ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αυτοματοποιημένη Δημιουργία Σεναρίων σε Θέματα Κυβερνοασφάλειας

Δημήτριος Γ. Ζάμπος

Επιβλέπων: **Νικόλαος Κολοκοτρώνης,** Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2020

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αυτοματοποιημένη Δημιουργία Σεναρίων σε Θέματα Κυβερνοασφάλειας

Δημήτριος Γ. Ζάμπος
Α.Μ.: ΜΟΠ 496

ΕΠΙΒΛΕΠΩΝ: **Νικόλαος Κολοκοτρώνης,** Αναπληρωτής Καθηγητής

ΟΚΤΩΒΡΙΟΣ 2020

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία στόχο έχει την παρατήρηση των τεχνολογιών για την προστασία στον κυβερνοχώρο και πως με τα κατάλληλα εργαλεία μπορεί κανείς να υλοποιήσει ένα περιβάλλον δοκιμών και για τη διαρκή εκπαίδευση των ενδιαφερομένων. Η ροπή των τελευταίων ετών στην πληροφορική δείχνει το δρόμο στην αυτοματοποίηση διαδικασιών και λειτουργιών για την αντιμετώπιση του ανθρώπινου λάθους και την επιτάχυνση της επίτευξης επιθυμητού αποτελέσματος.

Η προσέγγιση που ακολουθήθηκε στην εργασία, εφάπτεται στην ανάγκη της αποτροπής των κινδύνων που αντιμετωπίζουν καθημερινά όλοι οι εκτιθέμενοι στο διαδίκτυο και τις απειλές που περικλείονται.

Τα βασικά δομικά στοιχεία της εργασίας αποτελούνται από τα διάφορα εργαλεία προσομοίωσης και αυτοματισμού, τα οποία και θα δούμε συγκριτικά, θα αιτιολογήσουμε τις επιλογές μας, για την υλοποίηση του εργαστηρίου καθώς την υποδομή που χρησιμοποιήθηκε.

Να τονίσουμε ότι για το εργαστηριακό μέρος της άσκησης χρειάστηκε, ένα μόνο φυσικό hardware, ενώ όλη η υλοποίηση έχει γίνει σε εικονικό περιβάλλον, με τη χρήση εικονικών μηχανών και την κατανομή των πόρων ανάλογα με τις ανάγκες του καθενός.

Τέλος γίνεται μια συνοπτική περιγραφή στο πως αυτά μπορούν να ενσωματωθούν σε μία ενιαία εκπαιδευτική πλατφόρμα και να αποτελέσουν τη βάση για τη δημιουργία μιας σειράς εργαστηριακών ασκήσεων.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Προσομοίωση, Αυτοματοποιημένες διαδικασίες

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: προσομοίωση, εξομοίωση, κυβερνοασφάλεια, εργαστήριο, πλατφόρμα εκπαίδευσης, αυτοματισμοί, gns3, Ansible, Vmware

ABSTRACT

The purpose of this paper is to observe the technologies for cyber protection and how with the appropriate tools one can implement a test environment for the continuous education of those interested. The momentum of recent years in computer science, shows the way in the automation of processes and functions to deal with human error and accelerate the achievement of the desired result.

The approach followed, touches on the need to prevent from the dangers faced daily by all those exposed to the internet and the threats that are contained.

The basic structural elements of the paper consist of the various simulation and automation tools, which we will see comparatively, and we will justify our choices, for the implementation of the laboratory as well as the infrastructure used.

We have to emphasize the fact that for the laboratory part of the exercise, only one physical hardware was needed, while all the implementation has been done in a virtual environment, with the use of virtual machines and the distribution of resources according to the needs.

Finally, a brief description is given of how these can be integrated into a single educational platform and form the basis for the creation of a series of laboratory exercises.

SUBJECT AREA: Simulation, Automated Procedures

KEYWORDS: simulation, emulation, cyber security, security, lab environment, training platforms, educational platforms, automation, gns3, Ansible, Vmware

ΕΥΧΑΡΙΣΤΙΕΣ

Τίποτα δυστυχώς δεν έρχεται χωρίς κόπο και προσωπική προσπάθεια. Κάθε μέρα, είναι μια ξεχωριστή δοκιμασία με ξεχωριστή έκβαση. Όσο χρόνο και να χρειάζεται κάτι για να παράξει αποτέλεσμα είναι μια μοναδική εμπειρία. Με τον ίδιο ακριβώς τρόπο θα χαρακτηρίσω το αποτέλεσμα αυτής της δουλειάς.

Οι ευχαριστίες μου θα ξεκινήσουν φυσικά από τον κ. Κολοκοτρώνη, Αν. Καθηγητή, για την εμπιστοσύνη και την καθοδήγηση στην ολοκλήρωση της εργασίας.

Ακολούθως, με την ευκαιρία αυτή θα ευχαριστήσω τους γονείς μου που με έμαθαν να μην τα παρατάω, να παλεύω γι αυτό που θέλω και αποτελούν καθημερινά οδηγό για τη ζωή μου.

Καθώς επίσης και τη σύζυγό μου που με στηρίζει συνεχώς και με υπομονή τα τελευταία 8 χρόνια, στις επιλογές και τις αναζητήσεις μου.

Τέλος να ευχαριστήσω τους φίλους και συναδέλφους που με συνόδεψαν σε αυτήν την προσπάθεια και ξοδέψαμε παραγωγικό χρόνο αλληλεπιδρώντας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά την περίοδο 2019 - 2020, στα πλαίσια του διατμηματικού προγράμματος μεταπτυχιακών σπουδών " Διοίκηση και οικονομική των τηλεπικοινωνιακών δικτύων". Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Κολοκοτρώνη Νικόλαου, καθηγητή του Ε.Κ.Π.Α, τμήμα Πληροφορικής και Τηλεπικοινωνιών.

Αντικείμενο της εργασίας αποτελεί η διερεύνηση εργαλείων για την προσομοίωση δικτυακών τοπολογιών και την εφαρμογή τους σε εκπαιδευτικά σενάρια στον τομέα της κυβερνοασφάλειας, παράλληλα με την προσάρτηση αυτοματοποιημένων διαδικασιών για την υλοποίηση και την εκπόνηση εργαστηριακών ασκήσεων.

Μαζί με την έρευνα και την καταγραφή των λύσεων, η εργασία συμπεριλαμβάνει και την υλοποίηση του αντικείμενου ενδιαφέροντος, ως απόδειξη και δοκιμή των προαναφερθέντων.

1. ΕΙΣΑΓΩΓΗ

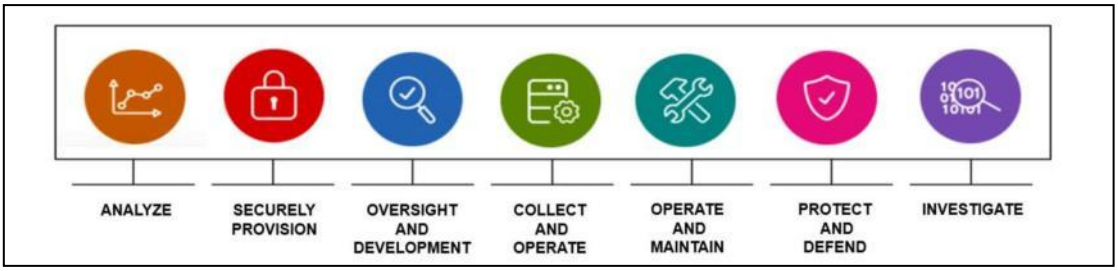
Η κεντρική ιδέα της εργασίας είναι η δημιουργία μιας τοπολογίας η οποία θα μπορεί να χρησιμοποιηθεί για την προσομοίωση μίας άσκησης κυβερνοασφάλειας. Τέτοιες δομές συναντούνται σε εκπαιδευτικές πλατφόρμες ιδρυμάτων και οργανισμών, όπου ο χρήστης δέχεται αλληλεπιδράσεις από το σύστημα αλλά και από άλλους χρήστες.

Λέξεις κλειδιά: Διαδικτυακή πλατφόρμα, στόχοι, ADDIE, ISD, κυβερνοασφάλεια, cybersecurity, LMS, LXP, GN3, VMware

2. NICE CYBERSECURITY WORKFORCE FRAMEWORK

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), εθνική πρωτοβουλία για την εκπαίδευση στον κυβερνοχώρο, το πλαίσιο εργατικού δυναμικού στον κυβερνοχώρο (γνωστό ως NICE πλαίσιο), λειτουργεί ως σημείο αναφοράς για την περιγραφή και την ανταλλαγή πληροφοριών σχετικά με την έρευνα στον τομέα της κυβερνοασφάλειας. Αυτό το πλαίσιο τυποποιεί τις γνώσεις, τις δεξιότητες και τις ικανότητες που απαιτούνται για την εφαρμογή των καθηκόντων και την εργασίας από ανθρώπους σε συγκεκριμένους ρόλους. Αποτελείται από τρία δομικά στοιχεία: Κατηγορίες, Περιοχές Ειδικών και Ρόλοι εργασίας (STUDIES). Ο επίσημος αριθμός εγγράφου είναι: NIST Special Publication 800-181. [1]

Η NICE, με επικεφαλής το NIST, είναι μια συνεργασία μεταξύ κυβέρνησης, ακαδημαϊκών κύκλων και του ιδιωτικού τομέα που εργάζονται για την προώθηση της εκπαίδευσης στον τομέα της ασφάλειας στον κυβερνοχώρο, της κατάρτισης και της ανάπτυξης του προσωπικού.[2] Το NICE Framework κατηγοριοποιείται χρησιμοποιώντας μία top-down προσέγγιση όπου κάθε μία από τις επτά κατηγορίες αποτελείται από περιοχές ειδικότητας (33 συνολικά) οι οποίες στη συνέχεια αναλύονται σε ρόλους εργασίας (σύνολο 52). Οι επτά κατηγορίες αντιπροσωπεύουν κοινές λειτουργίες όσων εργάζονται στον τομέα της κυβερνοασφάλειας. **Εικόνα 1**



Εικόνα 1: Nice Cybersecurity Workforce Framework

2.1 Εκπαίδευση

Η κατάρτιση είναι απαραίτητη για την προετοιμασία του εργατικού δυναμικού στον κυβερνοχώρο του αύριο και για την ενημέρωση των σημερινών εργαζομένων στον τομέα της ασφάλειας στον κυβερνοχώρο σχετικά με τις δεξιότητες και τις εξελισσόμενες απειλές. [3]

Ένα πλάνο αντίδρασης που δεν έχει δοκιμαστεί, δεν έχει πρακτικά καμία αξία αφού η εφαρμογή του κατά τη διάρκεια ενός πραγματικού συμβάντος δεν αποτελεί best practice. Πολλοί οργανισμοί συνήθως παραβλέπουν τη σημασία της πρόβλεψης της διαδικασίας λήψης τεχνικών αποφάσεων, της διαδικασίας και της λήψης επιχειρηματικών αποφάσεων που αποτελούν κρίσιμη συνιστώσα της προετοιμασίας για να ανταποκριθούν κυβερνοεπιθέσεις.

Όλο το προσωπικό ενός οργανισμού πρέπει να είναι ενημερωμένο και να έχει συνειδητοποιήσει την ιδιαιτερότητα της ασφάλειας στον κυβερνοχώρο και του τρόπου με τον οποίο επηρεάζει το ρόλο και τα καθήκοντά του. Δεν πρέπει να είναι απλώς ένα ζήτημα για τους ειδικούς στον τομέα της ασφάλειας στον κυβερνοχώρο, αλλά αντ ' αυτού να αποτελεί μέρος της συνολικής "υγείας" του οργανισμού. Όλοι οι χρήστες ενός εταιρικού δικτύου αποτελούν βασικό κίνδυνο – αλλά παράλληλα και ένα πρώτο

επίπεδο ελέγχου για την πρόληψη επιθέσεων στον κυβερνοχώρο. Ωστόσο, αυτό το "ανθρώπινο τείχος προστασίας" θα είναι αποτελεσματικό μόνο εάν οι χρήστες έχουν επίγνωση των ευθυνών τους για την ασφάλεια στον κυβερνοχώρο, δεδομένων των εργαλείων που διατίθενται για ασφαλή λειτουργία (π. χ . εγκατεστημένο anti-malware), και κίνητρα να ενεργούν κατάλληλα, συμπεριλαμβανομένης της προθυμίας να αναφέρουν κινδύνους ή/και επιθέσεις, άμεσα και αποτελεσματικά. Ένας οργανισμός πρέπει να διασφαλίζει ότι είναι ευκολότερο για το προσωπικό να ακολουθεί τις σωστές πρακτικές και να αποφεύγει λανθασμένες. Το κίνητρο περιλαμβάνει επίσης τη διασφάλιση ότι αναγνωρίζονται αυτές οι σωστές συμπεριφορές και φυσικά η παροχή θετικής ανάδρασης από τον χρήστη. Είναι απαραίτητη για παράδειγμα η άμεση απόκριση από το IT/SOC της εταιρείας μετά την αναφορά ενός μηνύματος ηλεκτρονικού "ψαρέματος", ώστε να οδηγήσει το θύμα να αναφέρει μελλοντικά περιστατικά.

Η δημιουργία εταιρικής κουλτούρας βασίζεται επίσης στο παράδειγμα που δίνουν τα στελέχη της εταιρεία. Για παράδειγμα ακόμα και για οι διευθυντές δεν πρέπει να αποτελούν εξαίρεση και να αποκλείονται από τους ελέγχους που εφαρμόζονται σε όλο το υπόλοιπο προσωπικό, όπως το να επιτρέπεται να χρησιμοποιούν τις δικές τους μη ασφαλείς συσκευές πληροφορικής.

2.2 Απειλές

Η διοίκηση του οργανισμού καλείται να διασφαλίσει ότι υπάρχουν αποτελεσματικές και αποδοτικές διαδικασίες για την κατανόηση των απειλών στον κυβερνοχώρο που αντιμετωπίζει, με βάση τα παρακάτω [4]:

- Ο τύπος της λειτουργίας και τυχόν επικείμενες αλλαγές.
- Η έκταση της ψηφιακής δραστηριότητας.
- Γεωγραφική περιοχή δραστηριοποίησης (π.χ εντός Ελλάδος, διεθνή).
- Ιστορικό συμβάντων στον κυβερνοχώρο;
- Ευαισθητοποίηση σε θέματα γενικών και ειδικών απειλών και γνωστά τρωτά σημεία.
- Τρωτά σημεία λόγω τεχνολογιών που χρησιμοποιούνται (π.χ. χρήση ξεπερασμένης τεχνολογίας (λειτουργικά συστήματα, βάσεις, ERP εφαρμογές με πρόσβαση στο διαδίκτυο) που μπορεί να επιφέρουν αδυναμίες στην ασφαλή λειτουργία.

Υπάρχουν αρκετοί διαθέσιμοι πάροχοι υπηρεσιών που παρέχουν τακτικές ενημερώσεις σχετικά με το συγκεκριμένο αναδυόμενο τοπίο απειλών. Όπου υπάρχει ασφάλεια στον κυβερνοχώρο, ο πάροχος μπορεί επίσης να παρέχει αναφορά πληροφοριών στον κυβερνοχώρο. Η διοίκηση θα πρέπει να λαμβάνει τακτικές εκθέσεις που συνοψίζουν τις παρεχόμενες πληροφορίες και να ενημερώνεται για την αποτελεσματικότητα, το κόστος και την αποδοτικότητα των παρεχόμενων υπηρεσιών.

3. ΒΑΣΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ

Ο κίνδυνος κυβερνοεπιθέσεων διαφέρει από τους παραδοσιακούς IT κινδύνους και παρουσιάζει ένα μοναδικό σύνολο προκλήσεων [5],[6]:

• Τα περιστατικά είναι υψηλής ταχύτητας, αδόμητα και ποικίλα - η διαχείριση των κρίσεων σε αυτές τις περιπτώσεις είναι έντονη και απαιτητική.

• Σε αντίθεση με τα κλασσικά περιστατικά που θα συμβούν μία φορά, οι επιτιθέμενοι στήνουν επίμονες και δυναμικές παραβιάσεις, με συνεχώς αυξανόμενη πολυπλοκότητα.

• Ο αντίκτυπος από άποψη κόστους και δυσφήμησης μπορεί να είναι πολύ σοβαρός

• Κάθε οργανισμός διαθέτει πληθώρα ευάλωτων σημείων που θα μπορούσαν να αποτελέσουν κερκόπορτα , συμπεριλαμβανομένων τρίτων συνεργατών αλλά φυσικά και του προσωπικού του.

• Η παραδοσιακή διαχείριση της επιχειρησιακής συνέχειας (BCM) επικεντρώνεται συνήθως στη διαθεσιμότητα συστημάτων και δεδομένων - αυτό μπορεί να είναι αναποτελεσματικό, για παράδειγμα όταν τα ζητήματα ακεραιότητας των δεδομένων αντιγράφονται αυτόματα σε DR συστήματα αποκατάστασης καταστροφής.

• Η διατήρηση των σύγχρονων και πολύπλευρων δυνατοτήτων σε ανθρώπους, διαδικασίες και up-to-date τεχνολογία καθώς και σε ομάδες τεχνικής διαχείρισης, διαχείρισης έργων και εκτελεστικών διοικητικών στελεχών μπορεί να είναι δύσκολη και να συμβαδίζει με τις προτεραιότητες του οργανισμού στον τομέα ενασχόλησης του.

• Η απόκτηση executive-buy-in και η συμμετοχή σε προγραμματισμό και ασκήσεις αντιμετώπισης περιστατικών μπορεί να είναι δύσκολη αν οι κίνδυνοι δεν είναι καλά κατανοητοί.

• Η έλλειψη δεξιοτήτων και η εσωτερική ικανότητα αντιμετώπισης ενός αυξανόμενου αριθμού σύνθετων επιθέσεων μπορεί να αφήσει έναν οργανισμό εκτεθειμένο σε οποιαδήποτε μορφή κυβερνοεπίθεσης.

• Οι οργανισμοί συχνά μαθαίνουν για την παραβίαση ασφαλείας από εξωτερικές πηγές, όπως από την αστυνομία, από το ρυθμιστή ή και από πελάτη, και στη συνέχεια προσπαθούν να ελέγξουν το συμβάν. (ακόμα και σε πολύ μεγάλες εταιρείες)

• Διαχείριση των μέσων μαζικής ενημέρωσης όταν τα νέα, σχετικά με την παραβίαση ασφάλειας, έχουν ήδη μεταδοθεί και συζητούνται από τους πελάτες σε κοινωνικά μέσα ενημέρωσης και άλλα κανάλια εκτός ελέγχου.

• Εξασφάλιση στους πελάτες, τους ρυθμιστές, τους επενδυτές και άλλα ενδιαφερόμενα μέρη ότι η παραβίαση είναι υπό έλεγχο.

• Συνεργασία με τους ρυθμιστικούς φορείς για την επίδειξη προληπτικής ικανότητας διαχείρισης περιστατικών (π.χ. ελαχιστοποίηση των οικονομικών επιπτώσεων και εξασφάλιση της προστασίας των πληροφοριών των πελατών)

Εταιρείες όπως η EY (https://www.ey.com) παρέχουν το πεδίο για εξομοίωση σεναρίων που περιλαμβάνουν:

Περιγραφή άσκησης - Αυτή η άσκηση διαρκεί συνήθως μισή μέρα και επικεντρώνεται στην πρόκληση του συντονιστή και της ομάδας του καθώς εκτελούν το σχέδιο αντίδρασης. Οι συμμετέχοντες εκτελούν όλες ή τις περισσότερες από τις διαδικασίες που περιγράφονται στο σχέδιο. (Οι συμμετέχοντες μπορούν να συζητήσουν τις ενέργειες που θα αναλάβουν χωρίς απαραίτητα να τις υλοποιήσουν.) Η άσκηση προσαρμόζεται στην οργάνωση και τα σχέδια διαχείρισης περιστατικών και συνήθως

περιλαμβάνει την παροχή στους συμμετέχοντες μιας σειράς προσαρμοσμένων επιθέσεων που προκαλούν την ικανότητά τους να ανταποκριθούν..

• Επιλογές - Η άσκηση μπορεί να προσαρμοστεί ώστε να περιλαμβάνει την εξέταση τεχνικών στοιχείων και σε επίπεδο PC. Μπορούν επίσης να προστεθούν στοιχεία τυποποίησης.

• Πρωταρχικοί στόχοι - Έλεγχος της ικανότητας της ομάδας συντονισμού των συμβάντων να διαχειριστεί το περιστατικό μέχρι την ολοκλήρωσή του, συμπεριλαμβανομένης της αλληλεπίδρασης με την ομάδα των ανώτατων στελεχών.

• Συμμετέχοντες - CTO, CIO, CISO, συντονιστής περιστατικών, ομάδα αντιμετώπισης, διεξαγωγή ερευνών, cyber threat intelligence, διαχείριση επιχειρησιακής συνέχειας και επαγγελματίες τεχνικούς.

4. ΠΡΟΣΟΜΟΙΩΣΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Μια προσομοιωμένη επιχείρηση πολέμου που περιλαμβάνει σχεδιασμό, προετοιμασία και εκτέλεση με σκοπό την εκπαίδευση και την αξιολόγηση.[7]

Η προσομοίωση είναι ένα σημαντικό πεδίο στη δοκιμή και την αξιολόγηση του κινδύνου για την ασφάλεια του κυβερνοχώρου, καθώς επιτρέπει την προσομοίωση των συστημάτων, τις αλληλεξαρτήσεις τους και τις αλληλεπιδράσεις μεταξύ των συστημάτων και των ανθρώπων που τα χρησιμοποιούν, παρακολουθούν ή ακόμα και επιτίθενται σε αυτά τα συστήματα.[8] Με τα σενάρια του κυβερνοασφάλειας προσπαθούμε να περιγράψουμε και να διαμορφώσουμε αυτές τις πολύπλοκες αλληλεξαρτήσεις.

4.1 Εξομοίωση έναντι της προσομοίωσης

Η εξομοίωση και η προσομοίωση χρησιμοποιούνται συχνά εναλλάξ. Ωστόσο, δεν είναι το ίδιο. Ένα Emulation τεστ (εξομοίωση) στόχο έχει να μιμηθεί, να αντιγράψει ή να αναπαραγάγει το ακριβές σενάριο έτσι ώστε να αναδημιουργήσει ένα στιγμιότυπο ή ακόμα και να αντιγράψει και τον τρόπο λειτουργίας του Hardware. Σε αντίθεση, η προσομοίωση είναι μια κατασκευή ενός σεναρίου με στόχο να μοιάζει με ένα τέτοιο σενάριο που θα μπορούσε να είναι πιθανό στην πραγματικότητα. [8] Αν και φαινομενικά λεπτές, αυτές οι διαφορές είναι ζωτικής σημασίας για την εξασφάλιση ρεαλιστικών δοκιμών. Σε ένα απλό παράδειγμα μπορούμε να σκεφτούμε ότι το MAME είναι ένας emulator που αντιγράφει τη λειτουργία ενός arcade device, ενώ ένας flight simulator στόχο έχει να εξομοιώσει με έμφαση στο software τις λειτουργίες ενός αεροπλάνου και να δημιουργήσει πιθανά σενάρια που να ανταποκρίνονται στην πραγματικότητα.

Η προσομοίωση είναι ένας οικονομικά αποδοτικός και συχνά ευέλικτος τρόπος δημιουργίας ενός αντιπροσωπευτικού συστήματος με τις αλληλεξαρτήσεις και τις σχέσεις του, το οποίο μπορεί να μελετηθεί μέσω της εκτέλεσης σεναρίων. Ωστόσο, δεν δημιουργούνται όλα τα σενάρια εξίσου και, στην πραγματικότητα, δεν περιλαμβάνουν όλα τα σενάρια προσομοίωσης μόνο προσομοιωμένα στοιχεία. Μπορούμε να ορίσουμε την προσομοίωση στους παρακάτω τύπους[9]:

- Ζωντανή προσομοίωση (cyber security): οι πραγματικοί ηθοποιοί σε σενάριο δοκιμών αλληλεπιδρούν με φυσικά συστήματα πραγματικών υπολογιστών που συνδέονται με πραγματικά και συνήθως απομονωμένα δίκτυα.
- Εικονική (cybersecurity) προσομοίωση: οι πραγματικοί ηθοποιοί σε ένα σενάριο δοκιμών αλληλεπιδρούν με την εξομοίωση/προσομοίωση δικτύων ή η προσομοιωμένοι παίχτες αλληλεπιδρούν με πραγματικά και συνήθως απομονωμένα δίκτυα.
- Εποικοδομητική (cybersecurity) προσομοίωση: οι προσομοιωμένοι/εξομοιωμένοι παίχτες (σε ένα σενάριο δοκιμής/αξιολόγησης) αλληλεπιδρούν με την προσομοιωμένα δίκτυα.

Πολλά ακαδημαϊκά εργαστήρια στοχεύουν στην εξεύρεση πρακτικών ώστε να γίνεται εκπαίδευση στο cybersecurity με hands on exercises. Αυτά τα εργαστήρια παρέχουν ένα τεχνολογικό περιβάλλον όπου ο φοιτητής μπορεί να εκπαιδευτεί σε αμυντικές και επιθετικές τεχνικές, κάποιες φορές σε τάξη μαζί εκπαιδευτή, είτε με πρόσβαση εξ αποστάσεως χωρίς άμεση εκπαιδευτική υποστήριξη.

Οι επιτραπέζιες ασκήσεις (tabletop exercises) είναι επίσης μια σχετική προσπάθεια προς την εκπαίδευση και την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο. Μία τέτοια άσκηση έχει σχεδιαστεί για να δοκιμάζει την ικανότητα μιας ομάδας να ανταποκρίνεται σε μια κατάσταση που αλλάζει βάσει των ενεργειών της. Η άσκηση αποσκοπεί συνήθως στη δοκιμή της συνεργασίας εκτός από την ετοιμότητα

αντιμετώπισης καταστάσεων κρίσης και έκτακτης ανάγκης. Ένα βασικό όφελος από μια επιτραπέζια άσκηση είναι η δυνατότητα που προσφέρει, να βάζουμε τους ανθρώπους σε υποθετικές ακραίες καταστάσεις χωρίς να προκαλούμε πραγματικό αποτέλεσμα. Ωστόσο, εξαιτίας αυτού δεν είναι σε θέση να εκπαιδεύσει και να αξιολογήσει πρακτικές ή να επιτύχει ρεαλιστική εκπαίδευση με τρόπο παρόμοιο με αυτόν που βρίσκουμε σε ένα πραγματικό συμβάν.

Μια άλλη επιλογή που κερδίζει δυναμική είναι αυτό που ονομάζεται άσκηση άμυνας στον κυβερνοχώρο (cyber defense exercise, CDX). Στο CDX οι συμμετέχοντες συγκεντρώνονται για να συνεργαστούν (ή να ανταγωνιστούν) σε ένα ενιαίο σενάριο όπου λαμβάνουν χώρα επιθέσεις και άμυνες, έχοντας να αντιμετωπίσουν τεχνικά, τα περιστατικά αλλά και να μάθουν πώς να προλαμβάνουν και να αντιδρούν καλύτερα με συνεργατικό τρόπο ενάντια σε σοβαρές καταστάσεις. Τα οφέλη του CDX ποικίλλουν. Υποστηρίζουν εξαιρετικά πολύπλοκες ασκήσεις που αποτελούνται από πολλούς stakeholders και προκλήσεις για το IT infrastructure. [11] Ενισχύουν τις ικανότητες συντονισμού καθώς και τις ανταγωνιστικές συμπεριφορές (παιχνίδι ρόλων). Επίσης, τα σενάρια που εκτελούνται είναι ρεαλιστικά, χρησιμοποιώντας πραγματικά προϊόντα και τεχνολογίες και δημιουργώντας χειροκίνητες επιθέσεις σε υφιστάμενα δίκτυα. Εν τούτοις, αυτό το είδος ασκήσεων συνεπάγεται και ορισμένα σημαντικά μειονεκτήματα. Δεν έχουν σχεδιαστεί για να καλύπτουν ποικίλα σενάρια, επομένως δεν είναι δυνατή μια ολιστική εκπαίδευση. Οι ασκήσεις απαιτούν για την αναπαραγωγή τους μεγάλη προσπάθεια και οργάνωση.[12]

Οι ασκήσεις περιλαμβάνουν πολύπλοκο συντονισμό στον προγραμματισμό την εκτέλεση, και το σχεδιασμό, την ανάπτυξη και τη διαμόρφωση καθώς και των πόρων που καταναλώνουν,. Δεν προορίζονται για την εκπαίδευση σε ατομικό επίπεδο δεδομένου ότι δεν είναι ευέλικτες.

