3 Network Security Concepts

3.1 Current State of Cybersecurity

Security Terms

- Assets: people, equipment, resources, data
- Vulnerability: weakness in a system
- Threat: potential danger
- Exploit: mechanism that takes advantage of a vulnerability
- Mitigation: counter-measure
- Risk: likelihood of a threat

Attack Vector

- External (from inside)
- Internal (from outside)

Data Loss Vectors

- Email/Social Networking
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control

3.2 Threat Actors

The Hacker

- White Hat Hackers
- Gray Hat Hackers
- Black Hat Hackers

Hacking Terms

Script Kiddies, Vulnerability Broker, Hacktivists, Cyber criminals, State-Sponsored

3.3 Threat Actor Tools

Penetration Testing Tool

- Password Crackers
- Wireless Hacking Tools
- Network Scanning
- Packet Crafting Tools
- Packet Sniffers
- Rootkit Detectors
- Fuzzers (search vulnerabilities)
- Forensic Tools
- Debuggers
- Hacking Operating Systems
- Encryption Tools
- Vulnerability Exploitation Tools
- Vulnerability Scanners

Attack Types

- Eavesdropping Attack
- Data Modification Attack
- IP Address Spoofing Attack
- Password-Based Attacks
- Denial of Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack

3.4 Malware

Types of Viruses

- Boot sector virus
- Firmware virus
- Macro virus
- Program virus
- Script virus

Type of Trojan Horse

- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- Security software disabler
- Denial of Service (DoS)
- Keylogger

Type of Trojan Horses

- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- Security software disabler
- Denial of Service (DoS)
- Keylogger

Other Types of Malware

- Adware
- Ransomware
- Rootkit
- Spyware
- Worm

3.5 Common Network Attacks

Reconnaissance Attacks

- Perform an information query of a target
- Initiate a ping sweep of the target network
- Initiate a port scan of active IP addresses
- Run vulnerability scanners
- Run exploitation tools

Access Attacks

- Password Attacks
- Spoofing Attacks

Social Engineering Attacks

- Pretexting
- Phishing
- Spear phishing
- Spam
- Something for Something
- Baiting
- Impersonation
- Tailgating
- Shoulder surfing
- Dumpster diving

DoS and DDoS Attacks

- Overwhelming Quantity of Traffic
- Maliciously Formatted Packets

3.6 IP Vulnerabilities and Threats

IPv4 and IPv6

- ICMP attacks
- Amplification and reflection attacks
- Address spoofing attacks
- Man-in-the-middle attack (MITM)
- Session hijacking

ICMP Attacks

- ICMP echo request and echo reply
- ICMP unreachable
- ICMP mask reply
- ICMP redirects
- ICMP router discovery

3.7 TCP and UDP Vulnerabilities

- TCP SYN Flood Attack
- TCP Reset Attack
- TCP Session Hijacking
- UDP Flood Attacks

3.8 IP Services

- ARP Cache Poisoning
- ARP Spoofing
- DNS cache poisoning attacks
- DNS amplification and reflection attacks
- DNS resource utilization attacks
- Fast Flux
- Double IP Flux
- Domain Generation Algorithms
- DNS Tunneling
- DHCP Spoofing Attack

3.9 Network Security Best Practices

- Confidentiality, Integrity, and Availability
- The Defense-in-Depth Approach
- Firewalls
- IPS
- Content Security Appliances
  - Cisco Email Security Appliance (ESA)
  - Cisco Web Security Appliance (WSA)

3.10 Cryptography

- Data Integrity
  - Hash Functions (MD5, SHA, SHA-2)
- Origin Authentication: HMAC
- Data Confidentiality
  - Symmetric Encryption: DES, 3DES, AES, SEAL, RC
  - Asymmetric Encryption: DH, DSS, DSA, RSA; ElGamal, Elliptical Curve
- Data Non-Repudiation