

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/teχνiko_sxedio_drasis_gia_tin_anaptixi_ki_vernoaminas_stis_ED.pdf)
- Τεχνικό εγχειρίδιο ασφαλείας
(http://www.geetha.mil.gr/files/it_security/teχνiko-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)

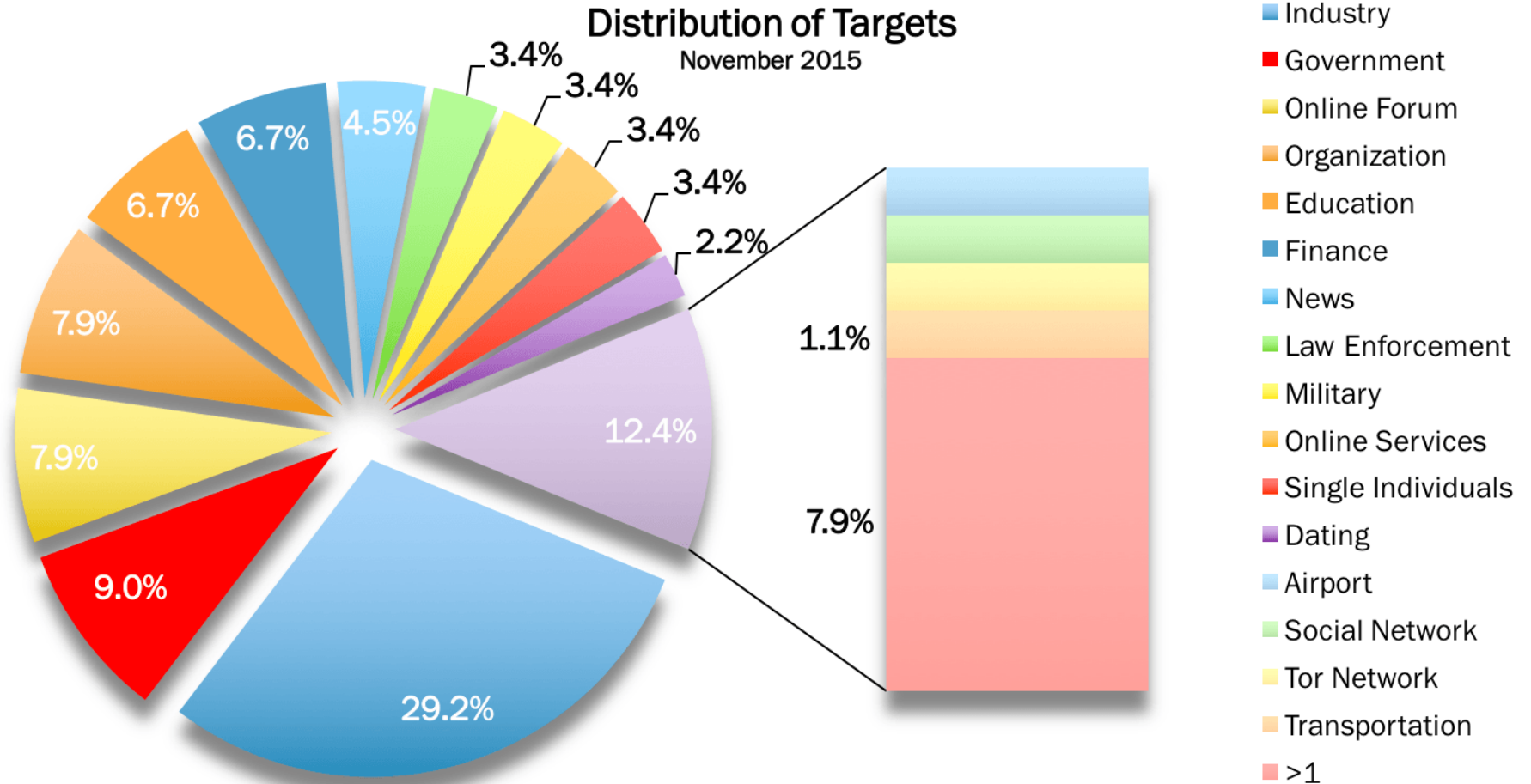
Ασκήσεις Κυβερνοάμυνας

- 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”

