Assessing Network Security

Paula Kiernan

Senior Consultant

Ward Solutions

Επισκοπηση μαθήματος

- Σχεδιασμος Αξιολογησης Ασφάλειας
- Συγκεντρωση πληροφοριων για τον Οργανισμο
- Ελεγχος διεισδυσης για παρεμβατικες επιθεσεις
- Case Study

Σχεδιασμος αξιολογησης ασφαλειας

- Σχεδιασμος Αξιολογησης Ασφάλειας
- Συγκεντρωση πληροφοριων για τον Οργανισμο
- Ελεγχος διεισδυσης για παρεμβατικες επιθεσεις
- Case Study

Γιατι αποτυγχανει η Ασφαλεια Δικτυου?

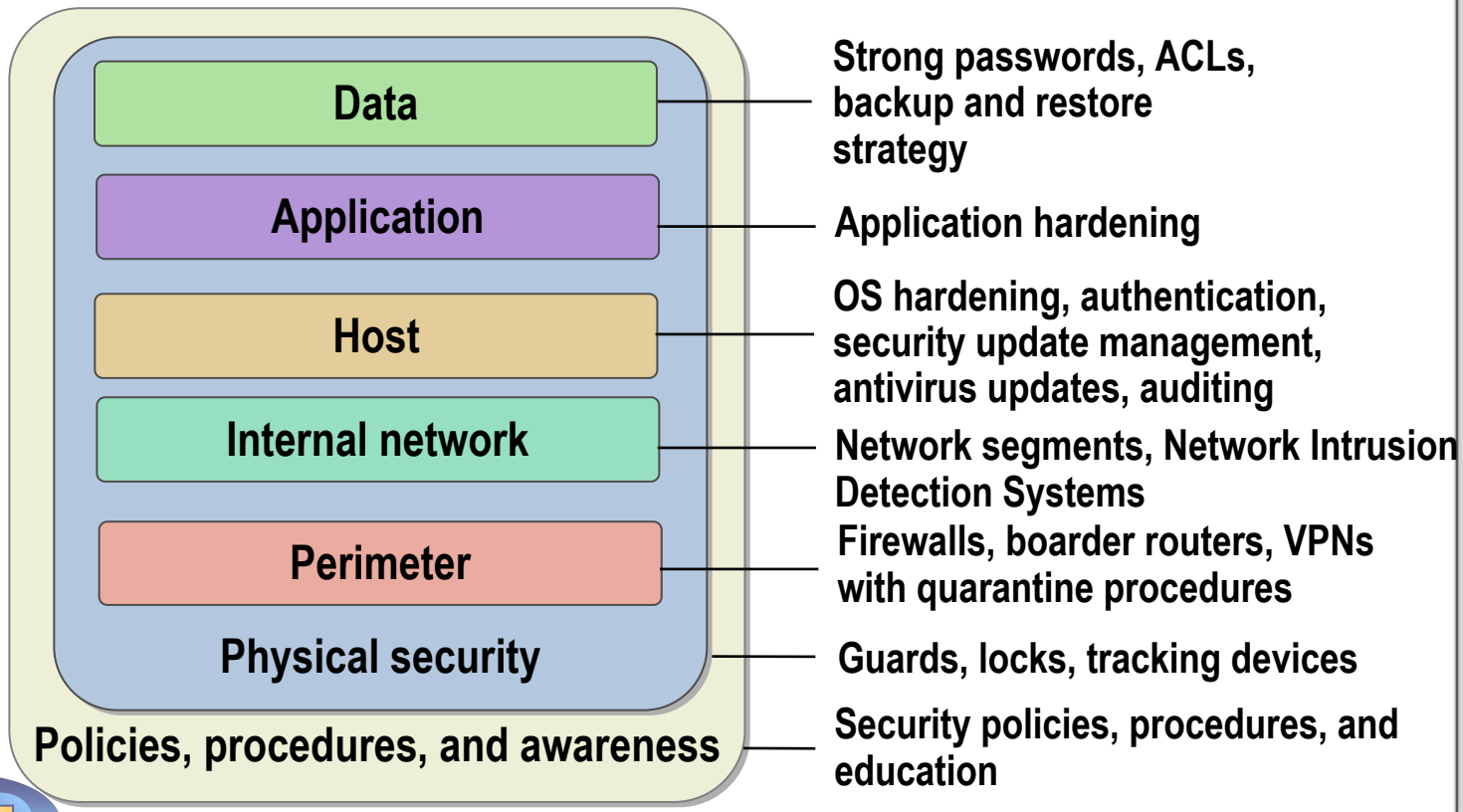
Η ασφαλεια δικτυου αποτυγχανει συνηθως στις εξης περιοχες:

- Ελλειπης ευαισθητοποιηση των ανθρωπων για θεματα ασφαλειας
- Παραγοντες πολιτικης
- Λανθασμενες διαμορφωσεις του Hardware ή του Software
- Ελλειπεις παραδοχες
- Αγνοια
- Αποτυχια να παραμεινει το συστημα up-to-date

Σε βαθος κατανοηση της Αμυνας

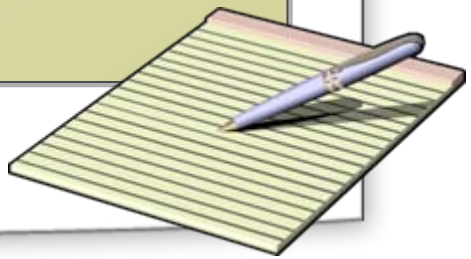
Η χρησιμοποιηση μας διαστρωματοποιημενης προσεγισης:

- Αυξανει την πιθανοτητα να ανιχνευτει ενας επιτιθεμενος
- Μειωνει την πιθανοτητα επιτυχιας μιας επιθεσης



Γιατι χρειαζονται οι αξιολογησεις ασφαλειας?

