# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

***Ασφάλεια Υπολογιστών και Δικτύων***


## Μεταπτυχιακή Διατριβή

# Dias: A Dynamic Cyber Range Scenario Generator And Visualization Tool


**Σάββας Θεοδούλου**

**Επιβλέπουσα Καθηγήτρια**
**Αδαμαντίνη Περατικού**



**Μάιος 2021**

# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

***Ασφάλεια Υπολογιστών και Δικτύων***


# Μεταπτυχιακή Διατριβή

## Dias: A Dynamic Cyber Range Scenario Generator And Visualization Tool


**Σάββας Θεοδούλου**

**Επιβλέπουσα Καθηγήτρια**
**Αδαμαντίνη Περατικού**



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.

**Μάιος 2021**

# Περίληψη

Η διατριβή επικεντρώνεται κυρίως στη χρήση των Ψηφιακών Πεδίων Βολής ως μέσο διερεύνησης των κυβερνοεπιθέσεων και εκπαίδευσης του προσωπικού που ασχολείται με την ασφάλεια πληροφοριών και πληροφοριακών συστημάτων. Επιδιωκόμενο αποτέλεσμα είναι η δημιουργία ενός εύχρηστου λειτουργικού εργαλείου βασισμένο σε ελεύθερο λογισμικό και λογισμικό ανοικτού κώδικα που να επιτρέπει την παραμετροποίηση και την προσομοίωση υποδομών πληροφοριακών συστημάτων και τη διεξαγωγή επιθετικών και αμυντικών διεργασιών για ερευνητικούς σκοπούς αλλά και για ρεαλιστική εκπαίδευση στον εντοπισμό και αντιμετώπιση πραγματικών περιστατικών.

Αρχικά παρουσιάζονται σημαντικά ερευνητικά προγράμματα που αφορούν τις κακόβουλες επιθέσεις και την προσομοίωση τους όπως επίσης και υφιστάμενα εργαλεία εκτέλεσης αυτοματοποιημένων επιθέσεων. Ακολούθως γίνεται μια εισαγωγή στα Ψηφιακά Πεδία Βολής και τις δυνατότητες τους και στη συνέχεια αφού γίνει μια αναφορά στο μοντέλο του κύκλου ζωής του λογισμικού, αναλύεται η υλοποίηση της παρούσας διατριβής.

Στη συνέχεια αναλύεται η ορολογία που χρησιμοποιείται στην παρούσα υλοποίηση και παρουσιάζονται η υφιστάμενη υποδομή που χρησιμοποιήθηκε, οι βασικές βιβλιοθήκες κώδικα, η δομή της Βάσης Δεδομένων, τα Δικαιώματα των Χρηστών της πλατφόρμας και η υλοποίηση των διασυνδέσεων και του τρόπου επικοινωνίας μεταξύ των διαφορετικών υποσυστημάτων που αποτελούν την πλατφόρμα στο σύνολο της.

Ακολουθεί η επεξήγηση των βασικότερων τμημάτων κώδικα και χαρακτηριστικών των 4 εφαρμογών που αναπτύχθηκαν για την δημιουργία της πλατφόρμας και στη συνέχεια παρουσιάζονται οι προϋποθέσεις για την πλήρη λειτουργία της υλοποίηση και τα αποτελέσματα από τον πειραματικό έλεγχο που εκτελέστηκε.

Η διατριβή ολοκληρώνεται με την αξιολόγηση της υλοποίησης λαμβάνοντας υπόψη τα ερωτήματα που τέθηκαν στο 1ο κεφάλαιο και προτείνονται μελλοντικές κατευθύνσεις για περαιτέρω διερεύνηση και εξέλιξη της πλατφόρμας που δημιουργήθηκε.

# Summary

The dissertation focuses mainly on the use of Cyber Ranges as a tool for researching malicious actions and for performing realistic training. The aim is to develop a user friendly platform based on existing free and open source solutions with the ability to simulate and interact with different topologies.

This thesis begins with a detailed bibliographic review of cyber-attacks and their automation followed by an introduction to Cyber Ranges and their most important characteristics. Moving towards the implementation part, a short overview about the software development cycle and some basic terms will help by building common ground for the upcoming solution.

What follows next is a detailed description of the existing infrastructure, the programming frameworks and libraries chosen for the implementation, the structure of the database and users' permissions as well as how the different entities of the platform interact with each other.

The above preparation leads to the presentation of the most significant pieces of code of the 4 different applications which were developed for the current implementation and the minimum requirements for a full operational platform.

Concluding the research an evaluation is carried out followed by suggestions for future works and further research.

# Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τη σύζυγο μου για την αμέριστη υποστήριξη που μου παρείχε κατά τη διάρκεια της παρακολούθησης του Μεταπτυχιακού αυτού προγράμματος.

Θα ήθελα επίσης να ευχαριστήσω τους μικρούς Αντρέα και Ελεάνα για την κατανόηση και την αποδοχή της ανταλλαγής του χρόνου παιχνιδιού με χρόνο μελέτης ώστε να καταστεί εφικτή η ολοκλήρωση αυτού προγράμματος.

Κλείνοντας θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια Αδαμαντίνη Περατικού και τον καθηγητή Σταύρο Σταύρου, οι οποίοι με κατεύθυναν και με βοήθησαν στη σωστή προσέγγιση του θέματος και τη διεξαγωγή της έρευνας. Εκφράζω την ευγνωμοσύνη μου για τις υποδείξεις και τις πολύτιμες συμβουλές τους οι οποίες υπήρξαν καταλυτικές για την δημιουργία της πλατφόρμας Dias.

# Περιεχόμενα

# Παραρτήματα

# Πίνακας Εικόνων

# Ακρωνύμια

| | |
|---|---|
| ΒΔ | Βάση Δεδομένων |
| ΕΕ | Ευρωπαϊκή Ένωση |
| ΕΠΜ | Εικονικό Πεδίο Μάχης |
| ΕΣ | Εικονικό Σενάριο |
| ΛΣ | Λειτουργικό Σύστημα |
| ΠΕ | Πρότυπο Επίθεσης |
| ΣΔΒΔ | Σύστημα Διαχείρισης Βάσης Δεδομένων |
| ΨΠΒ | Ψηφιακό Πεδίο Βολής |

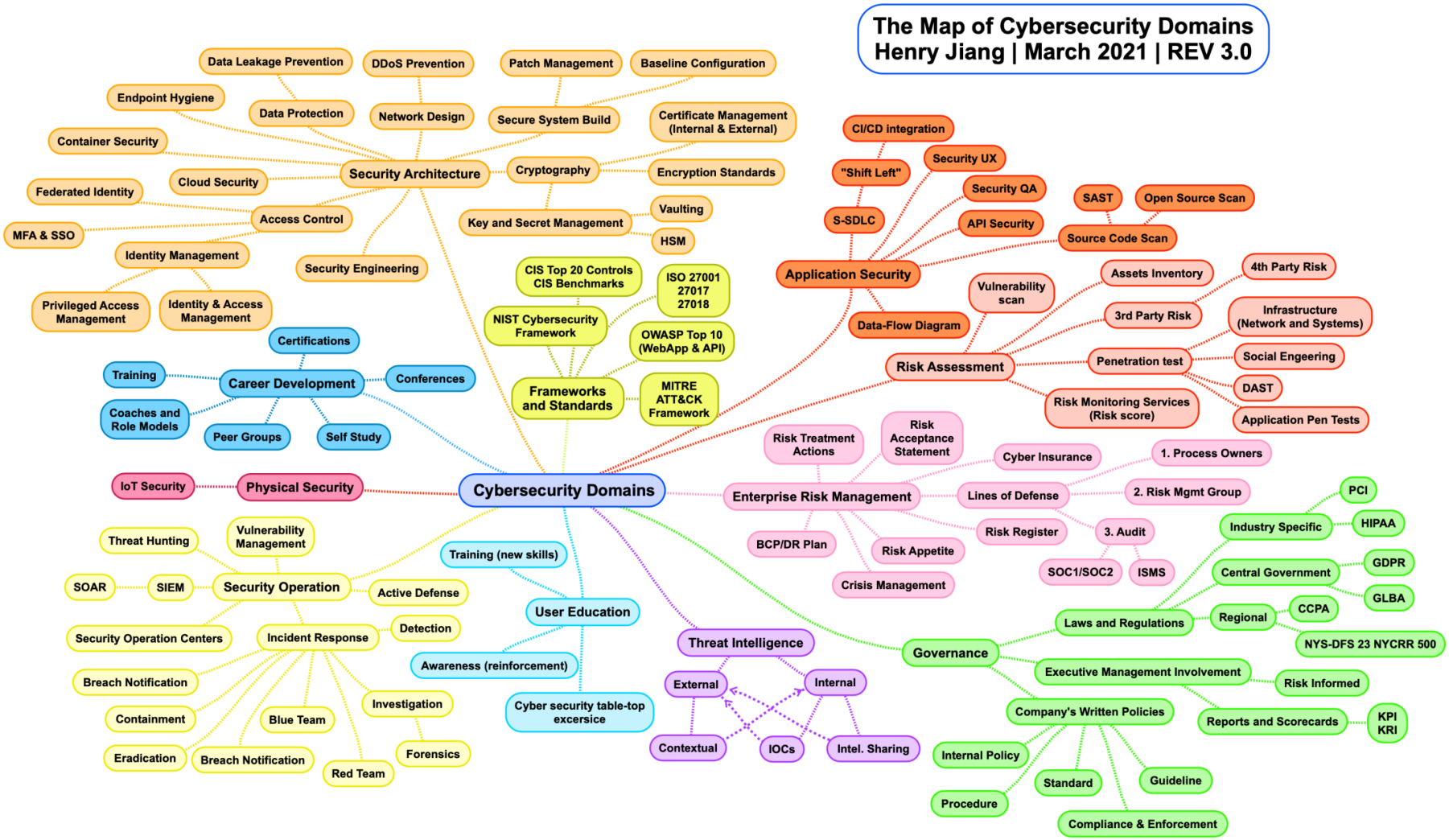
| | |
|---|---|
| ATT&CK | Adversarial Tactics Techniques and Common Knowledge |
| C2 | Command and Control |
| CMS | Content Management System |
| CVE | Common Vulnerabilities and Exposures |
| DoS | Denial of Service |
| ECSO | European Cyber Security Organization |
| HTML | Hypertext Markup Language |
| ICT | Information and Communications Technology |
| IDS | Intrusion Detection System |
| IoC | Indicators of Compromise |
| IPS | Intrusion Prevention System |
| LDAP | Lightweight Directory Access Protocol |
| NIST | National Institute of Standards and Technology |
| OSINT | Open Source Intelligence |
| POS | Point Of Sale |
| SCADA | Supervisory control and data acquisition |
| TCP | Transmission Control Protocol |
| TTP | Tactics Techniques, Procedures |
| UI | User Interface |
| UX | User Experience |

# Κεφάλαιο 1

# Εισαγωγή

Στον 21ο αιώνα που διανύουμε ή διατήρηση της ασφάλειας των πληροφοριακών συστημάτων, αποτελεί ένα από τα σημαντικότερα προβλήματα τόσο σε διεθνή όσο και σε εταιρικό επίπεδο. Από την καθιέρωση του κυβερνοχώρου ως το 5ο πεδίο επιχειρήσεων των πολεμικών συρράξεων και την διερεύνηση του πρώτου θανάτου [1] που πιθανόν οφείλεται σε κυβερνοεπίθεση μέχρι την απώλεια πολλών εκατομμυρίων ευρώ και την αδυναμία παροχής υπηρεσιών, οι ειδικοί του τομέα βρίσκονται σε μια διαρκή προσπάθεια για τον εντοπισμό του καλύτερου τρόπου αντιμετώπισης κάθε είδους απειλής που αφορά τις πληροφορίες και τα πληροφοριακά συστήματα.

Σε ένα διαρκώς μεταβαλλόμενο περιβάλλον, με εξελίξεις και νέες τεχνολογίες να εμφανίζονται καθημερινά η κυβερνοασφάλεια μπορεί να παρομοιωθεί ώς ένα αχανές σύμπαν. Χαρακτηριστική είναι η απεικόνιση του ερευνητή Henry Jiang με τα πεδία της κυβερνοασφάλειας που δημοσίευσε τον Μάρτιο του 2021 (3η ανανεωμένη επανέκδοση) και φαίνεται στην Εικόνα 1 που ακολουθεί. Επί της επικρατούσας κατάστασης, σχετική είναι και η αναφορά M-Trends 2020 [2] της εταιρείας Fireeye, που παρουσιάζει τις τάσεις και τα χαρακτηριστικά που εντοπίστηκαν στις κακόβουλες επιθέσεις που διαδραματίστηκαν μεταξύ 1ης Οκτωβρίου 2018 και 30 Σεπτεμβρίου 2019. Στη συγκεκριμένη αναφορά ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι το 41% των επιθέσεων κακόβουλου λογισμικού (malware) που χρησιμοποιήθηκε την υπόψη περίοδο ήταν εντελώς άγνωστες, επιβεβαιώνοντας την διαρκή εξέλιξη των επιτιθέμενων. Ένα επίσης σημαντικό στατιστικό που αναφέρεται είναι η μείωση του μέσου χρόνου εντοπισμού επιθέσεων από 78 μέρες το 2018 σε 56 το 2019, δείχνοντας ότι οι εταιρείες και οι οργανισμοί αντιλαμβάνονται το μέγεθος του κινδύνου και προετοιμάζονται καλύτερα.




**Εικόνα 1.** Τα πεδία της Κυβερνοάμυνας

Έπειτα από αρκετά χρόνια μελέτης και διερεύνησης του τρόπου δράσης των επιτιθέμενων έχουν προταθεί διάφορες μεθοδολογίες για την ταξινόμηση αλλά και το διαχωρισμό των επιθέσεων σε επί μέρους τμήματα. Το σύνολο των ενεργειών μιας ολοκληρωμένης επίθεσης διαφέρει σε αριθμό και περιεχόμενο από εταιρεία σε εταιρεία ή οργανισμό. Δύο από τις δημοφιλέστερες προσεγγίσεις επί του θέματος αποτελούν το Cyber Kill Chain της εταιρείας Lockheed-Martin και το ATT&CK framework του οργανισμού MITRE. Το όφελος από την ανάλυση των επιθέσεων σε μικρότερες συνιστώσες είναι η πληρέστερη μελέτη και η ανάπτυξη αποτελεσματικότερων εργαλείων και μηχανισμών για τον έγκαιρο εντοπισμό και αντιμετώπιση μελλοντικών επιθέσεων.

Αναλύοντας λοιπόν το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων, μπορούν να εξαχθούν κάποιες κρίσιμες ερωτήσεις, τις οποίες καλείται να απαντήσει ο κάθε υπεύθυνος ασφάλειας πληροφοριακών συστημάτων:

- Σε περίπτωση εκδήλωσης μιας επίθεσης, θα ανιχνευτεί από τα υφιστάμενα συστήματα;
- Μετά από πόσο περίπου χρόνο αναμένεται να γίνει η ανίχνευση;
- Σε ποιο εύρος της υποδομής εκτιμάται ότι θα αποκτηθεί πρόσβαση από τον/τους επιτιθέμενο/ους;
- Με ποιους τρόπους μπορούν να βελτιωθούν ο εντοπισμός και η αποτροπή των κακόβουλων χρηστών και ενεργειών;
- Αναμένεται πρόκληση ζημιών; Αν ναι πιο είναι το εκτιμώμενο εύρος;
- Πώς και πότε θα εφαρμοστούν οι διαδικασίες αντιμετώπισης / επιχειρησιακής συνέχειας;

Κατά διαστήματα πολλοί ερευνητές, εταιρείες και οργανισμοί που ασχολούνται με την ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων έχουν προσπαθήσει να προσομοιώσουν τον τρόπο εκτέλεσης διαφόρων τύπων επιθέσεων ή ακόμα και τον τρόπο δράσης ολόκληρων ομάδων κακόβουλων χρηστών σε μια προσπάθεια εξεύρεσης απαντήσεων στα πιο πάνω ερωτήματα. Κυριότερο συστατικό αυτών των προσομοιώσεων αποτελούν τα αποκαλούμενα «Attack Scripts» ή «Red Team Attack Scripts» τα οποία όταν εκτελεστούν εκδηλώνουν κάποια ενέργεια ή ένα σύνολο ενεργειών οι οποίες συμβάλλουν στην υλοποίηση του στόχου του επιτιθέμενου. Η

χρήση των προσομοιώσεων αποτελεί σημαντική βοήθεια στην κατανόηση των μεθόδων, των τακτικών και των τεχνικών που χρησιμοποιούν οι επιτιθέμενοι καθώς και τον τρόπο χειρισμού των διάφορων μέσων και εργαλείων που διαθέτουν. Ιδιαίτερο ενδιαφέρον παρουσιάζει επίσης η χρήση των προσομοιώσεων για τον έλεγχο της αποτελεσματικότητας των υφιστάμενων λύσεων προστασίας, των διαδικασιών ανάγκης και των δυνατοτήτων αντίδρασης μιας εταιρείας ή ενός οργανισμού ή για την εκπαίδευση του προσωπικού σε θέματα ασφαλείας. Ως επιβεβαίωση της αυξανόμενης ζήτησης που υπάρχει στο συγκεκριμένο τομέα, με μια σύντομη αναζήτηση στο διαδίκτυο μπορεί να εντοπιστεί ένας μεγάλος αριθμός από εταιρείες με υπηρεσίες και προϊόντα που αφορούν την προσομοίωση κακόβουλων επιθέσεων αλλά και υλοποιήσεις Ελεύθερου Λογισμικού ή Λογισμικού Ανοικτού Κώδικα όπως τα Adversary Emulation Library, Caldera [3] και Infection Monkey.

Μια εξίσου δημοφιλής προσέγγιση των κακόβουλων ενεργειών γίνεται με την χρήση Ψηφιακών Πεδίων Βολής (Cyber Ranges). Τα Ψηφιακά Πεδία Βολής είναι εικονικά περιβάλλοντα τα οποία μπορούν να χρησιμοποιηθούν ως χαμηλού κόστους λύσεις για την προσομοίωση πληροφοριακών συστημάτων. Λόγω της φύσης τους τα ΨΠΒ παρέχουν ιδιαίτερη ευελιξία και μπορούν συνήθως να προσομοιώσουν μεγάλους αριθμούς διαφορετικών συσκευών και υποδομών, με αποτέλεσμα να έχουν μια πληθώρα εφαρμογών στον τομέα της ασφάλειας πληροφοριών. Στις πιο συχνές χρήσεις των ΨΠΒ περιλαμβάνονται η προσομοίωση ενός αντίστοιχου πραγματικού περιβάλλοντος για σκοπούς ελέγχων των μηχανισμών και των διαδικασιών ασφαλείας και η χρήση τους για την εκπαίδευση του προσωπικού σε επιθετικές και αμυντικές πρακτικές που αφορούν την ασφάλεια πληροφοριών. Τα κυριότερα πλεονεκτήματα της χρήσης των ΨΠΒ είναι η εξοικείωση του προσωπικού με την χρήση των μέσων, των εργαλείων και των διαδικασιών, η ευκολία με την οποία μπορεί να τροποποιηθεί η υποδομή και ο μικρός αντίκτυπος που έχει η εκτέλεση λανθασμένων χειρισμών σε αντίθεση με το πραγματικό περιβάλλον. Τα ΨΠΒ αν και δεν αποτελούν πρόσφατη τεχνολογία, εντούτοις η αύξηση της υπολογιστικής ισχύς, οι νέες δυνατότητες virtualization και cloud computing, και η ραγδαία αύξηση των επιθέσεων έχουν συμβάλει στο να αποκτήσουν μια σημαντική ώθηση μετατρέποντας τα σε μια νέα τάση. Μεταξύ των παροχών υπηρεσιών ΨΠΒ περιλαμβάνονται αμυντικές βιομηχανίες (Raytheon, Thales, IABG, Northrop Grumman ), πολυεθνικές εταιρείες (Deloitte, KPMG), ερευνητικά ιδρύματα, ενώ ιδιαίτερο ενδιαφέρον έχουν επιδείξει και εθνικές και διεθνής

οντότητες όπως η DARPA με το National Cyber Range, αλλά και η ΕΕ με το KYPO Cyber Range του προγράμματος Concordia Horizon 2020 [4].

Συνδυάζοντας λοιπόν τις Αυτοματοποιημένες Επιθέσεις με τα ΨΠΒ, γίνεται εύκολα αντιληπτό ότι δημιουργείται ένα σύστημα το οποίο μπορεί να βοηθήσει τόσο στην αποτροπή όσο και στον καλύτερο χειρισμό και αντιμετώπιση ανεπιθύμητων καταστάσεων που μπορεί να προκύψουν από κακόβουλες ενέργειες ή λάθος χειρισμούς.

## 1.1 Σκοπός

Ο σκοπός της παρούσας διατριβής είναι η δημιουργία ενός εργαλείου εύκολης διαχείρισης ενός Ψηφιακού Πεδίου Βολής με δυνατότητα προσομοίωσης διαφορετικών δικτυακών υποδομών, Εικονικών Πεδίων Μάχης, στα οποία να μπορούν να εκτελεστούν διαφορετικά Σενάρια και Αυτοματοποιημένες Επιθέσεις. Τα Σενάρια θα πρέπει να μπορούν να εκμεταλλευτούν στο έπακρο τις δυνατότητες των εικονικών μηχανημάτων των ΕΚΠ λειτουργώντας είτε πλήρως αυτοματοποιημένα με την χρήση Red Team Attack Scripts, ή με αλληλεπίδραση πραγματικών χρηστών ή συνδυασμό των δύο.

Τα προσδοκώμενα αποτελέσματα είναι η υλοποίηση ενός φιλικού προς τον χρήστη περιβάλλοντος τόσο για την δημιουργία όσο και την παρακολούθηση όλων των επί μέρους τμημάτων της πλατφόρμας, περιλαμβανομένων των ΕΠΜ των Σεναρίων, των Εικονικών Μηχανών και των Αυτοματοποιημένων Επιθέσεων. Το γραφικό περιβάλλον πρέπει να έχει τη δυνατότητα να απεικονίζει την εξέλιξη των Σεναρίων λαμβάνοντας ανατροφοδότηση από τόσο από τις εφαρμογές όσο και από τις ενέργειες των χρηστών που χρησιμοποιούν τα ΕΠΜ ώστε να επιτυγχάνεται η μέγιστη δυνατή επίγνωση της κατάστασης καθ’ όλη τη διάρκεια της εξέλιξης των σεναρίων.

Είναι ιδιαίτερα σημαντικό επίσης, η πλατφόρμα να δομηθεί με τέτοιο τρόπο ώστε να είναι εύκολη η μελλοντική της αναβάθμιση για την προσθήκη νέων χαρακτηριστικών και ενσωμάτωση άλλων τεχνολογιών, όπως για παράδειγμα τα Deep και Machine learning, ώστε να συμβαδίζει με τις εξελίξεις.

## 1.2 Βασικά Ερευνητικά Ερωτήματα

- Είναι δυνατή η δημιουργία ενός εύχρηστου εργαλείου που με την χρήση γραφικού περιβάλλοντος να μπορεί να χρησιμοποιηθεί σαν πλατφόρμα Cyber Range χρησιμοποιώντας ελεύθερο λογισμικό και λογισμικό ανοικτού κώδικα;
- Μπορεί να δημιουργηθεί ένα Εικονικό Κέντρο Ελέγχου το οποίο να παρουσιάζει σε πραγματικό χρόνο την εξέλιξη της εκτέλεσης διαφόρων τύπων επιθέσεων και τα αποτελέσματα τους στο περιβάλλον που εκτελούνται;
- Είναι δυνατή η αυτοματοποίηση της απεικόνισης της κατάστασης των υπηρεσιών και του εξοπλισμού που χρησιμοποιείται στο σενάριο;

## 1.3 Αναγκαιότητα Και Σπουδαιότητα έρευνας

Ο συνδυασμός των αυτοματοποιημένων επιθέσεων με τα Ψηφιακά Πεδία Βολής για τη δημιουργία μιας κοινής πλατφόρμας ενδέχεται να αποτελέσει ένα σημαντικό βήμα για την δημιουργία καλύτερων εργαλείων και πληρέστερων διαδικασιών για τον εντοπισμό και την αντιμετώπιση μελλοντικών κακόβουλων επιθέσεων. Η χρήση αυτού του κοινού περιβάλλοντος για την αυτοματοποίηση και τον συνδυασμό διαφορετικών Attack Scripts παράλληλα με τη δυνατότητα για ταυτόχρονη παρακολούθηση της εξέλιξης των επιθέσεων, αναμένεται να συμβάλει στην ευκολότερη προσομοίωση πραγματικών περιστατικών ελαχιστοποιώντας το κόστος και την προσπάθεια. Με την αξιοποίηση υφιστάμενων μελετών για την προσομοίωση του τρόπου δράσης γνωστών ομάδων κακόβουλων χρηστών, πρόκειται να δημιουργηθεί καλύτερη αντίληψη του τρόπου διαχείρισης των διαφορετικών τύπων επιθέσεων από το προσωπικό αλλά και εντοπισμός πιθανών αδυναμιών ή σημείων τα οποία χρήζουν βελτίωσης. Με αυτό τον τρόπο δημιουργείται ένα πολύ-επίπεδο εργαλείο με υψηλό βαθμό ρεαλισμού το οποίο θα μπορεί να χρησιμοποιηθεί για σκοπούς εκπαίδευσης αλλά και έρευνας στον τομέα της ασφάλειας των πληροφοριών.

# Κεφάλαιο 2

# Βιβλιογραφική Ανασκόπηση

Η μελέτη και η κατανόηση του τρόπου διενέργειας των κακόβουλων επιθέσεων και του τρόπου σκέψης και δράσης αυτών που τις εκτελούν, αποτελούν τους σημαντικότερους παράγοντες για τον εντοπισμό και την αντιμετώπιση τους. Η προσομοίωση της εκτέλεσης κακόβουλων επιθέσεων για σκοπούς ανάλυσης και εξαγωγής συμπερασμάτων για τις κινήσεις των επιτιθέμενων δεν είναι μια καινούρια ιδέα, αλλά κάτι γνωστό εδώ και τουλάχιστον 2 δεκαετές [5]. Πολλοί ερευνητές, οργανισμοί και εταιρείες έχουν ασχοληθεί με την δημιουργία εργαλείων τα οποία προσομοιώνουν ή και αναπαριστούν με αρκετή ακρίβεια μεθόδους που χρησιμοποιούνται για την εκτέλεση κακόβουλων επιθέσεων.

Κυριότερο σημείο αναφοράς, των περισσότερων προσπαθειών αποτελεί το πλαίσιο MITRE ATT&CK [6] το οποίο βασίζεται κυρίως σε πίνακες ανάλυσης των ενεργειών προ και μετά της επίτευξης πρόσβασης σε ένα Πληροφοριακό Σύστημα. Η κατηγοριοποίηση των ενεργειών μπορεί να γίνει αναλόγως της χρήσης τους από συγκεκριμένες κακόβουλες ομάδες [7], βάση λειτουργικών συστημάτων υπολογιστών [8] και κινητών συσκευών ή πλατφόρμων δικτυακών παρόχων [9]. Δυστυχώς όμως, το εύρος των συστημάτων που πρέπει να προστατευτούν είναι τόσο μεγάλο και η εξέλιξη του τομέα των πληροφοριών τόσο ραγδαία που απαιτείται κάτι πιο σύνθετο ή τουλάχιστον ένας συνδυασμός από περισσότερες από μία υλοποιήσεις [10].

Από το 2015 [11] υπάρχουν αναφορές για την ανάγκη δημιουργίας αυτοματοποιημένων ελέγχων διείσδυσης σε πληροφοριακά συστήματα τα οποία να προσομοιάζουν τη δραστηριότητα και τις κινήσεις των επιτιθέμενων στο σύνολο τους και όχι απλά να εκτελούν μια σειρά προκαθορισμένων βημάτων. Έχει επίσης επισημανθεί [7] ότι είναι πολύ σημαντικό οι αυτοματοποιημένες επιθέσεις να

λαμβάνουν υπόψη όλους τους περιορισμούς που ενδέχεται να αντιμετωπίζει ο επιτιθέμενος. Τις περισσότερες φορές, μια εξωτερική οντότητα διαθέτει πολύ περιορισμένες πληροφορίες σχετικά με την υποδομή και τα διατιθέμενα συστήματα στα οποία επιτίθεται. Για να ξεπεραστεί αυτός ο περιορισμός ο επιτιθέμενος μέσα από ένα δυναμικό πλαίσιο δοκιμής διαφόρων τεχνικών καλείται να αποφύγει τον εντοπισμό και να κατορθώσει να φτάσει στο στόχο του. Επίσης, ένα σύνηθες σφάλμα [9] που παρατηρείτε σε αρκετά συστήματα αυτοματοποιημένων επιθέσεων είναι το ότι βασίζουν τις αποφάσεις τους σε εργαλεία και μεθόδους τα οποία αποδεδειγμένα έχουν περιορισμούς ως προς τις δυνατότητες τους. Δεν είναι βέβαιο ότι ο επιτιθέμενος έχει τα ίδια κριτήρια λήψης αποφάσεων όπως οι ρυθμίσεις της αυτοματοποιημένης επίθεσης, ούτε ότι θα ακολουθήσει το συντομότερο δρόμο για την επίτευξη του στόχου του, ούτε καν για το ποιος είναι ο πραγματικός του στόχος. Όλα αυτά θα πρέπει να λαμβάνονται υπόψη ώστε οι αυτοματοποιημένες επιθέσεις να αντικατοπτρίζουν τις πραγματικές επιθέσεις στο μεγαλύτερο δυνατό βαθμό και να μπορούν να παρουσιάσουν περισσότερα από ένα πιθανά ενδεχόμενα.

Σε αυτό το σημείο γίνεται ήδη αντιληπτό ότι πέρα από το χρόνο, υπεισέρχεται και το κόστος σε πόρους, ώστε να μπορέσει να καλυφθεί το μεγάλο εύρος των μέσων και των πληροφοριών που ο κάθε ειδικός καλείτε να προστατεύσει. Σε μια εποχή όπου όλα μετατρέπονται και παρέχονται ως υπηρεσίες το ίδιο συμβαίνει και με τα πληροφοριακά συστήματα και την ασφάλεια των πληροφοριών, με τα ΨΠΒ να γίνονται όλο και πιο δημοφιλή. Όπως και με την αυτοματοποίηση των επιθέσεων, έτσι και τα ΨΠΒ δεν αποτελούν μια νέα ιδέα, τα προηγούμενα χρόνια όμως οι χρήσεις τους περιορίζονταν κυρίως σε στρατιωτικές και κρατικές υπηρεσίες [12] [13]. Με την αύξηση όμως της επεξεργαστικής ισχύς, των ταχυτήτων του διαδικτύου και την εξέλιξη της τεχνολογίας του νέφους προέκυψε και αυξανόμενη ζήτηση καθιστώντας τα πιο προσιτά σε ένα ευρύτερο κοινό. Η ευελιξία που προσφέρουν τα ΨΠΒ σε σχέση με τις ελάχιστες απαιτήσεις σε χρόνο και προσωπικό για τη διαχείριση τους, παράλληλα με τις αμελητέες επιπτώσεις σε περιπτώσεις λαθών τα έχουν καθιερώσει ως σημαντικά εργαλεία στον τομέα της ασφάλειας πληροφοριών.

Η ανάγκη της χρήσης των ΨΠΒ στην ασφάλεια των πληροφοριών επισημαίνεται από τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ECSO), μέσω έκδοσης [14] αποκλειστικά για τα ΨΠΒ τις χρήσεις και τις δυνατότητες τους τον Μάρτιο του 2020, και τον Μάιο του ίδιου έτους από παρόμοια έκδοση του ινστιτούτου SANS [15].

Περισσότερο εξειδικευμένες δημοσιεύσεις [16], [17] αφορούν την δημιουργία σεναρίων με αυτοματοποιημένες επιθέσεις για την σωστή εκπαίδευση του προσωπικού σε θέματα ασφαλείας ενώ ένα από τα σημαντικότερα θέματα που απασχολεί τους ερευνητές όσο αφορά τα ΨΠΒ είναι η μη ύπαρξη τυποποιημένης κωδικοποίησης [18], [19] για την δημιουργία σεναρίων κάτι το οποίο συχνά δημιουργεί πολλά προβλήματα κατά την προετοιμασία των σεναρίων αλλά και κατά την εκτέλεση τους.

Λαμβάνοντας υπόψη όλα τα ανωτέρω είναι ορατό το ενδιαφέρον που επιδεικνύεται από την ερευνητική κοινότητα σε θέματα προσομοίωσης επιθέσεων με την χρήση αυτοματοποιημένων διαδικασιών αλλά και στην ενσωμάτωση αυτών των διαδικασιών σε ΨΠΒ. Η διαφοροποίηση της παρούσας διατριβής από προηγούμενες έρευνες, αφορά την δημιουργία μιας ενοποιημένης πλατφόρμας η οποία θα μπορεί να συνδυάσει σε μεγάλο βαθμό τις γνώσεις και τις εμπειρίες από τις σημαντικότερες δημοσιεύσεις σε ένα εύχρηστο γραφικό περιβάλλον. Διατηρώντας ως βάση υφιστάμενα υποσυστήματα της υποδομής του πανεπιστημίου, όπως το λογισμικό διαχείρισης εικονικών μηχανών oVirt και η αυθεντικοποίηση με την χρήση LDAP και σε συνδυασμό με λύσεις αυτοματοποιημένων επιθέσεων ανοικτού κώδικα [10], σκοπός της παρούσας διατριβής είναι η δημιουργία ενός εργαλείου το οποίο θα παρέχει στους χρήστες δυνατότητα δημιουργίας, διαχείρισης ή χρήσης των Σεναρίων ανάλογα με τα δικαιώματα τους για εξοικείωση, εκπαίδευση και έρευνα στον τομέα της Ασφάλειας Πληροφοριών.

# Κεφάλαιο 3

# Ορισμοί

Οι ακόλουθοι ορισμοί, αφορούν την κυβερνοασφάλεια και αναφέρονται για την καλύτερη κατανόηση και αντίληψη των κεφαλαίων που θα ακολουθήσουν.

## 3.1 Attack-Scripts

Αν και αποτελούνται από ένα σύνολο εντολών, διαφέρουν από τα κοινά προγράμματα γιατί συνήθως δεν αποθηκεύονται αυτόνομα αλλά αποτελούν “φορτίο” το οποίο ενσωματώνεται σε άλλα αρχεία ή εκτελούνται on the fly από την μνήμη τυχαίας προσπέλασης. Η φύση τους, συνεπάγεται την μη ύπαρξη μεταγλωττιστή για την εκτέλεση τους και οι δημοφιλέστερες γλώσσες που χρησιμοποιούνται είναι η JavaScript, η Visual Basic for Applications (VBA), η Visual Basic Script (VBS) και οι γλώσσες που χρησιμοποιούνται από τις γραμμές εντολών των λειτουργικών (Powershell, Command Prompt, Unix Shells). Η χρήση των Attack Scripts είναι ιδιαίτερα δημοφιλής, γιατί η μη αποθήκευση τους σε συνδυασμό με τις δυνατότητες απόκρυψης τους σε κωδικοποιήσεις τα καθιστούν ιδιαίτερα δυσανάγνωστα, και δύσκολο να εντοπιστούν. Αυτή η μορφή κακόβουλου κώδικα τις περισσότερες φορές προϋποθέτει την εκτέλεση κάποιας ενέργειας από τον χρήστη, όπως για παράδειγμα την εκτέλεση κάποιου άλλου αρχείου, την ενεργοποίηση επιπρόσθετων δυνατοτήτων, όπως για παράδειγμα τα Macros στα αρχεία του Office, την Javascript στους φυλλομετρητές κλπ.

Στη υλοποίηση της παρούσας διατριβής, τα Attack-Scripts που χρησιμοποιούνται είναι κώδικας γραμμένος σε κάποια από τις γλώσσες που υποστηρίζουν οι γραμμές εντολών των λειτουργικών Windows, Linux και Mac OS ο οποίος στη συνέχεια χρησιμοποιείται για την εκδήλωση επιθέσεων.

## 3.2 Cyber-security Teams

Οι Ομάδες Ελέγχου Ασφαλείας (Red Team, Blue Team) αποτελούν μια ολιστική προσέγγιση των μηχανισμών άμυνας μιας εταιρείας ή ενός οργανισμού. Ο συνδυασμός των δύο ομάδων αποτελεί μια πλήρη προσομοίωση του τρόπου εξέλιξης μιας επίθεσης κατά την οποία ελέγχονται όχι μόνο τα συστήματα για ευπάθειες αλλά και οι γνώσεις, η εξοικείωση, οι αντιδράσεις του προσωπικού, όπως επίσης και οι διαδικασίες για αντιμετώπιση κακόβουλων περιστατικών.

### 3.2.1 Blue Team

Η ομάδα, που αποτελείται από το προσωπικό του οργανισμού/εταιρείας το οποίο είναι επιφορτισμένο με την ασφάλεια και τον εντοπισμό μη ομαλών καταστάσεων στο πληροφοριακό σύστημα του οργανισμού/εταιρείας. Η Μπλε ομάδα μετά την αξιολόγηση των κινδύνων των υποσυστημάτων που καλούνται να προστατέψουν, είναι υπεύθυνη για την ρύθμιση των συστημάτων, την εγκατάσταση εργαλείων παρακολούθησης, ελέγχου και ασφαλείας και την δημιουργία της κατάλληλης πολιτικής και διαδικασιών. Για τις Μπλε ομάδες τα πολυτιμότερα εργαλεία συνήθως είναι τα αρχεία καταγραφών και οι εφαρμογές παρακολούθησης-επιτήρησης. Οι Μπλε ομάδες επιδιώκουν την συνεχή βελτίωση της ασφάλειας της εταιρείας/οργανισμού.

### 3.2.2 Red Team

Ομάδα που αποτελείται από το προσωπικό της εταιρείας/οργανισμού ή το οποίο προσλαμβάνεται με σκοπό την προσομοίωση των κινήσεων κακόβουλων χρηστών. Χρησιμοποιούν εργαλεία και μεθόδους όπως ακριβώς και οι επιτιθέμενοι και ο σκοπός τους είναι ο έλεγχος της αποτελεσματικότητας των μέτρων ασφαλείας που διατηρεί η εταιρεία/οργανισμός ή σε περίπτωση άσκησης η αντίπαλη ομάδα. Αν και παρατηρούνται αρκετές ομοιότητες μεταξύ Penetration Testing και Red Teaming, η κυριότερη διαφορά είναι ότι οι ομάδες που εκτελούν Penetration Testing βασίζονται κυρίως σε αναφορές αδυναμιών που προκύπτουν από λογισμικά ελέγχου ευπαθειών, ενώ η συμπεριφορά των κόκκινων ομάδων προσεγγίζει περισσότερο τον τρόπο συμπεριφοράς των κακόβουλων χρηστών. Επίσης είναι σύνηθες τακτική στη Κόκκινες

Ομάδες να ανατίθενται συγκεκριμένοι στόχοι, κάτι που δεν συμβαίνει συνήθως με τα Penetration Tests.

### 3.2.3 Λοιπές Ομάδες

Όταν οι έλεγχοι εκδηλώνονται στα πλαίσια εκπαίδευσης του προσωπικού συνήθως, χρησιμοποιούνται και οι ακόλουθες ομάδες:

#### *3.2.3.1 Grey Team*

Εικονικές μηχανές οι οποίες δεν έχουν κάποιο ρόλο στο σενάριο και μπορεί να χρησιμοποιηθούν για να δημιουργούν συνηθισμένη κίνηση στο δίκτυο.

#### *3.2.3.2 Purple Team*

Αποτελεί συνδυασμό Red Team, και Blue Team. Το προσωπικό της ομάδας καλείται να προστατεύσει κάποιους στόχους ενώ παράλληλα να επιτεθεί σε κάποιους άλλους.

#### *3.2.3.3 Yellow Team*

Η ομάδα που είναι υπεύθυνη για την δημιουργία του Πεδίου Μάχης.

#### *3.2.3.4 White Team*

Η ομάδα που είναι υπεύθυνη για την τήρηση της βαθμολογίας των ομάδων και την επιτήρηση της εκτέλεσης του σεναρίου.

