Εθνική άσκηση Κυβερνοάμυνας ΠΑΝΟΠΤΗΣ

Παναγιώτης Κρανιδιώτης Μέλος ΔΣ ΕΕΛΛΑΚ
panagiotis.kranidiotis@eellak.gr

Αντχος (Μ) Σ. Παπαγεωργίου Π.Ν. Δ/Ε6(ΔΙΚΥΒ)
spapageorgiou@mil.gr
ppspyros@gmail.com

Περίγραμμα

- ΓΕΕΘΑ/Ε6(ΔΙΚΥΒ)
- Ασκήσεις Κυβερνοάμυνας
- Άσκηση ΠΑΝΟΠΤΗΣ
  - Πανόπτης Γενικά -Κατάσταση
  - Σενάριο
  - ΑΝΣΚ
  - Σχεδιασμός και εκτέλεση του ΠΑΝΟΠΤΗ
  - Το Μέλλον
  - Συμπεράσματα
- Επίλογος

ΓΕΕΘΑ/ΔΙΚΥΒ

- Η αντιμετώπιση των κυβερνοεπιθέσεων σε καθημερινή βάση για την προστασία των πληροφοριακών δικτύων & υποδομών των ΕΔ.
- Είμαστε υπεύθυνοι για την κυβερνοάμυνα στις ΕΔ.

ΓΕΕΘΑ/ΔΙΚΥΒ

- 2002 τμήμα στο ΓΕΝ
- 2004 Διεύθυνση στο ΓΕΕΘΑ.
- Διαθέτει εκπαιδευμένα και πιστοποιημένα στελέχη.
- Διαθέτει Στρατιωτικό CERT (MCIRC-Military Computer Incident Response Center).

Κυβερνοάμυνα-ορισμός

- Η Κυβερνοάμυνα απαιτεί μία σειρά από μηχανισμούς, διαδικασίες και συνεχώς ανεπτυγμένες και δοκιμασμένες δυνατότητες, με σκοπό την πρόληψη, τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση, την αποκατάσταση και την εξαγωγή συμπερασμάτων, στην περίπτωση των κυβερνοεπιθέσεων, που έχουν σαν στόχο να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριακών υποδομών.

ΔΡΑΣΕΙΣ
(τι έχουμε κάνει μέχρι τώρα)

- Κατευθυντήριο πλαίσιο (Στρατιωτική Στρατηγική) Κυβερνοάμυνας
- Δόγμα επιχειρήσεων Κυβερνοχώρου
- Πολιτική Κυβερνοάμυνας (http://www.geetha.mil.gr/media/dikib/cyberdefence/cyberpolicy.pdf)
- Τεχνικό σχέδιο δράσεως ανάπτυξης κυβερνοάμυνας στις ΕΔ. (http://www.geetha.mil.gr/media/pdf-arxeia/2014/cyberdefence/texniko_sxedio_drasis_gia_tin_anaptixi_kivernoaminas_stis_ED.pdf)
- Τεχνικό εγχειρίδιο ασφαλείας (http://www.geetha.mil.gr/files/it_security/texniko-egxeiridio.pdf)
- Mailing list Κυβερνοασφάλειας-Κυβερνοάμυνας (cd@lists.grnet.gr)
- **Βασικό σχολείο κυβερνοάμυνας**
- **Προκεχωρημένο σχολείο κυβερνοάμυνας**

ΔΡΑΣΕΙΣ ΣΕ ΕΞΕΛΙΞΗ
(Τι κάνουμε)

- Εφαρμογή του σχεδίου δράσης ανάπτυξης κυβερνοάμυνας στις ΕΔ
- Διαδραστικό σχολείο ενημέρωσης σε θέματα Κυβερνοάμυνας-κυβερνοασφάλειας.
- Επικαιροποίηση τεχνικού εγχειριδίου ασφαλείας προσωπικού υπολογιστή
- Εκπόνηση τεχνικού εγχειριδίου διαχείρισης κυβερνοεπιθέσεων σε windows OS.
- Εκπόνηση τεχνικού εγχειριδίου διαχείρισης κυβερνοεπιθέσεων σε Linux OS.
- Ανάπτυξη λογισμικού συλλογής πληροφοριών, από διάφορα λειτουργικά συστήματα, για τον εντοπισμό κυβερνοεπιθέσεων
- Ενεργοποίηση διακλαδικού κέντρου αντιμετώπισης κυβερνοπεριστατικών
- Συμμετοχή στην ομάδα Σύνταξης Εθνικής Στρατηγικής Κυβερνοασφάλειας (Έτοιμο προσχέδιο)