- Να απαντησουν στις ερωτησεις: “Ειναι ασφαλες το δικτυο μας?” και “Πως ξερουμε οτι το δικτυο μας ειναι ασφαλες?”
- Παρεχουν μια αφετηρία για τη βελτιωση της ασφαλειας
- Βρισκει λαθη στη διαμορφωση του δικτυου ή ελλειψεις στις ενημερωσεις ασφαλειας
- Ανακαλυπτει μη αναμενομενες αδυναμιες στην ασφαλεια ενος οργανισμού
- Διασφαλιζει τη συμμορφωση με τους κανονισμους ασφαλειας



Σχεδιαζοντας μια Αξιολογηση Ασφαλειας

Φαση του Project	Σχεδιαστικα στοιχεια της καθε φασης
Προ-αξιολογηση	• Σκοπος • Στοχοι • Χρονοδιαγραμματα • Βασικοι Κανονες
Αξιολογηση	• Επιλογη Τεχνολογιων • Υλοποιηση Αξιολογησης • Οργάνωση των αποτελεσματων
Προετοιμασια Αποτελεσματων	• Εκτιμηση του κινδυνου που προκυπτει απο τις αποκαλυφθεισες αδυναμιες • Δημιουργια πλανου για αποκατασταση • Προσδιορισμος των αδυναμιων που δεν εχουν αποκατασταθει • Προσδιορισμος της βελτιωσης της ασφαλειας
Αναφορα των ευρηματων	• Δημιουργια τελικης αναφορας • Παρουσιαση των ευρηματων • Δρομλογηση της νεας Αξιολογησης Ασφαλειας

Κατανοηση του Σκοπου της Αξιολογησης Ασφαλειας

Στοιχεια	Παραδειγματα
Στοχος	All servers running: • Windows 2000 Server • Windows Server 2003
Περιοχη του Στοχου	Ολοι οι servers στα υποδικτυα: • 192.168.0.0/24 • 192.168.1.0/24
Χρονοδιαγραμμα	Το σαρωμα (scanning) θα πραγματοποιηθει μεταξυ 26 και 30 Μαρτίου κατα η διαρκεια μη σημαντικων εργασιμων ωρων
Τρωτα σημεια για τα οποια θα ψαξουμε	• RPC-over-DCOM vulnerability (MS 03-026) • Anonymous SAM enumeration • Guest account enabled • Greater than 10 accounts in the local Administrator group

Κατανοηση των Στοχων της Αξιολογησης Ασφαλειας

Στοχος του project	
Ολοι οι υπολογιστες που τρεχουν Windows 2000 Server και Windows Server 2003 στα υποδικτυα 192.168.0.0/24 και 192.168.1.0/24 θα σαρωθουν για τα παρακατω πιθανα τρωτα σημεια και θα αποκατασταθουν με τον τροπο που φαινεται παρακατω	
Τρωτο σημειο	**Αποκατασταση**
RPC-over-DCOM vulnerability (MS 03-026)	Install Microsoft security updates 03-026 and 03-39
Anonymous SAM enumeration	Configure RestrictAnonymous to: 2 on Windows 2000 Server 1 on Windows Server 2003
Guest account enabled	Disable Guest account
Greater than 10 accounts in the local administrator group	Minimize the number of accounts on the administrators group

Ειδη Αξιολογησεων Ασφαλειας

Σαρωση Τρωσιμοτητας (Vulnerability scanning):

- Εστιαζει σε γνωστες αδυναμιες
- Μπορει να ειναι αυτοματοποιημενη
- Δεν απαιτει να ειναι καποιος expert

Ελεγχος διεισδυσης (Penetration testing):

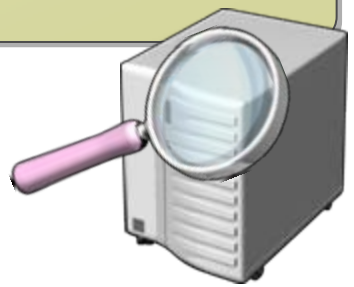
- Εστιαζει σε γνωστες και αγνωστες αδυναμιες
- Απαιτει πολυ ικανους ελεγκτες
- Ενεχει σημαντικα νομικα προβληματα σε ορισμενες χωρες ή οργανισμους

Ελεγχος ασφαλειας IT (IT security auditing):

- Εστιαζει σε πολιτικες και διαδικασιες ασφαλειας
- Χρησιμοποιειται για να παρασχει βαση για τους βιομηχανικους κανονισμους ασφαλειας

Χρησιμοποιωντας τη Σαρωση Τρωσιμοτητας (Vulnerability Scanning) για την εκτιμηση της Ασφαλειας Δικτυου

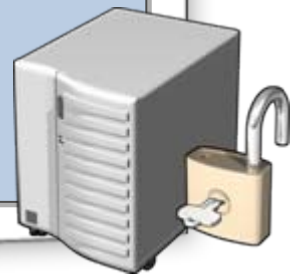
- Ανιχνευει τα τρωτα σημεια
- Προσδιοριζει τα επιπεδα κινδυνου για τα τρωτα σημεια που ανακαλυφθηκαν
- Προσδιοριζει τρωτα σημεια που δεν εχουν αποκατασταθει
- Προσδιοριζει τη βελτιωση της ασφαλειας του δικτυου στο χρονο



