ATTACK DEFENSE

by PentesterAcademy

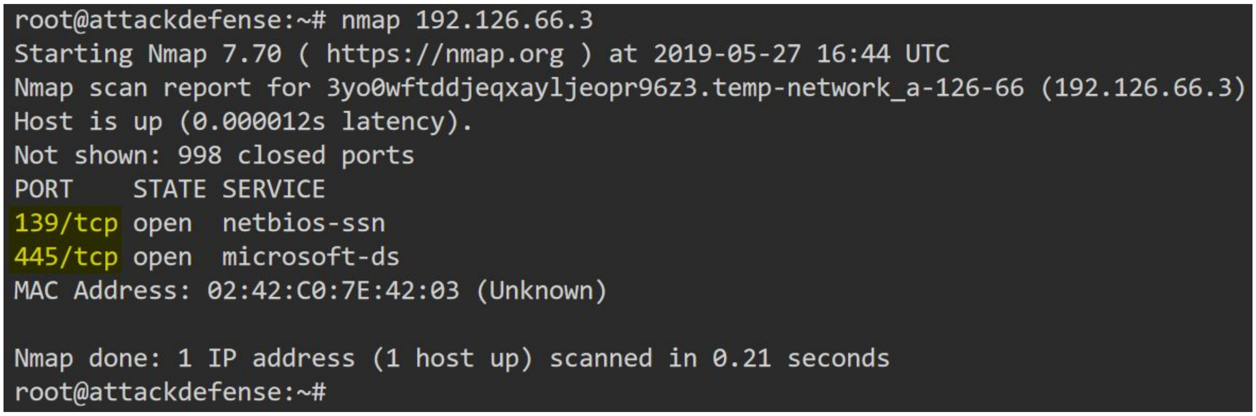
Name	Samba Recon: Basics I
URL	https://www.attackdefense.com/challengedetails?cid=553
Type	Network Recon : SMB Servers

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 default tcp ports used by smbd.