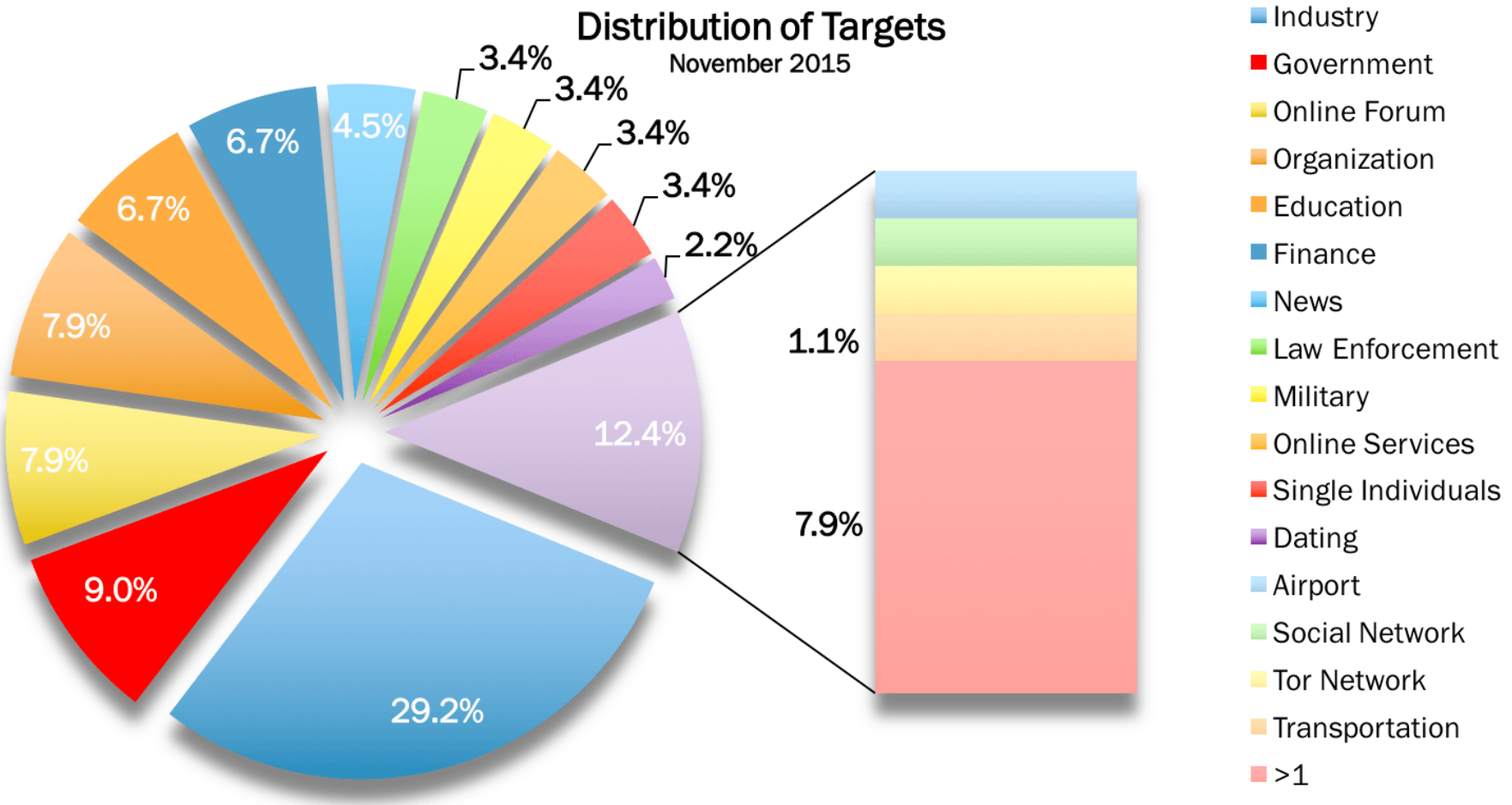
Ασκήσεις Κυβερνοάμυνας

- Διοργάνωση της Εθνικής Άσκησης Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ” (5 ασκήσεις μέχρι τώρα)
- Συμμετοχή στην Νατοϊκή άσκηση Κυβερνοάμυνας “Cyber Coalition” από το 2009
- Συμμετοχή στην άσκηση Κυβερνοάμυνας “Locked Shields” από το 2014
- Συμμετοχή στην Cyber Europe
- Συμμετοχή στην άσκηση Κυβερνοάμυνας “Crossed Swords 16”.
- Επόμενη Εθνική άσκηση κυβερνοάμυνας τον **Μάιο του 2016**.

Εθνική Άσκηση Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ”

Στατιστικά

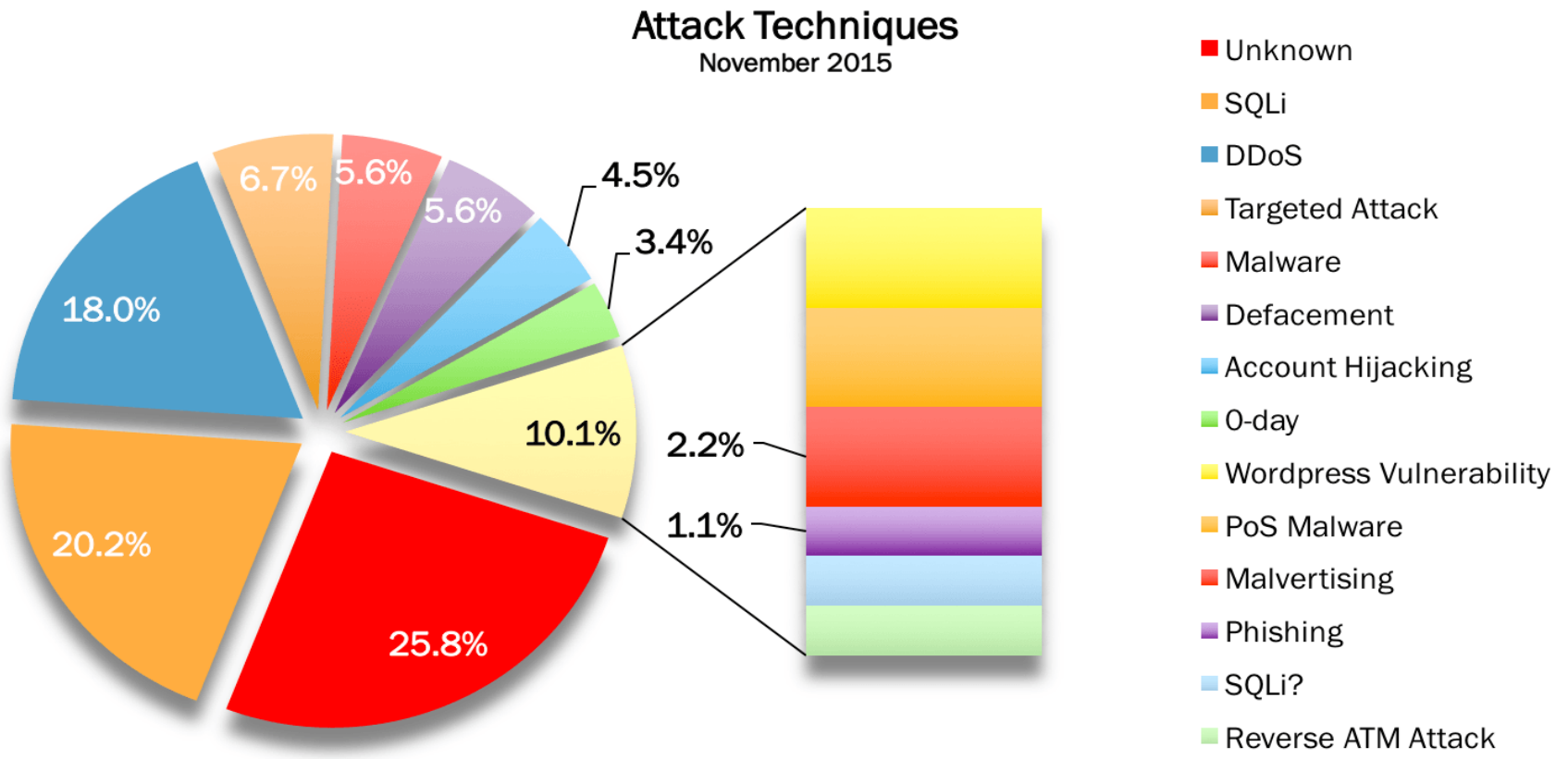
Στόχοι κυβερνοεπιθέσεων



Όλοι ειμαστε στόχοι, συνεπώς πρέπει να εκπαιδευτούμε!!

Source: Hackmageddon.com

Τεχνικές κυβερνοεπιθέσεων



Μεγάλο ποσοστό αγνώστων επιθέσεων, πρέπει να είμαστε σε θέση να τις αναγνωρίζουμε

Source: Hackmageddon.com

Άσκηση Κυβερνοάμυνας - ορισμός

√ Μία άσκηση κυβερνοάμυνας έχει σαν σκοπό να προσομοιώσει πραγματικές κυβερνοεπιθέσεις τις οποίες θα πρέπει να αντιμετωπίσουν οι επαγγελματίες των οργανισμών, στηριζόμενοι στην πολιτική τους.

√ Ως αντικειμενικός σκοπός των ασκήσεων κυβερνοάμυνας είναι να εξεταστούν οι διαδικασίες και οι δυνατότητες του οργανισμού, στην αντιμετώπιση των κυβερνοεπιθέσεων. Με λίγα λόγια, **δοκιμάζεται η ετοιμότητα ενός οργανισμού, στην αντιμετώπιση κυβερνοεπιθέσεων**

√ Τύποι ασκήσεων κυβερνοάμυνας:

- **Σε πραγματικό χρόνο**,
- **σε μη πραγματικό χρόνο**
- και **μεικτές**

Άσκηση πραγματικού χρόνου

Κόκκινη και μπλε ομάδα (Red & Blue Teams)

- Σκοπός η υπεράσπιση ενός εικονικού δικτύου, όπου γίνονται πραγματικές επιθέσεις και έχουμε πραγματικούς αμυνόμενους.

