ATTACK DEFENSE

by PentesterAcademy

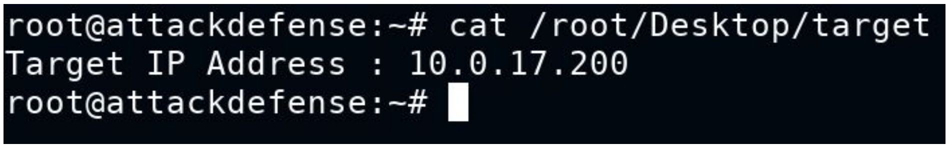
Name	Windows Recon: SMB: Nmap Scripts
URL	https://attackdefense.com/challengedetails?cid=2222
Type	Windows Reconnaissance: SMB

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: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

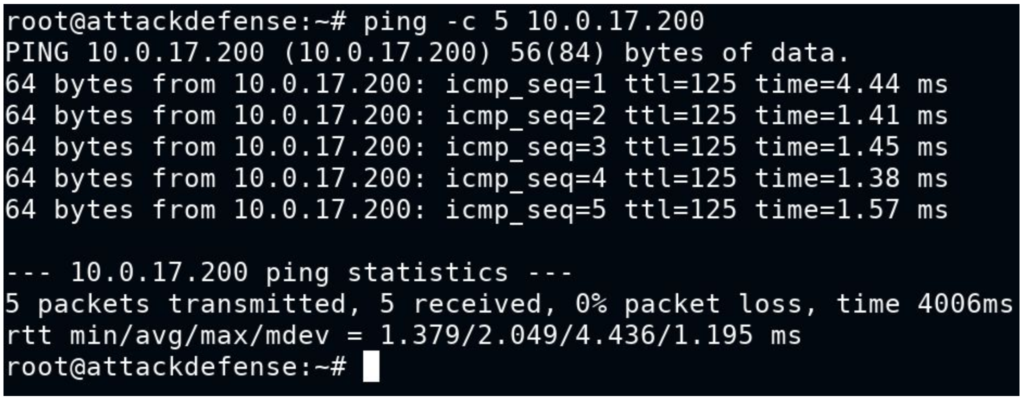
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.17.200
root@attackdefense:~# 
```

Step 2: Ping the target machine to see if it's alive or not.

Command: ping -c 5 10.0.17.200

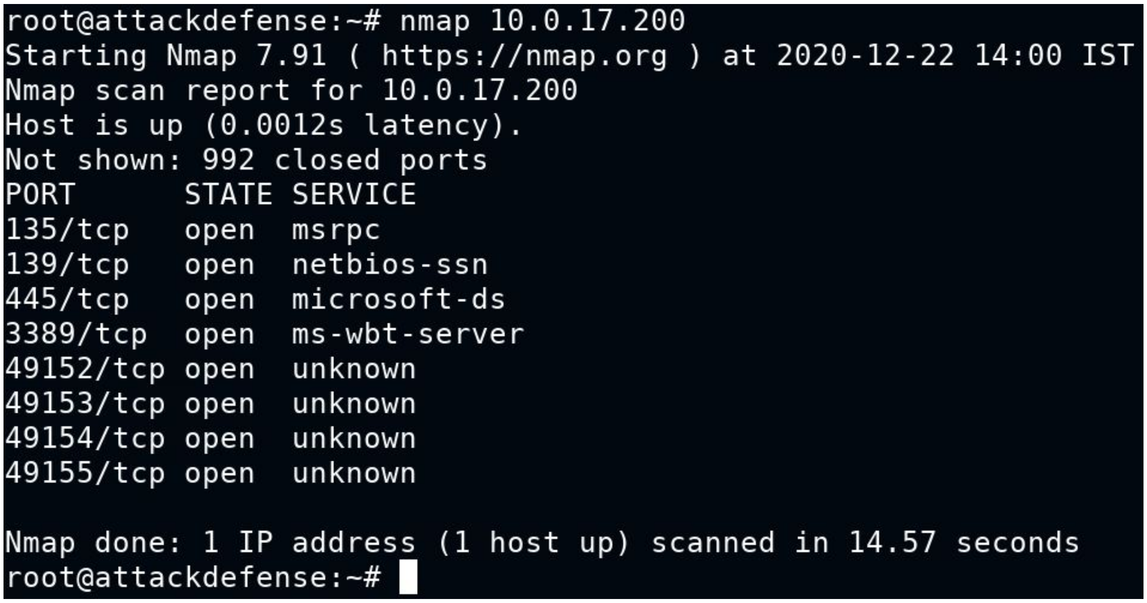