## 3.3 Cyber Range

Τα Ψηφιακά Πεδία Βολής (ΨΠΒ) αποτελούν πλατφόρμες οι οποίες χρησιμοποιούνται για την προσομοίωση υποδομών και δικτύων για ελέγχους ασφαλείας, ελέγχους πειραματικών διατάξεων και εκπαίδευσης του προσωπικού. Με την προσομοίωση του περιβάλλοντος μιας εταιρείας ή ενός οργανισμού σε ένα ΨΠΒ μπορούν να γίνει έλεγχος

των επιπτώσεων που ενδέχεται να προκύψουν μετά την εκδήλωση μιας κακόβουλης ενέργειας/επίθεσης χωρίς να διακινδυνεύεται η επιχειρησιακή συνέχεια ή η πρόκληση ανεπιθύμητων ζημιών. Συχνά επίσης χρησιμοποιούνται για την δοκιμή διαφορετικών διαμορφώσεων των συστημάτων, για την εκπαίδευση του προσωπικού σε θέματα ασφάλειας και για την βελτίωση των διαδικασιών εντοπισμού και αντίδρασης κατά την εκδήλωση επιθέσεων. Χρησιμοποιώντας τα ΨΠΒ το προσωπικό εξοικειώνεται με τα διαθέσιμα συστήματα, μέσα και διαδικασίες και επιτυγχάνεται η δημιουργία καλύτερης αντίληψης και μειωμένων χρόνων αντίδρασης σε περίπτωση ανεπιθύμητων περιστατικών.

## 3.4 Pentest

Τα Penetration Tests είναι διαδικασίες ελέγχου και εντοπισμού ευπαθειών των πληροφοριακών συστημάτων και ελέγχου της επίγνωσης του προσωπικού μιας εταιρείας ή ενός οργανισμού σε θέματα ασφάλειας πληροφοριών. Τις πλείστες φορές, κυρίως σε μικρομεσαίες επιχειρήσεις και οργανισμούς, οι ομάδες ελέγχου δεν αποτελούνται από προσωπικό της εταιρείας αλλά από προσωπικό το οποίο προσλαμβάνεται για αυτό το συγκεκριμένο σκοπό. Τα πλαίσια στα οποία εκτείνεται ο έλεγχος και οι πληροφορίες οι οποίες θα γίνουν γνωστές στην ομάδα ελέγχου καθορίζονται πριν την έναρξη του ελέγχου, ενώ μια ειδική συμφωνία μη αποκάλυψης (Non-Disclosure Agreement) πριν την έναρξη του ελέγχου εξασφαλίζει την διατήρηση της διαρροής πληροφοριών από το προσωπικό που εμπλέκεται με τους ελέγχους . Συνήθως η χρονική διάρκεια περιορίζεται μεταξύ μιας και τριών εβδομάδων.

# Κεφάλαιο 4

# Κακόβουλες Επιθέσεις – (Red Team Attacks)

## 4.1 Ο οργανισμός MITRE

Ο Mitre είναι ένας Αμερικάνικος μη κερδοσκοπικός οργανισμός που εργάζεται προς το δημόσιο συμφέρον με ομοσπονδιακές, πολιτειακές και τοπικές κυβερνήσεις, τη βιομηχανία και τον ακαδημαϊκό χώρο. Μέσα από ομοσπονδιακά χρηματοδοτούμενα κέντρα έρευνας και καινοτομίας (Federally Funded Research and Development Centers) αλλά και ανεξάρτητα ερευνητικά προγράμματα συνεισφέρει στην επιστημονική έρευνα καθώς και στην ανάπτυξη και ενσωμάτωση καινοτόμων συστημάτων και τεχνολογιών. Μεταξύ των τομέων ενασχόλησης των ερευνητικών κέντρων ιδιαίτερο ενδιαφέρον παρουσιάζει το έργο που αφορά την Κυβερνοασφάλεια. Το έργο που έχει να επιδείξει ο Mitre στον συγκεκριμένο τομέα είναι θεμελιώδες και ουσιαστικά αποτελεί τη βάση για μια σειρά από εξελίξεις γύρω από την ασφάλεια των πληροφοριακών συστημάτων. Παρακάτω αναφέρονται ενδεικτικά το Μητρώο Αδυναμιών και Ευπαθειών (Common Vulnerabilities and Exposures - CVE) το πλαίσιο ATT&CK (Adversarial Attacks Techniques & Common Knowledge) και το Adversary Emulation Plan.

### 4.1.1 Μητρώο CVE

Η βάση δεδομένων CVE αποτελεί ένα μητρώο καταχώρησης ευπαθειών και κενών ασφαλείας που εντοπίζονται και αφορούν την κυβερνοασφάλεια. Για κάθε μεμονωμένη ευπάθεια καταχωρείται ένα αναγνωριστικό CVE το οποίο εκτός από το να την χαρακτηρίζει μοναδικά φανερώνει και την χρονιά την οποία καταχωρήθηκε στο

μητρώο. Κάθε ευπάθεια βαθμολογείτε στην κλίμακα από 0 μέχρι 10, με τις κρίσιμες ευπάθειες να είναι αυτές με βαθμολόγηση μεγαλύτερη ή ίση με 9. Το συγκεκριμένο μητρώο βρίσκεται σε ισχύ από το 1999, και ενημερώνεται διαρκώς. Ενδεικτικά τα έτη 2017,2018 και 2019 καταχωρήθηκαν 14714, 15556 και 12174 ευπάθειες αντίστοιχα. Το μητρώο αυτό χρησιμοποιείται από τους ειδικούς σε θέματα ασφαλείας για να τηρούνται ενήμεροι για νέες ευπάθειες που εντοπίζονται αλλά και διερεύνηση υφιστάμενων κενών ασφαλείας και αποτελεί επίσης την βάση της πλειοψηφίας των λογισμικών εντοπισμού και αναφοράς ευπαθειών και κενών ασφαλείας.

### 4.1.2 ATT&CK framework

Το 2010, σε μια προσπάθεια για την ανίχνευση παραβιάσεων πληροφοριακών συστημάτων ξεκίνησε η διερεύνηση της ιδέας του εντοπισμού των κακόβουλων χρηστών από τις ενέργειες που εκτελούν μετά την απόκτηση πρόσβασης σε ένα σύστημα (post compromise). Από τα αποτελέσματα αυτής της πρώτης προσπάθειας, συνδυάζοντας ίχνη από τα τερματικά μηχανήματα και την κίνηση του δικτύου, και διαχωρίζοντας την όλη διαδικασία μετά την απόκτηση πρόσβασης σε επί μέρους τμήματα, το 2013 δημιουργήθηκε το πλαίσιο ATT&CK το οποίο δημοσιοποιήθηκε το 2015. Θεμέλιο της δημιουργίας του πλαισίου ATT&CK ήταν η διερεύνηση της συμπεριφοράς των επιτιθέμενων σε πραγματικά περιστατικά και συγκεκριμένα των Τακτικών και των Τεχνικών που χρησιμοποιούν. Ως Τακτικές ορίζονται οι στόχοι του επιτιθέμενου, δηλαδή το ΤΙ θέλει να επιτύχει, ενώ ως Τεχνικές ορίζονται οι ενέργειες του επιτιθεμένου για την επίτευξη των στόχων του. Το πλαίσιο διαχωρίζεται μεταξύ «εταιρικού περιβάλλοντος» και «κινητών συσκευών», ενώ το 2018 δημοσιεύτηκε και ο πίνακας Pre-ATT&CK, ο οποίος περιλαμβάνει 2 τακτικές με τις αντίστοιχες τεχνικές τους που αφορούν τις ενέργειες των κακόβουλων χρηστών πριν την απόκτηση πρόσβασης εντός του συστήματος.

Το τελικό αποτέλεσμα του πλαισίου ATT&CK είναι ένα διαδραστικό εργαλείο πλήρως επικαιροποιημένο με το οποίο μπορούν να δημιουργηθούν μοντέλα επιθέσεων, για την καλύτερη προετοιμασία και την κατάλληλη αντίδραση σε περίπτωση αντιμετώπισης ενός κακόβουλου περιστατικού. Οι πληροφορίες που προέκυψαν και διατίθενται από το πλαίσιο ATT&CK, χρησιμοποιούνται από αρκετά λογισμικά τα οποία είτε υλοποιούν τις

συγκεκριμένες τεχνικές (Red Team Attack Scripts) είτε τις συνδυάζουν και τις αυτοματοποιούν για σκοπούς εκπαίδευσης, έρευνας, προετοιμασίας και ελέγχων.

### 4.1.3 Adversary Emulation Plan Library

Η Adversary Emulation Plan Library, αποτελεί την εξέλιξη προηγούμενων προσπαθειών του οργανισμού για την προσομοίωση του τρόπου δράσης συγκεκριμένων κακόβουλων ομάδων. Το 2017 ο Mitre παρουσίασε μια προσομοίωση του τρόπου δράσης της κινέζικης ομάδας APT-3 ακολουθώντας στις αρχές του 2020 η προσομοίωση της ρωσικής APT-29. Το αυξημένο ενδιαφέρον που επιδείχθηκε για τις συγκεκριμένες προσομοιώσεις, οδήγησε στη δημιουργία μέσω του Mitre Engenuity's Center for Threat-Informed Defense, στο οποίο συμμετέχουν 27 εταιρείες και οργανισμοί από όλο τον κόσμο, μιας νέας κοινής δομής για την προσομοίωση της δράσης κακόβουλων ομάδων.

Η πρώτη προσομοίωση που βασίζεται στην Adversary Emulation Plan Library παρουσιάστηκε τον Σεπτέμβριο του 2020 και αφορά την ομάδα FIN6, μιας ομάδας που στοχεύει κυρίως εταιρείες που χρησιμοποιούν τερματικά πληρωμών POS μεγάλης οικονομικής δραστηριότητας για την υποκλοπή των στοιχείων των πιστωτικών καρτών.

Οι προσομοιώσεις που παρουσιάζει ο οργανισμός Mitre, βασίζονται σε πληροφορίες από δημοσιοποιημένες αναφορές περιστατικών ασφαλείας που αποδίδονται σε συγκριμένες ομάδες. Με την δημιουργία της Adversary Emulation Plan Library και την υιοθέτηση ανοικτών πρότυπων (Markdown, YAML) γίνεται μια προσπάθεια για την δημιουργία μιας βιβλιοθήκης προσομοιώσεων κακόβουλων ομάδων με συγκεκριμένη δομή και τυποποίηση και ελεύθερα προσβάσιμη από όλους.

## 4.2 Αυτοματοποιημένες Επιθέσεις

Δεν υπάρχει αμφιβολία ότι οι ειδικοί του τομέα της ασφάλειας πληροφοριών χρησιμοποιώντας τις γνώσεις και την εμπειρία τους καταφέρνουν να διακρίνουν ευπάθειες και αδυναμίες εκεί που οι υπόλοιποι χρήστες αδυνατούν. Στοιχεία και συμπεριφορές οι οποίες μπορεί φαινομενικά να μην σχετίζονται, υπό την διερεύνηση ενός ειδικού μπορεί να αποτελούν μια άριστα σχεδιασμένη και εκτελεσμένη επίθεση.

Μπορεί η λογική και η νοημοσύνη ως κάποιο βαθμό να μπορούν να αυτοματοποιηθούν, η εμπειρία ωστόσο αποτελεί μια ιδιαίτερα δύσκολη περίπτωση.

Όπως όμως κάθε νόμισμα έχει δύο όψεις, έτσι και στην ασφάλεια πληροφοριών, η χρήση της επεξεργαστικής ισχύς μπορεί να συνεισφέρει σημαντικά. Υπάρχουν ενέργειες, όπως για παράδειγμα η εκτέλεση επαναλαμβανόμενων διαδικασιών, ο έλεγχος και εντοπισμός ανωμαλιών ή συγκεκριμένων μοτίβων εντός μεγάλου εύρους δεδομένων, η κατηγοριοποίηση και ο διαχωρισμός, οι κωδικοποιήσεις/αποκωδικοποιήσεις αλλά και πολλές άλλες ενέργειες οι οποίες μπορεί να εκτελεστούν πολύ πιο αποτελεσματικά σε πολύ μικρότερους χρόνους από τους υπολογιστές.

Η απαίτηση για διερεύνηση του πολύ μεγάλου αριθμού διαφορετικών τεχνικών που χρησιμοποιούν οι επιτιθέμενοι και το μειωμένο συνήθως προσωπικό που καλείτε να τους αντιμετωπίσει οδήγησαν στη δημιουργία πληθώρας εργαλείων και υπηρεσιών αυτοματοποίησης επιθέσεων. Τόσο το λογισμικό όσο και οι υπηρεσίες προσομοίωσης χρησιμοποιούνται κυρίως για τον έλεγχο των μηχανισμών ασφαλείας, αυτοματοποιημένων ή μη, ενός πληροφοριακού συστήματος και κατά πόσο αυτοί είναι σε θέση να εντοπίσουν επιθέσεις πριν, κατά τη διάρκεια και μετά την πραγματοποίησή τους και να τις αντιμετωπίσουν.

### 4.2.1 Caldera – Cascade

Τα Caldera και Cascade είναι πλατφόρμες του οργανισμού Mitre τα οποία χρησιμοποιούνται για την αυτοματοποίηση των διεργασιών και των ενεργειών που καλούνται να εκτελέσουν οι Κόκκινες και οι Μπλε ομάδες αντίστοιχα. Και οι δύο πλατφόρμες βασίζονται στο πλαίσιο ATT&CK και στα υπόλοιπα ερευνητικά προγράμματα του οργανισμού και διατίθενται δωρεάν.

#### *4.2.1.1 Caldera*

Η πλατφόρμα του Caldera αποτελείται από το Κέντρο Διοίκησης και Ελέγχου (C2), και επί μέρους πρόσθετα. Η κύρια χρήση της πλατφόρμας είναι η εκτέλεση και η προσομοίωση αυτοματοποιημένων επιθέσεων με την χρήση Agents. Οι Agents αυτοί, είναι μικρές εφαρμογές οι οποίες δεν απαιτούν εγκατάσταση και οι οποίοι όταν

εκτελεστούν σε ένα σύστημα περιμένουν εντολές από το C2 τις οποίες στη συνέχεια τρέχουν στο σύστημα στο οποίο επιτίθενται και με την ολοκλήρωση τους επιστρέφουν τα αποτελέσματα στο C2. Η πλατφόρμα μπορεί να εκτελέσει πλήρως αυτοματοποιημένες επιθέσεις ή να χρησιμοποιηθεί από Κόκκινες Ομάδες για την εκτέλεση συγκεκριμένων επιθέσεων. Μεταξύ των προσθέτων που είναι διαθέσιμα με την εγκατάσταση, περιλαμβάνονται πρόσθετα τα οποία χρησιμοποιούνται για την παρουσίαση και την ανάλυση των αποτελεσμάτων, για την εκτέλεση πιο εξειδικευμένων επιθέσεων και επιπρόσθετο εκπαιδευτικό υλικό.

#### *4.2.1.2 Cascade*

Η πλατφόρμα Cascade, είναι η αντίστοιχη πλατφόρμα αυτοματισμών για χρήση από τις Μπλε ομάδες. Αυτοματοποιεί την αναζήτηση ενδείξεων παραβίασης (IoC), σε δεδομένα αποθηκευμένα σε περιβάλλον Splunk ή Elasticsearch για την δημιουργία συναγερμών. Στη συνέχεια οι συναγερμοί αυτοί ενεργοποιούν μια σειρά από επιπρόσθετες διερευνητικές διαδικασίες ώστε να εξαχθούν συμπεράσματα για τις τεχνικές που χρησιμοποιήθηκαν ή χρησιμοποιούνται από τους επιτιθέμενους. Τα αποτελέσματα από αυτούς τους ελέγχους παρουσιάζονται σε γράφους και διαγράμματα σχέσεων με πληροφορίες από το πλαίσιο ATT&CK.

### 4.2.2 Red Canary Atomic Red Team Project

Το Atomic Red Team Project της εταιρείας Red Canary αποτελείται από ελεύθερα διαθέσιμα Red Team Attack Scripts τα οποία είναι γραμμένα έτσι ώστε κάθε ένα από αυτά να υλοποιεί μια Τεχνική του πλαισίου Mitre ATT&CK. Η φιλοσοφία που ακολουθεί η συγκεκριμένη εταιρεία είναι ότι οι έλεγχοι πρέπει να είναι μικροί , γρήγοροι και να μπορούν με αυτό τον τρόπο να συνδυαστούν εύκολα ώστε να μπορεί να γίνει εκτεταμένος έλεγχος της κάλυψης των συστημάτων. Μέσα από την εκτέλεση των συγκεκριμένων Scripts δημιουργούνται Ενδείξεις Παραβίασης (IoC) οι οποίες θα πρέπει να γίνουν αντιληπτές από το προσωπικό ασφαλείας ή τις Μπλε ομάδες.

Μια από τις προσεγγίσεις η οποία δημιουργήθηκε από την κοινότητα των χρηστών της συγκεκριμένης υπηρεσίας και υιοθετήθηκε από την εταιρεία, είναι το «ρίξιμο του

ζαριού»1, η τυχαία δηλαδή επιλογή ενός Attack Script, και ο έλεγχος των επιπτώσεων και της ανίχνευσης του στο περιβάλλον που ελέγχεται.

Τα Scripts είναι γραμμένα σε αρχεία yaml, και χρησιμοποιούν ένα σύνολο από διαθέσιμες δωρεάν εφαρμογές για να υλοποιηθούν. Παράλληλα η εταιρεία προσφέρει ένα λογισμικό εκτέλεσης υλοποιημένο σε Powershell το οποίο παρέχει δυνατότητες μεμονωμένης ή συνδυασμένης εκτέλεσης των Scripts.

### 4.2.3 Infection Monkey

Όπως και οι προηγούμενες υλοποιήσεις που αναφέρθηκαν έτσι και το Infection Monkey της εταιρείας Guardicore είναι δωρεάν λογισμικό ανοικτού κώδικα το οποίο ελέγχει το δίκτυο σύμφωνα με το πλαίσιο Μηδενικής Εμπιστοσύνης (Zero Trust) τεχνικές από το πλαίσιο ATT&CK. Πρόκειται για ένα λογισμικό προσομοίωσης μη εξουσιοδοτημένης πρόσβασης και επιθέσεων για τον έλεγχο ιδιωτικών αλλά και βασισμένων στο νέφος υποδομών. Για την εκκίνηση των ελέγχων απαιτείτε η «μόλυνση» μιας συσκευής εντός του δικτύου με την εκτέλεση της αντίστοιχης εφαρμογής. Ακολούθως η εφαρμογή εκτελεί διαρκώς ελέγχους και εντοπίζει ευπάθειες οι οποίες αποτελούν κίνδυνο για την ασφάλεια της υποδομής. Τέλος τα αποτελέσματα από τους ελέγχους εναρμονίζονται και παρουσιάζονται σύμφωνα με το πλαίσιο ATT&CK.

[1] https://atomicredteam.io/roll-the-dice

# Κεφάλαιο 5

# Ψηφιακά Πεδία Βολής

Τα Ψηφιακά Πεδία Βολής αν και όπως αναφέρθηκε προηγουμένως δεν αποτελούν κάτι το πρωτόγνωρο εντούτοις εξακολουθούν να αποτελούν μια μη τυποποιημένη τεχνολογία με όλες τις συνέπειες που επιφέρει αυτό. Ο τρόπος λειτουργίας, η υλοποίηση της υποδομής, οι δυνατότητες και οι λειτουργίες που μπορεί να εκτελέσει ένα ΨΠΒ ακόμα και η ονοματολογία, είναι μόνο μερικά από τα χαρακτηριστικά τα οποία εναποφύονται αποκλειστικά στο δημιουργό. Ως αποτέλεσμα κατά την διάρκεια της προσπάθειας επίλυσης κάποιου προβλήματος με την χρήση ΨΠΒ τίποτα δεν μπορεί να θεωρηθεί δεδομένο και θα πρέπει να προηγηθεί αρκετή έρευνα για την καταλληλόλητα κάποιας συγκεκριμένης επιλογής.

Ο NIST, σε σχετικό έντυπο, περιγράφει τα ΨΠΒ ως διαδραστικές προσομοιωμένες αναπαραστάσεις του δικτύου, των συστημάτων, των εργαλείων και των εφαρμογών ενός οργανισμού διασυνδεδεμένες με μια επίσης ελεγχόμενη προσομοίωση του διαδικτύου ή συγκεκριμένων υπηρεσιών. Με την συνδεσμολογία αυτή, τα ΨΠΒ παρέχουν ένα ασφαλές περιβάλλον τόσο από φυσικής όσο και νομικής άποψης για εξάσκηση αλλά και έλεγχο της υποδομής σε συνθήκες κυβερνοεπιθέσεων.

Ο Ευρωπαϊκός Οργανισμός Κυβερνόασφάλειας (ECSO), σε ενημερωτική έκδοση σχετικά με τα ΨΠΒ, αναφέρει ότι έχουν επικρατήσει δύο κύριοι ορισμοί. Ο πρώτος, ο οποίος προσεγγίζει πολύ τον ορισμό του NIST, αφορά τον παραδοσιακό ορισμό του ΨΠΒ ως περιβάλλον προσομοίωσης των τεχνολογιών της πληροφορίας και των επικοινωνιών (ICT) που χρησιμοποιούνται από ένα οργανισμό  άλλοτε συμπεριλαμβανομένων και άλλοτε όχι των υπηρεσιών του διαδικτύου. Ο ορισμός αυτός θεωρείται στατικός και με πολύ συγκεκριμένες λειτουργίες, με συνέπεια τις υψηλές απαιτήσεις χρόνου και προσπάθειας όταν απαιτούνται αλλαγές. Ο δεύτερος ορισμός αφορά τα ΨΠΒ ως

πλατφόρμα ενοποίησης διαφόρων τεχνολογιών οι οποίες μπορούν να χρησιμοποιηθούν ως βάση για την δημιουργία και την χρήση ΨΠΒ. Κύριο σημείο αυτού του ορισμού επισημαίνεται ότι είναι η λέξη «χρήση» αφού για την χρήση των ΨΠΒ για συγκεκριμένους σκοπούς απαιτούνται και συγκεκριμένες δυνατότητες τις οποίες θα πρέπει να διαθέτει η πλατφόρμα. Ο ορισμός αυτός ξεκάθαρα αντικατοπτρίζει ένα δυναμικό περιβάλλον με ευελιξία ενσωμάτωσης διαφορετικών λειτουργιών αναλόγως των αναγκών του κάθε περιβάλλοντος που πρέπει να προσομοιωθεί. Καταλήγοντας, ο οργανισμός προτείνει την χρήση του ακόλουθου ορισμού:

«Ένα ΨΠΒ είναι μια πλατφόρμα που χρησιμοποιείται για την δημιουργία και την χρήση ενός διαδραστικού περιβάλλοντος προσομοίωσης ή και περισσότερων. Ένα περιβάλλον προσομοίωσης είναι μια αναπαράσταση των τεχνολογιών επικοινωνίας και πληροφοριών, του επιχειρησιακού εξοπλισμού, των κινητών και φυσικών συστημάτων, των εφαρμογών, των υποδομών καθώς και των προσομοιώσεων των επιθέσεων, των χρηστών συμπεριλαμβανομένων των δραστηριοτήτων τους, όπως επίσης και οποιασδήποτε υπηρεσίας του διαδικτύου εταιρικής ή δημόσιας η οποία απαιτείται για τις ανάγκες της προσομοίωσης. Ένα ΨΠΒ αποτελείται από ένα συνδυασμό επί μέρους κύριων τεχνολογιών οι οποίες χρησιμοποιούνται σύμφωνα με τις ανάγκες και τις χρήσεις του ΨΠΒ.»

Ένα ΨΠΒ, μπορεί να παρέχεται εξ ολοκλήρου ως υπηρεσία χωρίς την ύπαρξη φυσικού εξοπλισμού ή μπορεί να αποτελεί συνδυασμό εξοπλισμού και λογισμικού. Οι ελάχιστες απαιτήσεις κύριων υπηρεσιών ενός ΨΠΒ είναι:

1. Δυνατότητα δημιουργίας υποδομής/διαχείρισης δικτύου: υπεύθυνη για την δημιουργία και των διαχωρισμό των δικτύων που θα χρησιμοποιούνται από το ΨΠΒ.
2. Δυνατότητα δημιουργίας/διαχείρισης τερματικών: τα τερματικά μπορεί να είναι είτε ολοκληρωμένες εικονικές μηχανές είτε containers τα οποία να προσομοιώνουν πραγματικά τερματικά
3. Δυνατότητα ενορχήστρωσης: Μπορεί να εκτείνεται από απλά την αυτόματη δημιουργία πολλών τερματικών, την δυνατότητα πολλαπλής παραμετροποίησης, ακόμα και την αυτοματοποίηση διεργασιών μεταξύ διαφορετικών συστατικών του περιβάλλοντος.
4. Υπηρεσία αυθεντικοποίησης χρηστών: η υπηρεσία που χρησιμοποιείται για την εξουσιοδότηση της πρόσβασης και των δικαιωμάτων των χρηστών.

5. Περιβάλλον Διαχείρισης ΨΠΒ: το περιβάλλον που χρησιμοποιείται τόσο για την δημιουργία όσο και για την χρήση των προσομοιώσεων.
6. Πίνακα ελέγχου της κατάστασης των μέσων που χρησιμοποιούνται στην υποδομή

Επιπρόσθετα, αναλόγως του τρόπου χρήσης του ΨΠΒ μπορεί να περιλαμβάνονται και κάποιες από τις ακόλουθες δυνατότητες:

1. Ενσωμάτωση συστημάτων εντοπισμού/αποτροπής εισβολέων (IDS/IPS) τερματικών ή δικτύου.
2. Εξουσιοδότηση χρηστών με χρήση υφιστάμενων υπηρεσιών (Active Directory, LDAP, OpenID, Υπηρεσίες Νέφους)
3. Εκτέλεση ή/και αυτοματοποίηση επιθέσεων (Red Scripts).
4. Αυτόματη αξιολόγησης/βαθμολόγησης.
5. Προσομοίωση βιομηχανικών πρωτοκόλλων (SCADA, Modbus, RS485 κλπ)
6. Προσομοίωση υπηρεσιών του διαδικτύου.
7. Προσομοίωση ενεργειών χρηστών
8. Συμμετοχή χρηστών
9. Συνδυασμός πραγματικών χρηστών και αυτοματοποιημένων επιθέσεων
10. Συγκεντρωτική συλλογή και ανάλυση καταγραφών από τα συστήματα της υποδομής
11. Πίνακα ελέγχου με δυνατότητα παραμετροποίησης των Σεναρίων
12. Παρακολούθηση σε πραγματικό χρόνο της εξέλιξης των Σεναρίων
13. Εργαλεία εκπαιδευτή: Για παράδειγμα chat, δυνατότητα απάντησης ερωτήσεων, δυνατότητα ανατροφοδότησης από τους χρήστες, δυνατότητα ελέγχου της εξέλιξης και της ροής των Σεναρίων και των Μέσων κ.α.

## 5.1 KYPO Cyber Range

Το KYPO Cyber Range αποτελεί την μοναδική δωρεάν διαθέσιμη λύση ΨΠΒ η ανάπτυξη της οποίας οποία εξακολουθεί να παραμένει ενεργή. Δημιουργήθηκε στο πανεπιστήμιο Masaryk της Τσεχίας και η ανάπτυξη του άρχισε το 2013. Τα προηγούμενα χρόνια χρησιμοποιήθηκε εντατικά εντός του πανεπιστημίου για εκπαιδευτικούς σκοπούς αλλά και για την διεξαγωγή ασκήσεων με την Εθνική Αρχή Ασφάλειας Πληροφοριών και άλλες εθνικές και διεθνής οντότητες. Στη παρούσα έκδοση η οποία διατίθεται σαν

λογισμικό ανοικτού κώδικα μέσα από το Ευρωπαϊκό Πρόγραμμα Concordia H2020 η δημιουργία, διαχείριση και χρήση του ΨΠΒ βασίζεται κυρίως στις τεχνολογίες Openstack, Ansible, Redis, Docker και Elasticsearch, το γραφικό περιβάλλον βασίζεται σε Python Django και Angular και για η αυθεντικοποίηση των χρηστών στην πλατφόρμα OpenID. Η συγκεκριμένη υλοποίηση βασίζεται στα ακόλουθα κύρια χαρακτηριστικά:

- Sandbox Definition: Η δομή του πληροφοριακού συστήματος, ως Ansible Script.
- Pool - Sandbox Allocation: Η δέσμευση των πόρων η εκτέλεση του Ansible Script και η μετατροπή της δομής σε εικονικά μηχανήματα με τις κατάλληλες διασυνδέσεις.
- Training Definition: Οι εκπαιδεύσεις, οι οποίες αποτελούν τις ενέργειες που καλείται ο χρήστης να φέρει εις πέρας.
- Post Training Analysis: Την παρουσίαση των αποτελεσμάτων των χρηστών.

# Κεφάλαιο 6

# Μεθοδολογία

Η ανάπτυξη ενός ΨΠΒ, όπως και κάθε λογισμικού είναι μια πολύ απαιτητική διαδικασία η οποία δεν αποτελείται μόνο από τον προγραμματισμό αλλά από ένα σύνολο βημάτων που πρέπει να ακολουθηθούν για την διεκπεραίωση της. Το σύνολο αυτών των βημάτων, ή φάσεων, καθώς και οι ενέργειες που θα εκτελεστούν στην κάθε φάση καλείται μοντέλο κύκλου ζωής του λογισμικού και περιλαμβάνει όλες τις διαδικασίες από την σύλληψη της ιδέας μέχρι την διανομή του λογισμικού την χρήση και την υποστήριξη του. Με την χρήση των μοντέλων κύκλου ζωής, παρέχεται καλύτερος έλεγχος της εξέλιξης του λογισμικού. Όλοι οι εμπλεκόμενοι αντιλαμβάνονται το τι πρόκειται να δημιουργηθεί, γιατί και με ποιο τρόπο, αυξάνοντας έτσι τις πιθανότητες για την δημιουργία υψηλής ποιότητας λογισμικού. Η ύπαρξη σαφών χρονοδιαγραμμάτων και η χρήση τυποποιημένων και βέλτιστων τεχνικών για την αποφυγή κοινών προβλημάτων που παρουσιάζονται κατά την διάρκεια ανάπτυξης λογισμικών συμβάλλουν στον περιορισμό του απαιτούμενου χρόνου ανάπτυξης και την μείωση του κόστους. Τα μοντέλα κύκλου ζωής λογισμικού αναλόγως του τρόπου ανάπτυξης που χρησιμοποιούν διακρίνονται σε δύο κύριες κατηγορίες τα ακολουθιακά και τα επαναληπτικά. Στα ακολουθιακά μοντέλα η ανάπτυξη γίνεται σε διαδοχικές διακριτές φάσεις για το σύνολο του λογισμικού, ενώ στα επαναληπτικά η ανάπτυξη γίνεται σε τμήματα. Το μοντέλο που θα χρησιμοποιηθεί επιλέγεται κατά περίπτωση βάση των εκάστοτε συνθηκών και απαιτήσεων του λογισμικού και καθορίζει τον τρόπο δράσης καθ’ όλη της διάρκεια του κύκλου ζωής του λογισμικού. Τα μοντέλα κύκλου ζωής αποτελούνται συνήθως από τις ακόλουθες φάσεις, οι οποίες αναλόγως του μοντέλου που θα υλοποιηθεί μπορεί να τροποποιηθούν, να εκτελεστούν περισσότερες από μία φορές ή να συνδυαστούν:

## 6.1 Ανάλυση Προβλήματος - Προδιαγραφή

Η αρχή ενός λογισμικού ορίζεται πάντοτε από τον καθορισμό του προβλήματος το οποίο καλείται να επιλύσει. Περαιτέρω ανάλυση όπως για παράδειγμα η διερεύνηση του πώς αντιμετωπιζόταν μέχρι στιγμής το συγκεκριμένο πρόβλημα και ποια είναι τα δυνατά σημεία και οι αδυναμίες των υφιστάμενων λύσεων, ενδέχεται να συνεισφέρουν σημαντικά στην δημιουργία μιας ολοκληρωμένης άποψης και πιο σωστής προσέγγισης.

Είναι επίσης σημαντικό κατά τη διάρκεια αυτής της φάσης να εισακουστούν απόψεις και γνώμες από πιθανούς μελλοντικούς χρήστες, τους προγραμματιστές και όσος θα εργαστούν για την υλοποίηση του, και αν είναι δυνατόν ακόμη και από ειδικούς του τομέα που αφορά το λογισμικό.

## 6.2 Σχεδίαση - Πλάνο Ανάπτυξης

Σε αυτή τη φάση αναλύονται οι απαιτήσεις και καθορίζονται οι ανάγκες σε μέσα, πόρους και επιμέρους δομές για την δημιουργία του λογισμικού. Γίνεται επίσης εκτίμηση των κινδύνων που μπορεί να παρουσιαστούν και προβλέπεται εναλλακτικός σχεδιασμός για την μείωση του ρίσκου αυτών των κινδύνων. Σε αυτό το σημείο αποφασίζεται κατά πόσο είναι εφικτή η υλοποίηση μιας λύσης, και ο τρόπος που θα υλοποιηθεί ώστε να γίνει με το μικρότερο ρίσκο.

Στη συνέχεια καθορίζεται το Πλάνο Ανάπτυξης για την υλοποίηση του λογισμικού. Καταγράφονται σε έντυπη μορφή οι κύριες ενέργειες που πρέπει να εκτελεστούν, οι οποίες στη συνέχεια θα πρέπει να εγκριθούν από τους μετόχους της εταιρείας, ή το διοικητικό συμβούλιο. Τυχόν διαφοροποιήσεις από αυτά που θα καθοριστούν σε αυτό το στάδιο, είναι πολύ πιθανό να παρουσιάσουν οικονομικό αντίκτυπο ή στη χειρότερη περίπτωση ακόμα και αποτυχία ολόκληρου του προγράμματος.

## 6.3 Κωδικοποίηση

Η κωδικοποίηση είναι ουσιαστικά η φάση της κύριας υλοποίησης τους λογισμικού. Κατά τη φάση αυτή γίνεται ο προγραμματισμός του λογισμικού και τυχόν υποστηρικτικών υπηρεσιών που απαιτούνται για την λειτουργία του. Είναι πολύ

σημαντικό οι προγραμματιστές να τηρούν τα χρονοδιαγράμματα που καθορίστηκαν στο Πλάνο Ανάπτυξης και να φέρουν εις πέρας όλες τις απαιτούμενες προδιαγραφές.

## 6.4 Έλεγχος - Επαλήθευση

Αν και οι τάσεις της εποχής (Continuous Development/Continuous Integration) τείνουν να ενοποιήσουν αυτή τη φάση με την προηγούμενη, ενσωματώνοντας τους ελέγχους κατά τη διάρκεια της κωδικοποίησης, εντούτοις ένα λογισμικό θα πρέπει πάντα να ελέγχεται λεπτομερώς. Όλες οι λειτουργίες του λογισμικού πρέπει να ελεγχθούν ενδελεχώς καθώς και η συμπεριφορά του λογισμικού σε πιθανούς λάθος χειρισμούς των χρηστών ή προσπάθειες παραβίασης των δικλίδων ασφαλείας από κακόβουλους χρήστες. Σε κρίσιμες υποδομές μπορεί συγκεκριμένοι έλεγχοι να απαιτείται να πραγματοποιηθούν παρουσία του αγοραστή.

## 6.5 Λειτουργία - Εξέλιξη

Με την ολοκλήρωση όλων των φάσεων το λογισμικό είναι έτοιμο για χρήση. Αναλόγως της περίπτωσης μπορεί να απαιτείται αρχικά η χρήση του σε δοκιμαστικό περιβάλλον ώστε να διαπιστωθεί η συμπεριφορά του σε προσομοιωμένο περιβάλλον πριν τεθεί σε χρήση στο πραγματικό περιβάλλον. Ένα λογισμικό δεν ολοκληρώνεται ποτέ παρά μόνο με την απόσυρση του, για το λόγο αυτό κατά την διάρκεια της λειτουργίας του ενεργοποιείται και η διαδικασία της Συντήρησης. Σε όλη τη διάρκεια της χρήσης του λογισμικού ενδέχεται να παρουσιαστούν προβλήματα, νέες απαιτήσεις και κενά ασφαλείας για τα οποία θα πρέπει να ληφθούν οι κατάλληλες ενέργειες.

## 6.6 Το Μοντέλο Καταρράκτη

Το παλαιότερο ίσως μοντέλο κύκλου ζωής λογισμικού, είναι το μοντέλο του καταρράκτη. Ένα ακολουθιακό μοντέλο στο οποίο την ολοκλήρωση της κάθε φάσης διαδέχεται η επόμενη, όπως συμβαίνει με τα επίπεδα ενός καταρράκτη. Ολόκληρο το σύστημα μεταβαίνει από φάση σε φάση αφού προηγουμένως εκτελεστεί μια αξιολόγηση για την υλοποίηση των απαραίτητων ενεργειών της κάθε φάσης και η επόμενη φάση δεν μπορεί να ξεκινήσει αν προηγουμένως δεν έχει ολοκληρωθεί η

προηγούμενη. Το μοντέλο του καταρράκτη είναι ιδιαίτερα διαδομένο και χρησιμοποιείται κυρίως όταν όλες οι απαιτήσεις είναι ξεκάθαρες από την αρχή και δεν αναμένονται σημαντικές τροποποιήσεις κατά την διάρκεια της ανάπτυξης.

## 6.7 Το μοντέλο Πρωτοτυποποίησης

Το μοντέλο πρωτοτυποποίησης είναι ένα ιδιαίτερα ευέλικτο επαναληπτικό μοντέλο το οποίο όπως υποδηλώνει και το όνομα του βασίζεται σε πρωτότυπα. Σε κάθε πρωτότυπο επιλέγεται ένα τμήμα του λογισμικού το οποίο πρόκειται να αναπτυχθεί μέχρι ένα συγκεκριμένο σημείο και με την ολοκλήρωση του τίθεται σε δοκιμή. Μόλις ολοκληρωθεί η δοκιμή και καταγραφεί η συμπεριφορά και τυχόν παρατηρήσεις, ένα νέο πρωτότυπο δημιουργείται στο οποίο προστίθενται περισσότερες από τις απαιτήσεις. Η διαδικασία αυτή επαναλαμβάνεται μέχρις ότου όλα τα επιμέρους τμήματα του λογισμικού να ολοκληρωθούν και να γίνει αποδεκτό από τον αγοραστή. Το μοντέλο πρωτοτυποποίησης προσφέρει ταχύτερα μια πρώτη επαφή με το λογισμικό, δίνοντας την δυνατότητα για πρώτες εκτιμήσεις, τροποποιήσεις και ανάλογη διαμόρφωση της στρατηγικής που θα ακολουθηθεί. Παρέχει επίσης ένα ευμετάβλητο περιβάλλον το οποίο μπορεί να τροποποιηθεί αναλόγως νέων αναγκών ή απαιτήσεων που μπορεί να προκύψουν καθιστώντας το ιδανικό για την ανάπτυξη εφαρμογών για τις οποίες δεν υπάρχει βεβαιότητα στην αρχή της ανάπτυξης, όπως για παράδειγμα εφαρμογές για τις οποίες δεν υπάρχει η κατάλληλη εμπειρία ή κάποια αποδεκτή προηγούμενη υλοποίηση.

## 6.8 Μοντέλο Κύκλου Ζωής Της Παρούσας Διατριβής

Η απουσία εμπειρίας προγραμματισμού αυτής της κλίμακας σε συνδυασμό με το περιορισμένο χρονικό πλαίσιο και την έκταση της πλατφόρμας του Ψηφιακού Πεδίου Βολής δεν άφηναν και πολλές επιλογές για την επιλογή του κατάλληλου μοντέλου κύκλου ζωής. Στη παρούσα διατριβή χρησιμοποιήθηκε το μοντέλο πρωτοτυποποίησης, αφού αν και τέθηκαν συγκεκριμένες απαιτήσεις ο κυριότερος σκοπός παρέμενε η επαλήθευση της ορθότητας της υπόθεσης με ένα λειτουργικό ΨΠΒ και όχι ένα πλήρες τελικό προϊόν. Λαμβάνοντας υπόψη τα ανωτέρω η καλύτερη επιλογή υλοποίησης μπορεί να προκύψει με ευέλικτα διαδοχικά πρωτότυπα μέχρι μια τελική λύση που να περιλαμβάνει αν όχι όλες τις απαιτήσεις τότε το μεγαλύτερο ποσοστό τους.

