ATTACK DEFENSE

by PentesterAcademy

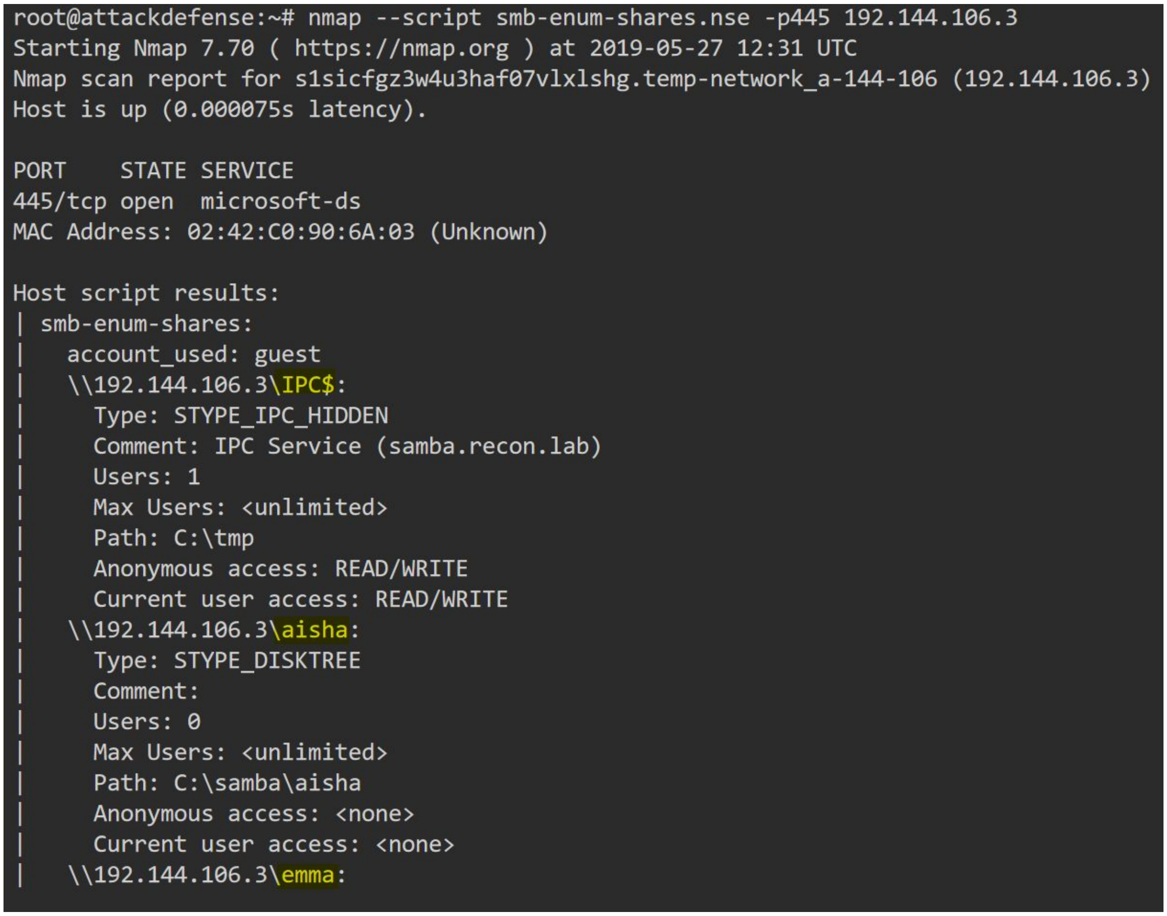
Name	Samba Recon: Basics III
URL	https://www.attackdefense.com/challengedetails?cid=555
Type	Network Recon : SMB Servers

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.

