William Prado
05/05/2025

Week 5 Network

Monday 9.1 Security Concepts

Brute Force Rainbow attack Dictionary

Confidentiality
Integrity
Availability

Non-repudiation
Risk likelihood - result of a sussesful exploitation.
threat harmful event → man made, natural
Vulnerability weakness
likelihood How many times? %, probability?
Impact high/med/low $$$

- Algorithm
  # MD5/SHA
- Symmetrics: key
  RC5, AES, 3DES, DES.
- Asymmetrics
  -ASA
  D-H
  ECC

Data
motion
Rest
use
zero-day
patch

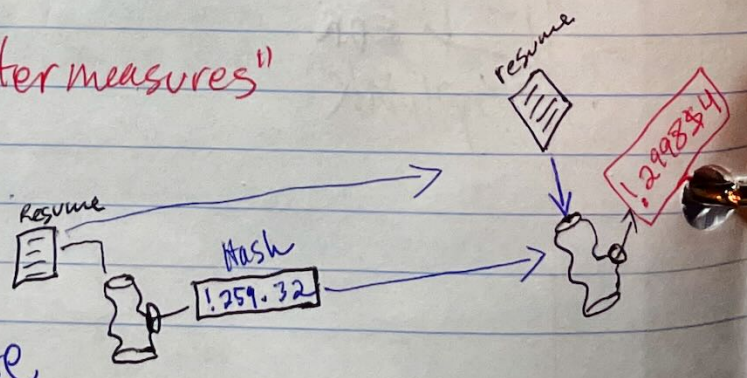
Types of Security Assessments.
Compliance Audits. compliance = "Laws"/"Regs"
Risk-Based Audits Risk = threat - harmful event
+echnical Audits

Regulatory Compliance
General Data Protection Regulation (GDPR)
GDPR = EU privacy Law

Payment Card Industry Data Security Standard (PCI DSS)
PCI DSS = credit card.

Security Controls: "countermeasures"

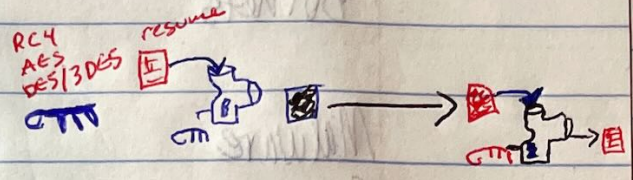
Cryptographic Concepts.
hash
-"Integrity"
-Non-reversable, file size



Willian Prado
05-05-2025
Week 5 Net+

hashing - used to validate information.
encryption - used to protect sensitive information.
Confidentiality
Hash algorithm converter

Symmetric Key - "Single" Key
Algorithm.
cypertext.
Key.



Youtube Sunny Classroom • How hash function work? Hash Algorithm
YTB Sunny • Private Key Encryption - Symmetric Key Encryption
Block Cyphers

Symmetric key encryption lets people hide & retrieve secret messages, while hashing is used to check & verify information without revealing it.

YTB Sunny • Public Key Encryption. - two different keys are used.

YTB Prof. messer Zero day vulnerabilities. cve.mitre.org
Zero day attacks.

YTB Honeypots & Honeynets.

9.2 - Threat Types & Assessments.
- Nation-State
- Interaal threat.
- Enumeration Attacks.
Enumeration - gather info about target
footprinting - non-intrusive
fingerprinting - intrusive

footprint
phone #
email address
domain name

William Prado
05/05/2025

Foot print
Finger print > Enumeration.

- Distributed DOS Attacks & Botnets.

DOS = availability
DDoS = DoS on Steroids
Botnets

Malware
Ransomware
Fileless Malware

9.3 Spoofing Attacks

Spoofing
MAC Spoofing
IP spoofing
ARP spoofing (arp cache poisining).
Email spoofing

ARP is the whole table

On Path Attacks - MiTM = man in the middle Attacker
Session Hijacking
SSL Stripping
DNS Spoofing
Wi-fi Eavesdropping
ARP Spoofing

MAC Flooding
VLan Hopping
- Switching Spoofing
- Double Tagging

Willian Prado
05-05-2025
9.04

Rogue Devices & Services

- Undetected presence
- Back-door access
- network vulnerability expoitation
- Rogue DHCP Server Attacks
  - distribute invalid configuration
  - traffic redirection

Rogue Devices
// Shadow IT"

DNS Attacks

- disrupted service
- domain hijacking
- cache poisioning

9.5. Social Engineering hacking the human.

Impesonation
Phishing
Shoulder Surfing
Dumpster Diving
Tailgating no consent
Piggybacking consent

Password Attacks

Password capture
Password hash cracking
- Dictionary
- Brute force