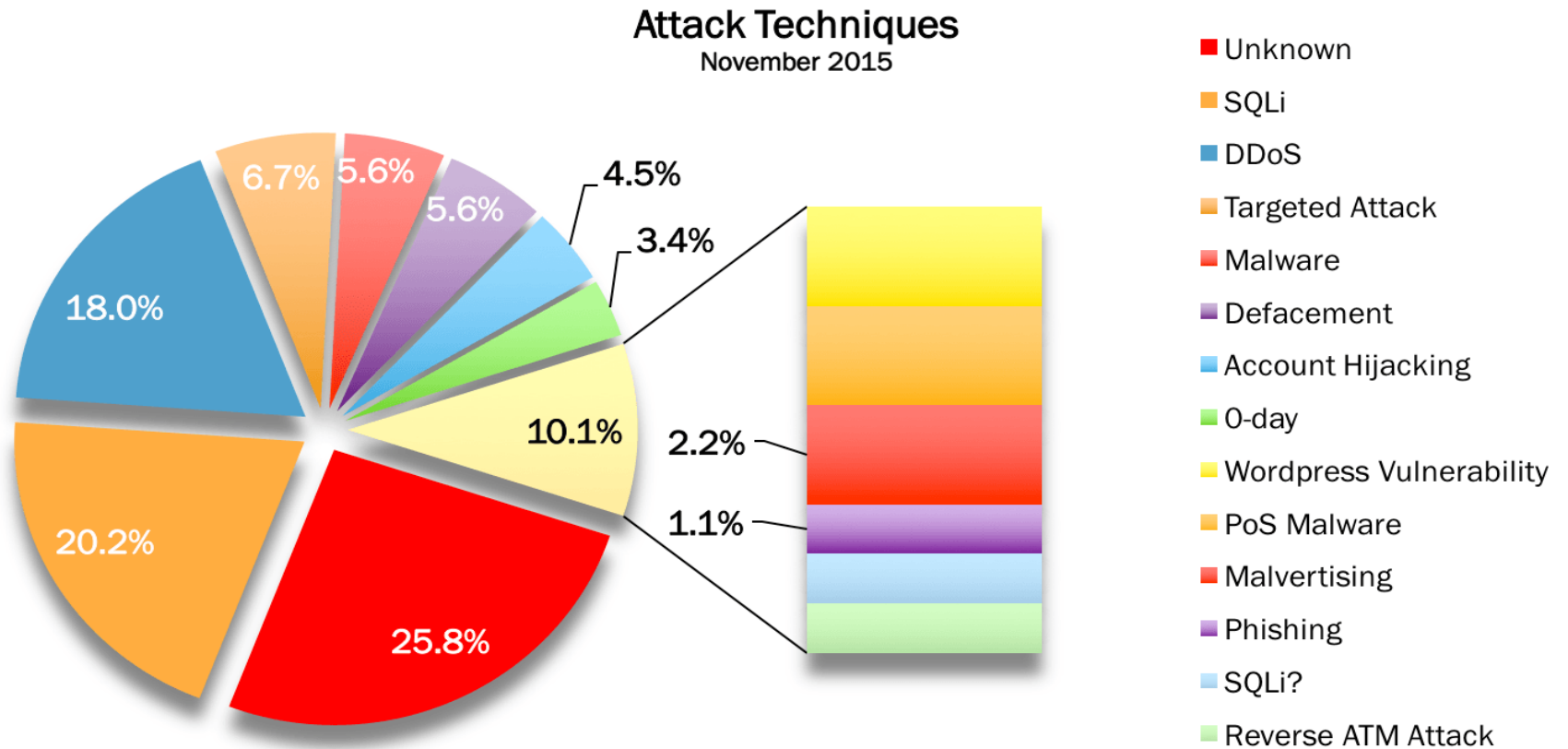
Στατιστικά

Στόχοι κυβερνοεπιθέσεων



Όλοι είμαστε στόχοι, συνεπώς πρέπει να εκπαιδευτούμε!!