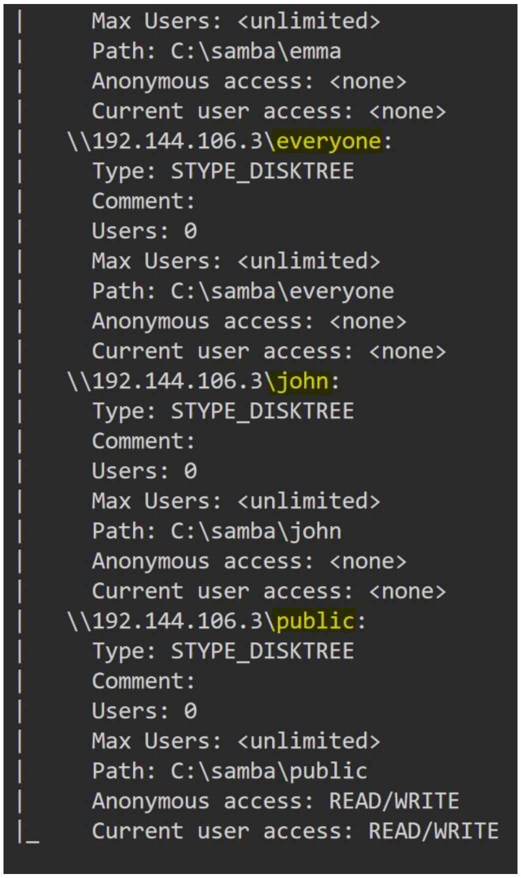
Q1. List all available shares on the samba server using nmap script.

Answer: IPC$, aisha, emma, everyone, john, public

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



```
root@attackdefense:~# nmap --script smb-enum-shares.nse -p445 192.144.106.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 12:31 UTC
Nmap scan report for s1sicfgz3w4u3haf07vlxlshg.temp-network_a-144-106 (192.144.106.3)
Host is up (0.000075s latency).

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

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.144.106.3\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (samba.recon.lab)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.144.106.3\aisha:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\aisha
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.144.106.3\emma:
```

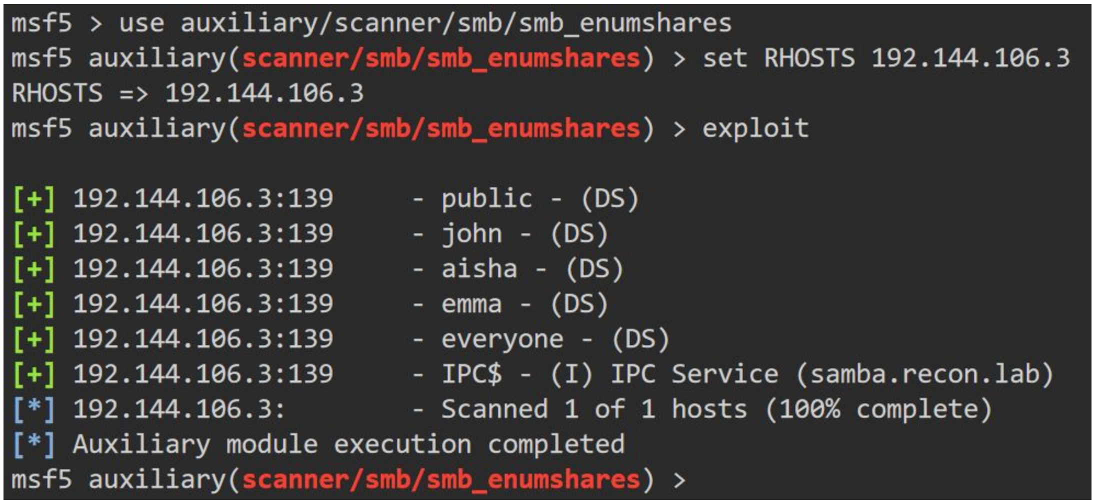


```
|     Max Users: <unlimited>
|     Path: C:\samba\emma
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.144.106.3\everyone:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\everyone
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.144.106.3\john:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\john
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.144.106.3\public:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\public
|     Anonymous access: READ/WRITE
|_    Current user access: READ/WRITE
```

Q2. List all available shares on the samba server using smb_enumshares metasploit module.

