Pentest +
Post Exploit Activities

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Post Exploit Activities

Post exploitation activities depends highly on which stage in the exploitation process / cyber-kill chain the attacker is in. In early stages the attacker will seek to analyze the information obtained in the previous exploitation and filter it for highly valuable information that can lead to privilege escalation on the current exploited system, or to gain access to another system on the network. In later stages of the cyber kill chain, the attacker will seek to exfiltrate valuable data directly or through a proxy chain and possibly conduct parallel operations such as encrypting organizational data.

During the process the attacker must take caution to avoid detection which means to remain as invisible on the network as possible. This can be done by piggy-backing on whitelisted applications through trojanized versions, or impersonating legitimate traffic such as web-traffic.

Authorization Vectors

Credential Attacks

- The goal is to be able to authenticate to increase authorization to resources
- Utilization of any passwords obtained during initial exploitation
- **OWASP Password Storage Cheat Sheet**
  - https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html
- **Obtain Credentials**
  - **pwdump** can acquire Windows passwords from **Windows Security Account Manager** or **SAM**
  - **/etc/passwd** and hashed passwords in **/etc/shadow**
  - **cachedump** and **creddump** from the **Windows Registry**
  - **SQL Queries** against databases can provide password hashes and usernames, email addresses, etc
  - Sniffing passwords on the network
  - **Mimikatz**
    - Windows post exploitation toolkit
    - Available in many forms

        - Meterpreter scripts
        - Stand-alone tool
        - Empire Powershell tool
        - PowerSploit
- **Pass the hash attacks**
    - https://capec.mitre.org/data/definitions/644.html
    - By obtaining an account's hashed credentials, the hash values can be passed to a system or service to authenticate, without needing to brute-force the hashes to obtain their cleartext values

Privilege escalation

- https://capec.mitre.org/data/definitions/233.html
- Elevate their privilege and perform an action that they are not supposed to be authorized to perform
- If the escalation cannot be done vertically (raised to higher level of privileges) perhaps it can be done horizontally to another user account with different access to resources
- Write access to executable files that will be executed by application or service with higher level of privilege is most fundamental method
- **Vertical escalation**
    - Gaining higher level privileges
- **Horizontal escalation**
    - Gaining access to another non-admin user account
- **Search for read / write access** to files and folders
    - https://askubuntu.com/questions/746818/terminal-list-all-directories-for-which-a-user-or-group-has-write-permission
- **List all users**
    - cut -d
    - -f 1 /etc/passwd
- **List all groups**
    - cut -d
    - -f 1 /etc/group
- **Get user home directory**
    - getent passwd user-name| cut -d: -f 6
- **Get all directories a user has write permission to**
    - sudo find -type d \(\(-user ftpgisdata -perm /u=w \) -o \(-group ftpgisdata -perm /g=w \) -o -perm /o=w \)
- There are different exploit classes for privilege escalation:
    - **Kernel exploits**
        - Very common for vertical escalation
    - **Application and service exploits**
        - Target accounts that the service runs under or target the application itself

- **Database privileges**
  - SQL injection or other database software flaws to query data
- **AC control configuration flaws**
  - **$ du /** in linux to see all directories you have read access to

Detection Evasion

- Using scheduler / cron
- **Inetd (Xinetd, Rlinetd, systemd)**
  - Install the malware as a service that is enabled at boot / runtime
- Getting into a lower runtime level you can install service as a privileged user
- Accessing other runtime levels
  - During the boot sequence can allow privilege escalation
  - Higher privileges can allow privileged logs to be modified
- Shimming existing services by replacing compiled binaries
  - **rkhunter** can scan files to notice modification of critical executable / binaries / system files
- **Trojan / Backdoor** can be effective at hiding a rouge process but usually more easily detected by virus **scanners / IDS**
- **Creating new users**
  - Easily detected by blue-team if using scanners on hosts
- **Clearing up logs**
  - Can be **simple or very complex**
  - **Sometimes impossible** depending on attack type, tools used, the network configuration / architecture
  - **Log files**
    - Do not simply delete or clear log files. This can look suspicious
    - **cat file.log | grep -r "[IP address or UUID]" > file.log**
    - Evading network detection on the LAN / Gateway
      - Advanced Penetration Testing: Hacking the World's Most Secured Networks by Will Allsopp (2017)
      - Developing tools such as malware / trojans / remote persistence tools that **do not look out of place** for normal network traffic
      - Anti-analysis
      - Anti-forensics
      - Packers
      - Encoders
- **Shutting down processes**
  - Disable virus scanners, or other network security applications to avoid detection