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:

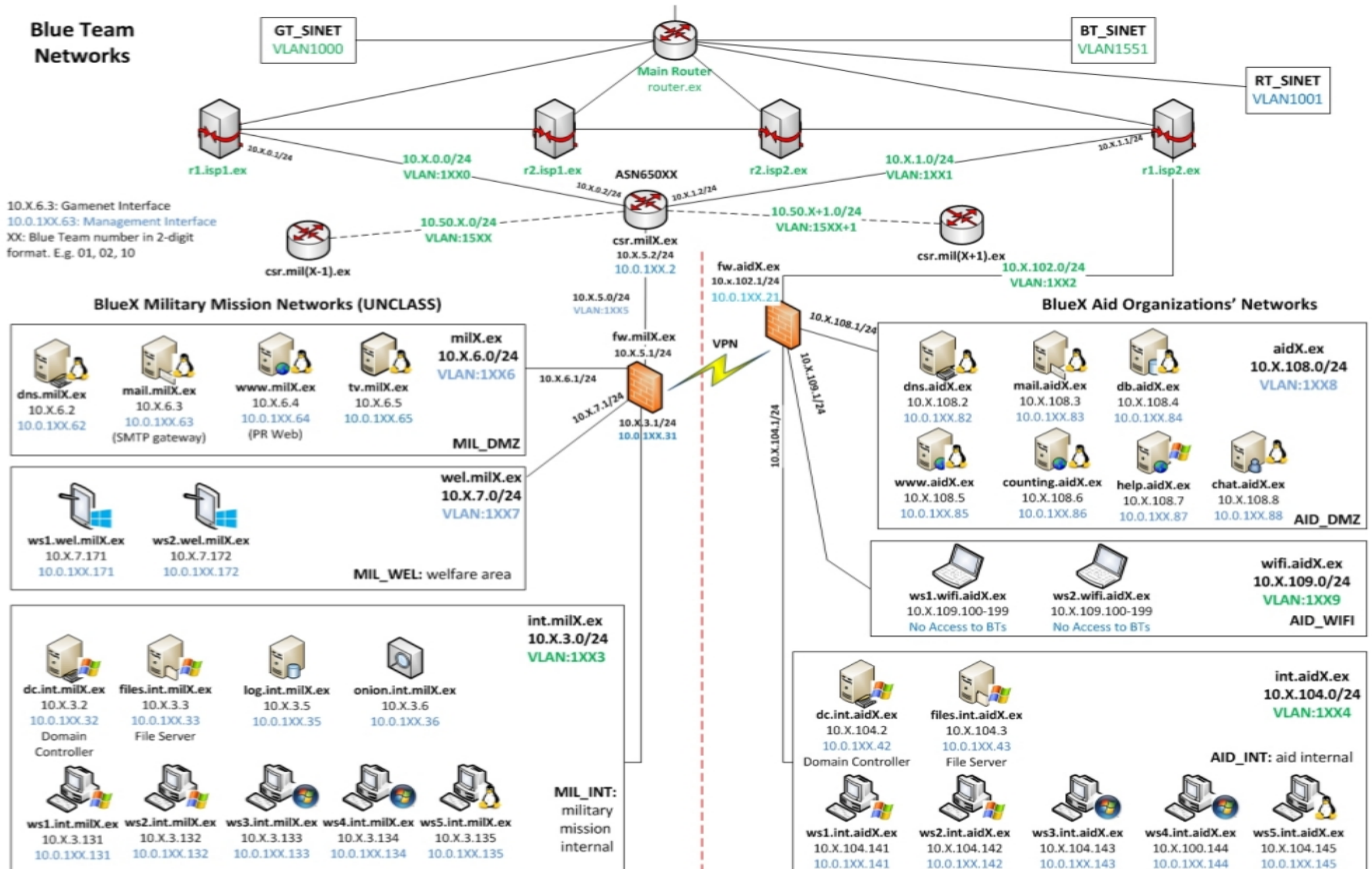
- ❖ Πραγματικά επιθετικά επεισόδια, με δυνατότητα αλλαγής στρατηγικής επίθεσης.
- ❖ Πραγματικές καταστάσεις αντιμετώπισης κυβερνοεπιθέσεων.

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)

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:

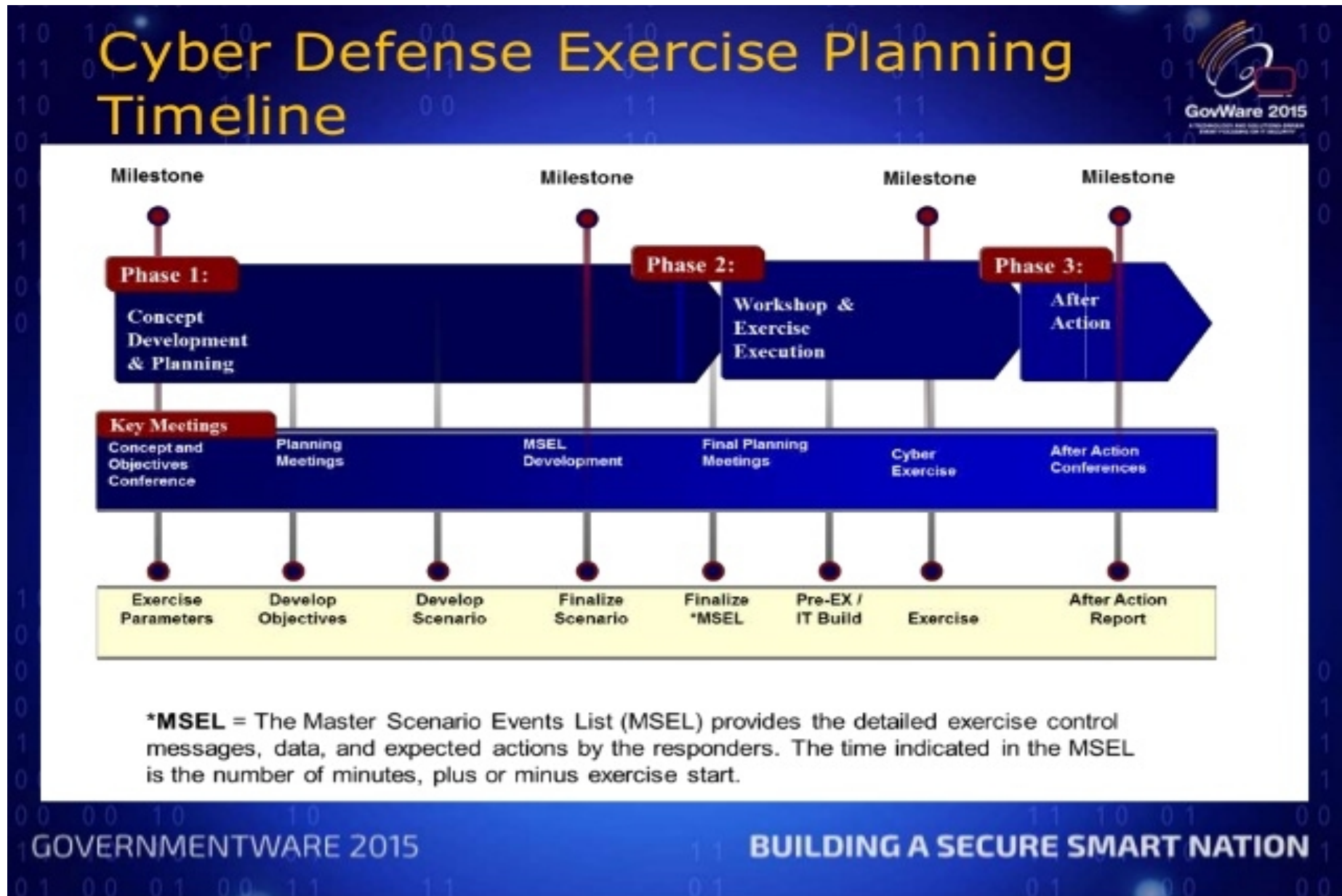
- ❖ Η πιο ολοκληρωμένη άσκηση

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: Αντικειμενικοί 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: Αντικειμενικοί 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-Επείσοδια

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 **συντονισμός** 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:

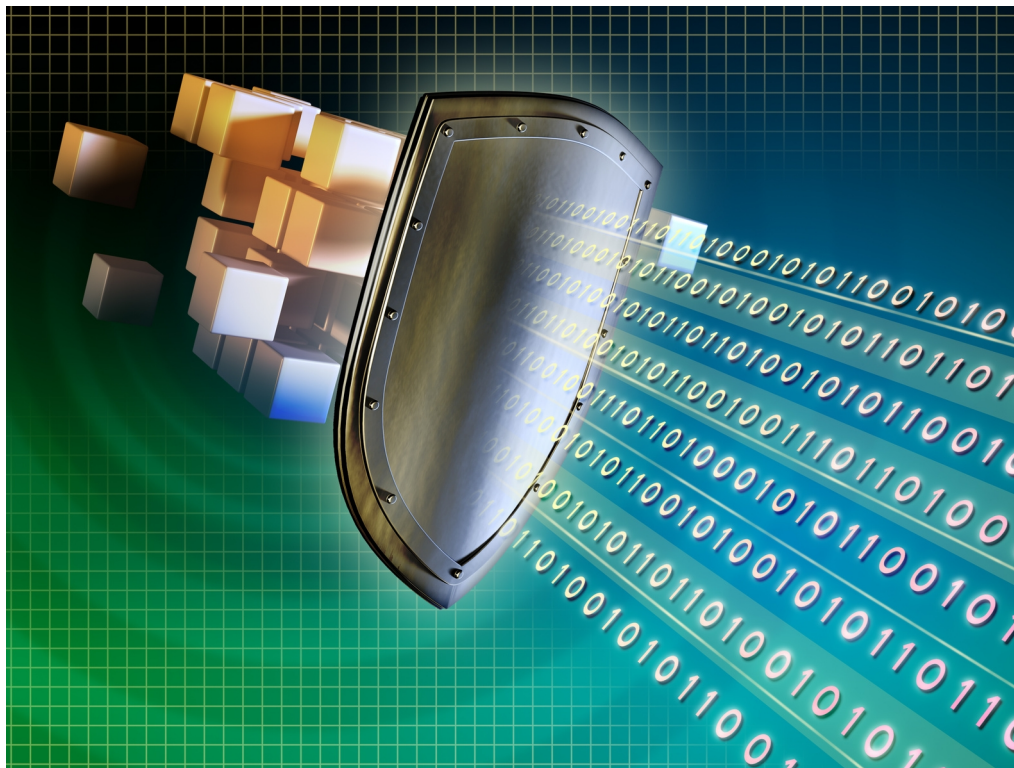
Οι ασκήσεις στον κυβερνοχώρο, παρέχουν τα μέσα για την αξιολόγηση:

- **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

ΣΚΟΠΟΣ

- 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



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΑΣΚΗΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ "ΠΑΝΟΠΤΗΣ 2015"

Αρχική Οδηγίες Επεισόδια Υποδείξεις Λύσεις Επικοινωνία Ερωτηματολόγιο Log out

ΑΣΚΗΣΗ ΠΑΝΟΠΤΗΣ 2015 – ΓΕΕΘΑ/ΔΙΚΥΒ

Καλώς ήρθατε στο portal της Εθνικής Άσκησης Κυβερνοάμυνας "ΠΑΝΟΠΤΗΣ 2015".

Εδώ θα βρείτε όλες τις απαραίτητες οδηγίες για τη διεξαγωγή της άσκησης, καθώς και τους απαραίτητους συνδέσμους για τα επεισόδια.

ΑΝΑΚΟΙΝΩΣΗ – ΥΠΟΔΕΙΞΕΙΣ ΕΠΕΙΣΟΔΙΟΥ 1 (29/5/2015): Έχουν αναρτηθεί υποδείξεις για την επίλυση του επεισοδίου. Διαβάστε λεπτομέρειες [εδώ](#).

ΑΝΑΚΟΙΝΩΣΗ – ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ (29/5/2015): Παρακαλούμε πείτε μας την άποψη σας απαντώντας στο ερωτηματολόγιο που έχει αναρτηθεί [εδώ](#).

ΑΝΑΚΟΙΝΩΣΗ – ΥΠΟΔΕΙΞΕΙΣ ΕΠΕΙΣΟΔΙΟΥ 1 (29/5/2015): Έχουν αναρτηθεί υποδείξεις για την επίλυση του επεισοδίου. Διαβάστε λεπτομέρειες [εδώ](#).

ΑΝΑΚΟΙΝΩΣΗ (28/5/2015): Η άσκηση θα συνεχιστεί και αύριο (29/05) έως τις 14:00.

ΑΝΑΚΟΙΝΩΣΗ – ΥΠΟΔΕΙΞΕΙΣ ΕΠΕΙΣΟΔΙΟΥ 4 (27/5/2015): Έχουν αναρτηθεί υποδείξεις για την επίλυση του επεισοδίου. Διαβάστε λεπτομέρειες [εδώ](#).

ΑΝΑΚΟΙΝΩΣΗ – ΕΠΕΙΣΟΔΙΟ 5 (27/5/2015): Οι απαντήσεις για τις ερωτήσεις του επεισοδίου θα πρέπει να αποστέλλονται στην διεύθυνση p15_ep5@cd.mil.gr σύμφωνα με το template που σας έχει δοθεί.