# Κεφάλαιο 7

# Προτεινόμενη Υλοποίηση

## 7.1 Προϋποθέσεις

Κατά τις φάσεις της ανάλυσης του προβλήματος και της σχεδίασης, αποφασίστηκε η δημιουργία της πλατφόρμας λαμβάνοντας υπόψη τους ακόλουθους παράγοντες:

1. Διαλειτουργικότητα Χρήσης: Η υλοποίηση θα πρέπει να μπορεί να χρησιμοποιηθεί από όσο το δυνατό περισσότερους τύπους συσκευών και λειτουργικών συστημάτων.
2. Διαλειτουργικότητα Μέσων: Θα πρέπει να υπάρχει η δυνατότητα προσομοίωσης διαφορετικών τύπων συσκευών και λειτουργικών συστημάτων καθώς και της μεταξύ τους αλληλεπίδρασης.
3. Φορητότητα - Ευελιξία: Να χρησιμοποιηθούν τεχνολογίες οι οποίες να καθιστούν τον κώδικα και γενικότερα το περιβάλλον ευέλικτο ώστε να μπορεί να χρησιμοποιηθεί σε άλλες παρόμοιες λύσεις, συστήματα ή έρευνες.
4. Συμβατότητα: Η πλατφόρμα θα πρέπει να παραμείνει συμβατή με την υφιστάμενη υποδομή του πανεπιστημίου και πιο συγκεκριμένα:
    a) Να μπορεί να χρησιμοποιήσει το σύστημα αυθεντικοποίησης (FreeIPA)
    b) Να εκμεταλλευτεί το υφιστάμενο περιβάλλον δημιουργίας εικονικών μηχανών (OVirt)
5. Επεκτασιμότητα: Ο τρόπος ανάπτυξης της πλατφόρμας να είναι τέτοιος ώστε να επιτρέπει τόσο την μελλοντική ανάπτυξη όσο και την αύξηση του όγκου των πληροφοριών που μπορεί να διαχειριστεί.

6. Χρήση Λογισμικού Ανοικτού Κώδικα: Να καταβληθεί προσπάθεια ώστε το σύστημα να βασιστεί στο μέγιστο βαθμό σε Λογισμικό Ανοικτού Κώδικα και Ελεύθερο Λογισμικό.
7. Αναβαθμίσεις: Η επιλογή των εργαλείων, των πρόσθετων και των βιβλιοθηκών που θα χρησιμοποιηθούν να γίνει με κυριότερο κριτήριο την ύπαρξη ενεργής κοινότητας και την συχνή αναβάθμιση τους, ώστε να αποφευχθεί ο κίνδυνος της εγκατάλειψης τους με συνέπεια τη δημιουργία προβλημάτων στην πλατφόρμα στο μέλλον.

## 7.2 Ορολογία Συστήματος

Η ορολογία του συστήματος αποτελεί την βάση για την κατανόηση του τρόπου λειτουργίας της πλατφόρμας. Επίσης κατανοώντας την ορολογία διευκολύνεται σε πολύ μεγάλο βαθμό και η κατανόηση της υλοποίησης που ακολουθεί.

### 7.2.1 Αυτοματοποιημένες Επιθέσεις

Οι Αυτοματοποιημένες Επιθέσεις είναι οι ενέργειες που πρόκειται να εκτελέσει ένα εικονικό μηχάνημα κατά την διάρκεια της εξέλιξης ενός Σεναρίου. Οι επιθέσεις αυτές βασίζονται στα Πρότυπα Επιθέσεων, και κατά την διάρκεια της παραμετροποίησης των Σεναρίων, οι μεταβλητές που χρησιμοποιούνται στο Πρότυπο στο οποίο θα βασιστεί μία επίθεση πρέπει να αντικατασταθούν με πραγματικές τιμές που αντικατοπτρίζουν το συγκεκριμένο Πεδίο Μάχης. Κατά τη διάρκεια εκτέλεσης του Σεναρίου ο κώδικας της Αυτοματοποιημένης Επίθεσης λαμβάνεται από το εικονικό μηχάνημα στο οποίο έχει προγραμματιστεί η εκτέλεση και αφού αποκωδικοποιηθεί και αντικατασταθούν οι μεταβλητές εκτελείται. Όλη η διαδικασία από την λήψη μέχρι και τα αποτελέσματα επιτυχή ή όχι αναφέρονται πίσω στην πλατφόρμα για απεικόνιση σε πραγματικό χρόνο.

### 7.2.2 Εικονικά Πεδία Μάχης - Battlefields

Τα Εικονικά Πεδία Μάχης αποτελούν τη βάση ολόκληρου του συστήματος. Ένα ΕΠΜ αποτελείται από Δίκτυα, Δικτυακό Εξοπλισμό και Εικονικές Μηχανές διασυνδεδεμένα κατά τέτοιο τρόπο ώστε να προσομοιάζουν συνήθως μια πραγματική υποδομή. Υπάρχει μεγάλη ευελιξία στα ΕΠΜ που μπορούν να δημιουργηθούν αφού τόσο ο αριθμός και η

τοπολογία των δικτύων και του δικτυακού εξοπλισμού όσο και ο αριθμός και η διασύνδεση των Εικονικών Μηχανών περιορίζονται μόνο από τους διαθέσιμους πόρους του περιβάλλοντος oVirt. Επίσης είναι σημαντικό ότι για κάθε ΕΠΜ μπορούν να δημιουργηθούν περισσότερα από ένα Σενάρια.

### 7.2.3 Πρότυπα Εικονικών Μηχανών

Τα Πρότυπα (Templates), είναι μια δυνατότητα που προσφέρεται από την πλατφόρμα oVirt και χρησιμοποιείται για την ταχύτερη δημιουργία Εικονικών Μηχανών χρησιμοποιώντας ως βάση υφιστάμενες εικονικές μηχανές. Αρχικά δημιουργήθηκαν Εικονικές Μηχανές με συγκεκριμένα χαρακτηριστικά και εγκαταστάθηκαν σε αυτές τα απαιτούμενα λειτουργικά και εφαρμογές αναλόγως της χρήσης της οποίας προορίζονται να επιτελέσουν στο ΕΠΜ. Κατά την διάρκεια της δημιουργίας των ΕΠΜ ο χρήστης χρησιμοποιεί τα συγκεκριμένα πρότυπα επιτρέποντας του να εξοικονομήσει πολύτιμο χρόνο αποφεύγοντας περιττές επαναλήψεις. Αυτή η τεχνική δεν έχει κανένα περιορισμό στην παραμετροποίηση των εικονικών μηχανών αφού αυτές μπορούν στη συνέχεια να τροποποιηθούν όπως συμβαίνει με κάθε εικονική μηχανή στο περιβάλλον oVirt. Επίσης είναι πολύ εύκολο να δημιουργηθούν και να ενσωματωθούν νέα πρότυπα εντός της πλατφόρμας αφού το μόνο που απαιτείται είναι το Πρότυπο να αρχίζει με το πρόθεμα «dias_». Οποιοδήποτε πρότυπο αρχίζει με αυτό το πρόθεμα λαμβάνεται υπόψη και παρουσιάζεται κατά την δημιουργία των ΕΠΜ ως επιλογή για το που θα βασιστεί η κάθε εικονική μηχανή.

Για τις ανάγκες της παρούσας πτυχιακής χρησιμοποιούνται τρία πρότυπα εικονικών μηχανών τα οποία είναι τα ακόλουθα:

- dias_caldera: βασισμένο σε λειτουργικό Ubuntu 20.04 server, διαθέτει εγκατεστημένο το πλαίσιο αυτοματοποιημένων επιθέσεων Caldera του οργανισμού Mitre. Χρησιμοποιείται ως επιτιθέμενος.
- dias_neth_rt: βασισμένο σε λειτουργικό σύστημα CentOS 7, χρησιμοποιεί την υλοποίηση Nethserver, και χρησιμοποιείται ως προσομοίωση δρομολογητή.
- dias_Ubuntu_Desktop βασίζεται σε λειτουργικό σύστημα Ubuntu 18.04 Desktop, διαθέτει εγκατεστημένη την εφαρμογή Sinon που χρησιμοποιείται για την αυτοματοποίηση επιθέσεων και μπορεί να χρησιμοποιηθεί είτε ως επιτιθέμενος είτε

ως αμυνόμενος. Επίσης μπορεί να χρησιμοποιηθεί από τους χρήστες σε διαδραστικά σενάρια που απαιτούν την συμμετοχή πραγματικών χρηστών.

Οι ρυθμίσεις του κάθε πρότυπου είναι διαθέσιμες στο Παράρτημα Γ

## 7.3 Host

Οι «Host» είναι οι εικονικές μηχανές οι οποίες δημιουργούνται για να συμμετέχουν στα Εικονικά Πεδία Μάχης. Οι «Host» έχουν υποχρεωτικά ένα ρόλο («Red Team», «Blue Team», κ.α.), ανήκουν σε μια ομάδα και δημιουργούνται βάση των Πρότυπων Εικονικών Μηχανών. Μετά την δημιουργία τους μπορούν να παραμετροποιηθούν περεταίρω μέσω απομακρυσμένης σύνδεσης ώστε να προσομοιάζουν συγκεκριμένες αδυναμίες ή ευπάθειες και η κατάσταση τους να αποθηκευτεί ώστε να είναι γρήγορη η επαναφορά τους στην επιθυμητή κατάσταση.

### 7.3.1 Σενάρια

Τα Σενάρια αποτελούν την ουσία της παρούσας διατριβής και δημιουργούνται για να δοκιμαστούν οι διάφορες καταστάσεις που μπορούν να προκύψουν στο κάθε περιβάλλον. Σε κάθε ΕΠΜ μπορούν να δημιουργηθούν ένα ή περισσότερα Σενάρια με τον περιορισμό ότι μόνο ένα μπορεί να είναι ενεργό για το κάθε ΕΠΜ ανά πάσα στιγμή. Τα Σενάρια χρησιμοποιούνται για την εξοικονόμηση πόρων και χρόνου με την επαναχρησιμοποίηση των ίδιων μηχανημάτων και την επαναφορά τους κάθε φορά στην αρχική τους κατάσταση. Μέσα από τα Σενάρια μπορούν να επιλεγούν και να παραμετροποιηθούν οι επιθέσεις που θα εκτελέσει η κάθε οντότητα καθώς και να καθοριστούν δικαιώματα πρόσβασης σε χρήστες έτσι ώστε να μπορούν να χειριστούν τα εικονικά μηχανήματα για τους σκοπούς του Σεναρίου.

### 7.3.2 Πρότυπα Επίθεσης

Τα Πρότυπα Επίθεσης αποτελούν βασικό χαρακτηριστικό των Σεναρίων. Κάθε Πρότυπο Επίθεσης αποτελείται από ένα σύνολο εντολών, το Attack Script, το οποίο όταν εκτελεστεί αναμένεται ότι θα επιφέρει κάποια συγκεκριμένα αποτελέσματα. Το σημαντικότερο χαρακτηριστικό κατά την καταχώρηση των Προτύπων Επίθεσης είναι η

επιλογή του κατάλληλου μέσου που θα χρησιμοποιηθεί για την εκτέλεση της επίθεσης. Τα διαθέσιμα μέσα είναι τα:

- Shell
- Command Prompt
- PowerShell

Ο όρος Πρότυπο χρησιμοποιείται, γιατί κατά την δημιουργία τους, οι επιθέσεις αυτές δεν είναι ολοκληρωμένες λόγω της χρήσης μεταβλητών. Οι μεταβλητές αυτές αντικαθίστανται κατά τον ορισμό των Επιθέσεων στα Σενάρια αναλόγως των Στόχων. Με αυτό τον τρόπο αποφεύγονται αχρείαστες επαναλήψεις κώδικα, ανάγκη για περισσότερο αποθηκευτικό χώρο και μεγαλύτερη ευελιξία σε περίπτωση όπου απαιτούνται αλλαγές.

## 7.4 Βασικά Χαρακτηριστικά

Ως βασικά χαρακτηριστικά που θα πρέπει να διαθέτει η υλοποιημένη πλατφόρμα ορίστηκαν τα ακόλουθα:

1. Δημιουργία και επαναχρησιμοποίηση Εικονικών Πεδίων Μάχης.
2. Δημιουργία και επαναχρησιμοποίηση Σεναρίων.
3. Δημιουργία και επαναχρησιμοποίηση Αυτοματοποιημένων Επιθέσεων
4. Εκτέλεση Αυτοματοποιημένων Επιθέσεων.
5. Δυνατότητα συμμετοχής πραγματικών χρηστών στα Σενάρια.
6. Παρακολούθηση της εξέλιξης των επιθέσεων σε πραγματικό χρόνο.

# Κεφάλαιο 8

# Υλοποίηση

Η τελική υλοποίηση αποτελείται από τις ακόλουθες εφαρμογές, κωδικοποιημένες σε γλώσσα προγραμματισμού Python 3:

1) **Dias:** Το Γραφικό Περιβάλλον Δημιουργίας Εικονικών Πεδίων Μάχης, Σεναρίων και Αυτοματοποιημένων Επιθέσεων.
2) **Argos:** Η Διασύνδεση του Γραφικού Περιβάλλοντος με την πλατφόρμα oVirt.
3) **Sinon:** Η Αυτόματη Εκτέλεση Επιθέσεων, βάση του Σεναρίου, από τα Εικονικά Μηχανήματα του περιβάλλοντος oVirt
4) **Hermes:** Η αυτόματη προώθηση αρχείων καταγραφής από τον Wazuh/Suricata Manager προς το Περιβάλλον Απεικόνισης.

Για την πλήρη και ορθή λειτουργία της πλατφόρμας θα πρέπει όλες οι πιο πάνω εφαρμογές να εκτελούνται ταυτόχρονα μαζί με ένα σύνολο από επί μέρους υπηρεσίες και διεργασίες. Η συνολική δομή της πλατφόρμας φαίνεται στο Παράρτημα Α.

Στο παρόν κεφάλαιο παρουσιάζονται οι βιβλιοθήκες και οι λειτουργίες στις οποίες βασίστηκε η ανάπτυξη των πιο πάνω εφαρμογών, καθώς και τα υπόλοιπα κρίσιμα χαρακτηριστικά που αποτελούν την πλατφόρμα.

## 8.1 Σύστημα Διαχείρισης Περιεχομένου (CMS)

Ο όρος Content Management System (CMS, Σύστημα Διαχείρισης Περιεχομένου) αναφέρεται σε εφαρμογές που επιτρέπουν τη διαχείριση δικτυακού περιεχόμενου μέσω απλού και εύχρηστου περιβάλλοντος. Οι εφαρμογές αυτές επιτρέπουν την τροποποίηση

των δεδομένων χωρίς να είναι απαραίτητες ειδικές γνώσεις σχετικές με τη δημιουργία ιστοσελίδων ή τις Βάσεις Δεδομένων, καθώς οι πληροφορίες εισάγονται σε ειδικά διαμορφωμένες φόρμες εισαγωγής στοιχείων. Η παρουσίαση και η διαγραφή των δεδομένων γίνεται συνήθως με την χρήση απλών πινάκων και κουμπιών χωρίς περίπλοκες διαδικασίες.

### 8.1.1 Django

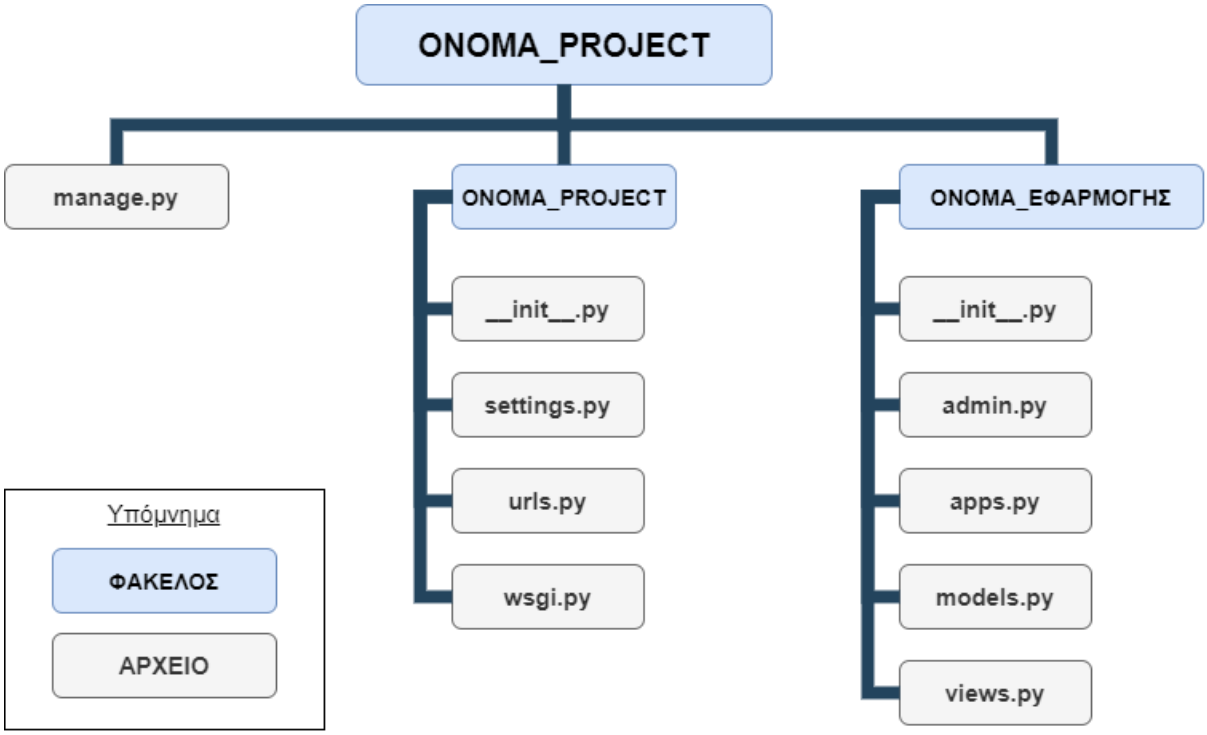
Το Django είναι ένα web framework γραμμένο σε Python το οποίο πρωτοεμφανίστηκε το 2005. Είναι ανοικτού κώδικα, διανέμεται δωρεάν μέσω του συστήματος διαχείρισης πακέτων της Python (pip), και αναβαθμίζεται περίπου ανά 8 μήνες. Ακολουθώντας το πρότυπο εκτενούς υποστήριξης, κάποιες από τις εκδόσεις χαρακτηρίζονται σαν Long Term Support (LTS) και υποστηρίζονται για 3 χρόνια.

Αντιλαμβανόμενοι το επαναλαμβανόμενο μοτίβο από εργαλεία και υπηρεσίες που χρειάζονται για την ανάπτυξη μιας λειτουργικής ιστοσελίδας, και συνδυάζοντας το με το μοντέλο σχεδίασης Model - View - Template οι δημιουργοί του Django απλοποίησαν σε πολύ μεγάλο βαθμό τις ενέργειες που απαιτούνται για την δημιουργία, τη διαχείριση και την αποσφαλμάτωση μιας ιστοσελίδας. Μεταξύ των διαδικασιών που διαχειρίζεται το Django, είναι αυτόματη δημιουργία των απαιτούμενων αρχείων για την δημιουργία μιας απλής ιστοσελίδας, η δυνατότητα διαχωρισμού διαφορετικών τμημάτων της σελίδας σε διαφορετικές εφαρμογές για την ευκολότερη διαχείριση τους, η αντιστοίχιση των αιτημάτων προς την κατάλληλη εφαρμογή και η προβολή του αντίστοιχου περιεχομένου, η διαχείριση των χρηστών και των δικαιωμάτων τους και η διαχείριση της βάσης δεδομένων καθώς και πολλές άλλες κρίσιμες λειτουργίες. Όλα αυτά γίνονται μέσα από ένα πλαίσιο το οποίο είναι δομημένο λαμβάνοντας υπόψη την ασφάλεια, την επεκτασιμότητα, την επαναχρησιμοποίηση και τη φορητότητα του κώδικα καθιστώντας το με αυτό τον τρόπο ιδιαίτερα δημοφιλές ακόμα και μεταξύ ιστοσελίδων όπως τα Instagram, Disqus, National Geographic κ.α.

Η εγκατάσταση του Django, η δημιουργία ενός νέου Project και η δημιουργία μιας νέας εφαρμογής εντός του Project γίνεται με τις ακόλουθες εντολές:

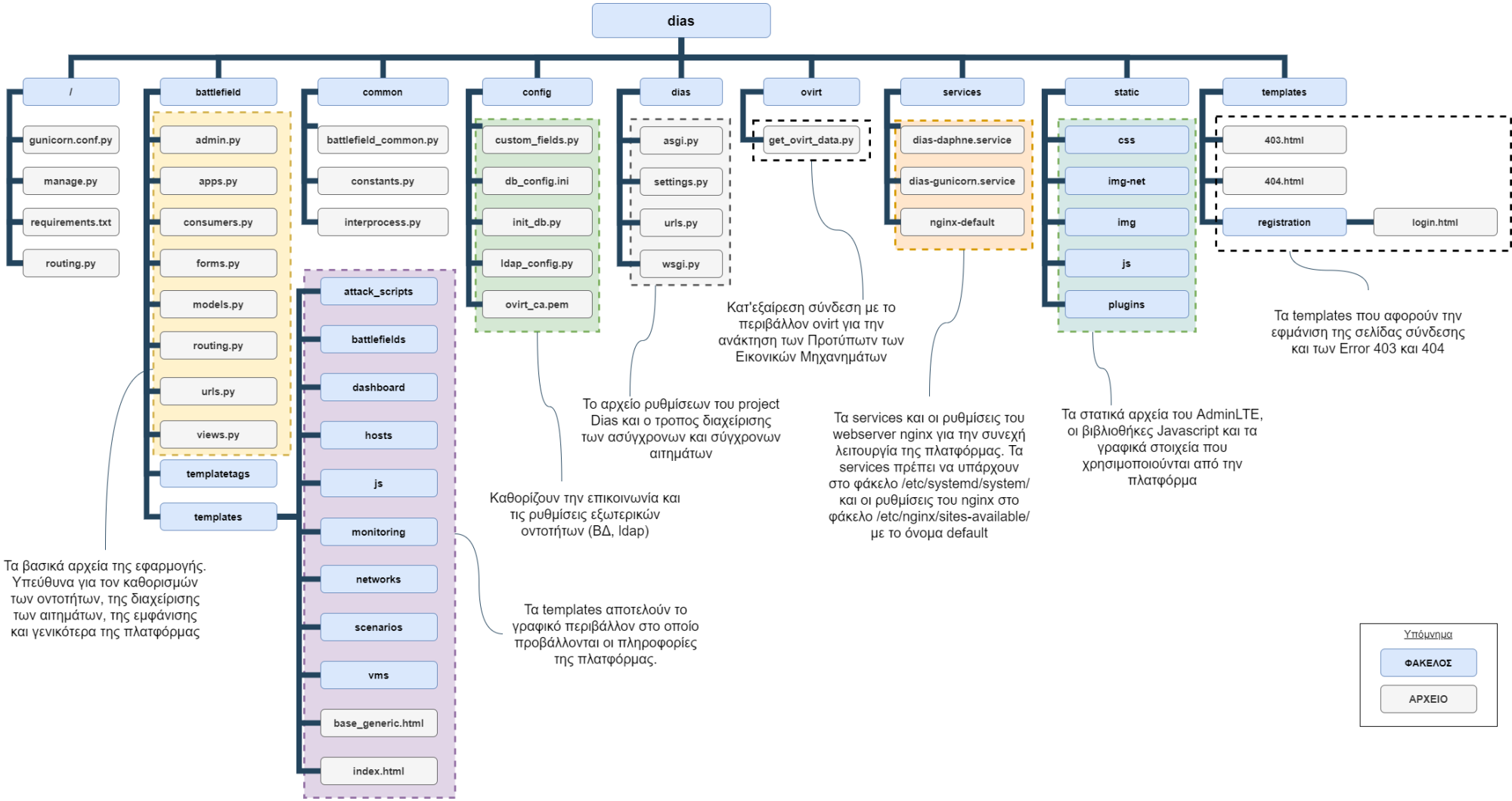
```
# Εγκατάσταση του django framework
pip install django
# Δημιουργία νέου Project
django-admin startproject ONOMA_PROJECT
# Από τον φάκελο του project τρέχουμε την ακόλουθη εντολή
# η οποία δημιουργεί μια νέα εφαρμογή
python3 manage.py startapp ONOMA_ΕΦΑΡΜΟΓΗΣ
```

Οι εντολές αυτές έχουν σαν αποτέλεσμα τη δημιουργία μιας δομής από τα απαραίτητα αρχεία, όπως αυτή της Εικόνα 2 που ακολουθεί.




**Εικόνα 2.** Τυπική δομή αρχείων ενός Django Project

Στην παρούσα διατριβή, δημιουργήθηκε το project Dias και εντός αυτού η εφαρμογή Battlefield η οποία αποτελεί το γραφικό περιβάλλον της πλατφόρμας διαχείρισης του ΨΠΒ. Όλη η δομή των αρχείων του project Dias φαίνεται στο διάγραμμα της Εικόνα 3 που ακολουθεί:




**Εικόνα 3.** Δομή αρχείων εφαρμογής Dias

### 8.1.2 AdminLTE

Αν και το Django αποτελεί ένα πολύ σημαντικό εργαλείο για τη δημιουργία της κεντρικής πλατφόρμας διαχείρισης περιεχομένου από μόνο του δεν μπορεί να μας εξασφαλίσει ούτε το Γραφικό Περιβάλλον ούτε τις αλληλεπιδράσεις με αυτό. Για τον λόγο αυτό χρειάζεται μια βιβλιοθήκη με τα κατάλληλα βοηθήματα για την δημιουργία τόσο του γραφικού περιβάλλοντος (UI) όσο και της εμπειρίας του χρήστη (UX).

Όπως και τα υπόλοιπα συστατικά που αποτελούν την πλατφόρμα έτσι και το περιβάλλον στο οποίο βασίζεται η απεικόνιση της πλατφόρμας, επιλέχθηκε με κύρια κριτήρια τον ανοικτό κώδικα και την ενεργή κοινότητα συντήρησης-υποστήριξης. Το AdminLTE, βασίζεται στο Bootstrap 4.6 και το πρόσθετο jQuery και διατίθεται με άδεια χρήσης MIT[2]. Η έκδοση που χρησιμοποιήθηκε στην παρούσα υλοποίηση είναι η 3.0.5, ενώ η έκδοση 3.1.0 κυκλοφόρησε στις 22 Μαρτίου 2021. Χρησιμοποιώντας τη βιβλιοθήκη Bootstrap, επιτυγχάνεται ένα περιβάλλον το οποίο μπορεί να χρησιμοποιηθεί το ίδιο εύχρηστα σε φορητές συσκευές με μικρές οθόνες αλλά και σε μεγάλες οθόνες σε κέντρα επιχειρήσεων. Επίσης είναι πλήρως συμβατό και ενσωματώνει μεγάλο αριθμό από άλλα δημοφιλή πρόσθετα τα οποία μπορούν να χρησιμοποιηθούν για την απεικόνιση γραφικών παραστάσεων, σελίδων καταχώρησης, διαδραστικών πινάκων κ.α.

## 8.2 Βάση Δεδομένων

Η βάση δεδομένων υλοποιείται σε ένα ξεχωριστό εικονικό μηχάνημα με λειτουργικό σύστημα Fedora και χρησιμοποιεί το Σύστημα Διαχείρισης Βάσης Δεδομένων (ΣΔΒΔ) MariaDB (έκδοση 10.3.18). Η ΒΔ χρησιμοποιείται από το σύνολο των εφαρμογών που αναπτύχθηκαν και σε αυτή αποθηκεύονται οι ακόλουθες πληροφορίες

a. Όλες οι απαραίτητες πληροφορίες για την λειτουργία του Django Framework (Χρήστες, Άδειες και Δικαιώματα, Αρχείο Ενεργειών κλπ)
b. Όλες οι πληροφορίες που αφορούν τα Εικονικά Πεδία Μάχης, συμπεριλαμβανομένων όλων των επί μέρους τμημάτων (Εικονικές

[2] https://opensource.org/licenses/MIT

Μηχανές, Δίκτυα, Δικτυακός Εξοπλισμός, Χρήστες των Εικονικών Μηχανών)

c. Όλες οι πληροφορίες που αφορούν τα Εικονικά Σενάρια Μάχης (Συμπεριλαμβανομένων των επιθέσεων και των διαμορφώσεων της κάθε επίθεσης)
d. Αρχείο καταγραφών των ενεργειών των χρηστών αλλά και των εικονικών μηχανημάτων.

Μετά την εγκατάσταση του ΣΔΒΔ τροποποιήθηκε κατάλληλα το τοίχος προστασίας ώστε να επιτρέπει την χρήση της ΒΔ από τις υπόλοιπες συσκευές του δικτύου και διαγράφηκαν οι ανώνυμοι χρήστες και η δοκιμαστική βάση δεδομένων, συμπεριλαμβανομένων των δικαιωμάτων πρόσβασης σε αυτή ώστε να αποφευχθούν ανεπιθύμητα περιστατικά ασφαλείας λόγω χρήσης των τυπικών ρυθμίσεων. Στη συνέχεια δημιουργήθηκε η βάση δεδομένων της πλατφόρμας και οι χρήστες με τα κατάλληλα δικαιώματα. Οι ανωτέρω ενέργειες υλοποιήθηκαν με τις εντολές:

```
# Εγκατάσταση του ΣΔΒΔ
dnf install mariadb-server
# Ενεργοποίηση της υπηρεσίας mariadb με την εκκίνηση του συστήματος
systemctl enable mariadb.service
# Εκκίνηση της υπηρεσίας mariadb
systemctl start mariadb.service
# Ρύθμιση τύχους προστασίας ώστε να επιτρέπει την επικοινωνία με την ΒΔ
sudo firewall-cmd --add-service=mysql --permanent
# Τροποποίηση των αρχικών ρυθμίσεων για καλύτερη ασφάλεια
# (Ορισμός κωδικού διαχειριστή, Διαγραφή δοκιμαστική ΒΔ, κλπ)
sudo mysql_secure_installation
# Εκκίνηση ΣΔΒΔ
mysql -p
# Ενδεικτικκή Δημιουργία χρήστών και ορισμός των δικαιωμάτων πρόσβασης
CREATE USER 'ΧΡΗΣΤΗΣ_1' IDENTIFIED BY 'ΚΩΔΙΚΟΣ_1';
GRANT SELECT ON `ΒΑΣΗ_ΔΕΔΟΜΕΝΩΝ.ΠΙΝΑΚΑΣ` TO `ΧΡΗΣΤΗΣ_1`@`%`;
GRANT INSERT ON `ΒΑΣΗ_ΔΕΔΟΜΕΝΩΝ.ΠΙΝΑΚΑΣ_2` TO `ΧΡΗΣΤΗΣ_1`@`%`;
...

# Ενδεικτικκή Δημιουργία διαχειριστή με όλα τα δικαιώματα πρόσβασης
CREATE USER `ΔΙΑΧΕΙΡΙΣΤΗΣ_1` IDENTIFIED BY 'ΚΩΔΙΚΟΣ_2';
GRANT ALL privileges ON `ΒΑΣΗ_ΔΕΔΟΜΕΝΩΝ`.* TO `ΔΙΑΧΕΙΡΙΣΤΗΣ_1`@`%`;

# Ανανέωση των δικαιωμάτων πρόσβασης
FLUSH PRIVILEGES;
```

### 8.2.1 Δομή Βάσης Δεδομένων

Η δομή της βάσης δεδομένων μπορεί να διαχωριστεί νοητά σε 2 τμήματα. Το τμήμα που περιέχει τις πληροφορίες που αφορούν το Django, που αποτελείται από 10 πίνακες και το Τμήμα με τις πληροφορίες της πλατφόρμας που αποτελείται από 34 πίνακες. Από τους 34 πίνακες οι 30 είναι οι πίνακες για κάθε μία ξεχωριστή οντότητα της ΒΔ, ενώ οι υπόλοιποι 4 είναι πίνακες που χρησιμοποιούνται για την υλοποίηση σχέσεων Many To Many. Στο σύνολο της η ΒΔ περιλαμβάνει 44 Πίνακες οι οποίοι φαίνονται στο Παράρτημα Β.

### 8.2.2 Διασύνδεση ΒΔ - Django

Με την ολοκλήρωση της δημιουργίας της ΒΔ και των δικαιωμάτων χρήσης της, τροποποιήθηκε κατάλληλα το αρχείο ρυθμίσεων του Django ώστε να γίνει η απαραίτητη διασύνδεση μεταξύ της ΒΔ και του CMS. Οι αλλαγές που έγιναν το αρχείο settings.py του Django είναι οι ακόλουθες:

```
import os

# Τροποποίηση της μεταβλητής DATABASES:
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
    'OPTIONS': {
            'read_default_file': os.path.join(BASE_DIR, 'config/db_conf
ig.ini'),
        },
    }
}
```

Στη συνέχεια δημιουργήθηκε το αρχείο db_config.ini στο φάκελο config ώστε να διαχωριστούν οι κωδικοί πρόσβασης από τα αρχεία ρυθμίσεων, μια κοινή πρακτική που ακολουθείτε για την καλύτερη διαφύλαξη των κωδικών ασφαλείας:

```
[client]
# Στοιχεία πρόσβασης στη ΒΔ
database=urn
host=10.8.9.252
port=3306
user=username
password=password
```

Με την σύνδεση της εφαρμογής Django, στην ΒΔ και χρησιμοποιώντας τις ακόλουθες εντολές από τον φάκελο διαχείρισης της εφαρμογής Django, δημιουργούνται όλοι οι απαραίτητοι πίνακες για την διαχείριση του Django backend αλλά και όλες οι οντότητες που αφορούν την πλατφόρμα και δηλώθηκαν σαν μοντέλα στο περιβάλλον Django μέσω του αρχείου models.py της εφαρμογής Battlefield.

```
python manage.py makemigrations
python manage.py migrate --run-syncdb
```

Στη συνέχεια με την εντολή create superuser, δημιουργείται ένας διαχειριστής της εφαρμογής Django, ο οποίος μπορεί να εκτελέσει κάθε είδους ενέργεια είτε αυτή αφορά ρύθμιση της εφαρμογής είτε ενέργεια επί των οντοτήτων της πλατφόρμας.

```
python manage.py createsuperuser
```

Ακολούθως απαιτείται η εκτέλεση μία φορά της εντολής

```
python manage.py shell < config/init_db.py
```

ώστε να αρχικοποιηθεί η ΒΔ με κάποιες αρχικές τιμές και να δημιουργηθούν οι ομάδες και τα δικαιώματα των χρηστών.

Ένας πολύ σημαντικός περιορισμός της υλοποίησης του Django, ο οποίος πρέπει να ληφθεί υπόψη είναι ότι κατά την δήλωση των χαρακτηριστικών της κάθε οντότητας ενώ μπορούν να οριστούν σχέσεις και περιορισμοί μεταξύ των οντοτήτων, κάποιες από αυτές λαμβάνονται υπόψη μόνο από το Σύστημα Διαχείρισης Βάσης Δεδομένων του Django και δεν μεταβιβάζονται στην Βάση Δεδομένων. Αυτό συμβαίνει για την εξασφάλιση μεγαλύτερης ευελιξίας όσο αφορά τους υποστηριζόμενους τύπους βάσης δεδομένων που μπορούν να χρησιμοποιηθούν από το Djano, ωστόσο σε περίπτωση που χρησιμοποιείται κατευθείαν η ΒΔ για επεξεργασία των δεδομένων μπορεί να δημιουργήσει προβλήματα στην πλατφόρμα.

### 8.2.3 Λειτουργία Event Scheduler

Μια επίσης σημαντική ρύθμιση της βάσης δεδομένων είναι η ενεργοποίηση και η χρήση των συμβάντων (events) μέσω της λειτουργίας Event Scheduler. Η ρύθμιση αυτή παρέχει την δυνατότητα αυτόματου τερματισμού των σεναρίων μετά την παρέλευση

του χρόνου διάρκειας τους. Η ενεργοποίηση αυτής της ρύθμισης έγινε τροποποιώντας το αρχείο ρυθμίσεων του ΣΔΒΔ /etc/my.cnf ως ακολούθως:

```
[mysqld]
event_scheduler = on
```

Ενεργοποιώντας τον scheduler, μπορούν πλέον να δημιουργηθούν εγγραφές στον πίνακα events, οι οποίες σε συγκεκριμένο χρόνο αλλάζουν την κατάσταση του σεναρίου από active σε completed. Ένα τέτοιο event μπορεί να καταχωρηθεί με τον πιο κάτω κώδικα:

```
CREATE EVENT `%s`
ON SCHEDULE AT CURRENT_TIMESTAMP + INTERVAL %s DAY + INTERVAL %s HOUR +
 INTERVAL %s MINUTE
DO
    BEGIN
        INSERT INTO battlefield_scenariostate (scenario_id, state_id, t
imestamp, results) VALUES (%s, %s, CURRENT_TIMESTAMP(),"");
        INSERT INTO battlefield_battlefieldstate (battlefield_id, state
_id, timestamp) VALUES (%s, %s, CURRENT_TIMESTAMP());
        INSERT INTO battlefield_log (message,battlefield_id, log_type_i
d,log_level,submitted_by,timestamp) VALUES (%s, %s, %s, %s, %s, CURRENT
_TIMESTAMP());
    END
```

## 8.3 Δικαιώματα Χρηστών

Τα δικαιώματα των χρηστών καθορίζονται βάση των ομάδων στις οποίες ανήκει ο χρήστης στον εξυπηρετητή FreeIPA. Για τον σκοπό αυτό οι ομάδες αυτές συγχρονίζονται αυτόματα με αντίστοιχες ομάδες που δημιουργήθηκαν κατά την αρχικοποίηση της ΒΔ στο περιβάλλον Django και συγχρονίζονται κάθε φορά που ο χρήστης συνδέεται μέσω της εφαρμογής Dias.

Το περιεχόμενο που προβάλλεται στις σελίδες και οι ενέργειες που μπορεί να εκτελέσει ο κάθε χρήστης διαφοροποιείται ανάλογα με τα δικαιώματα του. Η αντιστοίχιση των ομάδων με τα δικαιώματα των χρηστών φαίνεται στον Πίνακας 1 που ακολουθεί:

| Ομάδα FREEIPA | DIAS Django permissions | Δικαιώματα στην πλατφόρμα |
|---|---|---|
| dias_admins | | Superadmin – Πλήρης πρόσβαση σε όλες τις λειτουργίες που αφορούν τα ΕΠΜ, τα Σενάρια και τις επιθέσεις |
| dias_scenario_admins | add_logentry<br>view_host<br>add_scenario<br>view_scenario<br>change_scenario<br>delete_scenario<br>add_hostuser<br>view_hostuser<br>change_hostuser<br>delete_hostuser<br>add_attack<br>view_attack<br>change_attack<br>delete_attack<br>add_scenario_state<br>view_scenario_state<br>change_scenario_state<br>delete_scenario_state | Δυνατότητα Δημιουργίας, Επεξεργασίας, Διαγραφής, Προετοιμασίας, Εκκίνησης και Τερματισμού Σεναρίων |
| dias_scenario_managers | add_logentry<br>view_host<br>view_scenario<br>add_scenario_state<br>view_scenario_state | Δυνατότητα Προετοιμασίας, Εκκίνησης και Τερματισμού Σεναρίων<br>Δυνατότητα Προβολής των διάφορων Εικονικών Μηχανών |
| dias_attackscript_admins | add_logentry<br>view_attackscript<br>add_attackscript<br>change_attackscript<br>view_attackvariable<br>add_attackvariable<br>change_attackvariable | Δυνατότητα Προβολής και Δημιουργίας Νέων Προτύπων Επίθεσης<br>Διαγραφή μπορεί να γίνει μόνο από διαχειριστή |
| dias_players | add_logentry<br>view_scenario | Δυνατότητα εισόδου εντός της πλατφόρμας, επισκόπησης των πληροφοριών που αφορούν τα σενάρια στα οποία συμμετέχει και χρήσης εικονικού μηχανήματος σε περίπτωση που του έχει διατεθεί. |

**Πίνακας 1.** Ομάδες και Δικαιώματα Χρηστών

## 8.4 Παρακολούθηση Εξέλιξης Σεναρίων

Η παρακολούθηση των συμβάντων σε πραγματικό χρόνο γίνεται με τη μεταφορά δεδομένων από τις επιμέρους εφαρμογές με την χρήση συνδέσεων websocket. Η επιλογή της χρήσης των websocket έγινε γιατί προσφέρουν τη δυνατότητα πολλαπλών συνδέσεων και σε συνδυασμό με την τεχνολογία AJAX (Asynchronous Javascript and XML) η απεικόνιση γίνεται σχεδόν σε πραγματικό χρόνο χωρίς την ανάγκη για ανανέωση της ιστοσελίδας από τον χρήστη.

### 8.4.1 Συνδέσεις Websocket

Το websocket είναι ένα πρωτόκολλο, αμφίδρομης επικοινωνίας στο OSI Layer 7 το οποίο όπως και το http βασίζεται σε συνδέσεις TCP. Το βασικό του πλεονέκτημα έναντι του http, είναι ότι παρέχει τη δυνατότητα αμφίδρομης επικοινωνίας πραγματικού χρόνου χωρίς την απαίτηση για ερώτημα από τον χρήστη. Η δυνατότητα αυτή σε συνδυασμό με άλλες τεχνολογίες που χρησιμοποιούνται για την δημιουργία ιστοσελίδων, όπως η γλώσσα προγραμματισμού Javascript, είναι πολύ σημαντικές σε διαδραστικές εφαρμογές που λαμβάνουν και παρουσιάζουν δεδομένα σε πραγματικό χρόνο από διαφορετικές πηγές χωρίς την απαίτηση για περεταίρω ενέργειες από τον χρήστη όπως για παράδειγμα ανανέωση της ιστοσελίδας.

