Εθνική άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ-Επεισόδια

Περίγραμμα

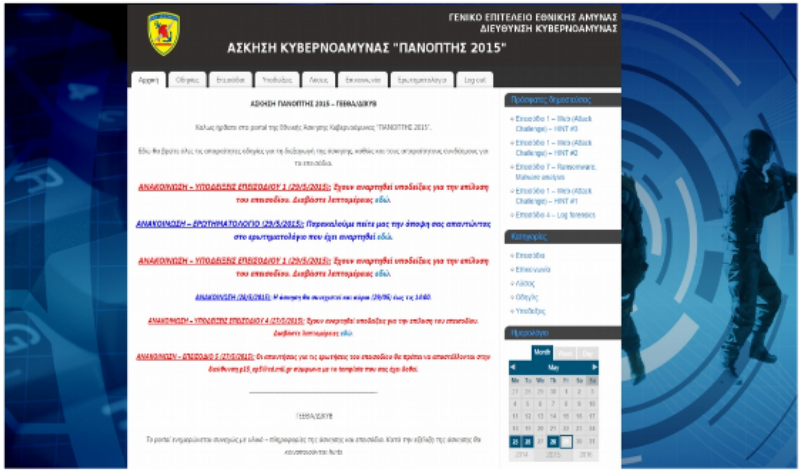
- Σκοπός
- Συστήματα Επικοινωνιών
- Οργάνωση Επεισοδίων
- Ανάλυση επί των Επεισοδίων
- Ερωτήσεις

Σκοπός

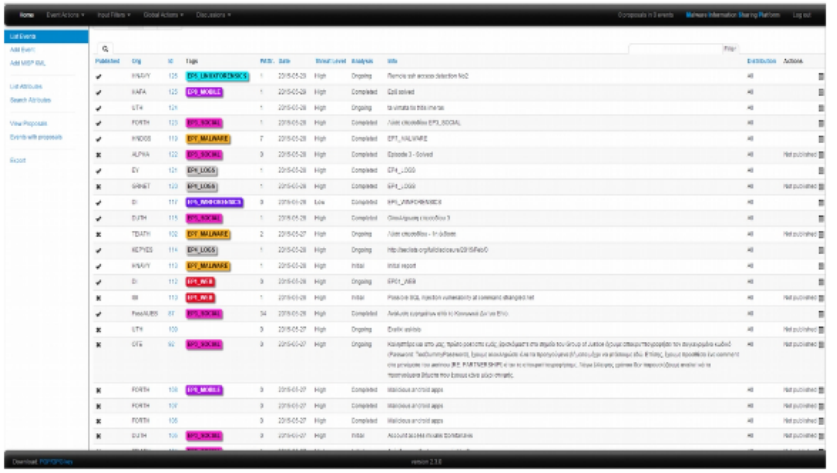
Σκοπός επεισοδίων:

- Η εξάσκηση των συμμετεχόντων σε τεχνικά θέματα.
- Η συνεργασία μεταξύ των παικτών σε τεχνικό και διαδικαστικό επίπεδο.
- Ο διαμοιρασμός τεχνικών, ιδεών και διαδικασιών αντιμετώσπισης συμβάντων.
- Η προσομοίωση τεχνικών συμβάντων υψηλού επιπέδου με γνώμονα νέες τεχνολογίες και ρεαλισμό.
- Η κλιμάκωση σε δυσκολία με σκοπό την αναγνώριση του επιπέδου των συμμετεχόντων και των αδυναμιών τους από τους ίδιους.
- Η δυνατότητα εκπαίδευσης επί των επεισοδίων και εκτός χρονικής διάρκειας άσκησης.
- Η κάλυψη μεγάλου φάσματος τύπων επιθέσεων και τεχνικών συμβάντων της κυβερνοάμυνας – κυβερνοασφάλειας.