Η παρακολούθηση των συμμετεχόντων και η προσαρμογή σε ετερογενείς δεξιότητες είναι δύσκολα εφικτή και η αξιολόγηση της επιτυχίας σε κάθε σενάριο είναι πολύ περίπλοκη χωρίς τη συμμετοχή εξειδικευμένων εκπαιδευτών και μηχανισμούς ελέγχου. Είναι προφανής η ανάγκη ύπαρξης ενός οικονομικά αποδοτικού περιβάλλοντος κατάρτισης για τη συνεχή βελτίωση των τεχνικών δεξιοτήτων σε εξελισσόμενα και απαιτητικά σενάρια.

Υπολογιστικά μοντέλα γνωστικών διεργασιών μπορούν να χρησιμοποιηθούν σε εργαλεία ασφάλειας και προσομοιώσεις για την αντιμετώπιση της ανθρώπινης πρακτικής και της αποτελεσματικής λήψης αποφάσεων για την ασφαλή διατήρηση των δικτύων.

Στα σενάρια προσομοίωσης δικτύου μπορούν να γίνουν πολλές υποθέσεις σχετικά με τους χρήστες, τους επιτιθέμενους / αμυνόμενους ή ακόμη και με τις ατομικές διαφορές μεταξύ των ανθρώπων.

Το γνωστικό μοντέλο είναι παρόμοιο με το συμπεριφοριστικό μοντέλο και συχνά χρησιμοποιείται για παρόμοιους σκοπούς. Για παράδειγμα, ένα μοντέλο συμπεριφοράς ενός desktop user μπορεί να είναι ένας πίνακας πιθανοτήτων μεταβατικής κατάστασης Markov, το οποίο δηλώνει ότι εάν ο χρήστης είναι στην κατάσταση όπου πληκτρολογεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου, μπορεί να μεταβεί σε μια κατάσταση όπου αναζητεί κάτι στο Google με μια πιθανότητα x και σε μια κατάσταση όπου εγκαθιστά λογισμικό με πιθανότητα y. Ένα γνωστικό μοντέλο παρουσιάζει τις ίδιες μεταβάσεις κατάστασης ως μετάβαση ενέργειας (state-transitions as state-actions) και να αναθέτει utilities σε κάθε ζεύγος [13].

5. ΚΟΙΝΟ ΣΥΣΤΗΜΑ ΒΑΘΜΟΛΟΓΗΣΗΣ ΕΥΠΑΘΕΙΑΣ (CVSS)

Τα ψηφιακά περιουσιακά στοιχεία ενός οργανισμού είναι επιρρεπή σε επίθεση οποιαδήποτε στιγμή. Με τις απειλές να αποκτούν νέες διαστάσεις, οι οργανισμοί θα πρέπει να είναι σε θέση να αξιολογούν αντικειμενικά τους κινδύνους των υφιστάμενων και των νέων εφαρμογών. Με βάση αυτόν τον κίνδυνο, μπορούν να διατεθούν επαρκείς πόροι για τον περιορισμό των κινδύνων ασφαλείας. Η ποσοτική πρόβλεψη της πιθανότητας επίθεσης μπορεί να βοηθήσει τους οργανισμούς να αντιμετωπίσουν τα περιστατικά εισβολής.

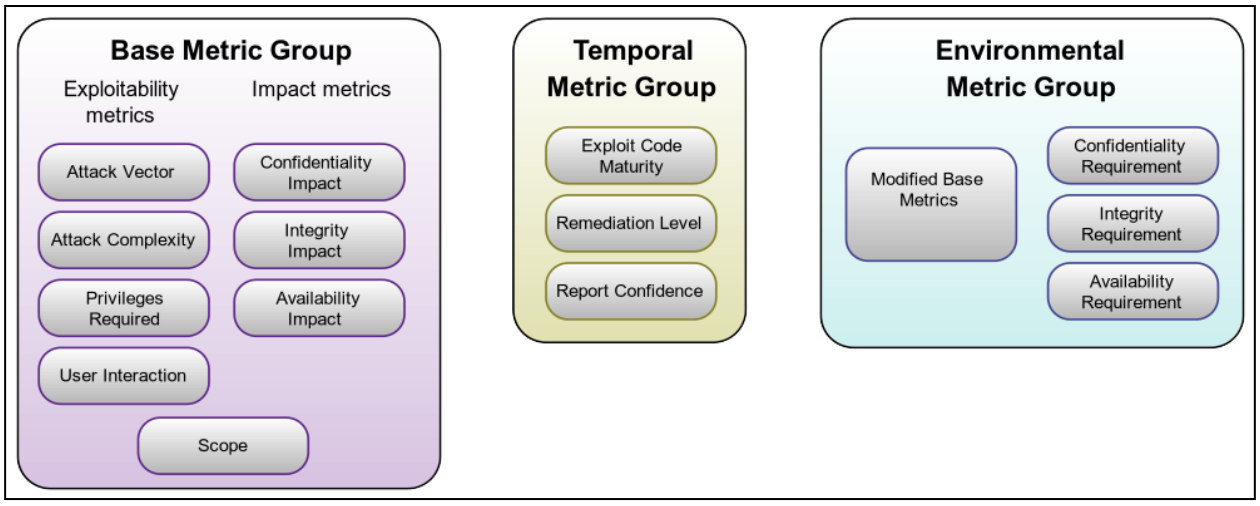
Το κοινό σύστημα βαθμολόγησης ευπάθειας (CVSS) [14], [15] είναι ένα τυποποιημένο πλαίσιο που χρησιμοποιείται από πολλούς οργανισμούς. Επικοινωνεί τα χαρακτηριστικά και τις επιπτώσεις των τρωτών σημείων. **Εικόνα 2**.

Το πλαίσιο αυτό έχει τρεις ομάδες, βασική, χρονική και περιβαλλοντική. Η ομάδα βάσης υπογραμμίζει τις ιδιότητες ευπάθειας που παραμένουν αμετάβλητες με την πάροδο του χρόνου και του χρήστη. Η χρονική ομάδα καλύπτει τα χαρακτηριστικά της ευπάθειας που μεταβάλλονται με το χρόνο εξαιτίας γεγονότων πέραν της ευπάθειας και η περιβαλλοντική ομάδα υπογραμμίζει το συγκεκριμένο περιβάλλον χρήστη και κατά πόσο έχει αυτό επίδραση στον οργανισμό . Το CVSS συμβάλλει στη δημιουργία μιας κοινής γλώσσας στην κοινότητα πληροφορικής [16].

Το CVS εισήχθη το 2005 από το Εθνικό Συμβουλευτικό Συμβούλιο υποδομών (NIAC), το οποίο παρέδωσε τη διαχείριση και την ανάπτυξη του προτύπου στον FIRST. Η τρέχουσα έκδοση, CVSS 3.0, εισήχθη τον Ιούνιο του 2015. Ως ελεύθερο και ανοιχτό πρότυπο, αρκετοί vendors όπως η Oracle έχουν προσαρμόσει τις δικές τους εκδόσεις του CVSS.

Τα συστήματα που εκτελούν PHP και Apache βρίσκονται υψηλά στη λίστα ευπάθειας λόγω της αδύναμων components και της διαχείρισης των patches.

Δυστυχώς, πολλοί οργανισμοί μπορεί να έχουν εκτεθειμένα συστήματα που προκαλούν αυξημένη πιθανότητα επίθεσης και παραβίασης της ασφάλειας τους. Συστήματα όπως το Remote desktop, SMB, βάσεις δεδομένων, Telnet κ.λπ. Πολλά εκτεθειμένες πόρτες έχουν χρησιμοποιηθεί για επιθέσεις όπως μεταξύ άλλων τα Wannacry, NotPetya, Mirai, ADB Miner, PyRoMine. [17] Τέτοιες εκτεθειμένες πόρτες μπορεί να αποτελούν πρόσβαση παραδοσιακών επιθέσεων hacking, που προκαλούν επίσης παραβίαση και απώλεια δεδομένων.



Εικόνα 2. CVSS Metric Groups

6. ΔΟΚΙΜΗ ΔΙΕΙΣΔΥΣΗΣ (PENETRATION TESTING)

Ο έλεγχος διείσδυσης είναι ένας μη αυτόματος έλεγχος που συνήθως διεξάγεται παράλληλα με μια αξιολόγηση ευπάθειας και χρησιμοποιείται για να βοηθήσει στη δοκιμή της αποτελεσματικότητας του προγράμματος διαχείρισης ευπάθειας ενός οργανισμού και των συναφών ελέγχων μέσα σε ένα καθορισμένο πεδίο εφαρμογής (blue teaming). Οι δοκιμές χρησιμοποιούνται για να ελέγξουν εάν το δίκτυο, εταιρικές πλατφόρμες, ή εφαρμογές, το hardware είναι ευάλωτα σε πιθανή εισβολή. Οι δοκιμές διείσδυσης δεν επικεντρώνονται στη μυστικότητα, την αποφυγή ή την ικανότητα της μπλε ομάδας να ανιχνεύει και να ανταποκρίνεται, καθώς η μπλε ομάδα έχει πλήρη επίγνωση των δοκιμών που διεξάγονται. Παρόμοια με τις δοκιμές διείσδυσης βάσει σεναρίων, το πλάνο της κόκκινης ομάδας (red teaming) έχει σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων, όπως η πρόσβαση σε έναν ευαίσθητο διακομιστή ή σε μια εφαρμογή, κρίσιμη για την επιχείρηση [18].

Red Teaming**.** Οι Red teaming ασκήσεις διαφέρουν ως προς το ότι επικεντρώνονται σε μεγάλο βαθμό στην εξομοίωση ενός προηγμένου σεναρίου απειλής, χρησιμοποιώντας μυστικότητα, ανατρέποντας τους καθιερωμένους αμυντικούς ελέγχους και εντοπίζοντας κενά στην αμυντική στρατηγική του οργανισμού. Η αξία αυτού του τύπου εμπλοκής μπορεί να προέλθει από την καλύτερη κατανόηση του τρόπου με τον οποίο ένας οργανισμός ανιχνεύει και ανταποκρίνεται σε επιθέσεις πραγματικού χρόνου.

Τα pen tests μπορούν να συνυπάρχουν με τις red team ασκήσεις και αυτό μπορεί να είναι λίγο συγκεχυμένο κάποιες φορές. Οι Pen testers και οι κόκκινες ομάδες μπορούν να είναι οι ίδιοι άνθρωποι, χρησιμοποιώντας διαφορετικές μεθόδους και τεχνικές για διαφορετικό σκοπό . Είναι σαν τις πολεμικές τέχνες – η μία δεν είναι απαραίτητα καλύτερη από την άλλη και γι αυτό ένας οργανισμός βλέπει αξία και στα δύο.

Πρόσφατα, προέκυψε μια νέα τεχνική που έρχεται να συμπληρώσει το red Teaming. Οι λύσεις προσομοίωσης παραβίασης και επίθεσης (Breach and Attack Simulation - BAS) αντιπροσωπεύουν μια νέα και αναδυόμενη αγορά και είναι άμεσα συσχετισμένη με την αξιολόγηση ευπάθειας, σύμφωνα με τον οδηγό αγοράς για την αξιολόγηση ευπάθειας (Market Guide for Vulnerability Assessment). Εκτελεί αυτοματοποιημένες δοκιμές ασφαλείας. Δοκιμάζει την υπάρχουσα υποδομή ασφαλείας και τρέχει ορισμένες μοντέλα επιθέσεων για να προσδιορίσει την πιο πιθανή διαδρομή που θα χρησιμοποιούσε ένας εισβολέας για να θέσει σε κίνδυνο ένα εταιρικό δίκτυο. Τα προϊόντα BAS γίνονται όλο και πιο διαδεδομένα (AttackIQ, Cymulate, XM Cyber, κλπ) και έχουν αρχίσει να μεταμορφώνουν το τοπίο δοκιμών ασφαλείας.

Purple Team: Μία "purple team" συνδυάζει τις δραστηριότητες τόσο της red team (της ομάδας ασφαλείας που δοκιμάζει την οργάνωση ενάντια στις τεχνικές που χρησιμοποιούνται κατά τη διάρκεια πραγματικών παραβιάσεων) όσο και της blue team (το προσωπικό πληροφορικής/ασφάλειας της εταιρείας που υπερασπίζεται τον οργανισμό του όλο το εικοσιτετράωρο). [19] Η μωβ ομάδα επιτρέπει τόσο την επίθεση (κόκκινη ομάδα) όσο και την άμυνα (μπλε ομάδα) να ανταλλάσσουν ιδέες και παρατηρήσεις πιο παραγωγικά. Θεωρητικά, μια μωβ ομάδα συνδυάζει τους παράγοντες που οδήγησαν στην επίθεση και τα τρωτά σημεία που βρέθηκαν από την κόκκινη ομάδα με τις αμυντικές τακτικές από την μπλε ομάδα, για να χτίσει το ισχυρότερο δυνατό πρόγραμμα ασφαλείας. Ουσιαστικά μία BAS πλατφόρμα είναι μια αυτοματοποιημένη μωβ ομάδα.

7. ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΕΦΑΡΜΟΓΗ ΑΣΚΗΣΗΣ

Ένας οργανισμός μπορεί να εκτελέσει πολλά διαφορετικά σενάρια κατά τη διάρκεια μιας άσκησης. Παρ όλα αυτά πρέπει να εστιάζει στα κρίσιμα συστήματα και δεδομένα που θα έχουν αντίκτυπο στην επιχείρηση.

Ένα playbook πρέπει να δείχνει τα βήματα που εκτελείται η άσκηση, να περιγράφει λεπτομερώς τις βασικές πτυχές του σχεδιασμού και της εκτέλεσης ασκήσεων μαζί με με τους εμπλεκόμενους που προκαλούν απειλές ενάντια στον οργανισμό.

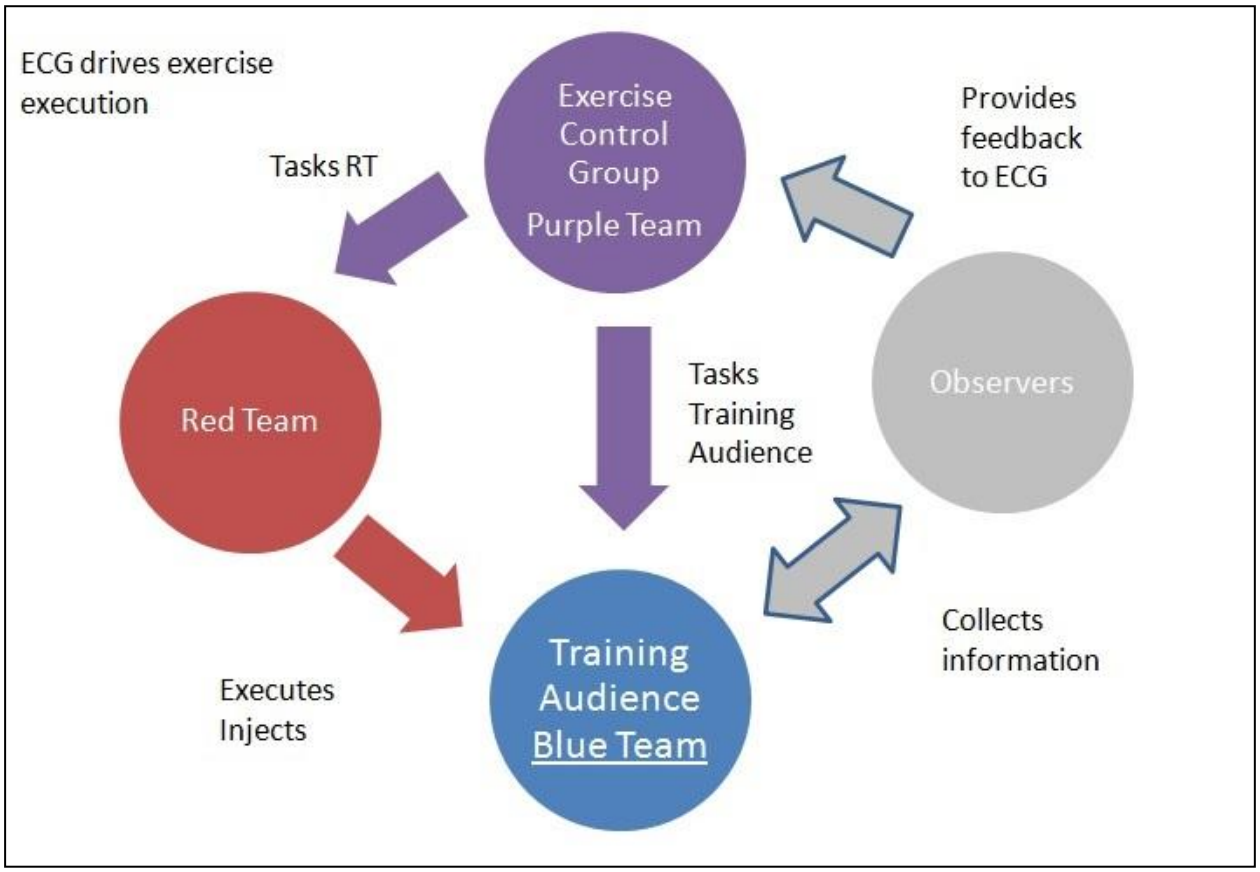
Στο playbook περιγράφονται τα παρακάτω [25]:

- Βασική ορολογία και η πρακτική εφαρμογή
- Οι καθορισμένοι στόχοι για την εκτέλεση σεναρίων απειλής για την αξιολόγηση των επιχειρήσεων στον κυβερνοχώρο
- Οι βέλτιστες πρακτικές για τη λειτουργία μιας άσκησης στον κυβερνοχώρο
- Αναφορές σχετικά με την αποτελεσματικότητα των επιθέσεων στον κυβερνοχώρο και τα σενάρια
- Οι απαραίτητες πληροφορίες για την εκτέλεση και την αξιολόγηση σεναρίων απειλής στον κυβερνοχώρο μέσα σε μια άσκηση
    - Δομή της άσκησης
    - Παραδείγματα σεναρίων
    - Πλάνο αντιμετώπισης περιστατικών
    - Παραδείγματα παρατήρησης και αναφοράς συμβάντων
    - Αρχιτεκτονική δικτύου
    - Εργαλεία που θα μπορούσαν να διευκολύνουν διάφορα σενάρια

Η διαδικασία σχεδιασμού μιας άσκησης καθορίζει τους συμμετέχοντες, το σενάριο άσκησης, τις επιθέσεις και τη σειρά ή τα βήματα κατά τα οποία θα εκτελεστεί. Η ομάδα σχεδίασης επικεντρώνεται στην επιλογή των απαραίτητων μέσων για την επίτευξη των στόχων και αναπτύσσουν ένα πλήρες σχέδιο άσκησης γνωστό ως λίστα συμβάντων κύριου σεναρίου (MSEL). Το MSEL χρησιμεύει ως σενάριο για την εκτέλεση της άσκησης και περιλαμβάνει την σειρά των επιθέσεων, τον χρόνο εκτέλεσης, και τις αναμενόμενες αντιδράσεις από το εκπαιδευτικό κοινό.

Κατά την εφαρμογή της άσκησης η μωβ ομάδα επιβλέπει την εκτέλεση και παράλληλα αναθέτει τις δραστηριότητες και στις δύο ομάδες. **Εικόνα 3**

Δεδομένου ότι έχει γίνει ο σχεδιασμός η εκτέλεση της άσκησης, ακολουθούνται τα προκαθορισμένα βήματα. Είναι φυσικά μέσα στα πλαίσια της άσκησης να παρεκκλίνει από το αρχικό σχέδιο, ανάλογα με τις συνθήκες της εκτέλεσης



Εικόνα 3: Διαδικασία εκτέλεσης της άσκησης.

Χωρίς σαφείς στόχους, δε γίνεται να σχεδιαστεί μια ουσιαστική άσκηση. Οι στόχοι επιτρέπουν στους σχεδιαστές να διαρθρώνουν με σαφήνεια τα σενάρια μέσα στην άσκηση και να καθορίζουν εάν η οργάνωσή τους διαθέτει τις απαραίτητες ικανότητες για να λειτουργήσει με επιτυχία μέσα σε ένα εχθρικό περιβάλλον στον κυβερνοχώρο και να υπερασπιστεί τις απειλές. Οι διαφορετικοί οργανισμοί έχουν διαφορετικές κατευθυντήριες αρχές, εργαλεία, τακτικές και διαδικασίες, οι οποίες καθιστούν σημαντική, τη δημιουργία μιας βασικής γραμμής για κάθε άσκηση.

Τα επιθυμητά αποτελέσματα διαφέρουν για κάθε άσκηση, αλλά πάντα πρωταρχικός ρόλος είναι η παροχή ενός ρεαλιστικού σεναρίου για την επίδειξη μεθόδων απειλής στον κυβερνοχώρο, στο εκπαιδευτικό κοινό καθώς επίσης και για η αξιολόγηση της επιτυχίας του προγράμματος και των εργαλείων που χρησιμοποιούνται για την επίτευξη των στόχων. Τα αποτελέσματα θα πρέπει να στοχεύουν στην οικοδόμηση ευαισθητοποίησης απέναντι στις αμέτρητες απειλές που κρύβονται στη έκθεση των δικτύων στο διαδίκτυο.

8. ISD FRAMEWORK

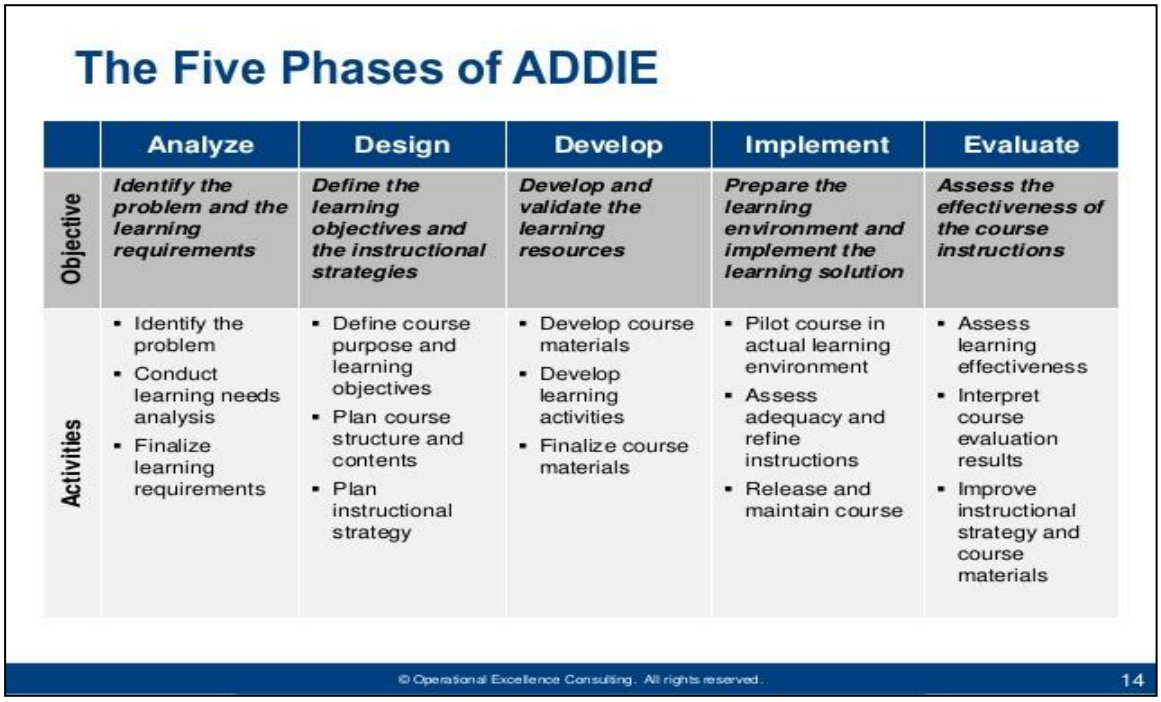
Στην παρούσα εργασία, το πρακτικό τμήμα που θα υλοποιηθεί θα είναι εκπαιδευτικού χαρακτήρα. Η ανάπτυξη εφαρμογών που εξυπηρετούν τη διαδικτυακή ή την εξ αποστάσεως εκπαίδευση παρουσιάζει μεγάλη ανάπτυξη και γι αυτό θα δούμε περιληπτικά πως αναπτύσσεται μία τέτοια πλατφόρμα.

Ο σχεδιασμός διδασκαλίας (ID), γνωστός και ως σχεδιασμός εκπαιδευτικών συστημάτων (ISD), είναι μία πρακτική συστηματικού σχεδιασμού, ανάπτυξης και παράδοσης εκπαιδευτικών προϊόντων και εμπειριών, τόσο ψηφιακών όσο και φυσικών, με τρόπο ελκυστικό και αποτελεσματικό και με απώτερο στόχο την απόκτηση γνώσης του ενδιαφερόμενου.

8.1 ADDIE

Το ADDIE [27] είναι ένα πλαίσιο σχεδιασμού εκπαιδευτικών συστημάτων (ISD) το οποίο χρησιμοποιούν πολλοί εκπαιδευτικοί σχεδιαστές και εκπαιδευτές για την ανάπτυξη μαθημάτων. Το όνομα είναι ένα αρκτικόλεξο για τις πέντε φάσεις που ορίζει για την κατάρτιση στην κατασκευή και τα εργαλεία υποστήριξης της απόδοσης [28]:

- Ανάλυση
- Σχεδίαση
- Ανάπτυξη
- Εφαρμογή
- Αξιολόγηση



Εικόνα 4: ADDIE phases

8.2 ΑΛΛΑ ΣΥΣΤΗΜΑΤΑ

Rapid prototyping, Dick and Carey, Guaranteed Learning. Άλλα χρήσιμα εκπαιδευτικά μοντέλα περιλαμβάνουν: το μοντέλο Smith / Ragan, το μοντέλο Morrison / Ross / Kemp

και το μοντέλο OAR του διδακτικού σχεδιασμού στην τριτοβάθμια εκπαίδευση, καθώς και τη θεωρία του backward design της Wiggins. [27]

Οι θεωρίες μάθησης διαδραματίζουν επίσης σημαντικό ρόλο στο σχεδιασμό εκπαιδευτικών υλικών. Θεωρίες όπως ο συμπεριφορισμός, ο κονστρουκτιβισμός, η κοινωνική μάθηση και γνωστικότητα συμβάλλουν στη διαμόρφωση και τον προσδιορισμό του αποτελέσματος των διδακτικών υλικών. Παρακάτω δίνουμε τις ερμηνείες για τους όρους που συναντήσαμε [29].

- Συμπεριφορισμός: Βασίζεται στη διαδικασία σκέψης πίσω από τη συμπεριφορά. Οι αλλαγές στη συμπεριφορά παρατηρούνται και χρησιμοποιούνται ως ένδειξη για το τι συμβαίνει στο μυαλό του μαθητή.
- Γνωστικότητα: Βασίζεται στην προϋπόθεση ότι όλοι κατασκευάζουμε τη δική μας προοπτική για τον κόσμο, μέσα από ατομικές εμπειρίες.
- Κονστρουκτιβισμός: Βασίζεται στην προϋπόθεση ότι όλοι κατασκευάζουμε τη δική μας προοπτική για τον κόσμο, μέσω ατομικών εμπειριών. Ο κονστρουκτιβισμός εστιάζει στην προετοιμασία του μαθητή για επίλυση προβλημάτων σε διφορούμενες καταστάσεις.