Answer: public, john, aisha, emma, everyone, IPC$

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

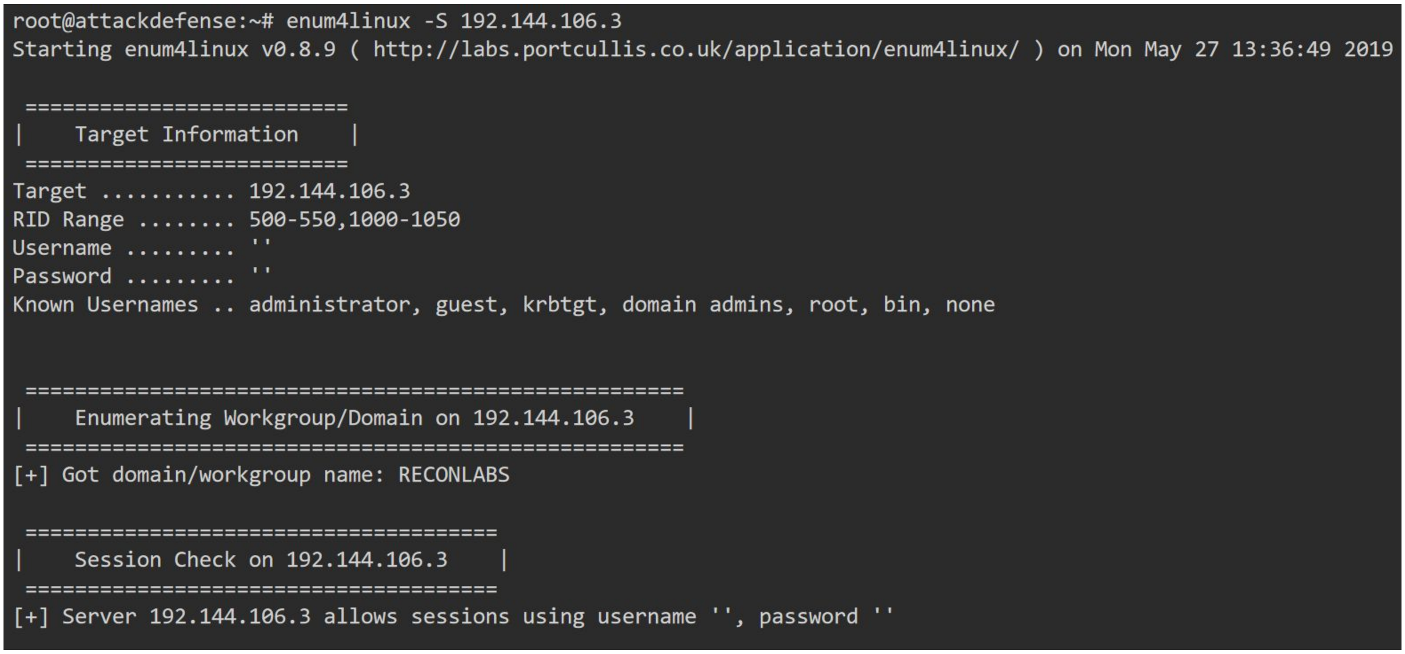


```
msf5 > use auxiliary/scanner/smb/smb_enumshares
msf5 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.144.106.3
RHOSTS => 192.144.106.3
msf5 auxiliary(scanner/smb/smb_enumshares) > exploit

[+] 192.144.106.3:139     - public - (DS)
[+] 192.144.106.3:139     - john - (DS)
[+] 192.144.106.3:139     - aisha - (DS)
[+] 192.144.106.3:139     - emma - (DS)
[+] 192.144.106.3:139     - everyone - (DS)
[+] 192.144.106.3:139     - IPC$ - (I) IPC Service (samba.recon.lab)
[*] 192.144.106.3:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_enumshares) >
```