Answer: 139,445

Command: nmap 192.126.66.3

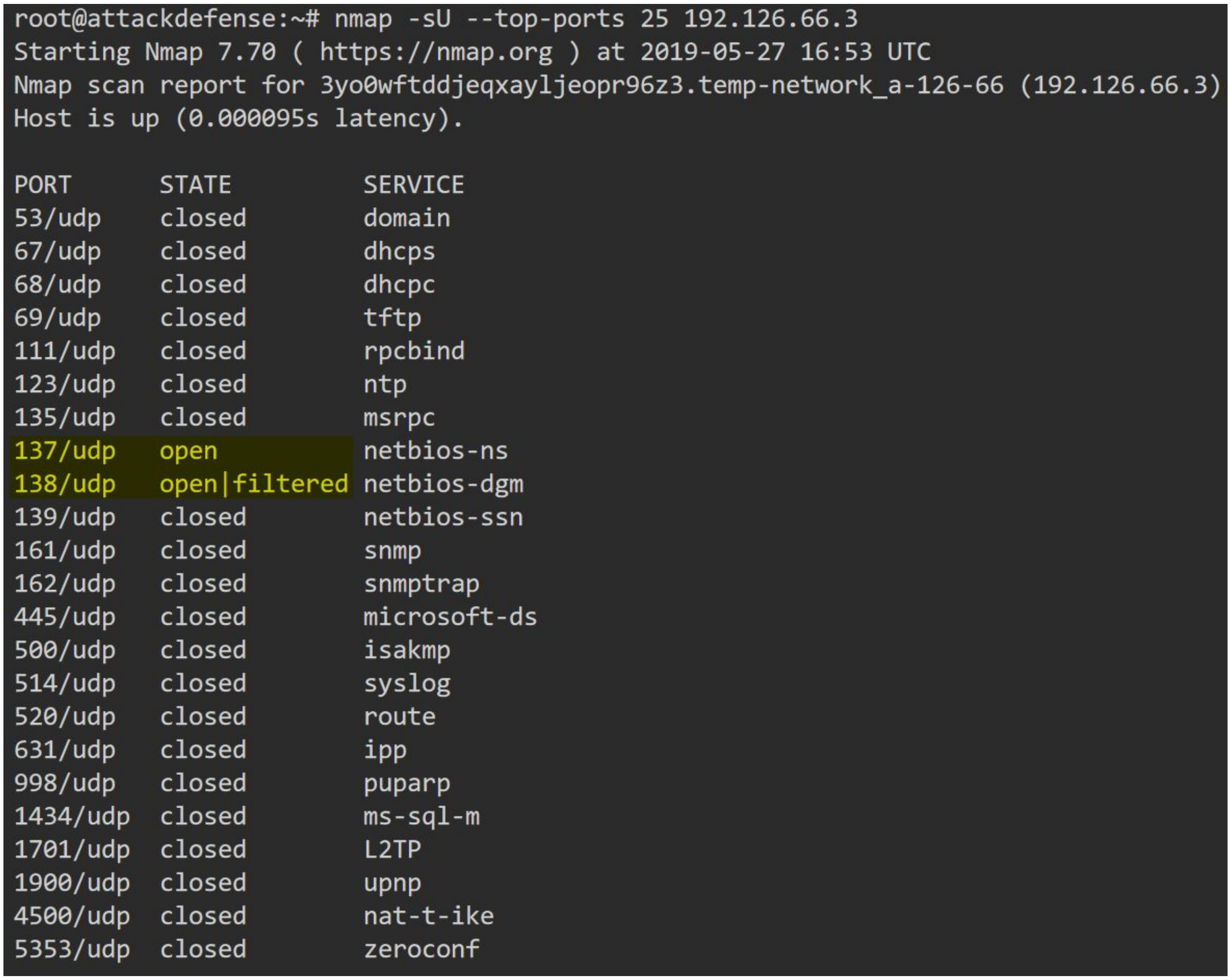


```
root@attackdefense:~# nmap 192.126.66.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 16:44 UTC
Nmap scan report for 3yo0wftddjeqxayljeopr96z3.temp-network_a-126-66 (192.126.66.3)
Host is up (0.000012s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:42:C0:7E:42:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@attackdefense:~#
```

Q2. Find the default udp ports used by nmbd.

Answer: 137, 138

Command: nmap -sU --top-ports 25 192.126.66.3

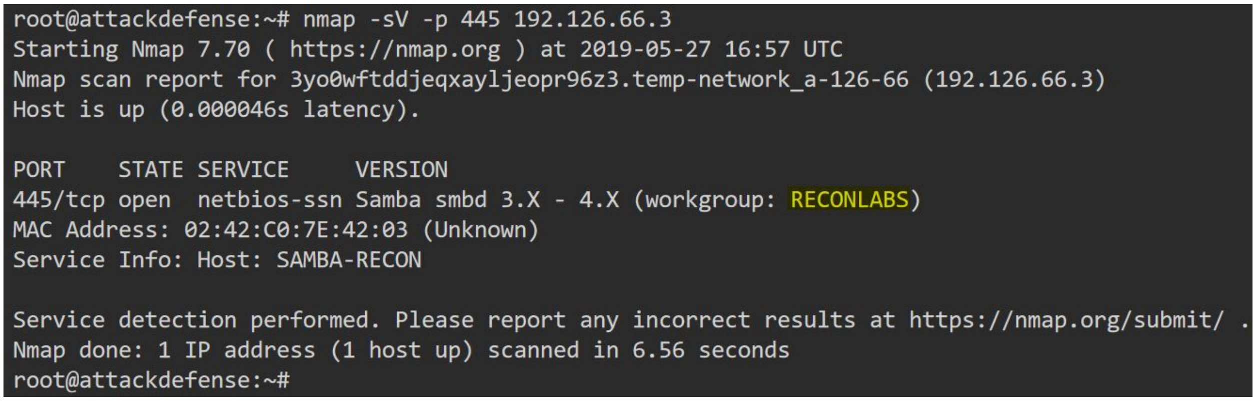


```
root@attackdefense:~# nmap -sU --top-ports 25 192.126.66.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 16:53 UTC
Nmap scan report for 3yo0wftddjeqxayljeopr96z3.temp-network_a-126-66 (192.126.66.3)
Host is up (0.000095s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    closed        dhcpc
69/udp    closed        tftp
111/udp   closed        rpcbind
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
998/udp   closed        puparp
1434/udp  closed        ms-sql-m
1701/udp  closed        L2TP
1900/udp  closed        upnp
4500/udp  closed        nat-t-ike
5353/udp  closed        zeroconf
```

Q3. What is the workgroup name of samba server?

