεται στην μεταπτυχιακή διατριβή μπορεί να εξελιχθεί και να οδηγήσει στην δημιουργία μιας εφαρμογής ή προγράμματος με «γραφικό περιβάλλον διεπαφής με τον χρήστη» (Graphical User Interface). Τα δεδομένα από τους ανθρώπινους παράγοντες θα εισέρχονται αρχικά στην εφαρμογή, ενώ παράλληλα να δημιουργείται αυτόματη ζωντανή ανάλυση της ανθρώπινης συμπεριφοράς και σάρωση ευπαθειών στο δίκτυο με την χρήση «διεπαφών προγραμματισμού εφαρμογών» (APIs - **A**pplication **P**rogramming **I**nterfaces). Δηλαδή, τα εργαλεία σάρωσης ευπαθειών όπως το «OpenVAS» να τροφοδοτούν συνεχώς την εφαρμογή με δεδομένα όπως τις τιμές «CVSS». Επομένως, η εκτίμηση του ρίσκου να πραγματοποιείται ζωντανά, δηλαδή συνεχώς.

Επομένως, με την χρήση του «Cyber Risk Assessment Box» διάφοροι οργανισμοί θα μπορούν να ενημερώνονται συνεχώς για τον βαθμό του ρίσκου. Αυτό θα οδηγήσει σε διορθωτικά βήματα για άμεση επίλυση των κινδύνων και των απειλών για μείωση του ρίσκου.

7.3 Περιορισμοί

Αρχικά, η συγκεκριμένη μεθοδολογία που αναπτύχθηκε θα μπορούσε να παρουσιάσει αποτελέσματα πιο κοντά στην πραγματικότητα αν πραγματοποιούνταν αληθινές δοκιμές στο ανθρώπινο δυναμικό και στο δίκτυο ενός οργανισμού. Όμως, η διαδικασία θα ήταν πιο χρονοβόρα.

Η διαμορφωμένη μεθοδολογία «Weighted Factor Analysis» θα μπορούσε να συμπεριλάβει πιο αναλυτικά τα ανθρώπινα χαρακτηριστικά στο κομμάτι της εκτίμησης του ρίσκου από τους ανθρώπινους παράγοντες όπως παρουσιάζουν οι συγγραφείς Henshel κ. ά. [14] με σκοπό να οδηγήσει σε πιο ακριβή αποτελέσματα. Για παράδειγμα, το επίπεδο εκπαίδευσης σε θέματα ασφαλείας που έχει λάβει το ανθρώπινο δυναμικό σε μια οντότητα. Αυτό το στοιχείο ίσως να επηρεάσει και το επίπεδο των γνώσεων. Δηλαδή, αυξάνοντας το επίπεδο των γνώσεων στο ανθρώπινο δυναμικό σε μια οντότητα λόγο εκπαίδευσης για κακόβουλες επιθέσεις, μπορεί να οδηγήσει σε μείωση των πιθανοτήτων υλοποίησης μιας κακόβουλης ενέργειας. Το ανθρώπινο δυναμικό θα μπορεί πιο εύκολα να αναγνωρίσει μια κακόβουλη ενέργεια όπως το «phishing». Έτσι, η τιμή στην κλίμακα του ρίσκου της μεθοδολογίας θα είναι πιο χαμηλή για τον συγκεκριμένο παράγοντα.

Επίσης, είναι πιθανή η χρήση επιπρόσθετων κριτηρίων στην διαμορφωμένη μεθοδολογία «Weighted Factor Analysis», όπως για παράδειγμα το ποσοστό (%) που μπορεί να επηρεάσει αρνητικά τους στόχους που έχει θέσει μια οντότητα. Έτσι, η εκτίμηση του ρίσκου βάση των ανθρώπινων παραγόντων θα είναι πιο αναλυτική.

Ακόμη, η κλίμακα του ρίσκου που έχει χρησιμοποιηθεί για τον υπολογισμό των πιθανοτήτων και επομένως του ρίσκου από τους ανθρώπινους παράγοντες, θα μπορούσε να περιέχει περισσότερες τιμές. Έτσι, οι τιμές θα αντικατοπτρίζουν πιο σωστά την πραγματικότητα. Παρόλα αυτά, πρέπει να σημειωθεί ότι η μεθοδολογία που αναπτύχθηκε στην μεταπτυχιακή διατριβή είναι αντιμέτωπη και με τις δυσκολίες που παρουσιάζει μια ποιοτική προσέγγιση για περισυλλογή δεδομένων. Εξακολουθεί να υπάρχει περιορισμός και απώλεια δεδομένων στην προσπάθεια αντιστοιχίας ποσοτικών δεδομένων της έρευνας με τα ποιοτικά δεδομένα της πραγματικότητας.

Στην συνέχεια, στο κομμάτι της ανάλυσης της ανθρώπινης συμπεριφοράς, θα μπορούσαν να προστεθούν περισσότερες λέξεις-κλειδιά και να δημιουργηθούν αρχεία με λίστες από λέξεις-κλειδιά. Επομένως, το πρόγραμμα να πραγματοποιεί μια ανάγνωση των αρχείων με τις λίστες των

λέξεων-κλειδιά, ώστε να παρουσιάζει πιο αναλυτικά και ακριβή αποτελέσματα. Οι λίστες αυτές θα μπορούν να ενημερώνονται συνεχώς για ακόμη πιο μεγάλη ακρίβεια στα αποτελέσματα.

Επιπλέων, η χρήση εργαλείων για αξιολόγηση ευπαθειών με κώδικα ανοικτό προς στο κοινό (open source), όπως το «OpenVAS», πραγματοποιεί μια περιορισμένη σάρωση των ευπαθειών συγκριτικά με εργαλεία επί πληρωμή. Επίσης, η αναβάθμιση της βάσης δεδομένων για ευπάθειες είναι αναγκαία πριν από την χρήση του «OpenVAS» στις διάφορες δοκιμές. Άρα, η μεθοδολογία θα οδηγούσε σε πιο ακριβή αποτελέσματα και συμπεράσματα αν γινόταν χρήση εργαλείου επί πληρωμής, όπου οι βάσεις δεδομένων για ευπάθειες είναι πιο μεγάλες. Ένα τέτοιο εργαλείο είναι το «Nessus» [04]. Παρόλα αυτά, η δημιουργία του «Cyber Risk Assessment Box» θα ήταν οικονομικά πιο δαπανηρή. Επίσης, η δημιουργία περισσοτέρων δικτύων με ευπάθειες θα παρουσίαζε πιο αναλυτικά αποτελέσματα για την εκτίμηση του ρίσκου.

Συνεχίζοντας, το «Cyber Risk Assessment Box» θα μπορούσε να συμπεριλάβει δεδομένα για τα μέτρα που έχει υλοποιήσει ένας οργανισμός για να αυξήσει το επίπεδο ασφαλείας στα συστήματα και στις υποδομές του. Για παράδειγμα, εργαλεία «anti-virus», σε οργανωτικό επίπεδο: «role-base access» για πρόσβαση σε δεδομένα, καθώς και φυσικά μέτρα όπως κάμερες ασφαλείας. Τα συγκεκριμένα δεδομένα θα μπορούσαν να αντιστοιχούν σε τιμές στον κώδικα οι οποίες να μείωναν το συνολικό ρίσκο.

Τέλος, η τιμή ρίσκου στο ανθρώπινο δυναμικό μιας οντότητας ίσως να οδηγήσει και προβλήματα στον ηθικό τομέα. Η δημιουργία ενός «προφίλ-ρίσκου» στο ανθρώπινο δυναμικό στην περίπτωση εκτίμησης ατομικής τιμής ρίσκου, ίσως να μειώσει το κίνητρο σε ένα χρήστη αν αντιπροσωπεύει ένα χρήστη με υψηλή τιμή ρίσκου. Φυσικά, αυτό μπορεί να οδηγήσει και σε θετικά αποτελέσματα. Αν ο χρήστης βλέπει ότι το ρίσκο που του αντιστοιχεί μειώνεται μετά από δικές του εποικοδομητικές και θετικές ενέργειες τότε το κίνητρο για προσφορά στον οργανισμό θα αυξηθεί. Σύμφωνα με τον Koks [16], τα αποτελέσματα είναι διαφορετικά σε περίπτωση που το ανθρώπινο δυναμικό σε ένα οργανισμό έχει ενημερωθεί ότι οι ενέργειες τους στον χώρο εργασίας καταγράφονται. Αυτό είναι το φαινόμενο «Hawthorne». Δηλαδή, η συλλογή δεδομένων από τα αρχεία καταγραφής συμβάντων θα παρουσιάσουν ένα πιο χαμηλό βαθμό ρίσκου στην περίπτωση ενημέρωσης ότι πραγματοποιείται ανάλυση συμπεριφοράς.

Κεφάλαιο 8

Επίλογος

Η μεταπτυχιακή διατριβή κατάφερε να παρουσιάσει μια διαφορετική προσέγγιση για την εκτίμηση του ρίσκου σε μια οντότητα όπως σε ένα οργανισμό. Σύμφωνα και με την βιβλιογραφική επισκόπηση που πραγματοποιήθηκε, οι κύριοι παράγοντες που επιλέγηκαν στην μεθοδολογία για την εκτίμηση του ρίσκου ήταν: i) οι ανθρώπινοι παράγοντες, ii) η ανάλυση της ανθρώπινης συμπεριφοράς και iii) ο εντοπισμός ευπαθειών στα πληροφοριακά συστήματα.

Στην συνέχεια, ήταν σημαντικό να βρεθεί μια χρυσή τομή ώστε να συνδυαστούν κατάλληλα τα δεδομένα από τους παράγοντες που επιλέγηκαν. Επομένως, η μεταπτυχιακή διατριβή έχει καταφέρει να παρουσιάσει ένα αποτέλεσμα που αντιστοιχεί σε μια ενιαία τιμή για τον υπολογισμό του συνολικού ρίσκου σε ποσοστό. Επιπλέων, η χρήση των «Insider Data Threats» ήταν σημαντική για την ανάλυση δεδομένων από κακόβουλες ενέργειες χρηστών [15].

Η χρήση της γλώσσας προγραμματισμού «Python» ήταν αναγκαία ώστε να συνδυαστούν κατάλληλα όλα τα δεδομένα της μεθοδολογίας και να πραγματοποιηθούν οι ανάλογες μαθηματικές πράξεις για την παρουσίαση των αποτελεσμάτων. Άρα, η μεταπτυχιακή διατριβή έχει επιτύχει την διαμόρφωση μιας προσέγγισης σε κώδικα έτσι ώστε να είναι και ευπροσάρμοστος σε μελλοντικές διαμορφώσεις. Για παράδειγμα, η προσθήκη παραγόντων και επιπλέων δεδομένων που μπορεί να οδηγήσουν σε πιο ακριβή αποτελέσματα εκτίμησης ρίσκου.

Συμπερασματικά λοιπόν και λαμβάνοντας υπόψη όλες τις πληροφορίες, η μεταπτυχιακή διατριβή έχει καταφέρει να επιβεβαιώσει τα στοιχεία από τις έρευνες στην βιβλιογραφική επισκόπηση, ότι η εκτίμηση του ρίσκου σε μια οντότητα επηρεάζεται από ένα σύνολο παραγόντων. Σύμφωνα με τις δοκιμές που έχουν πραγματοποιηθεί, τα αποτελέσματα υπογραμμίζουν ότι η τιμή του ρίσκου μεγαλώνει i) όταν το μέγεθος της αρνητικής επίδρασης των παραγόντων μεγαλώνει και ii) όταν οι πιθανότητες υλοποίησης μιας απειλής αυξάνονται. Επομένως, τονίζεται η μαθηματική σχέση ρίσκο = επίδραση x πιθανότητα.

Τέλος, η μεταπτυχιακή διατριβή παρουσιάζει την δημιουργία του «Cyber Risk Assessment Box» που περιλαμβάνει την μεθοδολογία και την προσέγγιση που αναπτύχθηκε με σκοπό την εκτίμηση του ρίσκου σε μια οντότητα. Δηλαδή, τον υπολογισμό του ρίσκου σε ένα τμήμα όπως σε ένα οργανισμό ή τον υπολογισμό του ρίσκου για κάθε χρήστη ξεχωριστά. Επιπλέων, η μεταπτυχιακή διατριβή θα αποτελέσει το έναυσμα για περεταίρω μελέτη και την βελτιστοποίηση της συγκεκριμένης προσέγγισης.

Βιβλιογραφία

[01] "Common Vulnerability Scoring System SIG", FIRST — Forum of Incident Response and Security Teams, 2020. [Online]. Available: https://www.first.org/cvss/. [Accessed: 23- Nov- 2020].

[02] "International Organization for Standardization", ISO, 2020. [Online]. Available: https://www.iso.org/. [Accessed: 23- Nov- 2020].

[03] "Metasploitable", SourceForge, 2020. [Online]. Available: https://sourceforge.net/projects/metasploitable/. [Accessed: 23- Nov- 2020].

[04] "Nessus Product Family", Tenable®, 2020. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed: 23- Nov- 2020].

[05] "Nmap: The Network Mapper - Free Security Scanner", Nmap.org, 2020. [Online]. Available: https://nmap.org/. [Accessed: 23- Nov- 2020].

[06] "OpenVAS - OpenVAS - Open Vulnerability Assessment Scanner", Openvas.org, 2020. [Online]. Available: https://www.openvas.org/. [Accessed: 23- Nov- 2020].

[07] "What is Keystroke Logging and Keyloggers?", www.kaspersky.com, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/keylogger. [Accessed: 23- Nov- 2020].

[08] Diesch, R., Pfaff, M., & Krcmar, H. "A Comprehensive Model of Information Security Factors for Decision-Makers". Computers & Security, 92, 101747, 2020.

[09] Enisa.europa.eu, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management. [Accessed: 23- Nov- 2020].

[10] Enisa.europa.eu, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity. [Accessed: 23- Nov- 2020].

[11] G. Stoneburner, A. Goguen and A. Feringa. "Risk Management Guide for Information Technology Systems", SP800-30, 1-41, 2002.

[12] Greitzer, F. & Hohimer, R. "Modeling Human Behavior to Anticipate Insider Attacks". Journal of Strategic Security, Volume IV, Issue. 2, 1944-472, 2011.

[13] Haaker, T., Bouwman, H., Janssen, W., & de Reuver, M. "Business Model Stress Testing: A Practical Approach to Test the Robustness of a Business Model". Futures, 89, 14–25, 2017.

[14] Henshel, D., Cains, M.G., Hoffman, B., Kelley, T. "Trust as a Human Factor in Holistic Cyber Security Risk Assessment". Procedia Manufacturing, 3, 1117 – 1124, 2015.

[15] I. Dataset, "Insider Threat Test Dataset", Resources.sei.cmu.edu, 2020. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099. [Accessed: 23- Nov- 2020].

[16] Koks, P., "Six Challenges of Qualitative Data Analysis", Online Metrics, 2020. [Online]. Available: https://online-metrics.com/qualitative-data/. [Accessed: 23- Nov- 2020].

[17] Mohammed, H. K., & Knapkova, A. "The Impact of Total Risk Management on Company's Performance". Procedia - Social and Behavioral Sciences, 220, 271–277, 2016.

[18] Nvlpubs.nist.gov, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed: 23- Nov- 2020].

[19] Oltramari, A., Henshel, D., Cains, M., & Hoffman, B. "Towards a Human Factors Ontology for Cyber Security". Conference STIDS 2015, 2015.

[20] Radanliev, P. et al., "Future Developments in Cyber Risk Assessment for The Internet of Things". Computers in Industry, 102, 14 – 22, 2018.

[21] S. Team, "Home — Spyder IDE", Spyder-ide.org, 2020. [Online]. Available: https://www.spyder-ide.org/. [Accessed: 23- Nov- 2020].