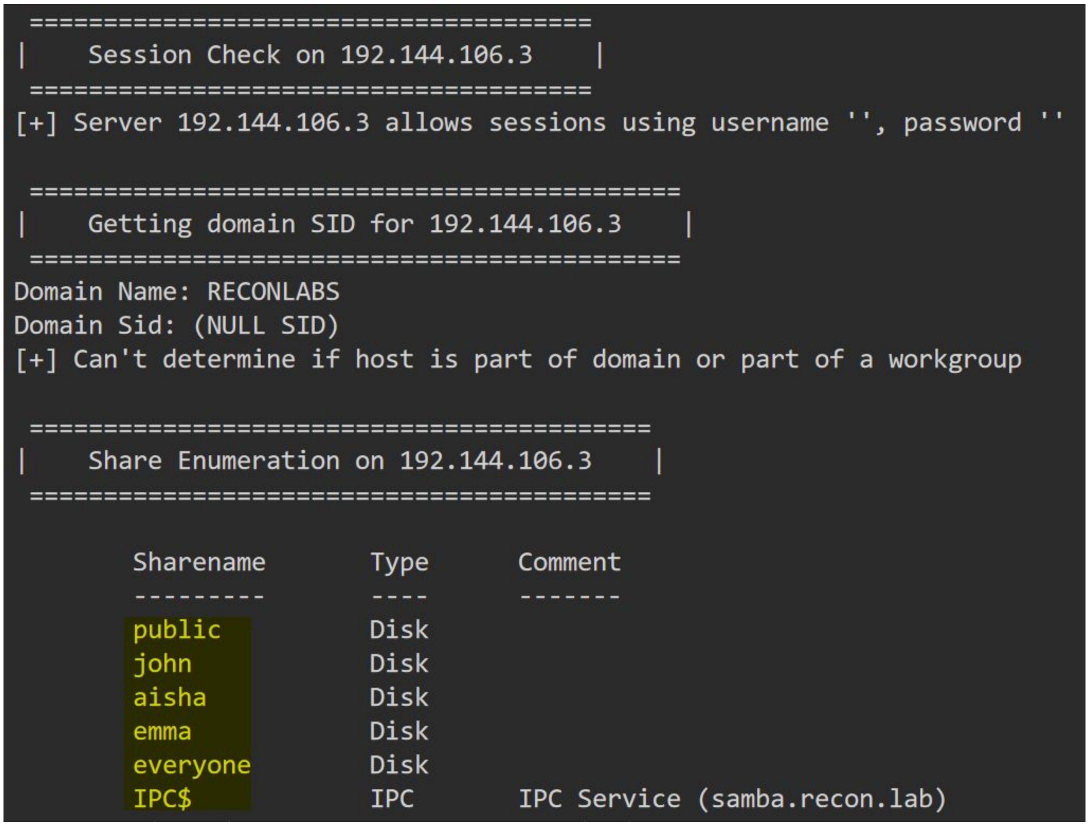
Q3. List all available shares on the samba server using enum4Linux.

Answer: public, john, aisha, emma, everyone, IPC$

Command: enum4linux -S 192.144.106.3



```
root@attackdefense:~# enum4linux -S 192.144.106.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon May 27 13:36:49 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 ''
```

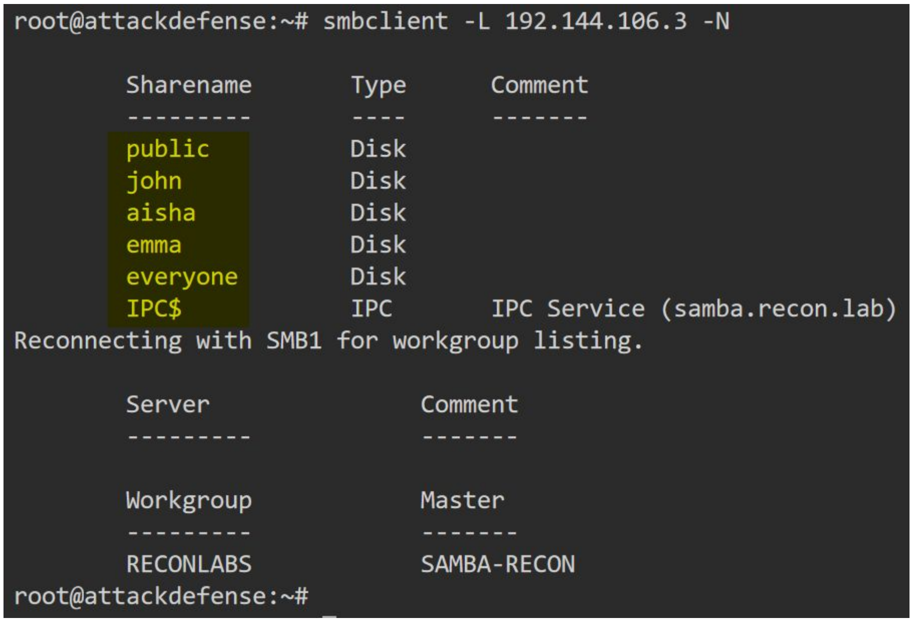


```
 ======================================
|    Session Check on 192.144.106.3    |
 ======================================
[+] Server 192.144.106.3 allows sessions using username '', password ''

 ============================================
|    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

 ==========================================
|    Share Enumeration on 192.144.106.3    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk
        john            Disk
        aisha           Disk
        emma            Disk
        everyone        Disk
        IPC$            IPC       IPC Service (samba.recon.lab)
```

Q4. List all available shares on the samba server using smbclient.