Answer: RECONLABS

Command: nmap -sV -p 445 192.126.66.3

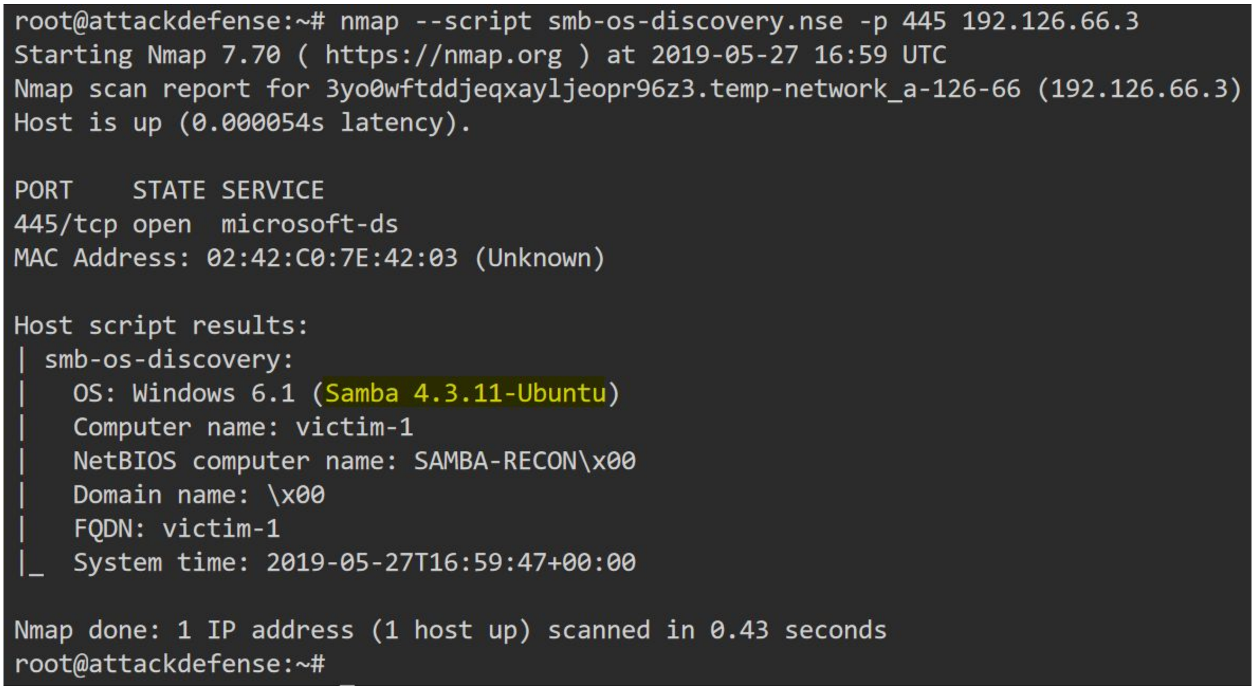


```
root@attackdefense:~# nmap -sV -p 445 192.126.66.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 16:57 UTC
Nmap scan report for 3yo0wftddjeqxayljeopr96z3.temp-network_a-126-66 (192.126.66.3)
Host is up (0.000046s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: RECONLABS)
MAC Address: 02:42:C0:7E:42:03 (Unknown)
Service Info: Host: SAMBA-RECON

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.56 seconds
root@attackdefense:~#
```

Q4. Find the exact version of samba server by using appropriate nmap script.