Προυποθέσεις:

- Κατάλληλη υποδομή (Cyber range)
- Πολύ καλή και έμπειρη κόκκινη ομάδα (Experienced Red Team)
- Πολύ ικανή τεχνική ομάδα (Green Team)

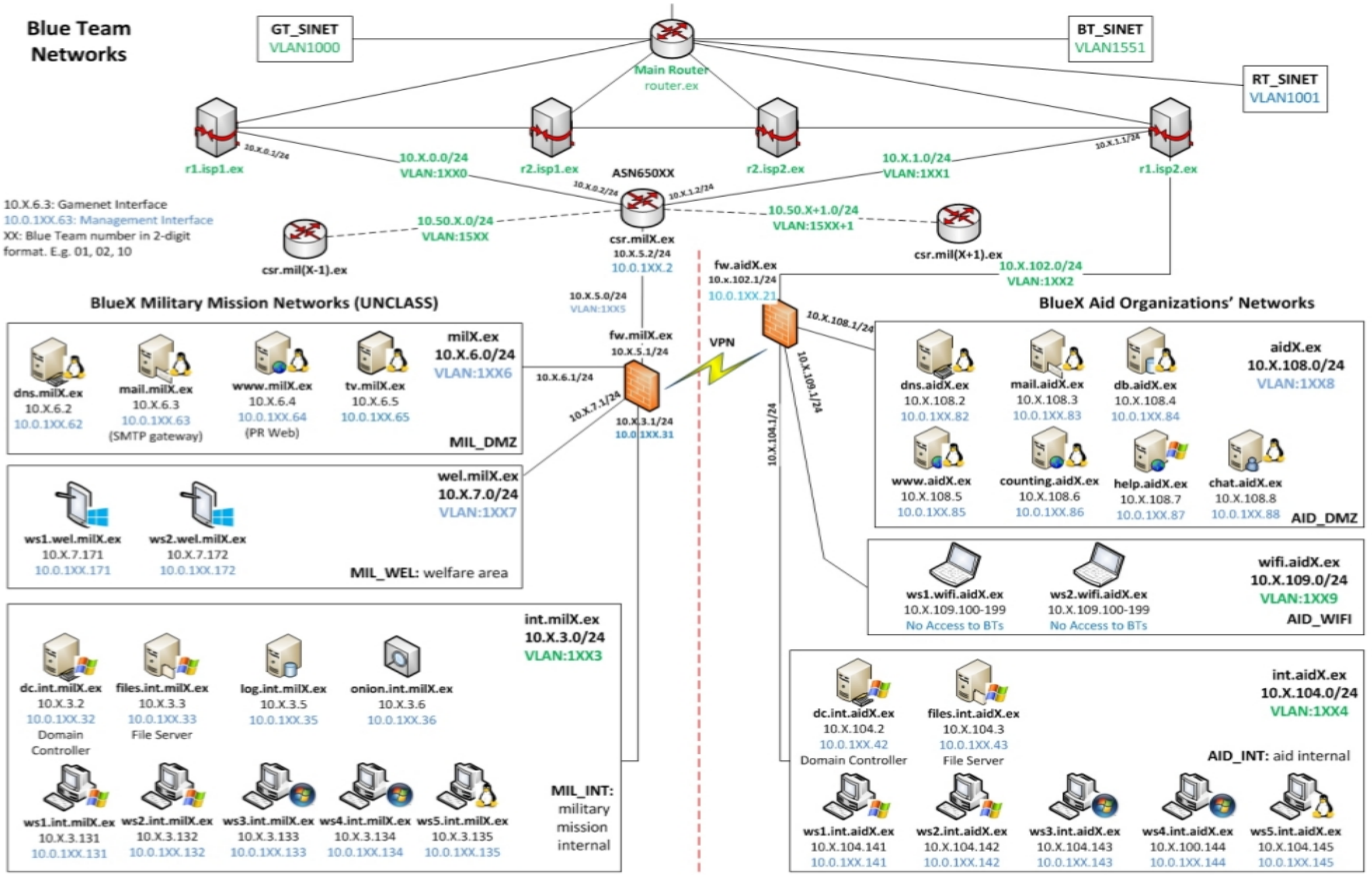
Πλεονεκτήματα:

- Πραγματικά επιθετικά επεισόδια, με δυνατότητα αλλαγής στρατηγικής επίθεσης.
- Πραγματικές καταστάσεις αντιμετώπισης κυβερνοεπιθέσεων.

Μειονεκτήματα:

- Σημαντικός χρόνος υλοποίησης, σχεδόν ένας χρόνος.
- Απαιτεί κατάλληλη υποδομή.
- Δεν περιλαμβάνει ανάλυση ιομορφικού λογισμικού και γενικότερα επεισόδια ψηφιακής σήμανσης.

Locked Shields 2013 (Blue Team Networks)



Άσκηση μη πραγματικού χρόνου

Επιδιώκουμε Αξιολόγηση:

- Των Διαδικασιών αντιμετώπισης κυβερνοεπιθέσεων (Incident handling process)
- Της Ψηφιακής σήμανσης (Digital forensics)
- Της Ανάλυσης ιομορφικού λογισμικού (Malware analysis)
- Των διαδικασιών αναφοράς - επικοινωνίας (Reporting → Follow procedures)
- Του τρόπου Διαμοιρασμού – ανταλλαγής των πληροφοριών

Προυποθέσεις:

- Χρήση των διαδικασιών του οργανισμού, εφαρμογή της πολιτικής κυβερνοασφάλειας και αναπτυγμένες δυνατότητες.

Πλεονεκτήματα:

- Μειωμένο χρόνο προετοιμασίας.
- Όχι υψηλές απαιτήσεις σε υποδομή (No specific infrastructure)
- Δοκιμάζονται οι δυνατότητες εντοπισμού, αντιμετώπισης και αναφοράς μιας κυβερνοεπίθεσης **που έχει ήδη συμβεί**.

Μειονεκτήματα:

- Δεν προσομοιώνει επιθέσεις σε πραγματικό χρόνο, θεωρούμε ότι έχει γίνει η κυβερνοεπίθεση.

Μεικτές ασκήσεις

Συνδυασμός των ασκήσεων πραγματικού και μη πραγματικού χρόνου.

Περιλαμβάνει επιθέσεις σε πραγματικό χρόνο και επίλυση επεισοδίων ψηφιακής σήμανσης, διαδικασιών αντιμετώπισης κυβερνοεπιθέσεων, ανάλυση ιομορφικού λογισμικού.