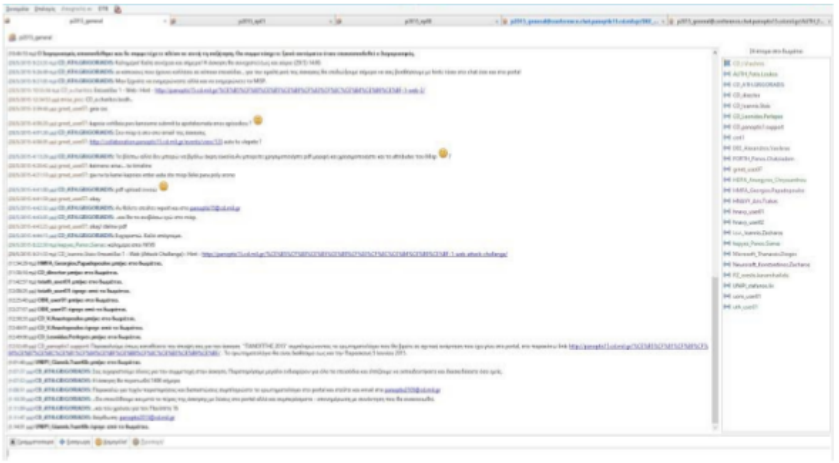
Συστήματα Επικοινωνίας – Ανταλλαγής Πληροφοριών



Portal



MISP



Chat

Επεισόδια

Τύπος	Αρ. Επεισοδίου
Web Application Security	1
Windows Forensics Analysis	2
Linux Forensics Analysis	3
Mobile Forensics Analysis	4
Network Forensics Analysis	5
SCADA	6
Capture the Flag	7

Web Application Security

Web Application Security

- Δεδομένα:
  - Ένα virtual image το οποίο αναπαριστά το παραβιασμένο σύστημα
- Ζητούμενα:
  - Εντοπισμός και ανάλυση των ενεργειών του κακόβουλου χρήστη

Mobile Forensics Analysis

Mobile Forensics Analysis

- Δεδομένα:
  - Ένα virtual image το οποίο αναπαριστά το παραβιασμένο σύστημα
- Ζητούμενα:
  - Εντοπισμός και ανάλυση των ενεργειών του κακόβουλου χρήστη

Forensics Analysis

Windows Forensics Analysis

- Δεδομένα:
  - Ένα virtual image (win 10) το οποίο αναπαριστά το παραβιασμένο σύστημα
- Ζητούμενα:
  - Εντοπισμός και ανάλυση των ενεργειών του κακόβουλου χρήστη

Linux Forensics Analysis

- Δεδομένα:
  - Ένα virtual image (linux) το οποίο αναπαριστά το παραβιασμένο σύστημα
- Ζητούμενα:
  - Εντοπισμός και ανάλυση των ενεργειών του κακόβουλου χρήστη

Network Forensics Analysis

Δεδομένα:

- Network packet captures (.pcap) από DMZ και LAN

Ζητούμενα:

- Υπάρχουν ενδείξεις για μόλυνση κάποιου συστήματος – Διερεύνηση.
- Διερεύνηση ύποπτων TCP συνδέσεων που πιθανόν εντοπίζονται.
- Η ομάδα αντιμετώπισης περιστατικών υποθέτει ότι ο μολυσμένος υπολογιστής είναι μέλος ενός δικτύου διοίκησης και ελέγχου (Command and Control network).

Αποστολή αναφοράς συνολικής διερεύνησης .

SCADA

Θα δοθεί επεισόδιο με ένα σύστημα παραβιασμένο που ελέγχει συστήματα scada.

Capture the Flag

- Θα δοθεί ssh πρόσβαση σε κάθε ομάδα σε ένα δίκτυο με linux συστήματα.
- Σκοπός να αποκτηθεί πρόσβαση με root δικαιώματα σε όλους τους υπολογιστές και να συλλεχθούν τα δεδομένα που θα κρύβονται στους συγκεκριμένους υπολογιστές.

Ερωτήσεις;