ΑΣΚΗΣΗ ΠΑΝΟΠΤΗΣ 2017

Σκοπός Άσκησης

- Εξάσκηση των συμμετεχόντων σε τεχνικά θέματα
- Συνεργασία των συμμετεχόντων σε τεχνικό και διαδικαστικό επίπεδο
- Διαμοιρασμός τεχνικών και διαδικασιών αντιμετώπισης συμβάντων στον κυβερνοχώρο
- Κάλυψη ευρέος φάσματος τύπου επιθέσεων και τεχνικών συμβάντων στον κυβερνοχώρο
- Δυνατότητα εκπαίδευσης και εκτός χρονικής διάρκειας άσκησης (αφορά offline επεισόδια)

Διαδικασία Διεξαγωγής πλην Επεισοδίου CTF

- Ημερομηνίες Διεξαγωγής: 29/05 – 2/06
  - 1η Ημέρα δοκιμή επικοινωνιών
  - 3 ημέρες άσκησης
  - Τελευταία ημέρα: Εσωτερική απενημέρωση
  - Ενδεχόμενη επέκταση εφόσον χρειαστεί και την τελευταία ημέρα

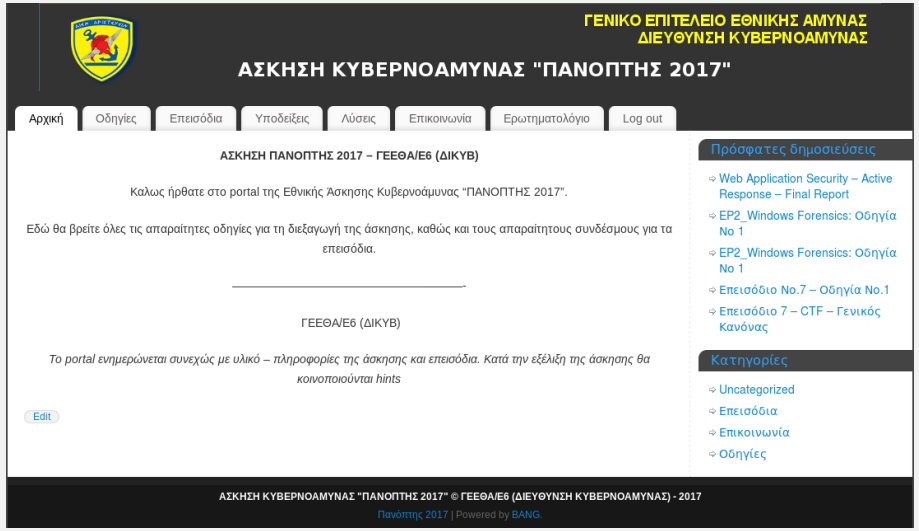
- Εργάσιμες ώρες (09:00-15:00) πλην επεισοδίου CTF– Καθένας επιλέγει πόσες ώρες θέλει να αφιερώσει

Διαδικασία Διεξαγωγής CTF

- Ημερομηνίες Διεξαγωγής: 29/05 – 2/06
- Ωράριο 10:00 – 19:00
- Τηλέφωνο επικοινωνίας κατά τη διάρκεια των επεισοδίων: 2106576275
- Στα δηλωθέντα email θα αποσταλούν credentials vpn για σύνδεση στο CTF
- Η επικοινωνία (email, chat κλπ) θα γίνεται μόνο με τον υπεύθυνο (αρχηγό) της κάθε ομάδας
- Στοιχεία (email, ονοματεπώνυμο, φορέας) θα υποβληθούν για όλα τα μέλη της ομάδας.

Πλατφόρμες Επικοινωνίας

- Portal (Domain: portal.cd.mil.gr)
  - Ενημέρωση για την άσκηση
  - Links για Download των επεισοδίων
  - Παρουσίαση hints
  - Επικοινωνία – Αναφορά Προβλημάτων



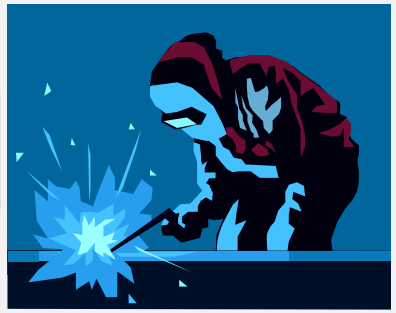
- Chat Server (Domain: chat.cd.mil.gr)
  - Chat Rooms ανά επεισόδιο για επικοινωνία των συμμετεχόντων
  - Οδηγίες στο Portal

Πλατφόρμες Επικοινωνίας

- MISP – Malware Information Sharing Platform (Domain:misp.cd.mil.gr)
  - Δε θα χρησιμοποιηθεί για το CTF
  - http://misp-project.org
  - Στοιχεία πρόσβασης: Θα αποσταλούν με email
  - Τι αναφέρουμε:
    - Επίπεδο απειλής συμβάντος: Καθόλου ή Χαμηλή, Μεσαία, Υψηλή απειλή
    - Ανάλυση Κατάστασης: Αρχικός εντοπισμός, σε εξέλιξη, Ολοκλήρωση
    - Περιγραφή Συμβάντος: Σύντομη, Αίτια, Επιπτώσεις, Ενέργειες

