Εθνική Άσκηση Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ”

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 και στις δυνατότητές τους.

√ Ως αντικειμενικός σκοπός των ασκήσεων κυβερνοάμυνας είναι να εξεταστούν οι διαδικασίες και οι δυνατότητες του οργανισμού, στην αντιμετώπιση των κυβερνοεπιθέσεων. 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

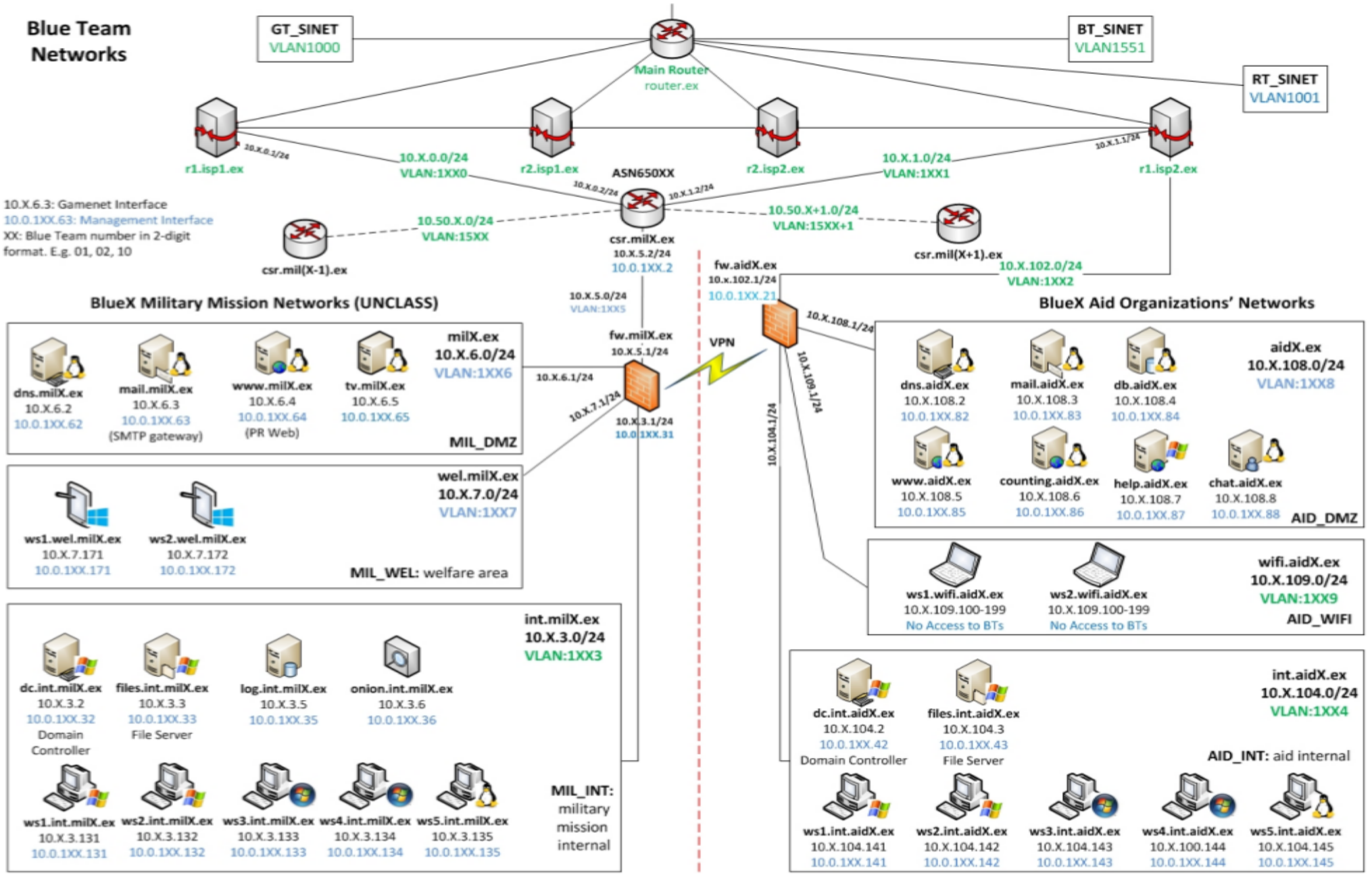
Πλεονεκτήματα:

- 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**

Ιστορία της Εθνικής άσκησης Κυβερνοάμυνας “ΠΑΝΟΠΤΗΣ”

Ελληνική Εθνική άσκηση Κυβερνοάμυνας
(Ελεύθερη συμμετοχή) Υποχρεωτική για τις ΕΔ.

Διοργανώνεται κάθε χρόνο από το 2010
(Το ΓΕΕΘΑ/Ε6 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: 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: 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

View Event
View Event History
Edit Event
Delete Event

Add Attribute
Add Attachment
Populate from IOC
Populate from ThreatConnect

Contact Reporter
Download as XML
Download as IOC
Download as CSV

List Events
Add Event

Event

ID	1097
Uuid	50f52fa6-912c-44dc-b330-55d7ac1d4fa4
Org	NCIRC
Owner org	ADMIN
Email	admin@admin.test
Date	2013-01-14
Risk	Undefined
Analysis	Completed
Distribution	All communities, this will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next..
Info	Kaspersky Red October Report
Published	Yes

Related Events

2012-10-31 (583) 2012-10-12 (1059)
2012-07-16 (1030) 2012-07-12 (1023)
2012-07-05 (476) 2012-07-05 (1010) 2012-07-03 (588)
2012-04-19 (412) 2012-01-01 (553)

Attributes

Category	Type	Value	Related Events	IDS	Distribution	Actions
Payload delivery	email-attachment	Katyn_-_opinia_Rosjan.xls		No	All	
	email-attachment	FIEO contacts update.xls		No	All	
	email-attachment	spisok sotrudnikov.xls		No	All	
	email-attachment	List of shahids.xls		No	All	

Επεισόδια ΠΑΝΟΠΤΗ 18

- **Windows forensics**
- **Linux forensics**
- **Mobile forensics**
- **Web forensics**
- **SCADA**
- **Network CTF**

Ερωτήσεις;