```
root@attackdefense:~# ping -c 5 10.0.17.200
PING 10.0.17.200 (10.0.17.200) 56(84) bytes of data.
64 bytes from 10.0.17.200: icmp_seq=1 ttl=125 time=4.44 ms
64 bytes from 10.0.17.200: icmp_seq=2 ttl=125 time=1.41 ms
64 bytes from 10.0.17.200: icmp_seq=3 ttl=125 time=1.45 ms
64 bytes from 10.0.17.200: icmp_seq=4 ttl=125 time=1.38 ms
64 bytes from 10.0.17.200: icmp_seq=5 ttl=125 time=1.57 ms

--- 10.0.17.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.379/2.049/4.436/1.195 ms
root@attackdefense:~# 
```

We can observe that the target machine is alive and we have successfully sent and received all five packets.

Step 3: Run a Nmap scan against the target IP.

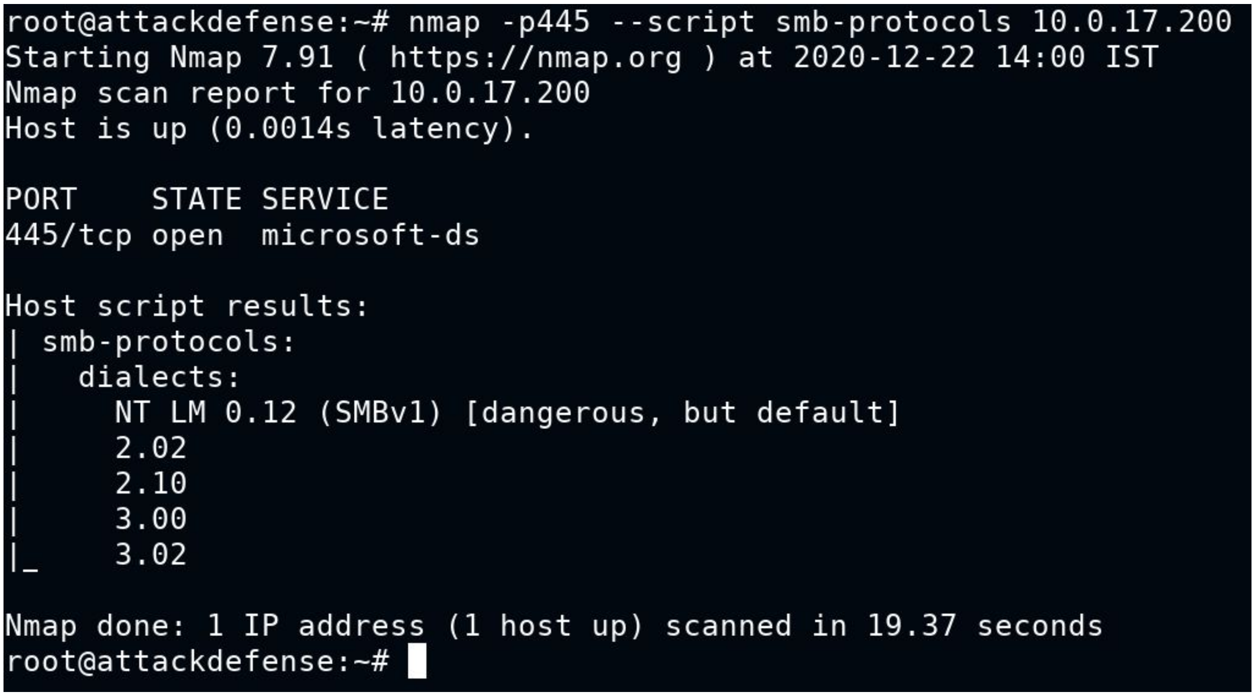
Command: nmap 10.0.17.200



