
ATTACK
DEFENSE
by PentesterAcademy

Name	Samba Recon: Basics II
URL	https://www.attackdefense.com/challengedetails?cid=554
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. Find the OS version of samba server using rpcclient.

Answer: 6.1

Commands:
rpcclient -U "" -N 192.144.106.3
srvinfo

```
root@attackdefense:~# rpcclient -U "" -N 192.144.106.3
rpcclient $> srvinfo
        SAMBA-RECON    Wk Sv PrQ Unx NT SNT samba.recon.lab
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03
rpcclient $>
```

Q2. Find the OS version of samba server using enum4Linux.

Answer: 6.1

Command: enum4linux -o 192.144.106.3

```
root@attackdefense:~# enum4linux -o 192.144.106.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon May 27 14:12:13 2019

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.144.106.3
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================================
|    Enumerating Workgroup/Domain on 192.144.106.3    |
 ======================================================
[+] Got domain/workgroup name: RECONLABS

 =====================================
|    Session Check on 192.144.106.3    |
 =====================================
[+] Server 192.144.106.3 allows sessions using username '', password ''
```

```
 =====================================
|    Session Check on 192.144.106.3    |
 =====================================
[+] Server 192.144.106.3 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.144.106.3    |
 ============================================
Domain Name: RECONLABS
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 =====================================
|    OS information on 192.144.106.3    |
 =====================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.144.106.3 from smbclient:
[+] Got OS info for 192.144.106.3 from srvinfo:
        SAMBA-RECON    Wk Sv PrQ Unx NT SNT samba.recon.lab
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03
enum4linux complete on Mon May 27 14:12:13 2019

root@attackdefense:~#
```

Q3. Find the server description of samba server using smbclient.

Answer: samba.recon.lab

Command: smbclient -L 192.144.106.3 -N

```
root@attackdefense:~# smbclient -L 192.144.106.3 -N

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk
        john            Disk
        aisha           Disk
        emma            Disk
        everyone        Disk
        IPC$            IPC       IPC Service (samba.recon.lab)
Reconnecting with SMB1 for workgroup listing.

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

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

Q4. Is NT LM 0.12 (SMBv1) dialects supported by the samba server? Use appropriate nmap script.

Answer: supported.

Command: nmap -p445 --script smb-protocols 192.144.106.3

```
root@attackdefense:~# nmap -p445 --script smb-protocols 192.144.106.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 14:21 UTC
Nmap scan report for s1sicfgz3w4u3haf07vlxlshg.temp-network_a-144-106 (192.144.106.3)
Host is up (0.000062s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:42:C0:90:6A:03 (Unknown)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
root@attackdefense:~#
```

Q5. Is SMB2 protocol supported by the samba server? Use smb2 metasploit module.

Answer: Supported

Commands:
msfconsole
use auxiliary/scanner/smb/smb2
set RHOSTS 192.144.106.3
exploit

```
msf5 > use auxiliary/scanner/smb/smb2
msf5 auxiliary(scanner/smb/smb2) > set RHOSTS 192.144.106.3
RHOSTS => 192.144.106.3
msf5 auxiliary(scanner/smb/smb2) > exploit

[+] 192.144.106.3:445     - 192.144.106.3 supports SMB 2 [dialect 255.2] and has been online for 3667622 hours
[*] 192.144.106.3:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb2) >
```

Q6. List all users that exists on the samba server using appropriate nmap script.

Answer: admin, aisha, elie, emma, john, shawn

Command: nmap --script smb-enum-users.nse -p445 192.144.106.3

```
root@attackdefense:~# nmap --script smb-enum-users.nse -p445 192.144.106.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 14:28 UTC
Nmap scan report for s1sicfgz3w4u3haf07vlxlshg.temp-network_a-144-106 (192.144.106.3)
Host is up (0.000044s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:42:C0:90:6A:03 (Unknown)

