Attack Methodology

Table of Contents

Recon

- Passive
  - OSINT/Search Engines: publicly available data about subcomponents
  - Social Media: Mapping responsible users for social engineering
  - Public Databases: Using databases like Whois about DNS
  - Social Engineering: Seeking contact
  - Eavesdropping: Listening in public settings
  - OS Fingerprints: Analyze packets to determine OS
- Active
  - Port Scan: Use tools like Nmap
  - Network Map: Creating Diagrams on devices and connections
  - Vulnerability Scanning: Scanning open servers
  - Service Fingerprint: identify type/version of services running
  - DNS Enumeration: Gathering info on DNS records
  - Traceroute: Mapping network paths to reach target
  - Banner Grabbing: Observing response headers from services

Access

- Phishing/Social Engineering
- Exploitation of Vulnerabilities
- Credential stuffing/Password Spraying
    - Using stolen credentials and applying across multiple entry points
    - Using public emails/usernames and applying common passwods

Execution

- Malware Deploy
- Boot or Logon Autostart Execution
  - Create system tasks
  - Modify Boot Execute Value
  - Place Executables in startup folders
  - Add Malware to Registry Run Keys
- Process Injection
  - Choose legitimate process
  - Allocate memory for the target process
  - Write the malicious code into the memory
  - Execute thread in existing process

Escalation

- Exploiting Vulnerabilities
- Lateral Movement

Exfiltration

- Stealing Sensitive Information
- Secure Data Transmission

Covering (OS Command Injection)

- Log Manipulation
- Log Deletion
- Data Destruction

Advanced Techniques

- Supply Chain Attacks
- Zero Day Vulnerability
- AI Enhanced Credential Attacks
- AI Enhanced Ransomware

Questions?