Pivoting

- **Re-map the network** from the perspective of a compromised system
- Passively listening to **ARP queries, SNMP** broadcast packets on the network can reveal information about network without scanning
- Identify new targets
- Attack network protocols
- Circumvent security controls such as NAC or encryption, authentication

VLAN hopping

- **Double tagging**
  - Used on 802.1Q (Dot1q) **trunked interfaces**
  - Modifying ethernet frames to include a second header with the second header destined for the target VLAN
  - Mostly useless since responses will not be routed back to
  - Largely mitigated
- **Switch spoofing**
  - Relies on making the attacking host act like trunking switches which allows other VLAN traffic to be forwarded to it
  - Requires that local network devices are configured to allow the attacking host to negotiate trunks with interface set to dynamic desirable, dynamic auto, or trunk mode
- **Versinia** tool in Kali Linux can perform these types of VLAN hopping attacks
- **Layer 2 attacks**
- **Spanning tree protocol**
- **DHCP**
- **802.1Q trunking attacks**

Network Proxies

- SOCKS connections
- SOCKS proxies
- Socket Secure Proxy via SSH
- ARP cache poisoning can allow system to proxy for another system on network

DNS Cache Poisoning

- A poisoned or MiTM DNS service can redirect URL requests to a rouge IP / host
- A race condition can also allow attacker to poison a DNS cache
- Some CVEs against DNS server

MiTM Man In The Middle

- Passive MiTM attack can sniff traffic

- Active MiTM attack can modify unencrypted traffic
- MiTM can intercept encrypted HTTPS traffic if client endpoints can be confirmed to accept a self-signed certificate or stolen certificate
- **Relay attacks**
  - Intercept traffic for other physical layer protocols such as Bluetooth, RFID, etc.
- **Replay Attacks**
  - A form of MiTM attack that captures and then re-uses the data captured
  - **Credentials of some protocols can be captured** and replayed, or decrypted using rainbow-tables
  - Pass the hash is an attack on **NTLM**, although NTLM is mostly depreciated
  - **Responder** or other tools can intercept
  - https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
  - Replay attacks are getting harder to conduct since most modern services use encryption and handshake with nonces

ARP Address Resolution Protocol Spoofing

- Used to map IP addresses to MAC address
- Race condition can allow attacker to spoof ARP requests to the gateway / router
- The ARP information is stored on clients in the ARP cache file
- The attacker can intercept traffic and act as a MiTM
- Kali Linux has **arpspoof** command:
- arpspoof -i eth0 -t 10.0.2.7 -r 10.0.2.1
- -t = target IP, -r = router IP / switch IP
- Metasploit contains arp poisoning tools (auxiliary/spoof/arp_poisoning)
- Tools exist to detect / mitigate ARP spoofing
- Highly likely to be detected

NAC Network Access Controller Bypass

- Modern networks often require **remote attestation** of devices to **provide security checks** before connecting to a wireless or even wired ethernet LAN connection.
- **Software client** on the client device can communicate with NAC when connecting / while connected
- DHCP client that listens for traffic like DHCP requests
- **Querying switches** with SNMP to find new devices connected to the network
- Sometimes MAC filtering can be bypassed by spoofing a MAC address