Answer: public, john, aisha, emma, everyone, IPC$

Command: smbclient -L 192.144.106.3 -N

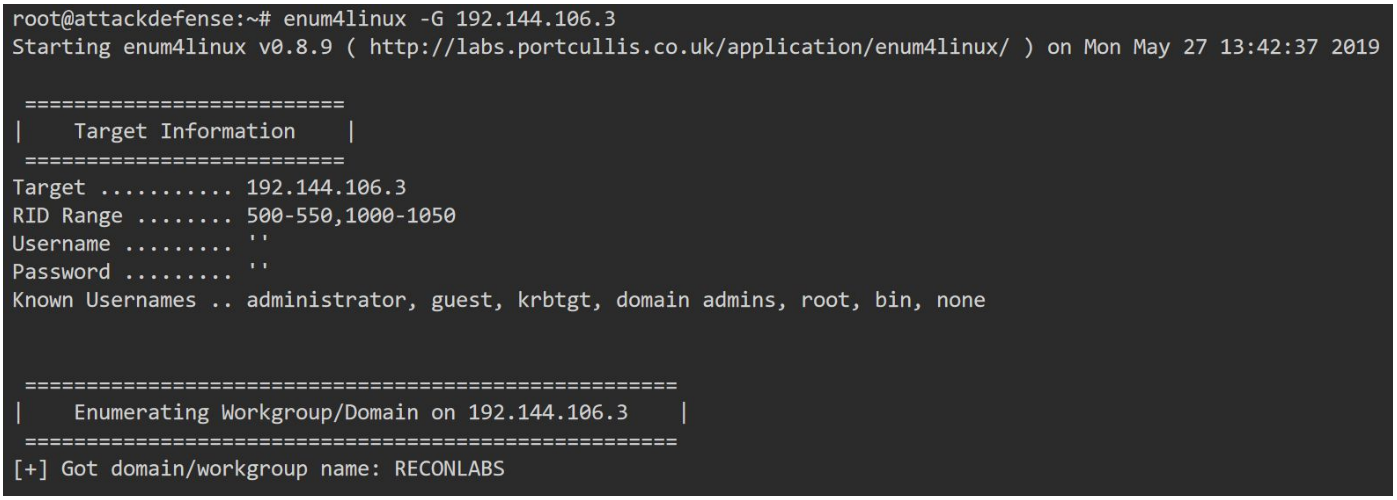


```
root@attackdefense:~# smbclient -L 192.144.106.3 -N

        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:~#
```

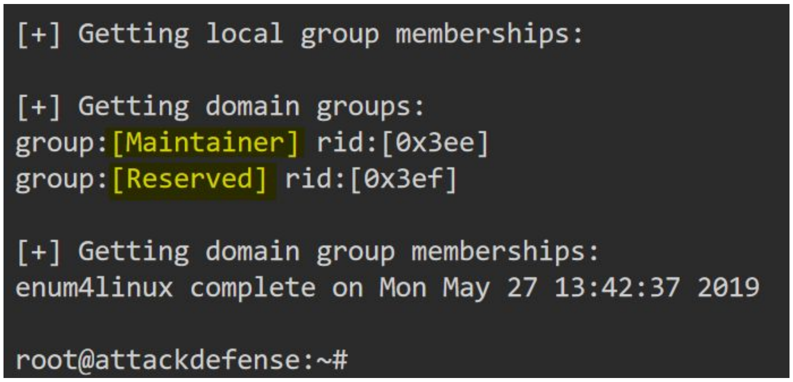
Q5. Find domain groups that exists on the samba server by using enum4Linux.

