1. Κεντρική Διαχείριση κυβερνοεπιθέσεων. Ανάπτυξη συνεργατικής πλατφόρμας
Ένα από τα βασικά προβλήματα που θα πρέπει να αντιμετωπίσουμε ως υπεύθυνοι αντιμετώπισης μιας κυβερνοεπίθεσης είναι και η κεντρική διαχείριση κυβερνοεπιθέσεων σε Εθνικό επίπεδο. Το πρόβλημα που θα πρέπει να επιλυθεί είναι πως μπορεί μία ομάδα διαχειριστών κυβερνοεπιθέσεων να συνεργαστούν μέσα από μία πλατφόρμα συνεργασίας. Το ερώτημα που θα ρέπει να απαντηθεί μεταξύ άλλων είναι: Τι εργαλεία θα πρέπει να περιλαμβάνει η συγκεκριμένη πλατφόρμα;
Σκοπός της εργασίας είναι να αναπτυχθεί μία πλατφόρμα συνεργασίας για την κεντρική διαχείριση κυβερνοεπιθέσεων. Θα πρέπει να συνδυάζει ελεύθερα εργαλεία (open source tools).

Θα διαθέτει ένα διαχειριστικό web interface. Σαν παράδειγμα μπορούμε να χρησιμοποιήσουμε το ακόλουθο framework:
https://github.com/pe3zx/mthc

Ξεκινάμε με την ανάπτυξη του web interface.

Μπορούμε να έχουμε και σαν πρότυπο το security onion.
Αντί για το TheHive να χρησιμοποιούμε το case (https://docs.securityonion.net/en/2.3/cases.html).
Αρχικά να στίσουμε το case με cortex και στην συνέχεια προσθέτουμε:
cortxe (https://github.com/TheHive-Project/Cortex)
MISP (https://github.com/MISP/MISP)
Mattermost (https://github.com/mattermost)
Cyberchef (https://github.com/gchq/CyberChef)
playbooks (https://github.com/gchq/CyberChef)

Η ιδέα είναι να διαθέτουμε μία πλατφόρμα όπου θα διαχειριζόμαστε μία κυβερνοεπίθεση. Θα ξεκινάμε με το άνοιγμα ενός ticket και στην συνέχεια με ροές εργασίας (workflows) θα μεταβαίνουμε στα επόμενα βήματα διαχείρισης μιας κυβερνοεπίθεσης, ακολουθώντας τις υποδείξεις των σχετικών playbooks.

Καλό μάθημα αναφοράς είναι και το ακόλουθο:
Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting
(https://www.amazon.com/Incident-response-Threat-Intelligence-intelligence-based/dp/1801072957)

2. Αρχική πρόσβαση σε ένα windows 11 λειτουργικό σύστημα.
Οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές για να αποκτήσουν αρχική πρόσβαση σε ένα windows 11 λειτουργικό σύστημα.
Σκοπός της εργασίας είναι να παρουσιαστούν όλες οι γνωστές τεχνικές αρχικής πρόσβασης και να παρουσιαστούν τα αντίμετρα προστασίας από αυτές τις επιθέσεις.
Στην συνέχεια να παρουσιαστούν τα αντίμετρα που λαμβάνει ένας επιτιθέμενος για να ξεπεράσει τους μηχανισμούς προστασίας με ιδιαίτερη έμφαση στις τεχνικές για να ξεπεράσει (by pass) antivirus και EDR.
Να αναπτυχθεί ένα εργαλείο το οποίο θα χρησιμοποιεί διάφορες τεχνικές εκτέλεσης κώδικα, δηλαδή τεχνικές απόκτησης πρόσβασης και σαν τελικό σκοπό θα έχει να δοκιμάζει την αποτελεσματικότητα ενός antivirus ή ενός EDR.
Σαν παράδειγμα μπορεί να χρησιμοποιηθεί το ακόλουθο powershell script:
https://github.com/op7ic/EDR-Testing-Script
Η ιδέα είναι να δημιουργηθούν πολλαπλά payloads και στην συνέχεια να εκτελούνται σε ένα windows 11 με εγκατεστημένο το EDR ή το antivirus που θέλουμε να δοκιμάσουμε και να καταγράφουμε τι εντοπίζει και τι δεν εντοπίζει με αυτόματη διαδικασία. Δηλαδή στο τέλος να εμφανίζει μία αναφορά αποτελεσμάτων.

3. Cloud forensics

Στην διπλωματική να παρουσιαστεί η διαδικασία διαχείρισης μιας κυβερνοεπίθεσης και ψηφιακής σήμανσης (digital forensics) σε ένα cloud.

Ως παραδείγματα θα πρέπει να χρησιμοποιηθούν cloud υπηρεσίες όπως SaaS (Software as a Service), IaaS (infrastructure as a service) και PaaS (platform as a service).

Θα πρέπει να αναφερθούν οι διαφορές διαχείρισης μιας κυβερνοεπίθεσης στην κάθε περίπτωση υπηρεσιών ξεχωριστά.

Τέλος να γίνει αναφορά στην διαχείριση μιας κυβερνοεπίθεσης σε private cloud.

Να παρουσιαστούν τακτική, τεχνικές, διαδικασίες και εργαλεία για την διαχείριση μιας κυβερνοεπίθεσης σε cloud υπηρεσίες.

Σχετικοί σύνδεσμοι:

https://github.com/google/cloud-forensics-utils

https://cforensicslab.medium.com/the-importance-and-challenges-in-cloud-forensics-d926629e6607

https://www.ijser.org/researchpaper/technical-challenges-of-cloud-forensics-and-suggested-solutions.pdf