ΓΕΕΘΑ/ΔΙΚΥΒ

Το portal ενημερώνεται συνεχώς με υλικό – πληροφορίες της άσκησης και επεισόδια. Κατά την εξέλιξη της άσκησης θα κοινοποιούνται hints

Πρόσφατες δημοσιεύσεις

- Επεισόδιο 1 – Web (Attack Challenge) – HINT #3
- Επεισόδιο 1 – Web (Attack Challenge) – HINT #2
- Επεισόδιο 7 – Ransomware, Malware analysis
- Επεισόδιο 1 – Web (Attack Challenge) – HINT #1
- Επεισόδιο 4 – Log forensics

Κατηγορίες

- Επεισόδια
- Επικοινωνία
- Λύσεις
- Οδηγίες
- Υποδείξεις

Ημερολόγιο

Month Week Day						
May						
Mo	Tu	We	Th	Fr	Sa	Su
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
2014	2015			2016		

ΠΑΝΟΠΤΗΣ 16

Επικοινωνία-MISP

Home

Event Actions

Input Filters

Global Actions

Discussions

0 proposals in 0 events

Malware Information Sharing Platform

Log out

List Events

Add Event

Add MISP XML

List Attributes

Search Attributes

View Proposals

Events with proposals

Export

Q

Filter

Published	Org	Id	Tags	#Attr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	HNAVY	126	EP6_LINUXFORENSICS	1	2015-05-29	High	Ongoing	Remote ssh access detection No2	All	
✓	HAFA	125	EP8_MOBILE	1	2015-05-29	High	Completed	Ep8 solved	All	
✓	UTH	124		1	2015-05-28	High	Ongoing	ta vimata tis tritis imeras	All	
✓	FORTH	123	EP3_SOCIAL	1	2015-05-28	High	Completed	Λύση επεισοδίου EP3_SOCIAL	All	
✓	HNDGS	119	EP7_MALWARE	7	2015-05-28	High	Completed	EP7_MALWARE	All	
✗	ALPHA	122	EP3_SOCIAL	0	2015-05-28	High	Completed	Episode 3 - Solved	All	Not published
✓	EY	121	EP4_LOGS	1	2015-05-28	High	Completed	EP4_LOGS	All	
✗	GRNET	120	EP4_LOGS	1	2015-05-28	High	Completed	EP4_LOGS	All	Not published
✓	DI	117	EP5_WINFORENSICS	0	2015-05-28	Low	Completed	EP5_WINFORENSICS	All	
✓	DUTH	115	EP3_SOCIAL	1	2015-05-28	High	Completed	Ολοκλήρωση επεισοδίου 3	All	
✗	TEIATH	102	EP7_MALWARE	2	2015-05-27	High	Ongoing	Λύση επεισοδίου - 1η έκδοση	All	Not published
✓	KEPYES	114	EP4_LOGS	1	2015-05-28	High	Ongoing	http://seclists.org/fulldisclosure/2015/Feb/0	All	
✓	HNAVY	113	EP7_MALWARE	1	2015-05-28	High	Initial	Initial report	All	
✓	DI	112	EP1_WEB	0	2015-05-28	High	Ongoing	EP01_WEB	All	
✗	ISI	110	EP1_WEB	1	2015-05-28	High	Initial	Possible SQL injection vulnerability at command.strangled.net	All	Not published
✓	FossAUEB	87	EP3_SOCIAL	34	2015-05-26	High	Completed	Ανάλυση ευρημάτων από το Κοινωνικό Δίκτυο Eho.	All	
✗	UTH	109		0	2015-05-27	High	Ongoing	Exelivi askisis	All	Not published
✗	OTE	92	EP3_SOCIAL	0	2015-05-27	High	Ongoing	Καλησπέρα και απο μας, πρώτο post απο εμάς, βρισκόμαστε στο σημείο του Group of Justice έχουμε αποκρυπτογραφήσει τον συγκεκριμένο κωδικό (Password: TooDummyPassword), έχουμε ολοκληρώσει όλα τα προηγούμενα βήματα μέχρι να φτάσουμε εδώ. Επίσης, έχουμε προσθέσει ένα comment στα μηνύματα του aerinou (RE: PARTNERSHIP!) όταν τα αποκρυπτογραφήσαμε. Λόγω έλλειψης χρόνου δεν παρουσιάζουμε αναλυτικά τα προηγούμενα βήματα που έχουμε κάνει μέχρι στιγμής.	All	Not published
✗	FORTH	108	EP8_MOBILE	0	2015-05-27	High	Completed	Malicious android apps	All	Not published
✗	FORTH	107		0	2015-05-27	High	Completed	Malicious android apps	All	Not published
✗	FORTH	106		0	2015-05-27	High	Completed	Malicious android apps	All	Not published
✗	DUTH	105	EP3_SOCIAL	0	2015-05-27	High	Initial	Account access mixalis tzontanakis	All	Not published