Answer: Maintainer, Reserved

Command: enum4linux -G 192.144.106.3



```
root@attackdefense:~# enum4linux -G 192.144.106.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon May 27 13:42:37 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
```

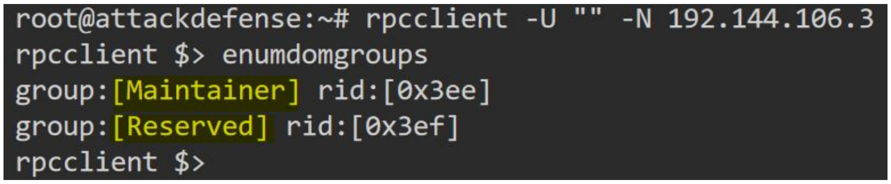


```
[+] Getting local group memberships:

[+] Getting domain groups:
group:[Maintainer] rid:[0x3ee]
group:[Reserved] rid:[0x3ef]

[+] Getting domain group memberships:
enum4linux complete on Mon May 27 13:42:37 2019

root@attackdefense:~#
```

Q6. Find domain groups that exists on the samba server by using rpcclient.

Answer: Maintainer, Reserved

Commands:
rpcclient -U "" -N 192.144.106.3
enumdomgroups

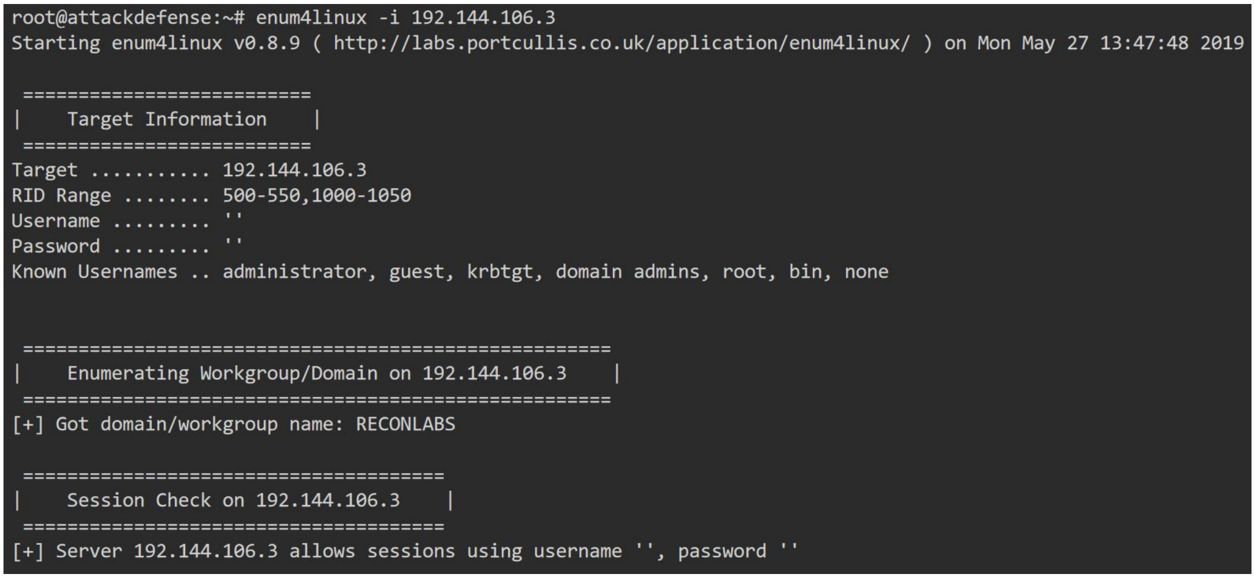


```
root@attackdefense:~# rpcclient -U "" -N 192.144.106.3
rpcclient $> enumdomgroups
group:[Maintainer] rid:[0x3ee]
group:[Reserved] rid:[0x3ef]
rpcclient $>
```