Πλεονεκτήματα:

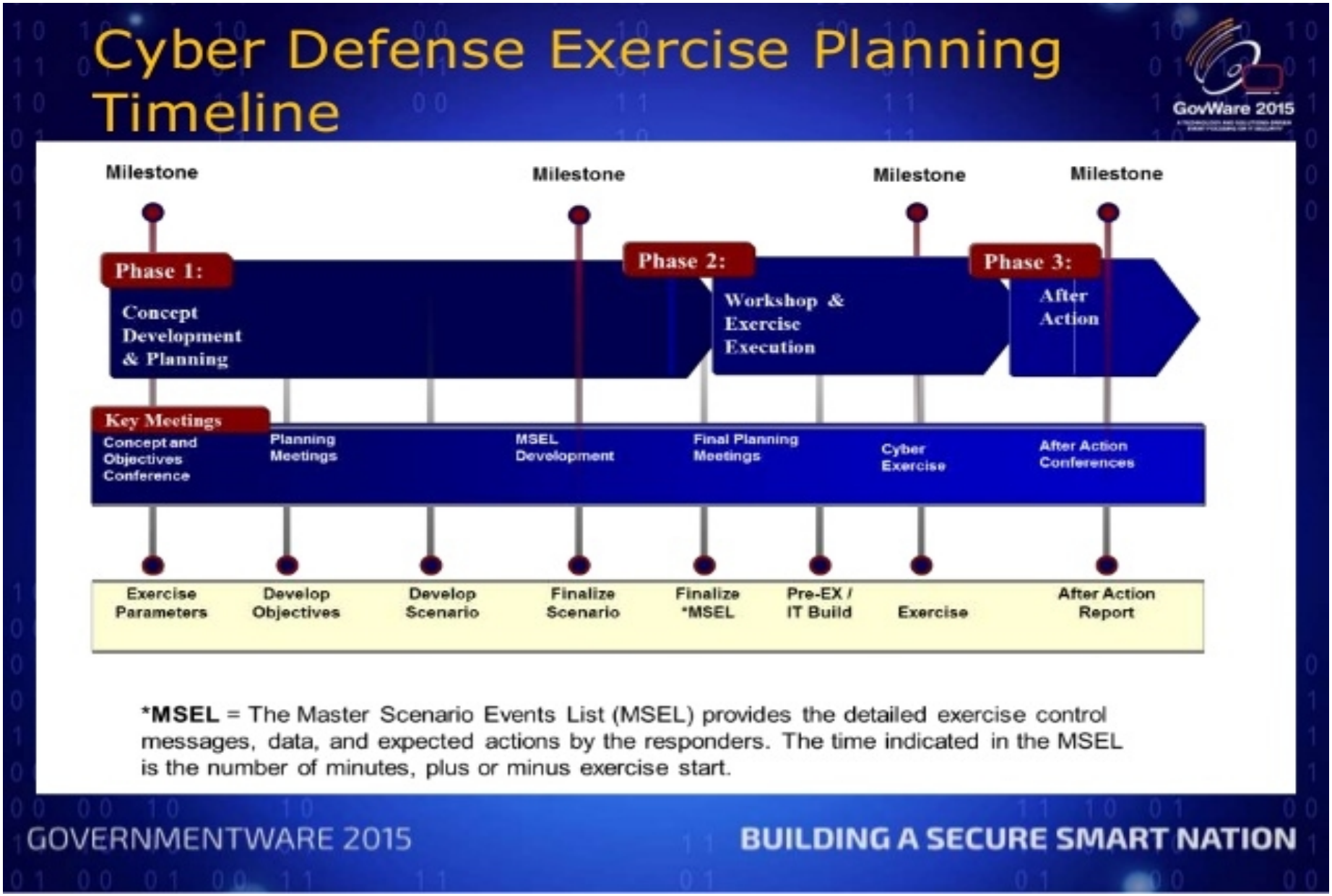
- Η πιο ολοκληρωμένη άσκηση

Μειονεκτήματα:

- Μεγάλος χρόνος προετοιμασίας.
- Απαιτεί υποδομή και σημαντικό αριθμό ειδικών.

Παράδειγμα: **Locked Shields**

Σχεδιασμός-οργάνωση μιας άσκησης κυβερνοάμυνας



Τρεις φάσεις, Σχεδιασμός, συναντήσεις και εκτέλεση, αναφορά αποτελεσμάτων

Ιστορία της Εθνικής άσκησης Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ”

Ελληνική Εθνική άσκηση Κυβερνοάμυνας
(Ελεύθερη συμμετοχή)

Διοργανώνεται κάθε χρόνο από το 2010
(Το ΓΕΕΘΑ/Ε6 (Διεύθυνση Κυβερνοάμυνας) 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.

ΠΑΝΟΠΤΗΣ: Γενική επισκόπηση

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 του διοργανωτή είναι να παραδώσει έγκαιρα τις λύσεις των επεισοδίων

ΠΑΝΟΠΤΗΣ: Συμμετέχοντες

200+ συμμετέχοντες από:

- ΕΔ και σώματα ασφαλείας
- Ακαδημαϊκό τομέα – ερευνητικά κέντρα
- Δημόσιο τομέα
- Εθνικές κρίσιμες υποδομές
- Ιδιωτικός τομέας

ΠΑΝΟΠΤΗΣ: Κατάσταση

Προσομοιώνουμε περίοδο κρίσης ή πολέμου, σε αυτή την περίπτωση:

Το **ΓΕΕΘΑ** έχει τον **έλεγχο** της Εθνικής Κυβερνοάμυνας, της αντιμετώπισης των κυβερνοεπιθέσεων σε Εθνικό επίπεδο.

ΠΑΝΟΠΤΗΣ: Αντικειμενικοι σκοποί σε στρατηγικό επίπεδο:

Εξάσκηση της εθνικής κοινότητας αντιμετώπισης κυβερνοεπιθέσεων με έμφαση στο:

- Συντονισμό των αρμοδίων φορέων στην αντιμετώπιση των κυβερνοεπιθέσεων σύμφωνα με το Εθνικό Σχέδιο Αντιμετώπισης (*θα πρέπει να έχουμε έτοιμο*).
- Εντοπισμό και βελτίωση των συνεργασιών μεταξύ ιδιωτικού, ακαδημαϊκού και δημοσίου τομέα, σε όλα τα επίπεδα.
- Εντοπισμό τυχόν αδυναμιών παραλήψεων όσο αφορά τις διαδικασίες, νομικές πτυχές που έχουν επίπτωση στην αντιμετώπιση.
- Εντοπισμό των διαδικασιών και των καναλιών επικοινωνίας για τον σωστό διαμοιρασμό των πληροφοριών.

Προβολή της σημαντικότητας των κυβερνοεπιθέσεων και της επίπτωσής τους σε Εθνικό επίπεδο.

ΠΑΝΟΠΤΗΣ: Αντικειμενικοι σκοποί σε τακτικό-τεχνικό επίπεδο:

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 σχηματίσουμε ομάδες ταχείας αντίδρασης όταν απαιτείται, αλλά και την αποθήκευση των συμπερασμάτων.

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: Οργάνωση-σχεδιασμός

Έξι (6) μήνες σχεδιασμού και προετοιμασίας

Δύο (2) διαφορετικές ομάδες
Μια τεχνική ομάδα, με αποστολή την υλοποίηση των τεχνικών σεναρίων
Μια οργανωτική ομάδα, με αποστολή να καθορίσει τους στόχους (αντικειμενικούς σκοπούς) της άσκησης

Τρεις (3) συναντήσεις για να σχεδιάσουμε και να καθορίσουμε τους στόχους της άσκησης

Έξι (6) μήνες για την προετοιμασία και τη συνεργασία, για την υλοποίηση των τεχνικών σεναρίων

ΠΑΝΟΠΤΗΣ: Τελική συνάντηση

Παρέχονται οδηγίες:

- **διεξαγωγής** της άσκησης (Επικοινωνία, υποδομή) αλλά και
- **εργαλεία - τεχνικές** για την επίλυση των τεχνικών επεισοδίων.