9. ΠΛΑΤΦΟΡΜΕΣ ΕΚΠΑΙΔΕΥΣΗΣ

9.1 Τι είναι το σύστημα διαχείρισης μάθησης (LMS);

Σύμφωνα με τη Wikipedia, ένα σύστημα διαχείρισης μάθησης είναι ένα λογισμικό για τη διαχείριση, τεκμηρίωση, παρακολούθηση, αναφορά και παροχή εκπαιδευτικών μαθημάτων, προγραμμάτων κατάρτισης και προγραμμάτων L & D. [30] Για να πληροί τις προϋποθέσεις της εταιρικής κατηγορίας LMS του G2, ενός δημοφιλούς ιστότοπου σύγκρισης προμηθευτών, μια εφαρμογή λογισμικού πρέπει να περιλαμβάνει [32]:

• Μαθήματα και άλλο εκπαιδευτικό υλικό σε ένα κεντρικό αποθετήριο που είναι προσβάσιμο στους υπαλλήλους

• Αποθήκευση των αρχείων προόδου και απόδοσης των ατόμων, τα οποία μπορούν να χρησιμοποιηθούν στην επαγγελματική τους αξιολόγηση

• Να επιτρέπεται στους διαχειριστές να προσαρμόζουν το εκπαιδευτικό υλικό με βάση τις ανάγκες των εργαζομένων

• Να προσφέρει είτε built-in μαθήματα, είτε τρίτων παρόχων

9.2 Τι είναι μια πλατφόρμα μαθησιακής εμπειρίας (LXP);

Μια πλατφόρμα μαθησιακής εμπειρίας (LXP ή LEP) είναι ένα φιλικό προς το χρήστη λογισμικό εταιρικής μάθησης που επικεντρώνεται στην παροχή εξατομικευμένης εμπειρίας κατάρτισης για τους εργαζομένους. [34] Σύμφωνα με το G2, για να πληροί τις προϋποθέσεις της κατηγορίας πλατφόρμας εκμάθησης, μια πλατφόρμα λογισμικού πρέπει:

• Παρέχει λύσεις εταιρικής μάθησης με μεγάλο εύρος περιεχομένου, γενικών γνώσεων και εξειδικευμένες λύσεις

• Δημιουργία, διαχείριση και παρακολούθηση της μαθησιακής εμπειρίας

• Βελτίωση της επαφής με τον τελικό χρήστη, της διατήρησης και της απόδοσης

9.3 Διαφορές μεταξύ ενός LMS και ενός LXP;

Ενώ τόσο τα LMSes όσο και τα LXP υπάρχουν κυρίως για να υποστηρίξουν τη μάθηση και την επαγγελματική εξέλιξη των υπαλλήλων μιας επιχείρησης, εκεί τελειώνουν οι ομοιότητες.[31]

9.4 Θεωρητική και πρακτική μάθηση

Όταν ο στόχος είναι να μάθουν οι εργαζόμενοι μια απλή διαδικασία (όπως πώς να καταθέσουν μια αναφορά εξόδων) ή να μάθουν μια θεωρητική έννοια που δεν μπορούν να εφαρμόσουν στην εργασία τους, ένα LMS θα λειτουργήσει καλά. Ωστόσο, σύμφωνα με τον κανόνα της μάθησης και ανάπτυξης 70/20/10, [31] οι εργαζόμενοι αποκτούν το 70% των γνώσεών τους από εργασιακές εμπειρίες. Αν θέλουμε οι εργαζόμενοί να εφαρμόσουν τα πράγματα που μαθαίνουν στην δουλειά τους, τότε καλύτερα με μια πλατφόρμα μαθησιακής εμπειρίας με διαδραστικές λειτουργίες όπως κουίζ, εξατομικευμένες εργασίες και κοινωνικά χαρακτηριστικά όπως η συνομιλία. Προσφέροντας στους συμμετέχοντες την ευκαιρία να αυτο-προβληματιστούν ενώ μαθαίνουν, είναι πολύ πιθανότερο να θυμούνται και να εφαρμόζουν αυτή τη μάθηση στο έργο τους στο μέλλον.

9.5 Self-paced μάθηση vs. Instructor led

Τα LMSes είναι τα καλύτερα προσαρμοσμένα για τη διαχείριση των απλών μεθόδων μάθησης που μπορούν να ξεκινήσουν και να ολοκληρωθούν στο ρυθμό και στο χρόνο που επιθυμεί ο χρήστης. Ενώ μερικά LXPs είναι επίσης κατάλληλα για τη φιλοξενία βασικών εκπαιδευτικών μαθημάτων όπως αυτά που περιγράφονται παραπάνω, κάποια άλλα όπως το Howspace είναι μια καλύτερα πλατφόρμα για πιο σύνθετα και πιο μακρόχρονα επιχειρησιακά ζωτικής σημασίας προγράμματα μάθησης όπως το management και άλλα εργαλεία επαγγελματικές ανάπτυξης.

9.6 Ατομική vs. κοινωνική μάθηση

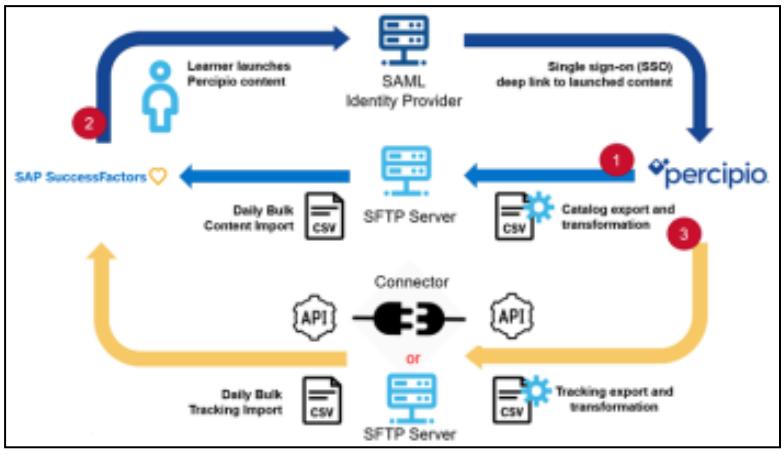
Τέλος, τα LMSes είναι κατάλληλα για εκμάθηση προγραμμάτων που δεν απαιτούν μεγάλη υποστήριξη από άλλους χρήστες για να είναι επιτυχημένα. Αν οι εκπαιδευόμενοι πρέπει απλώς να παρακολουθήσουν μερικά βίντεο ή και να διαβάσουν κάποιο υλικό για να περάσουν σε εξετάσεις ενός υποχρεωτικού μαθήματος κατάρτισης, ένα LMS μπορεί να είναι η σωστή λύση. Εάν, ωστόσο, το μάθημα επικεντρώνεται σε ένα πιο περίπλοκο θέμα, είναι καλό να θυμόμαστε ότι σύμφωνα με τον κανόνα 70/20/10 που συζητήσαμε προηγουμένως, το 20% της μάθησης γίνεται μέσω της αλληλεπίδρασης.

9.7 Ιδανικά Use cases για LMSes

Τα LMSes είναι ιδανικά για τη φιλοξενία και την παρακολούθηση απλών προγραμμάτων κατάρτισης όπως γενικά μαθήματα επιμόρφωσης για νέους υπαλλήλους, εκπαίδευση για την υγεία και την ασφάλεια και άλλα υλικά που σχετίζονται με θεωρητικές προσεγγίσεις όπως η κανονιστική συμμόρφωση. Στην πραγματικότητα, τα εταιρικά LMSes θα συνεχίσουν να είναι βασικά σε πολλούς μεγαλύτερους οργανισμούς, όπου είναι σημαντικό να παρακολουθείται η πρόοδος των εργαζομένων στα διάφορα μαθήματα.

9.8 Ιδανικά Use cases για LXP

Τα LXPs χρησιμοποιούνται επί του παρόντος επιπρόσθετα με τα LMSes και όχι ως αντικατάσταση γι 'αυτά. Αυτό συμβαίνει επειδή LXPs, επιτρέπουν πιο ολιστικές μαθησιακές εμπειρίες για κρίσιμα επιχειρηματικά προγράμματα κατάρτισης, όπως leadership trainings και άλλα στοιχεία επαγγελματικής ανάπτυξης όπου η μάθηση στη δουλειά και η κοινωνική μάθηση είναι καθοριστικής σημασίας. Π.χ. Το Percipio ενσωματώνεται με το Success Factor LMS.[35]



Εικόνα 5: Learner Data Flow Percipio with Success Factor

Τα παραπάνω συστήματα αποτελούν κύρια μέρη του σχεδιασμού και της κατασκευής μοντέλων ηλεκτρονικής μάθησης. Μια ομάδα ειδικών για μια τέτοια περίπτωση πρέπει να έχει ρόλους που παρουσιάζονται παρακάτω βάσει του μοντέλου ADDIE [28]:

• Διευθυντής ανάπτυξης ανθρώπινου δυναμικού

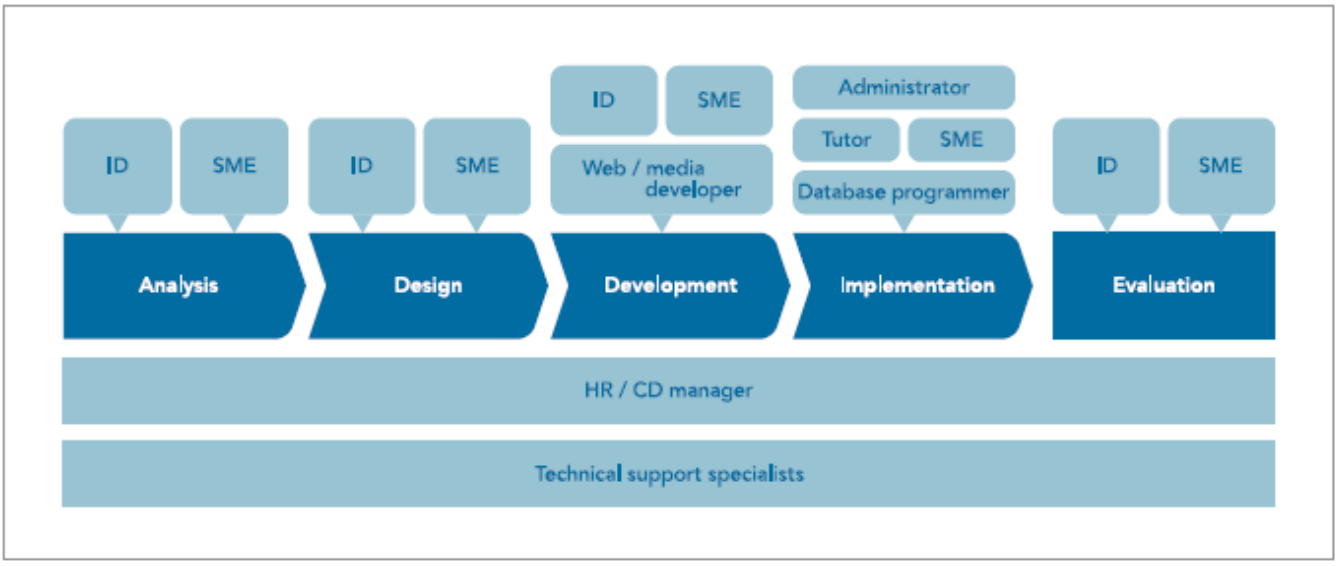
• Εκπαιδευτικοί σχεδιαστές (ID)

• Subject matter experts (MME)

• Προγραμματιστές και media editors

• Διαχειριστές μαθημάτων, και εκπαιδευτές

• Ειδικοί τεχνικής υποστήριξης



Εικόνα 6: Μοντέλο Ηλεκτρονικής Μάθησης

10. ΕΙΚΟΝΙΚΟ ΠΕΡΙΒΑΛΛΟΝ –ΕΙΚΟΝΙΚΕΣ ΜΗΧΑΝΕΣ (VMS) - ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ

10.1 Εικονικές Μηχανές (VMs)

Αρχικά, η ταχεία υιοθέτηση της εικονικοποίησης τροφοδοτήθηκε από σημαντική την εξοικονόμηση κόστους που προκύπτει από ενοποίηση των διακομιστών ενός δικτύου.[36] Πολλά VMs λειτουργούν σε έναν κεντρικό υπολογιστή επιτρέποντας στους διαχειριστές να «κάνουν περισσότερα με λιγότερα» και να μειώσουν τις δαπάνες για την αγορά εξοπλισμού. Αργότερα, πιο προηγμένες δυνατότητες όπως η κλωνοποίηση, η ανάπτυξη βάσει προτύπου (template-based development) και η σε πραγματικό χρόνο μετεγκατάσταση [37] λειτουργούντων VMs οδήγησε σε πιο ευέλικτες υποδομές πληροφορικής με αποτέλεσμα, την ευκολότερη δημιουργία και διαχείριση τέτοιων συστημάτων.

Ένας οργανισμός που ακολουθεί τις αρχές του DevOps συμπεριλαμβάνει ένα μοντέλο συνεργασίας, μεταξύ των στελεχών που λαμβάνουν επιχειρηματικές αποφάσεις, το προσωπικό ανάπτυξης των εφαρμογών, του IT και τους διαχειριστές της υποδομής. Γι αυτό και στηρίζεται σε μηχανισμούς αυτοματοποίησης που του παρέχουν ποικίλα οφέλη:

- Ελαχιστοποίηση ανθρώπινων σφαλμάτων
- Αύξηση της παραγωγικότητας του IT
- Μείωση του χρόνου υλοποίησης εφαρμογών
- Βελτίωση της απόδοσης των εφαρμογών
- Μείωση του κόστους της υποδομής

Ομοίως και στις ομάδες του NetOps έχει μεταφερθεί μεγάλο φορτίο για την διαρκή υποστήριξη των διαρκώς αναπτυσσόμενων απαιτήσεων του DevOps.[38] Οι δικτυακές υποδομές καλούνται να αντεπεξέλθουν στα επίπεδα ασφαλείας, διαθεσιμότητας και ευελιξίας που ζητούν οι εφαρμογές, με αποτέλεσμα οι παραδοσιακές μέθοδοι παραμετροποίησης του δικτύου να μην επαρκούν καθώς είναι αργές και είναι πιθανόν να εμπεριέχουν σφάλματα.

10.2 Αυτοματοποίηση

Τα παραπάνω οδήγησαν στην υιοθέτηση αυτοματοποίησης διαδικασιών και σε επίπεδο DevOps αλλά και NetOps.

Οι τεχνολογίες αυτοματισμού προσφέρουν στους μηχανικούς την δυνατότητα να αντιμετωπίσουν το δίκτυο ως σύνολο και να ξεφύγουν από την κλασική προσέγγιση της παραμετροποίησης ανά συσκευή, εκμεταλλευόμενοι το υποδομή ως κώδικα. Έτσι οι αυτοματισμοί είναι προσβάσιμοι από όλους με εργαλεία όπως το GitHub και οι Adhoc παρεμβάσεις είναι πλέον προγραμματισμένες, τεκμηριωμένες και ελεγχόμενες.

Τα παραπάνω βρίσκουν εφαρμογή και στον τομέα της διδασκαλίας της πληροφορικής και της ασφάλειας, Εκεί παράλληλα μπορεί να απαιτούνται, πολλαπλά λειτουργικά συστήματα, διαφορετικές αρχιτεκτονικές, και φυσικά πόροι οι οποίοι δεν είναι πάντα διαθέσιμοι στο εκπαιδευτικό κοινό.

Κάθε φορά η σχεδίαση και η εκτέλεση εργαστηριακών ασκήσεων μπορεί να αποτελέσει μία πρόκληση για τους σχεδιαστές, αφού πρέπει να εργαστούν με τα διαθέσιμα μέσα, τόσο σε λογισμικό όσο και σε υποδομή. Επίσης σε σενάρια κυβερνοασφάλειας ή hacking, δεν είναι πάντα επιτρεπτές οι ενέργειες σε ένα πραγματικό δίκτυο δεδομένου ότι θέτει σε κίνδυνο, ολόκληρη την δικτυακή υποδομή.[39]

Καθώς μια συσκευή προστίθεται ή αφαιρείται σε ένα δίκτυο, το περιβάλλον που το περιβάλλει αλλάζει επίσης: νέες υπηρεσίες, νέες εφαρμογές, κάποιοι κόμβοι ενδέχεται να μην είναι πλέον προσβάσιμοι. Αυτή η δυναμική μεταμόρφωση του δικτύου και, κατά συνέπεια, η διαμόρφωση της τοπολογίας, πρέπει να είναι όσο το δυνατόν ομαλότερη, ειδικά σε ένα εργαστηριακό περιβάλλον.

Σε πολλές περιπτώσεις, η υλοποίηση ενός εργαστηρίου είναι δύσκολη, επειδή η πρόσβαση σε φυσικούς υπολογιστές ή η απομακρυσμένη πρόσβαση δεν αποτελεί καλή πρακτική.

Παράλληλα η έλλειψη κεντρικού εξοπλισμού (servers, αίθουσες, κλπ) και προσωπικού, οι εκπαιδευτές ενδέχεται να μην είναι σε θέση να δημιουργήσουν εύκολα ελεγχόμενα και αναπτυγμένα περιβάλλοντα εργαστηρίου.

Ωστόσο, εάν οι μαθητές εκτελούν εργαστηριακές ασκήσεις απευθείας στους υπολογιστές τους, προκύπτουν άλλα προβλήματα: τα αποτελέσματα που παράγονται ενδέχεται να διαφέρουν από μαθητή σε μαθητή ανάλογα με το λογισμικό που είναι εγκατεστημένο στον υπολογιστή του καθενός και όλα τα εργαλεία που απαιτούνται για μια άσκηση ενδέχεται να μην μπορούν να εκτελεστούν σε όλα τα λειτουργικά.

Η λύση είναι ένα προσαρμοσμένο εργαστηριακό περιβάλλον για την υλοποίηση ασκήσεων πάνω στην κυβερνοασφάλεια και όχι μόνο ώστε να εξαλείφονται τα διαφορετικά αποτελέσματα που προκαλούνται από τις διαφορές του λογισμικού. Αυτό μπορεί να επιτευχθεί παρέχοντας στους μαθητές ένα εικονικό περιβάλλον που περιέχει ήδη το λογισμικό που σχετίζεται με εργαστήριο.

Από εκεί και πέρα, οι δυνατότητες είναι αμέτρητες και αυτό εξαρτάται από το σκοπό της εκπαίδευσης, της υποδομής του κάθε εργαστηρίου και τις δυνατότητες του εκπαιδευτή. Όπως θα δούμε παρακάτω, με μία μικρή υποδομή μπορεί να υλοποιηθεί μία εργαστηριακή διάταξη η οποία μπορεί να εξυπηρετήσει έναν hypervisor και έναν ικανοποιητικό αριθμό VMs και στοιχείων μιας δικτυακής τοπολογίας για την εξομοίωση οποιουδήποτε σεναρίου.

10.3 Παραδείγματα Εκπαιδευτικού Χαρακτήρα

Μερικές υλοποιήσεις αυτού του τύπου, όπου βρίσκουμε ένα συνδυασμό αυτοματοποιημένων διαδικασιών πάνω σε εικονικά περιβάλλοντα θα δούμε συνοπτικά στις παρακάτω παραγράφους.

10.3.1 ADLES

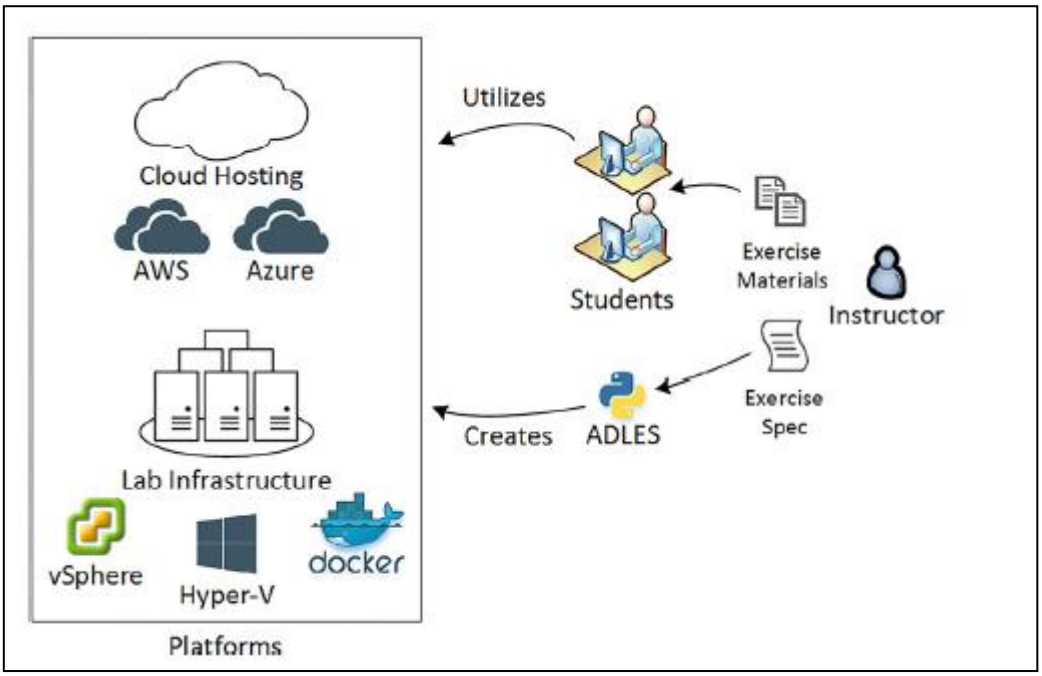
Αυτοματοποιημένη ανάπτυξη συστήματος εργαστηριακού περιβάλλοντος. Με τη χρήση των προδιαγραφών της ADLES και των εργαλείων της, ένας εκπαιδευτικός μπορεί να σχεδιάσει, να καθορίσει και να αναπτύξει σχεδόν αυτόματα το περιβάλλον που απαιτείται για μια εκπαίδευση. Επιπλέον, οι εκπαιδευτής είναι σε θέση να μοιραστεί με τους εκπαιδευόμενους.[42]

Η ADLES επιτρέπει:

(1) την αυτοματοποίηση του virtual-computing, της δικτύωσης και ασκήσεις ασφάλειας στον κυβερνοχώρο,

(2) την αυτόματη ανάπτυξη συγκεκριμένων ασκήσεων και

(3) την αποτελεσματική κοινή χρήση τέτοιων ασκήσεων και της υποδομής του hardware.

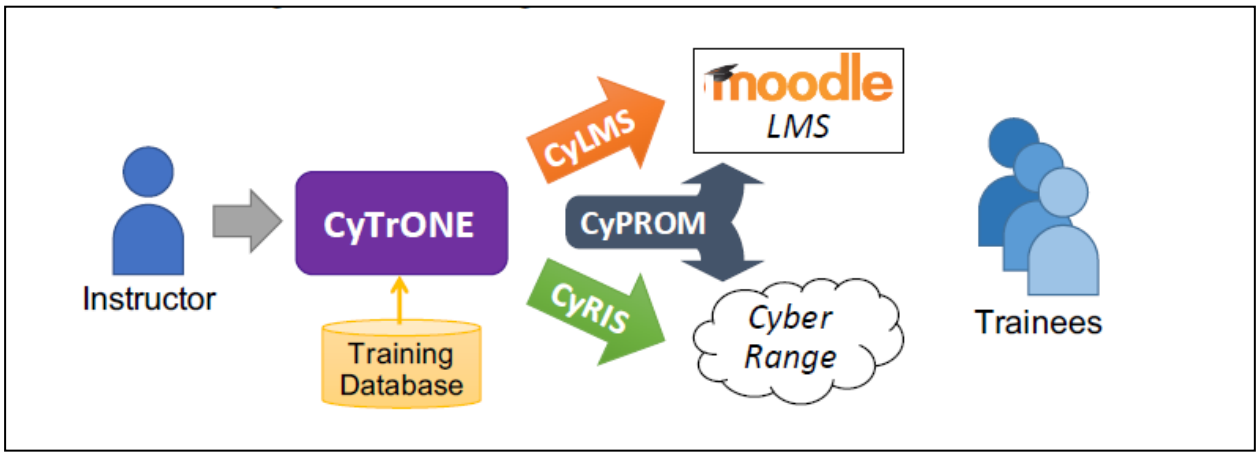


Εικόνα 7. Πλατφόρμα ADLES

10.3.2 CyTrONE

Το CyTrONE είναι ένα εκπαιδευτικό πλαίσιο κυβερνοασφάλειας που απλοποιεί τη διαδικασία εγκατάστασης ενός εκπαιδευτικού εργαστηρίου μέσω μιας προσέγγισης που ενσωματώνει το περιεχόμενο εκπαίδευσης και τη διαχείριση του εκπαιδευτικού περιβάλλοντος.[43]

Κατά τη χρήση του CyTrONE, ένας εκπαιδευτής παρέχει το υλικό της εκπαίδευσης βάσει του επιλεγμένου σεναρίου, και ακολούθως το πλαίσιο θα ανακτήσει το κατάλληλο περιεχόμενο από μια βάση δεδομένων εκπαίδευσης. **Εικόνα 8**



Εικόνα 8. Αρχιτεκτονική της πλατφόρμας CyTrONE

11. ΕΠΙΛΟΓΗ ΕΡΓΑΛΕΙΩΝ (ΠΡΟΣΟΜΟΙΩΣΗΣ ΚΑΙ ΑΥΤΟΜΑΤΙΣΜΟΥ)

11.1 Εξομοίωση

Όπως έχουμε προαναφέρει ένας εξομοιωτής στόχο έχει να μιμηθεί ή να αναπαραγάγει το ακριβές σενάριο έτσι ώστε να αναδημιουργήσει ή ακόμα και να αντιγράψει τον τρόπο λειτουργίας του Hardware. Τρία τέτοια διαθέσιμα παραδείγματα είναι το GN3, το EVE-ng και το NS3. Παρατηρήσαμε ότι υπάρχουν πλεονεκτήματα και μειονεκτήματα σε όλες περιπτώσεις.[49]

11.1.1 GNS3

Ο GNS3 [47] είναι ένας εξομοιωτής (emulator) δικτύων που προσομοιώνει σύνθετα δίκτυα, όσον το δυνατόν πιο κοντά στο τρόπο που λειτουργούν τα πραγματικά.

Είναι λογισμικό ανοικτού κώδικα και λειτουργεί σε διάφορα λειτουργικά συστήματα όπως Microsoft Windows, Linux, MacOS. Παρέχει ολοκληρωμένες και ακριβείς προσομοιώσεις χρησιμοποιώντας τους ακόλουθους εξομοιωτές για να τρέξει τα λειτουργικά συστήματα όπως σε ένα αληθινό περιβάλλον:

- Dynamips, Cisco IOS
- Virtual box, Vmware
- QEMU
- Dockers

11.1.1.1 Απαιτήσεις

- Windows 7 (64 bit) or later
- 4 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT
- Virtualization extensions required. You may need to enable this via your computer's BIOS.
- 16 GB RAM
- Solid-state Drive (SDD)
- 35 GB available space
- Virtualized devices is processor and memory intensive. More is better but properly configured device trumps RAM and Processing power.

11.1.2 EVE-NG

Δεν υπάρχει ορισμένο πεδίο χρήσης του EVE-NG [48], αφού φαίνεται πως εξαρτάται από το που θέλει να φτάσει ο χρήστης και φυσικά από τα διαθέσιμα hardware resourses. Μπορεί να βρει εφαρμογή σε διάφορα σενάρια δικτύωσης, σε vendor specific POCs, ή σε σενάρια network automation και SDN. Δεν είναι μόνο για troubleshooting δικτύων αλλά και δοκιμές software σε δίκτυα προσομοίωσης, servers ή και δοκιμές σε θέματα ευπάθειας ασφάλειας.