Η έναρξη επικοινωνίας websocket, γίνεται μέσω του πρωτοκόλλου http στη θύρα 80, ή 443 αν υποστηρίζεται κρυπτογράφηση, με χρήση της επικεφαλίδας upgrade, η οποία χρησιμοποιείται για να αλλάξει τον τρόπο επικοινωνίας. Για την επικοινωνία μέσω websocket, χρησιμοποιούνται τα URI, ws:// και wss:// σε αντιστοιχία με τα http:// και https://.

### 8.4.2 Αρχείο Καταγραφών Βάσης Δεδομένων

Η δομή της ΒΔ, είναι τέτοια ώστε να μπορεί να χρησιμοποιηθεί για την αναπαραγωγή προηγούμενων σεναρίων. Οι καταστάσεις (states) τις οποίες μεταβαίνουν οι οντότητες καταγράφονται χρησιμοποιώντας χρονοσφραγίδες σε πίνακες καταστάσεων ανά οντότητα, παρέχοντας έτσι τη δυνατότητα για εντοπισμό της κατάστασης που βρισκόταν η κάθε οντότητα ανά πάσα στιγμή. Επίσης όλες οι πληροφορίες οι οποίες λαμβάνονται μέσω websocket για απεικόνιση στο περιβάλλον παρακολούθησης

πραγματικού χρόνου καταγράφονται στον πίνακα καταγραφών (battlefield_log) μαζί με τον αποστολέα τους. Συνδυάζοντας τα πιο πάνω η ΒΔ με τις πληροφορίες που διαθέτει μπορεί να χρησιμοποιηθεί για πιστή αναπαραγωγή της εξέλιξης του σεναρίου χωρίς την απαίτηση της χρήσης των εικονικών μηχανημάτων που συμμετείχαν σε αυτό.

### 8.4.3 Extended Monitoring

Για την συλλογή των συμβάντων ασφαλείας από τον Wazuh Manager, απαιτείται η χρήση συγκεκριμένης υπηρεσίας από τους Wazuh Agents ώστε να εξουσιοδοτηθούν για την αποστολή των συμβάντων. Η υπηρεσία αυτή χρησιμοποιώντας τη θύρα 1515 και το πρωτόκολλο TCP δημιουργεί μια ασφαλή σύνδεση TLS μέσω της οποίας ο Wazuh Agent λαμβάνει ένα μοναδικό κλειδί το οποίο θα χρησιμοποιεί στη συνέχεια για την ασφαλή αποστολή των συμβάντων. Η αποστολή των συμβάντων από τους Agents προς το Wazuh Manager γίνεται μέσω της θύρας 1514 και του πρωτόκολλου UDP.

Ο Wazuh Agent (v.3.9.5-1) είναι προ-εγκατεστημένος στα πρότυπα εικονικών μηχανών, και έχει γίνει η κατάλληλη ρύθμιση με τη διεύθυνση IP του Manager (MANAGER_IP), στο αντίστοιχο αρχείο ρυθμίσεων (/var/ossec/etc/oosec.conf).

Για την εγγραφή του κάθε Agent στον Wazuh Manager εκτελείτε μέσω του Bastion Host, κατά την πρώτη εκκίνηση μετά τη δημιουργία της εικονικής μηχανής η εντολή:

```
/var/ossec/bin/agent-auth -m <manager_IP> -A $BF_DEVICE_NAME
```

Η μεταβλητή $BF_DEVICE_NAME αποτελεί environment variable που αποθηκεύεται κατά την δημιουργία της εικονικής μηχανής. Μα αυτό τον τρόπο ο κάθε Agent αναφέρει τα συμβάντα του χρησιμοποιώντας το συγκεκριμένο χαρακτηριστικό το οποίο χρησιμοποιείται επίσης για τη διαγραφή Agent από τον Manager κατά την καταστροφή της εικονικής μηχανής

## 8.5 Επικοινωνία

Η επικοινωνία και η ανταλλαγή δεδομένων μεταξύ των διαφόρων τμημάτων και εφαρμογών της πλατφόρμας υλοποιείται με συνδυασμό της χρήσης του δικτυακού

εξοπλισμού με πρωτόκολλα και υπηρεσίες επικοινωνίας όπως για παράδειγμα τα websocket και οι συνδέσεις ssh.

### 8.5.1 Δρομολογητής Διαχείρισης (Management Router)

Για την επίτευξη κεντρικής διαχείρισης και παρακολούθησης της δρομολόγησης του συνόλου των Πεδίων Μάχης, επιλέχθηκε η χρήση ενός κεντρικού δρομολογητή, στον οποίο διασυνδέονται όλοι οι υπόλοιποι δρομολογητές των ΕΠΜ ανεξάρτητα από τις υπόλοιπες τους συνδέσεις. Ο δρομολογητής αυτός υλοποιήθηκε ως εικονική μηχανή χρησιμοποιώντας το πρότυπο dias_neth_rt. Το πρότυπο αυτό όπως αναφέρθηκε και προηγουμένως, έχει εγκατεστημένη διανομή Nethserver που βασίζεται στο Centos 7. Μέσω της διανομής Nethserver, παρέχεται η δυνατότητα για εύκολη διαχείριση των δυνατοτήτων της εικονικής μηχανής, και κυρίως των ρυθμίσεων και των υπηρεσιών του δικτύου μέσω χρησιμοποιώντας ένα web περιβάλλον μέσω της θύρας 980 (tcp).

Ο συγκεκριμένος δρομολογητής αποτελεί τον κόμβο μεταξύ της πλατφόρμας, και ενός δικτύου VPN του πανεπιστημίου. Χρησιμοποιώντας τους κατάλληλους κανόνες στο τοίχος προστασίας τόσο του συγκεκριμένου δρομολογητή επιτρέπεται η πρόσβαση στους χρήστες του VPN, στην πλατφόρμα.

#### *8.5.1.1 Bastion Host*

Εκτός από τον έλεγχο της δρομολόγησης, ο συγκεκριμένος δρομολογητής χρησιμοποιείται και σαν πύλη πρόσβασης προς όλες τις Εικονικές Μηχανές των ΕΠΜ. Λόγω των περιορισμών που υπάρχουν μεταξύ των διαφόρων δικτύων για την όσο το δυνατό πιο πιστή προσομοίωση της κυκλοφορίας, αλλά και για την διατήρηση της ασφάλειας της υποδομής του συστήματος η κατευθείαν πρόσβαση από και προς τις Εικονικές Μηχανές των ΕΠΜ είναι αδύνατη. Χρησιμοποιώντας την δυνατότητα της αναπήδησης μεταξύ κόμβων (proxy jump, -J) που προσφέρει το SSH, μπορεί να επιτευχθεί σύνδεση στις Εικονικές Μηχανές των ΕΠΜ, μέσω αναπήδησης όπου πρωτεύον κόμβος είναι ο δρομολογητής διαχείρισης. Στην παρούσα εργασία η υλοποίηση έγινε χρησιμοποιώντας την βιβλιοθήκη jumpssh (v1.6.5) της Python.

```
from jumpssh import SSHSession

# δημιουργία νέας σύνδεσης στον δρομολογητή διαχείρισης
gw1_ses = SSHSession(constants.MGMT_ROUTER, ROOT_USERNAME, password=ROO
T_PASSWORD).open()

# χρήση της σύνδεσης του δρομολογητή διαχείρισης για δημιουργία νέας σύ
νδεσης στον δρομολογητή του συγκεκριμένου Π.Μ
gw2_ses = gw1_ses.get_remote_session(mgmt_ip, username= ROOT_USERNAME,
password=ROOT_PASSWORD)
# σύνδεση σε συγκεκριμένο τερματικό του ΠΜ χρησιμοποιώντας τις δύο προη
γούμενες συνδέσης
remote_ses = gw2_ses.get_remote_session(active_ip, username=ROOT_USERNA
ME, password=ROOT_PASSWORD, port=PORT)
# εκτέλεση εντολής στο συγκεκριμένο τερματικό –
 εδώ για παράδειγμα καταχώρηση του Wazuh Agent για το συγκεκριμένο τερμ
ατικό στον Wazuh Manager
remote_ses.get_cmd_output(f'sudo /var/ossec/bin/agent-auth -
m {constants.WAZUH_MANAGER} -A {agent_name}')
```

### 8.5.2 Επικοινωνία Εφαρμογής Dias και FreeIPA

Η επικοινωνία μεταξύ της εφαρμογής Dias και της πλατφόρμας FreeIPA για την αυθεντικοποίηση και τα δικαιώματα των χρηστών γίνεται χρησιμοποιώντας τα πρόσθετα python-ldap (έκδοση 3.3.1) και django-auth-ldap (έκδοση 2.2.0). Για την λειτουργία των συγκεκριμένων προσθέτων είναι απαραίτητη η εγκατάσταση των βιβλιοθηκών python-dev, libldap2-dev, libsasl2-dev και libssl-dev. Η εγκατάσταση των προαπαιτούμενων γίνεται με τις εντολές:

```
apt install libldap2-dev python-dev libsasl2-dev libssl-dev
# Για Ubuntu 20.04:
pip install python3-ldap
# Για προηγούμενες εκδόσεις
pip install python-ldap

pip install django-auth-ldap
```

Αφού ολοκληρωθεί η εγκατάσταση, πρέπει να γίνουν οι απαραίτητες τροποποιήσεις στο αρχείο settings.py του Django project Dias ώστε να καθοριστεί το domain στο οποίο θα γίνεται η αυθεντικοποίηση και να καθοριστούν οι υπόλοιπες ρυθμίσεις για τα δικαιώματα των χρηστών. Ο κώδικας που είναι υπεύθυνος για το σύνολο των λειτουργιών της διασύνδεσης μεταξύ Dias και FreeIPA είναι ο ακόλουθος:

```
from django_auth_ldap.config import LDAPSearch, GroupOfNamesType, LDAPG
roupQuery
import ldap

# ldap server
AUTH_LDAP_SERVER_URI = 'ldap://LDAP_SERVER_HOST_OR_IP:389'

# ldap bind password
AUTH_LDAP_BIND_PASSWORD = 'ΚΩΔΙΚΟΣ'

# user search
AUTH_LDAP_USER_SEARCH = LDAPSearch(
    'cn=users,cn=accounts,dc=sec,dc=ouc,dc=ac,dc=cy',
    ldap.SCOPE_SUBTREE,
    '(uid=%(user)s)',
)

# domain controller group search
AUTH_LDAP_GROUP_SEARCH = LDAPSearch(
    'dc=sec,dc=ouc,dc=ac,dc=cy',
    ldap.SCOPE_SUBTREE,
    "(objectClass=groupOfNames)",
)
AUTH_LDAP_GROUP_TYPE = GroupOfNamesType()

AUTH_LDAP_USER_FLAGS_BY_GROUP = {
    # Αν ο χρήστης ανήκει στην ομάδα dias_admins τότε γίνεται superuser
 και stuff αυτόματα
    "is_staff": "cn=dias_admins,cn=groups,cn=accounts,dc=sec,dc=ouc,dc=
ac,dc=cy",
    "is_superuser": "cn=dias_admins,cn=groups,cn=accounts,dc=sec,dc=ouc
,dc=ac,dc=cy",
}
# Μόνο χρήστες που ανήκουν στις συγκεκριμένες ομάδες μπορούν να
συνδεθούν
AUTH_LDAP_REQUIRE_GROUP = (
    LDAPGroupQuery("cn=dias_admins,cn=groups,cn=accounts,dc=sec,dc=ouc,
dc=ac,dc=cy")
    | LDAPGroupQuery("cn=dias_scenario_admins,cn=groups,cn=accounts,dc=
sec,dc=ouc,dc=ac,dc=cy")
    | LDAPGroupQuery("cn=dias_scenario_managers,cn=groups,cn=accounts,d
c=sec,dc=ouc,dc=ac,dc=cy")
    | LDAPGroupQuery("cn=dias_attackscript_admins,cn=groups,cn=accounts
,dc=sec,dc=ouc,dc=ac,dc=cy")
    | LDAPGroupQuery("cn=dias_players,cn=groups,cn=accounts,dc=sec,dc=o
uc,dc=ac,dc=cy")
)
```

```
# Οι ομάδες που αντιγράφονται στους πίνακες του Django
AUTH_LDAP_MIRROR_GROUPS = [
"dias_admins",
"dias_scenario_admins",
"dias_scenario_managers",
"dias_attackscript_admins",
"dias_players",
]

# Συγχρονισμός και ανανέωση των ομάδων κάθε φορά που ένας χρήστης συνδέ
εται
AUTH_LDAP_ALWAYS_UPDATE_USER=True
AUTH_LDAP_CACHE_GROUPS = False
AUTH_LDAP_BIND_AS_AUTHENTICATING_USER = True
```

Όπως και προηγουμένως για την αποφυγή της ενσωμάτωσης κωδικών στο αρχείο ρυθμίσεων, ο συγκεκριμένος κώδικας μεταφέρθηκε σε ξεχωριστό αρχείο (config/ldap_config.py) και εισάγεται εντός του settings.py με python import:

```
from config.ldap_config import *
```

### 8.5.3 Επικοινωνία Εφαρμογών Dias-Sinon

Λόγω της ιδιαιτερότητας της επικοινωνίας που απαιτείται για την εκτέλεση των αυτοματοποιημένων επιθέσεων, όλες οι ενέργειες τόσο από την εφαρμογή Dias προς την εφαρμογή Sinon όσο και το αντίστροφο, καταχωρούνται στην βάση δεδομένων σε συγκεκριμένους πίνακες και χρησιμοποιούνται όποτε απαιτηθεί.

Οι ιδιαιτερότητες που προκύπτουν σε αυτή την επικοινωνία είναι λόγω του ότι οι εικονικές μηχανές στις οποίες είναι εγκατεστημένη η εφαρμογή Sinon, μπορεί να είναι σε οποιαδήποτε κατάσταση (απενεργοποιημένες, σε διαδικασία εκκίνησης ή τερματισμού) και να μην έχουν άμεση επικοινωνία με τον εξυπηρετητή. Αποθηκεύοντας διαδοχικά όλες τις ενέργειες που αφορούν την κάθε εικονική μηχανή σε ένα πίνακα στη βάση δεδομένων μπορεί η κάθε εικονική μηχανή να γνωρίζει σε ποια ακριβώς φάση βρίσκεται το σενάριο και να εκδηλώνει τις απαιτούμενες ενέργειες.

Επιπρόσθετα με αυτή την υλοποίηση, παρέχεται η δυνατότητα τήρησης αρχείου καταγραφής αφού όλες οι ενέργειες που εκτελούν οι εικονικές μηχανές όσο και τα αποτελέσματα τους καταγράφονται με χρονο-σφραγίδες. Αυτό έχει σαν αποτέλεσμα την τήρηση λεπτομερούς ημερολογίου για τον τρόπο εξέλιξης του σεναρίου.

### 8.5.4 Προώθηση καταγραφών στην εφαρμογή Hermes

Για την προώθηση των αρχείων καταγραφών από τον Wazuh Manager και την εφαρμογή Suricata στην εφαρμογή Hermes στην εικονική μηχανή που βρίσκονται εγκατεστημένες οι εν λόγω εφαρμογές έγινε εγκατάσταση της εφαρμογής syslog-ng (v 3.5.6). Η εφαρμογή syslog-ng χρησιμοποιείται για την συλλογή των καταγραφών περιστατικών ασφαλείας από το αρχείο που βρίσκεται στην τοποθεσία /var/ossec/logs/alerts/alerts.json και την προώθηση τους στην εφαρμογή Hermes. Για την επίτευξη αυτής της προώθησης στο αρχείο ρυθμίσεων του syslog-ng που βρίσκεται στην τοποθεσία /etc/syslog-ng/syslog-ng.conf προστέθηκε ως πηγή το συγκεκριμένο αρχείο καταγραφών και ως έξοδος η εφαρμογή Hermes (log_to_ws.py).

```
source s_wazuh_alerts {
     file("/var/ossec/logs/alerts/alerts.json"
     flags(no-parse)
     );
};
parser p_json { json-parser(prefix(".json.")); };

destination d_remote {
     program("/root/hermes/hermes/log_to_ws.py -u"
     template("$(format-json --scope dot-nv-pairs)\n")
     flags(no_multi_line)
     flush_lines(1)
     flush_timeout(1000)
     );
};
log { source(s_wazuh_alerts); parser(p_json); destination(d_remote); };
```

# Κεφάλαιο 9

# Κωδικοποίηση Εφαρμογών

Σε αυτό το κεφάλαιο περιγράφεται ο τρόπος λειτουργίας των εφαρμογών και παρουσιάζονται κάποια από τα σημαντικότερα τμήματα του κώδικα και των πληροφοριών που τις αποτελούν. Λόγω του μεγάλου αριθμού αρχείων, αλλά και του μεγέθους του κώδικα αυτός δεν έχει ενσωματωθεί στην παρούσα εργασία σαν παράρτημα αλλά θα υποβληθεί ξεχωριστά σε ψηφιακό μέσο.

## 9.1 Εφαρμογή Dias

Η εφαρμογή Dias αποτελεί το Περιβάλλον Δημιουργίας Εικονικών Πεδίων Μάχης και Σεναρίων και βασίζεται στο web framework Django και την βιβλιοθήκη AdminLTE για την δημιουργία του γραφικού περιβάλλοντος.

Αποτελείτε από τις ακόλουθες κύριες προβολές:

1. Την Σελίδα Σύνδεσης Χρήστη (Login Page)
2. Την Αρχική Σελίδα (Dashboard)
3. Τα Εικονικά Πεδία Μάχης (Battlefields)
4. Τα Πρότυπα Επιθέσεων (Attack Scripts)
5. Τα Σενάρια (Scenarios)
6. Παρακολούθηση Συστημάτων (Monitoring)

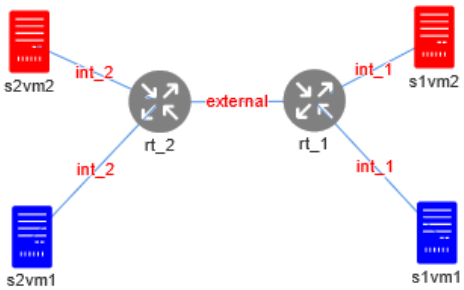
Η αυθεντικοποίηση των χρηστών για την σύνδεση στην πλατφόρμα μπορεί να γίνει είτε χρησιμοποιώντας την ενσωματωμένη λειτουργία διαχείρισης χρηστών του Django είτε μέσω ενός διακομιστή FreeIPA που υποστηρίζει συνδέσεις με την χρήση του πρωτοκόλλου LDAP. Μετά την εισαγωγή του ονόματος χρήστη και του κωδικού,

αποστέλλεται στον διακομιστή ένα ερώτημα σχετικά με την εγκυρότητα των συγκεκριμένων συνθηματικών. Ο εξυπηρετητής ελέγχει την βάση δεδομένων του και επιστρέφει μια απάντηση η οποία περιλαμβάνει όλα τα στοιχεία που αφορούν τον συγκεκριμένο χρήστη ή στην περίπτωση που είναι λανθασμένα ένα αντίστοιχο μήνυμα.

Μόλις φτάσει η απάντηση γίνεται έλεγχος και εφόσον ο συγκεκριμένος χρήστης βρίσκεται ήδη στη ΒΔ ανανεώνονται τυχόν αλλαγές που έχουν προκύψει στα δικαιώματα του, σε αντίθετη περίπτωση μια νέα εγγραφή καταχωρείται στη ΒΔ.

Στη συνέχεια ο χρήστης αναλόγως των δικαιωμάτων του μπορεί να χρησιμοποιήσει την πλατφόρμα εκτελώντας τις αντίστοιχες ενέργειες όπως αυτές περιγράφονται στον Εγχειρίδιο Χρήσης στο Παράρτημα Δ.

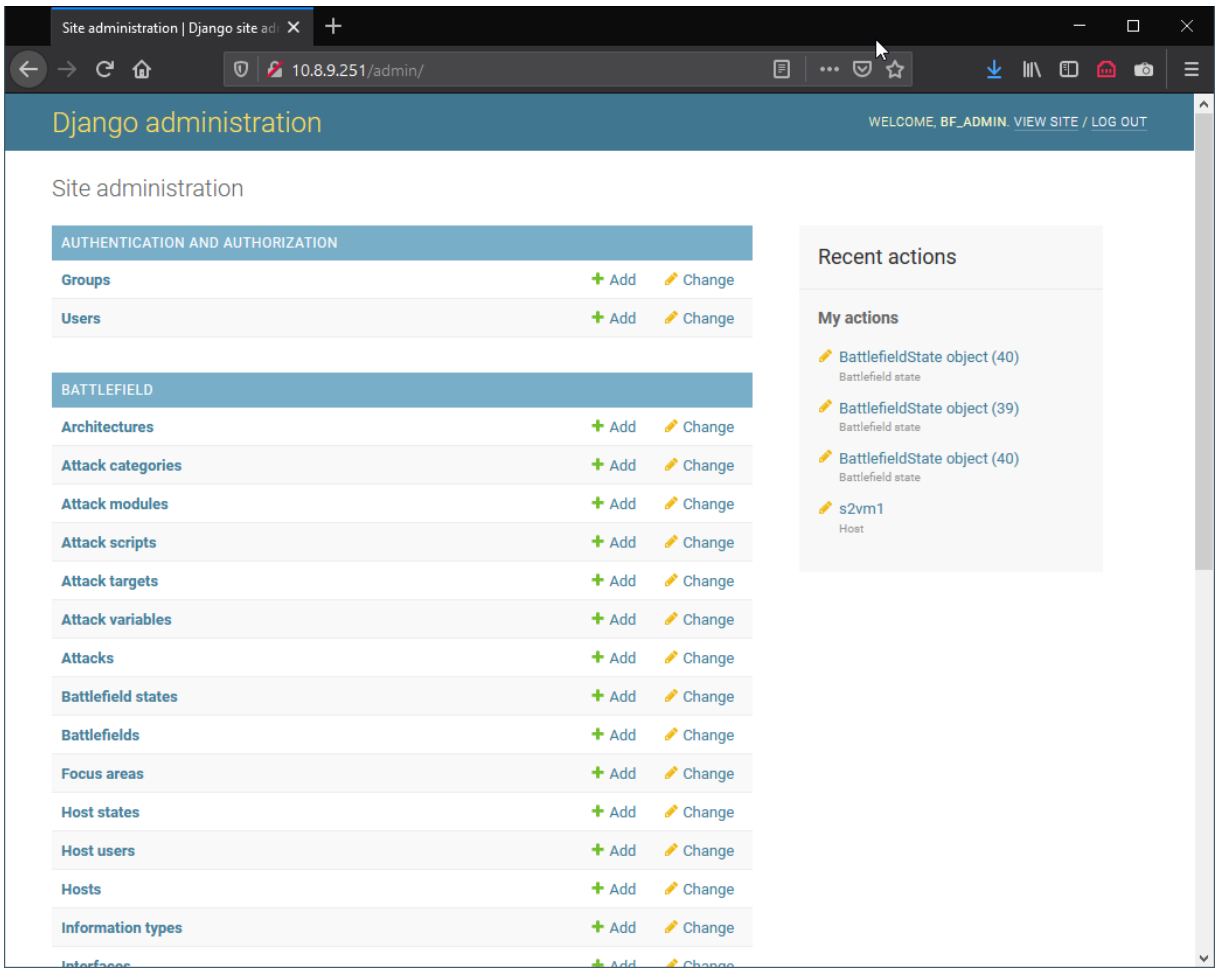
Για την υλοποίηση της εφαρμογής δημιουργήθηκαν 30 οντότητες (Models) που αποτελούν τον κορμό των δεδομένων τα οποία μπορούν να εισαχθούν και να διαχειριστούν από την εφαρμογή. Κατά την δημιουργία των οντοτήτων λήφθηκαν υπόψη τα ξεχωριστά χαρακτηριστικά, ανάγκες και απαιτήσεις της κάθε οντότητας και εκτός από τα κύρια πεδία τα οποία περιγράφουν την κάθε οντότητα δημιουργήθηκαν και οι αντίστοιχες βοηθητικές συναρτήσεις. Ένα χαρακτηριστικό παράδειγμα αποτελεί η οντότητα battlefield, η οποία αν και περιλαμβάνει 7 πεδία δεδομένων, με απαίτηση για συμπλήρωση από τον χρήστη μόνο του τίτλου και της περιγραφής, περιλαμβάνει επίσης 21 συναρτήσεις οι οποίες χρησιμοποιούνται για την καλύτερη ενσωμάτωση και διαχείριση της οντότητας. Μια από τις σημαντικότερες από αυτές τις συναρτήσεις είναι η get_vis_object, η οποία είναι υπεύθυνη για την δημιουργία του γραφήματος του Πεδίου Μάχης λαμβάνοντας υπόψη όλες τις συσκευές που το αποτελούν. Η συνάρτηση αυτή επιστρέφει τις απαραίτητες πληροφορίες σε μορφή JSON οι οποίες στη συνέχεια λαμβάνονται από τη βιβλιοθήκη vis-network.js στο αντίστοιχο html template και προβάλλονται με τον συνδυασμό Javascript και HTML.




**Εικόνα 4.** Γράφημα Δικτύου

```
def get_vis_object(self):
        networks = Network.objects.filter(battlefield_id_id=self.id)
        routers = Router.objects.filter(battlefield_id=self.id)
        hosts = Host.objects.filter(battlefield_id=self.id)
        # used for nodes numbering and linking
        index=0
        # the routers and the hosts
        nodes = []
        # the links between the nodes
        links = []
        nets = {}
        link_length=120
        for router in routers:
            index+=1
            nodes.append({"id":index, "label":router.name,  "shape": "i
con",  "icon": { "face": "next-
font", "code": "\ue61c",  "size": 50,  "color": "grey"}})
            interfaces = Interface.objects.filter(router_id_id=router.i
d)
            for interface in interfaces:
                # get interface's network
                network = Network.objects.get(id=interface.network_id_i
d).name.lower()
                # if the current network exists then link the current n
ode to the corresponding node
                if(network in nets):
                    links.append({"from":index, "to":nets[network],"la
bel":network, "length":link_length , "font": { "color": "#ff0000" }})
                # otherwise save a reference to the current node for th
is network
                else:
                    nets[network]=index

        for host in hosts:
            index+=1
            nodes.append({"id":index, "label":host.name, "title": host.
template , "shape": "icon",  "icon": { "face": "next-
font", "code": "\ue61b",  "size": 50,  "color": "green"}})
            network = host.configuration["network"]
            if(network):
                if(network in nets):
                    links.append({"from":index,"label":network , "to":n
ets[network],"length":link_length, "font": { "color": "#ff0000" }})

        net = {"nodes":nodes, "edges":links}
        return json.dumps(net)
```

Για τις οντότητες αυτές έχουν καταχωρηθεί στο αρχείο dias/battlefield/admin.py οι απαραίτητες εγγραφές ώστε το Django να επιτρέπει την διαχείριση των δεδομένων που περιλαμβάνει η κάθε οντότητα χρησιμοποιώντας το ειδικό περιβάλλον που διαθέτει προς αυτό τον σκοπό και που είναι προσβάσιμο στο σύνδεσμο http://10.8.9.251/admin. Το περιβάλλον αυτό αποτελεί ιδιαίτερα χρήσιμο εργαλείο για την διαχείριση της πλατφόρμας αφού παρέχει τη δυνατότητα διερεύνησης και διόρθωσης τυχόν σφαλμάτων που μπορεί να προκύψουν κατά την διάρκεια της χρήσης της λόγω του ότι είναι αποσυνδεδεμένο από το front-end της εφαρμογής. Επίσης παρέχεται η δυνατότητα για προσθήκη νέων εγγραφών σε όλες τις οντότητες, κάτι το οποίο μπορεί να χρησιμοποιηθεί για προσθήκη νέων δεδομένων σε περίπτωση που απαιτηθεί και για τις οποίες δεν προσφέρεται η δυνατότητα μέσω του Front End, όπως για παράδειγμα μια ένα νέο επίπεδο δυσκολίας των Σεναρίων ή ένα νέο Module εκτέλεσης επιθέσεων στα Attack Scripts.




**Εικόνα 5.** Σελίδα διαχείρισης του Django

Όλα τα αιτήματα http, εξυπηρετούνται μέσω των διαφορετικών προβολών(Views) που έχουν κωδικοποιηθεί στο αρχείο dias/battlefield/views.py. Η αντιστοίχιση των αιτημάτων με τις προβολές γίνεται μέσω του αρχείου dias/battlefield/urls.py. Για την κωδικοποίηση της εξυπηρέτησης των αιτημάτων χρησιμοποιήθηκαν προβολές βασισμένες σε συναρτήσεις για μικρής έκτασης και πολυπλοκότητας προβολές και βασισμένες σε κλάσεις για πιο πολύπλοκες προβολές. Στην αρχή κάθε προβολής ορίζεται η απαίτηση για συνδεδεμένο ή όχι χρήστη καθώς και τα δικαιώματα τα οποία πρέπει να έχει για να εκτελεστεί το συγκεκριμένο αίτημα. Επίσης, μέσω των προβολών αυτών υποδηλώνεται το Template που θα χρησιμοποιηθεί για την προβολή των αποτελεσμάτων, τα οποία μεταφέρονται σαν παράμετροι στο τέλος της εκτέλεσης της προβολής. Πιο κάτω παρατίθενται δύο παραδείγματα ένα βασισμένο σε συνάρτηση και ένα σε πιο πολύπλοκο που βασίζεται σε κλάση.

```
#προβολή βασισμένη σε συνάρτηση
@login_required
@permission_required('battlefield.manage_battlefield')
def bf_destroy(request,pk):
    bf = Battlefield.objects.get(pk=pk)
    if(bf.can_destroyed()):
        interprocess.send(f'destroy bf {pk}')
        return redirect('battlefield-detail',pk=pk)
    else:
        return HttpResponse(status=204)

# προβολή βασισμένη σε κλάση
class BattlefieldDetailView(PermissionRequiredMixin, generic.DetailView
):
    permission_required = ('battlefield.view_battlefield')
    model = Battlefield
    template_name = 'battlefields/battlefield_detail.html'

    def get_context_data(self, **kwargs):
        context = super().get_context_data(**kwargs)
        logs = Log.objects.filter(battlefield_id=context["battlefield"]
.id).filter(log_type_id=constants.ARGOS_LOG).order_by('-
timestamp')[:10]
        context["logs"] = logs

        argos_status = interprocess.sendAndWaitResponse("ping")
        context["argos_status"] = argos_status
        return context
```

Όπως φαίνεται και από τα παραδείγματα πιο πάνω κάποιες από τις προβολές είναι δυνατό να επιστρέφουν κάποια τυποποιημένη απάντηση HTTP (πχ 204) ή κάποιο

περιεχόμενο (context) αναλόγως του αιτήματος. Στο δεύτερο παράδειγμα, φαίνεται επίσης η χρήση του html template, battlefield_detail. Όλα τα templates που αφορούν τις προβολές για όλες τις ενέργειες που μπορούν να εκτελεστούν στη πλατφόρμας βρίσκονται στο φάκελο dias/battlefield/templates με εξαίρεση τα templates που αφορούν τα κοινά σφάλματα του http 403 και 404 τα οποία βρίσκονται στο φάκελο dias/templates.

Εκτός από τα templates, τα αιτήματα HTTP χρησιμοποιούν επίσης τις φόρμες καταχώρησης δεδομένων είτε για την εξυπηρέτηση αιτημάτων POST και την αποστολή πληροφοριών είτε για την προβολή ήδη συμπληρωμένων φορμών κατά τη διάρκεια επεξεργασίας κάποιας οντότητας. Οι φόρμες αυτές βρίσκονται στο αρχείο dias/battlefield/forms.py και μπορεί να είναι απλές, περιλαμβάνοντας για παράδειγμα μόνο τα πεδία μιας οντότητας τα οποία προβάλλονται για να συμπληρωθούν από τον χρήστη ή σύνθετες, περιλαμβάνοντας περισσότερες από μία οντότητες ή επεμβαίνοντας στα πεδία και τα δεδομένα κατά τις διάφορες φάσεις της χρήσης της φόρμας.

Με παρόμοιο τρόπο μέσω του αρχείου dias/battlefield/routing.py γίνεται η αντιστοίχηση των ws αιτημάτων στους consumers (αρχείο dias/battlefield/consumers.py) οι οποίοι είναι υπεύθυνοι για την διαχείριση της επικοινωνίας μέσω websocket. Στην περίπτωση της παρακολούθησης των Σεναρίων, τα websocket requests λαμβάνονται μέσω Javascript στο αντίστοιχο html template (dias/battlefield/templates/scenarios/monitor.html) και με την χρήση των βιβλιοθηκών vis-timeline-graph2d.js και moment.js προβάλλονται σε πραγματικό χρόνο σε ένα χρονοδιάγραμμα.

Μια σημαντική παράμετρος που απαιτείται για την σωστή λειτουργία της εφαρμογής είναι η ρύθμιση κατευθείαν επικοινωνίας με την πλατφόρμα oVirt. Αν και το μεγαλύτερο μέρος των πληροφοριών που αφορούν το oVirt, ανταλλάσσονται μέσω της εφαρμογής Argos. Υπάρχει μια εξαίρεση. Για την δημιουργία νέου ΕΠΜ οι πληροφορίες που αφορούν τα Clusters του περιβάλλοντος oVirt και τα διαθέσιμα Templates παρακάμπτουν την εφαρμογή Argos και λαμβάνονται κατευθείαν μέσω της εφαρμογής Dias. Ο μοναδικός λόγος για τον οποίο χρησιμοποιείται αυτή η πρακτική είναι για την ύπαρξη δυνατότητας χρήσης της πλατφόρμας για τη δημιουργία νέων ΨΠΒ στη ΒΔ όταν η εφαρμογή Argos είναι εκτός λειτουργίας. Για την επίτευξη της σύνδεσης απαιτείται η ύπαρξη έγκυρων στοιχείων που αφορούν το περιβάλλον oVirt στο αρχείο dias/oVirt/get_oVirt_data.py ως ακολούθως:

```
# Create connection to ovirt engine
def create_connection():

    logger = logging.getLogger('dias')
    # Create the connection to the server:
    return sdk.Connection(
        url='https://VM_ENGINE_URL/ovirt-engine/api',
        username='OVIRT_ADMIN_USERNAME',
        password='OVIRT_ADMIN_PASSWORD',
        ca_file='config/ovirt_ca.pem',
        debug=True,
        log=logger,
    )
```

και η ύπαρξη του πιστοποιητικού αυθεντικοποίησης του oVirt στο φάκελο dias/config με την ονομασία oVirt_ca.pem. Το πιστοποιητικό είναι διαθέσιμο μέσω του συνδέσμου https://VM_ENGINE_URL /oVirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA.

## 9.2 Εφαρμογή Argos

Η επικοινωνία μεταξύ της εφαρμογής Dias και της πλατφόρμας διαχείρισης των εικονικών μηχανημάτων oVirt γίνεται με τη χρήση της ενδιάμεσης εφαρμογής Argos μέσω Inter-Process Communication (IPC). Η επικοινωνία αυτή είναι υλοποιημένη μέσω του Socket API της Python και είναι τύπου «AF_INET». Αποτελεί επί της ουσίας ένα τοπικό (localhost) TCP Socket που χρησιμοποιεί τη θύρα 5826. Η επιλογή αυτή έγινε για τους ακόλουθους λόγους:

- Είναι συμβατή με λειτουργικά συστήματα Windows και Linux, άρα δεν υπάρχει περιορισμός στην υλοποίηση.
- Εξασφαλίζει την δυνατότητα διαχωρισμού των εφαρμογών απεικόνισης του Γραφικού Περιβάλλοντος (εφαρμογή Dias) με τον backend χειρισμό των ενεργειών (εφαρμογή Sinon) με την αντικατάσταση του localhost με κάποιο απομακρυσμένο εξυπηρετητή.
- μέσω της βιβλιοθήκης multiprocessing.connection είναι δυνατό να εξυπηρετούνται ταυτόχρονα περισσότερες από μία συνδέσεις.

Στη συνέχεια, χρησιμοποιώντας την βιβλιοθήκη oVirt-engine-sdk-python (έκδοση 4.4.9) και μέρος από τον κώδικα του «Cyberforce» που αναπτύχθηκε τα προηγούμενα χρόνια

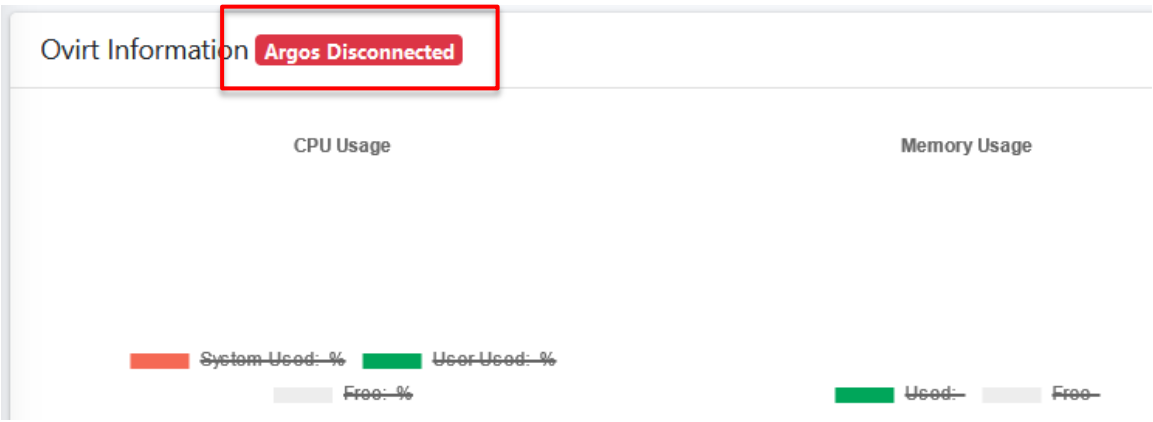
από το πανεπιστήμιο, εκτελούνται οι απαιτούμενες ενέργειες στα εικονικά μηχανήματα και την πλατφόρμα oVirt.

Όλες οι κύριες ενέργειες που αφορούν την υποδομή της πλατφόρμας και σχετίζονται με τα ΕΠΜ, τα Σενάρια και τις εικονικές μηχανές των σεναρίων (Routers και Hosts), βρίσκονται χωρισμένες σε κλάσεις στο φάκλεο /argos/cyberforce/argos_config

Για να είναι δυνατή η εκτέλεση ενεργειών στην πλατφόρμα oVirt, θα πρέπει στο αρχείο argos/cyberforce/module_utils/oVirt_utils.py να υπάρχουν έγκυρα στοιχεία που αφορούν το περιβάλλον oVirt. Συγκεκριμένα θα πρέπει να τροποποιηθεί κατάλληλα η συνάρτηση create_connection() όπως ακριβώς έχει προηγουμένως περιγραφεί για την εφαρμογή Dias.