Επιλύονται απορίες της τελευταίας στιγμής.

ΠΑΝΟΠΤΗΣ: 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

- MISP (Malware Information Sharing Platform)
- email
- Live chat

Το μέλλον

- Σκοπός να γίνει ο ΠΑΝΟΠΤΗΣ μεικτή άσκηση σε συνεργασία με **ΕΔΕΤ** και **CCDCOE** (συνδυασμός επεισοδίων σε πραγματικό και μη χρόνο).
- Συνεχής βελτίωση των επεισοδίων
- Μέγιστη συμμετοχή

- Ολοκλήρωση και σωστή εφαρμογή των διαδικασιών αντιμετώπισης κυβερνοεπιθέσεων σε Εθνικό επίπεδο μέσα από ένα Εθνικό σχέδιο αντιμετώπισης.

Συμπεράσματα:

- Το σημαντικότερο είναι η **επικοινωνία** και ο **συντονισμό**ς στην περίπτωση των κυβερνοεπιθέσεων.
- Θα πρέπει να γνωρίζουμε από πριν τα κανάλια επικοινωνίας, τις μεθόδους, τα μέσα και τα πρωτόκολλα, πριν από την ανάγκη αντιμετώπισης των κυβερνοεπιθέσεων.
- Θα πρέπει να γνωρίζουμε από πριν:
    - **Με ποιον πρέπει να μιλήσω, πότε και με πιο τρόπο.**

- Ο Συντονισμός της αντιμετώπισης των κυβερνοπεριστατικών είναι πολύ σημαντικός και σχετίζεται άμεσα με τον χρόνο.

- Τυποποιημένες Διαδικασίες Λειτουργίας (SOP) πρέπει να εκπονηθούν εκ των προτέρων.

Συμπεράσματα:

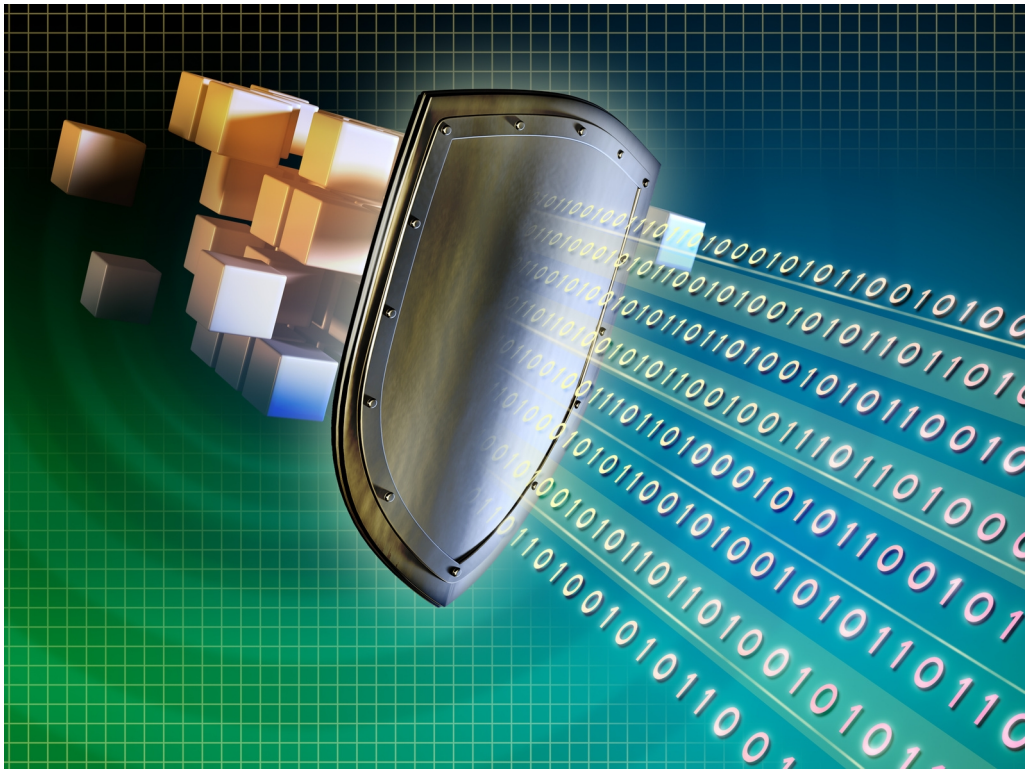
Οι ασκήσεις στον κυβερνοχώρο, παρέχουν τα μέσα για την αξιολόγηση:

- **του προσωπικού (χρήστες και εμπειρογνώμονες),**
- **των διαδικασιών**
- **και των υποδομών.**

Μπορούν να πραγματοποιηθούν σε διεθνές, εθνικό και σε επίπεδο οργανισμού.

Αποτελούν έναν πρακτικό τρόπο για έναν οργανισμό να αξιολογήσει την οργάνωση και την ικανότητα αντιμετώπισης κυβερνοεπιθέσεων.