Υπάρχουν δύο διαθέσιμες εκδόσεις η community και η Pro. Σύμφωνα με τη βιβλιογραφία η community version είναι ικανοποιητική για test labs και POCs.

11.1.2.1 Απαιτήσεις

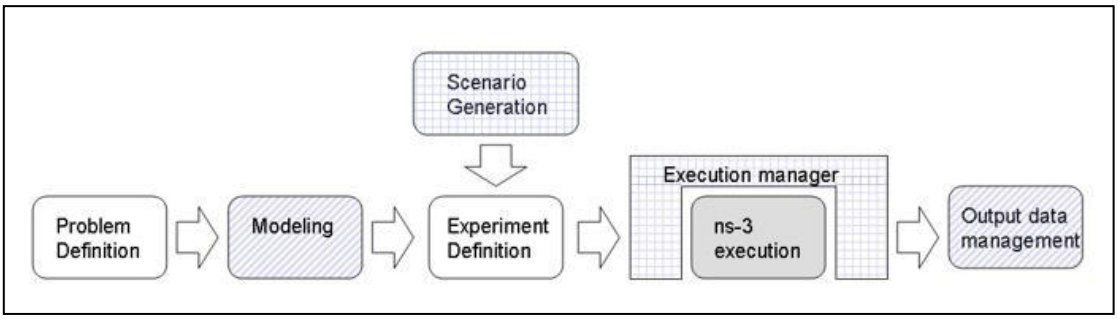
- Intel CPU VT-x/EPT
- Hypervisor

- Ubuntu Xenial Xerus 16.04.X LTS 64bit (suggested with any processors). (Ubuntu 18 and 19 are not supported due it still not have all necessary libs for EVE)
- VMware ESXi 6.0 or later
- VMware Workstation 14.0 or later
- VMware Fusion 8 or later
- VMware Player 14.0 or later
- Google Cloud platform VM
- AMD Ryzen 3900, Epyc or newer series. Older series AMD can have issues

11.1.3 NS-3

Ο NS-3 είναι ένας εξομοιωτής διακριτών γεγονότων (DES). [46] Μοντελοποιεί δηλαδή ένα σύστημα ως μία διακριτή σειρά γεγονότων. Κάθε πράξη συμβαίνει σε μία καθορισμένη σειρά στο χρόνο και πυροδοτεί μία αλλαγή στο σύστημα, με αποτέλεσμα να αλλάζει την κατάστασή του. Αυτό στον NS-3 επιτυγχάνεται με C++ συναρτήσεις οι οποίες προγραμματίζουν τα γεγονότα να συγκεκριμένους χρόνους της προσομοίωσης. [17]

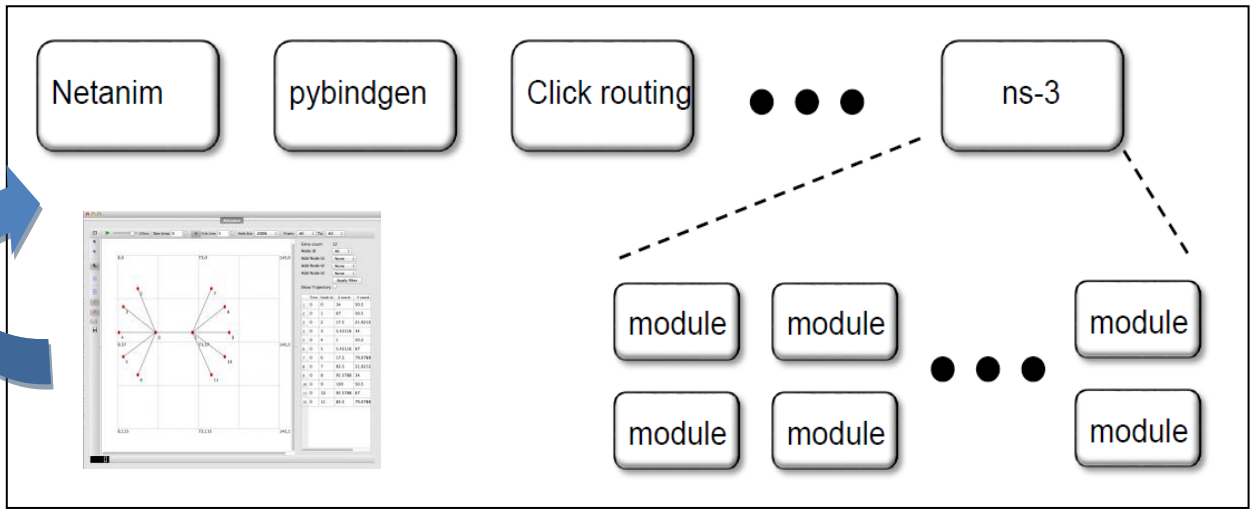
- simulation scheduler καλεί την εκτέλεση των γεγονότων,
- Simulation::Run()
- Η προσομοίωση σταματά σε καθορισμένο χρόνο, ή μετά το πέρας των γεγονότων



Εικόνα 9:. Evolution model of discrete events

Για την υποστηρικτική λειτουργία του NS3 υπάρχουν διάφορα Libraries, που δεν είναι εγκατεστημένες στο σύστημα, αλλά μπορούν να υπάρχουν παράλληλα, ενώ τα modules βρίσκονται στο directory του ns3. **Εικόνα 10**

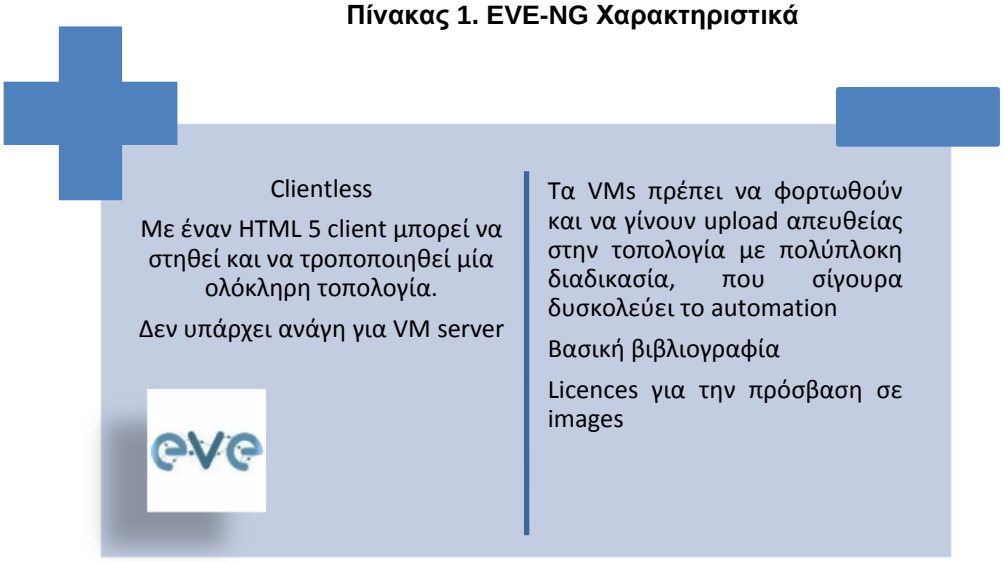
Ο NS-3 δε διαθέτει ένα IDE (Integrated Development Environment) για τη ρύθμιση, την εκτέλεση και την απεικόνιση των προσομοιώσεων σε ένα ενιαίο παράθυρο όπως σε άλλους προσομοιωτές. Υπάρχει ένα ευρύ φάσμα από animators και λογισμικά ανάλυσης δεδομένων όπως επίσης και εργαλεία απεικόνισης αποτελεσμάτων που μπορεί να αξιοποιήσει ο NS-3. Παρόλα αυτά , ο χρήστης πρέπει να είναι εξοικειωμένος με εργαλεία ανάπτυξης όπως η C++ και η Python.



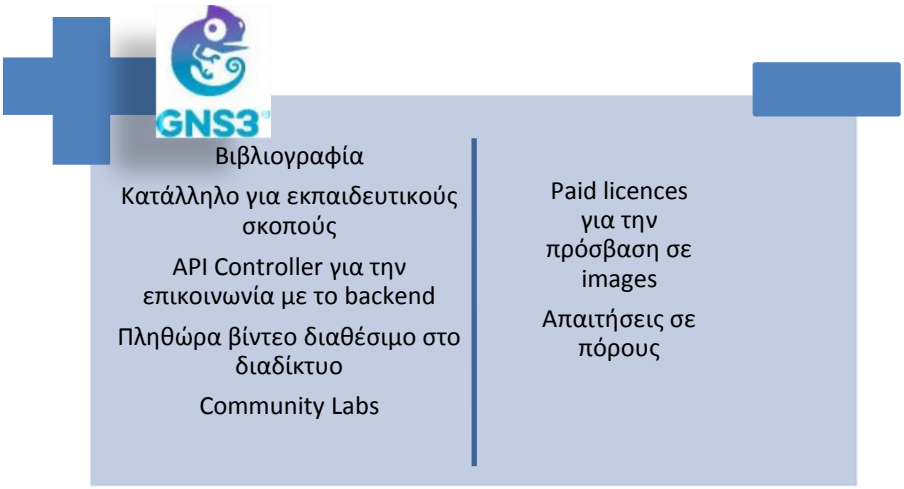
Εικόνα 10: NS3 Modules

Συνειδητά επιλέξαμε να χρησιμοποιήσουμε ως εξομοιωτή το GNS3, ως την πιο προσιτή λύση για ένα τέτοιο POC. Παρά τους όποιους περιορισμούς που μας ανέδειξε στην πορεία, θεωρήθηκε ως ο πιο πλήρης από άποψη συνδυασμού δυνατοτήτων, βιβλιογραφίας, και απλότητας στην υλοποίηση. Κατά την πορεία της άσκησης, υπήρχαν διαθέσιμες πληροφορίες, από forums και videos από το gns, τα οποία θα βοηθήσουν τον χρήστη να υλοποιήσει μία τέτοια άσκηση. Η δεύτερη μας επιλογή θα ήταν σίγουρα το EVE-ng, το οποίο είναι σίγουρα πολλά υποσχόμενο και με πολλές δυνατότητες. Υπάρχουν αρκετές ομοιότητες με το GNS3, από το documentation φαίνεται ότι έχει παρόμοιο τρόπο αρχικού setup, δυστυχώς όμως απαιτεί πολύ μεγαλύτερη προσωπική αναζήτηση στο κάθε πρόβλημα που μπορεί να συναντήσει ο χρήστης καθ' όλη την πορεία. Αν το ζητούμενο της παρούσας εργασίας ήταν αποκλειστικά η έρευνα πάνω στο EVE-ng ίσως θα είχε ενδιαφέρον η εμβάθυνση στις δυνατότητες του. Τέλος το NS-3 δεν προτείνεται για μία τέτοια δραστηριότητα, καθώς παρά τον εκπαιδευτικό χαρακτήρα του και την υποστηρικτική κοινότητα που το στηρίζει, παρουσιάζει αρκετές δυσκολίες στην αρχική του εγκατάσταση και παραμετροποίηση, η οποία στην προκειμένη περίπτωση θα προσέθετε περισσότερο χρόνο στην υλοποίηση. Επίσης χρησιμοποιείται κατά κόρον σε άλλου τύπου Test beds, δικτυακής προσομοίωσης, παρακολούθησης της κίνησης μεταξύ των κόμβων του συστήματος, παρά στο κομμάτι της αυτοματοποίησης και της συνεργασίας με τα εργαλεία που θα δούμε στην επόμενη ενότητα.

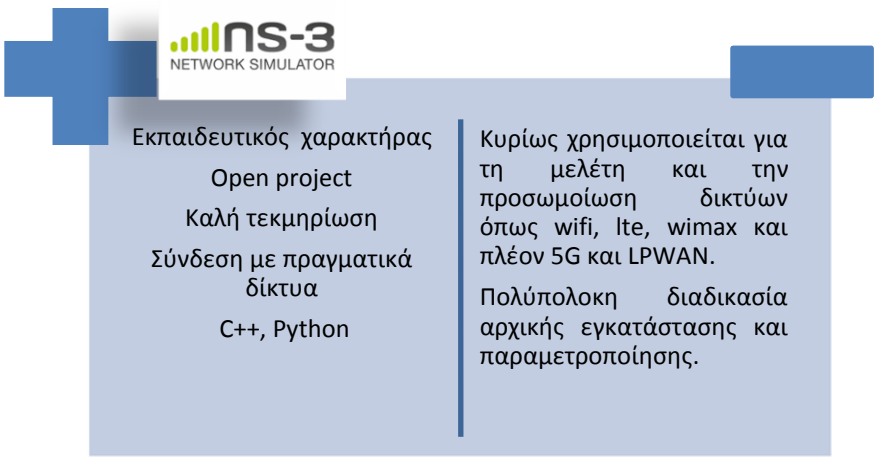
Πίνακας 1. EVE-NG Χαρακτηριστικά



Πίνακας 2. GNS3 Χαρακτηριστικά



Πίνακας 3. NS-3 Χαρακτηριστικά



11.2 Αυτοματισμοί

Όταν καλούμαστε να υιοθετήσουμε την Υποδομή ως Κώδικα (IaC) μπορούμε να παρατηρήσουμε ότι υπάρχουν διάφορες επιλογές όταν πρόκειται για εργαλεία ανοιχτού κώδικα που μπορούν να χρησιμοποιηθούν.

Για παράδειγμα, τα Chef, Ansible, Puppet, SaltStack και άλλα είναι όλα αυτά τα εργαλεία που μπορούν να χρησιμοποιηθούν ως μέρος μιας DevOps ή NetOps εργαλειοθήκης για την αυτοματοποιημένη υλοποίηση σε περιβάλλοντα δημιουργίας εφαρμογών είτε και δικτυακών υποδομών.

Η επιλογή του καταλληλου εργαλείου απαιτεί την κατανόηση από τον χρήστη των πολλών εργασιών που σχετίζονται με το provisioning εφαρμογών και υποδομών. Οι εργασίες χωρίζονται γενικά στους εξής τομείς: διαχείριση διαμόρφωσης (configuration management) και ενορχήστρωση διαμόρφωσης (configuration orchestration). [67]

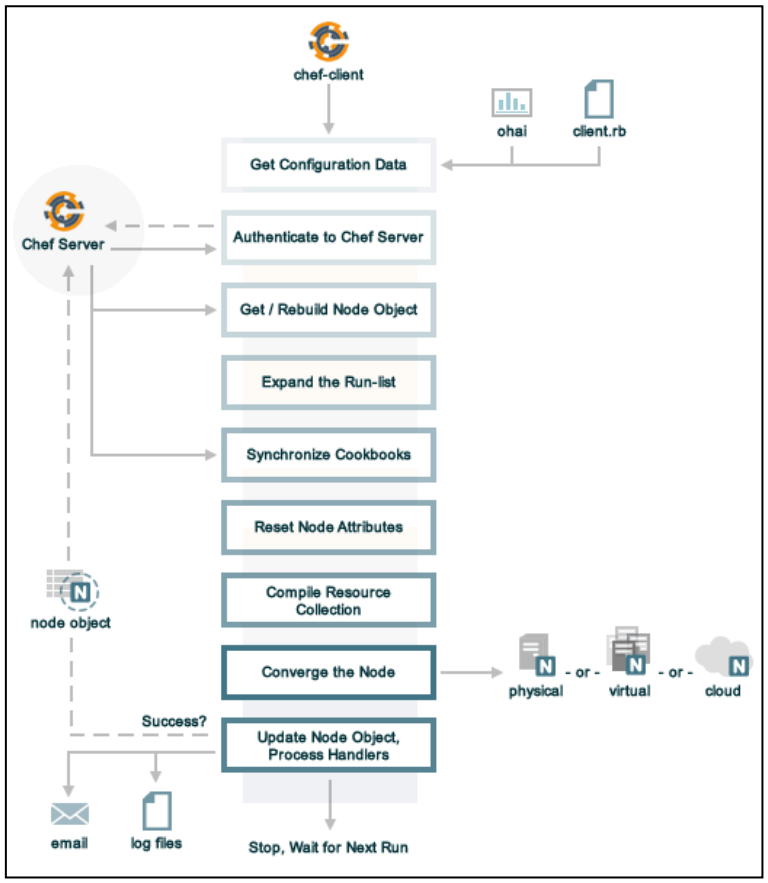
Τα εργαλεία που προαναφέρθηκαν και θα δούμε πιο αναλυτικά παρακάτω, μπορούν να χαρακτηριστούν ως CM εργαλεία και ως κύριο στόχο έχουν την αυτοματοποίηση σε επίπεδο servers, τη διαχείριση services κ.α, αποφεύγοντας έτσι τη χειροκίνητη παραμετροποίηση.

11.2.1 Chef

Εικόνα 11. Chef Infra Architecture

Το Chef Infra είναι η πλατφόρμα αυτοματοποίησης που μεταφράζει το hardware σε κώδικα.

Με το Chef Workstation μπορεί ο χρήστης να δημιουργήσει cookbooks και να διαχειριστεί όλη την υποδομή του δικτύου. Το Chef Workstation τρέχει στον προσωπικό υπολογιστή του χρήστη σε Linux, MAC OS, ή Windows. Με το workstation στο οποίο περιλαμβάνονται τα διάφορα εργαλεία όπως το Knife που αλληλεπιδρά με τον chef infra server και το chef που αλληλεπιδρά με το local repositories. Ο server λειτουργεί ως Hub όπου γίνεται upload η παραμετροποίηση. Οι clients έχουν εγκατεστημένο τον Infra client, ώστε πολλές διεργασίες να μην καταναλώνουν πόρους από το server. Επιτυγχάνεται έτσι η επικοινωνία μαζί του για περιοδικές ενημερώσεις για νέα cookbooks τα οποία αναλαμβάνει να εκτελέσει τοπικά. [53]



Εικόνα 12: Chef Infra cient Run

Παρακάτω γίνεται αναφορά σε δύο modules της chef και δύο παραδείγματα του πως μπορεί να συνδεθεί με ένα vmware hypervisor.

Knife

Το knife είναι ένα command-line tool that provides an interface between a local chef-repo and the Chef Infra Server. knife helps users to manage:

Το knife είναι ένα command-line tool το οποίο παρέχει ένα Interface μεταξύ του local chef-repo και του Chef Infra Server και παρέχει στο χρήστη τη δυνατότητα στο χρήστη να διαχειριστεί:

- Nodes
- Cookbooks και recipes
- Data Bags
- Το installation του Chef Infra Client στους nodes
- Την αναζήτηση των indexed data στον Chef Infra Server

Knife-vsphere

- vCenter > 5.0
- Starting point for Chef and VMware

```
knife[:vsphere_host] = "vcenter-hostname"
knife[:vsphere_user] = "privileged username" # Domain logins may need to be "user@domain.com"
knife[:vsphere_pass] = "password" #
knife[:vsphere_dc] = "your-datacenter"
knife[:vsphere_insecure] = true  # Set this if you have self signed certs
```

Εικόνα 13: Config.rb settings

```
knife vsphere vm clone MACHINENAME --template TEMPLATENAME --bootstrap --cips dhcp
```

Εικόνα 14: Clone VM from vcenter

knife-vcenter

- vCenter >= 6.5 REST API
- Για VCSA ή vCenter 6.5+, χρησιμοποιούμε αυτό το plug-in.

```
knife[:vcenter_username] = "root"
knife[:vcenter_password] = "*********"
knife[:vcenter_host] = "192.168.239.135"
knife[:vcenter_disable_ssl_verify] = true # if you want to disable SSL checking
```

Εικόνα 15: Config.rb settings

```
- knife vcenter vm clone example-01 --targethost 192.168.239.135 --folder example --connection-password \ ******* --datacenter Datacenter 1 –cluster Cluster 1 --template Lubuntu-template -N example-01
- Creating new machine
- Waiting for network interfaces to become available...
- ID: vm-183
- Name: example-01
- Power State: POWERED_ON
- Bootstrapping the server by using bootstrap_protocol: ssh and image_os_type: linux


- Waiting for sshd to host (192.168.239.131)
- ...
```

Εικόνα 16: Clone VM from vcenter

11.2.2 Puppet

Η Puppet είναι ένα εργαλείο με το οποίο επιτυγχάνεται η αυτοματοποιημένη διαχείριση των servers. Κατά τη χρήση της puppet, ορίζει ο χρήστης την επιθυμητή κατάσταση των

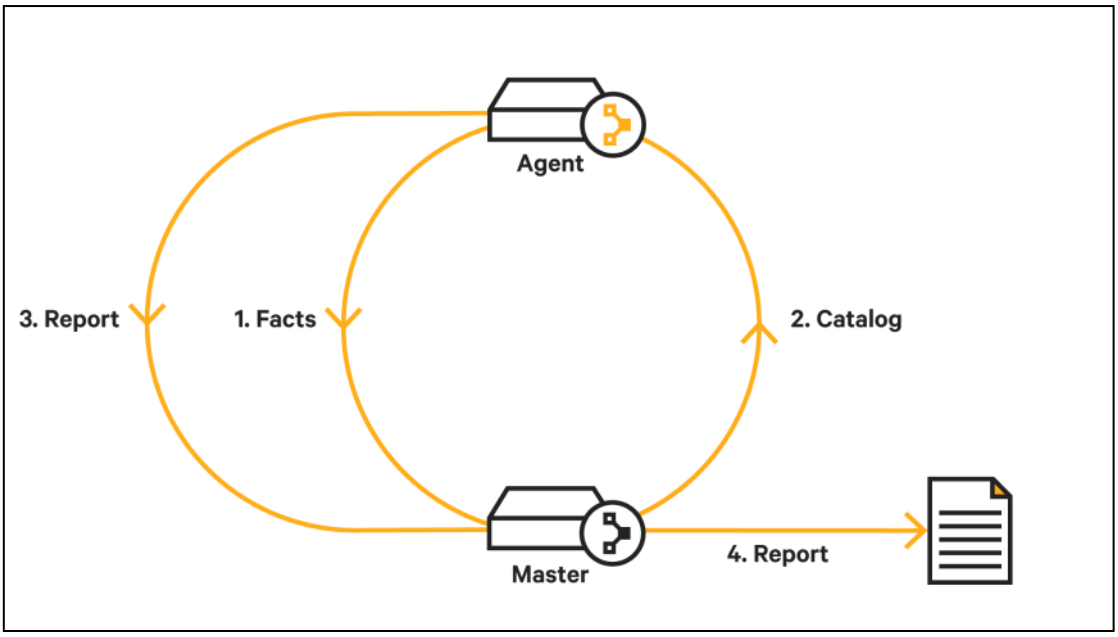
συστημάτων. [52] Όπως φαίνεται και στο συγκριτικό πίνακα χρησιμοποιείται infrastructure κώδικας Puppet's Domain-Specific Language (DSL) — Puppet Code, ο οποίος μπορεί να δουλέψει με πολλά λειτουργικά συστήματα και με πολλές συσκευές. Ο κώδικας puppet είναι declarative, δηλώνει δηλαδή ο χρήστης, την επιθυμητή κατάσταση του συστήματος και όχι τον τρόπο με τον οποίο θα φτάσουν στην κατάσταση αυτή. **Εικόνα 17**

Η puppet αυτοματοποιεί τη διαδικασία αυτή και το καταφέρνει μέσω του Puppet master και Puppet agent. **Εικόνα 18**

Ο Puppet master είναι ο διακομιστής που αποθηκεύει τον κώδικα που καθορίζει την επιθυμητή κατάσταση. Ο Puppet agent μεταφράζει τον κώδικα σε εντολές και στη συνέχεια το εκτελεί στα συστήματα που έχει καθορίσει ο χρήστης, η αλλιώς "puppet run".

```
- user { 'joe':
- ensure   => present,
- uid      => '1001',
- gid      => '1000',
- comment  => 'Joe User',
- managehome => true,
- }
```

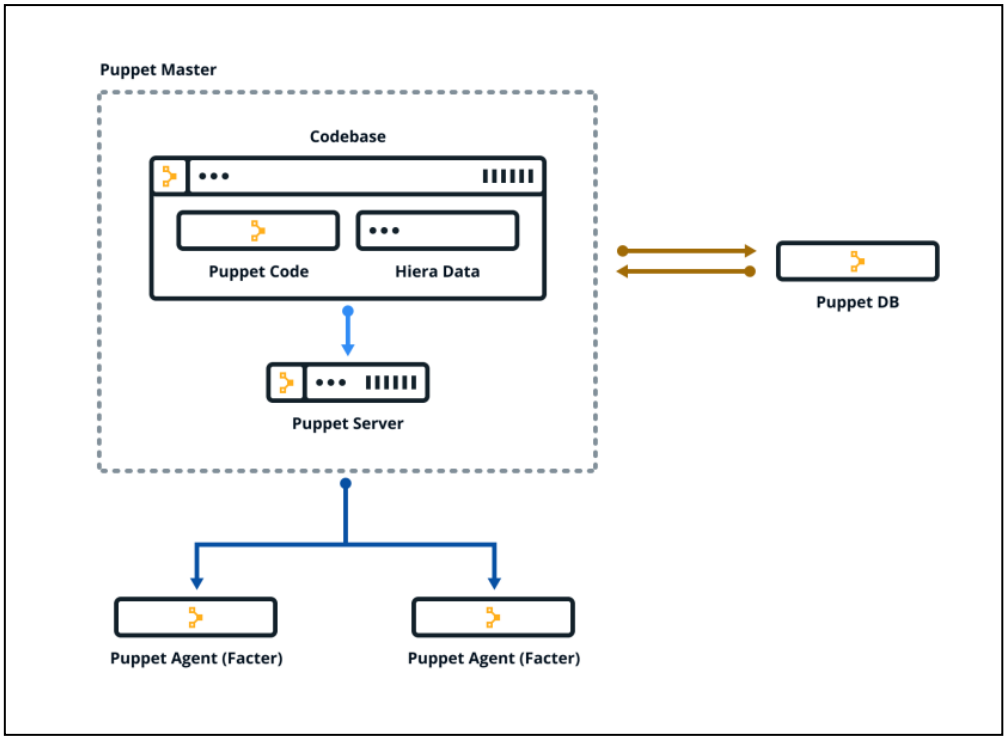
Εικόνα 17: Puppet declarative Code



Εικόνα 18: Master-agent architecture of a Puppet run

Όλα τα δεδομένα που παράγονται από το Puppet (για παράδειγμα facts, catalogs, reports) **Εικόνα 18,** αποθηκεύονται στη βάση δεδομένων (PuppetDB). Η αποθήκευση

δεδομένων στη βάση, επιτρέπει στο Puppet να λειτουργεί πιο γρήγορα και παρέχει ένα API για άλλες εφαρμογές για πρόσβαση στα δεδομένα που συλλέγονται σε αυτό. Μόλις η PuppetDB περιέχει πλέον όλα τα δεδομένα της υφιστάμενης υποδομής, γίνεται ένα inventory της υποδομής , εργαλείο reporting και αξιολόγησης ευπάθειας. Οι παραπάνω εργασίες μπορούν να ληφθούν με ερωτήματα (queries) στην PuppetDB.



Εικόνα 19: How puppet components fit together

Puppetlabs/vsphere

Αντίστοιχα θα εξετάσουμε το module της puppet που θα μας επιτρέψει να αλληλεπιδράσουμε με έναν hypervisor, στην προκειμένη περίπτωση το vcenter.