```
root@attackdefense:~# nmap 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:00 IST
Nmap scan report for 10.0.17.200
Host is up (0.0012s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
root@attackdefense:~# 
```

Step 4: We have discovered that multiple ports are open. SMB port 445 is also exposed. We will run the Nmap script to list the supported protocols and dialects of an SMB server.

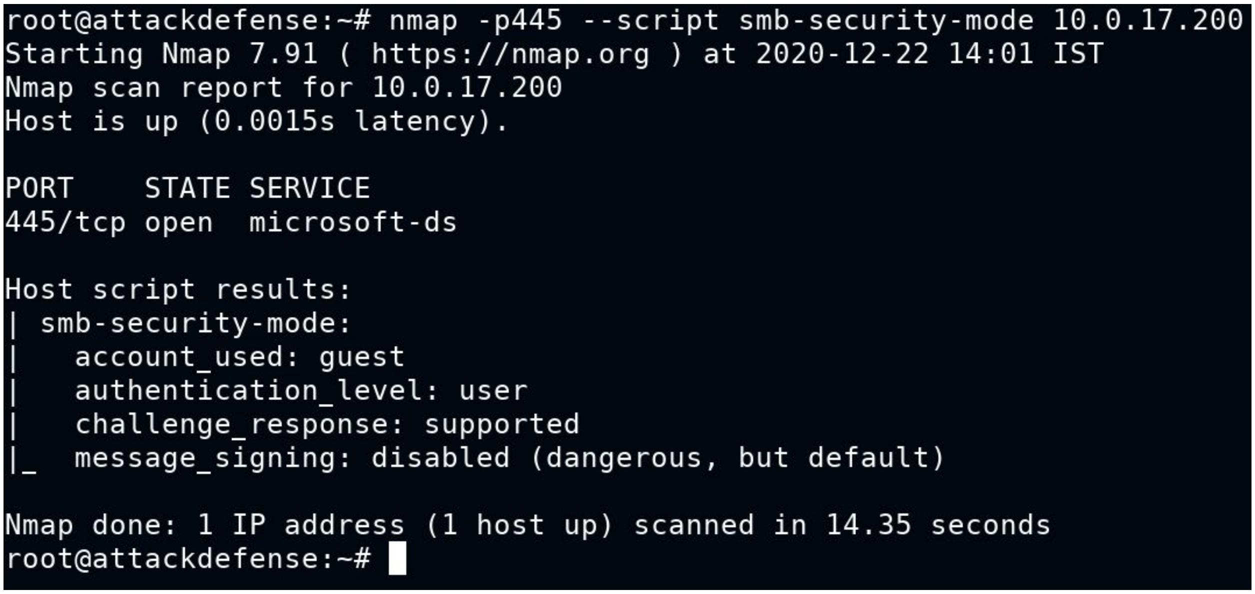
Command: nmap -p445 --script smb-protocols 10.0.17.200



```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:00 IST
Nmap scan report for 10.0.17.200
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

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

Nmap done: 1 IP address (1 host up) scanned in 19.37 seconds
root@attackdefense:~# 
```

Step 5: Running security mode script to return the information about the SMB security level.

Command: nmap -p445 --script smb-security-mode 10.0.17.200