ΠΑΝΟΠΤΗΣ 2016



ΠΑΝΟΠΤΗΣ 16

Ημερομηνία διεξαγωγής:**23-27 Μαΐου 2016**

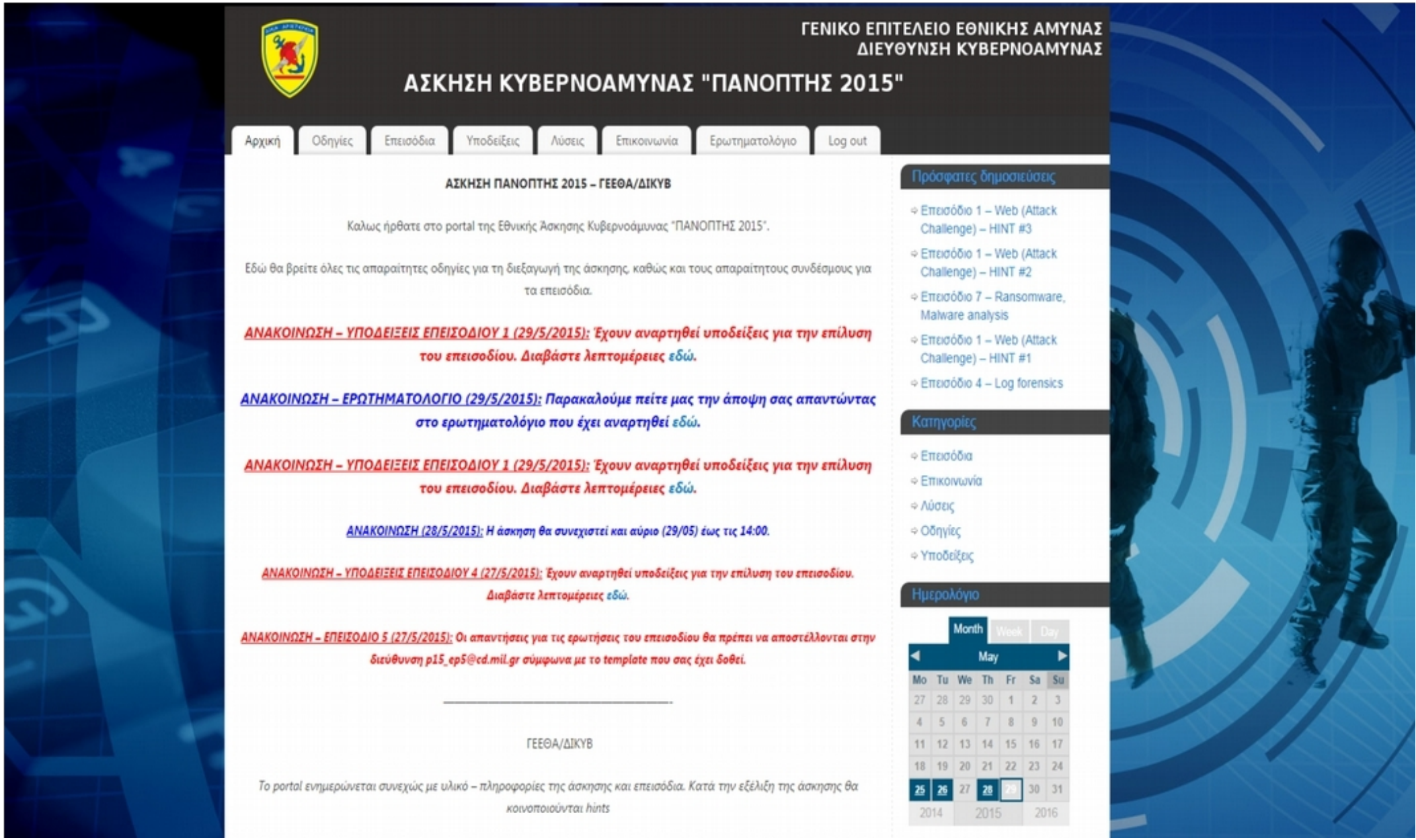
Κεντρική συνάντηση: **23 Μαρτίου**

Τελική συνάντηση: **18 Μαΐου**

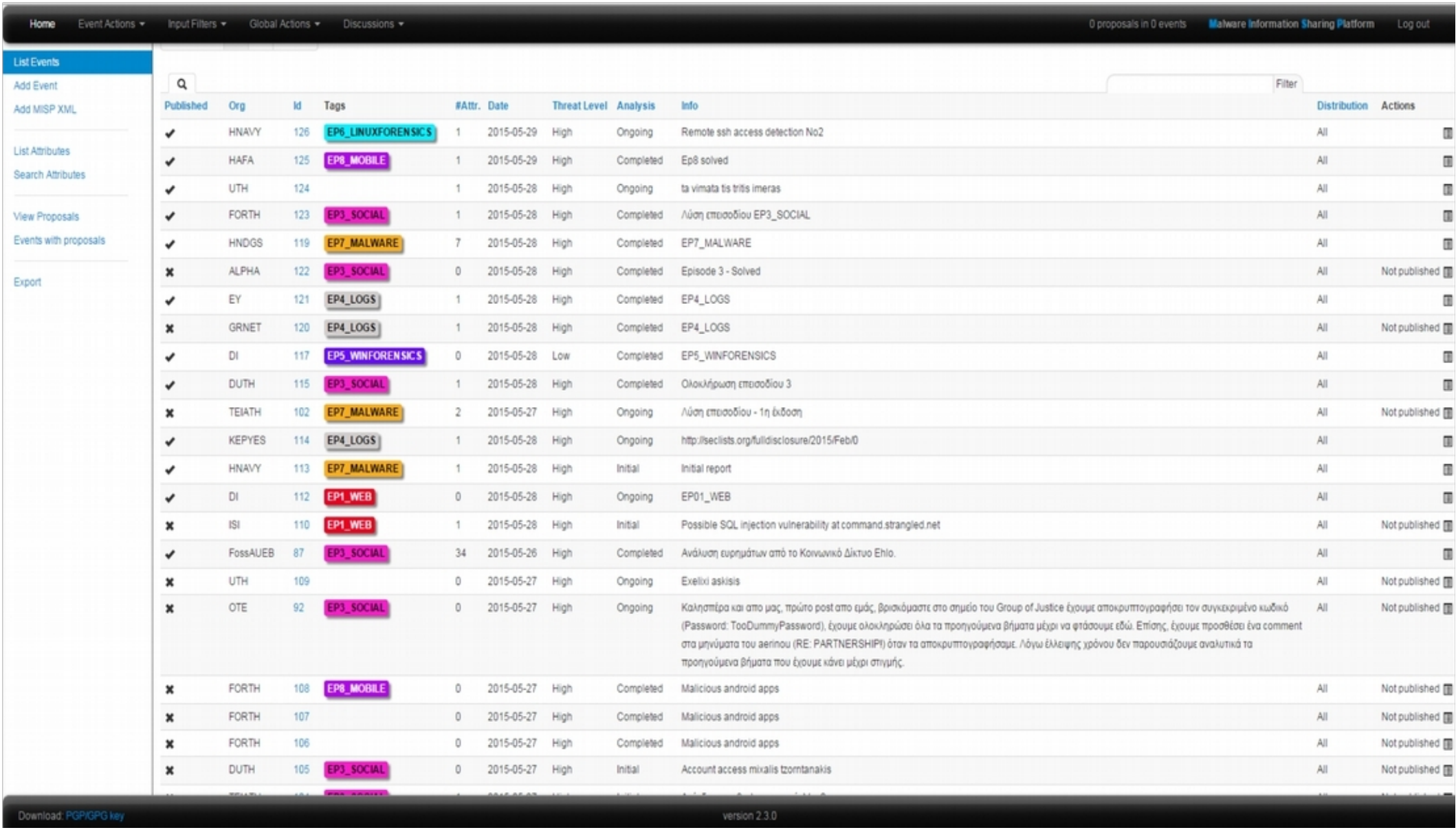
ΠΑΝΟΠΤΗΣ 16
Σκοπός

- Η εξάσκηση των συμμετεχόντων σε τεχνικά θέματα.
- Η συνεργασία μεταξύ των παικτών σε τεχνικό και διαδικαστικό επίπεδο.
- Ο διαμοιρασμός τεχνικών, ιδεών και διαδικασιών αντιμετώπισης 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.

