Chapter 10
Malware Attacks

Session Hijacking

- Hijacking Steps
  - Sniff the traffic between the client and the server
  - Monitor the traffic and predict the sequence numbering
  - Desynchronize the session with the client
  - Predict the session token and take over the session
  - Inject packets to the target server
- Countermeasures
  - Unpredictable Session IDs
  - Limit Incoming Connections
  - Minimize Remote Access
  - Regenerate Session Keys
  - IPSec
    - Modes
      - Transport Mode
        - Encryption & Authentication Each Packet
        - Payload Encrypted
        - ESP Trailer Encrypted
        - IP Header of Original Packet Not Encrypted
      - Tunnel Mode
        - May Be Used In NAT
        - Encrypts Everything
        - Incompatible with NAT
    - Architecture
      - Autentication Header (AH)
      - Encapsulating Security Payload (ESP)
      - Internet Key Exchange (IKE)
        - Oakley
        - ISAKMP

Denial of Service

- DoS vs DDoS
- Categories
  - Volumetric Attacks (L3)
  - Protocol Attacks (L4)
  - Application Attacks (L5/L7)
- Metrics
  - bps
  - pps
  - rps
- Types
  - Protocol
    - TCP Exhaustion
    - Volumetric
      - UDP Flood
    - Protocol
      - SYN Attack
      - SYN Flood
      - ICMP Flood
    - Protocol
      - Smurf
  - Application
    - Ping of Death
    - Teardrop
    - Pulse Wave
    - Zerodays
  - Physical Destruction/Bricking
- Tools
  - LOIC/HOIC
  - Slowloris
  - Trinity
  - RUDY

Concepts

- Malicious Code — Functionality of Malware
- Payload — Action on Target
- Exploit — Explore System Vulnerabilties
- Injector — Inject Code Into Running Processes
- Downloader — Program That Downloads Malware
- Dropper — Program That Unpacks Malware
- Obfuscator — Program That Camouflages Malware
- Wrappers — Bind Malware With Legitimate Software
- Fileless Malware — Resides in RAM, No Files on Disk
- Packers/Crypters

Malware Distribution

- Malvertising
- Drive-By
- Compromised Legitimate Sites
- Social Engineering
  - Clickjacking
  - SPAM Emails
  - Spear Phishing
- Manually Install on Target

Trojans

- Keylogger
- Proxy Server
- Botnet
- RAT
- E-banking
- Shell
- Ransomware
- Persistence
  - Windows
    - Registry
    - Run
    - RunOnce
    - RunServices

Communication

- Channels
  - Overt — Legitimate Communication Channels
  - Covert — Communication Channels Used In Unintented Way
- Tools
  - netstat
  - CurrPorts
  - Sysinternals
  - Sysanalyzer
  - Active Registry Monitor
  - Wireshark

Virus and Worms

- Self-replicating
- Reproduces Its Code
- Attaches to Other Executables

Malware Analysis

- Methods
  - Static Analysis
  - Dynamic Analysis
- Techniques
  - File Fingerprinting
  - Malware Scanning
  - String Search
  - Identify Packaging/Obfuscation
  - PE Info
  - File Dependencies
  - Disassembly
  - Use Sandboxes
  - Open/Closed Ports
  - API Calls
  - Network Traffic

XMind Evaluation Mode