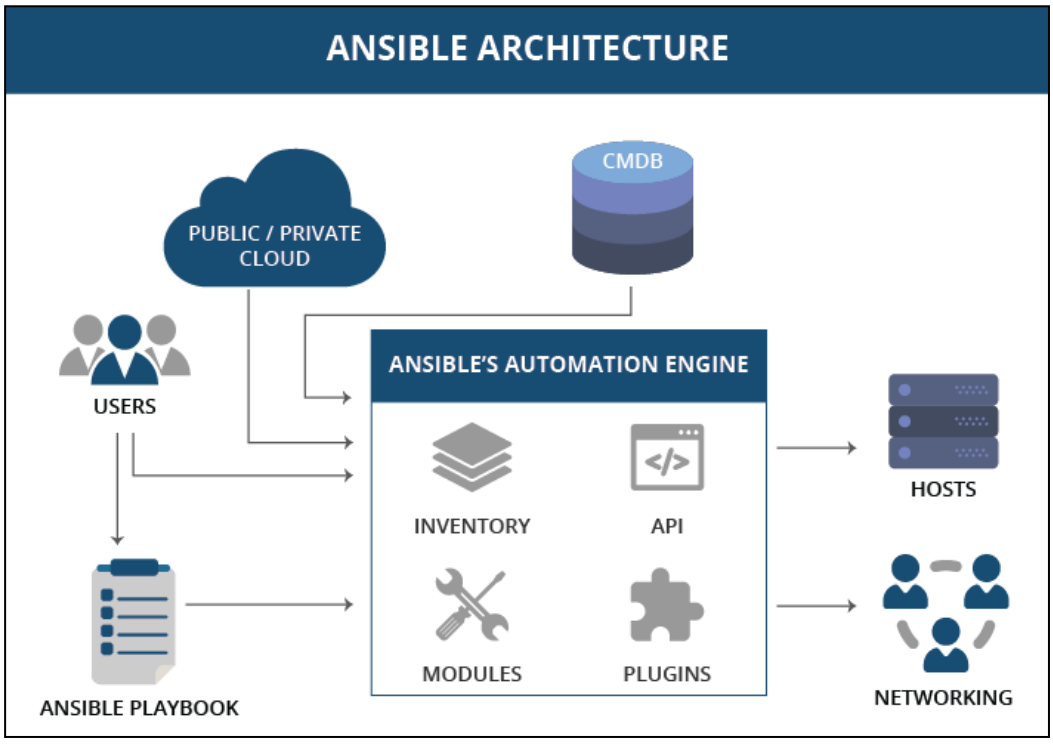
Απαιτήσεις –

- Puppet Enterprise 3.7 or greater
- Ruby 1.9 or greater
- Rbvmomi Ruby gem 1.8 or greater
- vSphere 5.5

```
- vsphere_vm {'/opdx1/vm/eng/sample':
- ensure               => 'present',
- resource_pool        => 'general1',
- cpu_reservation      => '0',
- cpus                 => '1',
- guest_ip             => '10.32.99.41',
- hostname             => 'debian',
- instance_uuid        => '501870f2-f891-879f-2bb7-f87023789959',
- memory               => '1024',
- memory_reservation   => '0',
- number_ethernet_cards => '1',
- power_state          => 'poweredOn',
- snapshot_disabled    => false,
- snapshot_locked      => false,
- snapshot_power_off_behavior => 'powerOff',
- template             => false,
- tools_installer_mounted => false,
- uuid                 => '4218419b-3b98-18ca-e77f-93b567dda463',
- }
```

Εικόνα 20: Puppet vsphere clone VM

11.2.3 Ansible



Εικόνα 21: Ansible Architecture

Ansible Framework

- Εύκολο set up and run
- Απλή αρχιτεκτονική (clientless)
- Push model (ο server επικοινωνεί με τους clients και εκτελεί τις εντολές)
- Host inventory: ο server διατηρεί λίστα, με τους hosts που επικοινωνεί που γίνεται Monitor από το config. File
- Λειτουργικά Modules, service modules και cron modules (δηλαδή προγραμματισμένα tasks).

Ενώ η salt σηκώνει ad-hoc minions και στέλνει commands, η ansible υπολογίζει τις εντολές στον server και στέλνει οδηγίες στον client μέσω SSH.

Επίσης να αναφέρουμε ότι η Ansible είναι ανεξάρτητη του λειτουργικού, που σημαίνει ότι μπορεί ο χρήστης να χρησιμοποιήσει το ίδιο playbook και να αφήσει το σύστημα να επιλέξει τον κατάλληλο package manager για την εγκατάσταση πχ. Του software που προσπαθεί να στείλει [50].

```
- name: install some essential packages
- action: >
    - {{ ansible_pkg_mgr }} name={{ items }} state=present
      update_cache=yes
- with_items:
    - vim
    - zsh
    - apache2
```

Εικόνα 22: Package Installation

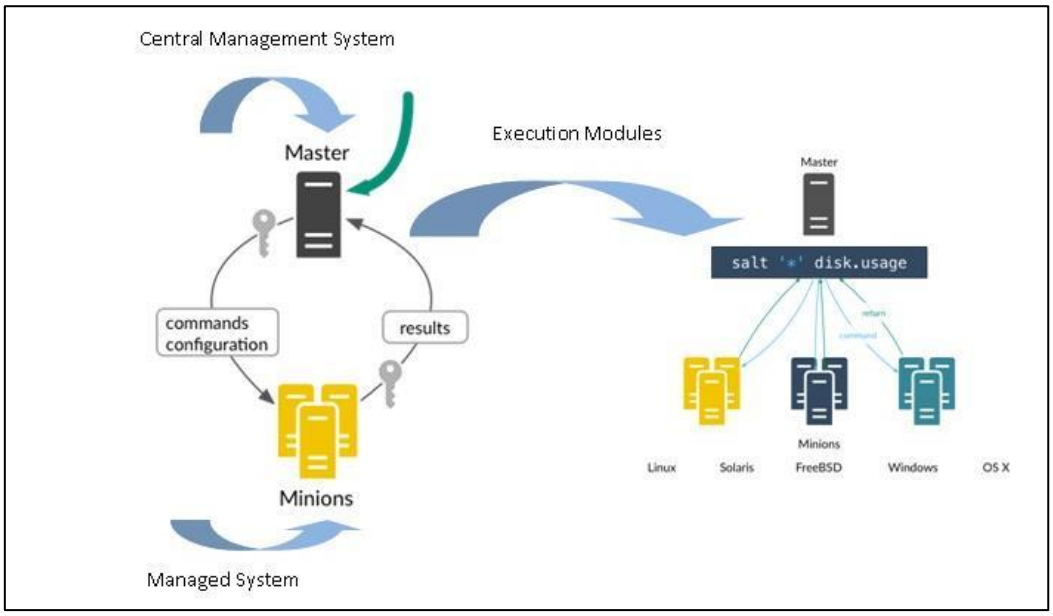
Όπως και σε όλες τις άλλες περιπτώσεις θα δώσουμε ένα παράδειγμα αλληλεπίδρασης ενός Ansible server με έναν hypervisor (esxi) για τη διαχείριση των VMs. **Εικόνα 23**

```
---
- hosts: webservers
- vars:
    - http_port: 80
    - max_clients: 200
    - remote_user: root
- tasks:
- name: ensure apache is at the latest version
- yum:
- name: httpd
- state: latest
        - name: write the apache config file
- template:
- src: /srv/httpd.j2
- dest: /etc/httpd.conf
- notify:
        - restart apache
        - name: ensure apache is running
- service:
- name: httpd
- state: started
- handlers:
        - name: restart apache
- service:
- name: httpd
- state: restarted
```

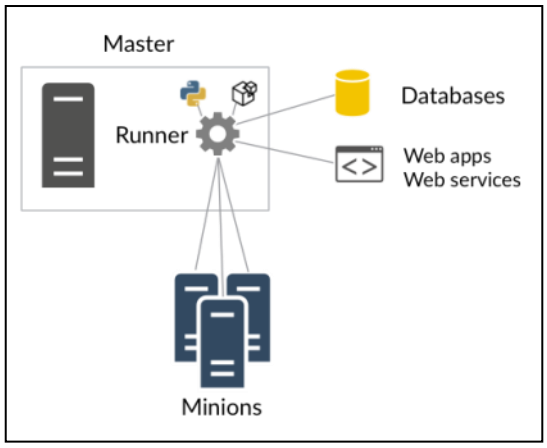
Εικόνα 23: Ansible playbook checking version of apache server

11.2.4 Saltstack

Εδώ συναντάμε την ίδια φιλοσοφία αφού όπως φαίνεται και στον πίνακα χρησιμοποιούμε yaml και Python modules (pyvomi), οπότε θεωρητικά όπου υπάρχει Python μπορεί να λειτουργήσει, όπως και στην Ansible. **Πίνακας 4**



Εικόνα 24: Saltstack Components

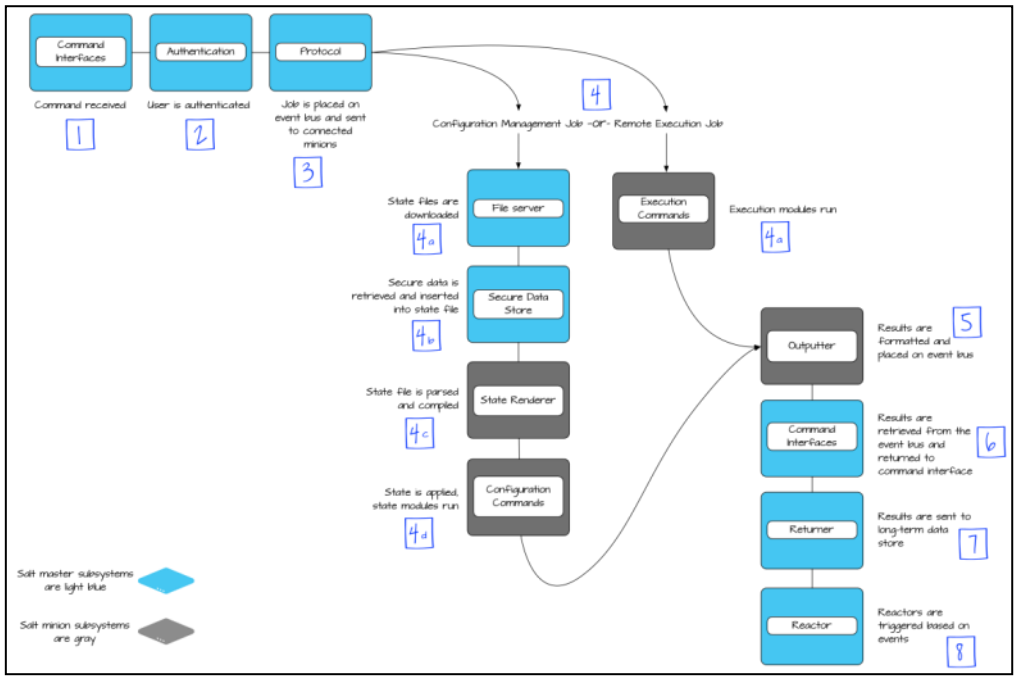


Εικόνα 25: Salt Runners

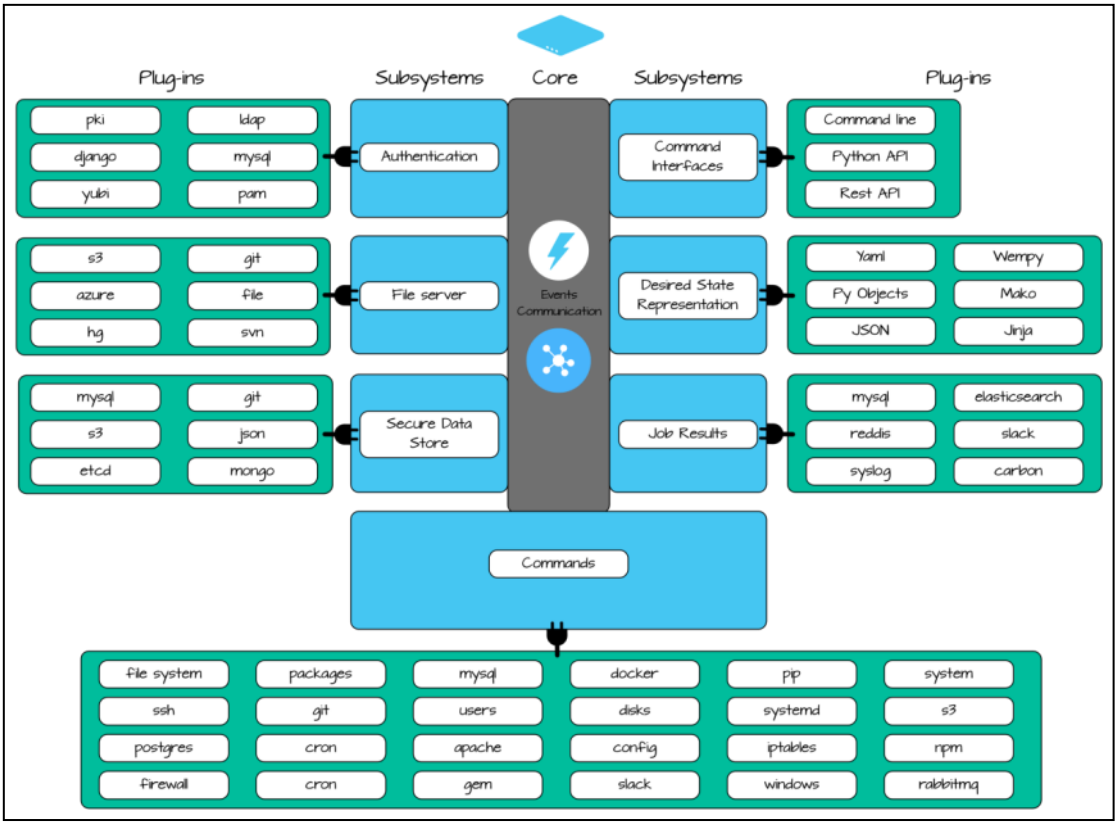
Τα modules που εκτελούνται στον server ονομάζονται runners και είναι υποστηρικτικά. Τα salt runners κάνουν reporting jobs και διαβάζουν δεδομένα από APIs τρίτων εφαρμογών.

Με την Saltstack επιτυγχάνεται real time communication.[51] Όλοι οι clients (minions), ενημερώνονται ταυτόχρονα, που σημαίνει ότι ο χρόνος που απαιτείται για να γίνουν update 10 ή 10000 συστήματα είναι περίπου ο ίδιος. Κάθε κόμβος εκτελεί τοπικά τις διεργασίες εφόσον πληροί τις προϋποθέσεις . Δύο από τα χαρακτηριστικά της Saltstack είναι το scalability και το normalization. Η εκτέλεση των διαφόρων εντολών γίνονται ανεξαρτήτως του λειτουργικού και πάντα υπάρχει ένα “return” σε καθορισμένη δομή για ευκολία ανάγνωσης και αποθήκευσης. **Εικόνα 26**

Η Saltstack χαρακτηρίζεται από τα πολλά Plug ins και τη μεγάλη ευελιξία της αφού δεν έχει σε πολλές περιπτώσεις built-in διαδικασίες και μεθόδους για την εκτέλεση ενός task από τα υποσυστήματα. Υπάρχουν τουλάχιστον 20 pluggable υποσυστήματα. **Εικόνα 27**



Εικόνα 26: Subsystems during a job run



Εικόνα 27: Available Subsystems and plug-ins

11.2.4.1 Modules

Κάθε υποσύστημα της Salt είναι ένα python script. Όλα τα modules βρίσκονται στο source στο salt folder και κάθε module είναι ένα .py.

Παραδείγματα

```
- salt.modules.useradd.add(name, uid=None, gid=None, groups=None,
  home=None,
- shell=None, unique=True, system=False, fullname='', roomnumber='',
- workphone='', homephone='', createhome=True, loginclass=None)
```

```
salt '*' user.add fred shell=/bin/zsh
```

```
- a state example that calls user.present:
- user.present:
- name: fred
- shell: /bin/zsh
```

Εικόνα 28: a. Python Module b.run salt command c. yaml calling script

VMware Cloud Module

```
- my-vmware-config:
- driver: vmware
- user: 'DOMAIN\user'
- password: 'verybadpass'
- url: '10.20.30.40'


- vcenter01:
- driver: vmware
- user: 'DOMAIN\user'
- password: 'verybadpass'
- url: 'vcenter01.domain.com'
- protocol: 'https'
- port: 443


- esx01:
- driver: vmware
- user: 'admin'
- password: 'verybadpass'
- url: 'esx01.domain.com'
```

Εικόνα 29: Salt VMware connection

```
- my-minimal-clone:
- provider: vcenter01
- clonefrom: 'Lubuntu 2'
```

Εικόνα 30: Salt VM clone

11.2.5 Σύγκριση

Συνοψίζοντας τα παραπάνω μπορούμε να παρατηρήσουμε μερικές από τις διαφορές στα προαναφερθέντα εργαλεία. **Πίνακας 4**

Η Ansible όπως και η Salt αποτελεί μία εναλλακτική λύση ως configuration management system χωρίς όμως να χρησιμοποιεί agents. Οι βασικοί λόγοι που στηρίξαμε την εργασία στη χρήση της Ansible, ήταν η χρήση της python, το clientless μοντέλο και η μεγάλη υποστήριξη στο github (44k αστέρια). [54]

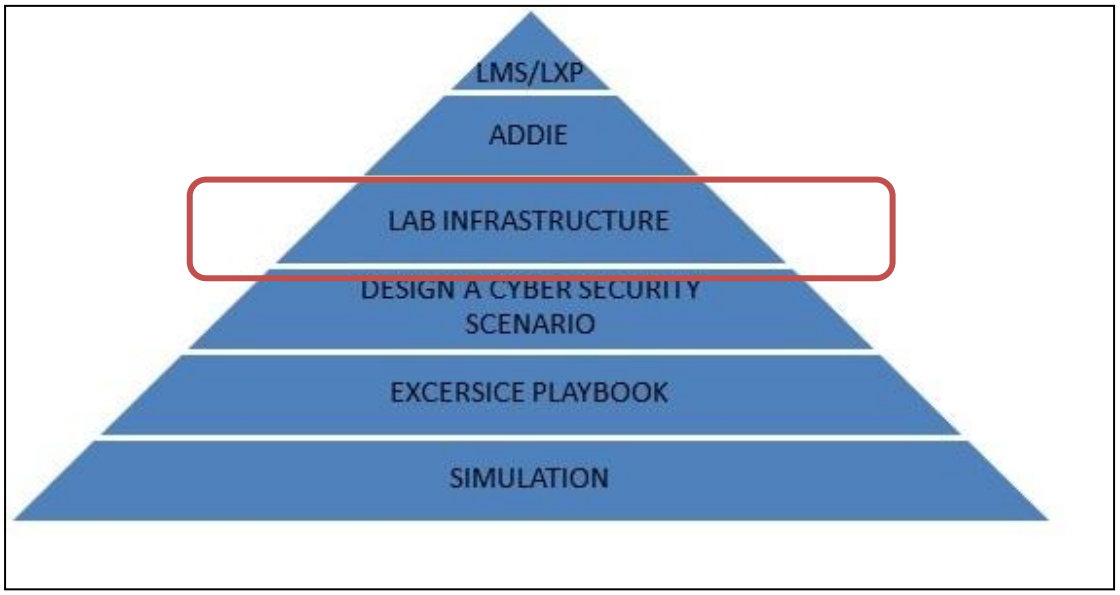
Πίνακας 4. Σύγκριση μεταξύ εργαλείων

Metrics	Ansible	Chef	Puppet	Saltstack
Programming Language	Python	Ruby, Erlang	C++, Clojure	Python
Configuration Language	YAML/JSON	Ruby	Propietary	YAML(Python)
Database	N/A	PostgreSQL	PuppetDB	N/A
Scalability	High	High	High	High
Deployment	push	pull	pull	push
Architecture	server	Server/client	Server/client	Server/client
Enterprise GUI	Ansible Tower	Opscode Manager	Puppet Enterprise	Saltstack Enterprise
Opensource GUI	Semaphore	Chef Manager	Foreman	Saltpad,Saltshaker
Github Stars	44K	6.3K	5.8K	11.1K

12. ΔΟΜΗ ΕΡΓΑΣΤΗΡΙΟΥ

Μια ολοκληρωμένη διαλειτουργικότητα των όσων περιγράφονται στην εργασία, μπορεί να αναλυθεί στο παρακάτω διάγραμμα. Σε μία εκπαιδευτική πλατφόρμα, μπορεί να στηριχτεί η κατάρτιση ενός εκπαιδευτικού μοντέλου, με τη δημιουργία ενός testbed περιβάλλοντος, στο οποίο εκπαιδευτής και εκπαιδευόμενος θα αλληλεπιδρούν με τα ενεργά στοιχεία της τοπολογίας, για την εκτέλεση ασκήσεων κυβερνοασφάλειας. Ο χρήστης θα μπορεί να επιλέξει μέσα από μία γκάμα έτοιμων ασκήσεων, οι οποίες θα μπορεί να μεταβληθούν και κατά το δωκούν, και φυσικά να αξιολογηθεί για το αποτέλεσμα αυτών. **Εικόνα 31**

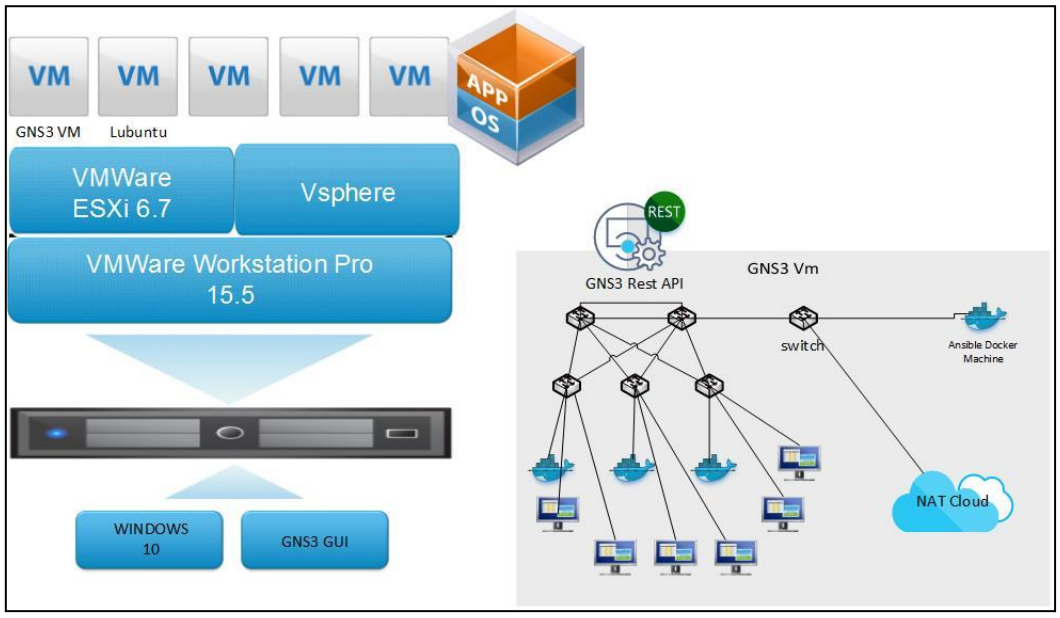
Στην εργασία μας θα ασχοληθούμε με την υποδομή που θα χρειαστεί ενά τέτοιο περιβάλλον, το lab infrastructure, ενώ τα υπόλοιπα είναι εκτός του στόχου μας, αλλά κρίθηκε απαραίτητο να αναφερθούν ώστε να πλαισιώσουν την άσκηση και να δώσουν στον αναγνώστη μία πιο σφαιρική εικόνα της ανάγκης υλοποίησης της και τη συνολική κατανόηση της χρησιμότητας της. Στο κεφάλαιο 13, ακολουθεί μία περιγραφή της συνολικής ιδέας.



Εικόνα 31. Συνολική υλοποίηση εργαστηριακού περιβάλλοντος

Για την υλοποίηση του πρακτικού μέρους της εργασίας χρείαστηκε να φτιάξουμε ένα test environment, ώστε να αποδείξουμε την ορθή λειτουργία μίας τέτοιας διάταξης και να διαπιστώσουμε τις απαιτήσεις, τις λειτουργίες και τις δυσκολίες που μπορεί να συναντήσει κανείς κατά τη δημιουργία.

Επιλέξαμε να δουλέψουμε με τον συνδυασμό των VM workstation Pro, VMware Esxi 6.7, Vsphere 6.7, GNS3, την Ansible ως automation tool, Ubuntu dockers και τα cisco switches τρέχουν cisco ViOS. Επίσης χρησιμοποιήσουμε ως test VM το Lubuntu δεδομένου, ότι διατείθεται σε lite έκδοση, κάτι το οποίο για την περίπτωσή μας ήταν αρκετό και ένα Kali Linux. **Εικόνα 33**



Εικόνα 33: Τοπολογία εργαστηρίου

Συνοπτικά θα περιγράψουμε την αρχική ιδέα του εργαστηρίου και τις δυνατότητες που δίνονται στο χρήστη καθώς και τη συμμετοχή του εκπαιδευτή κατά τη διάρκεια της άσκησης. **Πίνακας 5**

Πίνακας 5. Περιγραφή εργαστηριακής άσκησης

Εργαστήριο		
Α/Α	**ΒΗΜΑΤΑ**	**ΠΕΡΙΓΡΑΦΗ**
1	Start lab	Διαδικασία δημιουργίας εργαστηρίου: Τα labs δεν τρέχουν μόνιμα, αλλά όταν γίνουν start παίρνουν τα απαραίτητα resources από τον hypervisor στο GNS3 VM. Ο Ansible server δημιουργεί τους nodes και την τοπολογία, με ip, vlans χρησιμοποιώντας templates. Κάνει add έναν router που να σηκώνει έναν vpn server ώστε να μπορούν να συνδεθούν οι χρήστες.(optional). Ο χρήστης είναι συνδεδεμένος στην τοπολογία και έχει connectivity με όλα τα στοιχεία του δικτύου, nodes, VMs, hypervisor. Ο εκπαιδευτής μπορεί να παρέμβει και να κάνει οποιαδήποτε αλλαγή όπως να μετονομάσει κάποιο στοιχείο, να φτιάξει κλώνους, να δημιουργήσει κόμβους ή και να διαγράψει switches, VPCs, ή και VMs.
2	Resource allocation (not always run)	
3	Ansible server creates topology, nodes	
4	Lan, hosts, assign vlans (using templates)	
5	Add new router, node, running vpn to connect to virtual environment	

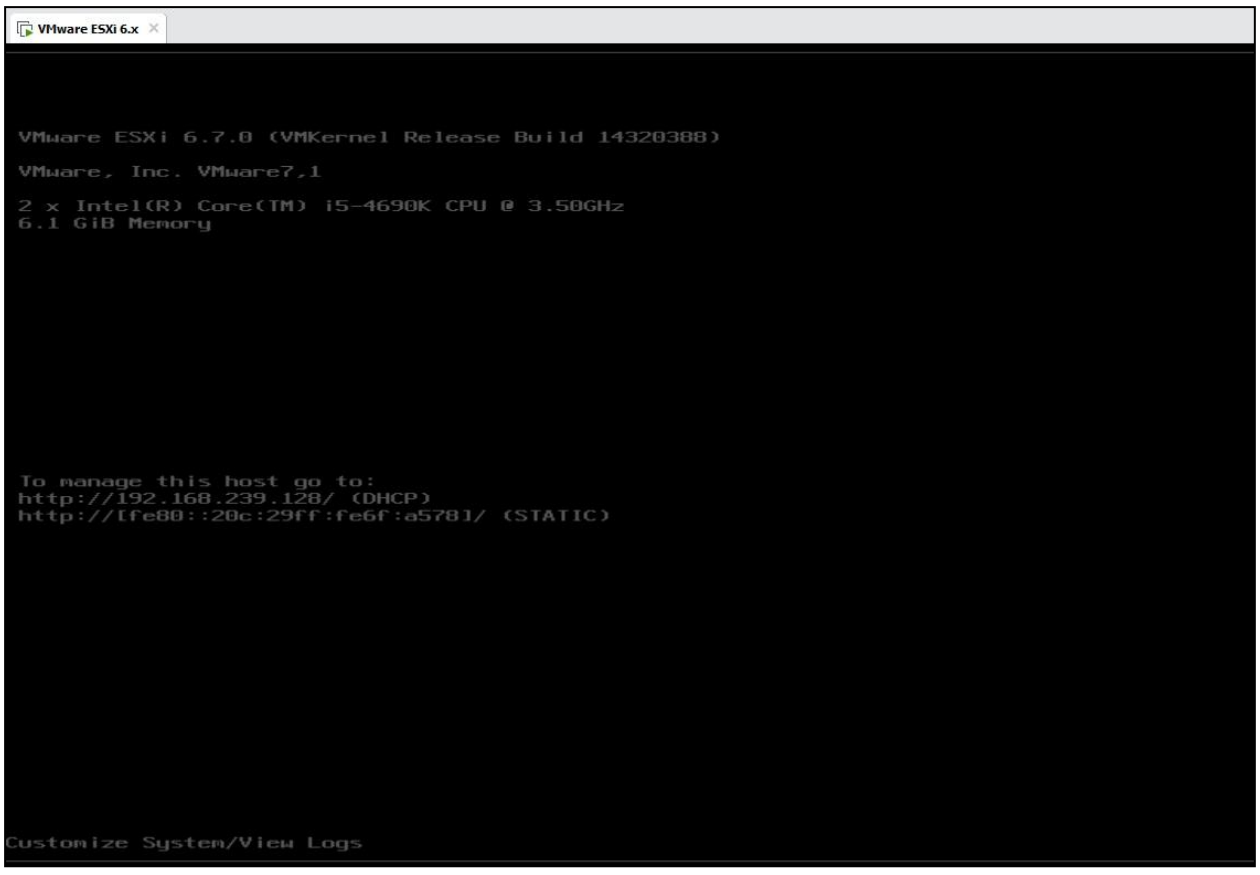
6	User connected to the net topology	
7	Trainer can interact with the eniv (copy, rename, delete, create)	

12.1 Περιγραφή εργαστηρίου

Ως βάση χρησιμοποιήθηκε ένας windows 10 host στον οποίο στήθηκε ένα VMware workstation Pro. Εκεί θα παίξουν ο hypervisor esxi 6.7 και το Vcenter για τη διαχείριση του esxi και των VMs. Εδώ να τονίσουμε ότι προφανώς για μία τέτοιου μεγέθους υλοποίηση δε θα χρειαζόταν Vcenter για τη διαχείριση των στοιχείων, αποδείχτηκε όμως ότι είναι απαραίτητος για τη συνεργασία με την Ansible και τα δοκιμαστικά Playbooks που τρέξαμε.