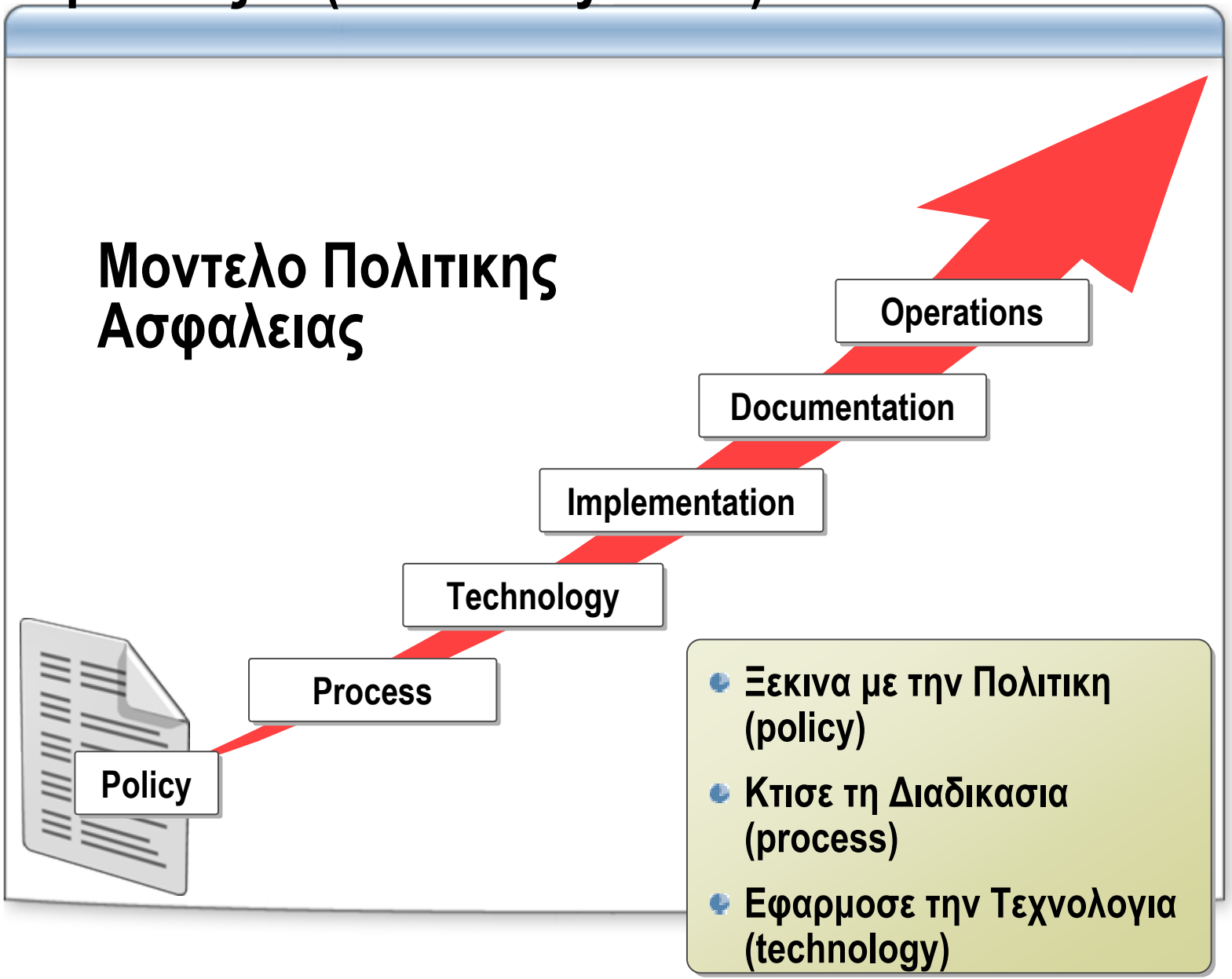
Χρησιμοποιωντας τον Ελεγχο Διεισδυσης για την Εκτιμηση της Ασφαλειας Δικτυου

Βηματα για εναν επιτυχημενο Ελεγχο Διεισδυσης:

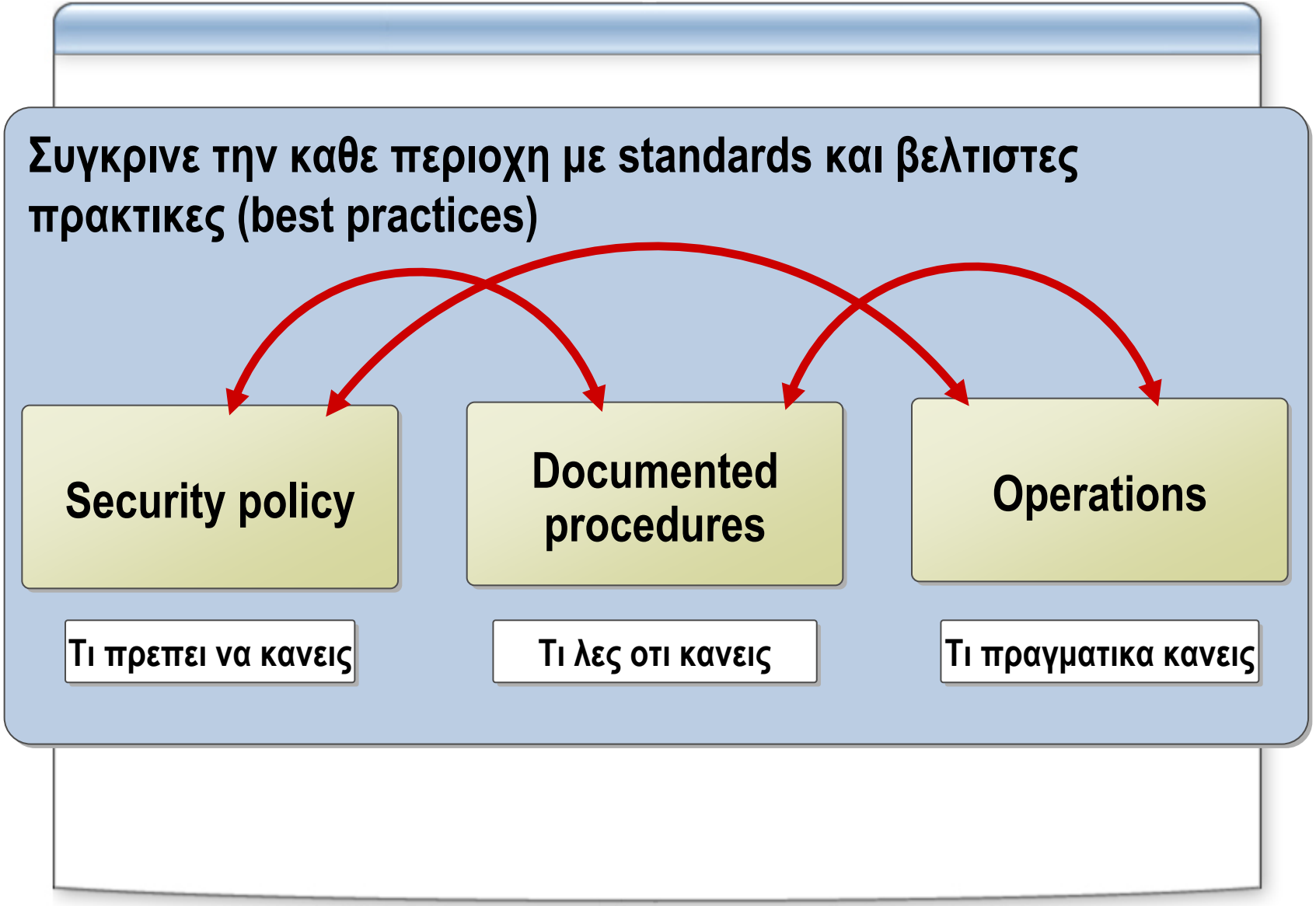
1. Προσδιορισε με ποιον τροπο ειναι πιο πιθανο ο επιτιθεμενος να επιτεθει σε ενα δικτυο ή σε μια εφαρμογη
2. Εντοπισε περιοχες αδυναμιων στην αμυνα του δικτυου ή των εφαρμογων
3. Προσδιορισε πως ενας επιτιθεμενος θα μπορουσε να εμεταλλευτει τις αδυναμιες
4. Εντοπισε σημεια που θα μπορουσαν να προσπελαστουν, να αλλαχθουν ή να καταστραφουν
5. Προσδιορισε αν η επιθεση εντοπιστηκε
6. Προσδιορισε ποιο ειναι το αποτυπωμα της επιθεσης
7. Κανε συστασεις



Κατανοηση των Συνιστωσων ενος Ελεγχου Ασφαλειας IT (IT Security Audit)



Υλοποιηση ενος Ελεγχου Ασφαλειας IT



Αναφορα των Ευρηματων της Αξιολογησης Ασφαλειας

Οργανωσε την πληροφορια κατα το παρακατω πλαισιο αναφορας:

- Ορισε το τρωτο σημειο
- Τεκμηριωσε τα σχεδια αντιμετωπισης του
- Προσδιορισε που πρεπει να επελθουν αλλαγες
- Αναθεσε σε υπευθυνους την υλοποιηση των εγκεκριμενων συστασεων
- Προτεινε το ποτε θα γινει η επομενη αξιολογηση ασφαλειας

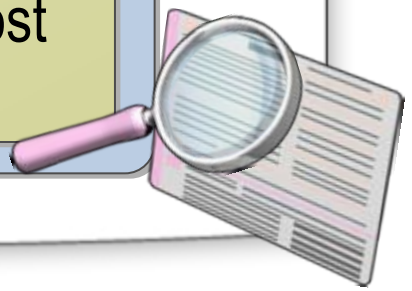
Συγκεντρωση πληροφοριων για τον οργανισμο

- Σχεδιασμος Αξιολογησης Ασφάλειας
- Συγκεντρωση πληροφοριων για τον Οργανισμο
- Ελεγχος διεισδυσης για παρεμβατικες επιθεσεις
- Case Study

Τι ειναι μια Μη-Παρεμβατικη Επιθεση (Nonintrusive Attack)?

Μη-Παρεμβατικη επιθεση: Η προσπαθεια να ληφθουν πληροφοριες σχετικα με το δικτυο ενος οργανισμου με σκοπο να προετοιμαστει μια πιο παρεμβατικη επιθεση στο μελλον

- Αναγνωριση Πληροφοριων (Information reconnaissance)
- Σαρωση Θυρων (Port scanning)
- Ληψη Πληροφοριων για ενα host χρσιμοποιωντας τεχνικες «Δακτυλικων Αποτυπωματων» (fingerprinting techniques)
- Ανακαλυψη δικτυου και host (Network and host discovery)



Τεχνικες Αναγνωρισης Πληροφοριων (Information Reconnaissance Techniques)

Τυποι πληροφοριας που αναζητουν οι επιτιθεμενοι:

- Η Διαμορφωση του Συστηματος (System configuration)
- Νομιμοι Λογαρισαμοι Χρηστων (Valid user accounts)
- Πληροφοριες Επικοινωνιας (Contact information)
- Extranet και Servers μακρυνης προσβασης (Extranet and remote access servers)
- Εταιρικοι partners και προσφατες εξαγορες ή συγχωνευσεις