Επίσης στον φάκελο argos/config πρέπει να βρίσκεται το πιστοποιητικό του περιβάλλοντος oVirt με όνομα αρχείου oVirt_ca.pem. Το πιστοποιητικό είναι διαθέσιμο μέσω του συνδέσμου https://VM_ENGINE_URL /oVirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA

Η εφαρμογή Argos είναι ιδιαίτερα κρίσιμη αφού χωρίς αυτή αποκόπτεται ουσιαστικά το περιβάλλον oVirt από την υπόλοιπη πλατφόρμα. Πριν εκτελεστεί οποιαδήποτε ενέργεια στην πλατφόρμα η οποία προϋποθέτει επικοινωνία με το oVirt, γίνεται έλεγχος και στην περίπτωση που δεν είναι εφικτή η επικοινωνία, τότε παρουσιάζεται ένα μήνυμα σφάλματος όπως αυτό της Εικόνα 6 που ακολουθεί:




**Εικόνα 6. Μήνυμα σφάλματος σύνδεσης με εφαρμογή Argos**

Η διαχείριση της επικοινωνίας μεταξύ της εφαρμογής Dias και της εφαρμογής Argos επιτυγχάνεται με την ενεργοποίηση ενός εξυπηρετητή συνδέσεων ο οποίος αναμένει για

συνδέσεις και στη συνέχεια για συγκεκριμένα μηνύματα. Αφού λάβει ένα μήνυμα ο εξυπηρετητής το αναλύει σε επί μέρους λέξεις κλειδιά και εκτελεί τις κατάλληλες ενέργειες. Η διαδικασία αυτή φαίνεται στον κώδικα που ακολουθεί ενώ τα μηνύματα και οι χρήσεις τους φαίνονται στον Πίνακας 2. Μηνύματα επικοινωνίας εφαρμογών Dias - Argos

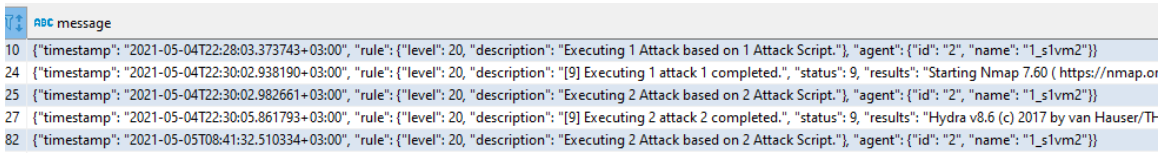
```
from multiprocessing.connection import Listener
_address = ('localhost', 5826)
_listener = Listener(_address)
_interprocess = None
_terminate = False

def handle_connection():
    _interprocess = _listener.accept()
    try:
        # όταν ανοίξει μια νέα σύνδεση
        while _interprocess:
            # αναμονή για λήψη μηνύματος
            msg = _interprocess.recv()
            # διαχωρισμός εντολών χρησιμοποιώντας τα κενά διαστήματα
            msg = msg.split(' ')
            # έλεγχος του είδους του μηνύματος
            if(msg[0] == "create"):
                if(msg[1] == "bf"):
                        # αποστολή διαβεβαίωσης λήψης
                        _interprocess.send(1)
                        ...εκτέλεση λοιπών ενεργειών
             ...
             ... υπόλοιπες λέξεις-κλειδιά
             ...

            elif(msg[0] == "destroy"):
                if(msg[1] == "bf"):
                    # αποστολή διαβεβαίωσης
                    _interprocess.send(1)
                    ... εκτέλεση λοιπών ενεργειών
            elif(msg[0] == "exit"):
                _terminate=True

    # επαναφορά στην αρχική κατάσταση όταν τερματιστεί η σύνδεση
    except EOFError:
        handle_connection()
    except Error as e:
        if(_terminate):
            _interprocess.close()
            _listener.close()
        else:
            handle_connection()
```

| Λέξεις κλειδιά (Keywords) | | | Παραμέτροι | Παράδειγμα | Σκοπός |
|---|---|---|---|---|---|
| create | bf | | bf_id | create bf 1 | Δημιουργία τοπολογίας ΕΠΜ |
| destroy | bf | | bf_id | destroy bf 1 | Καταστροφή τοπολογίας ΕΠΜ |
| poweroff | bf | | bf_id | poweroff bf 1 | Τερματισμός Λειτουργίας τοπολογίας ΕΠΜ |
| poweron | bf | | bf_id | poweron bf 1 | Εκκίνηση Λειτουργίας τοπολογίας ΕΠΜ |
| stop | scenario | | scenario_id | stop scenario 1 | Τερματισμός Σεναρίου |
| start | scenario | | scenario_id | start scenario 1 | Εκκίνηση Σεναρίου |
| configure | scenario | | scenario_id | configure scenario 1 | Αρχικοποίηση Σεναρίου |
| set | state | bf | state | set state init_snap | Επαναφορά τοπολογίας ΕΠΜ σε συγκεκριμένη κατάσταση (snapshot) |
| get | console | | vm_name | get console abc | Ανάκτηση αρχείου σύνδεσης σε τερματικό |
| | management_url | | host_id | get management_url 2 | Ανάκτηση διεύθυνσης ελέγχου δρομολογητή |
| | stats | | | get stats | Ανάκτηση σε μορφή json των στατιστικών της κονσόλας oVirt |
| ping | | | | ping | Έλεγχος επικοινωνίας εφαρμογής Argos |
| status | | | | status | Έλεγχος και αναφορά κατάστασης της υποδομής της πλατφόρμας |

**Πίνακας 2.** Μηνύματα επικοινωνίας εφαρμογών Dias - Argos

## 9.3 Εφαρμογή Sinon

Η εφαρμογή Sinon αποτελεί στην ουσία έναν daemon ο οποίος βρίσκεται προ-εγκατεστημένος στην Πρότυπη Εικονική Μηχανή γενικής χρήσης Ubuntu Desktop. Κατά την διαδικασία της ανάπτυξης του έχει επίσης δοκιμαστεί σε λειτουργικά συστήματα ωστόσο στο περιβάλλον oVirt χρησιμοποιήθηκε μόνο σε διανομές Linux Ubuntu και Fedora. Η βασική λειτουργία της εφαρμογής είναι η ανά 60 δευτερόλεπτα σύνδεση στην βάση δεδομένων και  ο έλεγχος κατά πόσον υπάρχει ενεργοποιημένο κάποιο Σενάριο στο οποίο συμμετέχει η συγκεκριμένη εικονική μηχανή στην οποία βρίσκεται εγκατεστημένη. Σε περίπτωση που εντοπιστεί κάποιο ενεργό Σενάριο τότε λαμβάνει από την ΒΔ όσα Attack Scripts αφορούν την συγκεκριμένη συσκευή και τα εκτελεί. Τα Attack Scripts αποθηκεύονται στην ΒΔ κωδικοποιημένα σε Base64 για να αποφεύγεται ο εντοπισμός τους από προγράμματα εντοπισμού κακόβουλου λογισμικού, έτσι μετά την λήψη ενός AttackScript ακολουθεί η αποκωδικοποίηση και στη συνέχεια η αντικατάσταση τυχών μεταβλητών που χρησιμοποιεί το συγκεκριμένο script. Η λήψη, η επιτυχής ανάγνωση και τα αποτελέσματα της εκτέλεσης των Attack Scripts αναφέρονται στο σύστημα παρακολούθησης πραγματικού χρόνου και καταγράφονται στην ΒΔ (Εικόνα 7).




**Εικόνα 7.** Καταγραφές από την εξέλιξη αυτοματοποιημένων επιθέσεων της εφαρμογής Sinon

## 9.4 Εφαρμογή Hermes

Ο ρόλος της εφαρμογής Hermes είναι η προώθηση των καταγραφών από τον Wazuh Manager και την εφαρμογή Suricata στην πλατφόρμα παρακολούθησης πραγματικού χρόνου μέσω συνδέσεων websocket.

Η εφαρμογή Hermes, εκκινεί κάθε φορά που μια νέα καταγραφή προστίθεται στο αρχείο καταγραφών του Suricata, /var/ossec/logs/alerts/alerts.json. Στη συνέχεια αφού διαβάσει την καταγραφή την προωθεί μέσω σύνδεσης websocket στο κατάλληλο κανάλι απεικόνισης και παράλληλα δημιουργεί μια νέα εγγραφή στο αρχείο καταγραφών της Β.Δ. Κατά την φάση της ανάγνωσης της καταγραφής εξάγεται το

όνομα του Wazuh Agent ο οποίος ανέφερε την ανώμαλη κατάσταση και το ΕΠΜ στο οποίο ανήκει. Με αυτό τον τρόπο διαφορετικές καταγραφές μπορούν να αποστέλλονται σε διαφορετικές σελίδες απεικόνισης και να διακρίνονται οι διαφορετικές συσκευές.

```
while True:
    try:
        msg = sys.stdin.readline().rstrip()
        alert = json.loads(msg)["_json"]
        content = json.dumps(alert)
        if (alert):
            agent_name = alert["agent"]["name"]
            bf_id = int(alert["agent"]["name"].split("_")[0])
            if(bf_id and not agent_name=='my.sensor.local'):
                submit_log(content,bf_id,alert["manager"]["name"])
        exit()
    except Exception as e:
        f = open('/tmp/error.txt','a')
        f.write(msg)
        f.close()
        exit()

def submit_log(msg,bf_id,agent_name):
    try:
        db = Database()
        #only send logs if the current scenario is active
        if (db.get_is_battlefield_active(bf_id)):
            ws.log_to_ws(msg,f'{URI}{bf_id}/')
            db.submit_log(msg,bf_id,agent_name)
            db.close(False)
    except:
        f = open('/tmp/error.txt','a')
        f.write(msg)
        f.close()
        exit()
```

# Κεφάλαιο 10

# Προϋποθέσεις Πλήρους Λειτουργίας

Για την πλήρη λειτουργία του Περιβάλλοντος Δημιουργίας Εικονικών Πεδίων Μάχης και Σεναρίων (ΠΔΕΠΜκΣ) απαιτείται:

a) να είναι ενεργοποιημένος ο εξυπηρετητής FreeIPA,
b) να είναι ενεργοποιημένος ο εξυπηρετητής της ΒΔ
c) να είναι ενεργοποιημένος ο εξυπηρετητής στον οποίο τρέχει το περιβάλλον oVirt
d) να είναι ενεργοποιημένος ένας webserver ο οποίος να ανακατευθύνει όλα τα αιτήματα στην εφαρμογή Dias η οποία αποτελεί το Περιβάλλον Δημιουργίας Εικονικών Πεδίων Μάχης και Σεναρίων .
e) να είναι ενεργοποιημένη η εφαρμογή Argos η οποία είναι υπεύθυνη για τη Διασύνδεση του Web Interface με το περιβάλλον oVirt

Ένα πλήρες διάγραμμα του συστήματος μπορείτε να δείτε στο ΠΑΡΑΡΤΗΜΑ Α

Στην περίπτωση που η εφαρμογή Argos δεν είναι ενεργοποιημένη τότε το ΠΔΕΠΜκΣ θα λειτουργεί αλλά με μειωμένες δυνατότητες. Συγκεκριμένα μπορούν να δημιουργηθούν Εικονικά Πεδία Μάχης, Σενάρια σε υφιστάμενα Πεδία Μάχης και να καταχωρηθούν νέα Πρότυπα Επιθέσεων. Όλες οι πιο πάνω ενέργειες θα αποθηκευτούν στην βάση δεδομένων, οποιαδήποτε όμως ενέργεια απαιτεί την αλληλεπίδραση με το περιβάλλον oVirt δεν θα εκτελεστεί παρά μόνο μετά την ενεργοποίηση της εφαρμογής Argos.

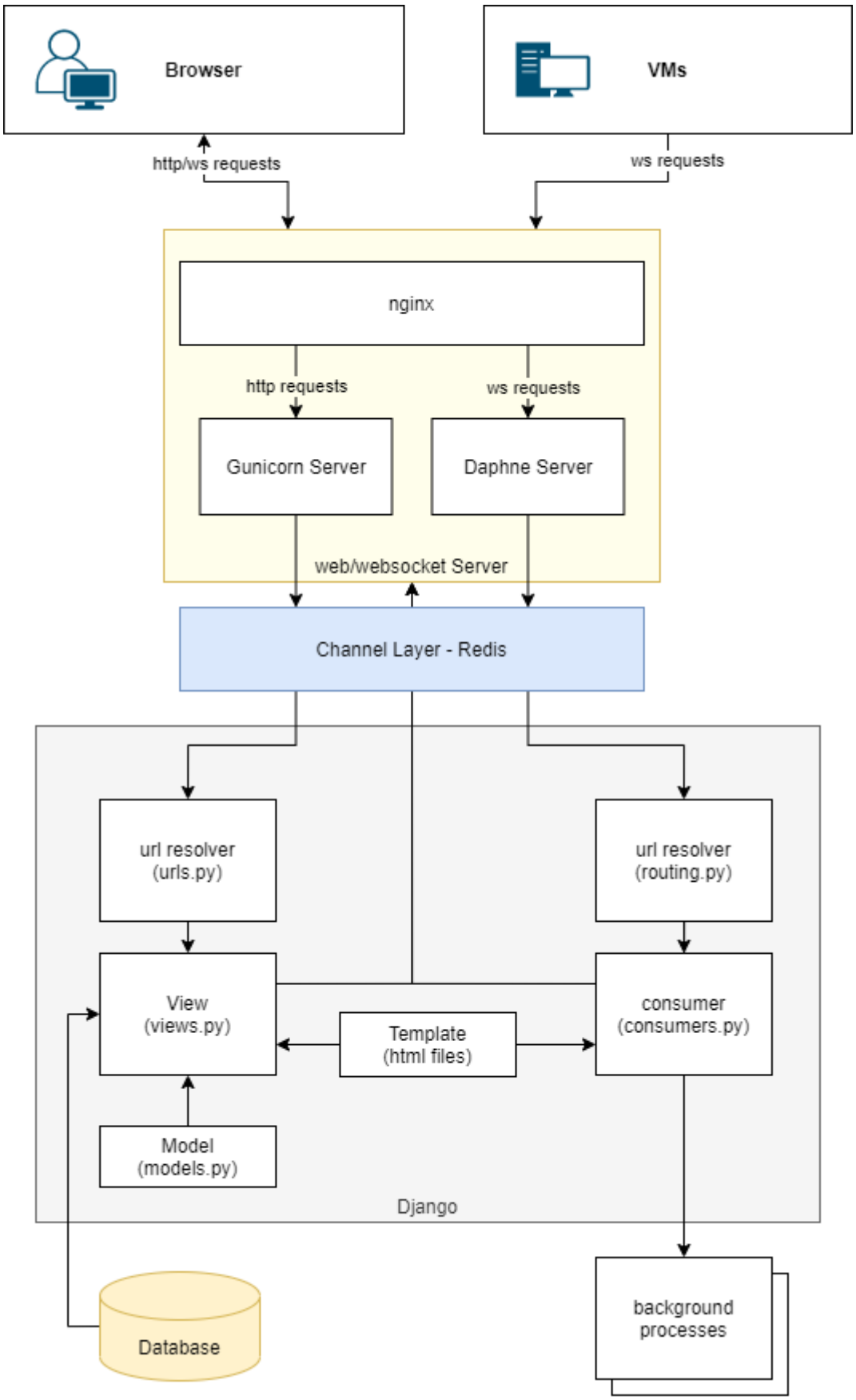
## 10.1 WebServer

Για την διαχείριση όλων των web requests χρησιμοποιείται ο Nginx web server ο οποίος ανακατευθύνει τα αιτήματα http και ws ανάλογα με τον τύπο τους στις εφαρμογές Gunicorn, και Daphne αντίστοιχα. Οι εφαρμογές Gunicorn και Daphne προτείνονται από τη βιβλιογραφία του Django για το διαχωρισμό των ασύγχρονων (ASGI) και σύγχρονων (WSGI) αιτημάτων ώστε να γίνεται η καλύτερη δυνατή εξυπηρέτηση τους και να υπάρχει η δυνατότητα και η ευελιξία για περαιτέρω ανάπτυξη και διαχείριση μεγαλύτερου όγκου αιτημάτων.

Η εφαρμογή Gunicorn αποτελεί ένα Web Server Gateway Interface, ο οποίος αναλαμβάνει να μεταφέρει όλα τα αιτήματα http στον url reslover του Django ώστε να εξυπηρετηθούν με δεδομένα που προέρχονται από την βάση δεδομένων και να παρουσιαστούν χρησιμοποιώντας τις πρότυπες δομές παρουσίασης που είναι συνήθως αρχεία html.

Όλα τα αιτήματα websocket προωθούνται στο daphne ASGI (Asynchronous Server Gateway Interface) και στη συνέχεια στο πρόσθετο channels του Django το οποίο με τη σειρά του τα ανακατευθύνει μέσω του urls.py στους αντίστοιχους consumers.

Το διάγραμμα ροής των αιτημάτων φαίνεται στην Εικόνα 8 που ακολουθεί:




**Εικόνα 8.** Ροή αιτημάτων προς και από τον WebServer

# Κεφάλαιο 11

# Δοκιμές

Όλες οι ενέργειες που εκτελέστηκαν κατά την φάση των δοκιμών είναι πλήρως συμβατές με τα λογισμικά:

- Mozilla Firefox v88.0 (64-bit)
- Google Chrome v90.0.4430.93 (Official Build) (64-bit).

Οι δοκιμές έγιναν σε διαφορετικούς χρόνους με διαφορετικές συνθήκες λειτουργίας της πλατφόρμας oVirt της οποίας η διαμόρφωση φαίνεται στον Πίνακας 3 που ακολουθεί:

| | |
|---|---|
| **Datacenter** | 1 |
| **Hosts** | 4 x Intel(R) Xeon(R) CPU X5670 @ 2.93GHz<br>12 Cores (2 sockets x 6 cores) |
| **Total Memory** | 230.9 GiB |
| **Total Storage** | 13 TiB |
| **Total Virtual Machines (συμπεριλαμβανομένης της υποδομής της υλοποίησης DIAS χωρίς ΕΠΜ)** | 35 |

**Πίνακας 3.** Η διαμόρφωση της πλατφόρμας oVirt

Αρχικά έγιναν δοκιμές οι οποίες αφορούσαν τους χρόνους δημιουργίας νέου ΕΠΜ, προετοιμασίας νέου Σεναρίου, και επαναφοράς Σεναρίου στην αρχική του Κατάσταση. Οι δοκιμές επαναλήφθηκαν σε διάφορες συνθήκες είτε μεμονωμένα είτε παράλληλα με άλλες λειτουργίες της πλατφόρμας.

## 11.1 Ενδεικτικοί χρόνοι δημιουργίας νέου ΕΠΜ

| Αριθμός Host | Αριθμός Δρομολογητών | Μέσος χρόνος |
|---|---|---|
| 2 | 1 | 44Λ 46Δ |
| 2 | 2 | 56Λ 53Δ |
| 4 | 2 | 1Ω 1Λ 56Δ |

**Πίνακας 4.** Ενδεικτικοί χρόνοι δημιουργίας Νέου ΕΠΜ

## 11.2 Ενδεικτικοί χρόνοι προετοιμασίας νέου ΕΣ

Προετοιμασία Εικονικού Σεναρίου γίνεται μόνο την πρώτη φορά μετά την δημιουργία του ώστε να δημιουργηθούν τα κατάλληλα snapshots των εικονικών μηχανών. Όλες τις επόμενες φορές γίνεται επαναφορά σε αυτά τα snapshot.

| Αριθμός Host | Αριθμός Δρομολογητών | Μέσος χρόνος |
|---|---|---|
| 2 | 1 | 9Λ 11Δ |
| 2 | 2 | 11Λ 05Δ |
| 4 | 2 | 17Λ 03Δ |

**Πίνακας 5.** Ενδεικτικοί χρόνοι προετοιμασίας νέου Εικονικού Σεναρίου

## 11.3 Ενδεικτικοί χρόνοι επαναφοράς ΕΣ

| Αριθμός Host | Αριθμός Δρομολογητών | Μέσος χρόνος |
|---|---|---|
| 2 | 1 | 6Λ 31Δ |
| 2 | 2 | 6Λ 39Δ |
| 4 | 2 | 14Λ 34Δ |

**Πίνακας 6.** Ενδεικτικοί χρόνοι επαναφοράς Εικονικού Σεναρίου

## 11.4 Βασικές λειτουργίες Πλατφόρμας

Ακολουθεί η παρουσίαση των αποτελεσμάτων από τις δοκιμές των βασικών λειτουργιών της πλατφόρμας. Όλες οι οδηγίες για τον τρόπο εκτέλεσης των ενεργειών που αναφέρονται βρίσκονται στο Εγχειρίδιο Χρήσης Παράρτημα Δ

### 11.4.1 Σύνδεση και Βασικά Δικαιώματα Χρηστών

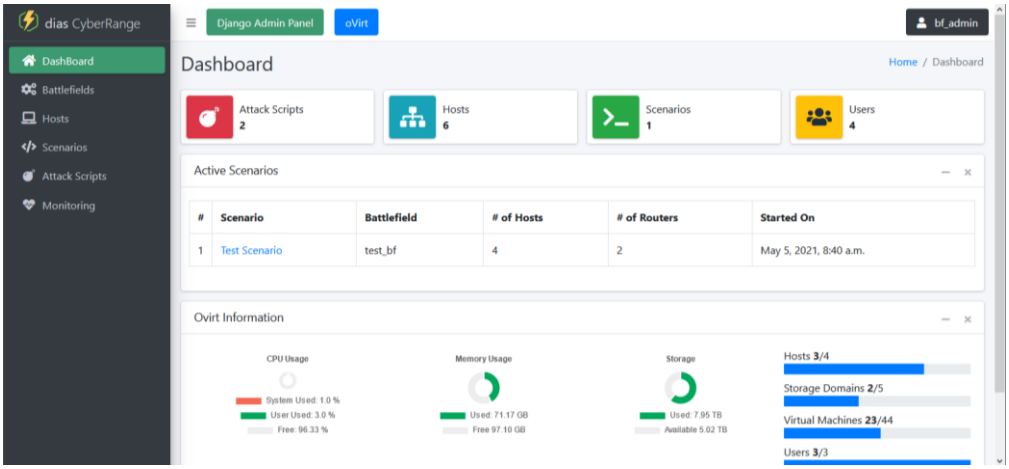
Στην πλατφόρμα FreeIPA καταχωρήθηκαν οι χρήστες με τις ομάδες όπως φαίνονται στον Πίνακας 7 που ακολουθεί.

| Χρήστες | Ομάδες που ανήκουν |
|---|---|
| admin | trust admins<br>admins |
| as_admin | ipausers<br>dias_attackscript_admins |
| bf_admin | ipausers<br>dias_admins |
| sc_admin | ipausers<br>dias_scenario_admins |
| sc_man | ipausers<br>dias_scenario_managers |
| user1 | ipausers<br>dias_players |
| user2 | ipausers<br>dias_players |
| user3 | ipausers<br>dias_players |

**Πίνακας 7.** Λογαριασμοί χρηστών για σκοπούς δοκιμών

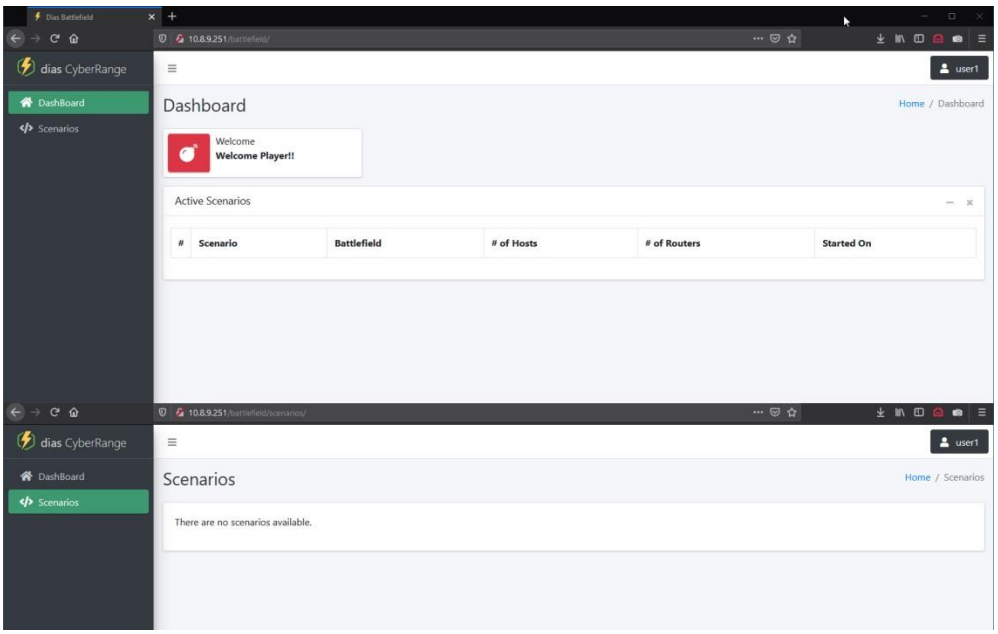
Στη συνέχεια επιχειρήθηκε σύνδεση με τον χρήστη admin, η οποία απέτυχε λόγω του ότι ο συγκεκριμένος χρήστης (αν και διαχειριστής της πλατφόρμας FreeIPA) δεν ανήκει σε καμιά από τις έγκυρες ομάδες της πλατφόρμας Dias. Ακολούθησε επιτυχημένη σύνδεση με τον χρήστη bf_admin και εμφανίστηκε η οθόνη με τις πληροφορίες της

πλατφόρμας Dias και του περιβάλλοντος oVirt. Στην Εικόνα 9 που ακολουθεί φαίνεται ότι υπάρχει μόνο ένας ενεργοποιημένος χρήστης (ο bf_admin). Αυτό συμβαίνει γιατί κάθε χρήστης ενεργοποιείται την πρώτη φορά που θα συνδεθεί. Όλες τα υπόλοιπα στοιχεία (Attack Scripts, Hosts και Scenarios είναι μηδενικά)

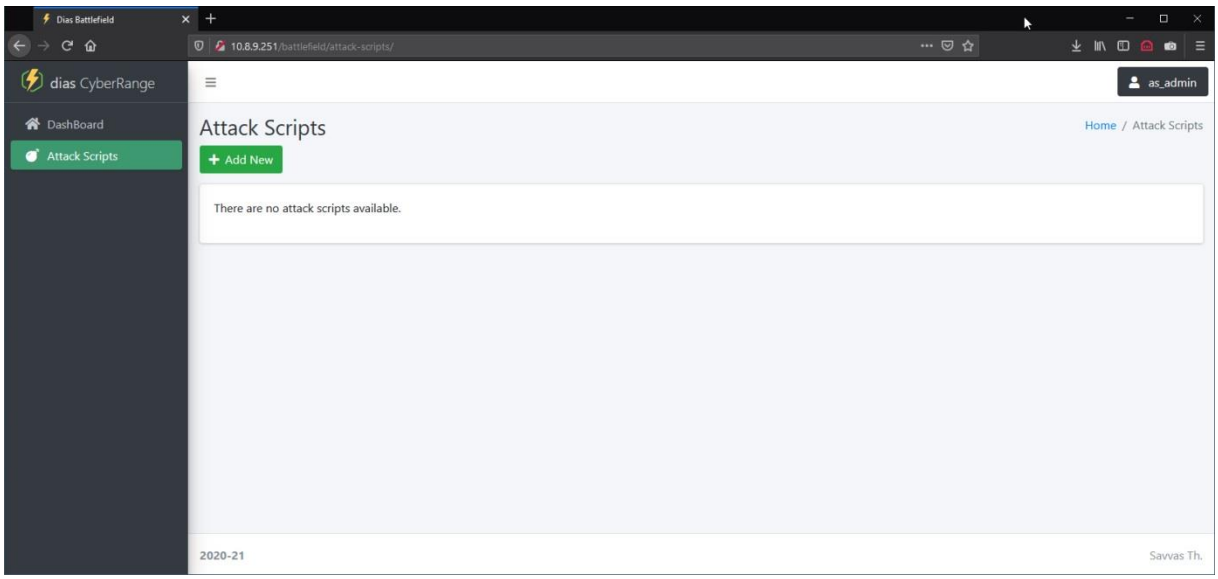



**Εικόνα 9.** Η αρχική σελίδα της εφαρμογής Dias (DashBoard)

Στη συνέχεια έγινε σύνδεση με τους υπόλοιπους χρήστες για επιβεβαίωση ότι τα δικαιώματα του κάθε χρήστη είναι σωστά και προβάλλονται πληροφορίες βάση της ανάγκης γνώσης. Έτσι, στις εικόνες που ακολουθούν μπορείτε να διακρίνετε ότι ο χρήστης user1 δεν έχει καμία διαθέσιμη πληροφορία, ενώ ο χρήστης as_admin μπορεί να προσθέσει νέα Attack-Scripts ή να δει τα υφιστάμενα εφόσον υπάρχουν.

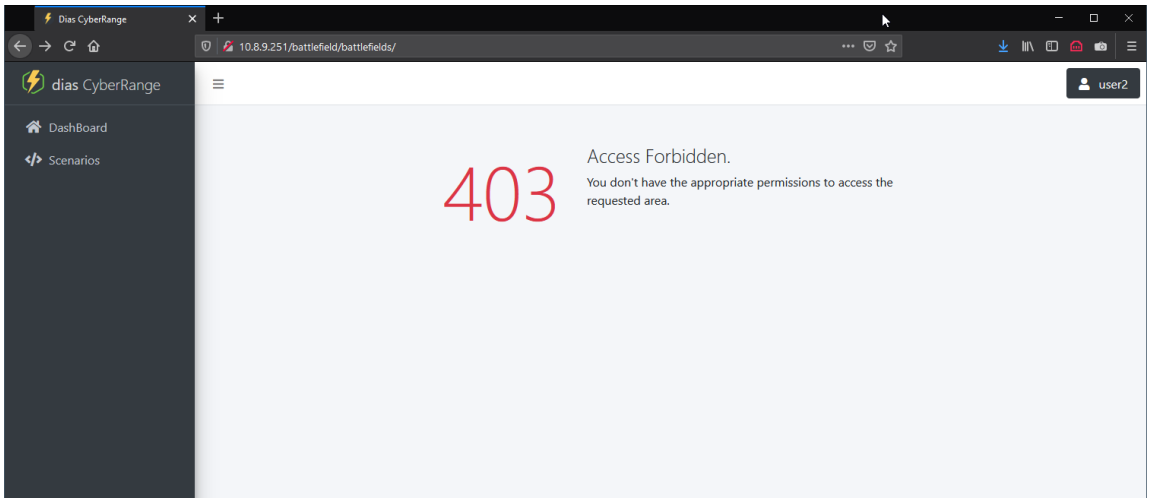



**Εικόνα 10.** Χρήστης της ομάδας dias_players χωρίς διαθέσιμες πληροφορίες




**Εικόνα 11.** Δυνατότητες χρήστη με δικαιώματα dias_attackscript_admins

Σε περίπτωση προσπάθειας πρόσβασης σε σελίδα χωρίς εξουσιοδοτημένη πρόσβαση εμφανίζεται το σφάλμα 403 «Access Forbidden». Αν για παράδειγμα ένας απλός χρήστης προσπαθήσει να αποκτήσει πρόσβαση στην σελίδα με τα ΕΠΜ πληκτρολογώντας κατευθείαν τον σύνδεσμο που αντιστοιχεί σε αυτή τη σελίδα. Τότε εμφανίζεται το πιο κάτω μήνυμα:

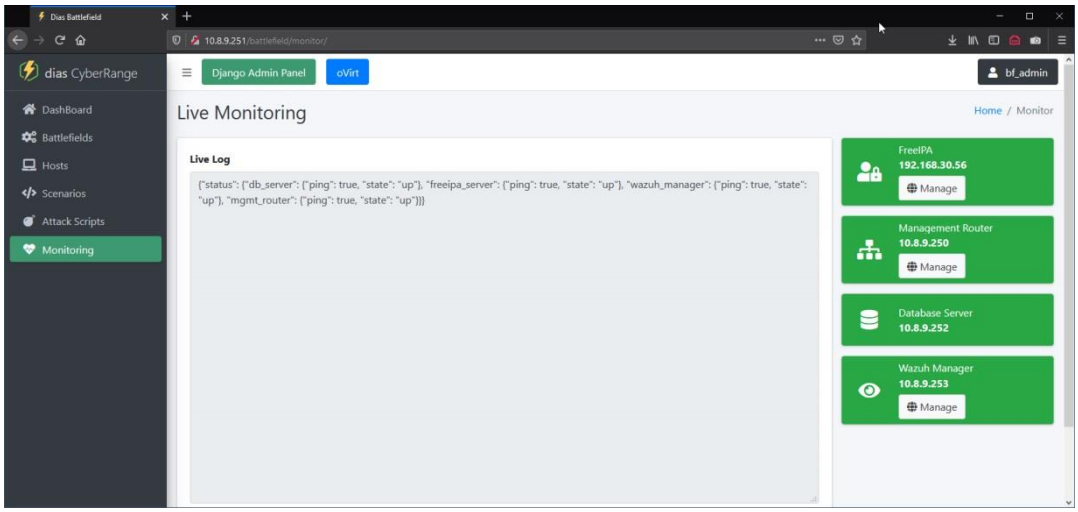



**Εικόνα 12.** Παράβαση Δικαιωμάτων Access Forbidden

### 11.4.2 Οθόνη παρακολούθησης λειτουργίας υποσυστημάτων

Οι διαχειριστές του συστήματος έχουν την δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την κατάσταση των κύριων υποσυστημάτων της πλατφόρμας. Αυτό

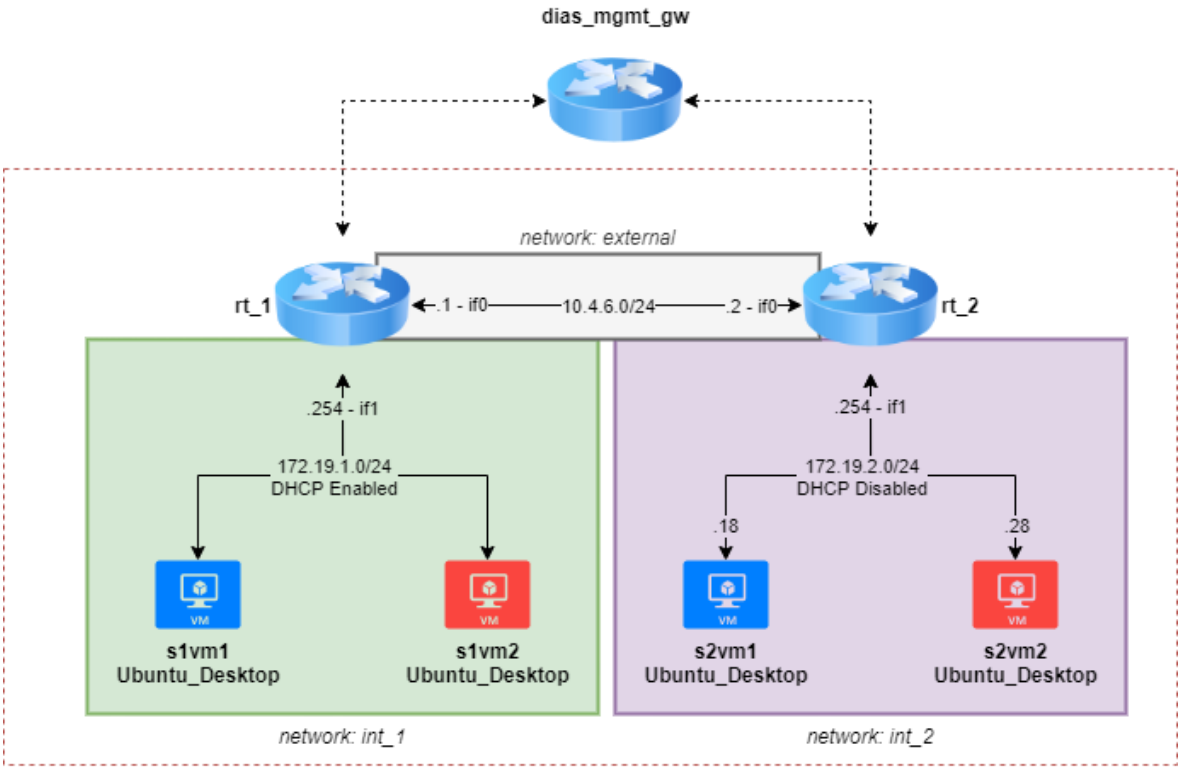
γίνεται από την επιλογή «Monitoring» του Κυρίως Μενού. Σε αυτή την οθόνη στα αριστερά φαίνονται οι καταστάσεις όπως αυτές λαμβάνονται από την εφαρμογή Argos και αποστέλλονται στην πλατφόρμα Dias κάθε 5 λεπτά. Οι καταστάσεις αυτές περιλαμβάνουν απάντηση σε ping request καθώς και την κατάσταση του εικονικού μηχανήματος στο οποίο τρέχει η υπηρεσία όπως αυτό αναφέρεται από το περιβάλλον oVirt. Στο δεξιό τμήμα υπάρχει οπτική αναπαράσταση αυτών των μηνυμάτων, καθώς και δυνατότητα για μετάβαση στη σελίδα διαχείρισης του κάθε υποσυστήματος.




**Εικόνα 13.** Σελίδα παρακολούθησης κατάστασης υποσυστημάτων (Monitoring)

### 11.4.3 Δημιουργία Σύνθετου Εικονικού Πεδίου Μάχης

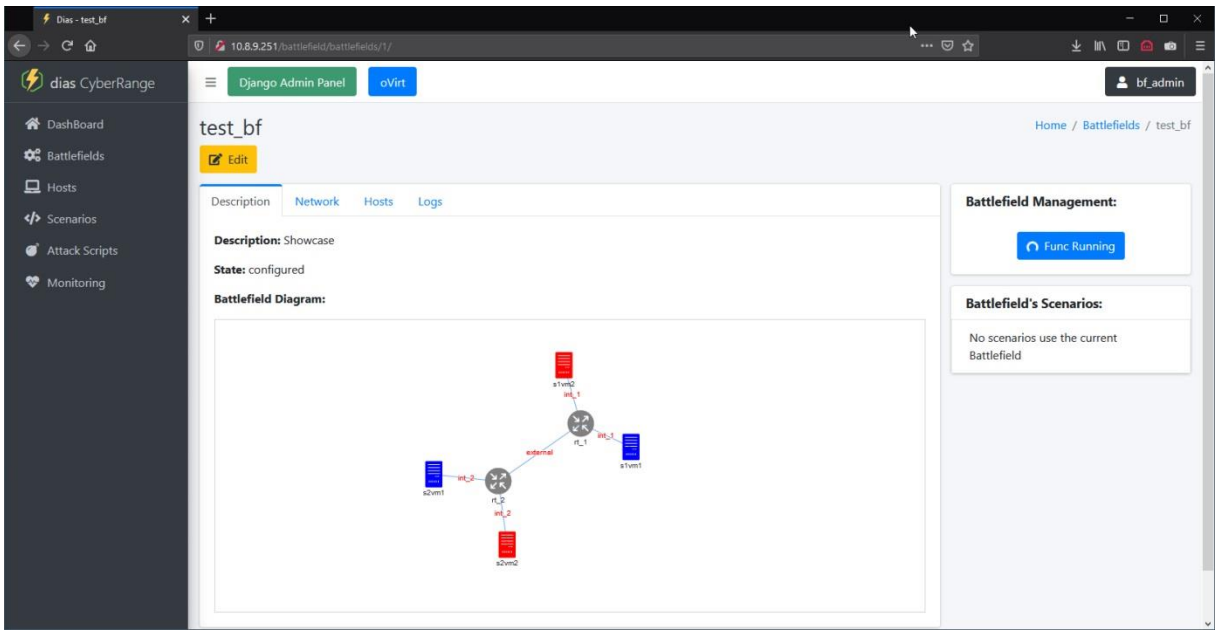
Για τον έλεγχο των βασικών λειτουργιών των ΕΠΜ, δημιουργήθηκε ένα σύνθετο ΕΠΜ με 3 δίκτυα, δύο συσκευές δρομολόγησης και 4 hosts, σε συνδεσμολογία όπως της Εικόνα 14. Στον δρομολογητή 1 (rt_1) ενεργοποιήθηκε η δυνατότητα DHCP για αυτόματη εκχώρηση των διευθύνσεων στο τοπικό δίκτυο, ενώ στον δρομολογητή 2 οι διευθύνσεις καταχωρήθηκαν κατά την δημιουργία του ΕΠΜ μέσω της πλατφόρμας.