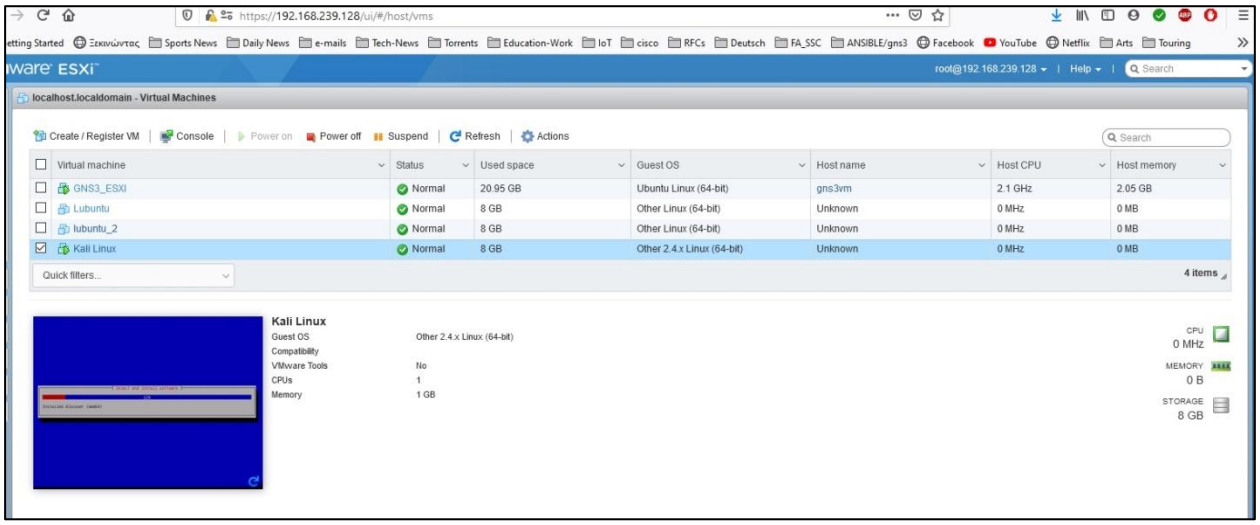
Windows Host: window 10 pro, i5-4690K, hd 1TB, 16gb RAM dd3 3200MHz

Από το download center του VMWare κατεβάσαμε το 6.7 esxi και κάναμε import το ISO στο workstation. (4gb ram min requirement και nested virtualization enabled). **Εικόνα 34**



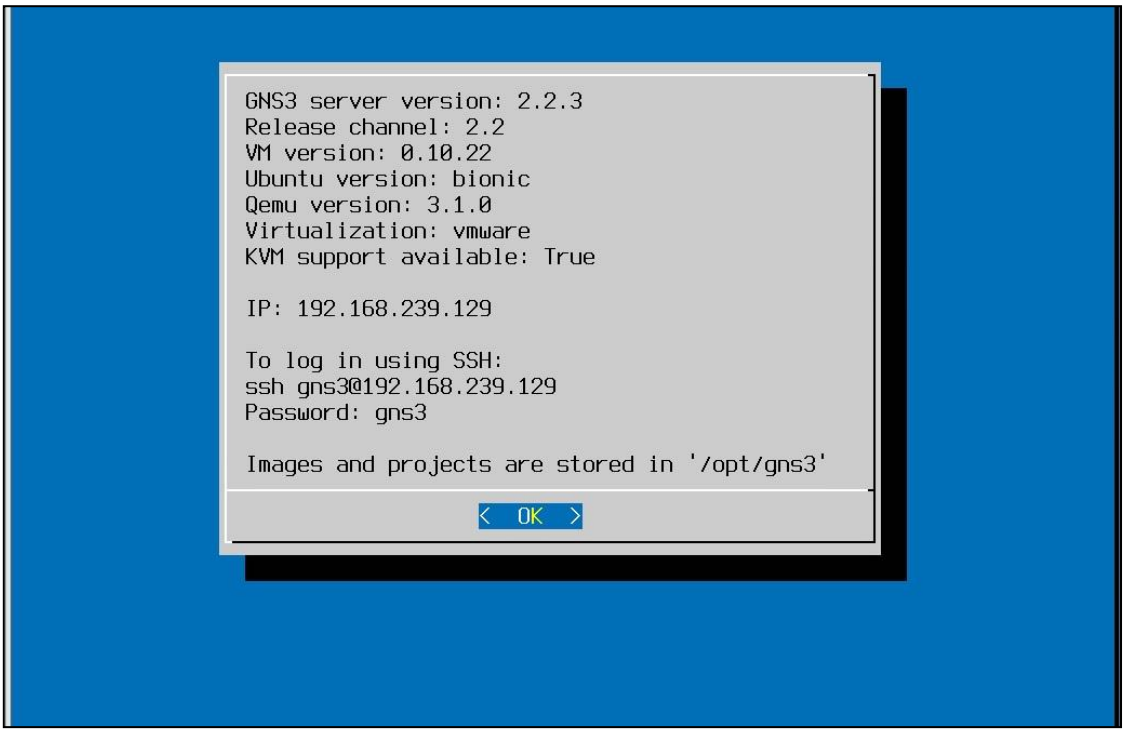
Εικόνα 34: Workstation 15.5 hosting VMEsxi

Πάνω στον esxi θα στήσουμε το VM του GNS3 και όσα λειτουργικά θα χρειαστούν. Για την παρούσα εργασία έχουμε ένα lightweight Lubuntu και ένα Kali Linux. Μπορούμε να τα δούμε και να τα διαχειριστούμε μέσα από το web interface του esxi *(https://192.168.239.128/ui/#/login),* ή από το web interface του Vcenter που θα παρουσιάσουμε παρακάτω. **Εικόνα 35**



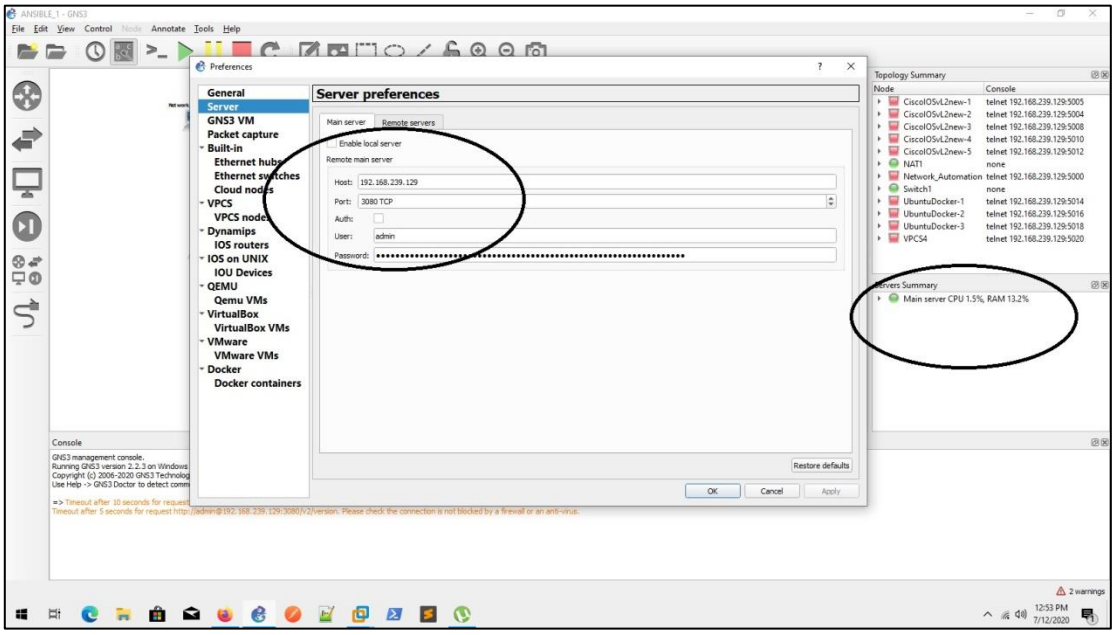
Εικόνα 35: Esxi web Interface

Το VM του GNS3 **Εικόνα 36,** θα το χρησιμοποιήσουμε ως server για τον local agent του gns, ώστε τα resources που θα χρησιμοποιεί να είναι από τον hypervisor.



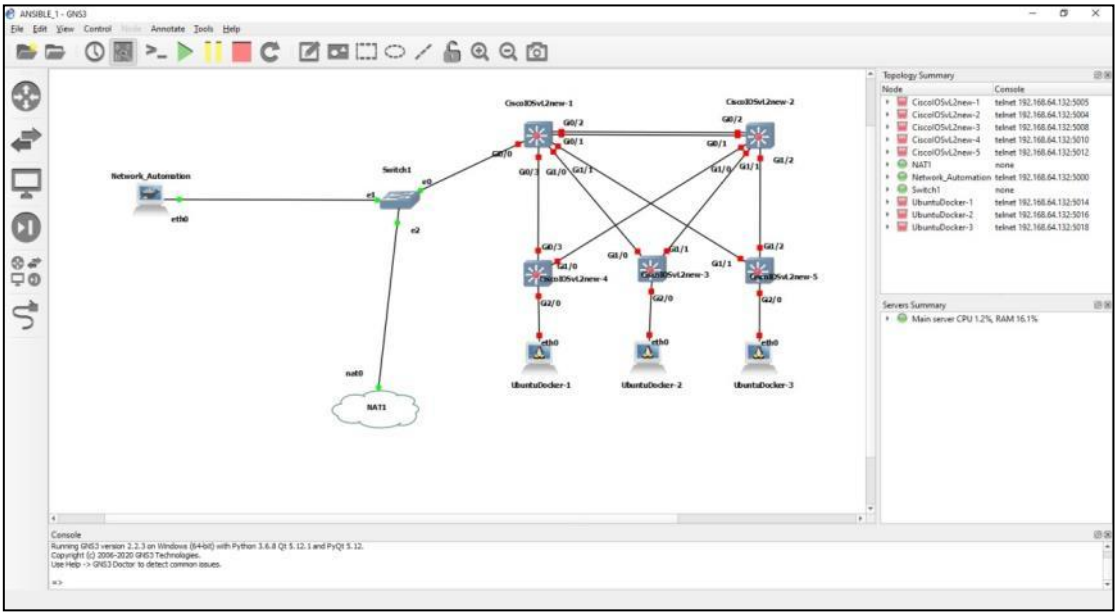
Εικόνα 36: GNS3 VM running on ESXi

Στην περίπτωσή μας είναι το ίδιο machine, αλλά στην περίπτωση ενός πραγματικού εργαστηρίου, θέλουμε τα απαραίτητα resources να τα παίρνει από την υποδομή μας και όχι από τον κάθε agent που θα τρέχει τοπικά τον gns3 client. **Εικόνα 37**



Εικόνα 37: Ρυθμίσεις client για τον remote server

Στην παραπάνω εικόνα βλέπουμε μία τυπική τοπολογία μέσα στο GNS3. **Εικόνα 38**



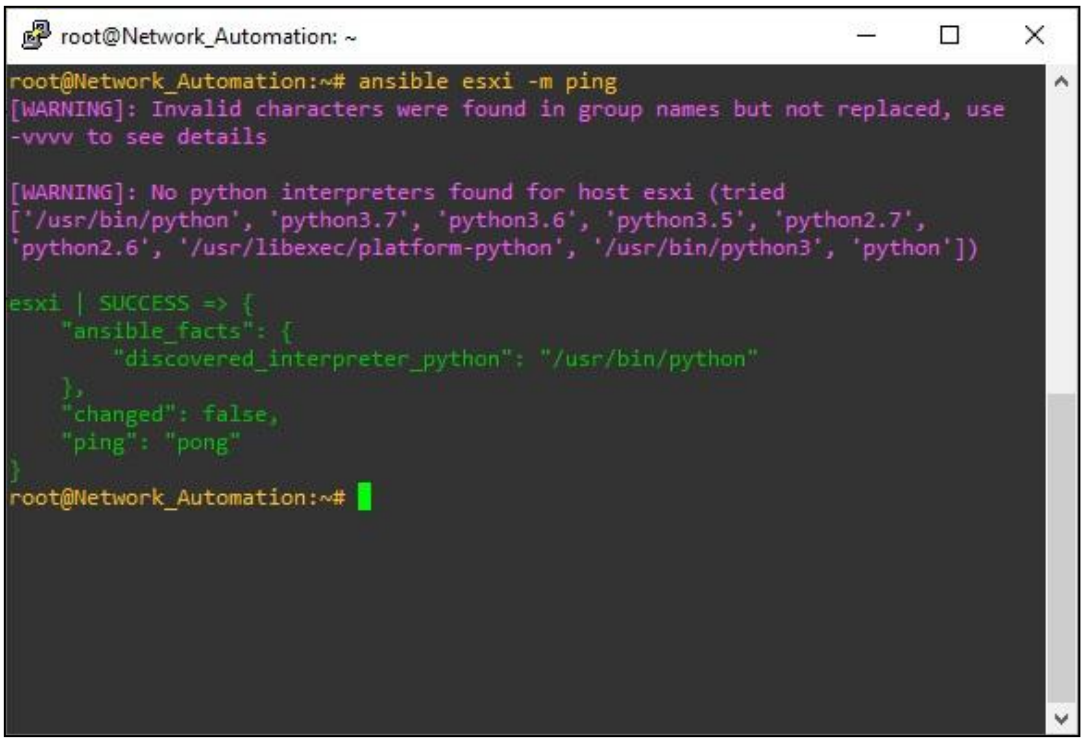
Εικόνα 38: GNS3 GUI

Για τις ανάγκες της εργασίας στήσαμε έναν ansible server μέσα στην τοπολογία μας ο οποίος έχει επικοινωνία με τα στοιχεία του δικτύου στο gns3, switches, pcs κλπ, αλλά και με τον esxi, το vcenter και τα VMs. Για το αρχικό setup ακολουθήσαμε τα βήματα που φαίνονται στον παρακάτω πίνακα για την εγκατάσταση της Ansible και την επικοινωνία με τον esxi. **Πίνακας 6**

Πίνακας 6. Εγκατάσταση της Ansible

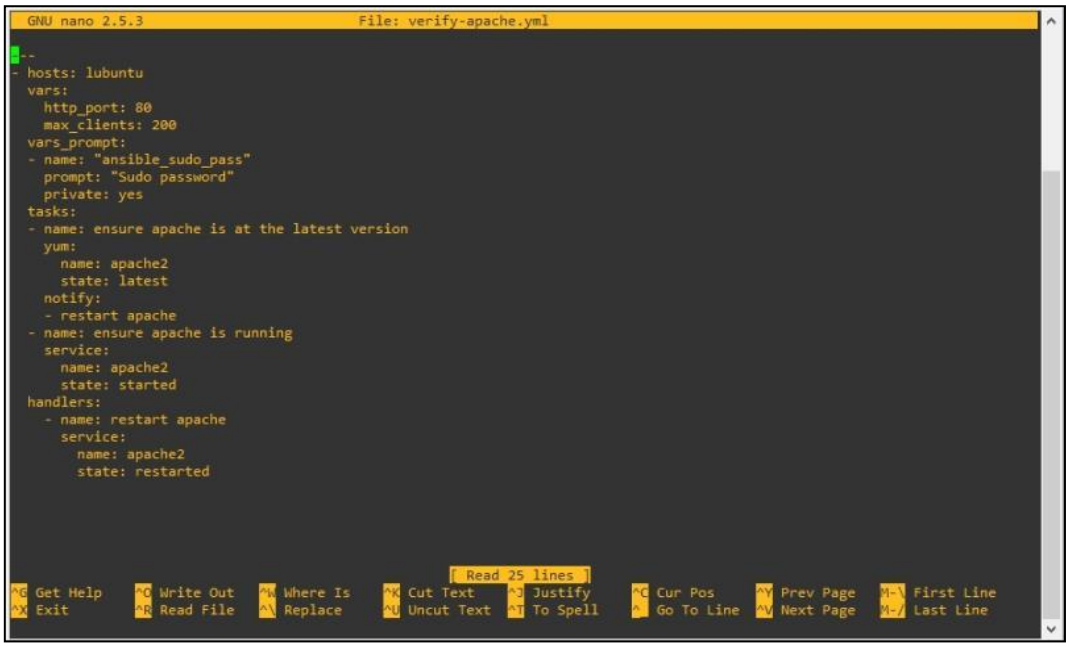
Ansible persistent docker machine PC μέσα στο GNS3		
Α/Α	**ΒΗΜΑΤΑ**	**ΠΕΡΙΓΡΑΦΗ**
1	install ansible	Για τις δοκιμές μας στήσαμε έναν ansible server μέσα στο gns3 πάνω σε ένα ubuntu persistent docker PC. Συνοπτικά βλέπουμε τα βήματα που ακολουθήσαμε για το installation και τη σύνδεση με τον esxi
2	create host file with esxi ip	
3	create new ansible.cfg	
4	establish ssh connection with esxi	
5	create ssh key	
6	ssh-keygen	
7	#copy to the server	

Μετά την εγκατάσταση του Ansible server δοκιμάζουμε επιτυχώς το ping με τον esxi. Να υπενθυμίσουμε ότι για να επιτύχει το ping έχουμε βάλει τον esxi στο αρχείο host και έχει στηθεί το ssh, **Εικόνα 39**



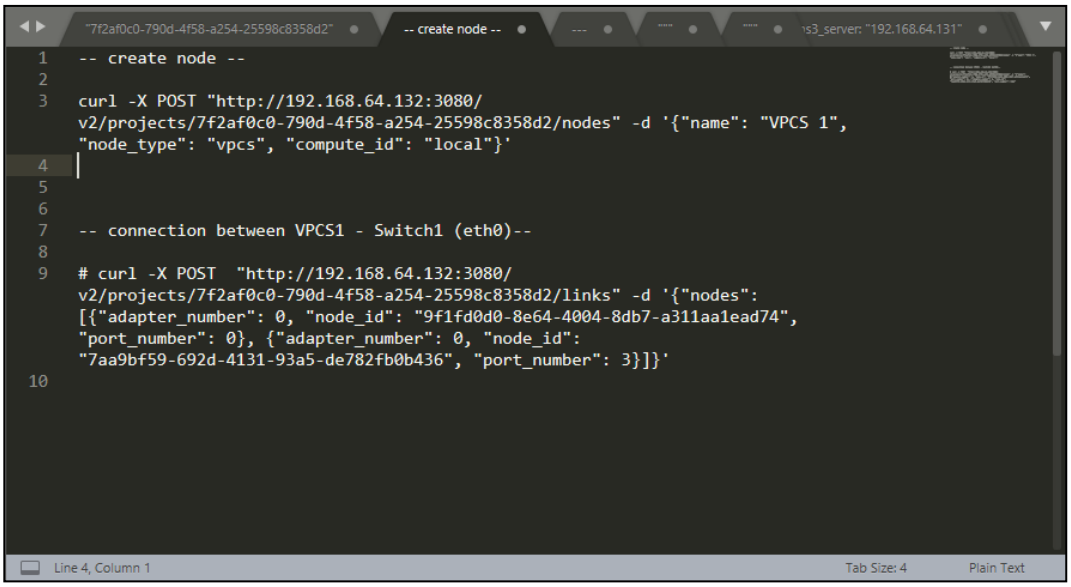
Εικόνα 39: Έλεγχος επικοινωνίας του Ansible server με τον esxi

Δοκιμάζουμε ότι υπάρχει επικοινωνία και με ένα από τα VMs, τρέχοντας ένα playbook [60] το οποίο βλέπει αν υπάρχει εγκατεστημένος apache στον host. **Εικόνα 40**



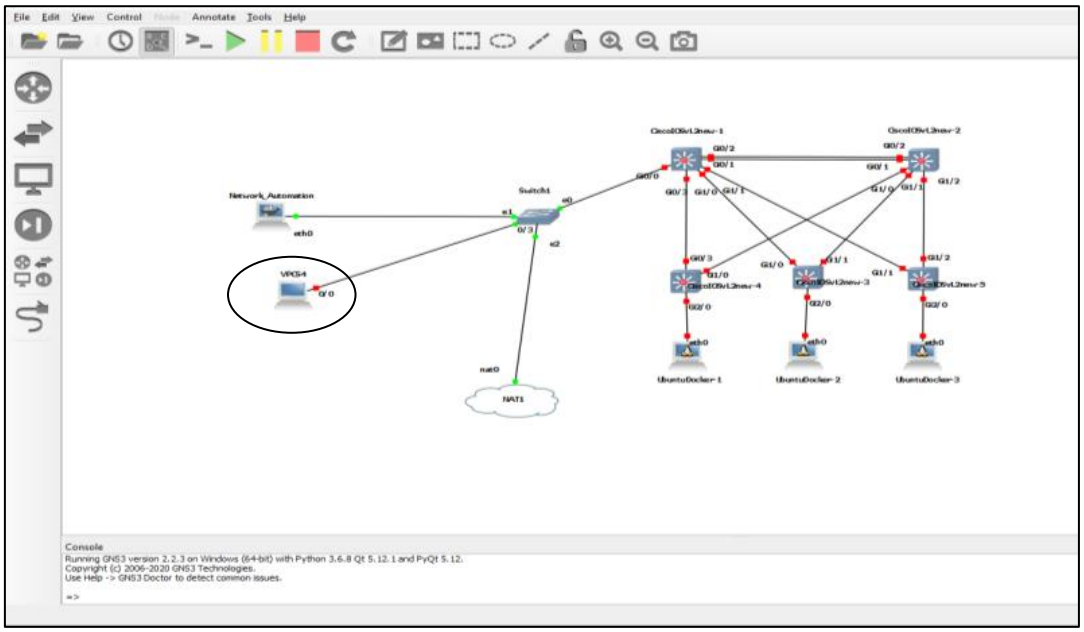
Εικόνα 40: Ansible Test Playbook. Ensure service running on a VM.

