Security+
Κεφάλαιο 1

Presentation:
Alexia & Chris

3 κεντρικοί στόχοι της Ασφάλειας (Security)

Confidentiality (εμπιστευτικότητα, απόρρητο)

Αποτροπή μη εξουσιοδοτημένης πρόσβασης/εμφάνισης των δεδομένων.

Integrity (ακεραιότητα)

Διαβεβαίωση ότι τα δεδομένα δεν έχουν αλλάξει

Availability (διαθεσιμότητα)

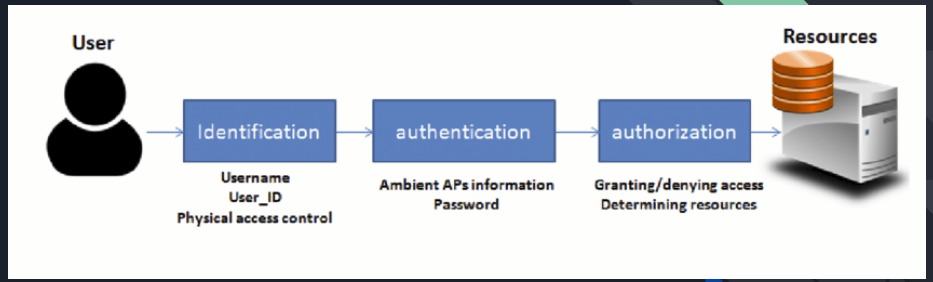
Υποδηλώνει ότι τα δεδομένα και οι υπηρεσίες θα είναι διαθέσιμα.

1.Εξασφάλιση Confidentiality

➔ **Encryption** (κρυπτογράφηση)

➔ **Access Controls** (έλεγχοι πρόσβασης)

- ➢ Identification
- ➢ Authentication
- ➢ Authorisation



➔ **Steganography & Obfuscation**

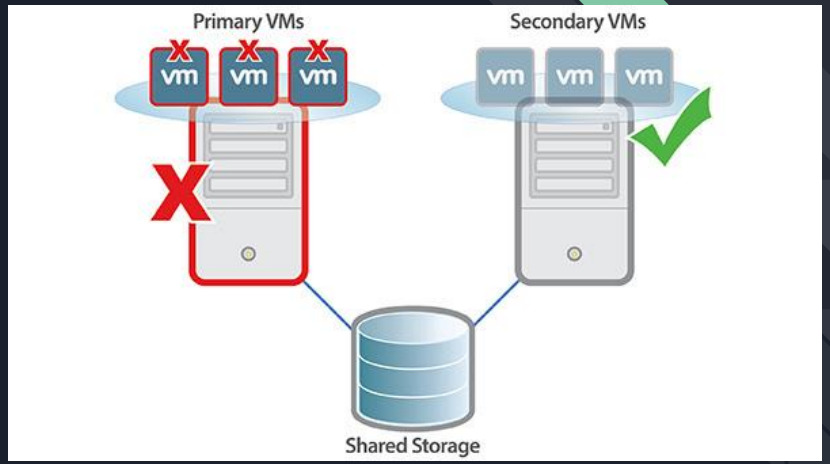
2.Εξασφάλιση Integrity

- **Hashing**
  - Για παράδειγμα MD5, md5sum, sha1sum, sha256sum
- **Digital Signatures**
  - Authentication
  - Non-repudiation
  - Απαραίτητα certificates

```
chris@chris-VirtualBox:~$ md5sum /home/chris/example.iso
d41d8cd98f00b204e9800998ecf8427e  /home/chris/example.iso
chris@chris-VirtualBox:~$ sha1sum /home/chris/example.iso
da39a3ee5e6b4b0d3255bfef95601890afd80709  /home/chris/example.iso
chris@chris-VirtualBox:~$ sha256sum /home/chris/example.iso
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855  /home
/chris/example.iso
```

3.Εξασφάλιση Availability

- ➔ **Redundancy** (πλεονασμός, π.χ. Με αντίγραφα)
- ➔ Στόχος ανοχής σε σφάλματα (fault tolerance)
  - ➢ Πλεόνασμα server
  - ➢ Backups δεδομένων
  - ➢ Γεννήτριες κλπ.
- ➔ **Patching**



Βασικές έννοιες Ρίσκου / Κινδύνου (Risk)

▲ **Risk** (Ρίσκο)

→ Η πιθανότητα μία απειλή να εκμεταλλευτεί μία αδυναμία (**Vulnerability)**, με αποτέλεσμα κάποια ζημία

▲ **Threat** (Απειλή)

→ Οποιοδήποτε γεγονός έχει την πιθανότητα να οδηγήσει σε διακινδύνευση της τριάδας C-I-A

▲ **Security Incident** (Περιστατικό Ασφάλειας)

→ Σειρά γεγονότων με αρνητική επίδραση στην C-I-A

▲ **Risk Mitigation** (Διαδικασία μείωσης ρίσκου)

Κατανόηση των τύπων ελέγχου

Technical

Χρήση τεχνολογίας για την μείωση των ευπαθειών (Encryption, Antivirus, IDS/IPS, Firewall).

Administrative

Χρήση μεθόδων που επιβάλλονται από οργανωτικές πολιτικές ή άλλους κοινούς διοικητικούς ελέγχους (Risk Assessments, Vulnerabilities Assessments).

Physical

Κάθε είδους ελέγχους που μπορούμε φυσικά να αγγίξουμε (Φωτισμός, Σήματα, Φύλακες Ασφαλείας).

Virtualization

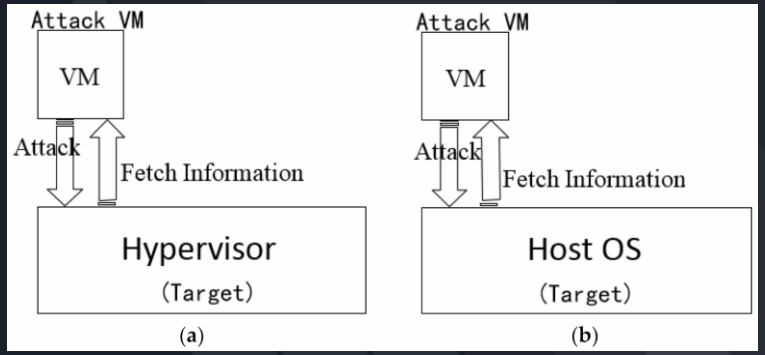
Hypervisor

Πρόγραμμα που δημιουργεί, τρέχει και διαχειρίζεται εικονικές μηχανές. Τεχνολογίες όπως VMWare, Microsoft Hyper-V, Oracle VM VirtualBox έχουν το δικό τους Hypervisor πρόγραμμα.

Κίνδυνοι του Virtualization

VM Escape

- Επίθεση που επιτρέπει σε κάποιον attacker να τρέξει κώδικα στο εικονικό σύστημα ώστε να αλληλεπιδράσει με το κεντρικό σύστημα.



VM Sprawl

- Όταν δεν γίνεται σωστή διαχείριση και ενημέρωση στις εικονικές μηχανές, υπάρχει κίνδυνος να παραμείνουν απροστάτευτες σε επιθέσεις, λόγω αδυναμιών που δεν έχουν γίνει patch.

Commands (Homework)

- ping
- ipconfig
- ip
- netstat
- tracert
- arp

Ευχαριστούμε και Happy Hacking!

Alexia (Cyberd0xed) & Chris (“Mr. Robot”)