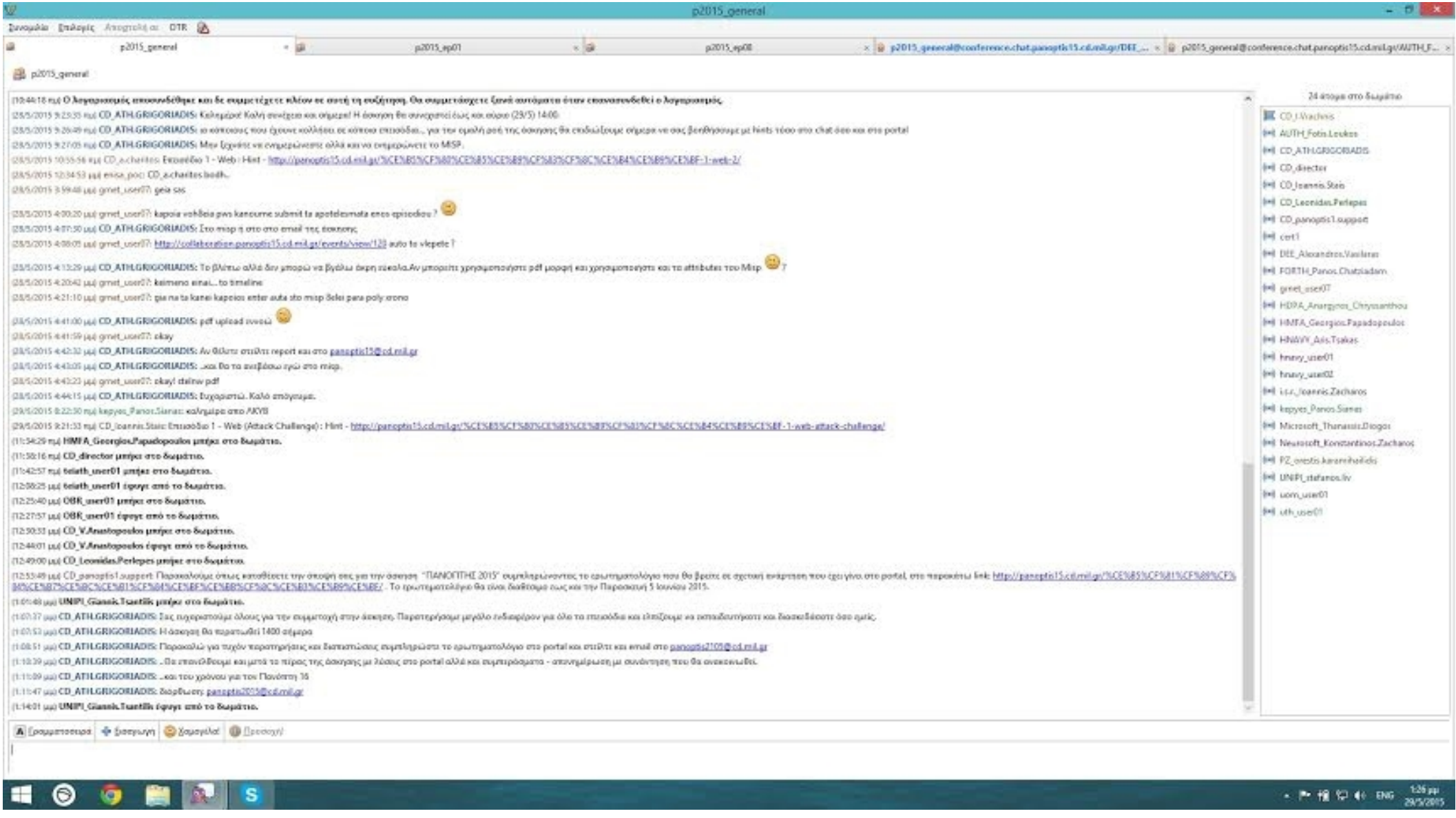
ΠΑΝΟΠΤΗΣ 16
Επικοινωνία-Portal



ΠΑΝΟΠΤΗΣ 16
Επικοινωνία-MISP



ΠΑΝΟΠΤΗΣ 16
Επικοινωνία-CHAT



Γενικές Οδηγίες συμμετοχής - Επικοινωνίας

Υποβολή ανά φορέα:
- Email συμμετεχόντων
- Ένα τηλέφωνο επικοινωνίας (σταθερό)

User name και password θα αποσταλούν από διοργανωτές στα ανωτέρω email

Τυποποίηση Ονομάτων
- [Φορέας]_[Όνομα].[Επώνυμο]
  - Dimokritos_Giannis.Agiannis
  - Unipi_Fotis.Karafotis

Στοιχεία επικοινωνίας διοργανωτών:
- panoptis16@cd.mil.gr,
- 210 657 6150

Δήλωση συμμετοχής:
Συμμετοχή στα emails: cd1@cd.mil.gr, mcirc@cd.mil.gr

Επεισόδια ΠΑΝΟΠΤΗ 16

Τύπος	**Αρ. Επεισοδίου**
Web Application Security – Active Response	1
Windows Forensics Analysis	2
Linux Forensics Analysis	3
Mobile Forensics Analysis	4
Network Forensics Analysis	5
Data Leakage Investigation Analysis	6
Capture the Flag	7

Web Application Security – Active Response

Σενάριο: Αποτέλεσμα κάποιων κακόβουλων επιθέσεων είναι η διακοπή κάποιων δικτυακών κυβερνητικών υπηρεσιών. Κάποιοι εξυπηρετητές (server hosts) αναγνωρίζονται ως η πηγή αυτών των επιθέσεων.

Οι παίκτες καλούνται να εκτελέσουν «επίθεση» (να αποκτήσουν πρόσβαση) στους ήδη αναγνωρισμένους στόχους (servers) προκειμένου να τερματιστεί η κακόβουλη δραστηριότητα.

Δεδομένα:

Δύο συστήματα (στόχοι) τα οποία θα είναι ενεργά και θα περιέχουν τις αδυναμίες προς ανάλυση.

Ζητούμενα:

Να εντοπιστούν και να επιβεβαιωθούν (exploitation) οι αδυναμίες στα συστήματα.

Windows Forensics Analysis

Δεδομένα:

Ένα virtual image (win 8) 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

Mobile Forensics Analysis

Κινητή συσκευή (OS Android) έχει προεγκατεστημένες 2 εφαρμογές οι οποίες φαίνεται πως χρησιμοποιούνταν από τους χρήστες κινητών τηλεφώνων για να αποθηκεύουν αρχεία με ασφάλεια.

Οι εφαρμογές δεν είναι δημόσια διαθέσιμες στο GooglePlay. - Μετά από επιτυχημένη εξαγωγή (extract) των *.apk αρχείων των εφαρμογών απεστάλησαν με ασφαλή τρόπο στην Ομάδα Αντιμετώπισης.

Δεδομένα:

APK αρχεία

Ζητούμενα:

Α' φάση (basic)

Ανάλυση λειτουργίας εφαρμογών.

Εντοπισμός αδυναμιών.

Β' φάση (advanced)

Δημιουργία εφαρμογής για εκμετάλλευση των αδυναμιών που εντοπίστηκαν και η οποία θα υποκλέπτει τα δεδομένα σε plain text.

Θα υποβληθούν το αρχείο .apk και ο πηγαίος κώδικας.

Network Forensics Analysis

Δεδομένα:
Network packet captures (.pcap) από DMZ και LAN

Ζητούμενα:
• Υπάρχουν ενδείξεις για την μόλυνση ενός συγκεκριμένου συστήματος κατόπιν διερεύνησης.
• Η αρχική διερεύνηση έδειξε ύποπτες TCP συνδέσεις.
• Η ομάδα αντιμετώπισης περιστατικών υποθέτει ότι ο μολυσμένος υπολογιστής είναι μέλος ενός δικτύου διοίκησης και ελέγχου (Command and Control network) και καλείται να διερευνήσει τα στοιχεία.

Τελικό παραδοτέο η αποστολή αναφοράς της συνολικής διερεύνησης.