Στη συνέχεια θα δοκιμάσουμε να «μιλήσουμε» από τον ansible server με τον VM του GNS3 και μέσω POST και GET [61] εντολών να δημιουργήσουμε κόμβους πάνω στην τοπολογία μας. **Εικόνα 41**



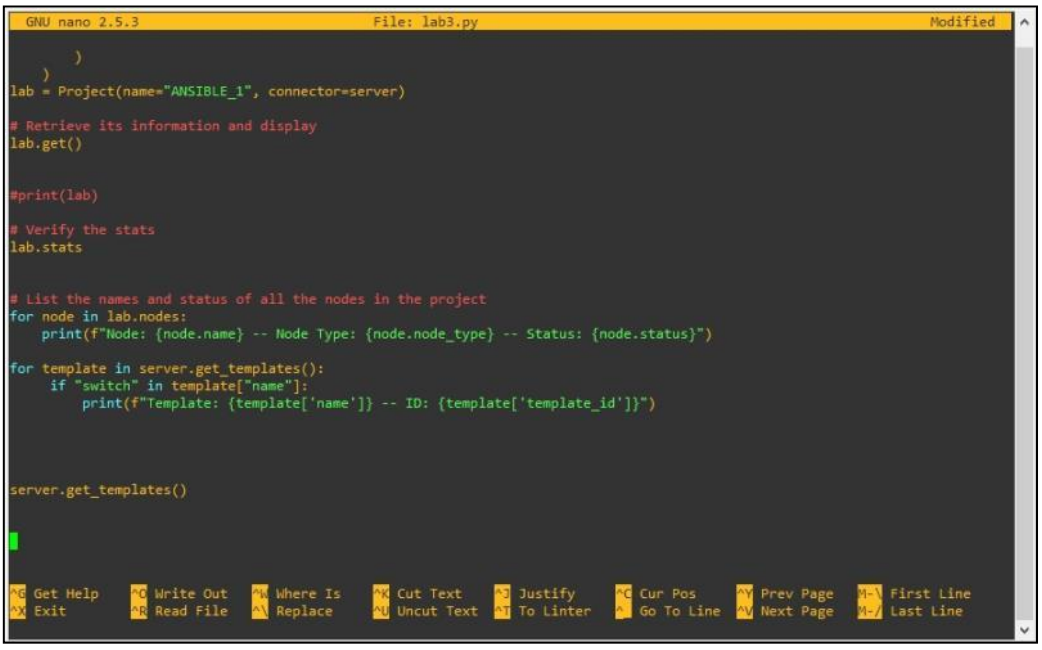
Εικόνα 41: Curl (post/get) στο VM του GNS3

Στο παραπάνω script φτιάξαμε έναν νέο κόμβο (vPC) και το συνδέσαμε με το switch1. Το αποτέλεσμα του script φαίνεται στο παρακάτω σχήμα. **Εικόνα 42**



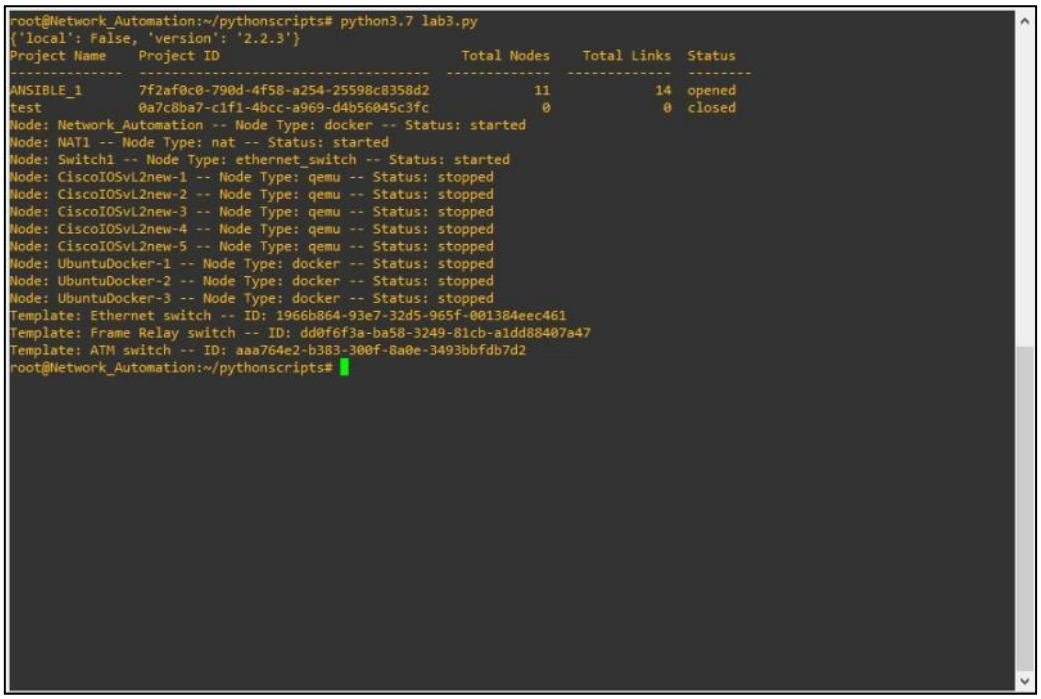
Εικόνα 42: Δημιουργία νέου node μέσα από το API του GNS

Στην επόμενη εικόνα μπορούμε να δούμε ότι και με τη χρήση της python, μπορούμε να δούμε το δίκτυο μας και να επέμβουμε ή να πάρουμε πληροφορίες από αυτήν. **Εικόνα 43**



Εικόνα 43: Python script lab3.py

Παρατηρούμε ότι μπορούμε να έχουμε εικόνα των ανοιχτών projects στο GNS3 και το status των κόμβων, ποιοι είναι started και ποιοι είναι down. **Εικόνα 44**

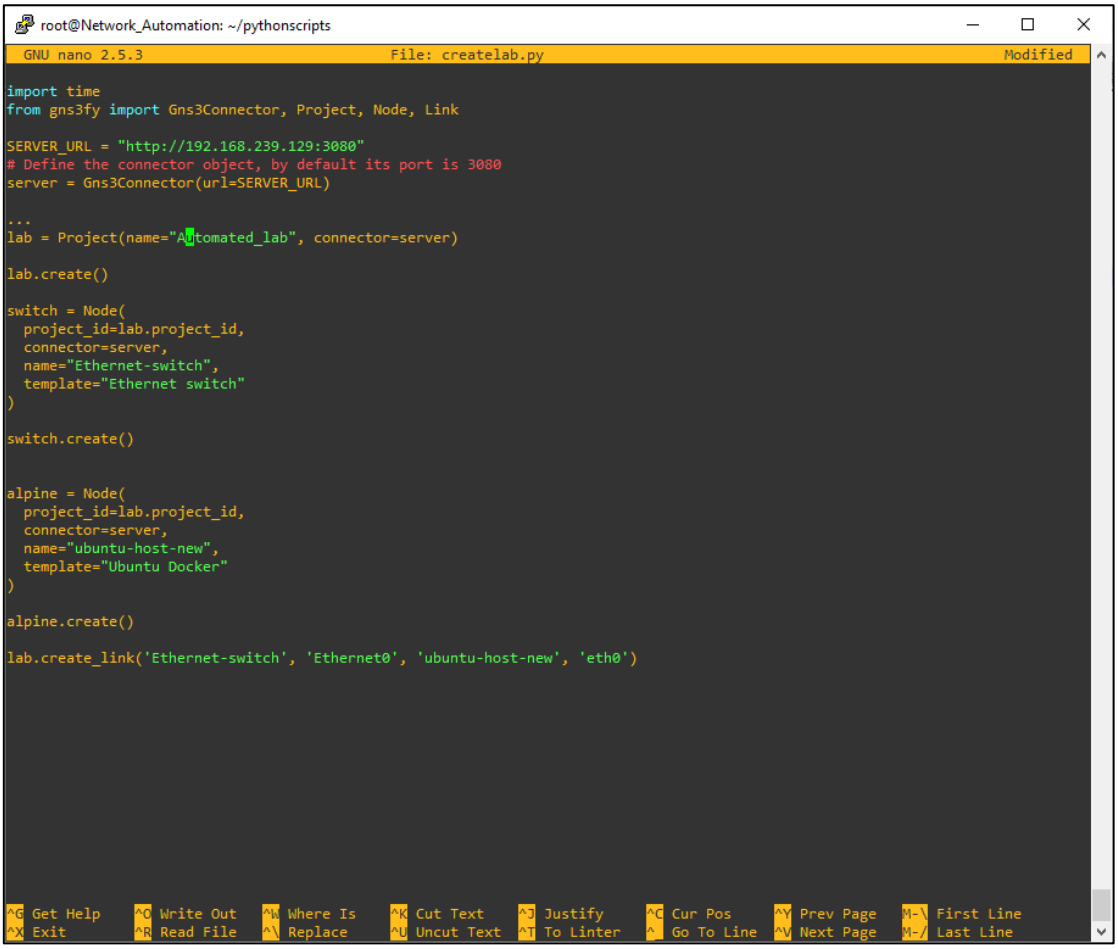


Εικόνα 44: Python script lab3.py

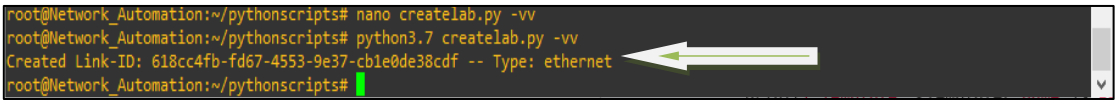
Παρακάτω θα προσπαθήσουμε με ένα από τα modules της python να συνδυάσουμε τις απεριόριστες δυνατότητες της με rest commands του API του GNS3.

```
pip install gns3fy
```

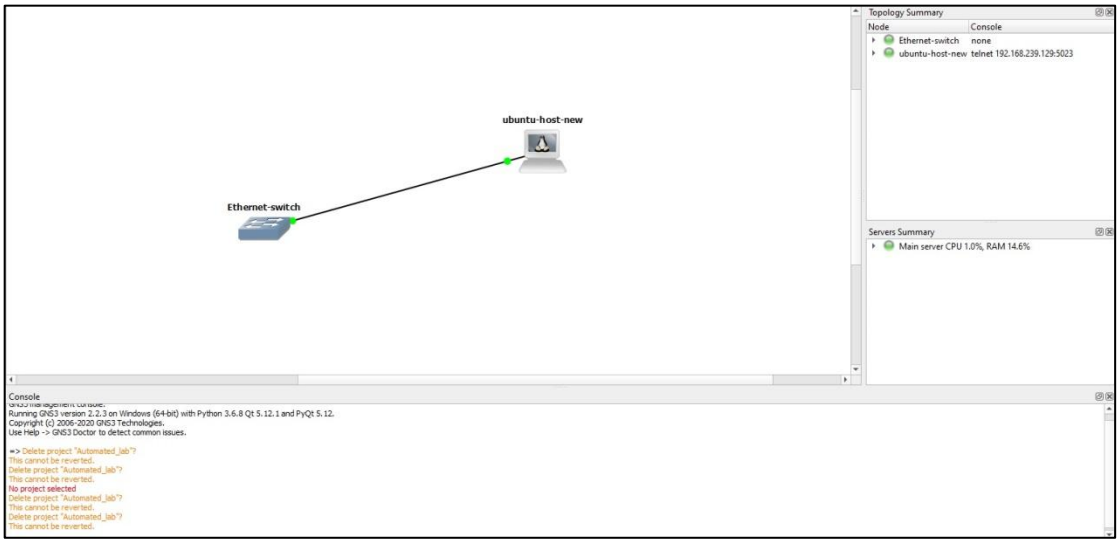
Με τη χρήση του gns3fy [63] το οποίο είναι ένα wrapper του GNS3 API μπορούμε να αλληλεπιδρούμε με το σύστημα με έναν πιο προγραμματιστικό τρόπο. Μπορεί να γίνει Intergrated με ansible σενάρια και μας διευκολύνει καθώς χρησιμοποιώντας τις μεταβλητές xxxx_id, μπορούμε σειριακά να δημιουργήσουμε ένα ολόκληρο Lab. Ενδεικτικά όπως και παραπάνω με τη χρήση του gns3 API δημιουργήσαμε ένα project με ένα Ubuntu docker και ένα Ethernet switch. **Εικόνα 45** Τα IDs αντιστοιχούν από κάθε στοιχείο της τοπολογίας και τα χρησιμοποιεί η REST ως αναγνωριστικό, μέχρι και το ίδιο το project. Έτσι σειριακά μπορούμε να δημιουργήσουμε όποιο κόμβο θέλουμε από τους εγκατεστημένους στο inventory του GNS3.



Εικόνα 45: Δημιουργία Project με 2 nodes από templates (Ubuntu-docker και eth switch)



Εικόνα 46. Εκτέλεση του py script



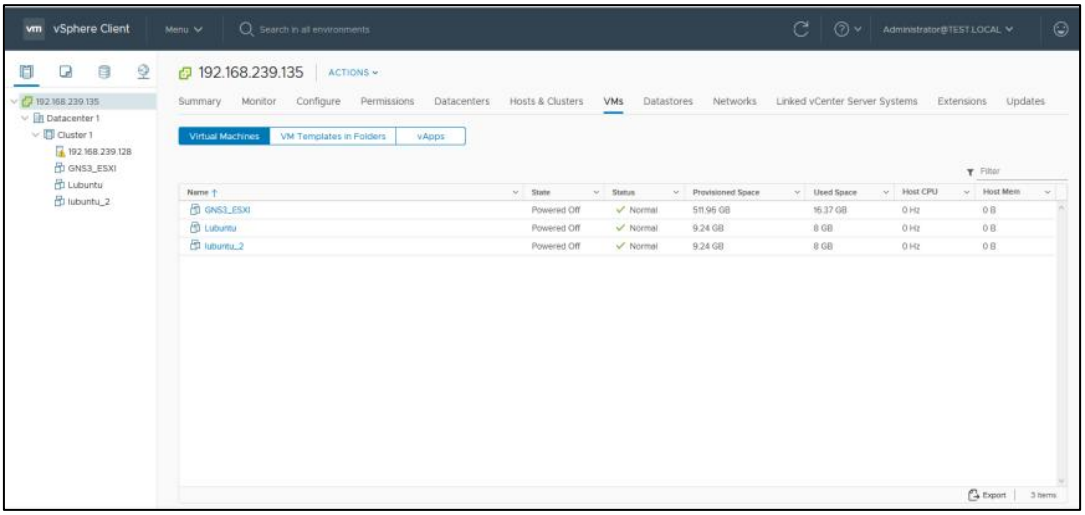
Εικόνα 47: Δημιουργία ενός κόμβου συνδεδεμένου με ένα switch

Επίσης στο setup της **Εικόνα 42** έχουμε τη δυνατότητα να παραμετροποιήσουμε, τα στοιχεία του δικτύου της τοπολογίας. Για την εργασία απαιτούνται τα modules "**ios_command**" και "**ios_config**". **Εικόνα 48**

```
--- # Cisco IOS managment
- hosts: CISCO_SWITCH1
  connection: local
  gather_facts: no
  vars:
    cli:
      host: CISCO_SWITCH1
      username: admin
      password: cisco
      transport: cli
  tasks:
    - name: run show run
      ios_command:
        provider: "{{ cli }}"
        commands: show run
      register: showrun
    - debug: var=showrun
    - name: set loopback interface
      ios_config:
        provider: "{{ cli }}"
        authorize: yes
        parents: interface loopback0
        lines:
          - description test loopback interface
          - ip address xxx.xxx.xxx.xxx 255.255.255.255
```

Εικόνα 48. Εισαγωγή Configuration σε κόμβο της τοπολογίας.

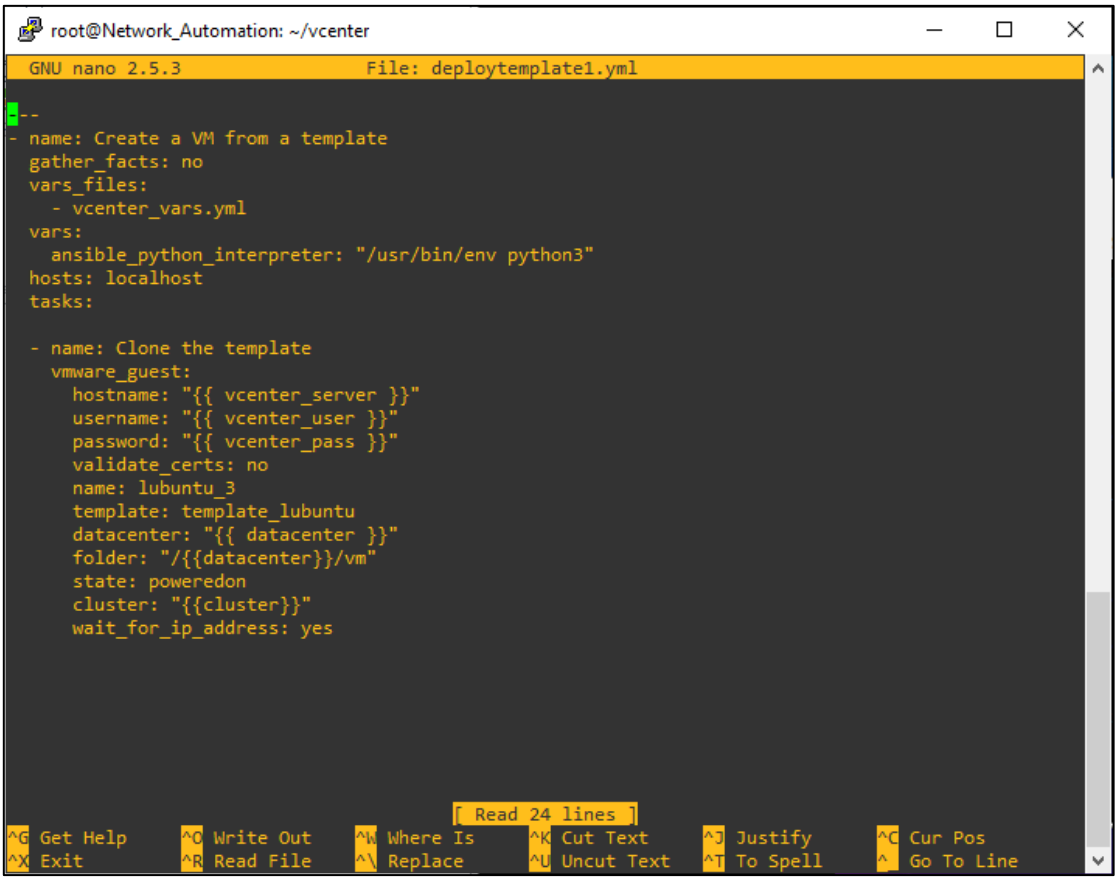
Όπως έχουμε αναφέρει παραπάνω για τη διασύνδεση της Ansible με το Hypervisor χρειάστηκε να στήσουμε ένα Vsphere για τη διαχείριση του esxi και των VMs. Μας βοήθησε γιατί μας δίνει τη δυνατότητα να διαχειριζόμαστε τα VMs, να δημιουργούμε templates και clones, τα οποία αποθηκεύονται στο datastore του esxi και θα τα χρησιμοποιήσουμε για τα δοκιμαστικά playbooks. **Εικόνα 49**



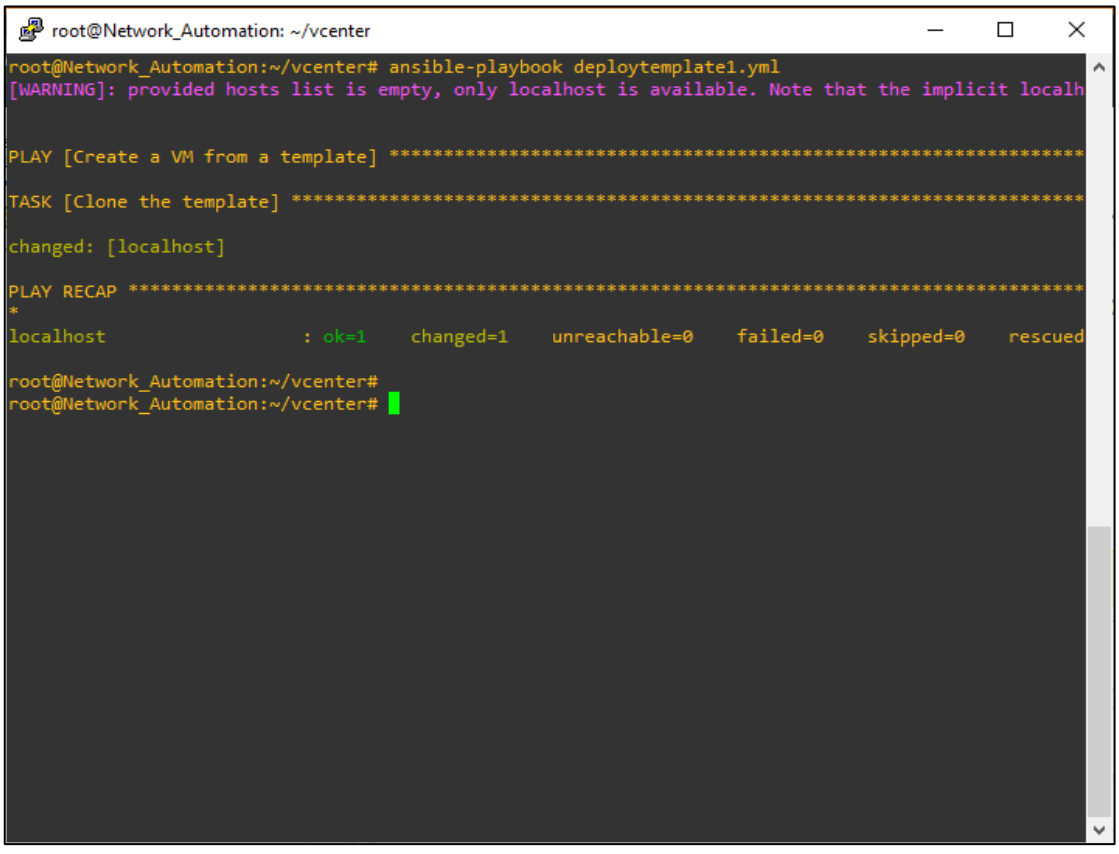
Εικόνα 49: VCSA managing ESXi and VMs

Στη συνέχεια θα τρέξουμε δύο playbooks, ένα για να δημιουργήσουμε ένα νέο VM στον esxi, με τη χρήση template, το οποίο μπορεί να δημιουργήσει κανείς μέσα από το UI του vcenter από ήδη στημένο VM. **Εικόνα 50.** Το template είναι ένα Master copy ενός VM το οποίο μπορεί να χρησιμοποιηθεί για να φτιάξουμε πολλούς κλώνους αυτού. Ο κλώνος περιέχει ακριβώς τα ίδια χαρακτηριστικά με το αρχικό και μπορεί να παραχθεί πολλές φορές, το οποίο μπορεί να γλιτώσει από τον χρήστη πολύ χρόνο, αφού φτιάχνει μία φορά το setup που επιθυμεί και το αντιγράφει όσες φορές θέλει. Παράλληλα είναι

ένα ανεξάρτητο VM, αφού μπορεί να έχει διαφορετικές δικτυακές ρυθμίσεις καθώς επίσης οι αλλαγές στο αρχικό δε συμβαίνουν και σε αυτό.

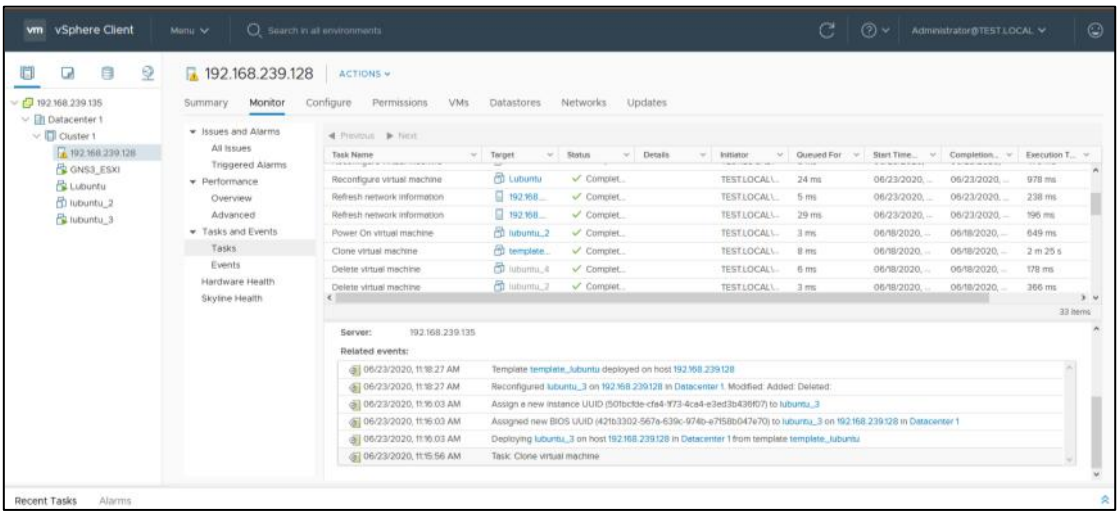


Εικόνα 50: Playbook για τη δημιουργία VM από template (clone)



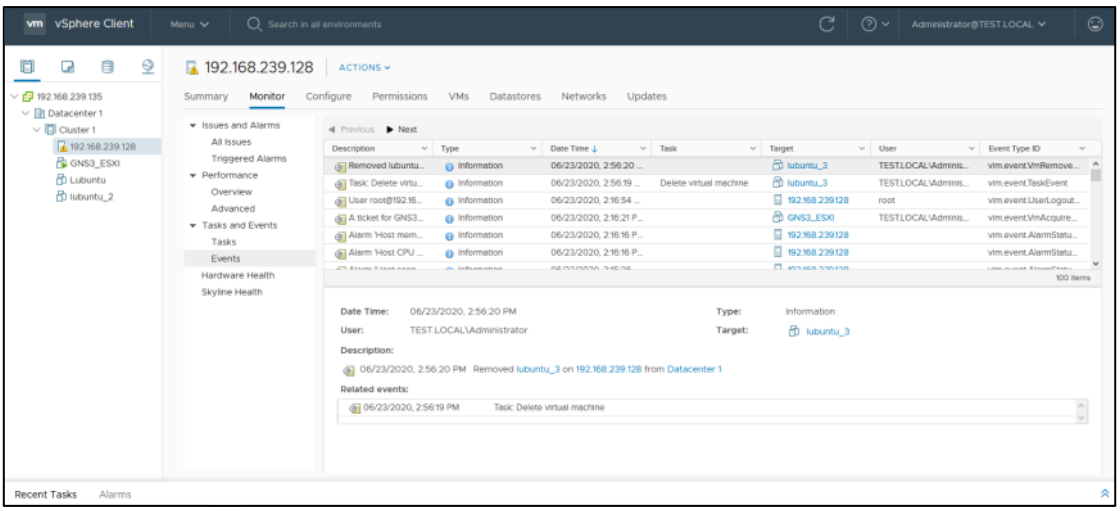
Εικόνα 51: Running ansible-playbook το οποίο δημιουργεί ένα VM από template

Τρέχουμε το playbook **Εικόνα 51** και παράλληλα μπορούμε να δούμε την εξέλιξη της διαδικασίας και μέσα στο interface του VCSA. **Εικόνα 52**

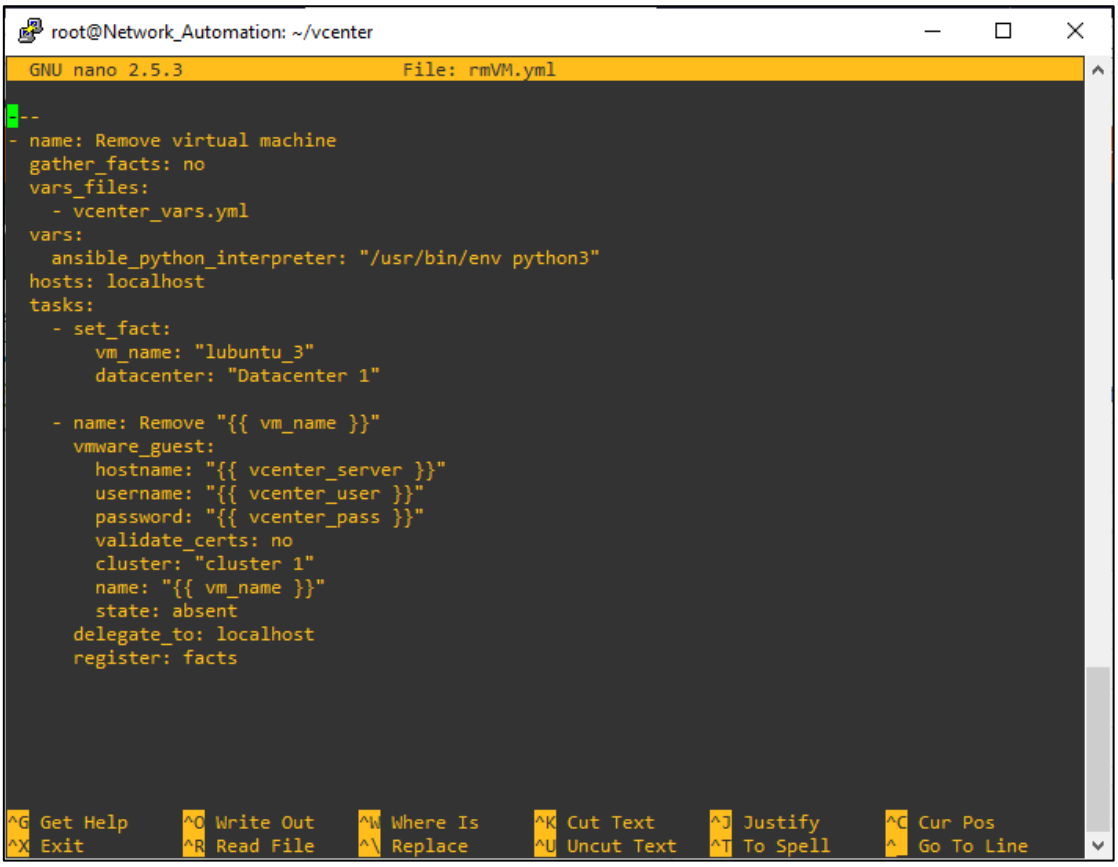


Εικόνα 52: Δημιουργία template από running VM

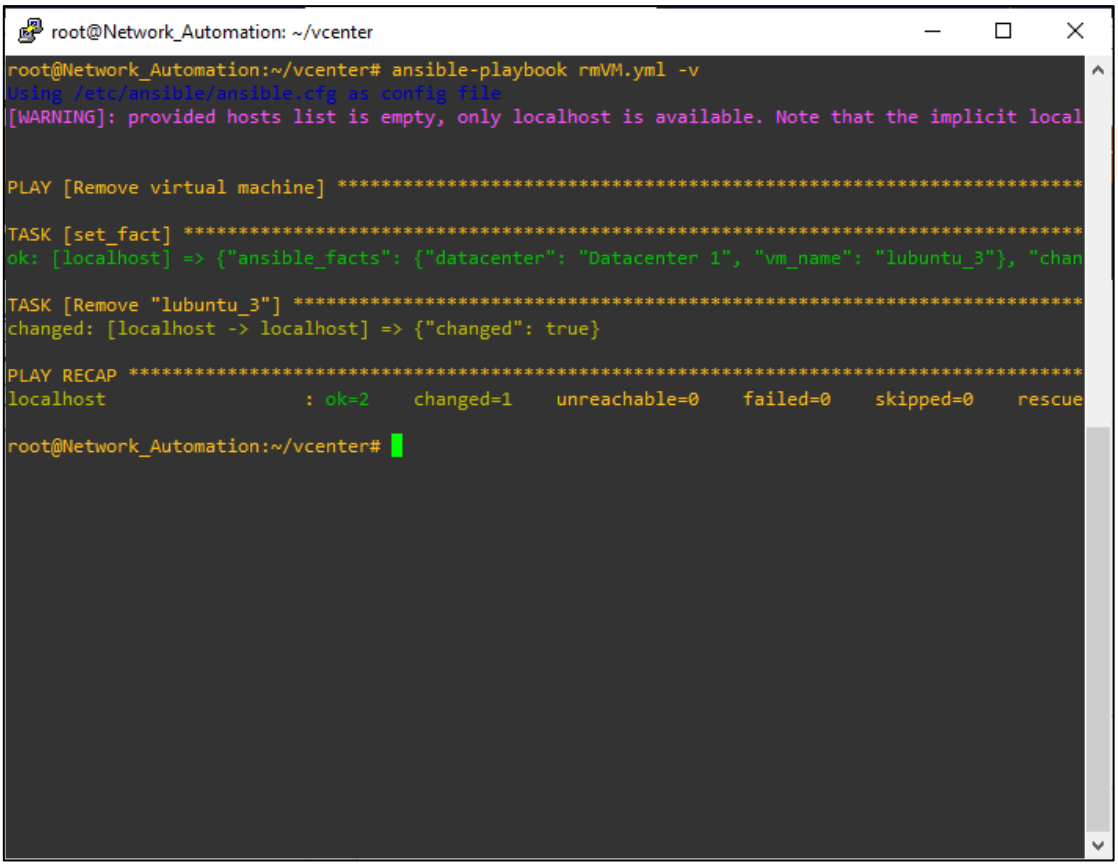
Αντίστοιχη διαδικασία cloning βλέπουμε και παρακάτω όπου θα κάνουμε το ίδιο, τρέχοντας το Playbook που θα μας διαγράψει το Lubuntu 3 κλώνο.**Εικόνα 54**