Answer: Samba 4.3.11-Ubuntu

Command: nmap --script smb-os-discovery.nse -p 445 192.126.66.3

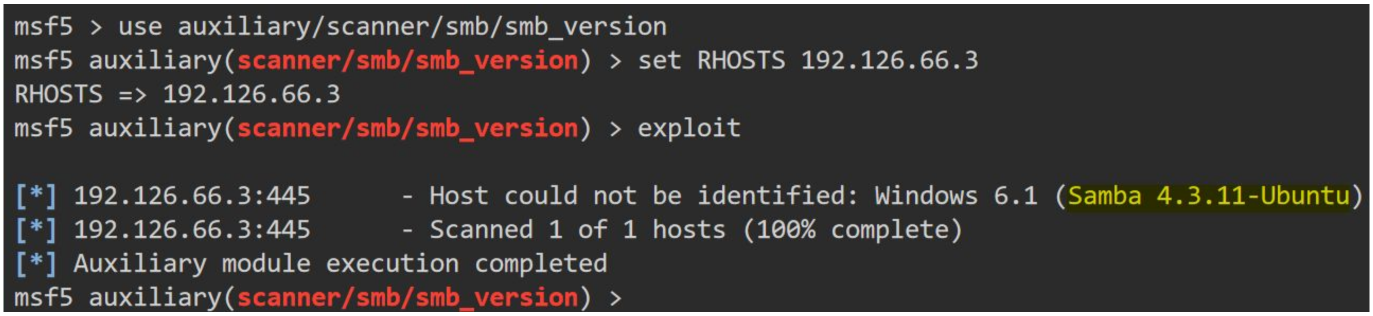


```
root@attackdefense:~# nmap --script smb-os-discovery.nse -p 445 192.126.66.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 16:59 UTC
Nmap scan report for 3yo0wftddjeqxayljeopr96z3.temp-network_a-126-66 (192.126.66.3)
Host is up (0.000054s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:42:C0:7E:42:03 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: victim-1
|   NetBIOS computer name: SAMBA-RECON\x00
|   Domain name: \x00
|   FQDN: victim-1
|_  System time: 2019-05-27T16:59:47+00:00

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
root@attackdefense:~#
```

Q5. Find the exact version of samba server by using smb_version metasploit module.

Answer: Samba 4.3.11-Ubuntu

Commands:
msfconsole
use auxiliary/scanner/smb/smb_version
set RHOSTS 192.126.66.3
exploit