Host script results:
| smb-enum-users:
|   SAMBA-RECON\admin (RID: 1005)
|     Full name:
|     Description:
|     Flags:       Normal user account
|   SAMBA-RECON\aisha (RID: 1004)
|     Full name:
|     Description:
|     Flags:       Normal user account
|   SAMBA-RECON\elie (RID: 1002)
|     Full name:
|     Description:
|     Flags:       Normal user account
|   SAMBA-RECON\emma (RID: 1003)
|     Full name:
|     Description:
|     Flags:       Normal user account
|   SAMBA-RECON\john (RID: 1000)
|     Full name:
|     Description:
|     Flags:       Normal user account
|   SAMBA-RECON\shawn (RID: 1001)
|     Full name:
|     Description:
|_    Flags:       Normal user account

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
root@attackdefense:~#
```

Q7. List all users that exists on the samba server using smb_enumusers metasploit modules.

Answer: john, elie, aisha, shawn, emma, admin

Commands:
msfconsole
use auxiliary/scanner/smb/smb_enumusers
set RHOSTS 192.144.106.3
exploit

```
msf5 > use auxiliary/scanner/smb/smb_enumusers
msf5 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.144.106.3
RHOSTS => 192.144.106.3
msf5 auxiliary(scanner/smb/smb_enumusers) > exploit

Error: 192.144.106.3 Rex::Proto::DCERPC::Exceptions::NoResponse no response from dcerpc service
[+] 192.144.106.3:445     - SAMBA-RECON [ john, elie, aisha, shawn, emma, admin ] ( LockoutTries=0 PasswordMin=5 )
[*] 192.144.106.3:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_enumusers) >
```

Q8. List all users that exists on the samba server using enum4Linux.

Answer: john, elie, aisha, shawn, emma, admin

Command: enum4linux -U 192.144.106.3

```
root@attackdefense:~# enum4linux -U 192.144.106.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon May 27 15:13:26 2019

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.144.106.3
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.144.106.3    |
 =====================================================
[+] Got domain/workgroup name: RECONLABS

 ====================================
|    Session Check on 192.144.106.3    |
 ====================================
[+] Server 192.144.106.3 allows sessions using username '', password ''
```

```
 ============================================
|    Getting domain SID for 192.144.106.3    |
 ============================================
Domain Name: RECONLABS
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ==============================
|    Users on 192.144.106.3    |
 ==============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: john     Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elie     Name:   Desc:
index: 0x3 RID: 0x3ec acb: 0x00000010 Account: aisha    Name:   Desc:
index: 0x4 RID: 0x3e9 acb: 0x00000010 Account: shawn    Name:   Desc:
index: 0x5 RID: 0x3eb acb: 0x00000010 Account: emma     Name:   Desc:
index: 0x6 RID: 0x3ed acb: 0x00000010 Account: admin    Name:   Desc:
```

Q9. List all users that exists on the samba server using rpcclient.

Answer: john, elie, aisha, shawn, emma, admin

Commands:

rpcclient -U "" -N 192.144.106.3

enumdomusers

```
root@attackdefense:~# rpcclient -U "" -N 192.144.106.3
rpcclient $> enumdomusers
user:[john] rid:[0x3e8]
user:[elie] rid:[0x3ea]
user:[aisha] rid:[0x3ec]
user:[shawn] rid:[0x3e9]
user:[emma] rid:[0x3eb]
user:[admin] rid:[0x3ed]
rpcclient $>
```

Q10. Find SID of user "admin" using rpcclient.

Answer: S-1-5-21-4056189605-2085045094-1961111545-1005

Commands:
rpcclient -U "" -N 192.144.106.3
lookupnames admin

```
root@attackdefense:~# rpcclient -U "" -N 192.144.106.3
rpcclient $> lookupnames admin
admin S-1-5-21-4056189605-2085045094-1961111545-1005 (User: 1)
rpcclient $>
```

References:

1. Samba (https://www.samba.org/)
2. smbclient (https://www.samba.org/samba/docs/current/man-html/smbclient.1.html)
3. enum4Linux (https://tools.kali.org/information-gathering/enum4linux)
4. rpcclient (https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html)
5. Nmap Script: smb-protocols (https://nmap.org/nsedoc/scripts/smb-protocols.html)
6. Nmap Script: smb-enum-users (https://nmap.org/nsedoc/scripts/smb-enum-users.html)
7. Metasploit Module: SMB 2.0 Protocol Detection (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb2)
8. Metasploit Module: SMB User Enumeration (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_enumusers)