Εικόνα 53: Διαγραφή του VM Lubuntu 3



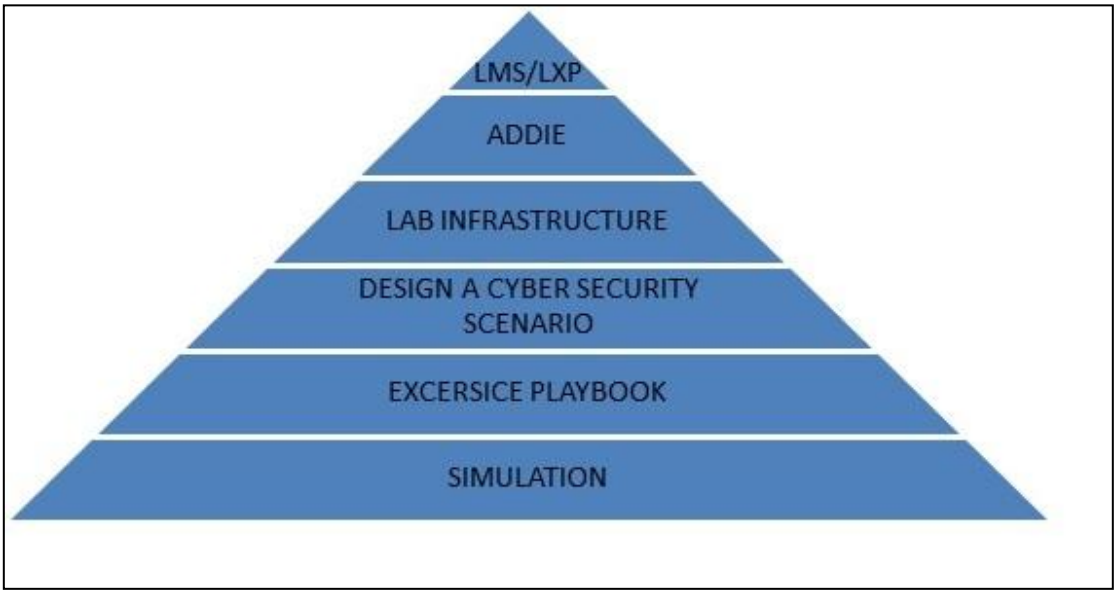
Εικόνα 54: Ansible-playbook με το οποίο διαγράφεται το VM από τον esxi



Εικόνα 55: Διαγραφή του Lubuntu 3

13. ΠΑΡΑΔΕΙΓΜΑ ΥΛΟΠΟΙΗΣΗΣ ΜΙΑΣ ΠΡΟΣΟΜΟΙΩΣΗΣ ΠΑΝΩ ΣΕ ΕΝΑ LMS

Όπως είδαμε στο κεφάλαιο 12, η υποδομή που φτιάξαμε στα πλαίσια της εργασίας πλαισιώνεται, από την ιδέα μιας συνολικής εφαρμογής της σε μία πλατφόρμα εκπαίδευσης, όπου ο χρήστης θα έχει τη δυνατότητα να δουλέψει πάνω σε αυτήν, παράλληλα με την εκπαίδευση.



Εικόνα 56. Συνολική υλοποίηση εργαστηριακού περιβάλλοντος

Παρακάτω παραθέτω ένα παράδειγμα υλοποίησης μίας εργαστηριακής προσέγγισης μιας άσκησης από τη στιγμή που ο χρήστης θα κάνει login στην εκπαιδευτική πλατφόρμα. **Πίνακας 7**

Πίνακας 7. Περιγραφή πλατφόρμας προσομοίωσης

Πλατφόρμα Προσομοίωσης		
Α/Α	**ΒΗΜΑΤΑ/**	**ΠΕΡΙΓΡΑΦΗ**
1	Web User Interface	Μία πλατφόρμα προσωμοίωσης, απαιτεί ένα web interface, ώστε οι χρήστες να αποκτήσουν πρόσβαση στο προσφερόμενο περιεχόμενο. Τα δομικά στοιχεία μίας τέτοιας πλατφόρμας είναι ένας course manager που στηρίζει το εκπαιδευτικό υλικό και καθορίζει την εμπειρία του χρήστη. Για τη βελτίωσή της πλαισιώνεται από collaboration tools, τα οποία ο end user θα μπορεί να τρέξει μέσα από την εφαρμογή, όπως skype, slack, instant messsaging,
2	Lms / course manager	
3	Collaboration tools	
4	Ασκήσεις και Εργαστήρια	

5	Gamification Aspects	cloud κλπ, για την επικοινωνία με άλλους χρήστες ή για την παροχή live help. Μέσα στη πλατφόρμα θα δίνεται η δυνατότητα στον χρήστη να διαλέξει από τα διαθέσιμα labs και τις ασκήσεις τύπου multiple choises, videos κλπ.Μια σύγχρονη πλατφόρμα δίνει έμφαση στα gamification futures και στο visualization, ώστε να επιβραβέυει το χρήστη και να του προσφέρει συνεχώς το απαραίτητο κίνητρο. Τέλος η προσοχή στο visualization συνδράμει στην ευκολία χρήσης και στην ενημέρωση του end user.
6	Visual Aspects	

Ακολουθούν τα βήματα και η περιγραφή ενός σεναρίου για τον εκπαιδευόμενο **Πίνακας 8** και για τον εκπαιδευτή. **Πίνακας 9**

Πίνακας 8. Περιγραφή των βημάτων που ακολουθεί ο εκπαιδευόμενος

Εκπαιδευόμενος		
Α/Α	**ΒΗΜΑΤΑ/**	**ΠΕΡΙΓΡΑΦΗ**
1	User log in	Τα βήματα που ακολουθεί ο χρήστης: Κάνει login, επιλέγει το course επιθυμεί και γίνεται redirect αυτό. Διαλέγει το course στο οποίο θα κάνει join και επιλέγει το module A πχ θεωρία-εισαγωγή. Μετά το πέρας της θεωρίας ο χρήστης επιλέγει το module που περιλαμβάνει το assignment με το εργαστηριακό κομμάτι και πατάει star Lab. Αυτόματα θα δημιοθργηθεί ένα LAB με μία τοπολογία (κόμβοι, pcs, VMs).
2	Redirect to course module	
3	Select from lms avaliable courses	
4	Decide course to join	
5	User begins course A / module A	
6	Θεωρία - Lab	
7	Αυτόματη δημιουργία Εργαστηρίου	

Πίνακας 9. Περιγραφή των βημάτων που ακολουθεί ο εκπαιδευτής

Εκπαιδευτής		
Α/Α	**ΒΗΜΑΤΑ/**	**ΠΕΡΙΓΡΑΦΗ**
1	Login	Αντίστοιχα ο εκπαιδευτής με διαφορετικά rights στο account του κάνει Login, και γίνεται redirect στα ενεργά labs της ομάδας / τάξης του. Μπορεί να επιλέξει ένα από τα open labs και να παρατηρήσει και να επέμβει, αλλάζοντας configuration, να προσθέσει hosts, VMs κλπ.
2	Redirect to active labs	
3	Observe real time labs	
4	Access lab	
5	Interact with labs	

14. FUTURE WORK

Μια στρατηγική multi-cloud είναι η χρήση δύο ή περισσότερων υπηρεσιών cloud computing. Ενώ μια υλοποίηση multi-cloud μπορεί να αναφέρεται σε οποιαδήποτε εφαρμογή πολλαπλού λογισμικού ως υπηρεσία (SaaS) ή πλατφόρμα ως υπηρεσία (PaaS), σήμερα, γενικά αναφέρεται σε συνδυασμό public infrastructures ως υπηρεσία (IaaS), όπως το Amazon Web Services και το Microsoft Azure.

Αυτό είναι γνωστό ως multi-cloud computing, ένα υποσύνολο του ευρύτερου όρου hybrid cloud. Σε μια πρόσφατη έρευνα του Gartner για τους χρήστες του cloud, το 81% των ερωτηθέντων δήλωσε ότι συνεργάζεται με δύο ή περισσότερους παρόχους.[64]

Το υβριδικό cloud computing αναφέρεται στην παροχή και τη χρήση policy-based υπηρεσιών οι οποίες πλέον διαχειρίζονται σε ένα συνδυασμό εσωτερικών και εξωτερικών υπηρεσιών cloud.

Οι πρακτικές αυτές έχουν προκύψει από την ανάγκη για redundancy και την αποφυγή του vendor lock-in. [65] Φυσικά όσο μεγαλώνει ο ανταγωνισμός, προσφέρονται συνεχώς νέες υπηρεσίες με ανταγωνιστικούς όρους, με μεγαλύτερες ταχύτητες και χωρητικότητες.

Για παράδειγμα, μια συγκεκριμένη πλατφόρμα cloud μπορεί να χειριστεί μεγάλο αριθμό αιτημάτων ανά μονάδα χρόνου, απαιτώντας μικρές μεταφορές δεδομένων κατά μέσο όρο, ενώ κάποια άλλη ενδέχεται να έχει καλύτερη απόδοση για μικρότερο αριθμό αιτημάτων ανά μονάδα χρόνου που περιλαμβάνει μεγάλες μεταφορές δεδομένων.

Το multicloud βασίζεται συνήθως σε τρεις υποθέσεις:

- Στην τάση να αυξήσουμε την ευελιξία και να αποφύγουμε το vendor lock-in.
- Στην αρχιτεκτονική: Οι σύγχρονες εφαρμογές, δημιουργούνται σε πιο αρθρωτό στυλ. Μπορούν να εκτείνονται σε πολλούς providers ή να καταναλώνουν υπηρεσίες και resources από πολλαπλά clouds.
- Τέλος στη διακυβέρνηση: Για να διασφαλιστεί ο επιχειρησιακός έλεγχος, οι επιχειρήσεις θέλουν να ενοποιήσουν τη διαχείριση και την παρακολούθηση των συστημάτων πληροφορικής τους.

Η παραπάνω συνοπτική ανάλυση έγινε για να παρουσιάσουμε τα οφέλη και την ιδέα του hybrid/ multi cloud. Έτσι λοιπόν όπως σε πολλές περιπτώσεις η εκπαίδευση πλέον δεν έχει σύνορα, γίνεται δικτυακά και με μαθητές απ’ όλο τον κόσμο γιατί να σχεδιάσουμε κάτι του οποίου η υποδομή θα βρίσκεται τοπικά σε ένα server room.

Όλα όσα είδαμε στην παρούσα εργασία στηρίζονται στην ιδέα υλοποίησης σεναρίων σε εικονικό περιβάλλον και στην αυτοματοποιημένη διαδικασία με στόχο την αποφυγή σφαλμάτων και τη μείωση του χρόνου που απαιτεί μια δικτυακή τοπολογία. Σίγουρα το στόχος μας είναι να δείξουμε την εφικτότητα μιας εργαστηριακής τοπολογίας με εκπαιδευτικό χαρακτήρα, δεν είναι όμως λίγοι οι οργανισμοί που πριν δοκιμάσουν ένα νέο στοιχείο, ή ένα νέο στοιχείο πάνω σε ένα λειτουργικό δίκτυο, το δοκιμάζουν πρώτα εργαστηριακά. Επίσης καθώς είδαμε στα πρώτα κεφάλαια της εργασίας, ένα σημαντικό πεδίο εφαρμογής ενός τέτοιου εργαστηρίου είναι η κυβερνοασφάλεια και η ιδιαιτερότητα ενός sandbox για συνεχείς δοκιμές και εκπαίδευση.

Αυτά φυσικά απαιτούν και βασίζονται στην ανθρώπινη συμμετοχή και προσπάθεια για να δουλέψουν και να βρουν τις ευπάθειες ενός «ζωντανού δικτύου». Για παράδειγμα projects όπως το Metasploit, το οποίο παρέχει στους χρήστες ένα ασφαλές περιβάλλον για την έρευνα στον τομέα της ασφάλειας. Θα ήταν αρκετά ενδιαφέρουσα μία προσέγγιση υλοποίησης computer bots, τα οποία θα μπορούσαν να τρέξουν σενάρια

επιθέσεων, scanning και mitigation και να βρουν τις ευπάθειες, εξισώνοντας το χρόνο που απαιτείται από μία ομάδα μηχανικών από ώρες, ίσως και μέρες, με milliseconds. [66]

15. ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε ένα δικτυακό περιβάλλον, δεν αρκεί να έχουμε όλους τους κόμβους, τους απαραίτητους πόρους και το κατάλληλο QOS, πρέπει να διαμορφώνει κανείς και το αντίστοιχο περιβάλλον ασφαλείας για την απρόσκοπτη λειτουργία και την προστασία του συστήματος. Επίσης η αυτοματοποίηση πολλών διαδικασιών, μειώνει το χρόνο που αφιερώνει το IT, σε προγραμματισμένες και τυποποιημένες εργασίες, το οποίο μεταφράζεται σε μείωση λειτουργικού κόστους.

Η Ansible είναι ένα εργαλείο για την αυτοματοποίηση διαδικασιών και σε συνδυασμό με έναν εξομοιωτή όπως το GNS3 επιτρέπει στο χρήστη να προσομοιώσει οποιοδήποτε σενάριο και να παρατηρήσει τις μεταβολές κατάστασης του συστήματος, σε εικονικό περιβάλλον. Παράλληλα όπως αναλύθηκε ένα τέτοιο σύστημα μπορεί να αποτελέσει εργαλείο εκπαίδευσης και παρατήρησης των εκπαιδευόμενων αν συνδυαστεί με μία πλατφόρμα LMS/LXP, με αμέτρητες δυνατότητες.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Cybersecurity	Κυβερνοασφάλεια
Framework	Πλαίσιο
Tabletop exercises	Επιτραπέζιες ασκήσεις
Stakeholders	Ενδιαφερόμενοι
Penetration testing	Άσκηση ευπάθειας
Playbook	Βιβλίο παιχνιδιού
Behaviorism	Συμπεριφορισμός
Libraries	Βιβλιοθήκες
Automation	Αυτοματισμός
Licences	Άδειες
Scalability	Δυνατότητα εξέλιξης/αναβάθμισης
Management	Διαχείριση
Interoperability	Διαλειτουργικότητα
Hypervisor	Επόπτης
Nodes	Κόμβοι
Normalization	Κανονικοποίηση
Lightweight	Ελαφρύς
Gamification	Παιχνιδοποίηση
Hybrid cloud	Υβριδικό υπολογιστικό νέφος
Multicloud	Πολλαπλό υπολογιστικό νέφος

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ADDIE	Analysis Design Development Implementation Evaluation
ISD	Instructional systems design
LMS	Learning Management System
LXP	Learning Experience Platform
NICE	National Institute for Health and Care Excellence
NIST	National Institute of Standards and Technology
IT	Information Technology
SOC	Security Operation Center
ERP	Enterprise resource planning
BCM	Business Continuity Management,
CTO	Chief technology officer
CIO	Chief information officer
CISO	Chief information Security officer
MAME	Multiple Arcade Machine Emulator
CDX	cyber defense exercise
CVSS	Common Vulnerability Scoring System
BAS	Breach and Attack Simulation
MSEL	Master Scenario Events List
ID	Instructional design
OAR	Objectives, Activities, Resources
SME	Subject matter experts
NS-3	Network Simulator 3
IDE	Integrated Development Environment
POC	Proof of Concept
LPWAN	low-power wide-area network
VCSA	vCenter Server Appliance
REST API	Representational state transfer application programming interface
DSL	Domain-Specific Language
YAML	A recursive acronym for "YAML Ain't Markup Language") is a human-readable data-serialization language.
VM	Virtual Maschine
QOS	Quality of service
CM	Configuration Management

ΑΝΑΦΟΡΕΣ

[1] National Initiative for Cybersecurity Education (NICE) [Online] Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf?trackDocs=NIST.SP.800-181.pdf [Προσπελάστηκε 15/1/20]

[2] The Mission Critical Institute [Online] Available: https://missioncriticalinstitute.org/nice-cybersecurity-workforce-framework/ [Προσπελάστηκε 17/1/20]

[3] Cybersecurity & Infrastructure Security Agency [Online] Available: https://www.cisa.gov/cybersecurity-training-exercises [Προσπελάστηκε 17/1/20]

[4] *How Cyber Security Can Protect Your Business—A Guide for All Stakeholders, Wright, Christopher, Cambridgeshire, IT Governance Publishing*

[5] *How fake cybersecurity incidents can improve real preparedness [Online] Available:* https://www.ey.com/en_gl/consulting/how-fake-cybersecurity-incidents-can-improve-real-preparedness [Προσπελάστηκε 10/2/20]

[6] *Cybersecurity incident simulation exercises, Paul Van Kessel, EY, 2018.*

[7] *CJCSM 3500.03D Joint Training Manual for the Armed Forces of the United States*

[8] *Why Real Testing Requires Emulation, Not Just Simulation for Layer 4-7, Spirent, 2018*

[9] *Kavak, Hamdi & Padilla, Jose & Vernon-Bido, Daniele & Gore, Ross & Diallo, Saikou. (2016). A Characterization of Cybersecurity Simulation Scenarios. 10.22360/SpringSim.2016.CNS.003. Chapter 5*

[10] Spirent [Online] Available: https://www.spirent.com/ [Προσπελάστηκε 25/3/20]

[11] *White, Gregory B.; Dietrich, G.; Goles, T. (2004). Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events.Proc. of the 37th Annual Hawaii International Conference on System Sciences*

[12] *Hernandez-Ardieta, Jorge L. & Santos, David & Parra, Pascual & Tapiador, Juan & Peris-Lopez, Pedro & Lopez, Javier & Fernandez, Gerardo. (2014). An Intelligent and Adaptive Live Simulator: A new Concept for Cybersecurity Training.*

[13] Veksler VD, Buchler N, Hoffman BE, Cassenti DN, Sample C, Sugrim S. Simulations in Cyber-Security: *A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. Front Psychol. 2018;9:691.* Published 2018 May 15. doi:10.3389/fpsyg.2018.00691

[14] Common Vulnerability Scoring System [Online] Available: https://www.first.org/cvss/ [Προσπελάστηκε 20/5/20]

[15] *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*

[16] Venkatesh Jaganathan, Priyesh Cherurveettil, and Premapriya Muthu Sivashanmugam, *Using a Prediction Model to Manage Cyber Security Threats, 2014*

[17] Edgescan 2019, VULNERABILITY STATISTICS REPORT [Online] Available: https://www.infosecurityeurope.com/__novadocuments/596178?v=636957724578400000 [Προσπελάστηκε 25/3/20]

[18] Gus Evangelakos, "Breach and attack simulation vs pen testing", XM Cyber, 2018; https://www.xmcyber.com/breach-and-attack-simulation-vs-pen-testing/ [Προσπελάστηκε 17/8/20]

[19] Maya Schirmann VP Marketing, XM Cyber, *Harness the Power of Purple Team Automation*, Info-Security Magazine, 24 MAY 20.

[20] *JP 3-0 Joint Operation.*

[21] *JP 6-0 Joint Communications Systems.*

[22] *NIST SP 800-53, 800-61, SP 800-84.*

[23] *NISTIR 7298 Glossary of Key Information Security Terms.*

[24] *NIST National Initiative for Cyber security Education.*

[25] Jason Kickm, *Cyber Exercise Playbook,* The MITRE Corporation, 2014.

[26] Common Weakness Enumeration (CWE™) [Online] Available: http://cwe.mitre.org/data/index.html#release_notes [Προσπελάστηκε 17/8/20]

[27] ISD Framework [Online] Available: https://en.wikipedia.org/wiki/Instructional_design, [Προσπελάστηκε 25/1/20]

[28] Food and Agriculture Organization of the United Nations , *E-learning methodologies, A guide for designing and developing e-learning courses*, FAO Trust Fund Project GCP/GLO/279/GER, , Rome, 2011

[29] Mergel, Brenda, *Instructional Design & Learning Theory*, 1998

[30] *Learning management system [Online] Available:* https://en.wikipedia.org/wiki/Learning_management_system

[31] Lms Vs Lxp: Definitions, Differences & Use Cases [Online] Available: *https://www.howspace.com/resources/lms-vs-lxp*

[32] Best Corporate Learning Management Systems [Online] Available: https://www.g2.com/categories/corporate-learning-management-systems [Προσπελάστηκε 25/1/20]

[33] G2 [Online] Available: https://www.g2.com/ [Προσπελάστηκε 25/1/20]

[34] G2, Best LXP Platforms [Online] Available: https://www.g2.com/categories/lxp-platforms [Προσπελάστηκε 26/1/20]

[35] Percipio Success factors Integration, 2020 [Online] Available: https://documentation.skillsoft.com/en_us/pes/Integration/LMS-Integration/SuccessFactors/int_sf_overview.htm [Προσπελάστηκε 27/1/20]

[36] VMware Distributed Resource Management: *Design, Implementation, and Lessons Learned,* VMware, Inc, 2019

[37] Nelson, B.-H. Lim, and G. Hutchins*, Fast transparent migration for virtual machines.* In Usenix Annual Technical Conference *(Usenix ATC '05), April 2005*

[38] NetOps Meets DevOps *The State of Network Automation,* 2018 Report

[39] Geoff Stoker, Todd Arnold, and Paul Maxwell, *Using Virtual Machines to Improve Learning and Save Resources in an Introductory IT Course,* Department of Electrical Engineering and Computer Science United States Military Academy West Point, NY October 2013.

[40] VMware [Online] Available: https://www.vmware.com/ [Προσπελάστηκε 5/4/20]

[41] Red Hat [Online] Available: https://www.redhat.com/en [Προσπελάστηκε 8/5/20]

[42] Daniel Conte de Leon, Christopher E. Goes, Michael A. Haney, AxelW. Krings *"ADLES: Specifying, deploying, and sharing, hands-on cyber*-exercise", Idaho, USA, *2 January 2018*

[43] Cyber Range Organization and Design Chair, CROND, [Online] Available: https://github.com/crond-jaist/cytrone [Προσπελάστηκε 10/8/20]

[44] The Official YAML Website [Online] Available: http://www.yaml.org/ [Προσπελάστηκε 27/1/20]

[45] R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, Y. Shinoda. *Integrated Framework for Hands-on Cybersecurity Training: CyTrONE.* Elsevier Computers & Security, vol. 78C, June 2018, pp. 43-59.

[46] NS3 [Online] Available: https://www.nsnam.org/ [Προσπελάστηκε 20/5/20]

[47] Gns3 [Online] Available: https://www.gns3.com/ [Προσπελάστηκε 14/5/20]

[48] EVE-ng [Online] Available: https://www.eve-ng.net/ [Προσπελάστηκε 14/5/20]

[49] Christopher Hart, *Career Progression - CBT Nuggets*, June 10, 2019

[50] Ansible [Online] Available: https://docs.ansible.com/ansible/latest/index.html [Προσπελάστηκε 27/1/20]

[51] Saltstack [Online] Available: https://docs.saltstack.com/en/master/topics/topology/index.html [Προσπελάστηκε 18/6/20]

[52] Puppet [Online] Available: https://puppet.com/docs/puppet/6.17/puppet_index.html [Προσπελάστηκε 19/6/20]

[53] Chef [Online] Available: https://docs.chef.io/vmware/ [Προσπελάστηκε 19/6/20]

[54] A short comparison of Ansible, Chef, Puppet and Saltstack, July 1, 2019, Niels Goosens, HCS Company, [Online] Available: https://www.hcs-company.com/blog/automation/comparison-ansible-chef-puppet-saltstack [Προσπελάστηκε 20/6/20]

[55] EVE-NG Professional Cookbook, Version 1.16, Uldis Dzerkals, 2018

[56] Docker [Online] Available: https://www.docker.com/ [Προσπελάστηκε 18/12/19]

[57] *Vmware Workstation [Online] Available:* https://www.vmware.com/products/workstation-pro.html [Προσπελάστηκε 15/11/19]

[58] *Vmware Vsphere [Online] Available:* https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/7_0 [Προσπελάστηκε 15/5/20]

[59] *VMware vSphere Documentation [Online] Available:* https://docs.vmware.com/en/VMware-vSphere/index.html [Προσπελάστηκε 15/5/20]

[60] *Playbook Language Example:* https://docs.ansible.com/ansible/latest/user_guide/playbooks_intro.html#playbook-language-example [Προσπελάστηκε 15/1/20]

[61] Curl [Online] Available: an open-source command line tool for transferring files withUniformed Resource Locator (URL) syntax.http://curl.haxx.se/ [Προσπελάστηκε 27/1/20]

[62] Postman [Online] Available: https://www.postman.com/ [Προσπελάστηκε 8/2/20]

[63] gns3fy 0.7.0 [Online] Available: https://pypi.org/project/gns3fy/ [Προσπελάστηκε 6/4/20]

[64] Laurence Goasduff, *"Most organizations choose to work with multiple cloud providers, for a host of different reasons*", Gartner May 7, 2019.

[65] *Deliver a seamless service experience across multicloud environments, Infradata [Online] Available:* https://www.infradata.com/services-solutions/cloud-networking/private-and-hybrid-cloud/multi-cloud-solutions/ [Προσπελάστηκε 1/7/20]

[66] Thanassis Avgerinos, David Brumley, John Davis, Ryan Goulden, Tyler Nighswander, Alex Rebert, andNed Williamson, *"The Mayhem Cyber Reasoning System"* | *ForAllSecure,* April 2018

[67] Choosing an Infrastructure as Code tool [Online] Available: https://www.ibm.com/cloud/blog/chef-ansible-puppet-terraform [Προσπελάστηκε 17/8/20]


Διπλωματική Εργασία
Δημήτριος Ζάμπος
2020