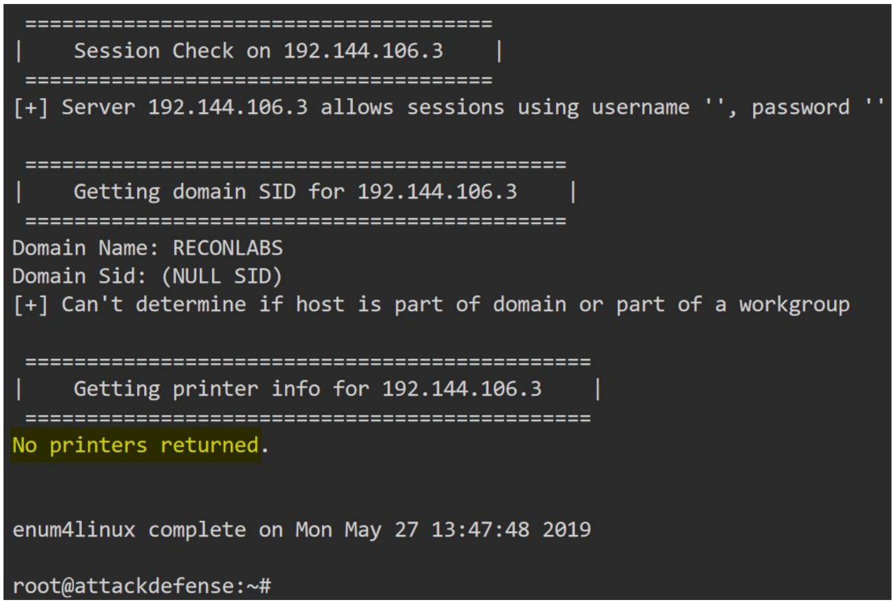
Q7. Is samba server configured for printing?

Answer: No

Command: enum4linux -i 192.144.106.3



```
root@attackdefense:~# enum4linux -i 192.144.106.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon May 27 13:47:48 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 ''
```

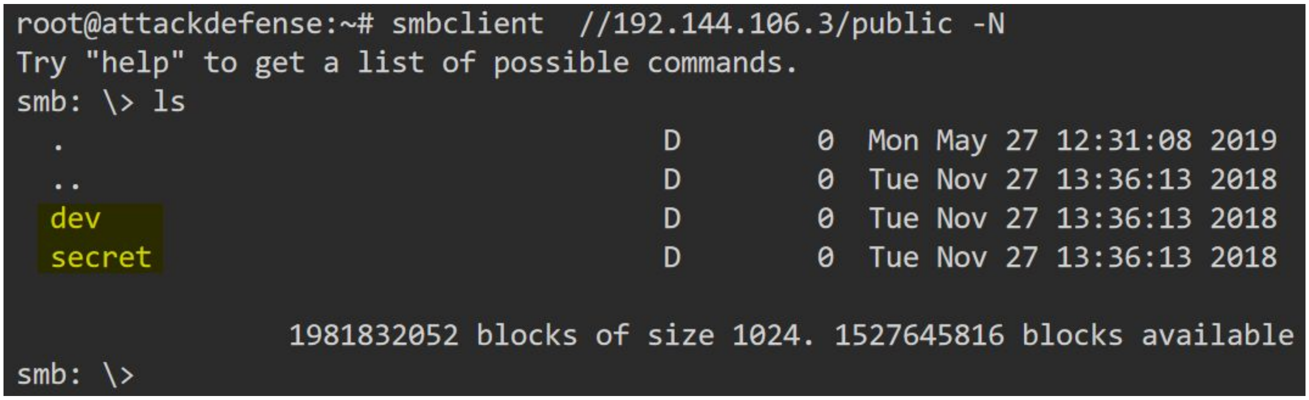


```
 ======================================
|    Session Check on 192.144.106.3    |
 ======================================
[+] Server 192.144.106.3 allows sessions using username '', password ''

 ============================================
|    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

 ==============================================
|    Getting printer info for 192.144.106.3    |
 ==============================================
No printers returned.


enum4linux complete on Mon May 27 13:47:48 2019

root@attackdefense:~#
```

Q8. How many directories are present inside share “public”?