Πηγες Πληροφοριων για το δικτυο σου:

- Οι Πληροφοριες του Καταχωρητη Ονοματων Διαδικτυου (registar information)
- Οι αναθεσεις διευθυνσεων IP
- Οι Ιστοσελιδες του Οργανισμου
- Οι Μηχανες Αναζητησης
- Forums Δημοσιων Συζητησεων

Αντιμετρα κατα της Αναγνωρισης Πληροφοριων

- Παρασχε μονο οση πληροφορια ειναι απαραιτητη για τον καταχωρητη ονοματων Διαδικτυου (Internet registrar)
- Ελεγχε τακτκα το Web site του οργανισμου για μη καταλληλη πληροφορια που μπορει να αξιοποιηθει απο εναν επιτιθεμενο
- Χρησιμοποιησε διευθυνσεις e-mail βασισμενες στους εργασιακους ρολους
- Δημιουργησε μια πολιτικη οριζοντας την ορθη χρηση των φορουμ δημοσιων συζητησεων

Τι πληροφορια μπορει να αποκτηθει μεσω της Σαρωσης Θυρων (Port Scanning)?

Τα Τυπικα αποτελεσματα μιας σαρωσης θυρων περιλαμβανουν:

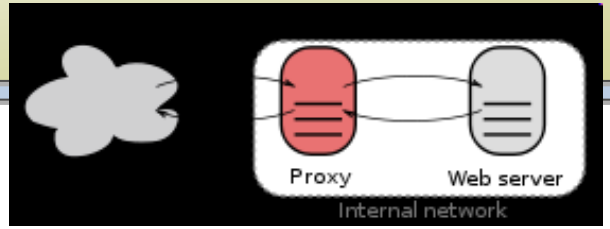
- Ανακαλυψη των θυρων που ειναι ανοιχτες ή ακουει σε αυτες ο υπολογιστης
- Ορισμος των θυρων που απορριπτουν συνδεσεις
- Προσδιορισμος των συνδεσεων που εκπνεουν (time out)

Συμβουλες για αποτελεσματικη σαρωση θυρων:

- Ξεκινα τη σαρωση σιγα, με μονο λιγες θυρες καθε φορα
- Για να αποφυγεις την ανιχνευση, δοκιμασε την ιδια θυρα σε διαφορετικα hosts
- Τρεξε σαρωσεις απο εναν αριθμο διαφιρετικων συστηματων, ή (αν ειναι εφικτο) και διαφορετικων δικτυων

Αντιμετρα κατα της Σαρωσης Θυρων

- Υλοποιησε αμυνα σε βαθος με πολλα επιπεδα φιλτραρισματος
- Ετοιμασε πλανο για πιθανες και αποτυχιες του συστηματος
- Υλοποιησε συστημα ανιχνευσης εισβολης (intrusion-detection system)
- Να τρεχουν μονο οι απαραιτητες υπηρεσιες
- Εκθεσε τις υπηρεσιες που πρεπει να ειναι διαθεσιμες μεσω ενος reverse proxy



Τι πληροφοριες μπορουν να συλλεχθουν σχετικα με τα hosts του δικτυου?

Ειδη πληροφοριας που μπορει να συλλεχθουν χρησιμοποιωντας τεχνικες δακτυλικων αποτυπωματων (fingerprinting: αποστολη αιτηματων στο host, και ελεγχος των απαντησεων του):

- Η υλοποιηση του IP και του ICMP
- Απαντησεις του TCP
- Θυρες στις οποιες «ακουει» το host
- Banners
- Συμπεριφορα των υπηρεσιων (Service behavior)
- Μακρυνα αιτηματα προς το λειτουργικο συστημα

Αντιμετρα για την προστασια των πληροφοριων ενος δικτυωμενου host

Fingerprinting source	Αντιμετρα
IP, ICMP, and TCP	• Να ειμαστε συντηρητικοι για τα πακετα που επιτρεπουμε να φτασουν στο συστημα μας • Να χρησιμοποιουμε ενα firewall ή inline συσκευη IDS • Υποθεσε οτι ο επιτιθεμενος γνωριζει τι εκδοση του λειτουργικου συστηματος τρεχει και καταστησε το ασφαλες
Banners	• Αλλαξε τα banners που δινουν πληροφοριες για το λειτουργικο συστημα • Υποθεσε οτι ο επιτιθεμενος γνωριζει τι εκδοση του λειτουργικου συστηματος και τι εφαρμογες τρεχουν και καταστησε τα ασφαλη
Port scanning, service behavior, and remote queries	• Απενεργοποιησε τις μη απαραιτητες υπηρεσιες • Φιλτραρισε το traffic που ερχεται να απομονωσει συγκεκριμενες θυρες στο host • Υλοποιησε IPSec σε ολα τα συστηματα του διαχειριζομενου δικτυου

Ελεγχος Διεισδυσης για Παρεμβατικες Επιθεσεις

- Σχεδιασμος Αξιολογησης Ασφάλειας
- Συγκεντρωση πληροφοριων για τον Οργανισμο
- Ελεγχος διεισδυσης για παρεμβατικες επιθεσεις
- Case Study

Τι ειναι ο διεισδυτικος ελεγχος για παρεμβατικες επιθεσεις?