Download: PGP/GPG key

version 2.3.0

ΠΑΝΟΠΤΗΣ 16

Επικοινωνία-CHAT

Chat interface for PANOPTIS 16. The chat window shows a list of participants on the right and a scrollable chat log on the left. The chat log contains messages from various users, including CD_ATHLGRIGORIADIS, gmet_user07, and UNIFI_Gianaki.Tsantili, discussing the event and providing hints.

Participants (24 άτομα στο δωμάτιο):

- CD_JVachris
- AUTH_Fotis.Leukos
- CD_ATHLGRIGORIADIS
- CD_director
- CD_Ioannis.Stas
- CD_Iecnidia.Perlepis
- CD_panoptis1.support
- cert1
- DIE_Alexandros.Vasilakis
- FORTH_Panos.Chatsiadam
- gmet_user07
- H2PA_Anargiros.Chrysanthou
- HMF4_Georgios.Papadopoulos
- H2WV_Adis.Tsakas
- hmsy_user01
- hmsy_user02
- Isr_Ioannis.Zacharos
- kepyes_Panos.Simes
- Microsoft_Thanasia.Diogos
- Newssoft_Konstantinos.Zacharos
- PZ_ostis.karenihilidis
- UNIFI_istefanos.liv
- uom_user01
- uth_user01

Chat Log:

12:44:18 μμ Ο λογαριασμός αποσυνδέθηκε και δε μπορεί τέχστε πλέον σε αυτή τη συζήτηση. Θα συμμετάσχετε ξανά αυτόματα όταν επανασυνδεθεί ο λογαριασμός.

12:52:2015 9:25:35 μμ CD_ATHLGRIGORIADIS: Καλημέρα! Καλή συνέχεια και σήμερα! Η άσκηση θα συνεχιστεί έως και αύριο (23/5) 14:00

12:52:2015 9:26:49 μμ CD_ATHLGRIGORIADIS: οι κόποιους που έχουν κολήσει σε κάποια επιδόσει... για την ομάδα από της άσκησης θα σταμάτουμε σήμερα να σας βοηθήσουμε με hints τόσο στο chat όσο και στο portal

12:52:2015 9:27:05 μμ CD_ATHLGRIGORIADIS: Μην ξεχνάτε να ενημερώνετε αλλά και να ενημερώνετε το MSP.

12:52:2015 10:55:58 μμ CD_acharitos: Επεισόδιο 1 - Web - Hint - <http://panoptis15.cd.mil.gr/%CE%93%CF%80%CE%83%CE%88%CF%83%CF%80%CE%84%CE%88%CE%8F-1-web-2/>

12:52:2015 12:34:53 μμ enka.pou: CD_acharitos:leath.

12:52:2015 3:59:48 μμ gmet_user07: geia sas

12:52:2015 4:00:20 μμ gmet_user07: kapota vathela gws kaneume submit ta apotelesmata enno episeidos ?

12:52:2015 4:01:30 μμ CD_ATHLGRIGORIADIS: Στο msp η στο στο email της άσκησης

12:52:2015 4:08:05 μμ gmet_user07: <http://collaboration.panoptis15.cd.mil.gr/events/view/12> auto ta vlepete ?

12:52:2015 4:13:29 μμ CD_ATHLGRIGORIADIS: Το βλέπω αλλά δεν μπορώ να βγάλω άκρη τίποτα.Αν μπορείτε χρησιμοποιήστε pdf μορφή και χρησιμοποιήστε και το attributes του Msp

12:52:2015 4:20:42 μμ gmet_user07: kalimeno einai... to timeline

12:52:2015 4:21:10 μμ gmet_user07: gia na ta kanei kapois enter auta sto msp dei para poly stono

12:52:2015 4:41:00 μμ CD_ATHLGRIGORIADIS: pdf upload innwda

12:52:2015 4:41:59 μμ gmet_user07: okay

12:52:2015 4:42:32 μμ CD_ATHLGRIGORIADIS: Αν θέλτε στείτε report και στο panoptis15@cd.mil.gr

12:52:2015 4:43:05 μμ CD_ATHLGRIGORIADIS: ...και δο το επιβόλο γρώ στο msp.