[22] Saleh, M. S., & Alfantookh, A. "A New Comprehensive Framework for Enterprise Information Security Risk Management". Applied Computing and Informatics, 9(2), 107–118, 2011.

[23] Wan Husin, W. S., Yahya, Y., Mohd Azmi, N. F., Amir Sjarif, N. N., Chuprat, S., & Azmi, A. "Risk Management Framework for Distributed Software Team: A Case Study of Telecommunication Company". Procedia Computer Science, 161, 178–186, 2019.

Παράρτημα Α

Αναφορά Ευπαθειών Δικτύου

IP	Port	Port Protocol	CVSS	Severity	Solution Type	NVT Name	Summary
10.0.2.5	512	tcp	10	High	Mitigation	rexec Passwordless / Unencrypted Cleartext Login	This remote host is running a rexec service.
10.0.2.5			10	High	Mitigation	OS End Of Life Detection	OS End Of Life Detection. The Operating System on the remote host has reached the end of life and should not be used anymore.
10.0.2.5	80	tcp	10	High	VendorFix	TWiki XSS and Command Execution Vulnerabilities	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
10.0.2.5	8787	tcp	10	High	Mitigation	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.
10.0.2.5	1524	tcp	10	High	Workaround	Possible Backdoor: Ingreslock	A backdoor is installed on the remote host.
10.0.2.5	3632	tcp	9.3	High	VendorFix	DistCC Remote Code Execution Vulnerability	DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
10.0.2.5	3306	tcp	9	High	Mitigation	MySQL / MariaDB weak password	It was possible to login into the remote MySQL as root using weak credentials.

10.0.2.5	5900	tcp	9	High	Mitigation	VNC Brute Force Login	Try to log in with given passwords via VNC protocol.
10.0.2.5	5432	tcp	9	High	Mitigation	PostgreSQL weak password	It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
10.0.2.5	8009	tcp	7.5	High	VendorFix	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Apache Tomcat is prone to a remote code execution vulnerability in the AJP connector dubbed 'Ghostcat'.
10.0.2.5	514	tcp	7.5	High	Mitigation	rsh Unencrypted Cleartext Login	This remote host is running a rsh service.
10.0.2.5	80	tcp	7.5	High	Workaround	phpinfo() output Reporting	Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.
10.0.2.5	513	tcp	7.5	High	Mitigation	rlogin Passwordless / Unencrypted Cleartext Login	This remote host is running a rlogin service.
10.0.2.5	80	tcp	7.5	High	VendorFix	PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	PHP is prone to an information-disclosure vulnerability.
10.0.2.5	80	tcp	7.5	High	Mitigation	Test HTTP dangerous methods	Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.
10.0.2.5	6667	tcp	7.5	High	VendorFix	Check for Backdoor in UnrealIRCd	Detection of backdoor in UnrealIRCd.
10.0.2.5	6200	tcp	7.5	High	VendorFix	vsftpd Compromised Source Packages Backdoor Vulnerability	vsftpd is prone to a backdoor vulnerability.
10.0.2.5	21	tcp	7.5	High	VendorFix	vsftpd Compromised Source Packages	vsftpd is prone to a backdoor vulnerability.

						Backdoor Vulnerability	
10.0.2.5	22	tcp	7.5	High	Mitigation	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials. As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.
10.0.2.5	21	tcp	7.5	High	Mitigation	FTP Brute Force Logins Reporting	It was possible to login into the remote FTP server using weak/known credentials. As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.
10.0.2.5	80	tcp	6.8	Medium	VendorFix	TWiki Cross-Site Request Forgery Vulnerability - Sep10	The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.
10.0.2.5	6667	tcp	6.8	Medium	VendorFix	UnrealIRCd Authentication Spoofing Vulnerability	This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.
10.0.2.5	25	tcp	6.8	Medium	VendorFix	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.
10.0.2.5	21	tcp	6.4	Medium	Mitigation	Anonymous FTP Login Reporting	Reports if the remote FTP Server allows anonymous logins.

10.0.2.5	80	tcp	6	Medium	VendorFix	TWiki Cross-Site Request Forgery Vulnerability	The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.
10.0.2.5	445	tcp	6	Medium	VendorFix	Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
10.0.2.5	80	tcp	5.8	Medium	Mitigation	HTTP Debugging Methods (TRACE/TRACK) Enabled	Debugging functions are enabled on the remote web server. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
10.0.2.5	5432	tcp	5.8	Medium	VendorFix	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	OpenSSL is prone to security-bypass vulnerability.
10.0.2.5	25	tcp	5	Medium	Workaround	Check if Mailserver answer to VRFY and EXPN requests	The Mailserver on this host answers to VRFY and/or EXPN requests.
10.0.2.5	80	tcp	5	Medium	Mitigation	/doc directory browsable	The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.
10.0.2.5	25	tcp	5	Medium	Mitigation	SSL/TLS: Certificate Expired	The remote server's SSL/TLS certificate has already expired.
10.0.2.5	5432	tcp	5	Medium	Mitigation	SSL/TLS: Certificate Expired	The remote server's SSL/TLS certificate has already expired.
10.0.2.5	80	tcp	5	Medium	WillNotFix	awiki Multiple Local File Include Vulnerabilities	awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.
10.0.2.5	23	tcp	4.8	Medium	Mitigation	Telnet Unencrypted Cleartext Login	The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

10.0.2.5	80	tcp	4.8	Medium	Workaround	Cleartext Transmission of Sensitive Information via HTTP	The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
10.0.2.5	5900	tcp	4.8	Medium	Mitigation	VNC Server Unencrypted Data Transmission	The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.
10.0.2.5	2121	tcp	4.8	Medium	Mitigation	FTP Unencrypted Cleartext Login	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
10.0.2.5	21	tcp	4.8	Medium	Mitigation	FTP Unencrypted Cleartext Login	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
10.0.2.5	25	tcp	4.3	Medium	VendorFix	SSL/TLS: RSA Temporary Key Handling RSA_EXPORT Downgrade Issue (FREAK)	This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.
10.0.2.5	5432	tcp	4.3	Medium	Mitigation	SSL/TLS: Report Weak Cipher Suites	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
10.0.2.5	22	tcp	4.3	Medium	Mitigation	SSH Weak Encryption Algorithms Supported	The remote SSH server is configured to allow weak encryption algorithms.
10.0.2.5	5432	tcp	4.3	Medium	Mitigation	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
10.0.2.5	25	tcp	4.3	Medium	Mitigation	SSL/TLS: Deprecated SSLv2	It was possible to detect the usage of the

						and SSLv3 Protocol Detection	deprecated SSLv2 and/or SSLv3 protocol on this system.
10.0.2.5	25	tcp	4.3	Medium	VendorFix	SSL/TLS: DHE_EXPORT Man in the Middle Security Bypass Vulnerability (LogJam)	This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.
10.0.2.5	5432	tcp	4.3	Medium	Mitigation	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	This host is prone to an information disclosure vulnerability.
10.0.2.5	25	tcp	4.3	Medium	Mitigation	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	This host is prone to an information disclosure vulnerability.
10.0.2.5	80	tcp	4.3	Medium	VendorFix	TWiki < 6.1.0 XSS Vulnerability	bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.
10.0.2.5	80	tcp	4.3	Medium	WillNotFix	phpMyAdmin error.php Cross Site Scripting Vulnerability	The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.
10.0.2.5	80	tcp	4.3	Medium	VendorFix	Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability	This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.
10.0.2.5	5432	tcp	4	Medium	Workaround	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
10.0.2.5	25	tcp	4	Medium	Workaround	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

10.0.2.5	5432	tcp	4	Medium	Mitigation	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
10.0.2.5	25	tcp	4	Medium	Mitigation	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
10.0.2.5	22	tcp	2.6	Low	Mitigation	SSH Weak MAC Algorithms Supported	The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.
10.0.2.5			2.6	Low	Mitigation	TCP timestamps	The remote host implements TCP timestamps and therefore allows to compute the uptime.

Παράρτημα Β

Αρχείο Καταγραφής Δεδομένων «totalentitylogs1.csv»

Action	Number	Timestamp	User	Device	Activity
email	{B1Y9-Z7AR66CW-9353ONTE}	11/11/2010 10:21	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com
email	{A5Q3-L7MS05UI-3620UQII}	11/11/2010 10:22	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
email	{B2P6-F0ST65UC-0302NJJA}	11/11/2010 13:03	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
email	{T1C8-Q7CC58LS-7289GJFY}	11/11/2010 13:04	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com
email	{Z5M1-A0TV56TL-3102CFDH}	11/11/2010 13:39	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com

email	{K6C7-X6NX01ET-4527SHPO}	11/11/2010 13:40	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
email	{M4V2-C8ZS86KH-5652MPGJ}	11/11/2010 13:46	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
email	{B4Q0-W5QX16RW-7102LCFN}	11/11/2010 13:47	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com
http	{D5T6-M5VT84TZ-2060CMUL}	11/11/2010 15:26	BGC0686	PC-7309	http://www.relytec.com/Climate_of_Florida/suniest/NNXrlybttre1893061997.aspx
device	{I7N3-C6FQ76CA-8308ILFR}	11/11/2010 15:37	BGC0686	PC-7309	R:\;R:\BGC0686;R:\24h64f6
file	{H2Q6-Q8BN31JU-1543XFZN}	11/11/2010 15:41	BGC0686	PC-7309	R:\keylogger.exe
logon	{R7E5-S2JM42GS-7498OOCE}	11/11/2010 19:30	BGC0686	PC-2403	Logon

device	{P5H6-P3MD58MX-6958TXCW}	11/11/2010 19:33	BGC0686	PC-2403	R:\;R:\BGC0686;R:\24h64f6
file	{N8F5-R2LW02MY-3271EKFS}	11/11/2010 19:35	BGC0686	PC-2403	R:\keylogger.exe
logon	{Z5L0-D9QV40MP-8876JIMI}	11/11/2010 19:39	BGC0686	PC-2403	Logoff
logon	{M9I7-X7DG75MJ-7915BAHF}	11/12/2010 19:08	BGC0686	PC-2403	Logon
logon	{X7T4-H2BI85LN-2210PAMF}	11/12/2010 19:22	BGC0686	PC-2403	Logoff
logon	{T7Y4-B3HS66WG-3205FOAI}	11/12/2010 19:29	DKB0259	PC-2403	Logon
email	{B5N4-C7IX58TM-0955XNDA}	11/12/2010 19:37	DKB0259	PC-2403	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.

					Rahim.Sims@dtaa.com
logon	{N8N4-X0WB23KK-1872ALNE}	11/12/2010 19:44	DKB0259	PC-2403	Logoff
email	{L0A1-W9AB34GS-6692RUSO}	11/15/2010 07:31:00	MAH0683	PC-4972	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{Q7J8-Z5HV63PJ-8605VMZP}	11/15/2010 07:41:00	RNW0269	PC-0978	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com

email	{H0E1-H3ZA85IF-8421UAFV}	11/15/2010 07:44:00	HRS0274	PC-6791	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{D0A9-E3BX76OJ-7594KJSX}	11/15/2010 07:47:00	UNK0265	PC-0639	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{G2A8-K1CG56OG-4632GRKJ}	11/15/2010 07:48:00	GJB0268	PC-7173	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadm

					an.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{G0S2-W3YJ57JY-7476KNLM}	11/15/2010 07:48:00	SDP0271	PC-8034	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{L8H4-E5YX81ER-2429NIPP}	11/15/2010 07:52:00	SKR0266	PC-3004	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com

email	{W4D9-X3HP61JS-8881JNKA}	11/15/2010 07:53:00	ACB0270	PC-0442	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{N4I8-Y8LW94FP-7762JSFG}	11/15/2010 07:55:00	HCW0681	PC-3098	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{O7M3-A2AO80IY-0490CRBP}	11/15/2010 07:58:00	EHW0689	PC-8847	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadm

					an.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{X4Y4-R8DE32QB-6184JPSM}	11/15/2010 08:19:00	LHO0687	PC-4675	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{B1Y9-Z7AR66CW-9353ONTE}	11/11/2010 10:21	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com
email	{A5Q3-L7MS05UI-3620UQII}	11/11/2010 10:22	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
email	{B2P6-F0ST65UC-0302NJJA}	11/11/2010 13:03	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
email	{T1C8-Q7CC58LS-7289GJFY}	11/11/2010 13:04	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com

email	{Z5M1-A0TV56TL-3102CFDH}	11/11/2010 13:39	BGC0686	PC-7309	Daniel.Kibo.Bruce@dtaa.com
email	{K6C7-X6NX01ET-4527SHPO}	11/11/2010 13:40	DKB0259	PC-2403	Daniel.Kibo.Bruce@dtaa.com
email	{M4V2-C8ZS86KH-5652MPGJ}	11/11/2010 13:46	DKB0259	PC-2403	Berk.Griffin.Cooley@dtaa.com
email	{B4Q0-W5QX16RW-7102LCFN}	11/11/2010 13:47	BGC0686	PC-7309	Berk.Griffin.Cooley@dtaa.com
http	{D5T6-M5VT84TZ-2060CMUL}	11/11/2010 15:26	BGC0686	PC-7309	http://www.relytec.com/Climate_of_Florida/suniest/NNXrlybttre1893061997.aspx
device	{I7N3-C6FQ76CA-8308ILFR}	11/11/2010 15:37	BGC0686	PC-7309	R:\;R:\BGC0686;R:\24h64f6
file	{H2Q6-Q8BN31JU-1543XFZN}	11/11/2010 15:41	BGC0686	PC-7309	R:\keylogger.exe

device	{S5Q6-J0PN38XV-3573ONRU}	11/11/2010 15:43	BGC0686	PC-7309	
logon	{R7E5-S2JM42GS-7498OOCE}	11/11/2010 19:30	BGC0686	PC-2403	Logon
device	{P5H6-P3MD58MX-6958TXCW}	11/11/2010 19:33	BGC0686	PC-2403	R:\;R:\BGC0686;R:\24h64f6
file	{N8F5-R2LW02MY-3271EKFS}	11/11/2010 19:35	BGC0686	PC-2403	R:\keylogger.exe
device	{C3M5-E0HH69BC-7565TPAI}	11/11/2010 19:38	BGC0686	PC-2403	
logon	{Z5L0-D9QV40MP-8876JIMI}	11/11/2010 19:39	BGC0686	PC-2403	Logoff
logon	{M9I7-X7DG75MJ-7915BAHF}	11/12/2010 19:08	BGC0686	PC-2403	Logon
logon	{X7T4-H2BI85LN-2210PAMF}	11/12/2010 19:22	BGC0686	PC-2403	Logoff

logon	{T7Y4-B3HS66WG-3205FOAI}	11/12/2010 19:29	DKB0259	PC-2403	Logon
email	{B5N4-C7IX58TM-0955XNDA}	11/12/2010 19:37	DKB0259	PC-2403	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
logon	{N8N4-X0WB23KK-1872ALNE}	11/12/2010 19:44	DKB0259	PC-2403	Logoff
email	{L0A1-W9AB34GS-6692RUSO}	11/15/2010 07:31:00	MAH0683	PC-4972	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com

email	{Q7J8-Z5HV63PJ-8605VMZP}	11/15/2010 07:41:00	RNW0269	PC-0978	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{H0E1-H3ZA85IF-8421UAFV}	11/15/2010 07:44:00	HRS0274	PC-6791	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{D0A9-E3BX76OJ-7594KJSX}	11/15/2010 07:47:00	UNK0265	PC-0639	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadm

					an.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{G2A8-K1CG56OG-4632GRKJ}	11/15/2010 07:48:00	GJB0268	PC-7173	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{G0S2-W3YJ57JY-7476KNLM}	11/15/2010 07:48:00	SDP0271	PC-8034	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com

email	{L8H4-E5YX81ER-2429NIPP}	11/15/2010 07:52:00	SKR0266	PC-3004	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{W4D9-X3HP61JS-8881JNKA}	11/15/2010 07:53:00	ACB0270	PC-0442	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{N4I8-Y8LW94FP-7762JSFG}	11/15/2010 07:55:00	HCW0681	PC-3098	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadm

					an.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{O7M3-A2AO80IY-0490CRBP}	11/15/2010 07:58:00	EHW0689	PC-8847	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com
email	{X4Y4-R8DE32QB-6184JPSM}	11/15/2010 08:19:00	LHO0687	PC-4675	Scott.Drew.Page@dtaa.com;Galena.Jana.Burris@dtaa.com;Hyacinth.Camilla.Ware@dtaa.com;Adam.Cadman.Barton@dtaa.com;Hilel.Rahim.Sims@dtaa.com

email	{M5E7-W6HQ93IE-2962BFDO}	07/08/2010 11:51	KTW0365	PC-9776	Tatiana.Indira.Hanson@dtaa.com
email	{S7R0-O4QK56GS-0257MCIC}	07/08/2010 12:29	TIH0348	PC-2340	Kyle.Tanner.Whitaker@dtaa.com
email	{A0G8-T3CH95YI-0492KKLI}	07/08/2010 13:15	KTW0365	PC-9776	Tatiana.Indira.Hanson@dtaa.com
email	{T4C7-Y3QZ72HF-6480CLRQ}	07/08/2010 16:15	TIH0348	PC-2340	Kyle.Tanner.Whitaker@dtaa.com
http	{Z8O8-G2UI61TW-7042FUSY}	07/08/2010 17:25	KTW0365	PC-9776	http://download.cnet.com/Refog-Free-Keylogger/Climate_of_Ohio/snowiest/NNXrlybttre1252221508.aspx
device	{Z3S9-V3YA81DN-1035IEIF}	07/08/2010 17:57	KTW0365	PC-9776	Connect
file	{W5C3-R9ES43FF-7664ZAIM}	07/08/2010 17:58	KTW0365	PC-9776	4D7W09A2.exe

device	{G0P4-R1EV00ZR-7722JKII}	07/08/2010 18:11	KTW0365	PC-9776	Disconnect
logon	{G1X5-D2ZR13AT-3300FQAZ}	07/08/2010 22:16	KTW0365	PC-2340	Logon
device	{F2Y0-Y8NY32DV-1764XRMJ}	07/08/2010 22:21	KTW0365	PC-2340	Connect
device	{F5E9-U0CT29UL-9654KQOV}	07/08/2010 22:26	KTW0365	PC-2340	Disconnect
logon	{M9H2-F1UK97WG-7476USLW}	07/08/2010 22:29	KTW0365	PC-2340	Logoff
logon	{X0F1-T3HE84DE-7088YIEP}	07/09/2010 20:19	KTW0365	PC-2340	Logon
logon	{K0O9-Q9KG90FL-8984BVLW}	07/09/2010 20:30	KTW0365	PC-2340	Logoff
logon	{S1J4-J1EH68UV-8409PNZG}	07/09/2010 20:39	TIH0348	PC-2340	Logon

email	{L9P8-E9XP47IB-0015YTUX}	07/09/2010 20:43	TIH0348	PC-2340	Blaine.John.Whitney@dtaa.com;Jessamine.Hedwig.Holden@dtaa.com;Signe.Dora.Mcdowell@dtaa.com;Chava.Darrel.Lindsey@dtaa.com
logon	{A7X8-F2GA56AX-7571GQQE}	07/09/2010 20:54	TIH0348	PC-2340	Logoff
http	{R3D9-Q1LP45QH-0601CQKO}	08/02/2010 10:34	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{Z5W8-Q4QO69JI-5334SLVP}	08/02/2010 13:35	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{X2V2-V8FH03QW-4001TYHP}	08/02/2010 14:03	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchall.aspx?sitesel=All
http	{U5P7-E1PL80BQ-8026CJAL}	08/02/2010 14:33	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft

					/boomalli.html
http	{S7C8-J8GH90UP-8326WBLZ}	08/03/2010 10:47	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{D3I0-W4AX21FE-7902VRST}	08/03/2010 10:55	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{D0T0-S6GF06IY-3269RMVX}	08/03/2010 12:13	CCH0959	PC-0588	http://simplyhired.com/Amanita_bisporigera/amanita.html
http	{U3G7-Q3KC50IO-2100UDSU}	08/03/2010 12:48	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{D2Y3-S5HD53LN-3703LNMU}	08/03/2010 13:08	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{A2K0-Z8BF29QP-5159UTOG}	08/04/2010 12:45	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp

http	{C7A0-K7TS10US-8457IEAS}	08/04/2010 13:05	CCH0959	PC-0588	http://simplyhired.com/Amanita_bisporigera/amanita.html
http	{F6S2-S6ES37YC-8760PUVI}	08/04/2010 14:59	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{K7K7-M4OX72XJ-6609QVIT}	08/04/2010 15:02	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{W6Z7-Z6WQ52UQ-1547HAUN}	08/04/2010 15:42	CCH0959	PC-0588	http://lockheedmartin.com
http	{Y0Z8-R6QT22GL-7425QGQM}	08/04/2010 15:43	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{F5C6-X5AO91VE-1735AOPB}	08/05/2010 08:30	CCH0959	PC-0588	http://craigslist.org/sof/search.html
http	{T8S4-N1CN67FM-8779MYHQ}	08/05/2010 08:40	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html

http	{K7N1-P1ZZ62YX-1552YFQL}	08/05/2010 08:43	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{B6V1-H8IP86CG-7732MTSZ}	08/05/2010 09:56	CCH0959	PC-0588	http://simplyhired.com/Amanita_bisporigera/amanita.html
http	{I1V5-Z5CY05QR-9583IFLE}	08/05/2010 10:54	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{S1P2-O4WK86ZD-9650SEGA}	08/05/2010 13:22	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{G5Z4-Z2OE92NS-8979MJYK}	08/05/2010 14:37	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{H8A0-B7KW50FX-6170RSMT}	08/05/2010 14:52	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{T4P6-A6EH23MH-7486YHBI}	08/05/2010 15:24	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html

http	{H5A3-B8CV88VK-3218UYCG}	08/06/2010 08:11	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{S1X6-Y9AH17HM-4792DBFC}	08/06/2010 08:58	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{B2V4-Y4NY57DY-7778KLQK}	08/06/2010 09:18	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchall.aspx?sitesel=All
http	{H9L5-M4TS58OT-4418KDMI}	08/06/2010 11:30	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{X9A8-V2DW48RC-4565WWGZ}	08/06/2010 13:11	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{P7N4-D1ZP02RM-0817GZLO}	08/06/2010 13:21	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{E9L2-V2HW40VL-8835NQJL}	08/06/2010 13:25	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{X2S1-E5GS09IK-1174XSRE}	08/06/2010 14:12	CCH0959	PC-0588	http://careerbuilder.com/

					Bix_Beiderbecke/bix.html
http	{D2A7-W6RJ56IC-5091MFHY}	08/06/2010 15:00	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{N5F7-P7MC13AJ-1597CQXW}	08/09/2010 15:03	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{H1F9-I4IW91DL-7525CDBV}	08/10/2010 10:28	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{N9T2-N8TJ63PJ-6006NFIF}	08/10/2010 11:51	CCH0959	PC-0588	http://craigslist.org/sof/search.html
http	{O9W7-P1IS73ZG-1162EANL}	08/10/2010 12:46	CCH0959	PC-0588	http://lockheedmartin.com
http	{L7F9-G2TG63OQ-3997FYLO}	08/10/2010 14:19	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{L8A2-R3KM17KP-8424KPGU}	08/10/2010 15:36	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp

http	{K5K0-G2AQ53ZE-8571GQRZ}	08/11/2010 08:10	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{L5O8-F2EP78CO-7238GGGO}	08/11/2010 09:05	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{Y4E5-B6GS66XG-4196DFXP}	08/11/2010 10:16	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{M0P4-L1HC41HY-9895HGOF}	08/11/2010 10:56	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{R1E2-J1WP32EQ-0914NSGB}	08/11/2010 11:13	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{Y2J7-H9SX94RZ-6739MCXP}	08/11/2010 15:11	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{C0J6-H5TA31CA-2180FOGV}	08/11/2010 15:58	CCH0959	PC-0588	http://aol.com/jobs/software.html

http	{O3Z4-H0UV79QE-4184REMJ}	08/12/2010 08:52	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{E5W8-F3OT41LJ-6548BUIF}	08/12/2010 11:25	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{E5O5-A7ZU46HK-0544ZTKO}	08/12/2010 12:38	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{O7M1-L5HX63WL-8088UXZI}	08/12/2010 13:48	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{S9H3-V7RH02XC-3193DNAE}	08/12/2010 14:20	CCH0959	PC-0588	http://lockheedmartin.com
http	{K1Y5-U0AA82SG-4815ETHN}	08/12/2010 15:13	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html
http	{B7X6-P6OH87EK-5383LBXI}	08/12/2010 15:25	CCH0959	PC-0588	http://aol.com/jobs/software.html

http	{T6C9-D6OH53EH-5555OSOU}	08/12/2010 15:42	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{K0E6-R6BW28YI-7341GQAQ}	08/13/2010 14:21:49	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
email	{M7S3-H3EG03DM-7642VKON}	08/16/2010 09:41:20	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	17256
http	{S5K8-C4RB19DL-9529KQUV}	08/16/2010 10:49:43	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{Y9H1-U4FS75NB-6311DGHI}	08/16/2010 11:11:05	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html
http	{J9W3-A8BZ52TB-3948HLEM}	08/16/2010 14:38:36	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{U0M7-U0JM11YD-5814IUWS}	08/17/2010 09:17:55	CCH0959	PC-0588	http://lockheedmartin.com
http	{H6Q0-P8LA49DQ-5495TDXB}	08/17/2010 09:24:29	CCH0959	PC-0588	http://lockheedmartinjobs.com

http	{H8H5-O3XF99XO-5254VVMI}	08/17/2010 10:43:26	CCH0959	PC-0588	http://aol.com/jobs/software.html
http	{M3L1-Z5QN40ZC-0818XRLL}	08/17/2010 11:38:58	CCH0959	PC-0588	http://simplyhired.com/Amanita_bisporigera/amanita.html
http	{J1V9-X8OE22OF-3141VHPN}	08/17/2010 11:54:13	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{A1U4-I1GI65BW-0379RSMA}	08/17/2010 12:28:17	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{N4B7-K1DK15CS-6488VABE}	08/17/2010 13:02:26	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{K3Z0-E7YY37MP-0520KBLJ}	08/17/2010 13:34:24	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{Z6Z2-U5VC54PU-4737PMCF}	08/18/2010 09:27:41	CCH0959	PC-0588	http://craigslist.org/sof/search.html

http	{N5A1-E8AZ47EK-7452IAJB}	08/18/2010 11:54:30	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{D1U5-H0LM41GL-4205VVCM}	08/18/2010 13:50:27	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{C9X0-R6HV87ZQ-4662AWRZ}	08/19/2010 09:04:25	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{K1V0-R6OI63VT-7999RJBG}	08/19/2010 10:38:51	CCH0959	PC-0588	http://lockheedmartin.com
http	{N2E7-W2NU01HH-1613ZXEZ}	08/19/2010 11:28:08	CCH0959	PC-0588	http://lockheedmartin.com
http	{N0S4-F3QS33EO-3182LJLA}	08/19/2010 11:41:46	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{Y2F0-F4HX26TR-9087BZBC}	08/19/2010 11:56:40	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{A1C8-X7PM34OD-5241BBRA}	08/19/2010 13:07:24	CCH0959	PC-0588	http://aol.com/jobs/software.html

email	{C2E6-I9NS27OO-7245QCIV}	08/19/2010 13:20:37	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	26008
http	{V1W4-H3AO80UX-1008NQDR}	08/20/2010 09:09:25	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
http	{Y3O4-T0NG10LV-1669RXVN}	08/20/2010 10:20:13	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{K7F0-Y5GS01YD-6631IRIF}	08/20/2010 10:23:40	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{W9A2-T2II73UU-8259RXCV}	08/20/2010 13:39:36	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{P0M2-U6BX40YI-5853VIPM}	08/20/2010 15:51:41	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{U9I6-M2YS03WI-2156UTWB}	08/23/2010 11:05:35	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{I5O9-M1GZ78ZZ-5814JUTK}	08/23/2010 13:03:41	CCH0959	PC-0588	http://linkedin.com/jobs/

					displayhome.html
http	{O6S7-C0GS83NN-7572FAVB}	08/23/2010 14:54:34	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{R6R2-U2JW95KT-0210FWBI}	08/23/2010 15:29:13	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{E6I7-U7JP46OB-8106AFCH}	08/23/2010 15:55:16	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
email	{W5P6-C8PU34MC-9435YFUX}	08/24/2010 09:28:37	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	36158
http	{Z0G5-K7EE74FJ-0394CLJQ}	08/24/2010 10:07:51	CCH0959	PC-0588	http://lockheedmartin.com
http	{V1D4-W5WM29ZG-6313NPBW}	08/24/2010 13:53:38	CCH0959	PC-0588	http://craigslist.org/sof/search.html
email	{R2Z7-Z9LX43QK-3398GWZL}	08/24/2010 14:04:58	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	34351

http	{V3L3-M4EI36LW-1195QSQH}	08/24/2010 16:06:58	CCH0959	PC-0588	http://lockheedmartin.com
http	{Q9O4-H6NK12ZE-0472NXXH}	08/25/2010 12:29:07	CCH0959	PC-0588	http://lockheedmartin.com
http	{Y2K8-X3CE71OK-9678LIYC}	08/25/2010 12:59:13	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchall.aspx?sitesel=All
http	{V6I8-C3ON02FN-9505UAGG}	08/26/2010 08:24:55	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{X1N9-X3YN28ER-1628YCJG}	08/26/2010 08:36:41	CCH0959	PC-0588	http://monster.com/BAE_Systems/yamamah.html
http	{B3K1-W4UG89LD-1637JHXU}	08/26/2010 08:58:59	CCH0959	PC-0588	http://craigslist.org/sof/search.html
http	{N6Z0-R2ML49FO-2147PPQX}	08/26/2010 10:31:19	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{Q7M6-W1WP73AZ-0380WVNN}	08/26/2010 11:41:48	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchal

					l.aspx?sitesel=All
http	{V7T8-U8XR45BE-2680PRQI}	08/26/2010 12:33:12	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{L3J9-Z3VT79VT-0835YJBV}	08/26/2010 14:25:51	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx
http	{P0Q9-Q4OR87CG-4296ZMKR}	08/26/2010 14:38:57	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{V8F3-Z4AD16XH-9796NPFZ}	08/27/2010 09:24:29	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
email	{H2T1-Z5LH74TF-8734OPKC}	08/27/2010 10:00:43	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	20652
http	{V0D3-T4ER44IF-3150EWBH}	08/27/2010 10:21:16	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchhome.aspx

http	{M5F4-K0NC84KH-8853KQZC}	08/27/2010 11:07:00	CCH0959	PC-0588	http://indeed.com/Bronwyn_Bancroft/boomalli.html
http	{F4Z7-J3UT86EP-2581ISAX}	08/27/2010 13:46:52	CCH0959	PC-0588	http://lockheedmartin.com
http	{K9C1-Y5AF82DP-1948NNXE}	08/27/2010 14:42:54	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html
http	{X0D1-Y3RO03WX-1921DYHD}	08/27/2010 15:35:20	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchall.aspx?sitesel=All
http	{E1G1-G2NO97ED-6686ENJQ}	08/30/2010 08:03:43	CCH0959	PC-0588	http://craigslist.org/sof/search.html
email	{X3N5-E4QS91KA-8428GEKQ}	08/30/2010 08:23:48	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	33280
http	{T9X6-I9VF51JA-3761HHFG}	08/30/2010 10:09:17	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html

http	{N8F7-D0JO42YJ-3123TIUM}	08/30/2010 13:29:09	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{Z9C1-R7TQ45QZ-7754XHJR}	08/30/2010 14:13:12	CCH0959	PC-0588	http://lockheedmartinjobs.com/college.asp
email	{D0D1-E2BU14RD-2454QLSS}	08/30/2010 14:41:22	Mario.Truman.Telsa@lockheed.com	Cedric.Cyrus.Harrison@dtaa.com	19472
http	{C9Q0-M0NO67CT-3804JSCF}	08/30/2010 15:41:21	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
http	{N9V5-O9KT82KG-3703EHZY}	08/31/2010 10:03:30	CCH0959	PC-0588	http://lockheedmartinjobs.com/searchall.aspx?sitesel=All
http	{K9I5-T8RZ03CM-8497CVUU}	08/31/2010 14:17:42	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{E2N8-M6LW97SB-6837MTYW}	08/31/2010 15:23:53	CCH0959	PC-0588	http://lockheedmartinjobs.com
http	{Z1Z5-M0BD24HF-5861BUJU}	09/01/2010 08:16	CCH0959	PC-0588	http://lockheedmartinjobs.