**Εικόνα 14.** Το ΕΠΜ των δοκιμών

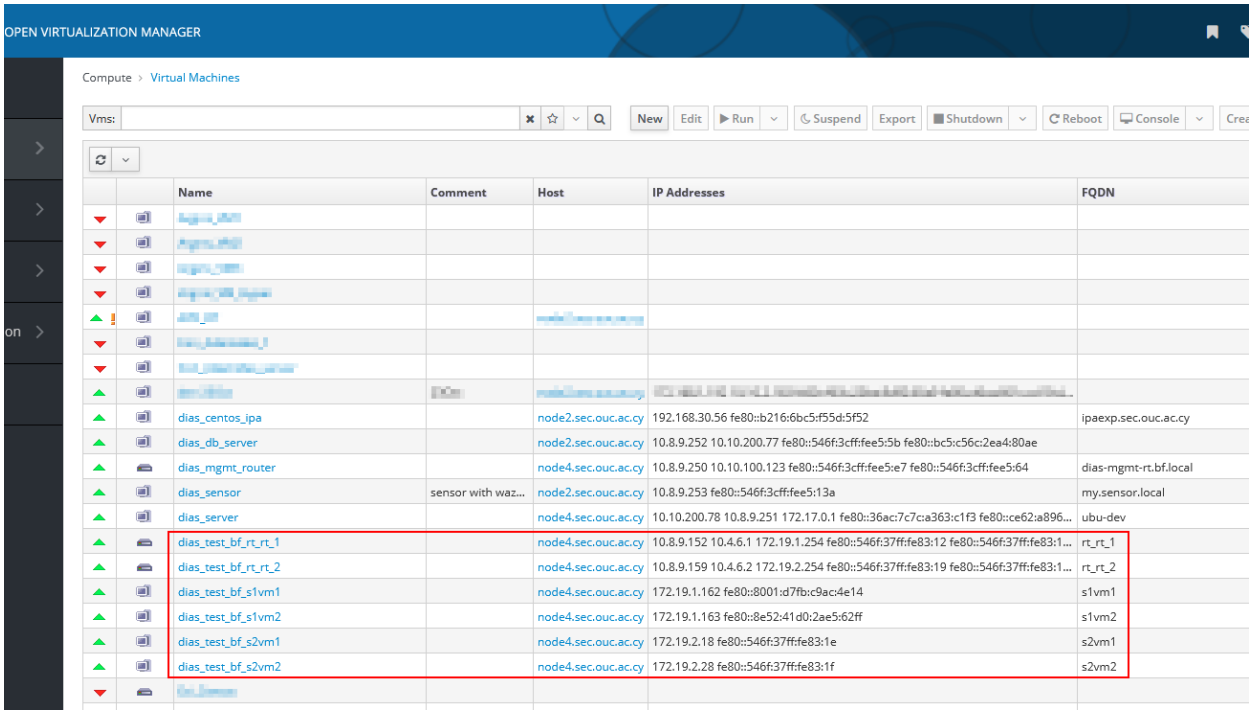
Με την ολοκλήρωση της καταχώρησης των στοιχείων για το νέο ΕΠΜ η πλατφόρμα Dias ανακατεύθυνε τον browser στην σελίδα με τις πληροφορίες του συγκεκριμένου ΕΠΜ η οποία φαίνεται στην Εικόνα 15 που ακολουθεί. Παράλληλα επικοινώνησε επιτυχώς με την εφαρμογή Argos και ξεκίνησε η δημιουργία του ΕΠΜ όπως υποδηλώνει η ένδειξη «Func Running» στην καρτέλα Battlefield Management με τις πληροφορίες του ΕΠΜ.

Επίσης δημιουργήθηκε το διάγραμμα της τοπολογίας που περιλαμβάνει τους Hosts, τους δρομολογητές και τα δίκτυα και στο πάνω μέρος της σελίδας δημιουργήθηκαν οι καρτέλες με τις αντίστοιχες πληροφορίες.




**Εικόνα 15.** Ολοκλήρωση καταχώρησης νέου ΕΠΜ

Με την ολοκλήρωση της δημιουργίας του ΕΠΜ, στην πλατφόρμα oVirt διακρίνονται όλα εικονικά μηχανήματα που δημιουργήθηκαν για το ΕΠΜ όπως επίσης οι διευθύνσεις IP και τα hostname του κάθε εικονικού μηχανήματος.




Επίσης στον Wazuh Manager χρησιμοποιώντας την εντολή :

```
/var/ossec/bin/agent_control -l
```

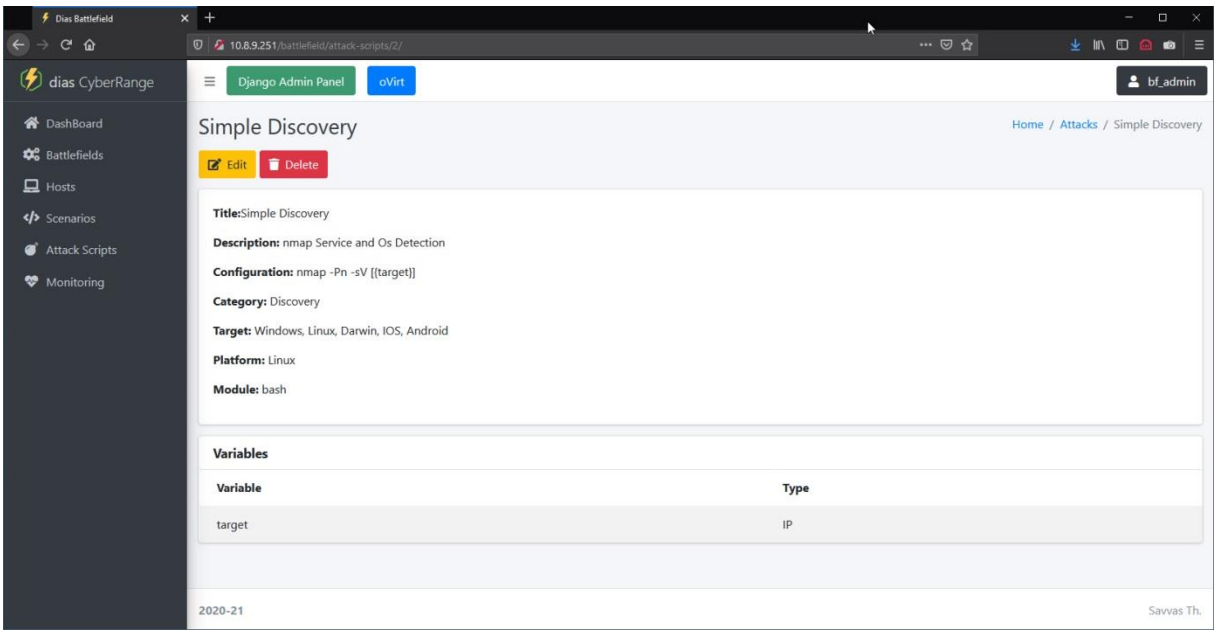
εμφανίζονται ενεργοποιημένοι οι Agents όλων των εικονικών μηχανημάτων που δημιουργήθηκαν:

```
[root@my ~]# /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
   ID: 000, Name: my.sensor.local (server), IP: 127.0.0.1, Active/Local
   ID: 067, Name: l_slvm2, IP: any, Active
   ID: 064, Name: l_rt_1, IP: any, Active
   ID: 065, Name: l_rt_2, IP: any, Active
   ID: 066, Name: l_slvm1, IP: any, Active
   ID: 068, Name: l_s2vm1, IP: any, Active
   ID: 069, Name: l_s2vm2, IP: any, Active

List of agentless devices:

[root@my ~]#
```

**Εικόνα 16.** Απεικόνιση των ενεργοποιημένων Wazuh Agents στον Wazuh Manager

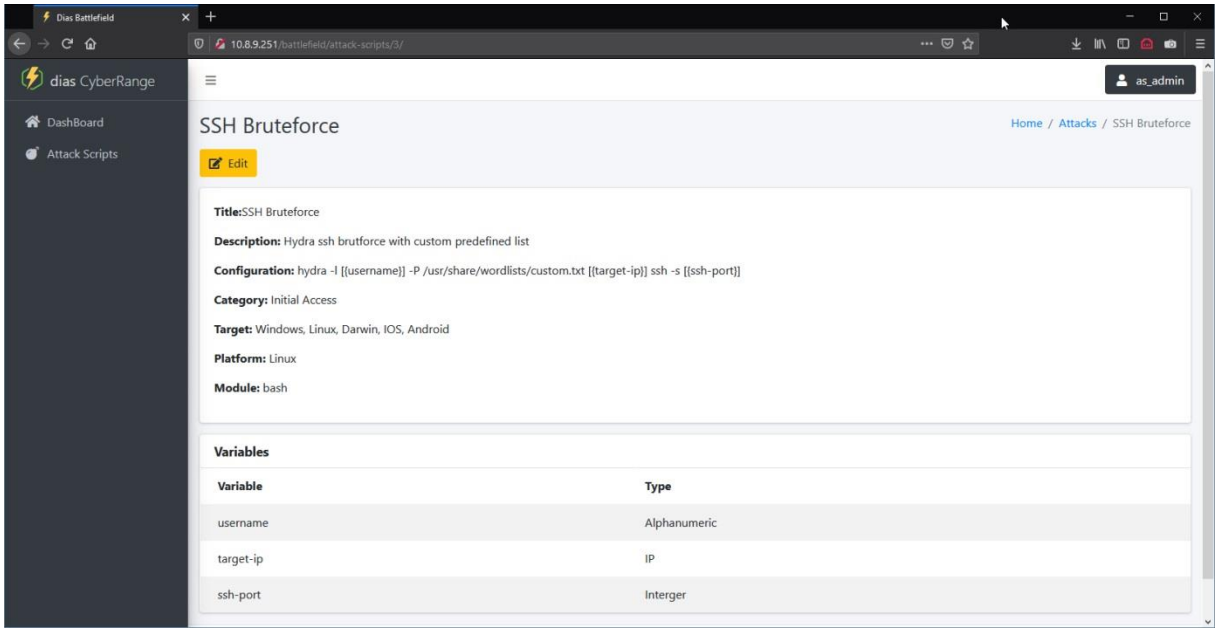
### 11.4.4 Δημιουργία Attack Scripts

Ακολούθησε η δημιουργία 2 Attack Scripts. Το Simple Discovery το οποίο χρησιμοποιώντας την εφαρμογή Nmap, ερευνά το δίκτυο για συσκευές και τις υπηρεσίες τους και το SSH Bruteforce το οποίο χρησιμοποιώντας την εφαρμογή hydra προσπαθεί να αποκτήσει πρόσβαση μέσω επίθεσης bruteforce σε υπηρεσία ssh. Στην Εικόνα 17 που ακολουθεί φαίνεται η επιτυχής δημιουργία του Simple Discovery, και η μεταβλητή target που δημιουργήθηκε αυτόματα από τον κώδικα που χρησιμοποιήθηκε.




**Εικόνα 17.** Η καταχώρηση του Simple Discovery Attack Script

Στην Εικόνα 18 που ακολουθεί και φαίνεται η δημιουργία του Attack Script «SSH Bruteforce» από τον χρήστη as_admin. Επιβεβαιώνετε με αυτό τον τρόπο ότι για την διαγραφή ενός Attack-Script απαιτούνται δικαιώματα διαχειριστή αφού το κουμπί «Delete» δεν εμφανίζεται δίπλα στο κουμπί «Edit» όπως συμβαίνει με την Εικόνα 17 που ο συνδεδεμένος χρήστης ήταν διαχειριστή.




**Εικόνα 18.** Η καταχώρηση του SSH Bruteforce Attack Script

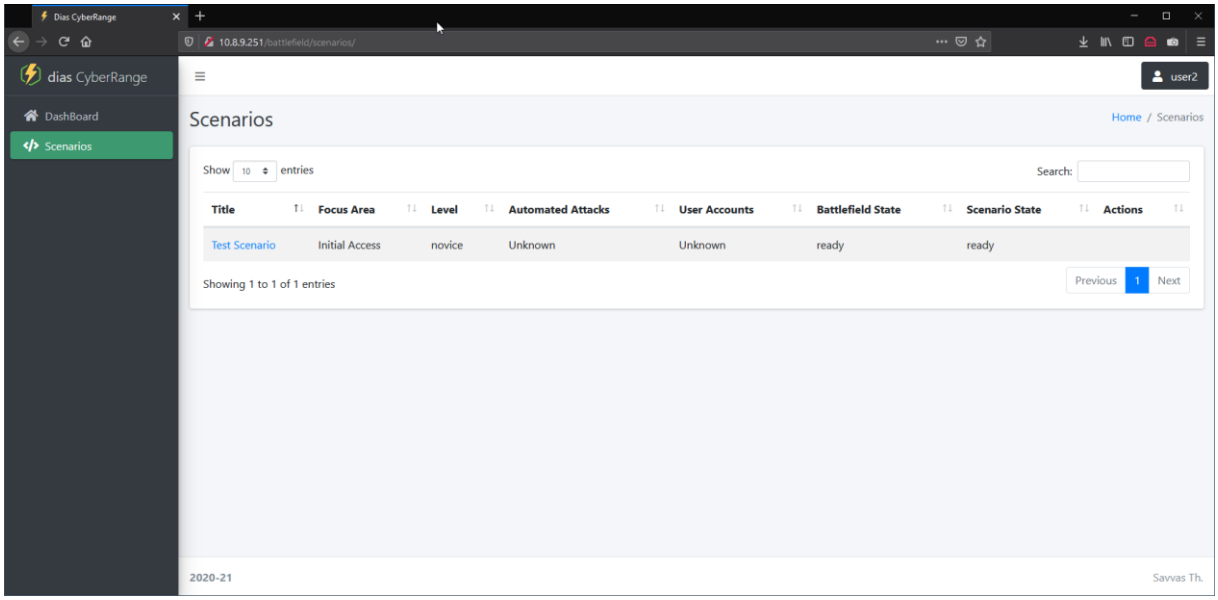
### 11.4.5 Δημιουργία Σεναρίου

Στη συνέχεια δημιουργήθηκε ένα Σενάριο διάρκειας 2 ωρών βασισμένο στο ΕΠΜ που δημιουργήθηκε προηγουμένως, με την ρύθμιση is Black Box ενεργοποιημένη και τα εξής χαρακτηριστικά:

| Host | Λογαριασμοί Χρηστών | Αυτοματοποιημένες Επιθέσεις |
|---|---|---|
| Host 1 | user1<br>user2 | |
| Host 2 | user2 | nmap_disc<br>hydra |
| Host 3 | user3 | |
| Host 4 | user4 | nmap_disc |

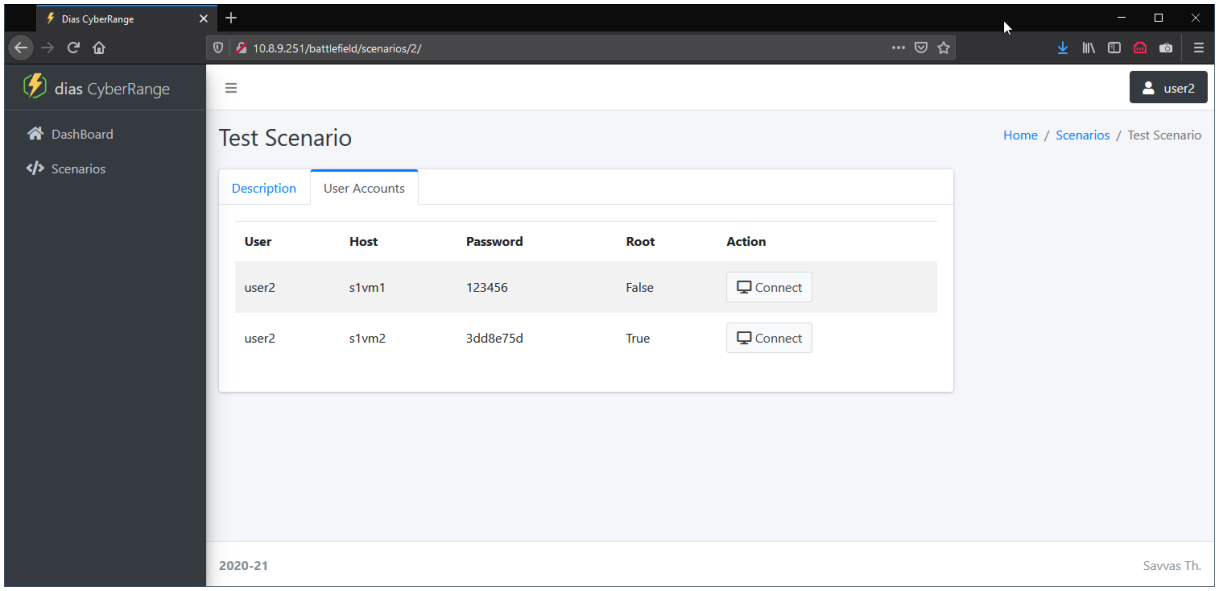
**Πίνακας 8.** Χαρακτηριστικά ΕΣ δοκιμών

Συνδεδεμένοι πλέον ως χρήστες που συμμετέχουν στο Σενάριο, όπως για παράδειγμα ο user2, στην αρχική οθόνη το Σενάριο δεν εμφανίζεται γιατί δεν έχει ξεκινήσει, αλλά είναι διαθέσιμο στην επιλογή Scenarios:



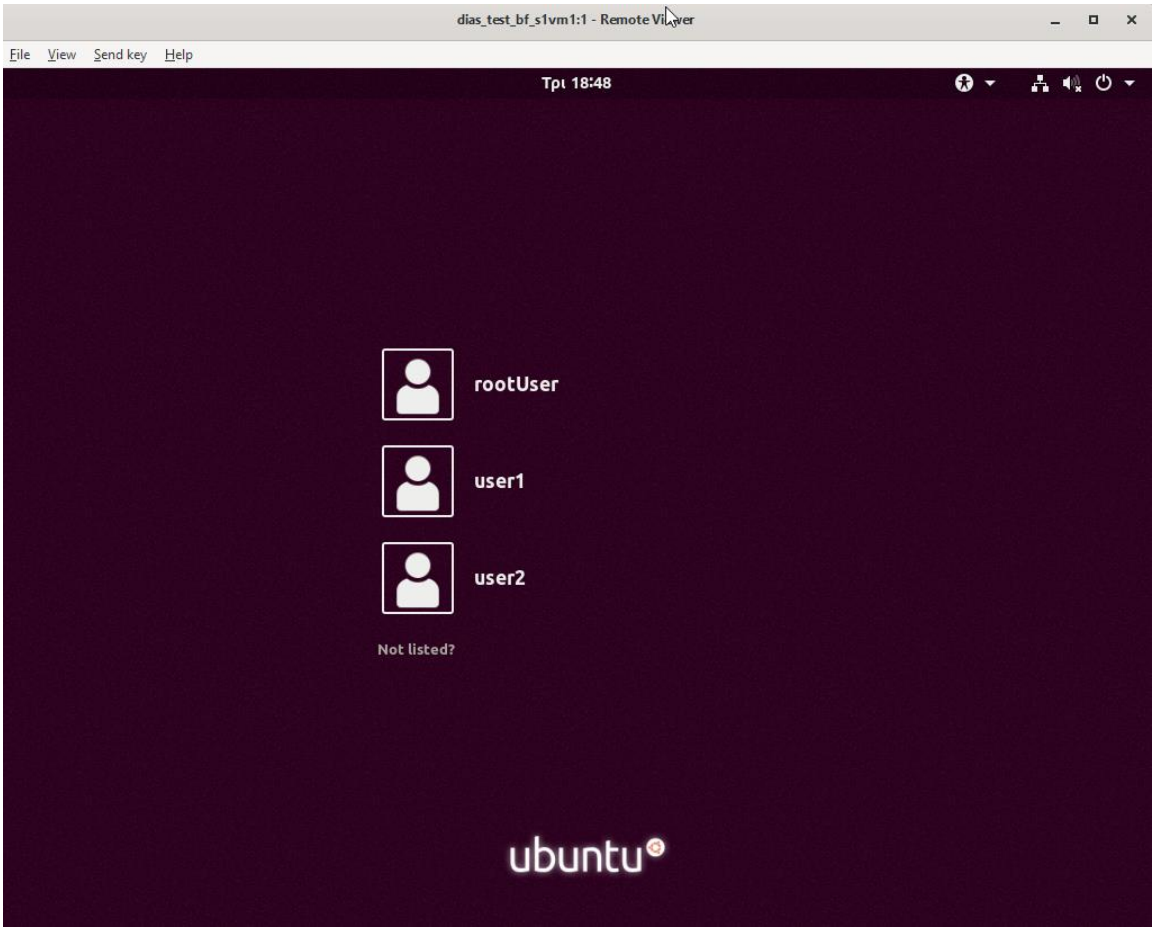

**Εικόνα 19.** Χρήστης που συμμετέχει σε Εικονικό Σενάριο

Επιλέγοντας ένα Σενάριο (ενεργοποιημένο ή όχι) στην καρτέλα «User Accounts» ο χρήστης μπορεί να δει τα διαθέσιμα εικονικά μηχανήματα στα οποία διαθέτει πρόσβαση, τον κωδικό πρόσβασης του και να συνδεθεί σε αυτά όπως ακριβώς θα μπορούσε να συνδεθεί μέσω της πλατφόρμας oVirt .




**Εικόνα 20.** Τα διαθέσιμα εικονικά μηχανήματα του χρήστη

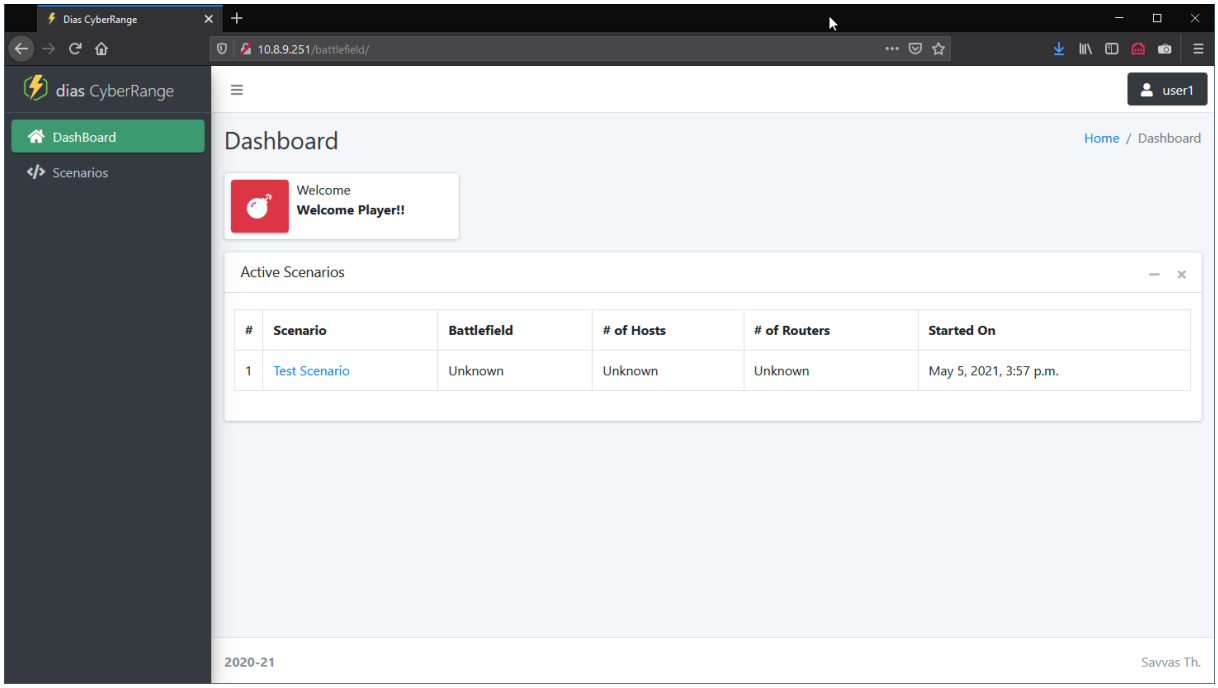
Πατώντας στο κουμπί «Connect» δημιουργείται ένα αρχείο connect.vv και εφόσον ο χρήστης έχει εγκατεστημένη στον υπολογιστή του την εφαρμογή VirtViewer μπορεί να συνδεθεί στη συγκεκριμένη εικονική μηχανή όπως φαίνεται στην Εικόνα 21.




**Εικόνα 21.** Σύνδεση σε Virtual Machine χρησιμοποιώντας την εφαρμογή VirtViewer

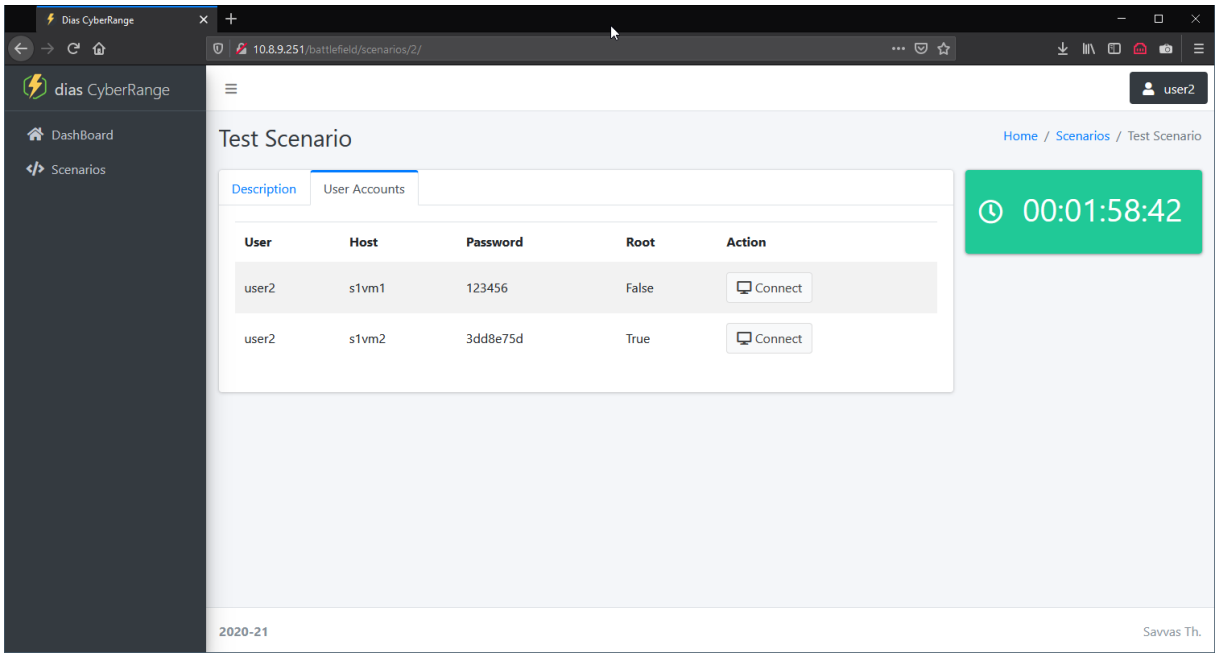
### 11.4.6 Εκκίνηση Σεναρίου

Αφού έγινε προετοιμασία και εκκίνηση του Σεναρίου η αρχική σελίδα πλέον αλλάζει και στον πίνακα με τα ενεργά Σενάρια των χρηστών user1, user2 και user3 εμφανίζεται το ενεργοποιημένο Σενάριο. Ο user4 ο οποίος δεν είναι καταχωρημένος στον FreeIPA δεν μπορεί να αποκτήσει πρόσβαση στην πλατφόρμα έστω και αν δηλώθηκε σαν χρήστης στο Εικονικό Μηχάνημα. Ωστόσο ο λογαριασμός του στο εικονικό μηχάνημα ισχύει και μπορεί να χρησιμοποιηθεί κανονικά.




**Εικόνα 22.** Αρχική σελίδα με ενεργοποιημένο Εικονικό Σενάριο

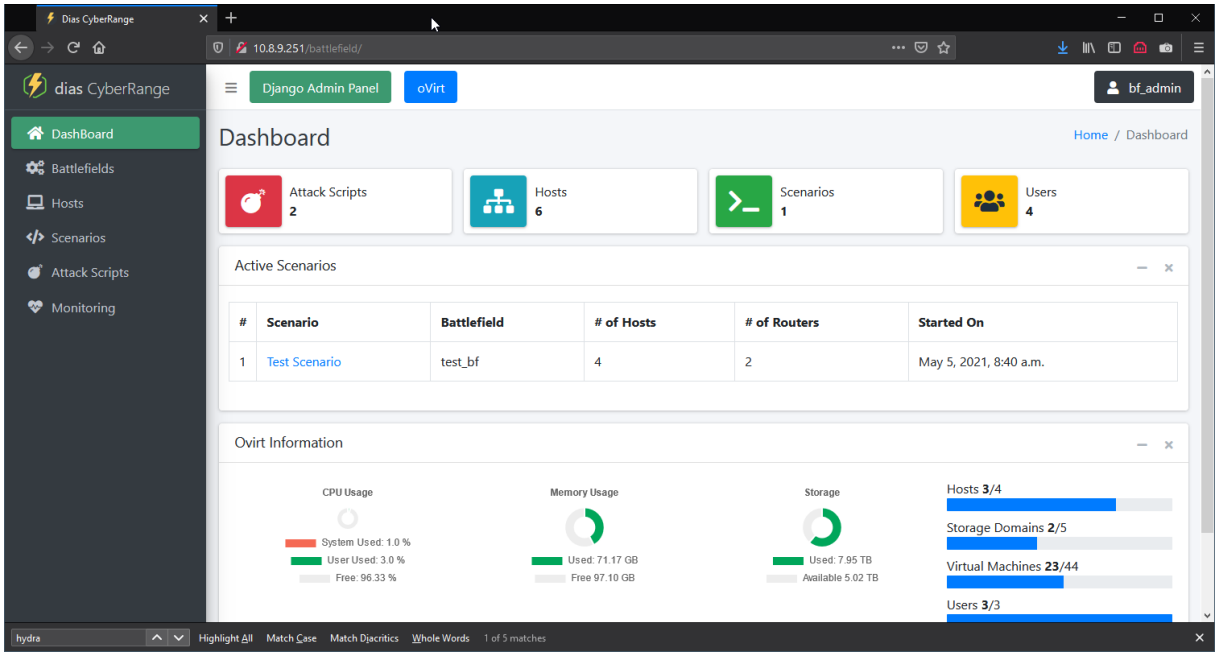
Επίσης, πατώντας στο όνομα του Εικονικού Σεναρίου παρουσιάζονται όπως και πριν οι πληροφορίες που αφορούν το συγκεκριμένο Εικονικό Σενάριο ενώ παράλληλα εμφανίζεται στο δεξί τμήμα της σελίδας ένα χρονόμετρο αντίστροφης μέτρησης μέχρι το προγραμματισμένο τέλος του Σεναρίου.




**Εικόνα 23** Περιβάλλον χρήστη που συμμετέχει σε ενεργοποιημένο ΕΣ

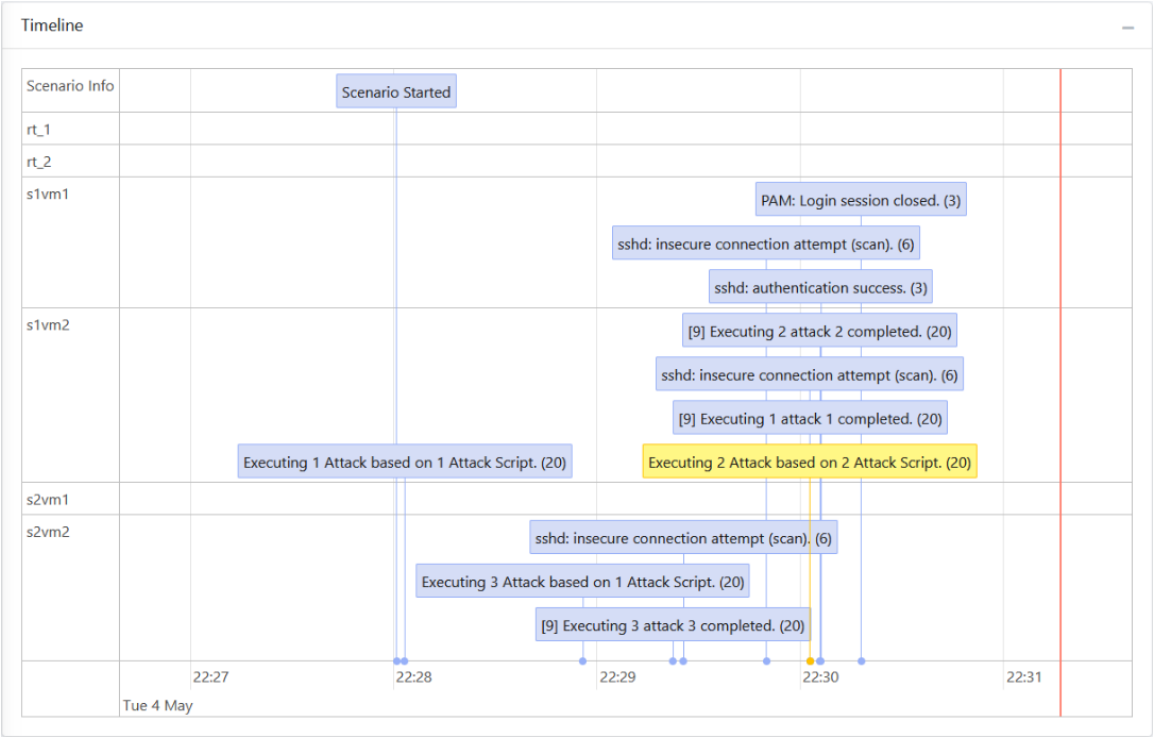
### 11.4.7 Παρακολούθηση Ροής Εικονικού Σεναρίου

Η μετάβαση στο περιβάλλον παρακολούθησης πραγματικού χρόνου έγινε πατώντας στο όνομα του Εικονικού Σεναρίου (Test Scenario) στον πίνακα Active Scenarios της Κεντρικής Σελίδας (Dashboard) με δικαιώματα διαχειριστή.

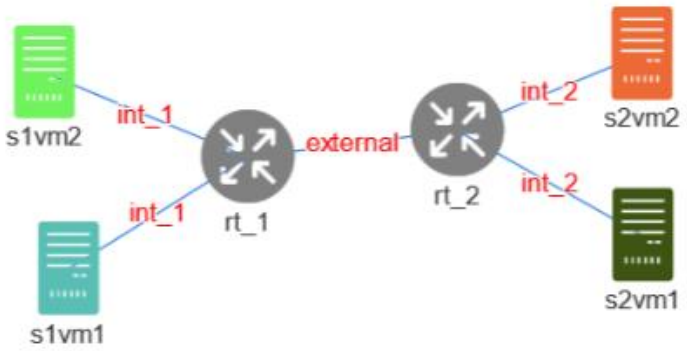



**Εικόνα 24.** Αρχική σελίδα διαχειριστή, όταν υπάρχει ενεργοποιημένο ΕΣ

Στην Εικόνα 25 που ακολουθεί φαίνεται ότι όντως λαμβάνονται αναφορές που αφορούν την εξέλιξη των επιθέσεων και καταγραφές περιστατικών ασφαλείας που παρουσιάζονται τόσο από την εφαρμογή Sinon που βρίσκεται εγκατεστημένη στο κάθε εικονικό μηχάνημα όσο και από τα Suricata και Wazuh. Οι αναφορές αυτές σε περίπτωση που ήταν στο παρελθόν (πριν την είσοδο στη σελίδα) δεν εμφανίζονται σαν κείμενα παρά μόνο σαν περιστατικά στο χρονοδιάγραμμα. Όλες οι αναφορές που λαμβάνονται σε πραγματικό χρόνο εμφανίζονται τόσο σαν κείμενο όσο και σαν περιστατικά στο χρονοδιάγραμμα. Η εμφάνιση ενός περιστατικού έχει σαν αποτέλεσμα την αλλαγή του χρώματος της αντίστοιχης συσκευής στο διάγραμμα δικτύου ώστε να γίνεται πιο εμφανές σε αυτούς που παρακολουθούν (Εικόνα 26).




**Εικόνα 25.** Αναφορές από Sinon και Wazuh Manager




**Εικόνα 26.** Εναλλαγή χρωμάτων στο διάγραμμα δικτύου για την επισήμανση συμβάντων

### 11.4.8 Επιτυχής Εκτέλεση των Αυτοματοποιημένων Επιθέσεων

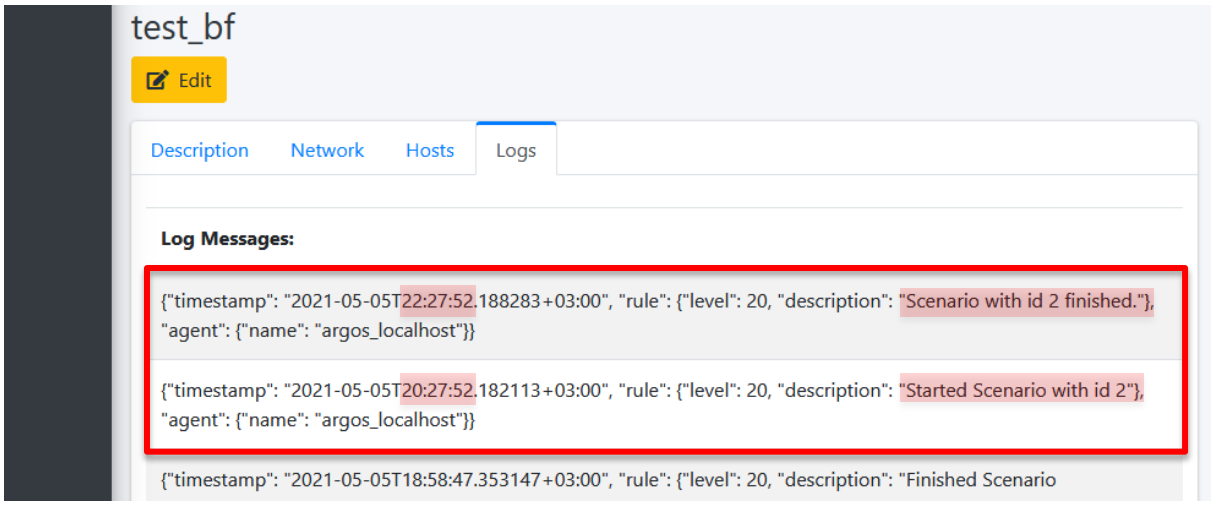
Τόσο από το περιβάλλον παρακολούθησης πραγματικού χρόνου (Εικόνα 25) όσο και στη ΒΔ (Εικόνα 7) εμφανίστηκαν οι καταγραφές που αφορούσαν την ροή της εκτέλεσης των Αυτοματοποιημένων επιθέσεων που καθορίστηκαν. Αν και οι συγκεκριμένες ενέργειες ήταν πολύ απλές ωστόσο οι επιθέσεις εκτελέστηκαν κανονικά και τα αποτελέσματα επέστρεψαν χωρίς κανένα πρόβλημα.

### 11.4.9 Τερματισμός Σεναρίου

Πατώντας στο κουμπί «Stop Scenario», το Σενάριο τερματίστηκε, και το προγραμματισμένο Event στη βάση δεδομένων για τον αυτόματο τερματισμό διαγράφηκε επιτυχώς.

### 11.4.10 Προετοιμασία και Επανεκτέλεση Σεναρίου

Μετά τον τερματισμό του Σεναρίου έγινε εκ νέου προετοιμασία του, η οποία διήρκησε 5 λεπτά και 46 δευτερόλεπτα. Στη συνέχεια το σενάριο επανεκτελέστηκε και αφέθηκε να ολοκληρωθεί αυτόματα. Όπως φαίνεται και στην Εικόνα 27 που ακολουθεί, το σενάριο τερματίστηκε στις 2 ώρες, όπως είχε καθοριστεί κατά την δημιουργία του.




**Εικόνα 27.** Αυτόματη ολοκλήρωση ΕΣ με την πάροδο της προγραμματισμένης διάρκειας

### 11.4.11 Καταστροφή ΕΠΜ

Με την ολοκλήρωση του Σεναρίου, εκτελέστηκε καταστροφή του ΕΠΜ. Η καταστροφή είχε σαν αποτέλεσμα την διαγραφή από το περιβάλλον ovirt των δικτύων και όλων των εικονικών μηχανημάτων που αφορούσαν το συγκεκριμένο ΕΠΜ. Επίσης από τον Wazuh Manager διαγράφηκαν αυτόματα οι εγγραφές των Agents που αφορούσαν το εν λόγω ΕΠΜ.

# Κεφάλαιο 12

# Αξιολόγηση

Η κύρια συνιστώσα της παρούσας διατριβής ήταν η ανάπτυξη μιας πλατφόρμας η οποία να μπορεί να εκτελέσει τις ενέργειες ενός ΨΠΒ. Χρησιμοποιώντας υφιστάμενα εργαλεία και υποδομές του πανεπιστημίου σε συνδυασμό με ελεύθερο λογισμικό και λογισμικού ανοικτού κώδικα επιτεύχθηκε η ανάπτυξη ενός ικανοποιητικού εργαλείου το οποίο είναι σε θέση να δημιουργήσει από μικρά τοπικά περιβάλλοντα σε πιο σύνθετα με την ύπαρξη περισσότερων του ενός δικτύου διασυνδεδεμένων μεταξύ τους με εικονικά μηχανήματα που προσομοιώνουν τις λειτουργίες εξυπηρετητών.

Επιπρόσθετα για εξοικονόμηση πόρων και χρόνου, ενσωματώθηκε επιτυχώς η δυνατότητα δημιουργίας διαφορετικών Σεναρίων για κάθε Πεδίο Μάχης. Με την χρήση των Σεναρίων προσφέρεται η δυνατότητα επαναχρησιμοποίησης των εικονικών μηχανημάτων σε μικρότερους χρόνους με διαφορετικές ρυθμίσεις όσον αφορά τους χρήστες με δικαιώματα πρόσβασης στα εικονικά μηχανήματα αλλά και τις αυτοματοποιημένες επιθέσεις που αυτά ενδέχεται να εκτελέσουν.