Answer: 2

Command: smbclient //192.144.106.3/public -N
ls



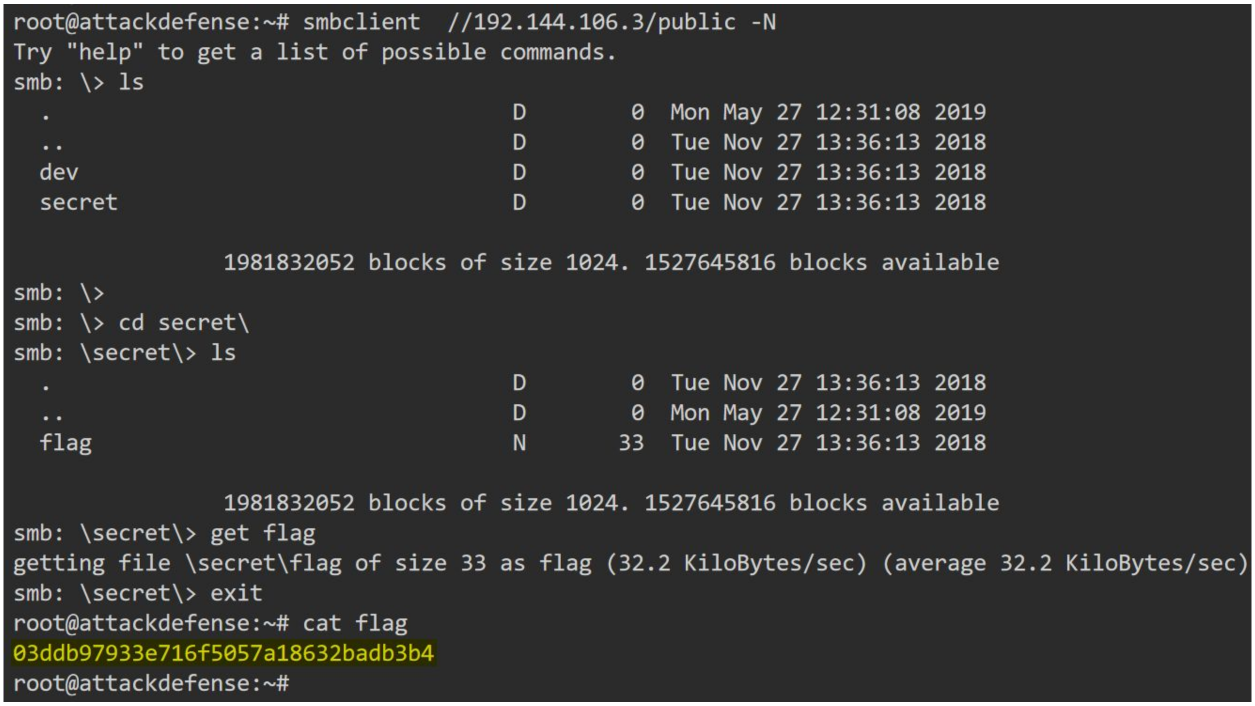
```
root@attackdefense:~# smbclient  //192.144.106.3/public -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 27 12:31:08 2019
  ..                                  D        0  Tue Nov 27 13:36:13 2018
  dev                                 D        0  Tue Nov 27 13:36:13 2018
  secret                              D        0  Tue Nov 27 13:36:13 2018

                1981832052 blocks of size 1024. 1527645816 blocks available
smb: \>
```

Q9. Fetch the flag from samba server.

Answer: 03ddb97933e716f5057a18632badb3b4

Commands:

```
smbclient  //192.144.106.3/public -N
ls
cd secret
ls
get flag
exit
cat flag
```



```
root@attackdefense:~# smbclient  //192.144.106.3/public -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 27 12:31:08 2019
  ..                                  D        0  Tue Nov 27 13:36:13 2018
  dev                                 D        0  Tue Nov 27 13:36:13 2018
  secret                              D        0  Tue Nov 27 13:36:13 2018

                1981832052 blocks of size 1024. 1527645816 blocks available
smb: \>
smb: \> cd secret\
smb: \secret\> ls
  .                                   D        0  Tue Nov 27 13:36:13 2018
  ..                                  D        0  Mon May 27 12:31:08 2019
  flag                                N       33  Tue Nov 27 13:36:13 2018

                1981832052 blocks of size 1024. 1527645816 blocks available
smb: \secret\> get flag
getting file \secret\flag of size 33 as flag (32.2 KiloBytes/sec) (average 32.2 KiloBytes/sec)
smb: \secret\> exit
root@attackdefense:~# cat flag
03ddb97933e716f5057a18632badb3b4
root@attackdefense:~#
```

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-enum-shares (https://nmap.org/nsedoc/scripts/smb-enum-shares.html)
6. Metasploit Module: SMB Share Enumeration (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_enumshares)