					com/searchhome.aspx
device	{K1A1-F4JG59AC-5400IJFL}	09/01/2010 08:34	CCH0959	PC-0588	Connect
device	{M6G8-V9OY48YZ-0733MKIV}	09/01/2010 08:51	CCH0959	PC-0588	Disconnect
http	{F6V3-N6YR66WY-7617MWQU}	09/01/2010 09:07	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html
device	{N9B8-K7AP64CT-2005IIEY}	09/01/2010 09:11	CCH0959	PC-0588	Connect
device	{I1A0-R9XY83LV-9221CCNX}	09/01/2010 09:32	CCH0959	PC-0588	Disconnect
http	{S8Z7-H3LU44CA-7519ENWY}	09/01/2010 10:46	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
device	{P1I7-K5LK43HT-1704ANYR}	09/01/2010 10:51	CCH0959	PC-0588	Connect

device	{A6O0-E2UQ48WY-8392HOUG}	09/01/2010 11:14	CCH0959	PC-0588	Disconnect
device	{W3I5-V1FT69SK-4587OAJZ}	09/01/2010 11:14	CCH0959	PC-0588	Connect
device	{I7H1-J8CU35TA-9939TJAQ}	09/01/2010 11:44	CCH0959	PC-0588	Disconnect
http	{I6V7-X6HT35RE-4057LRXJ}	09/01/2010 12:59	CCH0959	PC-0588	http://careerbuilder.com/Bix_Beiderbecke/bix.html
device	{L4P6-D2GP90JX-8799LOAU}	09/01/2010 13:12	CCH0959	PC-0588	Connect
device	{E1I8-H6CX64QS-7703XIUC}	09/01/2010 14:04	CCH0959	PC-0588	Disconnect
http	{O9U6-U8GO84UN-3585VXBU}	09/01/2010 14:09	CCH0959	PC-0588	http://craigslist.org/sof/search.html
device	{S0M8-R1KE34JX-4369NEKI}	09/01/2010 14:25	CCH0959	PC-0588	Connect

http	{S1A7-W7DB14OY-0862HSWA}	09/01/2010 14:30	CCH0959	PC-0588	http://yahoo.com/hotjobs/search.html
device	{U6S5-M9OJ24OR-4468FHZR}	09/01/2010 14:54	CCH0959	PC-0588	Disconnect
http	{R0E5-R5GN20AP-3876TRKW}	09/01/2010 15:25	CCH0959	PC-0588	http://linkedin.com/jobs/displayhome.html
http	{N4G3-C7OJ20DH-2457LSBX}	09/01/2010 15:51	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
http	{L2Y0-K1QR76NM-6111THQG}	09/01/2010 16:02	CCH0959	PC-0588	http://lockheedmartinjobs.com/chat.asp
device	{X0O4-N4MS32VI-2312JYJJ}	09/02/2010 11:03	CCH0959	PC-0588	Connect
device	{H4Y3-F6ND05XB-1884OAJV}	09/02/2010 11:28	CCH0959	PC-0588	Disconnect
device	{S6G2-F9FI08RH-4635VRNT}	09/02/2010 11:51	CCH0959	PC-0588	Connect

device	{E7V3-C8VR43GW-3869TUNL}	09/02/2010 12:14	CCH0959	PC-0588	Disconnect
device	{W2R7-I3UB93QI-2282IELB}	09/02/2010 12:43	CCH0959	PC-0588	Connect
device	{X8X0-R5AD30CB-6847HWSI}	09/02/2010 13:28	CCH0959	PC-0588	Disconnect
device	{K3L5-V2DY11KR-7494SDLL}	09/02/2010 13:58	CCH0959	PC-0588	Connect
device	{X8N5-X5GQ78VB-1199MRNW}	09/02/2010 15:08	CCH0959	PC-0588	Disconnect
device	{W5A5-K3RR35JB-2070KAQS}	09/03/2010 10:05	CCH0959	PC-0588	Connect
device	{A2M7-P5KZ45WN-0681ZNOC}	09/03/2010 10:09	CCH0959	PC-0588	Disconnect
device	{H8N3-V9XM03UW-3781VRPL}	09/03/2010 10:47	CCH0959	PC-0588	Connect

device	{L8E0-M4MU88MC-6570YNCU}	09/03/2010 11:22	CCH0959	PC-0588	Disconnect
device	{J5V1-K0MY48YA-6740IYMW}	09/03/2010 11:42	CCH0959	PC-0588	Connect
device	{C6G2-R2MQ88OO-4768YGNR}	09/03/2010 12:47	CCH0959	PC-0588	Disconnect
device	{S3X8-L1DR86XE-5617XGQN}	09/03/2010 13:40	CCH0959	PC-0588	Connect
device	{J1M3-P4LB49RE-6163KFDL}	09/03/2010 13:55	CCH0959	PC-0588	Disconnect
device	{X6W4-K1SO97GD-0533RIMY}	09/03/2010 14:05	CCH0959	PC-0588	Connect
device	{K5F4-X0KT43KY-9763UUMM}	09/03/2010 14:07	CCH0959	PC-0588	Disconnect
device	{C4D8-T7DG44HP-4529UTBC}	09/03/2010 14:10	CCH0959	PC-0588	Connect

device	{N1R8-Z2VA60MW-9893ZCLW}	09/03/2010 14:59	CCH0959	PC-0588	Disconnect
device	{J5R9-Q0HZ75OY-0315CWIE}	09/07/2010 11:30	CCH0959	PC-0588	Connect
device	{T3B8-K8IM68PL-2527BNJN}	09/07/2010 11:53	CCH0959	PC-0588	Disconnect
device	{W0U9-H1PM80YZ-8179OVXQ}	09/07/2010 12:19	CCH0959	PC-0588	Connect
device	{W1N1-U3ZA54IN-6889RURW}	09/07/2010 12:59	CCH0959	PC-0588	Disconnect
device	{I9V7-L4LA76RN-9019QUVX}	09/07/2010 14:57	CCH0959	PC-0588	Connect
device	{Z0E5-S1ER24LH-8269PYOB}	09/07/2010 15:48	CCH0959	PC-0588	Disconnect
device	{N2A8-P1SB57OX-3582IGYG}	09/08/2010 08:38	CCH0959	PC-0588	Connect

device	{Y2U1-G8KR60IT-6641GGIB}	09/08/2010 11:47	CCH0959	PC-0588	Disconnect
device	{I8O1-J2ZK56ET-2391SILQ}	09/09/2010 09:18	CCH0959	PC-0588	Connect
device	{H9D6-N8QP11UE-9052WINL}	09/09/2010 10:22	CCH0959	PC-0588	Disconnect
device	{R0T7-X5TQ89AH-2198IXBH}	09/09/2010 10:37	CCH0959	PC-0588	Connect
device	{G8R1-Y5SO26VX-4865VPON}	09/09/2010 11:23	CCH0959	PC-0588	Disconnect
device	{M4G5-D1NT99AB-2493QAQL}	09/09/2010 12:17	CCH0959	PC-0588	Connect
device	{T4G2-Q4VW02TJ-3060IFFX}	09/09/2010 12:36	CCH0959	PC-0588	Disconnect
device	{H1W6-I7TA23LO-5480MAVZ}	09/09/2010 13:18	CCH0959	PC-0588	Connect

device	{Q2O1-E3VJ16DU-9281DSLP}	09/09/2010 13:21	CCH0959	PC-0588	Disconnect
device	{I3R2-W9PC10DT-4519URIM}	09/09/2010 13:33	CCH0959	PC-0588	Connect
device	{K4L3-W2GE72HL-2603ACJG}	09/09/2010 15:09	CCH0959	PC-0588	Disconnect
device	{Q1S3-C2QZ14TA-3928WZMG}	09/09/2010 15:11	CCH0959	PC-0588	Connect
device	{Q7D2-O1BG26UI-7400KGMC}	09/09/2010 15:16	CCH0959	PC-0588	Disconnect
device	{I9O9-K7AJ28LM-6073URML}	09/09/2010 15:20	CCH0959	PC-0588	Connect
device	{T8E4-C5KV03GR-2583ZXVJ}	09/09/2010 15:40	CCH0959	PC-0588	Disconnect
device	{F1K5-M6IJ80UR-4799MACV}	09/10/2010 08:50	CCH0959	PC-0588	Connect

device	{X7C0-A3UF15XL-7526FIHB}	09/10/2010 09:19	CCH0959	PC-0588	Disconnect
device	{R7A3-M1WQ12HQ-7947RDRG}	09/10/2010 11:01	CCH0959	PC-0588	Connect
device	{G9J1-H5VC30NW-1708DWTN}	09/10/2010 11:04	CCH0959	PC-0588	Disconnect
device	{N7H0-L7VJ15ZE-8472EAKE}	09/10/2010 11:29	CCH0959	PC-0588	Connect
device	{B7K0-T9FK46YU-4323IUTB}	09/10/2010 11:54	CCH0959	PC-0588	Disconnect
device	{M9Z9-T8FY23FD-0408VXTX}	09/10/2010 12:07	CCH0959	PC-0588	Connect
device	{L3P5-W3EJ51YA-4311SWMO}	09/10/2010 12:25	CCH0959	PC-0588	Disconnect
device	{U8A8-A4BQ65IN-6808QXDI}	09/10/2010 12:48	CCH0959	PC-0588	Connect

device	{P1U6-Z8UX07WA-7605XTRR}	09/10/2010 12:54	CCH0959	PC-0588	Disconnect
device	{R4F1-X7MU39BV-3291JUKO}	09/10/2010 12:55	CCH0959	PC-0588	Connect
device	{X3W8-I6FO66US-2858VHUI}	09/10/2010 14:24	CCH0959	PC-0588	Disconnect
device	{Y8N3-Q3QM49GL-9794AGNO}	09/10/2010 14:51	CCH0959	PC-0588	Connect
device	{B3N5-Z3JA18EQ-4145YOCA}	09/10/2010 15:36	CCH0959	PC-0588	Disconnect
device	{G6M0-A7BP02EF-0947GEWI}	09/13/2010 08:34:15	CCH0959	PC-0588	Connect
device	{T1G9-R9YX56SN-8252TAII}	09/13/2010 08:40:18	CCH0959	PC-0588	Disconnect
device	{I9R2-E7NP28SU-6350AFMH}	09/13/2010 09:21:23	CCH0959	PC-0588	Connect

device	{Z9Q7-X4WQ16MP-1591IGUC}	09/13/2010 11:57:15	CCH0959	PC-0588	Disconnect
device	{W4O1-M8YM68GK-6891QRQV}	09/13/2010 14:00:14	CCH0959	PC-0588	Connect
email	{U1Q2-L9YA20OC-3177ZENY}	09/14/2010 08:50:10	Desiree.Claudia.Booth@dtaa.com	Cedric.Cyrus.Harrison@dtaa.com	23368
device	{Q3Y0-Q9KN77AI-7036BFXD}	09/14/2010 09:02:10	CCH0959	PC-0588	Connect
device	{M8T3-P8QF26YD-7675HSJT}	09/14/2010 09:13:33	CCH0959	PC-0588	Disconnect
device	{C6E2-E4BR68EF-9861UJHE}	09/14/2010 10:30:56	CCH0959	PC-0588	Connect
device	{V6B6-S6HT12RC-0315NDGX}	09/14/2010 12:16:06	CCH0959	PC-0588	Disconnect
device	{B6B9-P6UD96MC-2475LYLT}	09/14/2010 12:18:34	CCH0959	PC-0588	Connect

device	{I4G6-C5RI89QA-8257ZKSI}	09/14/2010 12:26:06	CCH0959	PC-0588	Disconnect
device	{A5R1-P9BC15QX-3575UXMA}	09/14/2010 12:42:16	CCH0959	PC-0588	Connect
device	{K4Z8-W0ZJ54SK-6297HAHQ}	09/14/2010 13:42:35	CCH0959	PC-0588	Disconnect
device	{C2F6-V3UY69WM-4998QPJY}	09/14/2010 14:14:08	CCH0959	PC-0588	Connect
device	{N4R6-V9RP41SP-4203DKGV}	09/14/2010 14:25:35	CCH0959	PC-0588	Disconnect
device	{U9P7-X4CA42GA-5867OEBI}	09/14/2010 14:28:11	CCH0959	PC-0588	Connect
device	{Y7C2-R9QJ78YX-6009CCYR}	09/14/2010 15:03:57	CCH0959	PC-0588	Disconnect
device	{D5T8-B0UZ21IX-0141BGIF}	09/14/2010 15:25:45	CCH0959	PC-0588	Connect

device	{U9I7-O4OO30GM-0831MPXP}	09/14/2010 15:28:49	CCH0959	PC-0588	Disconnect
device	{V5W4-W7EC28SW-4112IOWO}	09/15/2010 12:06:26	CCH0959	PC-0588	Connect
device	{K2R8-M4VX83ZC-3834UHZO}	09/15/2010 13:18:12	CCH0959	PC-0588	Disconnect
device	{W3Z7-U2EL34DS-9353UECX}	09/15/2010 14:09:38	CCH0959	PC-0588	Connect
device	{B3B5-S2MC33IG-4905VSGW}	09/15/2010 14:12:58	CCH0959	PC-0588	Disconnect
device	{L7G5-H8HL59YM-4287WAXM}	09/15/2010 14:14:30	CCH0959	PC-0588	Connect
device	{Z9U7-C3IS88ZT-5359BPBS}	09/16/2010 09:20:25	CCH0959	PC-0588	Connect
device	{W2E5-U5TQ67UT-5799SAUM}	09/16/2010 09:29:40	CCH0959	PC-0588	Disconnect

device	{D6L1-Y4NX35RU-3476FIXE}	09/16/2010 10:27:57	CCH0959	PC-0588	Connect
device	{C1E4-G7QO45HA-0500NSTY}	09/16/2010 11:26:56	CCH0959	PC-0588	Disconnect
device	{J7U2-T1KR64CM-7681JUBS}	09/16/2010 11:50:05	CCH0959	PC-0588	Connect
device	{I6C5-U3BK08CT-4184UGXW}	09/16/2010 12:36:30	CCH0959	PC-0588	Disconnect
device	{Z3Q1-L4HZ63GJ-7797SUIV}	09/16/2010 13:03:24	CCH0959	PC-0588	Connect
device	{J7G9-L9TY11FX-8451VDHM}	09/16/2010 13:38:27	CCH0959	PC-0588	Disconnect
device	{I7L4-R3XZ60RV-1806UVGY}	09/16/2010 14:28:43	CCH0959	PC-0588	Connect
device	{A9R8-F1AX65FP-2439QOET}	09/16/2010 14:57:27	CCH0959	PC-0588	Disconnect