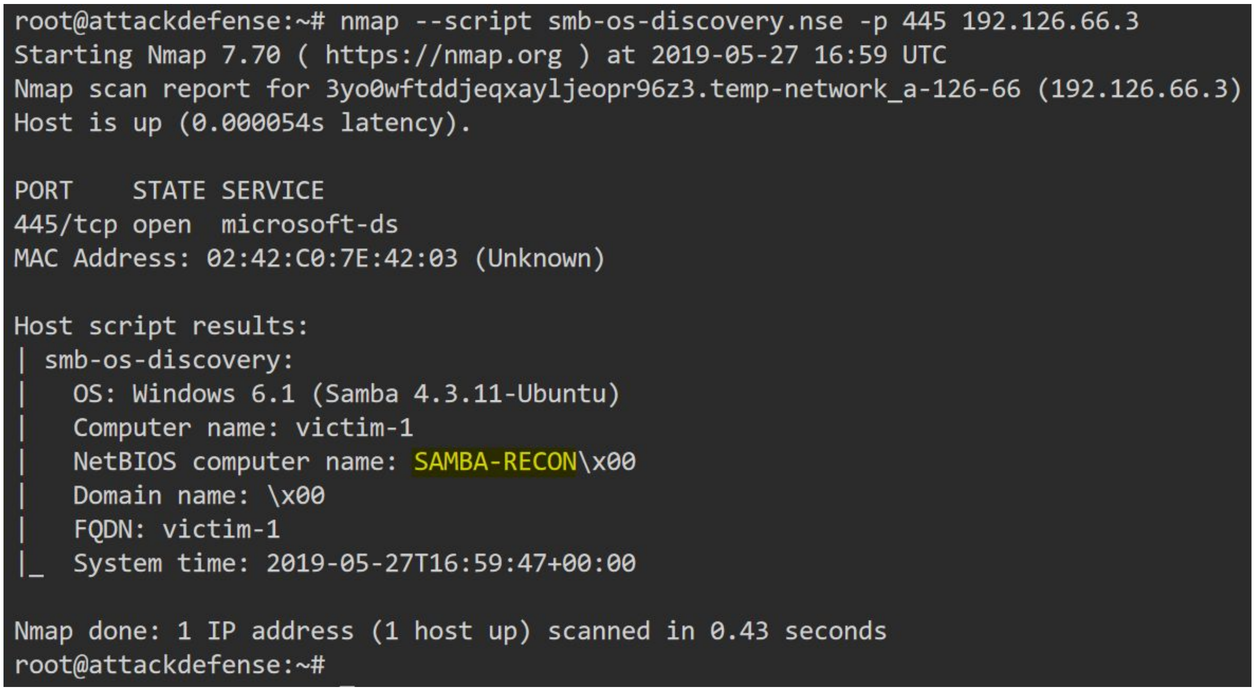


```
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.126.66.3
RHOSTS => 192.126.66.3
msf5 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.126.66.3:445      - Host could not be identified: Windows 6.1 (Samba 4.3.11-Ubuntu)
[*] 192.126.66.3:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Q6. What is the NetBIOS computer name of samba server? Use appropriate nmap scripts.

Answer: SAMBA-RECON

Command: nmap --script smb-os-discovery.nse -p 445 192.126.66.3

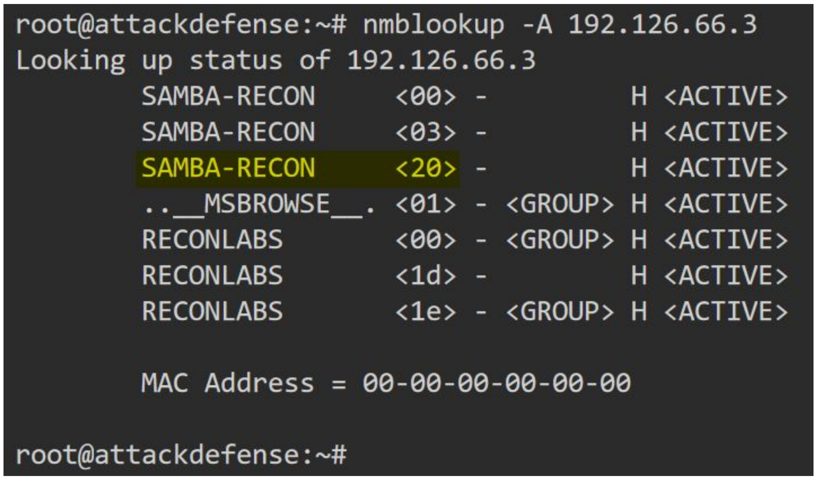


```
root@attackdefense:~# nmap --script smb-os-discovery.nse -p 445 192.126.66.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 16:59 UTC
Nmap scan report for 3yo0wftddjeqxayljeopr96z3.temp-network_a-126-66 (192.126.66.3)
Host is up (0.000054s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:42:C0:7E:42:03 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: victim-1
|   NetBIOS computer name: SAMBA-RECON\x00
|   Domain name: \x00
|   FQDN: victim-1
|_  System time: 2019-05-27T16:59:47+00:00

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
root@attackdefense:~#
```

Q7. Find the NetBIOS computer name of samba server using nmblookup

Answer: SAMBA-RECON

Command: nmblookup -A 192.126.66.3



```
root@attackdefense:~# nmblookup -A 192.126.66.3
Looking up status of 192.126.66.3
        SAMBA-RECON     <00> -         H <ACTIVE>
        SAMBA-RECON     <03> -         H <ACTIVE>
        SAMBA-RECON     <20> -         H <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> H <ACTIVE>
        RECONLABS       <00> - <GROUP> H <ACTIVE>
        RECONLABS       <1d> -         H <ACTIVE>
        RECONLABS       <1e> - <GROUP> H <ACTIVE>