Pivoting Windows Networks

- **NetBIOS Name Resolution Exploits**
  - Network File Sharing

    - Most local resources do not have DNS entries so the NetBIOS server is queried
    - **Spoofed response** can redirect traffic and allow proxy / MiTM sniffing and injection
    - Windows IP resolution process
        1. **Local host file**
            - C:/Windows/System32/drivers/etc/hosts
        2. **DNS via local cache** and then **via DNS server**
        3. **NBNS NeBIOS name service**
            - Link Local Multicast Name Resolution (LLMNR)
            - NetBIOS Na**me Server NetBIOS-NS**
- Windows Ports
    - **135/TCP MS-RPC** endpoint matter (epmap)
    - **137/UDP NetBIOS** name service
    - **138/UDP NetBIOS** datagram service
    - **139/TCP NetBIOS** session service
    - **445/TCP SMB**
    - **5535/UDP LLMNR** (multicast address of 224.0.0.252 for response to all network nodes)
- **Tools**
    - **Metasploit**
        - Modules for Windows that capture authentication hash to allow cracking
    - **Reponder**
        - Good for exploiting NetBIOS and LLMNR by responding to queries with rouge address
        - After capturing authentication data, it can be relayed to the NTLM server and allow remote code execution
        - https://notsosecure.com/pwning-with-responder-a-pentesters-guide/
        - **Mimikatz** built into **Responder** can capture more data for pivoting
- **Windows Network Discovery Commands**
    - Build into every system
    - **net view /domain –** List hosts in current domain
    - **net user /domain –** Lists users in current domain
    - **net accounts /domain –** Shows domain password policy
    - **net group /domain –** List groups in the domain
    - **net group 'Domain Admins' /domain –** List admin groups in the domain
    - **net share –** Shows current SMB shares
    - **net session –** Used to review SMB sessions
        - Used with find command can find active sessions
    - **net share [name-of-share] c:\directory/of/your/choice /GRANT:Everyone,FULL**
        - Grants access to a folder for any user with full rights

Cross compiling

- Exploit tool kits for the specific architecture platform you have gained access to may be required if binaries can't be transferred

Data Exfiltration

Removing Encryption

- **SSL Stripping Attacks**
  - Downgrading HTTPS to HTTP
  - All modern browsers warn people about SSL stripping attacks by validating certificates, expiration dates, etc.
  - **POODLE** is one such attack (??)
  - Local policies like certificate pinning can mitigate
  - Server policies like HSTS can mitigate
  - Modern browsers can be configured to accept rouge self-signed HTTPS certificates, and the attacker can MiTM and replace the certificates
- **SSL Downgrade Attacks**
  - MiTM can modify parts of the SSL/TLS handshake to remove ciphers from the list that are exchanged between the browser and server. The server or client will then downgrade the SSL/TLS version to one of the items listed in the handshake data.
  - Server can be configured to NOT accept legacy SSL / TLS version that are weak or have known vulnerabilities.
  - The client / server handshake will be dropped in the case that the client requests an SSL cipher that the sever does not support

Data Exfiltration

- Usually the final stage / goal in an attackers campaign, but can also happen in stages
- Large amounts of data being sent can lead to detection by an organization's IT security team / services
- Possible that using **HTTPS port 443** can reduce chances of being detected
- Also **piggy-backing on another service** and / or **through proxy-chain** can reduce detection chances
- Encrypted data can be exfiltrated for off-site decryption
- Backups contained in devices such as NAS can also be probed for valuable files
- Defensive security term for preventing data exfiltration or destruction is **data-loss-prevention** which can also refer to human error causing data-loss
- **Valuable data includes**
  - Organizational usernames, passwords / password hashes
  - Other authentication related information
  - Information associated with strategic business decisions
  - Intellectual Property, research and R&D documents
  - Cryptographic keys
  - Personal / corporate financial information
  - Personally identifiable information (PII), email addresses, names, social security numbers

    - Mailing addresses
    - Sensitive government documents

DOS Attacks and Stress Testing

- Penetration into the network may allow attacker to generating large amounts of network traffic which can result in DOS of the network due to congestion
- Unlikely that a modern APT attacker would simply DOS after gaining access
- Most pen-test engagements specifically prohibit DOS attacks
- **Stress testing** is a specific form of pen-test aimed at creating DOS effect
- Toolkits such as:
    - **Metasploit**
    - **hping**
    - **HTTP Unbearable Load King (HULK)**
    - **Low Orbit Ion Cannon (HOIC)**
    - **slowloris**
- Types of DOS:
    - **Application layer** seeking to crash service or whole server
    - **Protocol** based takes advantage of flaw in protocol such as amplification
    - **Traffic volume** DOS attacks
    - Amplification attacks
    - Synflood attacks