device	{G3F7-V2BU56IU-3588UTQM}	09/16/2010 15:24:49	CCH0959	PC-0588	Connect
device	{R7R3-B7PY09YT-8978JEJK}	09/16/2010 15:39:57	CCH0959	PC-0588	Disconnect
device	{D4C3-I7TA69LN-4100LOTW}	09/17/2010 08:05:22	CCH0959	PC-0588	Connect
device	{A2S4-E2KS62FQ-4697PXRH}	09/17/2010 08:23:19	CCH0959	PC-0588	Disconnect
device	{E3T6-M5OG66IR-2057PJXC}	09/17/2010 11:17:16	CCH0959	PC-0588	Connect
device	{X1W5-V3NK78GP-6320SXGV}	09/17/2010 11:24:54	CCH0959	PC-0588	Disconnect
device	{R3N8-J8NT41QP-0646GRIG}	09/17/2010 12:21:42	CCH0959	PC-0588	Connect
device	{Q5O4-J8DX74GJ-5476SYOT}	09/17/2010 12:45:18	CCH0959	PC-0588	Disconnect

device	{E5U4-H3SZ65OR-0866BMHD}	09/17/2010 13:30:53	CCH0959	PC-0588	Connect
device	{O6V3-G1RJ02QJ-3580DLJB}	09/17/2010 13:40:51	CCH0959	PC-0588	Disconnect
device	{T8S1-L3TC15OW-0983PTAS}	09/17/2010 14:00:03	CCH0959	PC-0588	Connect
device	{M0G2-K8GP59UN-7708ZNCP}	09/17/2010 15:51:49	CCH0959	PC-0588	Disconnect
device	{M3N7-A2PU43DF-7291MBUV}	09/20/2010 08:54:11	CCH0959	PC-0588	Connect
device	{N7Y6-M6FF62EW-9576PHND}	09/20/2010 09:51:26	CCH0959	PC-0588	Disconnect
device	{M4Z3-H9XB37WK-9560FXFC}	09/20/2010 11:08:34	CCH0959	PC-0588	Connect
device	{U6H0-R1UL07WI-9612CVNI}	09/20/2010 12:04:43	CCH0959	PC-0588	Disconnect

device	{K8O5-M3YP42OK-5069WOMZ}	09/20/2010 12:19:02	CCH0959	PC-0588	Connect
device	{F9B0-V9VU04XR-4634WHUA}	09/20/2010 13:11:58	CCH0959	PC-0588	Disconnect
device	{L9U6-V6HG74EO-8911ECAB}	09/21/2010 10:01:09	CCH0959	PC-0588	Connect
device	{A7X5-V2TN45EB-9203MHVL}	09/21/2010 11:20:59	CCH0959	PC-0588	Disconnect
device	{H6D7-L1RG17TC-5502JUWK}	09/21/2010 13:41:50	CCH0959	PC-0588	Connect
device	{X5H4-E5FX28GJ-8272YZFV}	09/21/2010 14:06:23	CCH0959	PC-0588	Disconnect
device	{S0X3-E1LE50SP-6414IDQT}	09/22/2010 09:16:03	CCH0959	PC-0588	Connect
device	{J4G3-F7RS95KA-0796VWIJ}	09/22/2010 09:33:41	CCH0959	PC-0588	Disconnect

device	{I1K4-H6XG04WM-9164ASUE}	09/22/2010 10:00:37	CCH0959	PC-0588	Connect
device	{Z3N1-M4FK21BH-4042WARQ}	09/22/2010 10:22:48	CCH0959	PC-0588	Disconnect
device	{R6Z5-D5CW84JQ-5310NPUL}	09/22/2010 11:28:48	CCH0959	PC-0588	Connect
device	{M3H3-U1NN04WQ-0285SDFC}	09/22/2010 12:01:17	CCH0959	PC-0588	Disconnect
device	{S3R7-L5BX26UB-5361SZFC}	09/22/2010 13:15:56	CCH0959	PC-0588	Connect
device	{R1O3-A1MJ15MY-2895NRXD}	09/22/2010 14:05:16	CCH0959	PC-0588	Disconnect
device	{C3M9-P3VC23HD-9450HROH}	09/22/2010 14:07:27	CCH0959	PC-0588	Connect
device	{R5W3-N7NC09EW-9566RMJU}	09/22/2010 14:10:31	CCH0959	PC-0588	Disconnect

device	{E7X5-J3NA29GH-2410VQZA}	09/22/2010 15:19:42	CCH0959	PC-0588	Connect
device	{R2G9-Y3GY98FB-5219IFFK}	09/22/2010 15:55:44	CCH0959	PC-0588	Disconnect
device	{Y6R6-U9QD49NM-6275SHHV}	09/23/2010 08:09:22	CCH0959	PC-0588	Connect
device	{P8M2-X2KK33LD-0967BUFM}	09/23/2010 08:41:49	CCH0959	PC-0588	Disconnect
device	{E9T7-L7CX17ON-3843MVUL}	09/23/2010 09:04:03	CCH0959	PC-0588	Connect
device	{I8Y2-B2BE67QJ-9322AXWF}	09/23/2010 10:19:53	CCH0959	PC-0588	Disconnect
device	{V0G0-X1VF69UD-9463GRZX}	09/23/2010 10:55:18	CCH0959	PC-0588	Connect
device	{G7N4-N4OC83NB-6186PQUO}	09/23/2010 11:00:41	CCH0959	PC-0588	Disconnect

device	{S5V8-E3HP80BP-3629MZWX}	09/23/2010 12:10:30	CCH0959	PC-0588	Connect
device	{E2Y7-D5WJ65MW-6444VZQK}	09/23/2010 12:49:02	CCH0959	PC-0588	Disconnect
device	{T5V1-K9OP43TX-4160DWRL}	09/23/2010 12:57:54	CCH0959	PC-0588	Connect
device	{S9Z4-Q2UI24PK-8233PSFG}	09/23/2010 14:53:25	CCH0959	PC-0588	Disconnect
device	{C9C0-C5UH35VT-8090GZAB}	09/23/2010 15:57:41	CCH0959	PC-0588	Connect
device	{E0M5-S7HV26FE-4612MUJV}	09/24/2010 08:27:18	CCH0959	PC-0588	Connect
device	{O7D0-V8XQ08LP-5159TSYS}	09/24/2010 09:09:51	CCH0959	PC-0588	Disconnect
device	{K8A4-T0GJ88VS-1740VSVK}	09/24/2010 09:27:59	CCH0959	PC-0588	Connect

device	{R3I5-Y1JR07PE-4365ZAUS}	09/24/2010 14:48:08	CCH0959	PC-0588	Disconnect
device	{F2J9-A7AI94XE-5657XKLU}	09/27/2010 08:45:30	CCH0959	PC-0588	Connect
device	{X5P2-R7EU12OP-5902KYPL}	09/27/2010 10:46:03	CCH0959	PC-0588	Disconnect
device	{Y4X4-O0LN54BV-0195WOQC}	09/27/2010 10:50:33	CCH0959	PC-0588	Connect
device	{R7B5-M8GM14ER-0394QOPE}	09/27/2010 13:20:54	CCH0959	PC-0588	Disconnect
device	{Y1Z9-E1BG13AK-2397VOPO}	09/27/2010 13:33:34	CCH0959	PC-0588	Connect
device	{W6W0-Q3LY53DA-9900XDMS}	09/27/2010 13:52:16	CCH0959	PC-0588	Disconnect
device	{C2O1-G2GG71UM-0361OHUV}	09/27/2010 14:18:36	CCH0959	PC-0588	Connect

device	{W9Z2-K3AB93GC-7441MFZZ}	09/27/2010 14:25:47	CCH0959	PC-0588	Disconnect
device	{D7Z4-C1MH27VC-7222ZSDA}	09/27/2010 14:41:22	CCH0959	PC-0588	Connect
device	{O6H1-U2BX43PT-1886SYKD}	09/27/2010 14:49:15	CCH0959	PC-0588	Disconnect
device	{B8W9-P3XC92MT-0815JFUS}	09/28/2010 11:55:22	CCH0959	PC-0588	Connect
device	{Z0H1-W5BP55UO-3432UCDW}	09/28/2010 14:15:36	CCH0959	PC-0588	Disconnect
device	{J3Z4-T4MJ07GB-1324RHYD}	09/28/2010 14:34:09	CCH0959	PC-0588	Connect
device	{Q1R9-C7ZL50OJ-8199WXKW}	09/28/2010 15:59:50	CCH0959	PC-0588	Disconnect
device	{F8E7-V6JK15OJ-7027BHTK}	09/29/2010 10:47:49	CCH0959	PC-0588	Connect

device	{Q5G6-P3EJ75NM-8389SCJR}	09/29/2010 11:57:13	CCH0959	PC-0588	Disconnect
device	{Q9I5-Y5IV20RH-9873YAON}	09/29/2010 12:09:32	CCH0959	PC-0588	Connect
device	{F1M1-G6KC28FT-4762KAND}	09/29/2010 12:29:58	CCH0959	PC-0588	Disconnect
device	{H3X0-K3DR76WL-3172IKFY}	09/29/2010 13:45:10	CCH0959	PC-0588	Connect
device	{C2U8-H9VR70QD-7501VOWY}	09/29/2010 14:26:08	CCH0959	PC-0588	Disconnect
device	{E8Y9-F0BS51KD-3248TGJJ}	09/29/2010 14:27:27	CCH0959	PC-0588	Connect
device	{W5C8-B2YJ31IQ-8493OUOZ}	09/29/2010 14:38:40	CCH0959	PC-0588	Disconnect
device	{H4G1-T1WZ32QP-9687BJYV}	09/30/2010 08:36:40	CCH0959	PC-0588	Connect

device	{W6T9-B2EE27OT-0918FXQX}	09/30/2010 08:43:43	CCH0959	PC-0588	Disconnect
device	{G1I8-V7UL85HC-4153GCCX}	09/30/2010 09:10:35	CCH0959	PC-0588	Connect
device	{T1O2-D2HI81TX-8661YSTZ}	09/30/2010 09:14:52	CCH0959	PC-0588	Disconnect
device	{Y3W0-U9WH86ZT-1230QRII}	09/30/2010 10:38:13	CCH0959	PC-0588	Connect
device	{Y3P5-X5FF83MO-7680QOEY}	09/30/2010 10:53:06	CCH0959	PC-0588	Disconnect
device	{N8G3-L0EI03UC-7477ZSTM}	09/30/2010 14:43:10	CCH0959	PC-0588	Connect
device	{K3W9-H6AX00ZD-8310SOKX}	09/30/2010 15:04:03	CCH0959	PC-0588	Disconnect
http	{P5F2-W0PW42YT-3105AQRC}	08/23/2010 10:40:56	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp

http	{Y7Q3-X6PW73PX-6568ORVX}	08/23/2010 10:50:29	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp
http	{Y8G8-Z8QC94AP-4719NLNF}	08/23/2010 12:10:18	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{D6U0-X5PO02PQ-4697AYDE}	08/23/2010 12:30:37	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{H2M3-O5HY40GR-7387HKQQ}	08/23/2010 13:10:25	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{M9V7-E9YJ43QD-8502BTRF}	08/23/2010 13:34:49	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{E3C3-K2XE84LC-7921GTMD}	08/24/2010 04:07:22	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{C9Z7-E9QN58MW-6608VULB}	08/24/2010 04:09:54	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html

http	{X4K7-V4SX20WB-9538NUBS}	08/24/2010 04:17:17	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{O0I9-T3SS05MZ-8369AXCY}	08/24/2010 04:31:11	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{Z4T8-H1CC22FJ-9886BUBR}	08/24/2010 04:43:35	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{Y5D0-D5QQ21CS-9566NRRE}	08/24/2010 04:49:06	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{Q0X1-S9EW93JP-0060FWNV}	08/24/2010 04:51:39	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{D4L4-O4ZS98WP-7271ONRB}	08/24/2010 05:06:26	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx

http	{H0K9-N2LW97WA-7720UMTL}	08/24/2010 05:43:14	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp
http	{B4A2-C2NV43GS-6665ZAHB}	08/24/2010 05:51:04	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{H9C9-W3TR22HF-9751BJYW}	08/24/2010 06:00:22	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{S3B6-D6NM53AT-6172QXVB}	08/24/2010 06:05:02	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{N7R5-T1JC08EE-3278UXCV}	08/24/2010 06:09:44	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{G5E1-V9CY27IP-6332VSIS}	08/24/2010 06:16:02	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php

http	{H2W7-X1IA03TK-7236OIZB}	08/24/2010 06:19:00	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{M8K4-K4EW27RF-0619FSHI}	08/24/2010 06:21:10	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{O7Y6-U8XG98OA-0492DZJE}	08/24/2010 06:24:28	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{Q7W4-D6JA43NV-5533HBUL}	08/24/2010 06:31:39	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{A7X1-Z4BT32CD-3365ZMOR}	08/24/2010 07:59:17	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{J1M1-S6RQ82IY-8759SPYG}	08/24/2010 10:30:12	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp

http	{A1O1-I2UL84GT-0486BHYL}	08/25/2010 11:46:23	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{X3Y7-L8WF27XC-5380NNGA}	08/25/2010 14:08:09	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{I6N5-T6DK26MF-3972TDFL}	08/25/2010 14:32:08	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx
http	{Y3I0-U5EG70MJ-3083AGDH}	08/25/2010 15:51:26	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{U9J0-M4HO91OP-0530DEKN}	08/25/2010 15:59:37	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx
http	{T3Q5-D2XD87IT-7538YZST}	08/25/2010 17:03:51	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx

http	{V8M5-D6FR10VU-2110GFYM}	08/26/2010 07:45:11	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{B6U7-B9WA43VI-1966BPVE}	08/26/2010 10:00:54	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{A2U2-H3RN79AH-8069KDNN}	08/26/2010 14:57:09	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{X5T5-C0PK29AQ-2865KWJL}	08/26/2010 15:07:39	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{M1N5-P5LU92RZ-7264LCNZ}	08/26/2010 16:40:18	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{K1G5-F3UP31IQ-1510LDUX}	08/27/2010 07:46:15	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm

http	{S5B6-Y9CM35ZR-9948QPPX}	08/27/2010 08:40:26	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{W0B5-W7UJ49PN-9673WQUC}	08/27/2010 09:35:26	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{D6Q6-U5BT27NN-3007KAFC}	08/27/2010 10:28:54	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{L1N0-E3LU79BH-2310UHDC}	08/27/2010 11:30:22	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{F8E6-L1SD03EN-0238RUSC}	08/27/2010 12:13:57	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{P4D1-J0NK74LC-2031GEGJ}	08/30/2010 11:04:07	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx

http	{F4F9-A8TV83AA-6653CLEJ}	08/30/2010 14:24:07	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{Q4R4-W9MF65LX-1274YVLJ}	08/30/2010 14:39:18	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp
http	{W7R3-Q8KW61HN-0617WUWS}	08/30/2010 16:34:32	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{O0G9-J4UI15SV-7064AHII}	08/31/2010 08:05:06	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{K0E1-K9JT28JS-5018QPNV}	08/31/2010 08:13:52	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{M0G7-T2OJ60JN-5919TSKV}	08/31/2010 08:42:22	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx
http	{J2W4-D9RF03KY-9986SMWQ}	08/31/2010 10:10:54	HFC0492	PC-4332	http://monster.com/Wbo