```
root@attackdefense:~# nmap -p445 --script smb-security-mode 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:01 IST
Nmap scan report for 10.0.17.200
Host is up (0.0015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds
root@attackdefense:~# 
```

We have tried to access the target SMB server using a guest user and we have received SMB security level information.

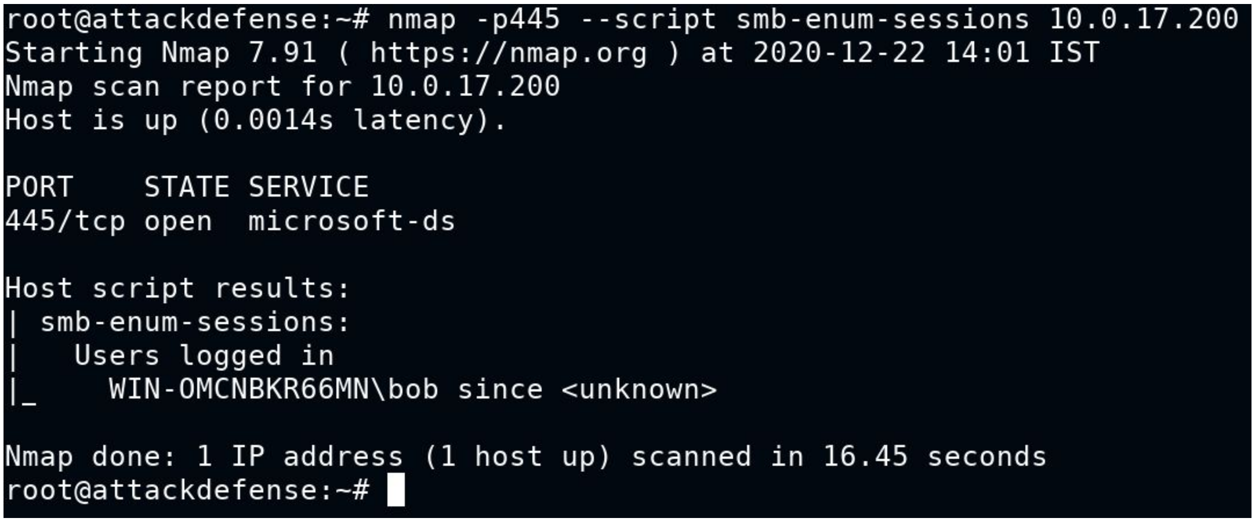
We can find more information from the following link:
https://nmap.org/nsedoc/scripts/smb-security-mode.html

Step 6: We have the SMB server credentials i.e **administrator:smbserver_771**. We will use it with Nmap script to scan the target to discover sensitive information.

Enumerating the users logged into a system through an SMB share with Nmap script.

First, we won't use any credentials to see the output.

Command: nmap -p445 --script smb-enum-sessions 10.0.17.200



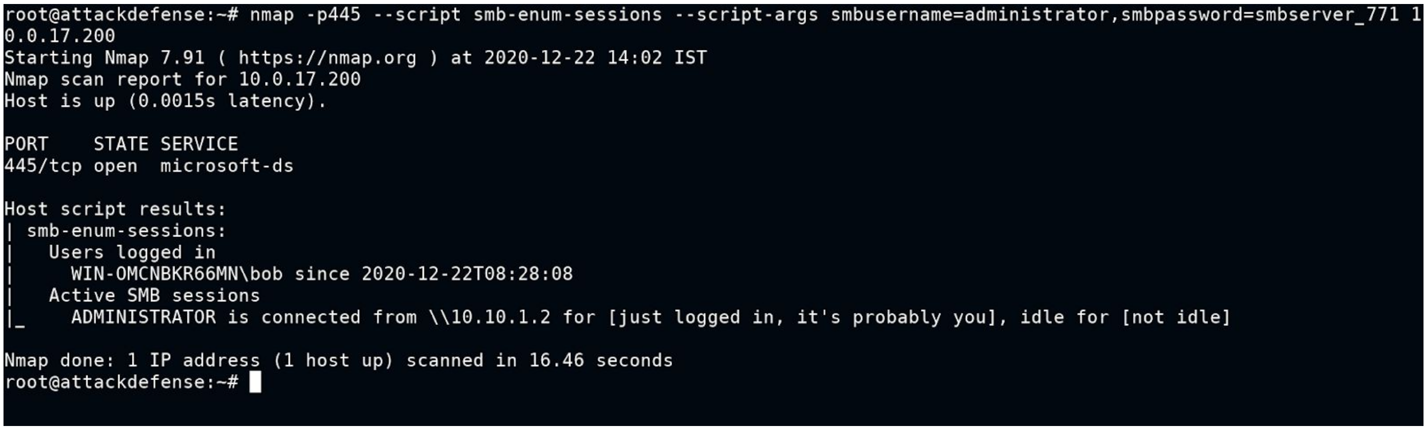
```
root@attackdefense:~# nmap -p445 --script smb-enum-sessions 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:01 IST
Nmap scan report for 10.0.17.200
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-sessions:
|   Users logged in
|_    WIN-OMCNBKR66MN\bob since <unknown>