        MAC Address = 00-00-00-00-00-00

root@attackdefense:~#
```

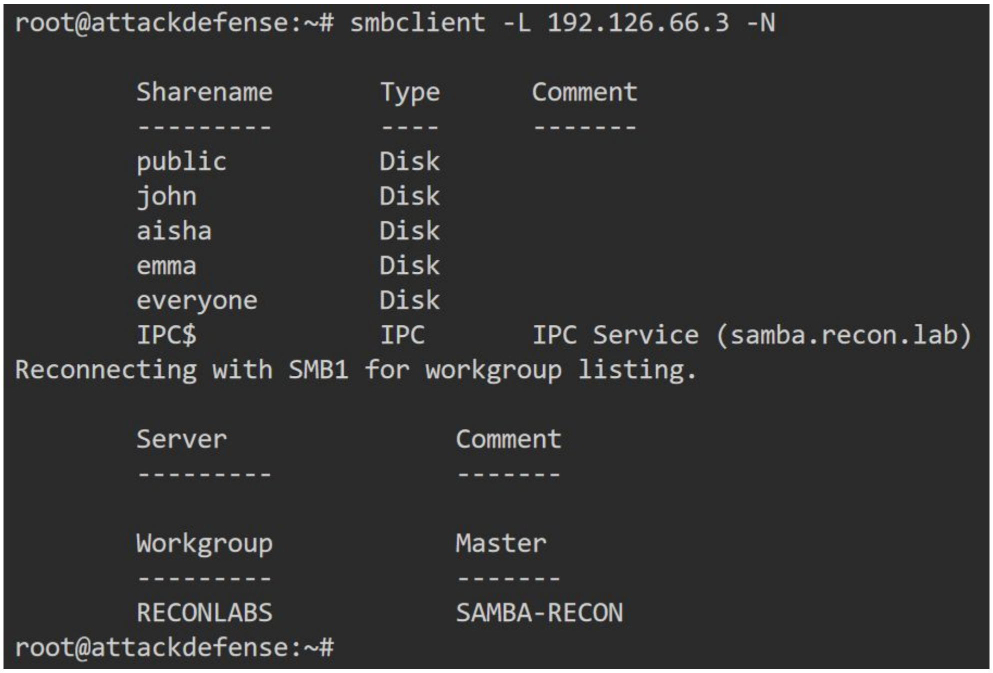
Q8. Using smbclient determine whether anonymous connection (null session) is allowed on the samba server or not.

Answer: Allowed

Solution:

Anonymous connection is allowed since shares are displayed without requirement of password.

Command: smbclient -L 192.126.66.3 -N



```
root@attackdefense:~# smbclient -L 192.126.66.3 -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:~#
```

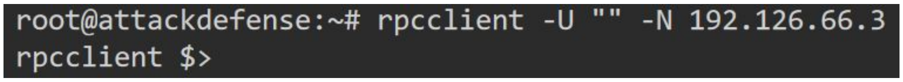
Q9. Using rpcclient determine whether anonymous connection (null session) is allowed on the samba server or not.

Answer: Allowed

Solution:

Anonymous connection is allowed since no errors are thrown while connecting to samba server without any credentials

Command: rpcclient -U "" -N 192.126.66.3



```
root@attackdefense:~# rpcclient -U "" -N 192.126.66.3
rpcclient $>
```

References:

1. Samba (https://www.samba.org/)
2. smbclient (https://www.samba.org/samba/docs/current/man-html/smbclient.1.html)
3. rpcclient (https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html)
4. nmblookup (https://www.samba.org/samba/docs/current/man-html/nmblookup.1.html)
5. Nmap Script: smb-os-discovery (https://nmap.org/nsedoc/scripts/smb-os-discovery.html)
6. Metasploit Module: SMB Version Detection (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_version)