					Uhagvat1180707852.html
email	{B5B3-J5PY75RL-8668CYEL}	08/31/2010 10:26:56	HFC0492	PC-4332	Banks-Kellie@harris.com
email	{M4I1-O7ZQ04DB-9450JQXZ}	08/31/2010 12:05:16	HFC0492	PC-4332	Banks-Kellie@harris.com
email	{G8T8-L0PU94AE-0564DXYU}	08/31/2010 12:42:24	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{R4W6-E9ZB68SG-3118IYVW}	09/01/2010 08:36	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{L5O2-O6AS90IU-8014AJHO}	09/01/2010 13:32	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{E6G1-X5DS43QM-5323CUKK}	09/01/2010 13:34	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
http	{W4D4-M4FO44SE-4570PETE}	09/01/2010 13:47	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx

http	{D1K1-R4ET60GA-5367AEZB}	09/01/2010 13:57	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{K9W5-Y0QQ75HR-0204ZWRZ}	09/01/2010 15:10	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{P9F8-T9RB53SR-4848HXLD}	09/01/2010 15:31	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{B7B2-E6IM87AE-7708YIBL}	09/01/2010 16:10	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
http	{Z5U7-J0GH64UT-8906QLDB}	09/01/2010 16:51	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{L6X6-Q5JB66HN-1270CDEL}	09/02/2010 08:29	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{K9V2-V4TF82VZ-8551GUGX}	09/02/2010 09:53	HFC0492	PC-4332	http://lockheedmartin.com/WboUhag

					vat1636367808.htm
http	{N4T6-R9EP95RT-2901HYNW}	09/02/2010 12:46	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{Q7C1-U9KF70PG-7323CRUJ}	09/02/2010 13:35	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp
http	{Z1Q6-J1FG47JL-8908ROPS}	09/02/2010 13:37	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{W1I9-E1XK31PY-8968GRTK}	09/02/2010 14:44	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{G4C2-B4JX06ME-7520JAGR}	09/02/2010 14:54	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx

http	{O5U2-L9OX98WU-1267CBNT}	09/02/2010 15:01	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{R2T2-Q5RS81VP-9794FQER}	09/02/2010 16:43	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{O5V6-E6ZJ02JZ-3027ZVKS}	09/02/2010 16:57	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx
http	{R8K8-T3NW30DY-7130CGQE}	09/02/2010 20:12	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
http	{W0U7-L8TB83PJ-4822VMGI}	09/02/2010 20:16	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{J5W8-C3YP07GM-7510SLFC}	09/02/2010 20:17	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{L4R9-Y7WK88SS-6132BYGR}	09/02/2010 20:18	HFC0492	PC-4332	http://raytheon.com/Wbo

					Uhagvat343187784.jsp
http	{W4F0-Z8HN58JA-2653TLQP}	09/02/2010 20:20	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{D1Q9-M6RP08RW-0644SJKR}	09/02/2010 20:22	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{Z3B8-J1UD01MV-0277VUXV}	09/02/2010 20:22	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{S2A1-N3AY30DH-4172GTHX}	09/02/2010 20:23	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{X8H0-M8UN36JE-3948GSUE}	09/02/2010 20:24	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{W2X4-X6GL46JP-4111YNEV}	09/03/2010 08:48	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx

email	{U6E4-T0SM22SE-1853GVEF}	09/03/2010 12:54	HFC0492	PC-4332	Banks-Kellie@harris.com
email	{V9K8-W0NA57OL-6612XVMS}	09/03/2010 13:00	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{V9I4-J4KL60ST-3620HUKZ}	09/07/2010 08:10	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{D4B2-R4WL59QG-4833UOGI}	09/07/2010 08:37	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{L0Q0-P1PK51QD-1418CAPL}	09/07/2010 08:53	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{N0I6-J6XY17EW-9648UWYA}	09/07/2010 09:38	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{O7Q8-V8NY16NJ-4860RTTM}	09/07/2010 10:58	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm

http	{A5E2-K1FD76ES-1839XFZI}	09/07/2010 11:56	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{H9W8-K4MV73WQ-2488QQVS}	09/07/2010 12:44	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{D8D9-X5JF64LF-5016KGLZ}	09/07/2010 13:52	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{V3N3-Q9OP21KQ-6542OQAG}	09/07/2010 17:08	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{K0Y2-C3NY79XY-8636ARGC}	09/08/2010 13:23	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{C6B9-V9PW72TN-0887FSXH}	09/08/2010 13:57	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm

http	{L1T7-G3KH29VV-1223VRSD}	09/08/2010 14:52	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{R5V2-F6SX97NF-8393KYRV}	09/08/2010 15:19	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{J4D7-O5SX86GH-4900ZKQG}	09/08/2010 15:36	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{G0W7-G0QE01VB-8028OSDO}	09/08/2010 15:37	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{H7E4-Z1NL54AZ-9759GTPN}	09/08/2010 16:21	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp
http	{R3V5-B5UA52HV-1964KLAP}	09/08/2010 16:32	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
http	{P9H9-M8YZ39VF-7550RGKA}	09/09/2010 08:40	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhag

					vat1258877042.aspx
http	{S2B0-Z6MH79NJ-3302SGPA}	09/09/2010 10:01	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp
email	{Z7T0-B8LH86PO-0207LFLO}	09/09/2010 14:46	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{F0A3-B2XP07QV-5154JZVT}	09/10/2010 07:45	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{Y1F0-L4WA76ZL-4090BUDA}	09/10/2010 08:00	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
email	{N7Z9-E0TO83ZC-7025HIRC}	09/10/2010 08:02	HFC0492	PC-4332	Banks-Kellie@harris.com
email	{V5X8-Z2BS76VW-6988JDYD}	09/10/2010 08:05	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{E7Z3-V9WT02FF-7853CRSE}	09/10/2010 08:32	HFC0492	PC-4332	http://raytheon.com/Wbo

					Uhagvat343187784.jsp
http	{J9O0-Q7BC88SC-5744YYQO}	09/10/2010 08:49	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{W5M7-C2ZE73QV-2029ZAEC}	09/10/2010 09:04	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp
http	{V1B2-I2NV31PA-1352FTLE}	09/10/2010 12:35	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
email	{X0Z5-W0CI63OS-2475JLUC}	09/10/2010 12:45	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{C4W3-I8BA64BJ-8970VDZJ}	09/10/2010 13:06	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{U4M0-K5SL19LX-2004UZEA}	09/10/2010 14:46	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagva

					t752138490.php
http	{N4S2-L4LH13FZ-9414RNSA}	09/10/2010 15:24	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhagvat1258877042.aspx
http	{K4G6-N8ZI92WT-8164HEWP}	09/10/2010 17:10	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{F3P4-T0YT08NR-6773HOMC}	09/13/2010 07:41:31	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{W2D4-M8XV66DV-9131CZLI}	09/13/2010 08:03:13	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{J9D0-C7AR84RA-9526FPBT}	09/13/2010 08:33:10	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm
http	{J2Z0-T4GR86CJ-1423FLUJ}	09/13/2010 09:42:44	HFC0492	PC-4332	http://jobhuntersbible.com/WboUhag

					vat1258877042.aspx
http	{C7S4-U1WY43WX-5717LLRL}	09/13/2010 12:44:43	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{Q0C5-J3OG76ZO-6307YNKM}	09/13/2010 12:52:32	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{P1H6-G3YS75ZY-1632WCKN}	09/13/2010 14:34:34	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{Y9V0-U8ZR39VN-4444EZSB}	09/13/2010 14:41:48	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat660170997.htm
http	{P8U6-X9GT58ZN-2432LBYC}	09/13/2010 15:30:26	HFC0492	PC-4332	http://aol.com/jobs/WboUhagvat1963819229.jsp
http	{S1S8-M7VN18KR-6606BBHG}	09/13/2010 17:01:01	HFC0492	PC-4332	http://lockheedmartin.com/WboUhagvat1636367808.htm

http	{Q0L1-W5NV88WI-2411UVEE}	09/14/2010 08:06:08	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{S1B9-M1FW83AY-5036BOUO}	09/14/2010 11:26:45	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
http	{J1N3-Z5IH10LS-7972RZGS}	09/14/2010 14:13:19	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{D2I2-I5ZT99KB-2429ZXRN}	09/14/2010 16:06:54	HFC0492	PC-4332	http://yahoo.com/hotjobs/WboUhagvat752138490.php
http	{Y6T9-Z4AM23TK-5692MSQQ}	09/14/2010 16:57:15	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp
http	{L4N0-X0TL00GQ-5391NSHV}	09/15/2010 07:43:42	HFC0492	PC-4332	http://craigslist.org/WboUhagvat1105403916.aspx

http	{Z5C5-R2PF29LG-4524HQSV}	09/15/2010 08:13:46	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{M1B8-Y2NI67KI-4692VEEF}	09/15/2010 11:15:41	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
email	{H8D3-P4KC15YP-7739SNHO}	09/15/2010 15:48:51	HFC0492	PC-4332	Banks-Kellie@harris.com
http	{S1Y8-F6MC14LB-2447SJQK}	09/15/2010 17:06:50	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp
http	{T3N4-S5CO25AV-4622ICZT}	09/16/2010 08:22:43	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{G0Q8-D9XE82VJ-6749XGUT}	09/16/2010 09:48:23	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{L5D4-A4AE25XO-0856ENPX}	09/16/2010 10:31:15	HFC0492	PC-4332	http://hp.com/WboUhagvat1944152218.jsp

http	{T3V2-H5YA72NE-7361VYYQ}	09/16/2010 11:15:43	HFC0492	PC-4332	http://boeing.com/WboUhagvat1904327536.htm
http	{N7O0-Z1AU10IA-9258MENP}	09/17/2010 09:44:18	HFC0492	PC-4332	http://linkedin.com/WboUhagvat1479839504.aspx
http	{Y2U0-Y7LP14EW-2225UFIH}	09/17/2010 10:15:58	HFC0492	PC-4332	http://harris.com/WboUhagvat1919385663.htm
http	{O8U8-W6OR16BU-9752HQXL}	09/17/2010 11:29:59	HFC0492	PC-4332	http://simplyhired.com/WboUhagvat57469130.jsp
http	{B8O6-X6TG47GN-0547PGGC}	09/17/2010 13:39:48	HFC0492	PC-4332	http://indeed.com/WboUhagvat1680703797.html
http	{Y8R9-P1NJ53EE-3866KQSQ}	09/17/2010 16:03:55	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
http	{T1F2-G8BU58IY-2542QLJM}	09/17/2010 16:31:55	HFC0492	PC-4332	http://careerbuilder.com/WboUhagvat

					660170997.htm
http	{Y1C4-H7LH84RL-9794WCHM}	09/17/2010 16:34:31	HFC0492	PC-4332	http://job-hunt.org/WboUhagvat919122234.html
http	{I9L2-R1SH39FI-8652ODVW}	09/17/2010 17:07:15	HFC0492	PC-4332	http://northropgrumman.com/WboUhagvat572113271.aspx
device	{H7K3-S1UG17VK-6673QYPQ}	09/20/2010 07:39:45	HFC0492	PC-4332	Connect
device	{I9Z2-J4OW48HC-3862SRXN}	09/20/2010 07:53:48	HFC0492	PC-4332	Disconnect
device	{K4F2-A5FE64DA-7531SLPT}	09/20/2010 08:38:44	HFC0492	PC-4332	Connect
device	{B0O6-T7UO29VY-8081QVHT}	09/20/2010 08:43:33	HFC0492	PC-4332	Disconnect
http	{N9M5-E2SH02CS-0741DFCC}	09/20/2010 11:14:48	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp

device	{P6Z2-Y9AG63OC-8172FYSI}	09/20/2010 11:41:28	HFC0492	PC-4332	Connect
device	{A4O4-D5PP09LN-7950KYWU}	09/20/2010 11:48:14	HFC0492	PC-4332	Disconnect
device	{K7S6-O2GA64OL-8234DFUQ}	09/20/2010 12:03:14	HFC0492	PC-4332	Connect
device	{Z8U3-V2NT42TK-4228TVEU}	09/20/2010 12:56:36	HFC0492	PC-4332	Disconnect
http	{K9V2-C4WS29OH-9713UFTL}	09/20/2010 13:30:07	HFC0492	PC-4332	http://raytheon.com/WboUhagvat343187784.jsp
device	{F9R0-X0BE71CI-3470TCBE}	09/20/2010 13:57:34	HFC0492	PC-4332	Connect
http	{G1J9-B5EG86SP-8135OSPS}	09/20/2010 14:05:57	HFC0492	PC-4332	http://monster.com/WboUhagvat1180707852.html
device	{E0W3-X2MR94HU-6177FVOI}	09/20/2010 14:08:12	HFC0492	PC-4332	Disconnect

device	{L2B1-G1VG50DH-9231IKID}	09/20/2010 14:38:37	HFC0492	PC-4332	Connect
device	{G9H7-D6LL52VG-0119CZCW}	09/20/2010 14:52:42	HFC0492	PC-4332	Disconnect
device	{N2V7-P7FT42HG-8169FGOE}	09/20/2010 15:15:09	HFC0492	PC-4332	Connect
device	{I6V9-A2HM84QM-4512XIFO}	09/20/2010 15:24:38	HFC0492	PC-4332	Disconnect
device	{C4A2-D8SX65UP-5579BPWU}	09/20/2010 15:31:14	HFC0492	PC-4332	Connect
device	{O9N1-D4YV98HX-1579SKIO}	09/20/2010 15:33:50	HFC0492	PC-4332	Disconnect
device	{S5T4-B0IY90JE-5025ELCD}	09/22/2010 07:48:40	HFC0492	PC-4332	Connect
device	{V2L7-Y1ON27QX-0994OUTL}	09/22/2010 08:07:19	HFC0492	PC-4332	Disconnect

device	{D7I1-E1NE26XI-3673NEXO}	09/22/2010 10:21:55	HFC0492	PC-4332	Connect
device	{B6A5-K5FV09LV-7078QGGI}	09/22/2010 11:01:05	HFC0492	PC-4332	Disconnect
device	{N0W6-O3YP70UE-8800LFLI}	09/22/2010 11:24:29	HFC0492	PC-4332	Connect
device	{S8Z1-W2AV92PL-8001KOGV}	09/22/2010 12:06:26	HFC0492	PC-4332	Disconnect
device	{S0S2-V6AF10OZ-9036GCHF}	09/22/2010 12:45:19	HFC0492	PC-4332	Connect
device	{W9O2-Z6HQ90CT-8275YKPT}	09/22/2010 12:49:52	HFC0492	PC-4332	Disconnect
device	{K4V4-W0JS69TR-7106BUOA}	09/22/2010 15:09:11	HFC0492	PC-4332	Connect
device	{H3C7-L8DX74EB-0488UXXE}	09/22/2010 15:16:04	HFC0492	PC-4332	Disconnect

device	{R6U9-G1OZ79DD-4258LDKP}	09/22/2010 15:23:02	HFC0492	PC-4332	Connect
device	{P1O5-Y0DX06GJ-0938AXNT}	09/22/2010 16:56:39	HFC0492	PC-4332	Disconnect
device	{Y8N3-D3OS22NE-8355TEXO}	10/01/2010 08:54	HFC0492	PC-4332	Connect
device	{J8N9-C7ZP26AM-4787GFLF}	10/01/2010 08:55	HFC0492	PC-4332	Disconnect
device	{Q3Q4-A2HD94KR-8676NWPV}	10/01/2010 10:09	HFC0492	PC-4332	Connect
device	{H7B8-N9ZY90KD-7050WUOK}	10/01/2010 10:14	HFC0492	PC-4332	Disconnect
device	{B4I2-D8TE07IX-8497BOOH}	10/01/2010 10:23	HFC0492	PC-4332	Connect
device	{A1L3-D5UA81QJ-9870GUIH}	10/01/2010 10:29	HFC0492	PC-4332	Disconnect

device	{Z8X6-L1AQ21QO-2604RZIB}	10/01/2010 12:47	HFC0492	PC-4332	Connect
device	{N8V4-L5JC15MZ-6033UTIQ}	10/01/2010 12:57	HFC0492	PC-4332	Disconnect
device	{J2T7-O2HQ61IJ-4387HXFQ}	10/01/2010 13:43	HFC0492	PC-4332	Connect
device	{S4M7-Z8KL10CM-5086PGXE}	10/01/2010 14:04	HFC0492	PC-4332	Disconnect
device	{I2U7-L3CH27ZC-3458WQHF}	10/01/2010 14:27	HFC0492	PC-4332	Connect
device	{C5D4-V4IB89BW-5728NJRB}	10/01/2010 14:37	HFC0492	PC-4332	Disconnect
device	{N4X8-C2ID66SV-4982HVII}	10/01/2010 16:32	HFC0492	PC-4332	Connect
device	{D5H7-T0WK13ZD-0717GVCZ}	10/01/2010 16:44	HFC0492	PC-4332	Disconnect