Φτάνοντας στο κρίσιμο σημείο των αυτοματοποιημένων επιθέσεων και των αποτελεσμάτων τους, δημιουργήθηκε ένα σύστημα βασισμένο σε Πρότυπα Επιθέσεων και μια εφαρμογή η οποία τρέχει σαν υπηρεσία στα εικονικά μηχανήματα και αναλαμβάνει να εκτελέσει όσες αυτοματοποιημένες επιθέσεις έχουν οριστεί μέσω του Σεναρίου και αφορούν το συγκεκριμένο εικονικό μηχάνημα. Κατά την δημιουργία των Προτύπων των Επιθέσεων μπορούν να χρησιμοποιηθούν μεταβλητές, οι οποίες αργότερα κατά την επιλογή των αυτοματοποιημένων επιθέσεων πρέπει να αντικατασταθούν με τις πραγματικές τιμές. Με αυτό τον τρόπο επιτρέπεται η επαναχρησιμοποίηση τους, χωρίς να απαιτείται κάθε φορά η επαναπληκτρολόγηση του συνόλου του κώδικα. Επίσης όλα τα πρότυπα των επιθέσεων διακινούνται και

αποθηκεύονται σε κωδικοποίηση Base64 για να αποφεύγεται τυχόν εντοπισμός τους από συστήματα ανίχνευσης κακόβουλου λογισμικού.

Σε μια τόσο πολυδιάστατη πλατφόρμα, που επικεντρώνεται σε τομείς που αφορούν την ασφάλεια των πληροφοριών ένας πολύ σημαντικός παράγοντας είναι η επίγνωση της κατάστασης και της εξέλιξης των Σεναρίων ανά πάσα στιγμή. Για την παρούσα υλοποίηση αυτό επιτεύχθηκε με τη χρήση συνδέσεων μέσω websockets, καταγραφές λογισμικών IDS, πληροφοριών της Βάσης Δεδομένων, βιβλιοθηκών Javascript και της τεχνολογίας AJAX. Το αποτέλεσμα, είναι ένα περιβάλλον απεικόνισης στο οποίο παρουσιάζονται σε πραγματικό χρόνο η εξέλιξη των Σεναρίων και της κατάστασης των μέσων. Όλες οι πληροφορίες εμφανίζονται σε ένα διαδραστικό χρονοδιάγραμμα με ένα αντίστοιχο διάγραμμα του Πεδίου Μάχης και παράλληλα καταγράφονται στην Βάση Δεδομένων ώστε να υπάρχει η δυνατότητα αναπαραγωγής τους.

Παράλληλα καταβλήθηκε μεγάλη προσπάθεια ώστε το περιβάλλον να είναι εύχρηστο και ευκολοκατανόητο από τους χρήστες και να μπορεί να χρησιμοποιηθεί με την ίδια ευκολία που χρησιμοποιούνται οι υπόλοιπες υπηρεσίες της καθημερινότητας μας. Η λειτουργία του εντός web browser, παρακάμπτει περιορισμούς διαλειτουργικότητας και διευκολύνει την χρήση του μέσω απομακρυσμένης πρόσβασης, κάτι ιδιαίτερα σημαντικό στις μέρες μας. Η κατηγοριοποίηση των χρηστών και η διαφοροποίηση των δικαιωμάτων τους προσφέρει μια κοινή εμπειρία η οποία διαφοροποιείται βάση της "ανάγκης γνώσης", ενώ η ενσωμάτωση συγκεντρωτικής διαχείρισης των χρηστών μέσω LDAP, διευκολύνει ακόμη περισσότερο την διαχείριση ολόκληρης της πλατφόρμας.

Τα αποτελέσματα από τις πειραματικές διατάξεις, οι χρόνοι απόκρισης και η γενικότερη εικόνα που παρουσίασε η πλατφόρμα κατά τις δοκιμές ήταν ιδιαίτερα ενθαρρυντικά. Σίγουρα υπάρχουν αρκετά περιθώρια βελτίωσης σε αρκετά σημεία, ωστόσο με την παρούσα διαμόρφωση είναι πολύ πιθανό ότι μπορεί να ανταπεξέλθει σε περιορισμένη χρήση για περαιτέρω εξαγωγή συμπερασμάτων και τελειοποίηση της σε βαθμό που να επιτρέπει την πιο ευρεία χρήση της.

# Κεφάλαιο 13

# Μελλοντικές Κατευθύνσεις

Σημαντικότερος ίσως τομέας ο οποίος επιδέχεται βελτίωση είναι η περαιτέρω ανάπτυξη του τρόπου λειτουργίας των αυτοματοποιημένων επιθέσεων ώστε να μπορεί να γίνει χρήση των αποτελεσμάτων από τις επιθέσεις που ακολουθούν. Μια πιθανή κατεύθυνση για αυτή την βελτίωση θα ήταν η εισαγωγή στην δημιουργία των Προτύπων Επιθέσεων κάποιας μεθόδου αξιολόγησης του αποτελέσματος, όπως για παράδειγμα η χρήση YARA rules και η τυποποίηση του τρόπου εξαγωγής των αποτελεσμάτων ώστε να μπορούν να χρησιμοποιηθούν σαν είσοδος στην επόμενη αυτοματοποιημένη επίθεση. Παράλληλα μπορούν να διερευνηθούν τρόποι για την κατάλληλη ενσωμάτωση υφιστάμενων λύσεων, όπως για παράδειγμα του Caldera και του Infection Monkey ώστε να υπάρχει η κατάλληλη ανταλλαγή πληροφορίων με την πλατφόρμα που δημιουργήθηκε.

Επίσης σημαντικός τομέας ο οποίος χρήζει διερεύνησης είναι η υλοποίηση εικονικών μηχανών σε περιβάλλον Microsoft Windows, η ενσωμάτωση εικονικών μηχανημάτων δικτυακού εξοπλισμού και η προσομοίωση συσκευών βιομηχανικού τύπου πχ Modbus, SCADA κλπ. Εφόσον ο σκοπός είναι η δημιουργία ρεαλιστικών σεναρίων τότε όλα τα ανωτέρω αποτελούν αδιαμφισβήτητα κρίσιμα χαρακτηριστικά τα οποία πρέπει να ενσωματωθούν, Στην παρούσα υλοποίηση η δημιουργία των εικονικών μηχανημάτων με πυρήνα Linux γίνεται χρησιμοποιώντας το cloud-init, ενώ για τις εικονικές μηχανές με λειτουργικό σύστημα Windows το περιβάλλον oVirt υποστηρίζει την αντίστοιχη τεχνολογία το sysprep. Αυτό που φάνηκε όμως στην πορεία είναι ότι αν και το oVirt υποστηρίζει τις εν λόγω τεχνολογίες αυτές είναι αρκετά προβληματικές. Μια λύση του τύπου Ansible ή Chef ίσως να είναι πολύ καλύτερη γι' αυτό και θα πρέπει να διερευνηθεί στο μέλλον. Όσον αφορά την προσομοίωση δικτυακού εξοπλισμού μια πολύ υποσχόμενη λύση φαίνεται να αποτελεί το Graphical Network Simulator 3 το οποίο

παρέχει τη δυνατότητα προσομοίωσης εξοπλισμού από εταιρείες όπως η Cisco, η Juniper, η Fortigate, η Microtik και άλλες το οποίο επίσης θα πρέπει να δοκιμαστεί κατά πόσον είναι δυνατό να ενσωματωθεί στην υφιστάμενη πλατφόρμα.

Ακόμη μία κατεύθυνση η οποία θα συνεισφέρει στην βελτίωση των λειτουργιών της πλατφόρμας είναι η ενσωμάτωση ενός συστήματος παρακολούθησης και ανατροφοδότησης όσο αφορά τα εικονικά μηχανήματα στο περιβάλλον oVirt. Για την λειτουργία της πλατφόρμας στην παρούσα διατριβή, έγινε η παραδοχή ότι οι καταστάσεις των εικονικών μηχανημάτων θα ελέγχονται πλήρως και αποκλειστικά από την πλατφόρμα που δημιουργήθηκε. Αυτό δημιουργεί αρκετά προβλήματα γιατί δεν είναι ρεαλιστικό. Για παράδειγμα αν μετά την δημιουργία ενός νέου ΨΠΒ όπου όλα τα εικονικά μηχανήματα είναι ενεργοποιημένα, απενεργοποιηθεί κάποιο μηχάνημα μέσω του περιβάλλοντος oVirt, αυτή η πληροφορία δεν φτάνει ποτέ στην πλατφόρμα με αποτέλεσμα το συγκεκριμένο εικονικό μηχάνημα να εξακολουθεί να εμφανίζεται ως ενεργοποιημένο. Τέτοιου είδους προβλήματα μπορούν να εξαλειφτούν με περαιτέρω ανάπτυξη των εφαρμογών που δημιουργήθηκαν ώστε να ενσωματώσουν λειτουργίες παρακολούθησης της κατάστασης των εικονικών μηχανημάτων.

Τέλος μία κατεύθυνση στην οποία μπορεί να υπάρξει σημαντική βελτίωση και αναμένεται να επιφέρει σημαντικά οφέλη από την μελλοντική χρήση της πλατφόρμας ως εργαλείο ηλεκτρονικής εκπαίδευσης (e-learning) είναι η ενσωμάτωση λειτουργιών αυτόματης βαθμολόγησης και αξιολόγησης. Στις περισσότερες από τις υφιστάμενες εμπορικές υλοποιήσεις ΨΠΒ η αξιολόγηση και η βαθμολόγηση των στόχων, βασίζεται στην αποστολή από τους χρήστες, αποδεικτικών στοιχείων για τις ενέργειες που εκτέλεσαν και τα αποτελέσματα που προέκυψαν τα οποία πρέπει στη συνέχεια να ελεγχθούν και να βαθμολογηθούν αναλόγως από το προσωπικό που διαχειρίζεται την πλατφόρμα. Υπάρχουν βέβαια και εξαιρέσεις αφού κάποιες από τις υφιστάμενες πλατφόρμες, όπως για παράδειγμα τα ΨΠΒ των εταιρειών Leonardo και IAI αναφέρουν το αυτοματοποιημένο σύστημα βαθμολόγησης στα διαθέσιμα χαρακτηριστικά τους. Η αυτόματη βαθμολόγηση είναι μια σύνθετη διεργασία η οποία για να επιτευχθεί απαιτείται η ύπαρξη των κατάλληλων πληροφοριών και η ανάπτυξη τεχνικών που να μπορούν να χρησιμοποιήσουν κατάλληλα τις πληροφορίες αυτές για να προκύψουν ορθά αποτελέσματα. Ωστόσο, παρόμοιες τεχνικές χρησιμοποιούνται τα τελευταία χρόνια και σε άλλους τομείς, όπως τα Ευφυή Συστήματα Διδασκαλίας (Intelligent

Tutoring Systems) και με την κατάλληλη παραμετροποίηση μπορούν να εφαρμοστούν και στην συγκεκριμένη εφαρμογή.

# Κεφάλαιο 14

# Επίλογος

Οι συσκευές που πριν μερικές δεκαετίες καταλάμβαναν ολόκληρα δωμάτια και κόστιζαν μια περιουσία για να αποκτηθούν, πλέον βρίσκονται στα χέρια του καθενός από εμάς και μάλιστα με περισσότερες δυνατότητες από τις συσκευές που χρησιμοποιήθηκαν για την μετάβαση του ανθρώπου στη σελήνη. Οι ολοένα αυξανόμενοι ρυθμοί ανάπτυξης της τεχνολογίας, η ενσωμάτωση της επιστήμης των υπολογιστών και των δικτύων σε κάθε άλλη μορφή επιστήμης αλλά και της βιομηχανίας δεν επέτρεψε την επίλυση σημαντικών προβλημάτων, σε θέματα ασφάλειας, τα οποία παρουσιάστηκαν από τα αρχικά στάδια αυτής της νέας εποχής.

Το 2020 υπήρξε η χρονιά η οποία μας υπενθύμισε ότι η ευελιξία και η προσαρμοστικότητα είναι χαρακτηριστικά τα οποία είναι απαραίτητα για την φυσική επιβίωση αλλά και για την επιβίωση των υποδομών, των υπηρεσιών και μέσων που αποτελούν την καθημερινότητα μας. Σε ελάχιστο χρόνο και στις πλείστες των περιπτώσεων εντελώς απροετοίμαστες, οι περισσότερες επιχειρήσεις και οργανισμοί κλήθηκαν να τροποποιήσουν εντελώς τον τρόπο εργασίας τους, εφαρμόζοντας σε μεγάλο βαθμό την τηλεργασία για την διατήρηση της επιχειρησιακής τους συνέχειας με άμεσο αντίκτυπο στις διαδικασίες ασφάλειας τους. Παράλληλα ο διαρκώς αυξανόμενος αριθμός των κυβερνοεπιθέσεων και ιδιαίτερα η αύξηση της χρήσης των ransomware καθιστούν τώρα αναγκαία όσο ποτέ την εξεύρεση άμεσων και αποτελεσματικών λύσεων.

Η σχολαστική διερεύνηση όλα αυτά τα χρόνια των διαφόρων τύπων επιθέσεων, έχει επιβεβαιώσει και στον κυβερνοχώρο ισχύει ότι ακριβώς και στις ένοπλες συρράξεις. Αν δεν γνωρίζεις τον αντίπαλο σου δεν μπορείς να τον αντιμετωπίσεις. Η γνώση του τρόπου δράσης των επιτιθέμενων και η ανάπτυξη βάση αυτής της γνώσης εργαλείων

προσομοίωσης θα υποβοηθήσουν με την σειρά τους στην καλύτερη εκπαίδευση του προσωπικού που ασχολείται με την ασφάλεια, και την δημιουργία ακόμα καλύτερων εργαλείων για τον έγκαιρο εντοπισμό και αντιμετώπιση των κακόβουλων περιστατικών.

Σίγουρα υπάρχουν και άλλοι τομείς οι οποίοι αναμένεται στο μέλλον να βοηθήσουν στον εντοπισμό και την αντιμετώπιση των κακόβουλων επιθέσεων, όπως η Τεχνητή Νοημοσύνη και η Μηχανική Μάθηση, ωστόσο οι ειδικοί του τομέα θα πρέπει πάντα να είναι σε θέση να μπορούν να διακρίνουν τις κακόβουλες ενέργειες και τον τρόπο δράσης των επιτιθέμενων ώστε να είναι βέβαιοι ότι ακόμα και οι νέες τεχνολογίες χρησιμοποιούνται σωστά και είναι αποτελεσματικές.

Η ανάπτυξη και η χρήση Ψηφιακών Πεδίων Βολής, ιδιαίτερα σε εκπαιδευτικά ιδρύματα, αποτελεί μια πολύ αποτελεσματική προσέγγιση για τον τρόπο διαχείρισης της κυβερνοασφάλειας. Χρησιμοποιώντας τις γνώσεις και τις εμπειρίες από τα προηγούμενα χρόνια, τα ΨΠΒ μέσω ερευνητικών προγραμμάτων μπορούν να εξασφαλίσουν την ανάπτυξη καλύτερων εργαλείων εντοπισμού και αντιμετώπισης ενώ επιπρόσθετα μπορούν να συνεισφέρουν στην αποτελεσματικά κατάρτιση του προσωπικού που θα κληθεί να αντιμετωπίσει αυτά τα περιστατικά.

# Βιβλιογραφία


[1] Robert Hackett. (2020, September) Fortune.com. [Online]. https://fortune.com/2020/09/18/ransomware-police-investigating-hospital-cyber-attack-death/

[2] Fireeye. (2020, February) Fireeye.com M-Trends 2020. [Online]. https://content.fireeye.com/m-trends/rpt-m-trends-2020

[3] Andy Applebaum, Doug Miller, Blake Strom, Chris Korban, and Ross Wolf, "Intelligent, automated red team emulation," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, Los Angeles, USA, 2016, pp. 363-373.

[4] E.U. Horizon 2020. (2021, Mar.) Concordia Horizon 2020. [Online]. https://www.concordia-h2020.eu/kypo-cyber-range/

[5] Fred Cohen, "Simulating cyber attacks, defences, and consequences," *Computers & Security*, vol. 18, no. 6, pp. 479-518, 1999.

[6] Blake Strom et al., "Mitre att&ck: Design and philosophy," Mitre, Technical Report 18-0944-11, 2018.

[7] Doug Miller et al. (2018, June) Mitre. [Online]. https://www.mitre.org/publications/technical-papers/automated-adversary-emulation-a-case-for-planning-and-acting-with

[8] Andy Applebaum, Doug Miller, Blake Strom, Henry Foster, and Cody Thomas, "Analysis of Automated Adversary Emulation Techniques," in *SummerSim-SCS*, Bellevue, 2017, pp. 155-166.

[9] Simon Yusuf Enoch, Zhibin Moon, Chun Yong Huang, Donghwan Lee, Myung Kil Ahn, and Dong Seong Kim, "HARMer: Cyber-Attacks Automation and Evaluation," *IEEE Access*, vol. 8, pp. 129397-129414, July 2020.

[10] Sunders Bruskin, Polina Zilberman, and Rami Puzi, "SoK: A Survey of Open Source Threat Emulators," *ArXiv*, vol. 2003.01518, Mar. 2020.

[11] Jörg Hoffmann, "Simulated Penetration Testing: From "Dijkstra" to "Turing Test++"," in *Proceedings of the International Conference on Automated Planning and Scheduling*, Jerusalem, Israel, 2015, pp. 364-372.

[12] Lori Pridmore, Patrick Lardieri, and Robert Hollister, "National Cyber Range (NCR) automated test tools: Implications and application to network-centric support tools," in *IEEE AUTOTESTCON*, Orlando, FL, USA, 2010, pp. 1-4.

[13] Bernard Ferguson, Anne Tall, and Denise Olsen, "National Cyber Range Overview," in *2014 IEEE Military Communications Conference*, Baltimore, 2014, pp. 123-128.

[14] Working Group 5. (2020, March) Understanding Cyber Ranges: From Hype to Reality. PDF. [Online]. https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[15] Carlos Perez Gonzalez. (2020, May) Cyber Range – The Future of Cyber Security Training. PDF. [Online]. https://www.sans.org/reading-room/whitepapers/training/paper/39550

[16] Enrico Russo, Gabriele Costa, and EAlessandro Armando, "Building next generation Cyber Ranges with CRACK," *Computers & Security*, vol. 95, no. 101837, pp. 1-23, August 2020.

[17] Thibault Debatty and Mees Wim, "Building a Cyber Range for training CyberDefense Situation Awareness," in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, Budva, 2019, pp. 1-6.

[18] Gabriele Costa, Enrico Russo, and Alessandro Armando, "Automating the Generation of Cyber Range Virtual Scenarios with VSDL," in *The Italian Conference on CyberSecurity (ITASEC2018)*, Milan, 2018.

[19] Cuong Pham, Dat Tang, Ken-ichi Chinen, and Razvan Beuran, "CyRIS: A Cyber Range Instantiation System for Facilitating Security Training," in *SoICT '16: Proceedings of the Seventh Symposium on Information and Communication Technology*, Ho Chi Minh City, Vietnam, 2016, pp. 251-258.

[20] Βασίλειος Βεσκούκης, *Στοιχεία τεχνολογίας λογισμικού*. Αθήνα, Ελλάδα: Εκδόσεις Κάλλιπος, 2015.

[21] Guy Propper. (2020, July) HELPNETSECURITY. [Online]. https://www.helpnetsecurity.com/2020/07/31/what-are-script-based-attacks/

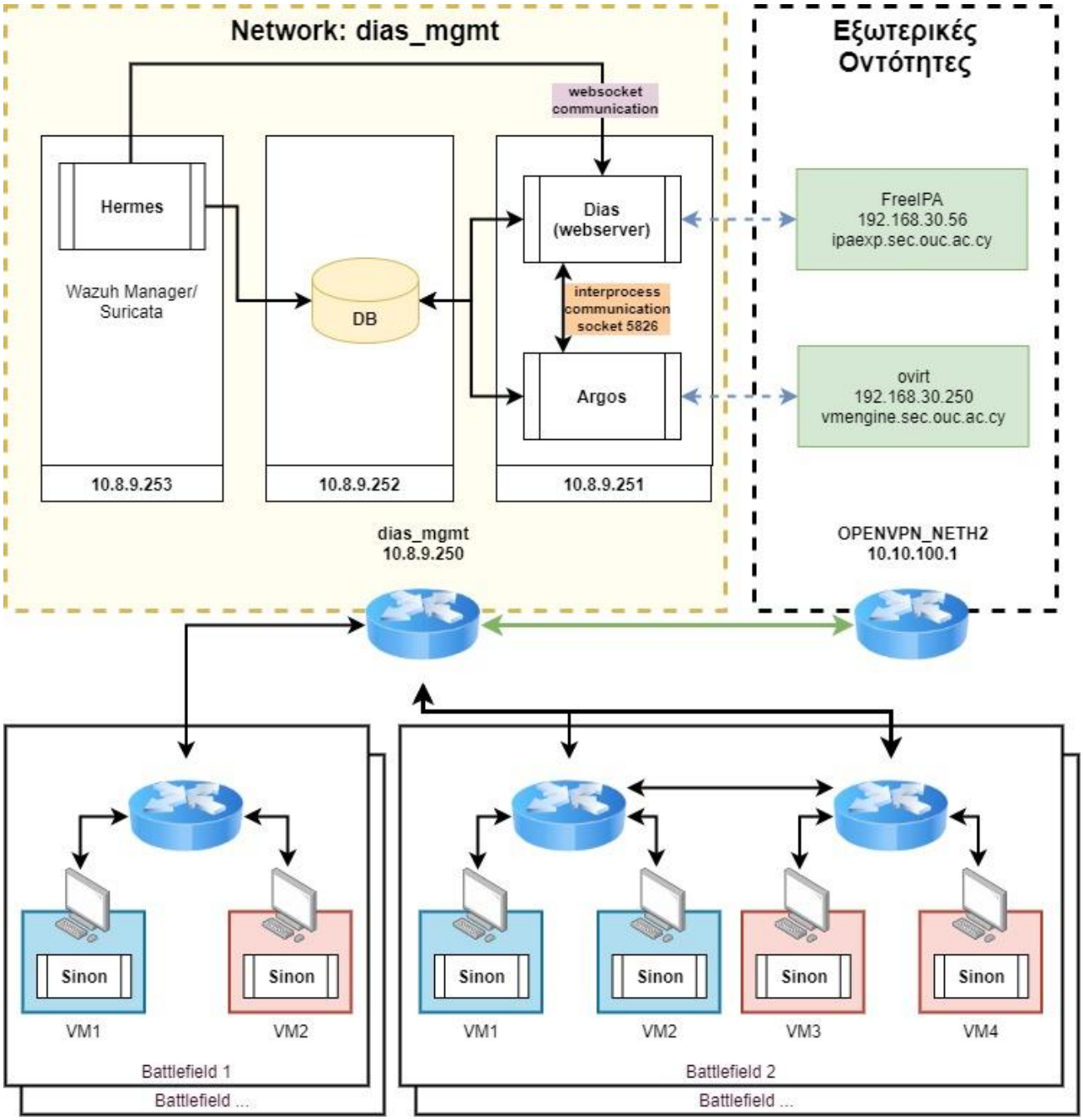
# Παράρτημα Α

# Δομή Συστήματος

Στο διάγραμμα που ακολουθεί με κίτρινο χρώμα πάνω αριστερά είναι το σύνολο των συστημάτων που αναπτύχθηκαν για την υλοποίηση της πλατφόρμας. Εκτός από τις διαφορετικές εικονικές μηχανές που αποτελούν την πλατφόρμα, απεικονίζονται επίσης οι εφαρμογές αλλά και ο τρόπος επικοινωνίας.

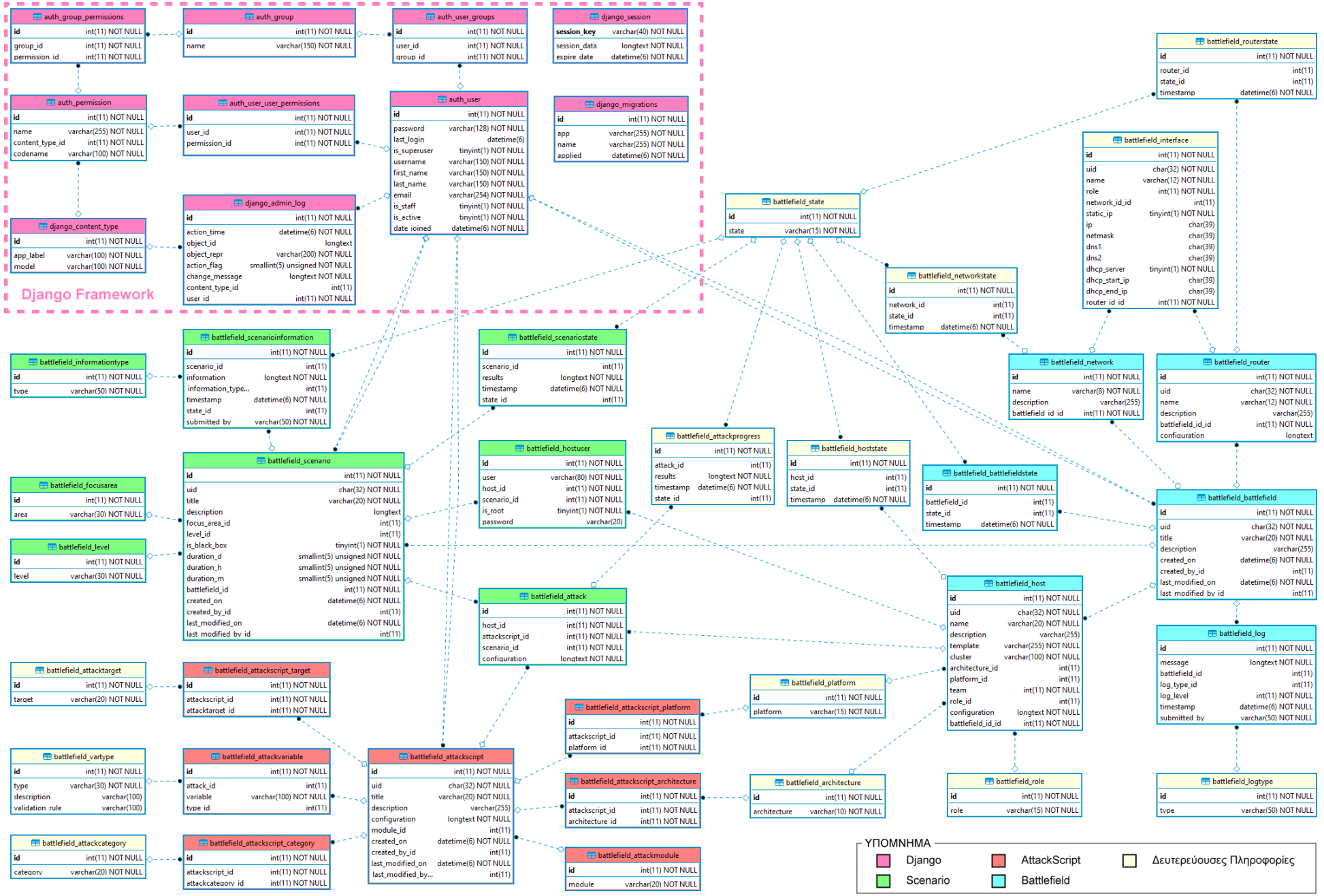
Η επικοινωνία με τις Εξωτερικές οντότητες επιτυγχάνεται μέσω μια του OPENVPN_NETH2 δρομολογητή ο οποίος είναι υλοποιημένος ως εικονική μηχανή με λειτουργικό σύστημα NethServer.

Τα Εικονικά Πεδία Μάχης που απεικονίζονται δεν ανήκουν στην δομή του συστήματος, σχεδιάστηκαν ώστε να γίνει αντιληπτή η συνδεσμολογία που ακολουθείται όταν ένα καινούριο ΕΠΜ δημιουργείται στην πλατφόρμα.


Network: dias_mgmt
Εξωτερικές Οντότητες
websocket communication
Hermes
Wazuh Manager/ Suricata
DB
Dias (webserver)
interprocess communication socket 5826
Argos
FreeIPA
192.168.30.56
ipaexp.sec.ouc.ac.cy
ovirt
192.168.30.250
vmengine.sec.ouc.ac.cy
10.8.9.253
10.8.9.252
10.8.9.251
dias_mgmt
10.8.9.250
OPENVPN_NETH2
10.10.100.1
Sinon
VM1
VM2
VM3
VM4
Battlefield 1
Battlefield ...
Battlefield 2
Battlefield ...

# Παράρτημα Β

# Δομή Βάσης Δεδομένων


Django Framework
auth_group_permissions
id int(11) NOT NULL
group_id int(11) NOT NULL
permission_id int(11) NOT NULL
auth_group
id int(11) NOT NULL
name varchar(150) NOT NULL
auth_user_groups
id int(11) NOT NULL
user_id int(11) NOT NULL
group_id int(11) NOT NULL
django_session
session_key varchar(40) NOT NULL
session_data longtext NOT NULL
expire_date datetime(6) NOT NULL
auth_permission
id int(11) NOT NULL
name varchar(255) NOT NULL
content_type_id int(11) NOT NULL
codename varchar(100) NOT NULL
auth_user_user_permissions
id int(11) NOT NULL
user_id int(11) NOT NULL
permission_id int(11) NOT NULL
auth_user
id int(11) NOT NULL
password varchar(128) NOT NULL
last_login datetime(6)
is_superuser tinyint(1) NOT NULL
username varchar(150) NOT NULL
first_name varchar(150) NOT NULL
last_name varchar(150) NOT NULL
email varchar(254) NOT NULL
is_staff tinyint(1) NOT NULL
is_active tinyint(1) NOT NULL
date_joined datetime(6) NOT NULL
django_migrations
id int(11) NOT NULL
app varchar(255) NOT NULL
name varchar(255) NOT NULL
applied datetime(6) NOT NULL
django_admin_log
id int(11) NOT NULL
action_time datetime(6) NOT NULL
object_id longtext
object_repr varchar(200) NOT NULL
action_flag smallint(5) unsigned NOT NULL
change_message longtext NOT NULL
content_type_id int(11)
user_id int(11) NOT NULL
django_content_type
id int(11) NOT NULL
app_label varchar(100) NOT NULL
model varchar(100) NOT NULL
battlefield_routerstate
id int(11) NOT NULL
router_id int(11)
state_id int(11)
timestamp datetime(6) NOT NULL
battlefield_interface
id int(11) NOT NULL
uid char(32) NOT NULL
name varchar(12) NOT NULL
role int(11) NOT NULL
network_id_id int(11)
static_ip tinyint(1) NOT NULL
ip char(39)
netmask char(39)
dns1 char(39)
dns2 char(39)
dhcp_server tinyint(1) NOT NULL
dhcp_start_ip char(39)
dhcp_end_ip char(39)
router_id_id int(11) NOT NULL
battlefield_state
id int(11) NOT NULL
state varchar(15) NOT NULL
battlefield_networkstate
id int(11) NOT NULL
network_id int(11)
state_id int(11)
timestamp datetime(6) NOT NULL
battlefield_network
id int(11) NOT NULL
name varchar(8) NOT NULL
description varchar(255)
battlefield_id_id int(11) NOT NULL
battlefield_router
id int(11) NOT NULL
uid char(32) NOT NULL
name varchar(12) NOT NULL
description varchar(255)
battlefield_id_id int(11) NOT NULL
configuration longtext
battlefield_scenarioinformation
id int(11) NOT NULL
scenario_id int(11)
information longtext NOT NULL
information_type... int(11)
timestamp datetime(6) NOT NULL
state_id int(11)
submitted_by varchar(50) NOT NULL
battlefield_scenariostate
id int(11) NOT NULL
scenario_id int(11)
results longtext NOT NULL
timestamp datetime(6) NOT NULL
state_id int(11)
battlefield_informationtype
id int(11) NOT NULL
type varchar(50) NOT NULL
battlefield_attackprogress
id int(11) NOT NULL
attack_id int(11)
results longtext NOT NULL
timestamp datetime(6) NOT NULL
state_id int(11)
battlefield_hoststate
id int(11) NOT NULL
host_id int(11)
state_id int(11)
timestamp datetime(6) NOT NULL
battlefield_battlefieldstate
id int(11) NOT NULL
battlefield_id int(11)
state_id int(11)
timestamp datetime(6) NOT NULL
battlefield_hostuser
id int(11) NOT NULL
user varchar(80) NOT NULL
host_id int(11) NOT NULL
scenario_id int(11) NOT NULL
is_root tinyint(1) NOT NULL
password varchar(20)
battlefield_scenario
id int(11) NOT NULL
uid char(32) NOT NULL
title varchar(20) NOT NULL
description longtext
focus_area_id int(11)
level_id int(11)
is_black_box tinyint(1) NOT NULL
duration_d smallint(5) unsigned NOT NULL
duration_h smallint(5) unsigned NOT NULL
duration_m smallint(5) unsigned NOT NULL
battlefield_id int(11) NOT NULL
created_on datetime(6) NOT NULL
created_by_id int(11)
last_modified_on datetime(6) NOT NULL
last_modified_by_id int(11)
battlefield_focusarea
id int(11) NOT NULL
area varchar(30) NOT NULL
battlefield_level
id int(11) NOT NULL
level varchar(30) NOT NULL
battlefield_battlefield
id int(11) NOT NULL
uid char(32) NOT NULL
title varchar(20) NOT NULL
description varchar(255)
created_on datetime(6) NOT NULL
created_by_id int(11)
last_modified_on datetime(6) NOT NULL
last_modified_by_id int(11)
battlefield_attack
id int(11) NOT NULL
host_id int(11) NOT NULL
attackscript_id int(11) NOT NULL
scenario_id int(11) NOT NULL
configuration longtext NOT NULL
battlefield_host
id int(11) NOT NULL
uid char(32) NOT NULL
name varchar(20) NOT NULL
description varchar(255)
template varchar(255) NOT NULL
cluster varchar(100) NOT NULL
architecture_id int(11)
platform_id int(11)
team int(11) NOT NULL
role_id int(11)
configuration longtext NOT NULL
battlefield_id_id int(11) NOT NULL
battlefield_log
id int(11) NOT NULL
message longtext NOT NULL
battlefield_id int(11)
log_type_id int(11)
log_level int(11) NOT NULL
timestamp datetime(6) NOT NULL
submitted_by varchar(50) NOT NULL
battlefield_attacktarget
id int(11) NOT NULL
target varchar(20) NOT NULL
battlefield_attackscript_target
id int(11) NOT NULL
attackscript_id int(11) NOT NULL
attacktarget_id int(11) NOT NULL
battlefield_platform
id int(11) NOT NULL
platform varchar(15) NOT NULL
battlefield_attackscript_platform
id int(11) NOT NULL
attackscript_id int(11) NOT NULL
platform_id int(11) NOT NULL
battlefield_vartype
id int(11) NOT NULL
type varchar(30) NOT NULL
description varchar(100)
validation_rule varchar(100)
battlefield_attackvariable
id int(11) NOT NULL
attack_id int(11)
variable varchar(100) NOT NULL
type_id int(11)
battlefield_attackscript
id int(11) NOT NULL
uid char(32) NOT NULL
title varchar(20) NOT NULL
description varchar(255)
configuration longtext NOT NULL
module_id int(11)
created_on datetime(6) NOT NULL
created_by_id int(11)
last_modified_on datetime(6) NOT NULL
last_modified_by... int(11)
battlefield_attackscript_architecture
id int(11) NOT NULL
attackscript_id int(11) NOT NULL
architecture_id int(11) NOT NULL
battlefield_architecture
id int(11) NOT NULL
architecture varchar(10) NOT NULL
battlefield_role
id int(11) NOT NULL
role varchar(15) NOT NULL
battlefield_logtype
id int(11) NOT NULL
type varchar(50) NOT NULL
battlefield_attackcategory
id int(11) NOT NULL
category varchar(20) NOT NULL
battlefield_attackscript_category
id int(11) NOT NULL
attackscript_id int(11) NOT NULL
attackcategory_id int(11) NOT NULL
battlefield_attackmodule
id int(11) NOT NULL
module varchar(20) NOT NULL
ΥΠΟΜΝΗΜΑ
Django
Scenario
AttackScript
Battlefield
Δευτερεύουσες Πληροφορίες

# Παράρτημα Γ

# Virtual Machine Templates

Σε αυτό το παράρτημα παρουσιάζονται τα τεχνικά χαρακτηριστικά, το λογισμικό και οι λοιπές ρυθμίσεις στις οποίες βασίζονται τα Templates των Εικονικών Μηχανημάτων του περιβάλλοντος oVirt. Όλα τα Templates που αφορούν την πλατφόρμα dias, αρχίζουν με το πρόθεμα dias_, για να είναι ευδιάκριτα και να μπορούν εύκολα να διαχωριστούν από άλλα Templates που πιθανόν να δημιουργηθούν για άλλους σκοπούς. Templates που δεν αρχίζουν με το πρόθεμα dias_ δεν λαμβάνονται υπόψη από την πλατφόρμα και δεν μπορούν να χρησιμοποιηθούν για τη δημιουργία Hosts.

Απαραίτητη προϋπόθεση για την σωστή ενσωμάτωση ενός νέου Template στην πλατφόρμα, είναι να σφραγιστεί (sealed) κατά τη δημιουργία του και να του αφαιρεθούν όλες οι κάρτες δικτύου. Η διαμόρφωση του δικτυακού εξοπλισμού αναλαμβάνεται πλήρως από την πλατφόρμα και ενδέχεται να προκύψουν προβλήματα αν υπάρχουν υφιστάμενες κάρτες δικτύου στο Template.

# 1 dias_caldera

| Ρόλος | Επιτιθέμενος |
|---|---|
| Λειτουργικό Σύστημα | Ubuntu 20.04.02 LTS (Focal Fossa) |
| CPU | 1 πυρήνας |
| RAM | 2048 MB |
| Κάρτες Δικτύου | Καμία - Προστίθενται δυναμικά κατά την παραμετροποίηση του ΕΠΜ |
| Σκληρός Δίσκος | 10 GB |
| Λογισμικό | Caldera (v3.0.0)<br>Cloud-init (v20.4.1-0ubuntu20.04.1)<br>Qemu-guest-agent (v4.2.1)<br>Wazuh agent (v3.9.5-1)<br>OpenSSh (v8.2p1) - OpenSSL (v1.1.1f)<br>Git(v.2.25.1)<br>Golang (go1.13.8) |
| Άλλες ρυθμίσεις | Προεγκατεστημένο service που επιτρέπει στο caldera να ξεκινά αυτόματα |

# 2 dias_ neth_rt

| Ρόλος | Δρομολογητής |
|---|---|
| Λειτουργικό Σύστημα | Cent OS 7-9.2009.1 |
| CPU | 1 πυρήνας |
| RAM | 1024 MB |
| Κάρτες Δικτύου | Καμία - Προστίθενται δυναμικά κατά την παραμετροποίηση του ΕΠΜ. |
| Σκληρός Δίσκος | 10 GB |
| Λογισμικό | NethServer (v7.9.2009)<br>Cloud-init (v19.4)<br>Qemu-guest-agent (v2.12.0)<br>Wazuh agent (v3.9.5-1)<br>Opensshserver (v7.4p1) - OpenSSL (v1.0.2k-fips) |
| Άλλες ρυθμίσεις | Εκτός από τις κάρτες δικτύου που προστίθενται δυναμικά κατά την δημιουργία του ΕΠΜ προστίθεται αυτόματα ακόμα μία η οποία χρησιμοποιείται για την διασύνδεση του με το Δρομολογητή Διαχείρισης. |

# 3 dias_Ubuntu_Desktop

| | |
|---|---|
| Ρόλος | Γενικής Χρήσης |
| Λειτουργικό Σύστημα | 18.04.5 LTS (Bionic Beaver) |
| CPU | 1 πυρήνας |
| RAM | 2048 MB |
| Κάρτες Δικτύου | Καμία - Προστίθενται δυναμικά κατά την παραμετροποίηση του ΕΠΜ. |
| Σκληρός Δίσκος | 15 GB |
| Λογισμικό | Cloud-init (v20.4.1-0ubuntu1~18.04.1)<br>Qemu-guest-agent (v2.11.1)<br>Wazuh agent (v3.9.5-1)<br>Opensshserver (v7.6p1) - OpenSSL (v1.0.2)<br>Git (v2.17.1)<br>Python 3(v3.6.9)<br>Mysql-common(v5.7.33)<br>Hydra(v8.6)<br>Nmap(v7.60) |
| Άλλες ρυθμίσεις | Περιλαμβάνει την εφαρμογή sinon η οποία είναι υπεύθυνη για την εκτέλεση αυτοματοποιημένων επιθέσεων εφόσον κάτι τέτοιο περιλαμβάνεται στο σενάριο. |

# Παράρτημα Δ

# Εγχειρίδιο Χρήσης

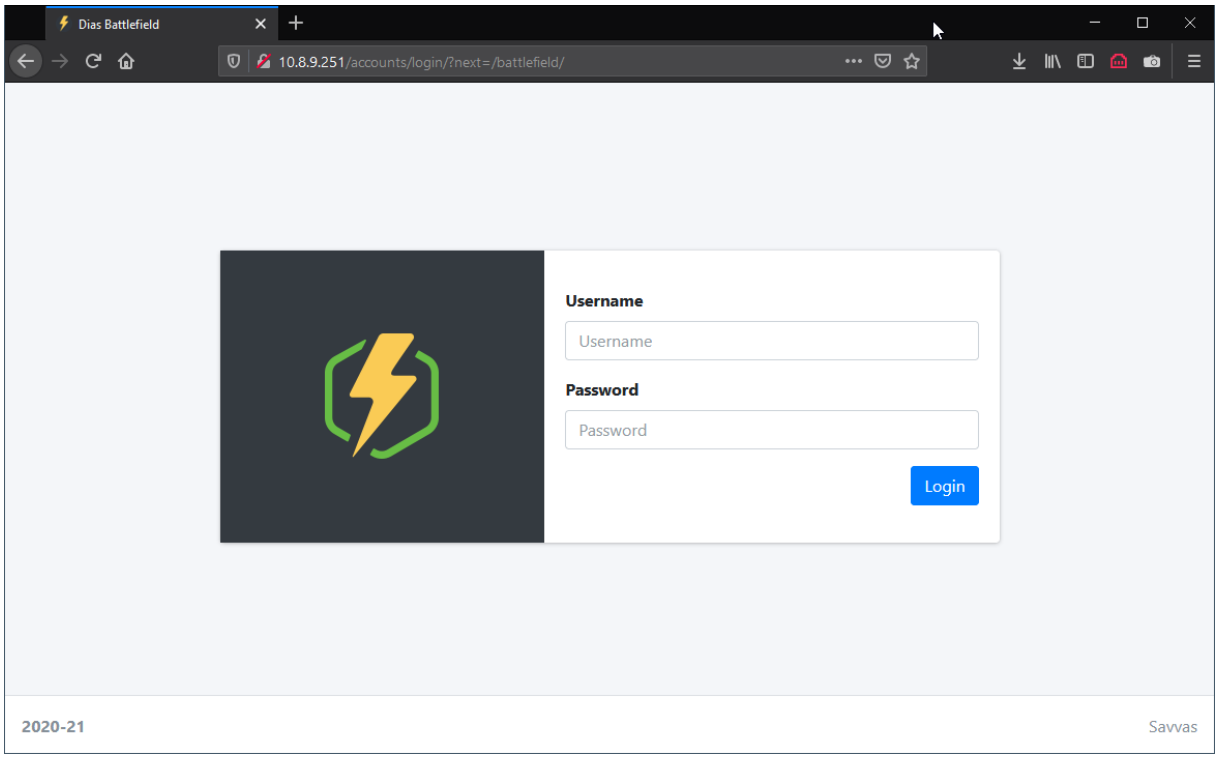
## Δ.1 Περιγραφή Ενεργειών

Στο εγχειρίδιο χρήσης περιγράφονται αναλυτικά τα βήματα για την εκτέλεση των διάφορων λειτουργιών που προσφέρει η πλατφόρμα Dias. Στις ενότητες του Παρατήματος που ακολουθούν, περιγράφονται αναλυτικά τα πεδία εισαγωγής δεδομένων κάθε οντότητας.