Παρεμβατικη επιθεση: Η εκτελεση συγκεκριμενων ενεργειων που εχουν ως αποτελεσμα την τρωση της πληροφοριας, της σταθεροτητας ή της διαθεσιμοτητας του συστηματος

Παραδειγμα ελεγχου διεισδυσης για παρεμβατικες επιθεσεις

- Αυτοματη σαρωση τρωσιμοτητας
- Επιθεσεις Συνθηματικων (Password attacks)
- Επιθεσεις Αρνησης Υπηρεσιας (DoS attacks)
- Επιθεσεις σε εφαρμογες και βασεις δεδομενων
- Network sniffing

Τι ειναι η Αυτοματη Σαρωση Τρωσιμοτητας (Automated Vulnerability Scanning)?

Η Αυτοματη Σαρωση Τρωσιμοτητας χρησιμοποιει εργαλεια σαρωσης για να αυτοματοποιησει τις ακολουθες εργασιες:

- Λήψη του Banner και fingerprinting
- Εκμεταλλευση της τρωσιμοτητας (Exploiting the vulnerability)
- Δοκιμη Συμπερασματος (Inference testing)
- Ανιχνευση Ενημερωσεων Ασφαλειας (Security update detection)

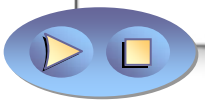
Τι ειναι επιθεση συνθηματικων (Password Attack)?

Δυο βασικοι τυποι επιθεσεων συνθηματικων:

- Επιθεσεις Brute-force
- Επιθεσεις αποκαλυψης του συνθηματικου (Password-disclosure attacks)

Αντιμετρα για την προστασια απο επιθεσεις συνθηματικων:

- Να απαιτουνται συνθετα passwords
- Να εκπαιδευονται οι χρηστες
- Να χρησιμοποιουνταιι smart cards
- Να δημιουργηθει πολιτικη που θα απαγορευει τα passwords σε batch files, scripts, ή Web pages



Τι ειναι επιθεση Αρνησης Υπηρεσιας (Denial-of-Service Attack)?

Denial-of-Service (DoS) attack: Καθε προσπαθεια ενος επιτιθεμενου να αρνηθει στο θυμα του την προσβαση σε εναν πορο

Οι επιθεσεις (DoS) μπορουν να χωριστουν σε τρεις κατηγοριες:

- Επιθεσεις πλημυρρισματος (Flooding attacks)
- Επιθεσεις Στερησης Πορων (Resource starvation attacks)
- Διακοπη υπηρεσιας (Disruption of service)

Σημειωση: Οι επιθεσεις Denial-of-service δεν πρεπει να εξαπολυονται κατα του δικτυου παραγωγης του οργανισμου

Αντιμετρα κατα των επιθεσεων Αρνησης Υπηρεσιας

Επιθεση DoS	Αντιμετρα
Flooding attacks	• Εξασφαλισε οτι οι ρουτερ σου εχουν κανονες anti-spoofing και κανονες που μπλοκαρουν κατευθυνομενες εκπομπες (directed broadcasts) • Ορισε περιορισμους ρυθμου στα μηχανηματα για να περιοριστουν οι επιθεσεις πλημυρρισματος • Δες μηπως πρεπει να μπλοκαρεις τα πακετα ICMP
Resource starvation attacks	• Εγκαταστησε τις τελευταιες ενημερωσεις του λειτουργικου συστήματος και των εφαρμογων • Ορισε quotas στο δισκο
Disruption of service	• Εγκαταστησε τις τελευταιες ενημερωσεις του λειτουργικου συστήματος και των εφαρμογων • Ελεγξε τις ενημερωσεις πριν τις εγκαταστησεις σε συστηματα παραγωγης • Απενεργοποιησε τις μη απαραιτητες υπηρεσιες

Κατανοηση των επιθεσεων σε Εφαρμογες και Βασεις Δεδομενων (Application and Database Attacks)

Συνηθεις επιθεσεις σε εφαρμογες και βασεις δεδομενων:

Buffer overruns:

- Write applications in managed code

SQL injection attacks:

- Validate input for correct size and type

Τι εναι το Network Sniffing?

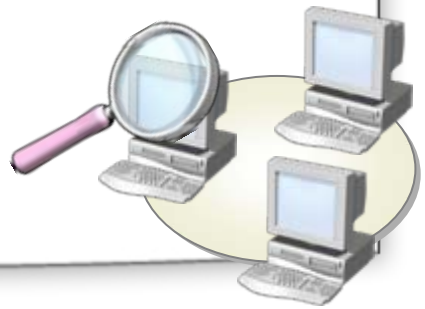
Network sniffing: Η ικανοτητα του επιτιθεμενου να υποκλεπτει τις επικοινωνιες μεταξυ των hosts

Ενας επιτιθεμενος μπορει να κανει network sniffing εκελωντας τις παρακατω εργασιες:

1. Τρωση του host
2. Εγκατασταση ενος network sniffer
3. Χρησιμοποιηση ενος network sniffer για να υποκλεπτει ευαισθητα δεδομενα οπως τα network credentials (username & password)
4. Χρηση των network credentials για την τρωση και αλλων hosts

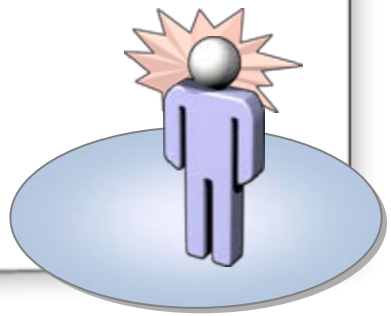
Αντιμετρα για επιθεσεις Network Sniffing

- Χρησιμοποιησε κρυπτογραφηση για την προστασια των δεδομενων
- Χρησιμοποιησε switches αντι για hubs
- Ασφαλισε τις βασικες συσκευες του δικτυου
- Χρησιμιοποιησε καλωδια crossover
- Αναπτυξε μια πολιτικη ασφαλειας
- Κανε σαρωσεις σε τακτικα χρονικα διαστηματα