Επεισόδια

- 01 – Web Challenge – Active Defence (Live)
- 02 – Windows 10 Forensics (Offline)
- 03 – Linux Forensics (Offline)
- 04 – Mobile Forensics (Offline)
- 05 – Capture the Flag (CTF) (Live)



Web Challenge – Active Defence

- Δεδομένα:
  - Δύο Online Web συστήματα (DMZ και εσωτερικά) που θα περιέχουν αδυναμίες που θα πρέπει να διερευνηθούν
- Ζητούμενα:
  - Εντοπισμός και επιβεβαίωση (exploitation) των αδυναμιών των συστημάτων
  - Έλεγχος (και υλοποίηση) δυνατότητας shutdown συστημάτων ενέργειας που ελέγχονται από ανωτέρω συστήματα

Windows 10 Forensics

- Δεδομένα:
  - Virtual Image win 10 το οποίο θα προσομοιώνει παραβιασμένο σύστημα

- Ζητούμενα:
  - Εντοπισμός και ανάλυση ενεργειών κακόβουλου χρήστη

Linux Forensics Analysis

- Δεδομένα:
  - Virtual Image λειτουργικού linux το οποίο προσομοιώνει παραβιασμένο σύστημα

- Ζητούμενα:
  - Εντοπισμός και ανάλυση ενεργειών κακόβουλου χρήστη

Mobile Forensics Analysis

- Δεδομένα:
  - APK αρχεία που αφορούν κινητή συσκευή (OS Android)

- Ζητούμενα
  - Ανάλυση λειτουργίας και εντοπισμός αδυναμιών

Capture the Flag (CTF) - Cyber Ops

- Ομάδα: Round Table Security
  - ΠΑΝΟΠΤΗΣ 2016: Find the Insider
  - ΠΑΝΟΠΤΗΣ 2015: Ehlo – Social Media
- Κλιμακωτό Επίπεδο δυσκολίας
- Scoreboard βαθμολόγησης ομάδας
- Log Server για παρακολούθηση δικτυακής κίνησης
- Κάθε ομάδα θα παραδώσει walkthrough με τεχνική ανάλυση επεισοδίου και περίληψη πλοκής

Capture the Flag (CTF) - Cyber Ops

- Χώρα σε τεταμένες σχέσεις με γειτονικό κράτος.
- Ενδείξεις για προσπάθεια εκδήλωσης επιθέσεων σε δίκτυο στρατιωτικής υποδομής.
- Ομάδα RRT (παίκτες) καλείται για έλεγχο Pen Test του δικτύου.

Capture the Flag (CTF) - Cyber Ops

- **ACT 1**
  - Αναγνώριση κακόβουλων ενεργειών σε δίκτυο του Υπουργείου Αμύνης
  - Συλλογή flags θα κατευθύνει το διαγωνιζόμενο για το επόμενο βήμα
  - Ανάλυση Forensics σε windows 10 OS επεισόδιο εντός του ACT1 θα παρέχει επιπλέον βοήθεια για την καθοδήγηση των παικτών προς τη λύση του επεισοδίου.
    - Τα ευρήματα(flags) της ανάλυσης δίνουν βαθμούς και hints για το τι έχει συμβεί.
    - Δεν είναι απαραίτητη η επίλυση του forensics για την επίλυση του CTF. Τα hints βρίσκονται και αλλού.
    - Μπορεί να γίνει ανάλυση και ανεξάρτητα με το CTF (ως offline επεισόδιο)

Capture the Flag (CTF) - Cyber Ops

- Act 2
  - Με βάση τα αποτελέσματα του Act 1 θα απαιτηθεί διερεύνηση τρωτοτήτων και εκμετάλλευση αυτών για πρόσβαση σε δεύτερο δίκτυο

Capture the Flag (CTF) - Cyber Ops

- Act 3
  - Αρχηγοί ομάδων θα κληθούν να λάβουν απόφαση που θα καθορίσει το πέρας του επεισοδίου
  - Εξετάζει τη σωστή επικοινωνία συντονισμό και κατανόηση αρμοδιοτήτων

Capture the Flag (CTF) – Τεχνικά Στοιχεία

- Τρόπος πρόσβασης -> VPN
  - Credentials θα αποσταλούν στον αρχηγό της ομάδας
- Για όλες τις ενέργειες και τις αποφάσεις της ομάδας υπεύθυνος και υπόλογος είναι ο αρχηγός της
- Η επικοινωνία σε chat, email κλπ θα γίνεται μόνο με τον αρχηγό της ομάδας
- Απαγορεύονται ενέργειες που θα εμποδίζουν την ομαλή διεξαγωγή του επεισοδίου
- Ανάρτηση βοηθειών (hints) μέσω Portal και Chat
- Θα τηρηθούν οι ενέργειες των παικτών και η κίνηση του δικτύου για παρουσίαση στατιστικών στοιχείων διεξαγωγής της άσκησης

Capture the Flag (CTF)

- Τομείς Κυβερνοασφάλειας που άπτονται του επεισοδίου:
  - Forensics
  - Source Code Review
  - Web Pentest
  - Network Pentest
  - OS Pentest (Linux)
  - Steganography
  - White hat Philosophy
  - Decision Making Analysis
  - Organizing Rapid Reaction Teams

ΕΡΩΤΗΣΕΙΣ - ΣΥΖΗΤΗΣΗ