device	{W3M3-R2XF54VM-7966IDJQ}	10/04/2010 08:11	HFC0492	PC-4332	Connect
device	{G2I4-V6SR63DO-3334VOHU}	10/04/2010 08:29	HFC0492	PC-4332	Disconnect
device	{R2Y0-W4UM73DJ-6253IKUE}	10/04/2010 09:14	HFC0492	PC-4332	Connect
device	{L2O4-X8XZ83UP-0711JHYP}	10/04/2010 09:18	HFC0492	PC-4332	Disconnect
device	{O3A3-M4FK37GZ-6171QOFQ}	10/04/2010 10:57	HFC0492	PC-4332	Connect
device	{R4U7-S8OO46MM-7049KTEL}	10/04/2010 11:06	HFC0492	PC-4332	Disconnect
device	{U3B9-R4CL51JB-5747YZZI}	10/04/2010 14:10	HFC0492	PC-4332	Connect
device	{H6N7-Q0KF25SE-7833SVXE}	10/04/2010 14:20	HFC0492	PC-4332	Disconnect

device	{O9N4-E4OE80LC-7033WRBV}	10/04/2010 15:35	HFC0492	PC-4332	Connect
device	{Y2E8-W8YN10YO-5089UTFH}	10/04/2010 15:47	HFC0492	PC-4332	Disconnect
device	{J0V3-R8CY68LQ-0253GGOE}	10/04/2010 16:06	HFC0492	PC-4332	Connect
device	{K4W0-E5LW65EO-5480CXUY}	10/04/2010 16:19	HFC0492	PC-4332	Disconnect
device	{C7K0-A4MX63GD-9855ZIZU}	10/04/2010 17:26	HFC0492	PC-4332	Connect
device	{T1L7-O8AE08SG-6471WAHT}	10/04/2010 17:34	HFC0492	PC-4332	Disconnect
device	{M0S2-H6HW07GE-6899MCSO}	10/05/2010 07:22	HFC0492	PC-4332	Connect
device	{C6D2-Z5AT12YL-5236GCYY}	10/05/2010 07:23	HFC0492	PC-4332	Disconnect

email	{L2W4-R5NX10VO-4144NUVY}	10/05/2010 07:30	HFC0492	PC-4332	Hayfa.Sheila.Donovan@dtaa.com
device	{K4T5-B5WC30PG-8319UCBY}	10/05/2010 07:42	HFC0492	PC-4332	Connect
device	{C9Q0-A6NH65TX-5501COCV}	10/05/2010 07:44	HFC0492	PC-4332	Disconnect
device	{J2F7-Z5YH97RY-8568FTJS}	10/05/2010 08:31	HFC0492	PC-4332	Connect
device	{X2B3-R2GF39HR-6509EHKE}	10/05/2010 08:34	HFC0492	PC-4332	Disconnect
device	{B1U6-T9MI70VG-5128DUTG}	10/05/2010 13:02	HFC0492	PC-4332	Connect
device	{Q0Q4-O5ZM00CW-6023AMJR}	10/05/2010 13:03	HFC0492	PC-4332	Disconnect
device	{H1G2-L4EF86IC-8835ZCWQ}	10/05/2010 13:51	HFC0492	PC-4332	Connect

device	{B5L2-G2JD58OL-4838RDVS}	10/05/2010 13:51	HFC0492	PC-4332	Disconnect
device	{M2M6-G4LZ33HK-5008PZEF}	10/05/2010 16:11	HFC0492	PC-4332	Connect
device	{L5T6-Z5SF41AS-2546XFXC}	10/05/2010 16:13	HFC0492	PC-4332	Disconnect
device	{W9H4-M8IC51PZ-4287TBRA}	10/05/2010 16:56	HFC0492	PC-4332	Connect
device	{Z6F9-J2TJ62IM-5222JNVV}	10/05/2010 17:06	HFC0492	PC-4332	Disconnect
device	{O2J2-A0IV45XO-8617PLYW}	10/07/2010 07:49	HFC0492	PC-4332	Connect
device	{E7X5-F1BS26CK-5323RLXT}	10/07/2010 07:51	HFC0492	PC-4332	Disconnect
device	{X1O3-R7TB62PC-5967NDZD}	10/07/2010 08:06	HFC0492	PC-4332	Connect

device	{E1E4-P9TV84SR-4825QQLF}	10/07/2010 08:11	HFC0492	PC-4332	Disconnect
device	{N1S0-P9SO97AG-4655IUYF}	10/07/2010 10:33	HFC0492	PC-4332	Connect
device	{O3W0-Q4ON65AA-7691MWTF}	10/07/2010 10:33	HFC0492	PC-4332	Disconnect
device	{M9P3-V6BJ97PE-5488XMWT}	10/07/2010 10:34	HFC0492	PC-4332	Connect
device	{F2U3-B5LA01FS-3866ZTEA}	10/07/2010 10:35	HFC0492	PC-4332	Disconnect
device	{Q1I3-A7SK10CK-8976PVNE}	10/07/2010 14:33	HFC0492	PC-4332	Connect
device	{N5D0-A9EE99JJ-9362YKPZ}	10/07/2010 14:35	HFC0492	PC-4332	Disconnect
device	{T1I0-S7HW41YD-6959SVKM}	10/14/2010 08:30:02	HFC0492	PC-4332	Connect

device	{O0U4-O4NX98MU-6439VBWU}	10/14/2010 08:47:07	HFC0492	PC-4332	Disconnect
device	{P0S6-J6IH62PM-5395BTBA}	10/14/2010 10:51:53	HFC0492	PC-4332	Connect
device	{R5E1-M0HJ40QP-3825FBVQ}	10/14/2010 10:53:23	HFC0492	PC-4332	Disconnect
device	{Z5E3-I7SR57NU-3093YQUH}	10/14/2010 12:29:42	HFC0492	PC-4332	Connect
device	{R2O4-V8FG38PQ-9300VKRQ}	10/14/2010 12:51:22	HFC0492	PC-4332	Disconnect
device	{Q4Z9-V0BS99AK-5162ROTN}	10/14/2010 13:29:23	HFC0492	PC-4332	Connect
device	{H3T0-S4WX28YR-2495QLQV}	10/14/2010 14:21:03	HFC0492	PC-4332	Disconnect
device	{U1Q2-C9AO26WU-5810ALQZ}	10/14/2010 15:14:42	HFC0492	PC-4332	Connect

device	{Z7F8-V0XP55TE-0683SOSL}	10/14/2010 15:18:08	HFC0492	PC-4332	Disconnect
device	{B4M0-S2GC15CL-5418RLGZ}	10/14/2010 17:09:26	HFC0492	PC-4332	Connect
device	{B0N6-I2KT24DA-9574IICO}	10/14/2010 17:11:42	HFC0492	PC-4332	Disconnect
logon	{U3J6-G9BV28TG-2769ODFV}	07/01/2010 01:24	CSF0929	PC-4442	Logon
device	{V1J9-P7JR21ZY-0017JSES}	07/01/2010 02:23	CSF0929	PC-4442	Connect
http	{D4G0-L1MD77CY-0097ZJPN}	07/01/2010 03:32	CSF0929	PC-4442	http://wikileaks.org
device	{Q7Q0-F7FL92IO-3645ARQH}	07/01/2010 03:53	CSF0929	PC-4442	Disconnect
device	{O4Y3-X5SF91ZE-7867MGPF}	07/01/2010 04:09	CSF0929	PC-4442	Connect

device	{V6B0-T8YP88MD-6528ZNPI}	07/01/2010 05:50	CSF0929	PC-4442	Disconnect
logon	{Z8H4-H4SF14QV-4937EVPM}	07/01/2010 06:41	CSF0929	PC-4442	Logoff
logon	{A0U8-W0TW50KX-6568YNYN}	07/02/2010 21:54	CSF0929	PC-4442	Logon
device	{F9X7-E1CP85QD-3175HSBP}	07/02/2010 21:57	CSF0929	PC-4442	Connect
device	{V2Q2-P1JW27KX-4514LWVQ}	07/02/2010 22:40	CSF0929	PC-4442	Disconnect
logon	{O3C3-C5YI63QU-1418PESL}	07/03/2010 00:26	CSF0929	PC-4442	Logoff
logon	{D7M2-X8TV94KG-1497LGLH}	07/08/2010 06:14	CSF0929	PC-4442	Logon
device	{O5Y9-E5LL15ZL-7586ILYR}	07/08/2010 06:18	CSF0929	PC-4442	Connect

device	{M0A0-U5AK71ET-3193XUDJ}	07/08/2010 06:46	CSF0929	PC-4442	Disconnect
logon	{A9P2-E5EL77AY-4093VZAE}	07/08/2010 07:12	CSF0929	PC-4442	Logoff
logon	{E9P9-G5RW21EF-9610NUTR}	07/09/2010 00:45	CSF0929	PC-4442	wikileaks
device	{N6J8-T9UV76LX-9928WBKB}	07/09/2010 01:07	CSF0929	PC-4442	Connect
device	{T0R8-Z6OF30MJ-4136OHNN}	07/09/2010 02:51	CSF0929	PC-4442	Logoff
device	{U7H9-L8SI56WF-6850MLWO}	07/09/2010 05:12	CSF0929	PC-4442	Connect
device	{R9C6-W2UF95VS-1863FCTY}	07/09/2010 05:15	CSF0929	PC-4442	Disconnect
logon	{Z8X9-X7QS96ZK-4403NXBG}	07/09/2010 05:17	CSF0929	PC-4442	Logoff

logon	{N5T7-C5QJ36OV-6256GORU}	07/14/2010 01:42:10	CSF0929	PC-4442	Logon
device	{J9P7-W0ZA96NY-4514SEGL}	07/14/2010 02:05:21	CSF0929	PC-4442	Connect
http	{L8D6-L5UN71HC-9011NFYE}	07/14/2010 04:20:11	CSF0929	PC-4442	http://wikileaks.org
device	{K3I9-M0QL80DN-2035LQRB}	07/14/2010 04:26:14	CSF0929	PC-4442	Disconnect
device	{L9W7-M9BF93IP-4747NKYR}	07/14/2010 05:44:39	CSF0929	PC-4442	Connect
device	{A7Q8-D1IE89FH-2009OYOL}	07/14/2010 05:50:31	CSF0929	PC-4442	Disconnect
logon	{Y4H8-O2NK94SR-3611TGTQ}	07/14/2010 06:24:35	CSF0929	PC-4442	Logoff
logon	{A0X2-G8CR06ZA-4524GIQH}	07/16/2010 03:52:16	CSF0929	PC-4442	Logon

device	{B9Y3-U9GL52SD-5897QORJ}	07/16/2010 04:11:05	CSF0929	PC-4442	Connect
http	{D4G5-M1HQ54WN-2859PYMU}	07/16/2010 04:12:16	CSF0929	PC-4442	http://wikileaks.org
device	{I4Y4-C3HG50VT-5601STPG}	07/16/2010 04:22:42	CSF0929	PC-4442	Disconnect
device	{W4O2-V6BQ94KQ-4625UKMC}	07/16/2010 05:28:47	CSF0929	PC-4442	Connect
device	{G9E7-Z4QA33UL-8711SMWL}	07/16/2010 05:43:03	CSF0929	PC-4442	Disconnect
logon	{V0R5-C2NN24NF-3434FXPE}	07/16/2010 06:52:00	CSF0929	PC-4442	Logoff
logon	{G3R8-G0BG91SZ-1111ZKPB}	08/18/2010 21:47:42	ACM2278	PC-8431	Logon
device	{F0N3-C5GS70QE-4575NRWF}	08/18/2010 22:59:20	ACM2278	PC-8431	R:\;R:\52G6677;R:\782bxm8;R:\ACM2278

file	{L8U4-E1KC17HI-2295QTAV}	08/19/2010 01:34:19	ACM2278	PC-8431	R:\52G6677\B7RGYJZC.jpg
file	{Z8S0-I9WK82HT-2702OXHW}	08/19/2010 01:37:20	ACM2278	PC-8431	R:\52G6677\B7RGYJZC.jpg
file	{M3U7-F9ZW51CX-5408MNTW}	08/19/2010 01:38:10	ACM2278	PC-8431	R:\52G6677\7QO6RIRR.txt
file	{I1R8-Z2OT23MQ-3906SEYL}	08/19/2010 01:46:04	ACM2278	PC-8431	R:\ACM2278\QP8YHH52.zip
device	{E7T1-Z4BN74BJ-2108LJAD}	08/19/2010 05:23:05	ACM2278	PC-8431	Disconnect
logon	{C0F6-J3LV50LO-8992SRMS}	08/19/2010 06:10:59	ACM2278	PC-8431	Logoff
logon	{N8G8-A3UJ42OL-2334MCCV}	08/24/2010 01:02:58	ACM2278	PC-8431	Logon
device	{R4V5-J1JK66OF-2014WDEN}	08/24/2010 03:24:16	ACM2278	PC-8431	R:\;R:\52G6677;R:\782bxm8;R:\ACM2278

file	{D2X2-X4AE75SO-9681RGTG}	08/24/2010 03:34:21	ACM2278	PC-8431	R:\52G6677\JMR2V1HC.txt
file	{S3M9-M7FP50TI-7818PRJO}	08/24/2010 03:43:48	ACM2278	PC-8431	R:\ACM2278\JGLCVL46.doc
file	{F9N3-T3ZH14TZ-0696YIFM}	08/24/2010 03:48:51	ACM2278	PC-8431	R:\ACM2278\PXZQFYVF.jpg
device	{X2R4-W6PP65ON-1448BKTE}	08/24/2010 04:15:32	ACM2278	PC-8431	Disconnect
logon	{D3U1-X0MN79ZE-0404OETN}	08/24/2010 04:20:39	ACM2278	PC-8431	Logoff
http	{E9K0-T0KL12CS-9706ONHN}	08/19/2010 01:34:19	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN1528513805.php/B7RGYJZC.jpg

http	{T2S1-D4NO90IT-7131JYCF}	08/19/2010 01:37:20	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN152851380 5.php/B7RGYJZC.jpg
http	{H1P7-O4WO11SJ-6718RXPK}	08/19/2010 01:38:10	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN152851380 5.php/7QO6RIRR.txt
http	{S2J0-W5II68BI-5010XUHO}	08/19/2010 01:46:04	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN152851380

					5.php/QP8YHH52.zip
http	{Q8M9-O4HT66UU-1449YTME}	08/24/2010 03:34:21	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN152851380 5.php/JMR2V1HC.txt
http	{N3Z9-Y2XU99QN-9915ELWN}	08/24/2010 03:43:48	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbel_Nobhg_QGN152851380 5.php/JGLCVL46.doc
http	{R7J1-H9MP31HE-0422QHDW}	08/24/2010 03:48:51	ACM2278	PC-8431	http://wikileaks.org/Julian_Assange/assange/The_Real_Story_About_DTAA/Gur_Erny_Fgbe

					l_Nobhg_QGN N152851380 5.php/PXZQF YVF.jpg

Παράρτημα Γ

Κώδικας «Cyber Risk Assessment Box»

#.....Thesis Title: Cyber Risk Assessment Box.....

#Open University of Cyprus

#MSc Computer and Network Security

#Developer/Author: Georgios Papamichael

#Supervisor: Dr. Stavros Shiaeles

#Date: November 2020

#Version Number: 35

#PROGRAM STARTS#

#import a data analytics toolkit to allow reading and writing of .csv files.

import pandas as pd

def main():

#Definition of Section Weights used in this Dissertation.

#Section 1 = Risk Rating Calculation.

#Section 2 = Behavioural Analysis Calculation.

#Section 3 = Vulnerability Assessment CAlculation.

#The values of the weights represent percentage values.

