ΕΕΛΛΑΚ
Οργανισμός Ανοιχτών Τεχνολογιών

Συμμετοχή στην Εθνική άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ 2023

Κώστας Παπαδήμας

Τι είναι ο Πανόπτης

- Ελληνική Εθνική άσκηση Κυβερνοάμυνας
- (Ελεύθερη συμμετοχή) Υποχρεωτική για τις ΕΔ.
- Διοργανώνεται κάθε χρόνο από το 2010
  (Το ΓΕΕΘΑ/Ε5 είναι υπεύθυνο για την οργάνωση της άσκησης)
- Κυρίως άσκηση μη πραγματικού χρόνου
- Παρέχεται ένα ελεγχόμενο περιβάλλον για να εξασκηθούν οι ΕΔ, ο δημόσιος και ιδιωτικός τομέας, καθώς και ο ακαδημαϊκός
- Μεγάλης έκτασης άσκηση με σκοπό την προσομοίωση αντιμετώπισης κυβερνοεπιθέσεων που έχουν επίπτωση σε Εθνικό επίπεδο.
- Δεν επηρεάζονται τα παραγωγικά δίκτυα

Τι είναι ο Πανόπτης

Άσκηση μη πραγματικού χρόνου, με διάφορα επεισόδια:

• Διαδικασιών αντιμετώπισης κυβερνοεπιθέσεων (Incident handling process)

• Ψηφιακής σήμανσης (Digital forensics)

• Ανάλυσης ιομορφικού λογισμικού (Malware analysis)

• Διαδικασιών αναφοράς συμβάντων σε επίπεδο οργανισμού και εθνικό

• Διαμοιρασμός πληροφοριών

Μπορεί να περιλαμβάνει και επεισόδια πραγματικού χρόνου, όπως:

Κυβερνοεπιθέσεις σε web services.

Κυβερνοεπιθέσεις σε μικρά εικονικά δίκτυα.

- Δεν υπάρχει αξιολόγηση- βαθμολόγηση.
- Υποχρέωση της ομάδας είναι να παραδώσει έγκαιρα τις λύσεις των επεισοδίων

ΠΑΝΟΠΤΗΣ: Σενάριο-Επεισόδια

Τα τεχνικά σενάρια του ΠΑΝΟΠΤΗ περιλαμβάνουν επιθέσεις στον κυβερνοχώρο εναντίον των υποδομών ΤΠΕ, σε εθνικό επίπεδο, με σκοπό να:

- υποβαθμίσουν την λειτουργία της κυβέρνησης και την παροχή δημόσιων υπηρεσιών
- μειώσουν την ικανότητα για την αποκατάσταση των επιπτώσεων μιας κυβερνοεπίθεσης σε κρίσιμες εθνικές υποδομές
- υπονομεύσουν την εμπιστοσύνη του κοινού

Παραδείγματα τεχνικών επεισοδίων:

Client side attacks (email attacks, Click-jacking)
Social Engineering
Digital Forensics challenges
Malware (Rootkit & Trojan) analysis
Attacking web services
Insiders
Data ex-filtration
Adversaries simulation (post exploitation attacks)
Legal injects
Scada

ΠΑΝΟΠΤΗΣ: Αντικειμενικοι σκοποί

Εξάσκηση της εθνικής κοινότητας αντιμετώπισης κυβερνοεπιθέσεων
με έμφαση:

- στις διαδικασίες αντιμετώπισης κυβερνοπεριστατικών
- στην ψηφιακή εγκληματολογία
- στην ανάλυση ιμομορφικού λογισμικού (malware)
- στην ανταλλαγή πληροφοριών
- στην ανταλλαγή εμπειριών

Η ανάπτυξη μιας βάσης δεδομένων με τους εθνικούς εμπειρογνώμονες, ώστε να σχηματιστούν ομάδες ταχείας αντίδρασης όταν απαιτείται, αλλά και την αποθήκευση των συμπερασμάτων.

Διεξαγωγή της άσκησης

Διάρκεια: Πέντε (5) ημέρες

- Η 1η μέρα είναι η ημέρα των δοκιμών επικοινωνίας
- Οι επόμενες τρεις ημέρες είναι η "διεξαγωγή της άσκησης", ημέρες κατά τις οποίες οι εκπαιδευόμενοι ανταποκρίνονται στα τεχνικά σενάρια
- Η 5η μέρα είναι η ημέρα των συμπερασμάτων
- Τα τεχνικά σενάρια παρέχονται τουλάχιστον 10 ημέρες πριν από την ημέρα εκτέλεσης (προστατεύονται με κωδικό πρόσβασης)
- Μέσα επικοινωνίας κατά τη διάρκεια της άσκησης
  Poseidon (θα δοθούν οδηγίες χρήσης)
  Portal+MISP (Malware Information Sharing Platform)
  email
  Live chat

Η ομάδα της ΕΕΛΛΑΚ

Συμμετέχει κάθε χρόνο από το 2016

- Στην ομάδα συμμετεχουν κάθε χρόνο πάνω από 40 ενδιαφερόμενοι προερχομενοι κυριως απο πανεπιστημια , ερευνητικα κεντρα αλλά και τον ιδιωτικό τομέα.
- Ολη η συνεργασία και η επικοινωνία των συμμετεχόντων της ομάδας γίνεται μέσω του Matrix/element server της ΕΕΛΛΑΚ https://matrix.to/#/#panoptis-2022:chat.ellak.gr) και ο διαμοιρασμός των επεισοδίων στους συμμετέχοντες θα γίνεται μέσω του nextcloud server της ΕΕΛΛΑΚ
- Μέσα από την ομάδα αναλαμβάνουν κάποιοι τον συντονισμό των επεισοδίων

Διαδικασία

- Η φετινή άσκηση θα διεξαχθεί μέσω της Ευρωπαϊκής πλατφόρμας POSEIDON (Platform-based Operational System for Events & Injects Distribution Online). Οσοι θελουν να συμμετέχουν online και στην πλατφόρμα poseidon θα χρειαστεί να προχωρησουν στην διαδικασία εγγραφής με EU Login (με το ιδιο email που εχουν δηλώσει συμμετοχή στην ομάδα) .
- Απαιτούνται να εισαγετε προσωπικά στοιχεία στην πλατφόρμα του EU-Login και στην πλατφόρμα Poseidon
- Για τους υπόλοιπους θα μοιραστούν τα επεισόδια για καθημερινή ανάλυση και επίλυση offline απο το Ποσειδων μέσω της πλατφόρμας matrix . Όλη η επικοινωνία θα γινεται μεσω του **https://matrix.to/#/#panoptis-2022:chat.ellak.gr**

Διαδικασία

- Η άσκηση διεξάγεται μέσω της πλατφόρμας Poseidon, όπου και δημοσιεύνται τα injections και οι ασκλησεις της ημέρας

Οδηγίες σύνδεσης με το Poseidon μπορείτε να βρείτε στο https://files.panoptis.cd.mil.gr/index.php/s/RXteaBfW9GwiY6t (θα σας σταλούν και μέσω email)

- Οσοι δεν συμμετέχουν στην πλατφόρμα Poseidon θα λαμβάνουν τα επεισόδια μεσα από το chat element στον matrix server της ΕΕΛΛΑΚ
- Ακόμα υπάρχει για τους συμμετεχοντες ένα Portal+MISP (Malware Information Sharing Platform)
- Rocket Live chat για την επικοινωνία

Ερωτήσεις;