12:52:2015 4:43:23 μμ gmet_user07: okay! stafin pdf

12:52:2015 4:44:15 μμ CD_ATHLGRIGORIADIS: Ευχαριστώ... Καλό απόγευμα.

12:52:2015 8:22:50 μμ kepyes_Panos.Simes: καλημέρα στο ΑΚΥΘ

12:52:2015 9:21:33 μμ CD_Ioannis.Stas: Επεισόδιο 1 - Web (Attack Challenge): Hint - <http://panoptis15.cd.mil.gr/%CE%93%CF%80%CE%83%CE%88%CF%83%CF%80%CE%84%CE%88%CE%8F-1-web-attack-challenge/>

12:52:2015 11:54:29 μμ HMF4_Georgios.Papadopoulos: μήτρε στο δωμάτιο.

12:52:2015 11:55:16 μμ CD_director: μήτρε στο δωμάτιο.

12:52:2015 11:55:27 μμ telath_user01: μήτρε στο δωμάτιο.

12:52:2015 11:55:35 μμ telath_user01: έφυγε από το δωμάτιο.

12:52:2015 11:55:40 μμ OBR_user01: μήτρε στο δωμάτιο.

12:52:2015 11:55:57 μμ OBR_user01: έφυγε από το δωμάτιο.

12:52:2015 11:56:33 μμ CD_V.Anasotopoulos: μήτρε στο δωμάτιο.

12:52:2015 11:56:40 μμ CD_V.Anasotopoulos: έφυγε από το δωμάτιο.

12:52:2015 11:56:50 μμ CD_Iecnidia.Perlepis: μήτρε στο δωμάτιο.

12:52:2015 11:56:59 μμ CD_panoptis1.support: Παρακαλώ να σας κοιτάξετε την άσκηση σας για την άσκηση "ΠΑΝΟΠΤΗΣ 16" συμπληρώνοντας το ερωτηματολόγιο που θα βρείτε σε σχετική ενότητα που έχει γίνει στο portal, στο παρακάτω link: <http://panoptis15.cd.mil.gr/%CE%93%CF%80%CE%83%CE%88%CF%83%CF%80%CE%84%CE%88%CE%8F-1-web-attack-challenge/>. Το ερωτηματολόγιο θα είναι διαθέσιμο έως και την Παρασκευή 5 Ιουνίου 2015.

12:52:2015 11:57:48 μμ UNIFI_Gianaki.Tsantili: μήτρε στο δωμάτιο.

12:52:2015 11:57:57 μμ CD_ATHLGRIGORIADIS: Για ευχαριστώ όλους για την συμμετοχή στην άσκηση. Παρατηρήσαμε μεγάλο ενδιαφέρον για όλο το επιδόσει και είπαμε να εκπαιδευτήκατε και ζωοκρίσετε όσο εμείς.

12:52:2015 11:58:52 μμ CD_ATHLGRIGORIADIS: Η άσκηση θα παύσει στις 14:00 σήμερα

12:52:2015 11:59:51 μμ CD_ATHLGRIGORIADIS: Παρακαλώ για πάλιν παρατηρήσεις και διαπιστώσεις συμπληρώστε το ερωτηματολόγιο στο portal και στείτε και email στο panoptis15@cd.mil.gr

12:52:2015 12:00:39 μμ CD_ATHLGRIGORIADIS: ...Πα επανέρχουμε και μετά το πέρας της άσκησης με βόλες στο portal αλλά και συμπληρώματα - απευθύμενα με συνάντηση που θα ανακοινωθεί.

12:52:2015 12:01:09 μμ CD_ATHLGRIGORIADIS: ...και του χρόνου για τον Πανόπτη 16

12:52:2015 12:01:47 μμ CD_ATHLGRIGORIADIS: Διαβάστε panoptis15@cd.mil.gr

12:52:2015 12:14:01 μμ UNIFI_Gianaki.Tsantili: έφυγε από το δωμάτιο.

Buttons: [Εγγραφή] [Εγγραφή] [Χωρίς] [Προσθήκη]

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:

A' φάση (basic)

Ανάλυση λειτουργίας εφαρμογών.

Εντοπισμός αδυναμιών.

B' 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 Μαΐου 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;