Nmap done: 1 IP address (1 host up) scanned in 16.45 seconds
root@attackdefense:~#
```

We can observe that on the target machine we have discovered that user bob is logged into without any credentials.

This is possible because the target machine is running with the guest login enable configuration and it is a misconfiguration.

In case guest login is not enabled we can always use valid credentials of the target machine to discover the same information.

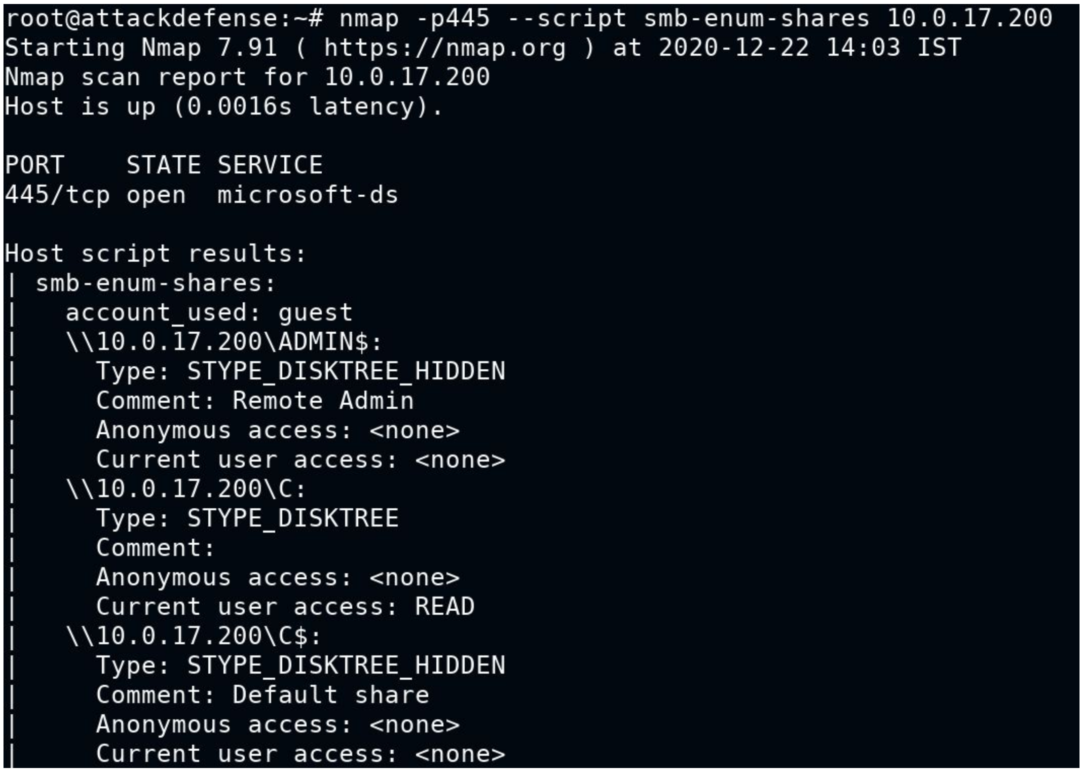
Command: nmap -p445 --script smb-enum-sessions --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



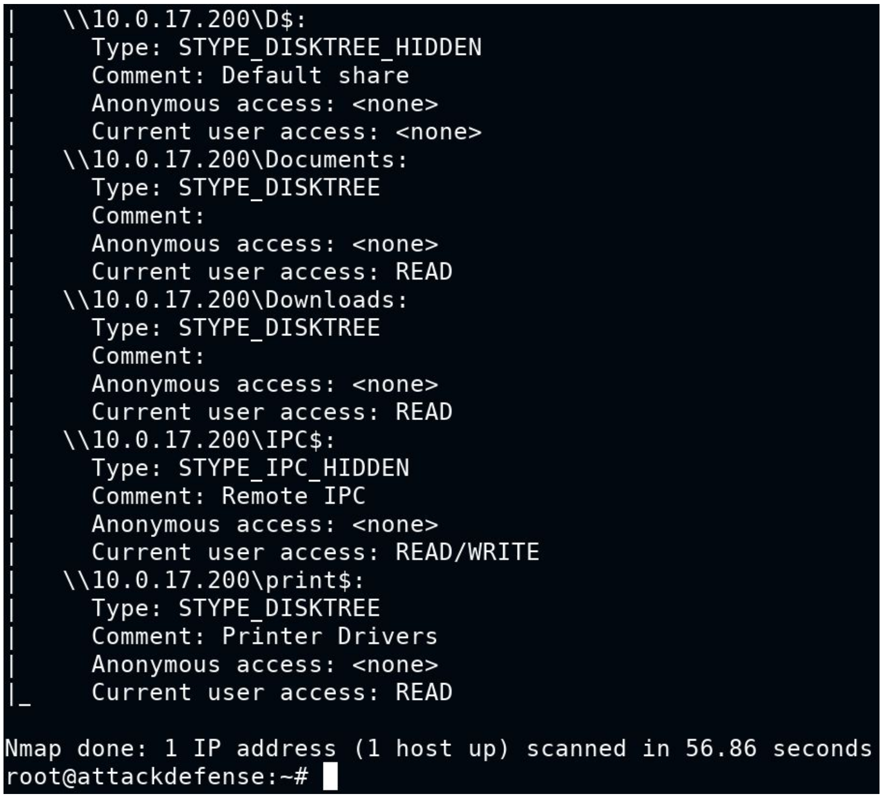
```
root@attackdefense:~# nmap -p445 --script smb-enum-sessions --script-args smbusername=administrator,smbpassword=smbserver_771 1
0.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:02 IST
Nmap scan report for 10.0.17.200
Host is up (0.0015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-sessions:
|   Users logged in
|     WIN-OMCNBKR66MN\bob since 2020-12-22T08:28:08
|   Active SMB sessions
|_    ADMINISTRATOR is connected from \\10.10.1.2 for [just logged in, it's probably you], idle for [not idle]