Πως οι επιτιθεμενοι αποφευγουν τον εντοπισμο τους κατα τη διαρκεια μιας επιθεσης

- Πλημμυριζοντας τα αρχεια καταγραφης (log files)
- Χρησιμοποιωντας τους μηχανισμους καταγραφης (logging mechanisms)
- Επιτιθεμενοι στους μηχανισμους ανιχνευσης
- Χρησιμοποιωντας επιθεσεις κανονικοποιησης (canonicalization attacks)
- Χρησιμοποιωντας αντιμετρα παραπλανησης (decoys)



Πως οι επιτιθεμενοι αποφευγουν τον εντοπισμο τους μετα απο μια επιθεση

- Εγκαθιστώντας rootkits
- Αλλοιώνοντας τα log files

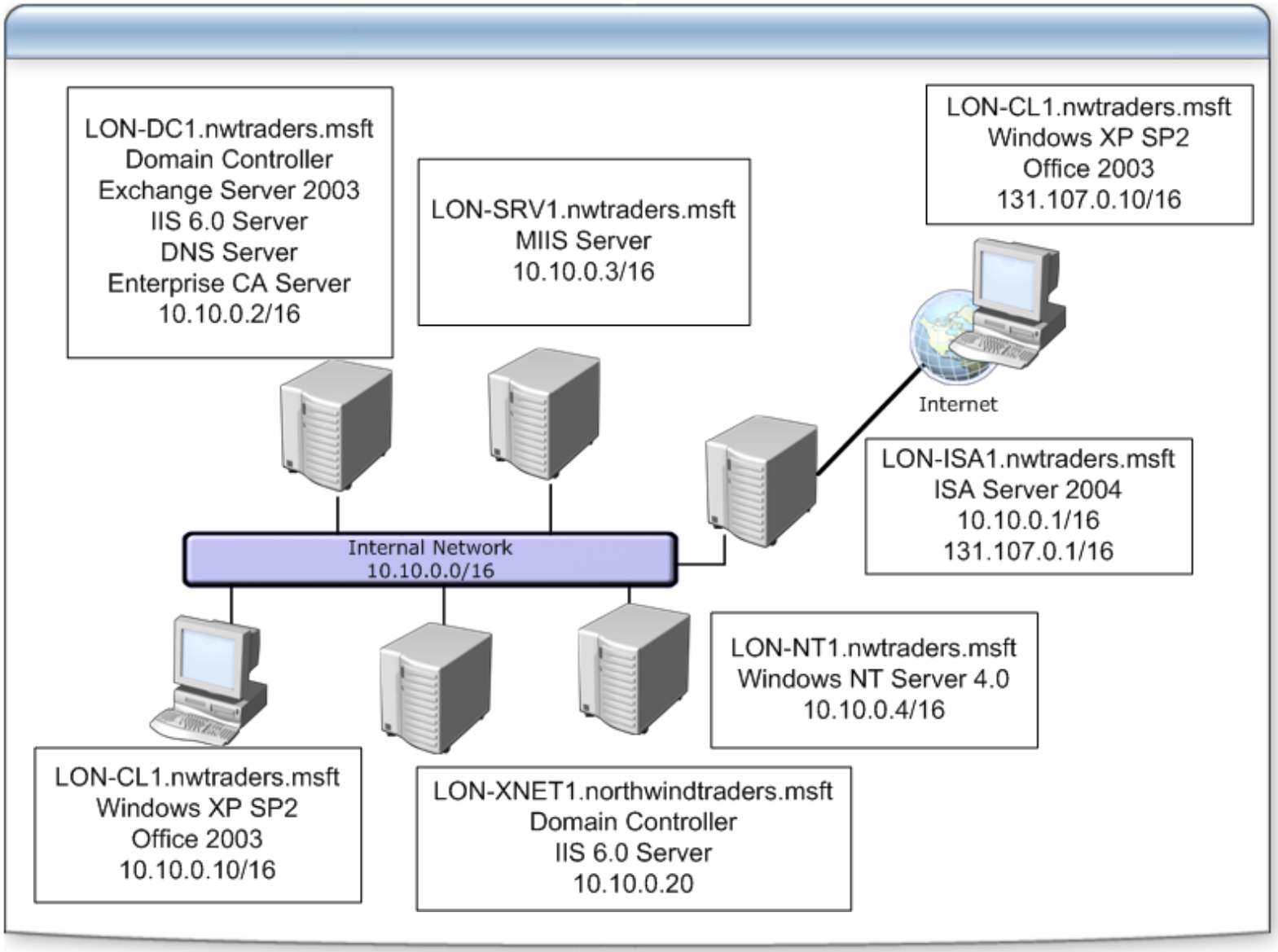
Αντιμετρα για τις τεχνικες αποφυγης εντοπισμου

Τεχνικη Αποφυγης Εντοπισμου	Αντιμετρο
Flooding log files	• Παρε Back up των log files πριν γραφτει κατι σε αυτα
Using logging mechanisms	• Επιβεβαιωσε οτι οι μηχανισμος καταγραφης χρησιμοποιει την πιο ενημερωμενη εκδοση του software και εχουν εκατασταθει ολες οι ενμημερωσεις
Attacking detection mechanisms	• Διατηρησε το software και τις υπογραφες ενημερωμενες
Using canonicalization attacks	• Εξασφαλισε οτι οι εφαμογες φερνουν τα δεδομενα στη κανονικη τους μορφη
Using decoys	• Ασφαλισε τα τερματικα συστηματα και τα δικτυα που δεχονται επιθεση
Using rootkits	• Υλοποιησε στρατηγικες αμυνας σε βαθος
Tampering with log files	• Ασφαλισε τις τοποθεσιες των log files • Αποθηκευσε τα logs σε αλλο host • Χρησιμοποιησε κρυπτογραφηση για την προστασια των log files • Παιρνε back up των log files