#Percentage sign, %, is omitted to make calculations easier and faster.

#The weights must add up to 100%.

riskr_weight = 25 #Section 1, Risk Rating Weight in Percentage.

ba_weight = 50 #Section 2, Behavioural Analysis Weight in Percentage.

va_weight = 25 #Section 3, Vulnerability Assessment Weight in Percentage.

#SECTION 1: Risk Rating#

#The first section of the program covers manual user input.
#It is based on the Risk Management Methodology: Weighted Factor Analysis.
#User defines the Weight of each of the 3 selected Citeria: Financial Impact, Legal Impact and Reputational Impact.
#The weight values of these criteria depend on decision-making by the entity and the importance it perceives each criteria to be for the entity.

#Financial Impact Criterion Weight
weight1 = input ("Enter a % value for Financial Impact Criterion Weight between 1%-100%: ") #Program asks for an input value.
while not float(weight1) in range(1,101): #Input value should be in the range 0% - 100%.
** weight1 = input("Please enter an integer % value for Financial Impact Criterion Weight between 1%-100%: ") #In case the value is outside the range, program asks user again for an acceptable value.**
financial_impact = int(weight1) #Input value should is an integer.

#Legal Impact Criterion Weight
weight2 = input ("Enter a % value for Legal Impact Criterion Weight between 1%-100%: ") #Program asks for an input value.
while not float(weight2) in range(0,100): #Input value should be in the range 0% - 100%.
** weight2 = input("Please enter an integer % value for Legal Impact Criterion Weight between 1%-100%: ") #In case the value is outside the range, program asks user again for an acceptable value.**
legal_impact = int(weight2) #Input value should is an integer.

#Reputational Impact Criterion Weight
weight3 = (100 - (financial_impact + legal_impact)) #Automatic calculation of the final criterion, Reputational Impact.
reputational_impact = int(weight3) #The value for the Reputational Impact Criterion is an integer value.

#Checking that the values for the 3 Criteria add up to 100%.
if reputational_impact >= 0:
** print("\n""% value of Reputational Impact Criterion Weight is: " + str(reputational_impact))**

else:
** print("\n""Error! Please re-start the program") #In case the values for the 3 Criteria do not add up to 100%, an Error Message is Displayed.**

#Risk Scale is Introduced where an input integer value is requested in the range 1-5 to represent the Size of Risk an entity or employee presents according to the 3 following factors.
#The factors selected are: Years Worked of the employee or average time per entity, Data Access Level and Profficiency/Knowledge Level.

```
print( "\n")

#Introduction to the Impact of Years Worked Factor on the 3 selected Criteria: Financial, Legal and Reputational.

print("\n""Risk Scale: 1-5. The greater the working period, the lower the value on the risk scale") #The working period of an entity or an employee is inversely proportional to the risk scale input value.

print("\n""In case Total Entity Risk is being Calculated Directly, an Average Value is used") #An average input value is used in case the calculation refers to an entity with a number of employees.

print( "\n")

#Impact of Years Worked Factor on the Financial Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
HF1a = input ("Enter a value for Years Worked Factor with Financial Impact: ")
while not float(HF1a) in range(1,6):
  HF1a = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF1_rating1 = int(HF1a)

#Impact of Years Worked Factor on the Legal Criterion.
#Range = 1-5.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
HF1b = input ("Enter a value for Years Worked Factor with Legal Impact: ")
while not float(HF1b) in range(1,6):
  HF1b = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF1_rating2 = int(HF1b)

#Impact of Years Worked Factor on the Reputational Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively Many Years Worked in the Company = 1.
#Minimum value for Relatively Many Years Worked in the Company = 5.
#HF stands for Human Factor.
```

```
HF1c = input ("Enter a value for Years Worked Factor with Reputational Impact: ")
while not float(HF1c) in range(1,6):
  HF1c = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF1_rating3 = int(HF1c)

print( "\n")

#Introduction to the Impact of Data Access Level Factor on the 3 selected Criteria: Financial, Legal and Reputational.

print("\n""Risk Scale: 1-5. The greater the Data Access Level, the higher the value on the risk scale")

print("\n""In case Total Entity Risk is being Calculated Directly, an Average Value is used")

print( "\n")

#Impact of Data Access Level Factor on the Financial Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Data Access Level = 5.
#Minimum value for Relatively Low Data Access Level = 1.
#HF stands for Human Factor.
HF2a = input ("Enter a value for Data Access Level Factor with Financial Impact: ")
while not float(HF2a) in range(1,6):
  HF2a = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF2_rating1  = int(HF2a)

#Impact of Data Access Level Factor on the Legal Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Data Access Level = 5.
#Minimum value for Relatively Low Data Access Level = 1.
#HF stands for Human Factor.
HF2b = input ("Enter a value for Data Access Level Factor with Legal Impact: ")
while not float(HF2b) in range(1,6):
  HF2b = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF2_rating2  = int(HF2b)

#Impact of Data Access Level Factor on the Reputational Criterion.
```

```
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Data Access Level = 5.
#Minimum value for Relatively Low Data Access Level = 1.
#HF stands for Human Factor.
HF2c = input ("Enter a value for Data Access Level Factor with Reputational Impact: ")
while not float(HF2c) in range(1,6):
  HF2c = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not integer or outside the range.
HF2_rating3  = int(HF2c)

print( "\n")

#Introduction to the Impact of Profficiency/Knowledge Level Factor on the 3 selected Criteria: Financial, Legal and Reputational.

print("\n""Risk Scale: 1-5. The greater the Profficiency/Knowledge Level, the higher the value on the risk scale")

print("\n""In case Total Entity Risk is being Calculated Directly, an Average Value is used")

print( "\n")

#Impact of Profficiency/Knowledge Level Factor on the Financial Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Profficiency/Knowledge Level = 5.
#Minimum value for Relatively Low Profficiency/Knowledge Level = 1.
#HF stands for Human Factor.
HF3a = input ("Enter a value for Profficiency/Knowledge Level Factor with Financial Impact: ")
while not float(HF3a) in range(1,6):
  HF3a = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF3_rating1 = int(HF3a)

#Impact of Profficiency/Knowledge Level Factor on the Legal Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Profficiency/Knowledge Level = 5.
#Minimum value for Relatively Low Profficiency/Knowledge Level = 1.
#HF stands for Human Factor.
```

```
HF3b = input ("Enter a value for Profficiency/Knowledge Level Factor with Legal Impact: ")
while not float(HF3b) in range(1,6):
  HF3b = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF3_rating2 = int(HF3b)

#Impact of Profficiency/Knowledge Level Factor on the Reputational Criterion.
#Range = 1-5.
#Only Integer Values are Accepted.
#Maximum value for Relatively High Profficiency/Knowledge Level = 5.
#Minimum value for Relatively Low Profficiency/Knowledge Level = 1.
#HF stands for Human Factor.
HF3c = input ("Enter a value for Profficiency/Knowledge Level Factor with Reputational Impact: ")
while not float(HF3c) in range(1,6):
  HF3c = input("Please enter an integer value between 1-5: ") #Error Message displayed in case the user input is either not an integer value nor insde the range.
HF3_rating3 = int(HF3c)

#Risk Rating Calculation based on the user input values regarding Criteria Weights and Impact Factors.
#Mathematical multiplication is being carried out between the above human factors and the criteria weights.
risk_HF1 = (HF1_rating1*(financial_impact/100)) + (HF1_rating2*(legal_impact/100)) + (HF1_rating3*(reputational_impact/100))
risk_HF2 = (HF2_rating1*(financial_impact/100)) + (HF2_rating2*(legal_impact/100)) + (HF2_rating3*(reputational_impact/100))
risk_HF3 = (HF3_rating1*(financial_impact/100)) + (HF3_rating2*(legal_impact/100)) + (HF3_rating3*(reputational_impact/100))

#Mathematical addition provides a sum of the risk of the above human factors.
#The result is named as risk rating.
risk_rating = risk_HF1 + risk_HF2 + risk_HF3

print("\n")

#Value of Risk Rating for Section 1.

print("\n""Value for Risk Rating: ")
print(risk_rating)

#Value of Risk Rating for Section 1 in Percentage, taking into account that maximum risk rating value is equal to 15.

risk_rating_perc = (risk_rating*riskr_weight)/15
```

```
print("\n")

print("Risk Rating in %: " + str(risk_rating_perc))

print("\n")
```

#SECTION 2: Behavioural Analysis#

```
print("Insider Activity of Behavioural Log Analysis: ")
```

#High Risk Activity of Behavioural Analysis.

#The program reads the report containing the activity of users.

```
df = pd.read_csv("totalentitylogs1.csv")
```

#Keywords were selected to be identified in the Behavioural Analysis procedure, by reading the activity report.
#In the instance that a keyword is being matched in the activity report, then the numerical value 1 replaces the particular word in the report.
#The remaining words in the activity report that are not matched, are replaced with the numerical value 0.

```
df[df.Activity.str.contains('wikileaks', na=False) | df.Activity.str.contains('keylogger', na=False) |
df.Activity.str.contains('Keylogger', na=False) ] = 1
df.loc[df["Activity"] != 1, "Activity" ] = 0
```

#New report is being generated, named as High Risk report, which only contains the values of 1 and 0 that have followed the above procedure.

```
df.to_csv("HighRisk.csv", index=False)
```

#The program now reads the Activity column of the newly generated High Risk report.
#The numerical value 1 is an indication of a high risk incident.

```
high_risk_activity_values = pd.read_csv("HighRisk.csv", usecols = ["Activity"])
print("\n", high_risk_activity_values)
```

#The program sums up the numerical values in the Activity column and prints out the result.
#The result represents a total idication of High Risk User Activity.

```
print("\n""Total Indications from High Risk User Activity: ")
print(high_risk_activity_values["Activity"].sum())
```

#Medium Risk Activity of Behavioural Analysis.

#The program reads the report containing the activity of users.

```
df = pd.read_csv("totalentitylogs1.csv")
```

#Keywords were selected to be identified in the Behavioural Analysis procedure, by reading the activity report.
#In the instance that a keyword is being matched in the activity report, then the numerical value 1 replaces the particular word in the report.
#The remaining words in the activity report that are not matched, are replaced with the numerical value 0.

```
df[df.Activity.str.contains('monster', na=False) | df.Activity.str.contains('jobhunter', na=False) |
df.Activity.str.contains('careerbuilder', na=False)] = 1
df.loc[df["Activity"] != 1, "Activity" ] = 0
```

#New report is being generated, named as Medium Risk report, which only contains the values of 1 and 0 that have followed the above procedure.

```
df.to_csv("MediumRisk.csv", index=False)
```

#The program now reads the Activity column of the newly generated Medium Risk report.
#The numerical value 1 is an indication of a medium risk incident.

```
medium_risk_activity_values = pd.read_csv("MediumRisk.csv", usecols = ["Activity"])
print("\n", medium_risk_activity_values)
```

#The program sums up the numerical values in the Activity column and prints out the result.
#The result represents a total idication of Medium Risk User Activity.

```
print("\n""Total Indications from Medium Risk User Activity: ")
print(medium_risk_activity_values["Activity"].sum())
```

#Low Risk Activity of Behavioural Analysis.

#The program reads the report containing the activity of users.

```
df = pd.read_csv("totalentitylogs1.csv")
```

#Keywords were selected to be identified in the Behavioural Analysis procedure, by reading the activity report.
#In the instance that a keyword is being matched in the activity report, then the numerical value 1 replaces the particular word in the report.
#The remaining words in the activity report that are not matched, are replaced with the numerical value 0.

```
df[df.Activity.str.contains('Logoff', na=False)] = 1
df.loc[df["Activity"] != 1, "Activity" ] = 0
```

#New report is being generated, named as Low Risk report, which only contains the values of 1 and 0 that have followed the above procedure.

```
df.to_csv("LowRisk.csv", index=False)

#The program now reads the Activity column of the newly generated Low Risk report.
#The numerical value 1 is an indication of a low risk incident.
low_risk_activity_values = pd.read_csv("LowRisk.csv", usecols = ["Activity"])
print("\n", low_risk_activity_values)

#The program sums up the numerical values in the Activity column and prints out the result.
#The result represents a total idication of Medium Risk User Activity.
print("\n""Total Indications from Low Risk User Activity: ")
print(low_risk_activity_values["Activity"].sum())


#Behavioural Activity Weight.

#In this part, a weight value is assigned to every high, medium or low incident.
#The particular weight values emphasize the degree of importance that each category of incident represents.
BA_weight_high = 5
BA_weight_medium = 2
BA_weight_low = 1

#Behavioural activity is being calculated by the mathematical addition of the total high, medium and low incidents, taking into account the above weight values.
Behavioural_Activity =
(high_risk_activity_values["Activity"].sum()*BA_weight_high)+(medium_risk_activity_values["Activity"].sum()*
BA_weight_medium)+(low_risk_activity_values["Activity"].sum()*BA_weight_low)

#The result of Behavioural Activity is printed out.
print("\n""Total Behavioural Activity Value: " + str(Behavioural_Activity))

#Policy Modes.
#Policy Modes are used to indicate the level of security strictness when the behavioural analysis calculation is being carried out.

#Strict Mode implies that the Percentage of Risk Calculation by Behavioural Analysis will be at a higher value.
#The base value used for the risk calculation in Behavioural Analysis in percentage is 10.

#Default Mode implies that the Percentage of Risk Calculation by Behavioural Analysis will be at a moderate value.
#The base value used for the risk calculation in Behavioural Analysis in percentage is 40.

#Light Mode implies that the Percentage of Risk Calculation by Behavioural Analysis will be at a lower value.
```

```
#The base value used for the risk calculation in Behavioural Analysis in percentage is 80.

#strict_mode = 10
default_mode = 40
#light_mode = 80

Policy_Level = default_mode

#Calculation of Behavioural Analysis Value in percentage.
#Behavioural Activity value is multiplied by the Behavioural Analysis Weight value which is then divided by the selected policy level value.
BA_perc_calc = (Behavioural_Activity*ba_weight)/Policy_Level

#An if statement is used in case the Behavioural Activity result exceeds the Behavioural Activity percentage Weight value set in the beggining of the program.
#If the result is greater than or equal to the behavioural Activity percentage Weight value, then the maximum percentage value is given out which is equal to the ba_weight.
if BA_perc_calc >= ba_weight:
  BA_perc = ba_weight

#Otherwise, the Behavioural Activity result is given out as the calculated percentage value.
else:
  BA_perc = BA_perc_calc

#The result of Behavioural Analysis value in percentage is printed out.
print("\n""Total Behavioural Analysis Value in %: " + str(BA_perc))

print("\n")

#SECTION 3: Vulnerability Assessment#

#The program uses the vulnerability assessment report generated by the OpenVAS tool.
#The program reads the CVSS column of the report and prints out the CVSS values.
print("CVSS Records of Vulnerability Assessment Scanning Report: ")
cvss_values = pd.read_csv("report.csv", usecols = ["CVSS"])
print("\n", cvss_values)

#A mean value of the CVSS values is being calculated which represents the average severity of the security vulnerabilites identified by the OpenVAS.
print("\n""Average Value from CVSS Records: ")
print(cvss_values["CVSS"].mean())
```

```
cvss_average = cvss_values["CVSS"].mean()

#The maximum CVSS value is 10, thus the base value used in calculating the average cvss value in percentage is 10.
#The average CVSS value is being multiplied by the vulnerability assessment weight set in the beggining of the program.
cvss_average_perc = (cvss_average*va_weight)/10

#The average CVSS value in percentage is printed out.
print("\n""% Value for CVSS Records: ")
print(cvss_average_perc)

#Calculation of the Total Risk#

#The Total Risk, named as Risk in the program, is being calculated by the mathematical addition of the percentage values of Risk Rating, Behavioural Analysis and CVSS Average.
risk = risk_rating_perc + BA_perc + cvss_average_perc
print("\n""Risk in %: " + str(risk))

print("\n""END")


main()

#PROGRAM ENDS#
```