Data Leakage Investigation Analysis

Από το εσωτερικό δίκτυο οργανισμού αποστέλλονται προς άγνωστο εξωτερικό παραλήπτη τέσσερα (4) e-mail με συνημμένες φωτογραφίες και αρχεία κειμένου.
Μετά από έλεγχο στην εξερχόμενη αλληλογραφία του συγκεκριμένου χρήστη, διαπιστώθηκε πως τους τελευταίους δύο (2) μήνες έχει γίνει ασυνήθιστη ανταλλαγή e-mail τέτοιας μορφής καθώς και δημιουργία προφίλ σε σελίδα κοινωνικής δικτύωσης χωρίς να υπάρχει κάποιο εμφανές περιεχόμενο.
Πραγματοποιείται έλεγχος στα εξερχόμενα συνημμένα, εάν σχετίζονται μεταξύ τους και ίσως να αφορούν υποκλοπή ευαίσθητων δεδομένων του οργανισμού.

Δεδομένα:
- Ένα αρχείο pcap από την κίνηση του εσωτερικού δικτύου και το mailbox.

Ζητούμενα:
- τα στοιχεία εκείνα που αποδεικνύουν τυχόν ύποπτη ενέργεια εις βάρος του οργανισμού .

Capture the Flag – Find the Insider

Διαβαθμισμένα αρχεία έχουν διαρρεύσει από οργανισμό που στο παρελθόν έχει υλοποιήσει projects των ενόπλων δυνάμεων της χώρας.

Το τεχνικό προσωπικό υπολείπεται τεχνικών γνώσεων για να λυθεί η υπόθεση και υπάρχει έλλειψη εμπιστοσύνης στους υπαλλήλους.

Ο παίκτης εξουσιοδοτείται από τον ιδιοκτήτη και CEO της εταιρείας ως εξωτερικός συνεργάτης να διεξάγει ένα penetration test - incident handling, προκειμένου να διαλευκάνει την υπόθεση.

ΣΚΟΠΟΣ - ΣΤΟΧΟΣ

Ο εντοπισμός των ευπαθειών των συστημάτων και του τρόπου που διέρρευσαν τα διαβαθμισμένα αρχεία καθώς και του ατόμου που βοήθησε στη διαρροή.

Στον παίκτη θα δοθεί μια λίστα από υπάλληλους που χρήζουν ιδιαίτερης προσοχής

Capture the Flag – Find the Insider

- Ο κάθε παίκτης έχει εξουσιοδότηση για συγκεκριμένες ενέργειές μέσα στο δίκτυο της εταιρείας.

- Οι συμμετέχοντες καλούνται να ανακαλύψουν και να χρησιμοποιήσουν τις τρωτότητες των συστημάτων και του συγκεκριμένου δικτύου ώστε να αποκτήσουν πρόσβαση σε αυτά και να ανακαλύψουν στοιχεία.

- Η εκμετάλλευση κάθε τρωτότητας και η αντίστοιχη εύρεση κάποιου στοιχείου αποτελεί το flag του αντίστοιχου μηχανήματος.

- Η συλλογή των flags που υπάρχουν στο επεισόδιο, αποτελούν τμήμα ενός συνολικού παζλ το οποίο θα κατευθύνει τον διαγωνιζόμενο στην σωστή λύση.

- Θα υπάρχει και πίνακας βαθμολόγησης για την επαλήθευση των flags και την επιβράβευση των παικτών.

ΕΕΛΛΑΚ και ΠΑΝΟΠΤΗΣ

- Από το 2012 συμμετοχή στις ασκήσεις
- Έχει δημιουργήσει Ομάδα για την Ασφάλεια Πληροφοριακών Συστημάτων
- Στόχος η συγκέντρωση των εργαλείων ανοικτού κώδικα που αφορούν την ασφάλεια
- Σύνδεση ανοικτής διακυβέρνησης με θέματα ασφάλειας
- Προτάσεις Πολιτικής προς την πολιτική ηγεσία
- Λίστα αλληλογραφίας της ομάδας εργασίας της ΕΕΛ/ΛΑΚ για την Ασφάλεια Πληροφοριακών Συστημάτων και Προστασία Προσωπικών Δεδομένων **wg-privacy@ellak.gr**

ΕΕΛΛΑΚ και ΠΑΝΟΠΤΗΣ 2016

- Recruiting

- Δίνουμε την δυνατότητα σε όποιον θέλει να συμμετάσχει στην άσκηση να το κάνει μέσω της ΕΕΛΛΑΚ

- Αποκλειστικά με εργαλεία ανοικτού κώδικα

- Συμμετοχή με αποστολή mail στο info@ellak.gr με τίτλο **ΠΑΝΟΠΤΗΣ 2016** και με στοιχεία
  - Όνομα Επίθετο
  - Τηλέφωνο Επικοινωνίας
  - Επεισόδια της άσκησης που θα θέλατε να συμμετέχετε
  - Τύπος συμμετοχής (Active - Παρατηρητής)
  - Λίγα λόγια για εσάς (προαιρετικό)

- Καταληκτική ημερομηνία συμμετοχής 1 Μαΐου 2016

ΕΕΛΛΑΚ και ΠΑΝΟΠΤΗΣ 2016

- Η συμμετοχή στην άσκηση θα γίνει με φορητούς προσωπικούς υπολογιστές τους συμμετέχοντα
- Προσυνάντηση 10 Μαϊου 2016 – Οργάνωση επόμενων συναντήσεων
- Παροχή σεναρίων παλαιότερων ασκήσεων
- Δοκιμή όλων των εργαλείων
- Εγκατάσταση και προετοιμασία
- Χώρος άσκησης – Θα ανακοινωθεί (Innovathens ή ακαδημαϊκό ίδρυμα στην Αθήνα)
- Προσπάθεια για συμμετοχή σε όλα τα σενάρια
- Στόχος η διατήρηση της ομάδας και μετά την άσκηση

Εργαλεία – Τεχνικές Ικανότητες

Εργαλεία

Forensics live cd

- SIFT v3 (http://digital-forensics.sans.org/community/downloads)

Memory analysis

- Volatility
- Rekall (http://www.rekall-forensic.com/)
- Mandiant RedLine

Registry analysis

- Reg ripper

File system analysis

- AUTOPSY
- Sleuth kit
- FTK Imager
- Bulk Extractor

Reverse malware

- Remnux live cd (https://remnux.org/)
- Ida pro
- Immunity debugger
- Olly debugger

Εργαλεία

Android analysis live cd

Androl4b (https://github.com/sh4hin/Androl4b)

Santoku (https://santoku-linux.com/)

MobSF (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF)

Network Forensic Analysis Tool (NFAT)

Xplico

Live response tools

https://www.brimorlabs.com/Tools/LiveResponseCollection-Allosaurus.zip

Ικανότητες

Η ομάδα αντιμετώπισης θα πρέπει να περιλαμβάνει άτομα που θα έχουν συνολικά τις παρακάτω ικανότητες:

- Incident handling
- Forensics windows
- Forensics Linux
- Forensics Network
- Forensics mobile
- Reversing malware
- Penetration test (system +network)
- Penetration test (WEB)
- Penetration test (MOBILE)

Επίλογος

Η Εθνική άσκηση κυβερνοάμυνας έχει σαν σκοπό να βοηθήσει στην ατομική και συλλογική βελτίωση των ικανοτήτων αντιμετώπισης των κυβερνοεπιθέσεων

Είναι ανοικτή με ελεύθερη συμμετοχή σε όλα τα επίπεδα (οργανωτικά, τεχνικά).

Διεξάγεται κάθε χρόνο και έχει σαν στόχο να βελτιώνεται.

Η πρόσκληση περιλαμβάνει όλους

Ερωτήσεις;