**Περιεχόμενα**

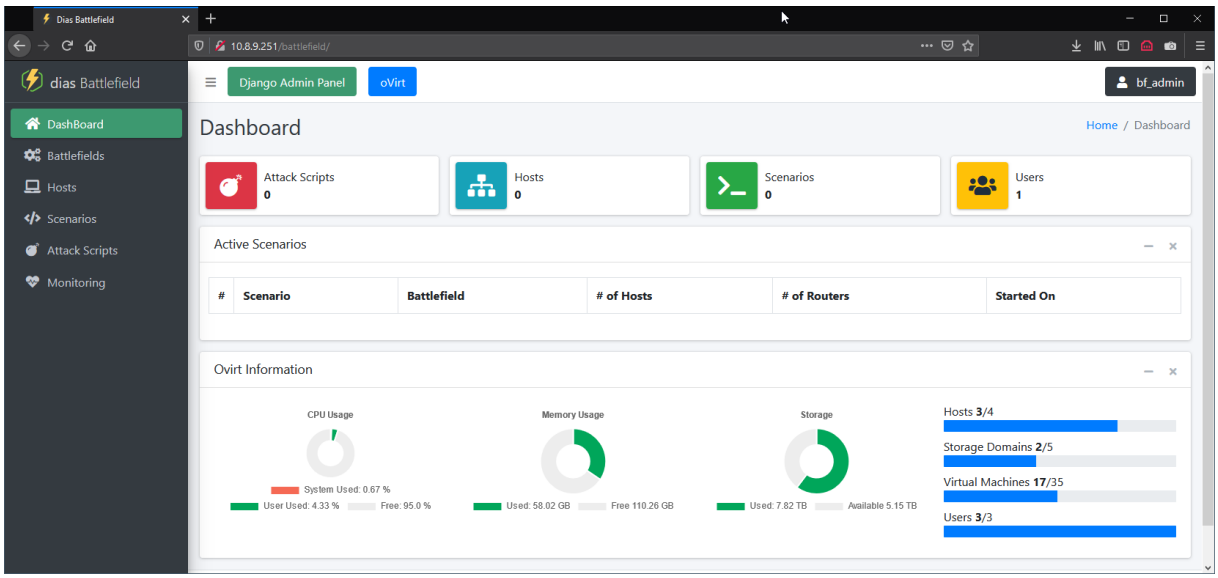
# 4 Σελίδα Σύνδεσης Χρήστη

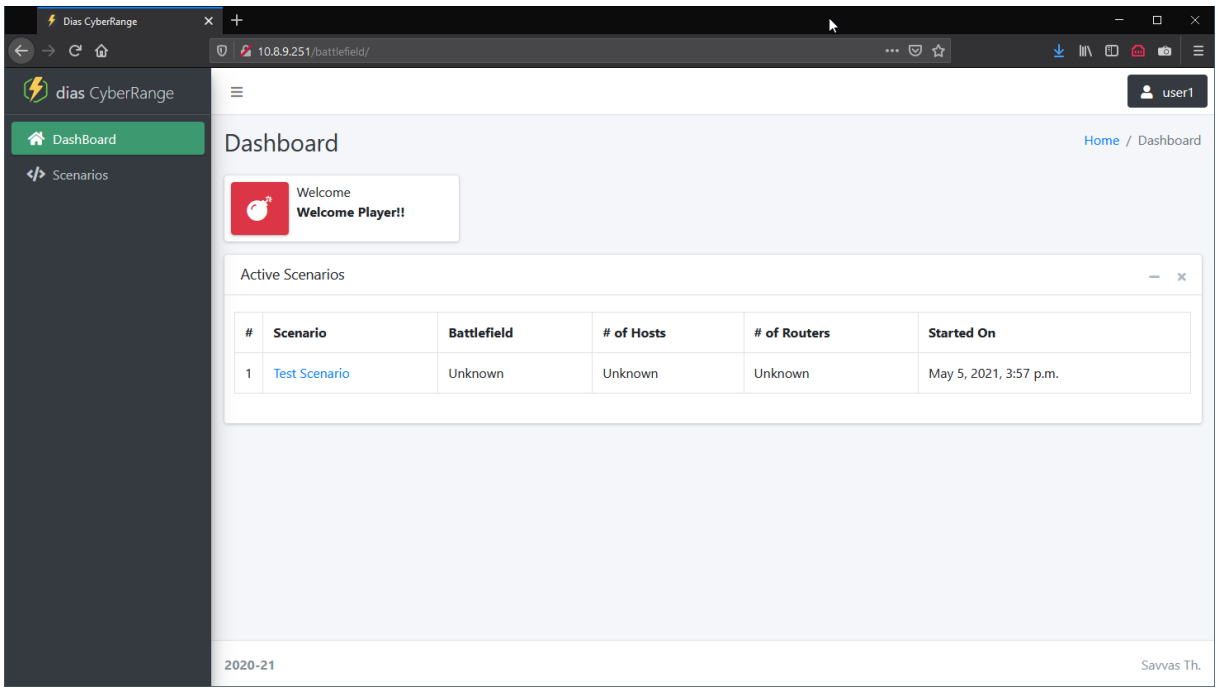
Πριν γίνει δυνατή η εμφάνιση οποιασδήποτε πληροφορίας ή η εκτέλεση οποιασδήποτε ενέργειας ο χρήστης πρέπει να συνδεθεί στην πλατφόρμα χρησιμοποιώντας το όνομα χρήστη και τον κωδικό που διατηρεί στον εξυπηρετητή FreeIPA. Με αυτό τον τρόπο επιτυγχάνεται κεντρική διαχείριση των χρηστών και των δικαιωμάτων τους.



# 5 Αρχική Σελίδα - Dashboard

Στην Αρχική Σελίδα εφόσον ο χρήστης συνδεθεί με δικαιώματα διαχειριστή τότε στο πάνω μέρος προβάλλονται στατιστικά που αφορούν το συγκεκριμένο περιβάλλον και το περιβάλλον oVirt. Ακολούθως αν ο χρήστης έχει δικαιώματα Διαχειριστή ή Διαχειριστή Σεναρίων τότε εμφανίζονται όλα τα σενάρια που βρίσκονται σε εξέλιξη ενώ αν έχει δικαιώματα χρήστη τότε εμφανίζονται μόνο τα ενεργά σενάρια στα οποία συμμετέχει.



# 6 Εικονικά Πεδία Μάχης

Τα Εικονικά Πεδία Μάχης αποτελούν τη βάση ολόκληρου του συστήματος. Ένα ΕΠΜ αποτελείται από Δίκτυα, Δικτυακό Εξοπλισμό και τους Hosts που αποτελούν τις τερματικές συσκευές, διασυνδεδεμένα κατά τέτοιο τρόπο ώστε να προσομοιάζουν συνήθως μια τοπολογία που αντιστοιχεί σε μια πραγματική κατάσταση. Υπάρχει μεγάλη ευελιξία στα ΕΠΜ που μπορούν να δημιουργηθούν αφού τόσο ο αριθμός και η τοπολογία των δικτύων και του δικτυακού εξοπλισμού όσο και ο αριθμός και η διασύνδεση των Hosts περιορίζονται μόνο από τους διαθέσιμους πόρους του περιβάλλοντος oVirt. Για κάθε ΕΠΜ μπορούν να δημιουργηθούν περισσότερα από ένα Σενάρια, ωστόσο μόνο ένα μπορεί να είναι ενεργό ανά πάσα στιγμή.

## 6.1 Δημιουργία Εικονικού Πεδίου Μάχης

Εικονικά Πεδία Μάχης μπορούν να δημιουργήσουν οι χρήστες που ανήκουν στην ομάδα:

- dias_admins

Το σύνολο των πεδίων με τον τύπο και τους περιορισμούς τους φαίνονται στην Ενότητα Δ.2 του Παραρτήματος

Για να ανοίξετε την σελίδα καταχώρησης ενός νέου ΕΠΜ

- Από το κυρίως μενού πατήστε στο “Battlefields”
- Πατήστε στο κουμπί Προσθήκη Νέου (“Add New”) που βρίσκεται στο πάνω μέρος της σελίδας

Με την εμφάνιση της σελίδας καταχώρησης ενός νέου ΕΠΜ, διακρίνονται τα ακόλουθα στοιχεία:

1. Τα πεδία Τίτλος και Περιγραφή, που αφορούν το ΕΠΜ.
2. Το κουμπί εισαγωγής Νέου Δικτύου (“Add Network”).
    i. Κάθε ΕΠΜ πρέπει να περιλαμβάνει ένα ή περισσότερα Δίκτυα.

    ii. Τα δίκτυα ουσιαστικά αποτελούν τις “φυσικές” διασυνδέσεις των συσκευών.

iii. Το κάθε δίκτυο στη συνέχεια μπορεί να χρησιμοποιηθεί στις διεπαφές (interfaces) των δρομολογητών για να ρυθμιστούν οι ιδιότητες του (subnet, dhcp κλπ)

3. Το κουμπί Αποθήκευσης των Δικτύων ("Save Networks"), το οποίο απαιτείται να πατηθεί ώστε τα δίκτυα που ορίστηκαν να γίνουν διαθέσιμα στις υπόλοιπες συσκευές του ΕΠΜ.
4. Το κουμπί εισαγωγής Νέου Δρομολογητή.
   i. Κάθε δρομολογητής αποτελείται από τα πεδία "Όνομα" και "Ρυθμίσεις". Το πεδίο ρυθμίσεις δεν είναι υποχρεωτικό και είναι τύπου json. Σε αυτό μπορούν να τοποθετηθούν εντολές για παραμετροποίηση της συσκευής του δρομολογητή.
   ii. Κάθε δρομολογητής αντιστοιχεί σε μια Εικονική Μηχανή με Λειτουργικό Σύστημα Nethserver.
   iii. Σε κάθε δρομολογητή μπορούν να δημιουργηθούν διεπαφές, οι οποίες αντιστοιχούν σε κάρτες δικτύου στην Εικονική Μηχανή του Nethserver.
   iv. Στην κάθε διεπαφή μπορούν να καταχωρηθούν στατικά χαρακτηριστικά δικτύου (ip/subnet/dns) ή να λαμβάνονται από υφιστάμενο DHCP Server.
   v. Επίσης στην κάθε διεπαφή μπορεί να ενεργοποιηθεί λειτουργία DHCP Server, ώστε να γίνεται διανομή ρυθμίσεων δικτύου (διευθύνσεων IP, subnet, gateway, nameserver) στο συγκεκριμένο δίκτυο.
   vi. Για την κάθε διεπαφή ορίζεται επίσης το δίκτυο στο οποίο συνδέεται και ο τύπος του δικτύου.
   vii. Οι πιθανοί τύποι των δικτύων ορίζονται στον Nethserver και είναι οι ακόλουθοι:
      1) Green: Τοπικό Δίκτυο. Οι χρήστες αυτών των δικτύων δεν έχουν περιορισμούς.
      2) Blue: δίκτυα φιλοξενούμενων (Guest Networks), οι πληροφορίες μετακινούνται προς τα Πορτοκαλί και Κόκκινα δίκτυα αλλά όχι προς τα Πράσινα.
      3) Orange: χρησιμοποιείται για να οριστούν DMZ περιοχές, οι πληροφορίες κυκλοφορούν ελεύθερα προς τα κόκκινα δίκτυα αλλά όχι προς τα Μπλε και πράσινα.

4) Red: Δημόσια Δίκτυα (πχ Internet), η κυκλοφορία επιτρέπεται μόνο μέχρι το επίπεδο του δρομολογητή, και όχι προς τα προηγούμενα δίκτυα.

viii. Σε κάθε δρομολογητή δημιουργείται αυτόματα και δεν φαίνεται στην πλατφόρμα, ακόμα μία διεπαφή η οποία συνδέει τον συγκεκριμένο εξυπηρετητή με το δίκτυο διαχείρισης (Management Network) του συστήματος για σκοπούς ελέγχου και ανατροφοδότησης.

5. Το κουμπί εισαγωγής Νέου Host ("Add Host")
   i. Οι Host αποτελούν τις τερματικές συσκευές του δικτύου.
   ii. Για τον κάθε host πρέπει να συμπληρωθούν το Όνομα και η Περιγραφή που θα εμφανίζονται στο ΠΔΕΠΜκΣ.
   iii. Να επιλεχθεί το "Πρότυπο" (Template) στο οποίο θα βασιστεί η συγκεκριμένη Εικονική Μηχανή. Τα "Πρότυπα" εμφανίζονται αυτόματα από το διασυνδεδεμένο περιβάλλον oVirt και είναι όσα πρότυπα στο περιβάλλον αρχίζουν από το πρόθεμα dias_[3].
   iv. Να επιλεχθεί η συστάδα ("Cluster"), στην οποία θα δημιουργηθεί ο host στο περιβάλλον oVirt. Και αυτή η ρύθμιση όπως και τα πρότυπα λαμβάνονται αυτόματα από το περιβάλλον oVirt.
   v. Να συμπληρωθούν τα στοιχεία του host, για σκοπούς διαχείρισης:
      1) Αρχιτεκτονική Συστήματος
      2) Λειτουργικό Σύστημα
      3) Ομάδα στην οποία συμμετέχει ο host. Η ομάδα είναι ένας ακέραιος αριθμός ο οποίος μπορεί να χρησιμοποιηθεί για την κατηγοριοποίηση των host.
      4) Ο ρόλος της οντότητας
         1. Blue
         2. Purple
         3. Red
         4. Viewer
         5. White

[3] Αυτό έγινε για να αποφευχθεί η εμφάνιση εντός του περιβάλλοντος προτύπων τα οποία δεν είναι παραμετροποιημένα για σωστή λειτουργία με την πλατφόρμα

5) Το δίκτυο στο οποίο θα διασυνδεθεί ο host.
6) Το όνομα του host.
7) Η στατική διεύθυνση IP σε περίπτωση που απαιτείται.
8) Για το αν η συγκεκριμένη εικονική μηχανή χρησιμοποιεί το Netplan για την ρύθμιση των δικτύων (Αφορά μόνο εικονικές μηχανές με λειτουργικό σύστημα Linux που χρησιμοποιούν τη συγκεκριμένη υπηρεσία για ρύθμιση των δικτυακών ρυθμίσεων)
9) Λοιπές ρυθμίσεις σε μορφή json με επεξεργασία του πεδίου "Configuration"

Με την ολοκλήρωση της συμπλήρωσης των πεδίων και αποθηκεύοντας το ΕΠΜ, ένα μήνυμα αποστέλλεται στην εφαρμογή Argos. Η εφαρμογή Argos είναι υπεύθυνη για την δημιουργία του ΕΠΜ στο περιβάλλον oVirt. Αν για κάποιο λόγο οι πόροι δεν επαρκούν ή η εφαρμογή Argos δεν είναι ενεργοποιημένη, τότε το ΕΠΜ αποθηκεύεται στη βάση σε κατάσταση "scheduled" και είτε θα δημιουργηθεί όταν θα υπάρχουν διαθέσιμοι πόροι είτε θα δημιουργηθεί όταν ξεκινήσει η εφαρμογή Argos.

## 6.2 Καταστροφή ΕΠΜ

Ως καταστροφή του Εικονικού Πεδίου Μάχης εννοούμε την διαγραφή όλης της υποδομής από το περιβάλλον oVirt, χωρίς καμία αλλαγή του ΕΠΜ στην πλατφόρμα Dias. Με αυτό τον τρόπο το ΕΠΜ μπορεί να ξαναδημιουργηθεί χωρίς την ανάγκη για επανακαταχώρηση του στην πλατφόρμα. Τα ΕΠΜ μπορούν να καταστραφούν μόνο από χρήστες της ομάδας:

- dias_admins

Προϋποθέσεις: Το ΕΠΜ θα πρέπει να έχει δημιουργηθεί ή να έχει αρχίσει η δημιουργία του.

- Από το κυρίως μενού πατήστε στην επιλογή "Battlefields".
- Από την λίστα με τα ΕΠΜ επιλέξτε αυτό που θέλετε να καταστρέψετε.
- Από την κάρτα διαχείρισης του ΕΠΜ στα δεξιά πατήστε το κουμπί Καταστροφή ("Destroy").

Η διαδικασία της καταστροφής του ΕΠΜ που ακολουθείτε περιλαμβάνει:

- Την απενεργοποίηση όλων των οντοτήτων που αποτελούν την συγκεκριμένη τοπολογία (host, δρομολογητές κλπ) στο περιβάλλον **oVirt**
- Την διαγραφή όλων των host από το περιβάλλον **oVirt**
- Την διαγραφή όλων των δρομολογητών από το περιβάλλον **oVirt**
- Τέλος τη διαγραφή όλων των δικτύων από το περιβάλλον **oVirt**

## 6.3 Διαγραφή ΕΠΜ

Τα Εικονικά Πεδία Μάχης μπορούν να διαγραφούν από την πλατφόρμα Dias μόνο από χρήστες της ομάδας:

- dias_admins

Προϋποθέσεις: Το ΕΠΜ θα πρέπει να έχει προηγουμένως καταστραφεί ή να μην έχει δημιουργηθεί.

Ενέργειες:

- Από το κυρίως μενού πατήστε στην επιλογή “Battlefields”.
- Από την λίστα με τα ΕΠΜ επιλέξτε αυτό που θέλετε να διαγράψετε.
- Από την κάρτα διαχείρισης του ΕΠΜ στα δεξιά πατήστε το κουμπί Διαγραφή (“Delete”).

# 7 Πρότυπα Επίθεσης

Τα Πρότυπα Επίθεσης είναι ανεξάρτητα από τα ΕΠΜ, αποτελούν όμως βασικό χαρακτηριστικό των Σεναρίων. Ο όρος Πρότυπο χρησιμοποιείται, γιατί κατά την δημιουργία τους, οι επιθέσεις αυτές δεν είναι ολοκληρωμένες λόγω της χρήσης μεταβλητών. Οι μεταβλητές αυτές αντικαθίστανται κατά τον ορισμό των Επιθέσεων στα Σενάρια αναλόγως των Στόχων. Με αυτό τον τρόπο αποφεύγονται αχρείαστες επαναλήψεις κώδικα, ανάγκη για περισσότερο αποθηκευτικό χώρο και μεγαλύτερη ευελιξία σε περίπτωση όπου απαιτούνται αλλαγές.

## 7.1 Δημιουργία Προτύπου Επίθεσης

Πρότυπα Επίθεσης μπορούν να δημιουργήσουν οι χρήστες που ανήκουν στις ομάδες:

- dias_admins
- dias_attackscript_admins

Το σύνολο των πεδίων με τον τύπο και τους περιορισμούς τους φαίνονται στην Ενότητα Α.3 του παρόντος Παραρτήματος.

Για να ανοίξετε την σελίδα καταχώρησης ενός νέου Προτύπου Επίθεσης

- Από το κυρίως μενού πατήστε στην επιλογή “Attack Scripts”
- Πατήστε στο κουμπί Προσθήκη Νέου (“Add New”) που βρίσκεται στο πάνω μέρος της σελίδας

Με την εμφάνιση της σελίδας καταχώρησης ενός νέου ΠΕ, διακρίνονται τα ακόλουθα στοιχεία:

1. Τα πεδία Τίτλος και Περιγραφή, που αφορούν το ΠΕ.
2. Το κουμπί επιλογής του εκτελεστή της επίθεσης με τις ακόλουθες επιλογές:
    i. Shell: Για την εκτέλεση θα χρησιμοποιηθεί το Shell (συνήθως πρόκειται για το Bash) της διανομής. Χρησιμοποιείται για επιθέσεις που τρέχουν σε UNIX.
    ii. CMD: Για την εκτέλεση θα χρησιμοποιηθεί το Command Prompt των Windows
    iii. Powershell: Για την εκτέλεση θα χρησιμοποιηθεί το Powershell των Windows

3. Το πεδίο εισαγωγής του κώδικα της επίθεσης (“Configuration”). Στο πεδίο αυτό τοποθετούνται όλες οι εντολές όπως θα αναγνωστούν από την εφαρμογή που θα εκτελέσει την επίθεση (εφαρμογή Sinon). Οτιδήποτε εσωκλείεται μεταξύ των χαρακτήρων [{ και }], θεωρείτε μεταβλητή και μετά από την απομάκρυνση του mouse από το συγκεκριμένο πεδίο θα δημιουργηθεί γι’ αυτό μια νέα μεταβλητή. Οι μεταβλητές αυτές θα πρέπει να οριστούν κατά τη διάρκεια του σεναρίου.
4. Τα πεδία Κατηγορία, Στόχος, Πλατφόρμα και Αρχιτεκτονική της Πλατφόρμας τα οποία χρησιμοποιούνται για την καλύτερη διαχείριση των Προτύπων.

Ο κώδικας της επίθεσης αποθηκεύεται στην βάση δεδομένων αφού πρώτα κωδικοποιηθεί σε base64. Η μετατροπή αυτή γίνεται για να αποφευχθούν τυχόν ασυμβατότητες μεταξύ της κωδικοποίησης των διαφορετικών λειτουργικών συστημάτων και αποφυγή εντοπισμού από τυχόν εφαρμογές εντοπισμού κακόβουλου λογισμικού. Με αυτό τον τρόπο διασφαλίζεται η σωστή μεταφορά και εκτέλεση του κώδικα από το αυτοματοποιημένο σύστημα εκτέλεσης επιθέσεων.

## 7.2 Διαγραφή Προτύπου Επίθεσης

Τα Πρότυπα Επίθεσης μπορούν να διαγραφούν από την πλατφόρμα Dias μόνο από χρήστες της ομάδας:

- dias_admins

Ενέργειες:

- Από το κυρίως μενού πατήστε στην επιλογή “Attack Scripts”.
- Από την λίστα με τα Πρότυπα Επίθεσης επιλέξτε αυτό που θέλετε να διαγράψετε.
- Στο πάνω αριστερά μέρος της σελίδας πατήστε το κουμπί Διαγραφή (“Delete”).

# 8 Εικονικά Σενάρια

Τα Εικονικά Σενάρια αποτελούν την ουσία της παρούσας διατριβής και δημιουργούνται για να δοκιμαστούν οι διάφορες καταστάσεις που μπορούν να προκύψουν στο κάθε περιβάλλον. Σε κάθε ΕΠΜ μπορούν να δημιουργηθούν ένα ή περισσότερα Σενάρια με τον περιορισμό ότι μόνο ένα μπορεί να είναι ενεργό για το κάθε ΕΠΜ ανά πάσα στιγμή. Τα Σενάρια χρησιμοποιούνται για την εξοικονόμηση πόρων και χρόνου με την επαναχρησιμοποίηση των ίδιων μηχανημάτων και την επαναφορά τους κάθε φορά στην αρχική κατάσταση του συγκεκριμένου σεναρίου με την χρήση της δυνατότητας Snapshot του περιβάλλοντος oVirt. Μέσα από τα Σενάρια μπορούν να επιλεγούν και να παραμετροποιηθούν οι επιθέσεις που θα εκτελέσει ο κάθε host καθώς και να καθοριστούν δικαιώματα πρόσβασης σε χρήστες έτσι ώστε να μπορούν να χειριστούν τα εικονικά μηχανήματα για τους σκοπούς του Σεναρίου.

## 8.1 Δημιουργία Εικονικού Σεναρίου

Εικονικά Σενάρια μπορούν να δημιουργήσουν οι χρήστες που ανήκουν στις ομάδες:

- dias_admins
- dias_scenario_admins

Το σύνολο των πεδίων με τον τύπο και τους περιορισμούς τους φαίνονται στην Ενότητα Α.4 του παρόντος Παραρτήματος

- Για να ανοίξετε την σελίδα καταχώρησης ενός νέου Σεναρίου
- Από το κυρίως μενού πατήστε στην επιλογή “Scenarios”

Πατήστε στο κουμπί Προσθήκη Νέου (“Add New”) που βρίσκεται στο πάνω μέρος της σελίδας

Με την εμφάνιση της σελίδας καταχώρησης ενός νέου Σεναρίου, διακρίνονται τα ακόλουθα στοιχεία:

1. Τα πεδία Τίτλος και Περιγραφή, Γνωστικός Τομέας και Επίπεδο τα οποία χρησιμοποιούνται για την καλύτερη διαχείριση των Σεναρίων.
2. Το πεδίο Ενεργοποίησης/Απενεργοποίησης της Διαβάθμισης των πληροφοριών που αφορούν το συγκεκριμένο Σενάριο. Με την Ενεργοποίηση της επιλογής “Is Black Box”, οι συμμετέχοντες χρήστες δεν θα μπορούν να δουν τις υπόλοιπες

οντότητες που συμμετέχουν στο Σενάριο παρά μόνο τα πεδία Τίτλος, Περιγραφή, Γνωστικός Τομέας, Επίπεδο. Στην αντίθετη περίπτωση, όλα τα στοιχεία του Σεναρίου θα είναι ορατά στους συμμετέχοντες.

3. Το πεδίο Διάρκεια, από το οποίο μπορεί να καθοριστεί ο χρόνος για τον οποίο θα είναι ενεργό το Σενάριο. Η προεπιλεγμένη τιμή είναι οι 2 ώρες, και ο μέγιστος χρόνος που μπορεί να είναι ένα Σενάριο ενεργό είναι οι 30 μέρες 23 ώρες και 59 δευτερόλεπτα.
4. Το πεδίο επιλογής του Εικονικού Πεδίου Μάχης στο οποίο βασίζεται το συγκεκριμένο Σενάριο. Η συγκεκριμένη επιλογή είναι ιδιαίτερα κρίσιμη αφού βάση αυτής θα εμφανίζονται τα διαθέσιμα εικονικά μηχανήματα στα οποία θα μπορούν να οριστούν Αυτοματοποιημένες Επιθέσεις και Δικαιώματα Πρόσβασης για τους Χρήστες.
5. Το κουμπί προσθήκης νέας Επίθεσης (“Add Attack”). Για κάθε νέα Επίθεση πρέπει:
    i. Να επιλεχθεί ο host που θα την εκτελέσει.
    ii. Να επιλεχθεί το Πρότυπο Επίθεσης στο οποίο θα βασιστεί.
    iii. Να συμπληρωθούν τυχόν μεταβλητές που χρησιμοποιούνται στο συγκεκριμένο Πρότυπο
    iv. Να επιλεχθεί ο χρόνος της εκτέλεσης μεταξύ των επιλογών:
        1) Σε σειρά, δηλαδή μόλις αυτή είναι διαθέσιμη από την Εφαρμογή Αυτόματης Εκτέλεσης Επιθέσεων της Οντότητας
        2) Τυχαία εντός του καθορισμένου χρονικού πλαισίου (σε λεπτά) – δεν έχει υλοποιηθεί στον κώδικα της εφαρμογής Sinon
        3) Ακριβώς με την έλευση του καθορισμένου χρόνου (σε λεπτά) – δεν έχει υλοποιηθεί στον κώδικα της εφαρμογής Sinon
6. Το κουμπί προσθήκης νέου Χρήστη (“Add User”). Για κάθε χρήστη πρέπει:
    i. Να επιλεχθεί ο Host στον οποίο θα έχει πρόσβαση
    ii. Να συμπληρωθεί το Όνομα χρήστη (πρέπει να αντιστοιχεί σε χρήστη ο οποίος θα είναι καταχωρημένος στον FreeIPA και να ανήκει στην ομάδα dias_players)
    iii. Να επιλεχθεί κατά πόσο ο κωδικός θα δημιουργηθεί αυτόματα ή θα προκαθοριστεί.

## 8.2 Προετοιμασία/Εκκίνηση/Τερματισμός Εικονικού Σεναρίου

Την κατάσταση των Εικονικών Σεναρίων μπορούν να την διαχειριστούν χρήστες που ανήκουν στις ομάδες:

- dias_admins
- dias_scenario_admins
- dias_scenario_managers

Ενέργειες:

- Από το κυρίως μενού πατήστε στην επιλογή “Scenarios”

Και οι τρείς επιλογές γίνονται από τα κουμπιά που βρίσκονται στα δεξιά του κάθε σεναρίου υπάρχουν ωστόσο οι ακόλουθοι περιορισμοί:

Για την Προετοιμασία ενός Εικονικού Σεναρίου απαιτείται:

- το ΕΠΜ στο οποίο βασίζεται να έχει δημιουργηθεί στο περιβάλλον oVirt (δηλαδή κατάσταση του να είναι READY ή να έχει ολοκληρωθεί η χρήση του από κάποιο άλλο Σενάριο (κατάσταση INACTIVE).

<u>Για την Εκκίνηση ενός Σεναρίου απαιτείται:</u>

- το ΕΠΜ στο οποίο βασίζεται να έχει προηγουμένως Προετοιμαστεί, χρησιμοποιώντας το αντίστοιχο κουμπί. Με την ολοκλήρωση της προετοιμασίας η κατάσταση του ΕΠΜ θα είναι “ACTIVE” και του Σεναρίου “READY”

<u>Τερματισμός Σεναρίου:</u>

Ο τερματισμός ενός Σεναρίου μπορεί να γίνει μόνο εφόσον αυτό βρίσκεται σε ενεργή κατάσταση ή αυτόματα εφόσον ολοκληρωθεί η χρονική διάρκεια η οποία καθορίστηκε κατά τη δημιουργία του.

# Δ.2 Πεδία Εικονικού Πεδίου Μάχης

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| Battlefield | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Title | ✓ | Αλφαριθμητικό | 20 χαρακτήρες | |
| | Description | | Αλφαριθμητικό | 255 χαρακτήρες | |
| Network | Name | ✓ | Αλφαριθμητικό | 12 χαρακτήρες | |
| | Description | | Αλφαριθμητικό | 50 χαρακτήρες | |
| Router | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Name | ✓ | Αλφαριθμητικό | 12 χαρακτήρες | |
| | Configuration | | JSON | Έγκυρο αρχείο JSON | |
| Interface | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Name | ✓ | Αλφαριθμητικό | 12 χαρακτήρες | |
| | Role | ✓ | Επιλογής | Green<br>Blue<br>Orange<br>Red | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός |
| | Network | ✓ | Επιλογής | Πρέπει να είναι ένα από τα δίκτυα που έχουν δηλωθεί στο συγκεκριμένο Πεδίο Μάχης | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID του συγκεκριμένου Δικτύου |
| | Static IP | | Boolean | True/False | |
| | IP | | IP | Έγκυρη διεύθυνση IP | |

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| | Netmask | | IP | | |
| | Dns 1 | | IP | | |
| | DHCP Server | | Boolean | True/False | |
| | DHCP Start IP | | IP | Έγκυρη διεύθυνση IP | |
| | DHCP End IP | | IP | | |
| Host | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Name | ✓ | Αλφαριθμητικό | 20 χαρακτήρες | |
| | Description | | Αλφαριθμητικό | 255 χαρακτήρες | |
| | Virtual Machine Template | ✓ | Αλφαριθμητικό | 255 χαρακτήρες | Οι πληροφορίες αυτές προέρχονται από το περιβάλλον oVirt και ανανεώνονται κατά τη διάρκεια του φορτώματος της σελίδας |
| | Cluster | ✓ | Αλφαριθμητικό | 100 χαρακτήρες | |
| | Architecture | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_architecture της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης αρχιτεκτονικής. |
| | Platform | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_platform της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης πλατφόρμας. |
| | Team | ✓ | Ακέραιος Αριθμός | | Χρησιμοποιείται για τον διαχωρισμό των οντοτήτων |
| | Role | ✓ | Επιλογής | Blue<br>Purple<br>Red<br>Viewer | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός |

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| | | | | White | |
| | Network | | Επιλογής | Πρέπει να είναι ένα από τα δίκτυα που έχουν δηλωθεί στο συγκεκριμένο Πεδίο Μάχης | Οι τιμές αυτές, αποθηκεύονται σαν πληροφορίες JSON στο πεδίο configuration |
| | Hostname | | | | |
| | IP | | | | |
| | Netmask | | | | |
| | Use Static IP | | | | |
| | Use Netplan | | | Εφαρμόζεται σε όσες εικονικές μηχανές το λειτουργικό χρησιμοποιεί το Netplan για τη ρύθμιση των δικτύων. | |
| | Configuration | ✓ | JSON | Έγκυρο αρχείο JSON | Ανανεώνεται αυτόματα κάθε φορά που χάνετε η εστίαση από κάποιο από τα προηγούμενα πεδία |

# Δ.3 Πεδία Προτύπου Επίθεσης

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| Attack Script | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Title | ✓ | Αλφαριθμητικό | 20 χαρακτήρες | |
| | Description | | Αλφαριθμητικό | 255 χαρακτήρες | |
| | Module | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_module της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης Focus Area. |
| | Configuration | ✓ | JSON | Έγκυρο αρχείο JSON | Ανανεώνεται αυτόματα κάθε φορά που το πεδίο χάνει την εστίαση του |
| | Category | | Επιλογής | Οι τιμές του πίνακα battlefield_category της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης κατηγορίας. |
| | Target | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_attacktarget της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID του συγκεκριμένου στόχου. |
| | Platform | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_platform της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης πλατφόρμας της εικονικής μηχανής από την οποία εκτελείτε η επίθεση. |
| | Architecture | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_architecture της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης αρχιτεκτονικής της |

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| | | | | | εικονικής μηχανής από την οποία εκτελείτε η επίθεση. |
| Variables | Name | ✓ | Αλφαριθμητικό | | Οι τιμές αυτές, αποθηκεύονται στον πίνακα battlefield_attackvariable της Β.Δ |
| | Type | | Επιλογής | Οι τιμές του πίνακα battlefield_vartype της ΒΔ | |

# Δ.4 Πεδία Εικονικού Σεναρίου

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| Scenario | UUID | ✓ | UUID | Δημιουργείται Αυτόματα | |
| | Title | ✓ | Αλφαριθμητικό | 20 χαρακτήρες | |
| | Description | | Αλφαριθμητικό | | |
| | Focus Area | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_focusarea της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID της συγκεκριμένης Focus Area. |
| | Level | ✓ | Επιλογής | Οι τιμές του πίνακα battlefield_level της ΒΔ | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός και αντιστοιχεί στο ID του συγκεκριμένου επιπέδου. |
| | Is Black Box | | Boolean | True/False | |
| | Days | ✓ | Ακέραιος Αριθμός | 0-30 | Σε περίπτωση που τοποθετηθεί η τιμή 0 σε όλα τότε ως χρονικός περιορισμός ορίζεται ο μέγιστος (30ημ 23ω 59λ) |
| | Hours | ✓ | Ακέραιος Αριθμός | 0-23 | |
| | Minutes | ✓ | Ακέραιος Αριθμός | 0-59 | |
| | Battlefield | ✓ | Επιλογής | Πρέπει να είναι ένα από τα υπάρχοντα Εικονικά Πεδία Μάχης | Με την επιλογή του Πεδίου Μάχης ενεργοποιούνται τα πεδία επιλογής οντοτήτων στις κάρτες των Επιθέσεων και των Χρηστών που ακολουθούν |
| Attack | Host | ✓ | Επιλογής | Πρέπει να είναι μία από τις Εικονικές Μηχανές του Πεδίου Μάχης που επιλέχθηκε προηγουμένως | |

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| | Attacksript | ✓ | Επιλογής | Πρέπει να είναι ένα από τα υπάρχοντα Πρότυπα Επιθέσεων | Με την επιλογή του Προτύπου Επίθεσης αυτόματα εμφανίζονται όσα πεδία όσες και οι μεταβλητές που περιλαμβάνει το συγκεκριμένο Πρότυπο |
| | Role | ✓ | Επιλογής | Green<br>Blue<br>Orange<br>Red | Η τιμή αποθηκεύεται στη ΒΔ ως ακέραιος αριθμός |
| | Execution Style | ✓ | Επιλογής | In Series<br>Random Before<br>Random After<br>Exactly | Ο χρόνος που θα εκτελεστεί η επίθεση.<br>In Series: Μόλις ληφθεί από την εφαρμογή αυτόματης εκτέλεσης<br>Random Before: Τυχαία πριν από τα καθορισμένα λεπτά<br>Random After: Τυχαία μετά από τα καθορισμένα λεπτά<br>Exactly: Ακριβώς όσα τα καθορισμένα λεπτά από την έναρξη του σεναρίου |
| | Execution Time | | Ακέραιος Αριθμός | 0-1400 | Ο χρόνος της εκτέλεσης της επίθεσης σε λεπτά |
| | Configuration | ✓ | JSON | Έγκυρο αρχείο JSON | Ανανεώνεται αυτόματα κάθε φορά που χάνετε η εστίαση από κάποιο από τα πεδία των μεταβλητών του Προτύπου Επιθέσεων ή του χρόνου εκτέλεσης της επίθεσης |
| User | Host | ✓ | Επιλογής | Πρέπει να είναι μία από τις Εικονικές Μηχανές του Πεδίου Μάχης που επιλέχθηκε προηγουμένως | |
| | User | ✓ | Αλφαριθμητικό | 80 χαρακτήρες | Εδώ δεν υπάρχει κάποιος έλεγχος αλλά αν |

| Οντότητα | ΠΕΔΙΟ | ΥΠΟΧΡ. | ΤΥΠΟΣ | ΠΕΡΙΟΡΙΣΜΟΙ | ΠΑΡΑΤΗΡΗΣΕΙΣ |
|---|---|---|---|---|---|
| | | | | | ο χρήστης δεν είναι έγκυρος χρήστης του διακομιστή FreeIPA τότε δεν θα μπορεί να συνδεθεί στην πλατφόρμα |
| | Is Root | | Boolean | True/False | |
| | Password | | Αλφαριθμητικό | 20 χαρακτήρες | Στην περίπτωση που δεν καθοριστεί κάποιος κωδικός τότε δημιουργείται αυτόματα ένας κωδικός 8 δεκαεξαδικών χαρακτήρων |