Case Study: Εκτιμηση Ασφαλειας Δικτυου για την Northwind Traders

- Σχεδιασμος Αξιολογησης Ασφάλειας
- Συγκεντρωση πληροφοριων για τον Οργανισμο
- Ελεγχος διεισδυσης για παρεμβατικες επιθεσεις
- Case Study

Εισαγωγη του Σεναριου της Case-Study



Ορισμος του σκοπου της Εκτιμησης Ασφαλειας

Components	Scope
Target	LON-SRV1.nwtraders.msft
Timeline	Scanning will take place December 2 during noncritical business hours
Assess for the following vulnerabilities	• Buffer overflow • SQL injection • Guest account enabled • RPC-over-DCOM vulnerability

Οριζοντας τους στοχους της Εκτιμησης Ασφαλειας

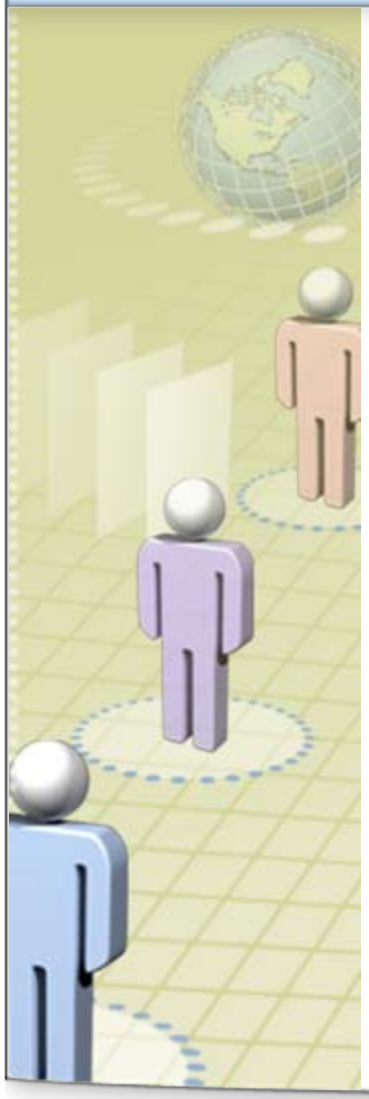
Project goal	
Το LON-SRV1 θα σαρωθει για τις παρακατω αδυναμιες και θα αποκατασταθει οπως οριζεται παρακατω	
Τρωσιμοτητα	**Αποκατασταση**
SQL Injection	Require developers to fix Web-based applications
Buffer Overflow	Have developers fix applications as required
Guest account enabled	Disable guest account
RPC-over-DCOM vulnerability	Install Microsoft security update MS04-012

Επιλογη των Εργαλειων για την Εκτιμηση Ασφαλειας

Θα χρησιμοποιηθουν τα παρακατω εργαλεια:

- Microsoft Baseline Security Analyzer
- KB824146SCAN.exe
- Portqry.exe
- Manual input

Demonstration: Εκτελωντας την Εκτιμηση Ασφαλειας



- Εκτελεση Σάρωσης Θυρων χρησιμοποιωντας το Portqry.exe
- Χρηση του KB824146Scan.exe για την εκτελεση της σαρωσης τρωσιμοτητας
- Προσδιορισε τις buffer overflow vulnerabilities
- Προσδιορισε SQL injection vulnerabilities
- Χρησιμοποιησε το Microsoft Baseline Security Analyzer για την εκτελεση μιας σαρωσης τρωσιμοτητας

Αναφορα των ευρηματων της Security Assessment

Απαντησε στα παρακατω ερωτηματα για να συμπληρωσεις την αναφορα:

- Τι κινδυνο παρουσιαζει η παρουσα τρωσιμοτητα?

  Ποια ειναι η πηγη της τρωσιμοτητας?

  Ποιες ειναι οι πιθανες συνεπειες της τρωσιμοτητας?

  Ποια ειναι η πιθανοτητα να εκμεταλλευτει καποιος την τρωσιμοτητα?
- Τι βελτιωσεις πρεπει να γινει για να μειωθει η τρωσιμοτητα?

  Δωσε τουλαχιστον τρεις επιλογες αν ειναι δυνατον
- Που πρεπει να γινουν βελτιώσεις?
- Ποιος πρεπει να ειναι υπευθυνος για την υλοποιηση των απαραιτητων βελτιωσεων?

Συνοψη

- Σχεδιαστε την εκτιμηση ασφαλειας και προσδιοριστε το σκοπο της
- Αποκαλυψτε μονο τις απαραιτητες πληροφοριες για τον οργανισμο σας σε Web sites και σε καταχωρησεις εγγραφης
- Υποθεστε οτι ο επιτιθεμενος ηδη γνωριζει το λειτουργικο συστημα και την εκδοση του και καντε οτι ειναι απαραιτητο για να ασφαλιστουν τα συστηματα αυτα
- Εκπαιδευστε τους χρηστες να χρησιμοποιησουν ισχυρα passwords ή pass-phrases
- Κρατηστε τα συστηματα ενημερωμενα με ενημερωσεις ασφαλειας και service packs

Βιβλιογραφια

- *Assessing Network Security*
  by Kevin Lam, David LeBlanc, and Ben Smith