Nmap done: 1 IP address (1 host up) scanned in 16.46 seconds
root@attackdefense:~#
```

Step 7: Enumerating all available shares.

Command: nmap -p445 --script smb-enum-shares 10.0.17.200



```
root@attackdefense:~# nmap -p445 --script smb-enum-shares 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:03 IST
Nmap scan report for 10.0.17.200
Host is up (0.0016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.0.17.200\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.0.17.200\C:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.0.17.200\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
```



```
|     \\10.0.17.200\D$:
|       Type: STYPE_DISKTREE_HIDDEN
|       Comment: Default share
|       Anonymous access: <none>
|       Current user access: <none>
|     \\10.0.17.200\Documents:
|       Type: STYPE_DISKTREE
|       Comment:
|       Anonymous access: <none>
|       Current user access: READ
|     \\10.0.17.200\Downloads:
|       Type: STYPE_DISKTREE
|       Comment:
|       Anonymous access: <none>
|       Current user access: READ
|     \\10.0.17.200\IPC$:
|       Type: STYPE_IPC_HIDDEN
|       Comment: Remote IPC
|       Anonymous access: <none>
|       Current user access: READ/WRITE
|     \\10.0.17.200\print$:
|       Type: STYPE_DISKTREE
|       Comment: Printer Drivers
|       Anonymous access: <none>
|_      Current user access: READ

Nmap done: 1 IP address (1 host up) scanned in 56.86 seconds
root@attackdefense:~#
```

We can observe, in the output that we have accessed all the shares using guest users and we have received the permission of each folder or drive.

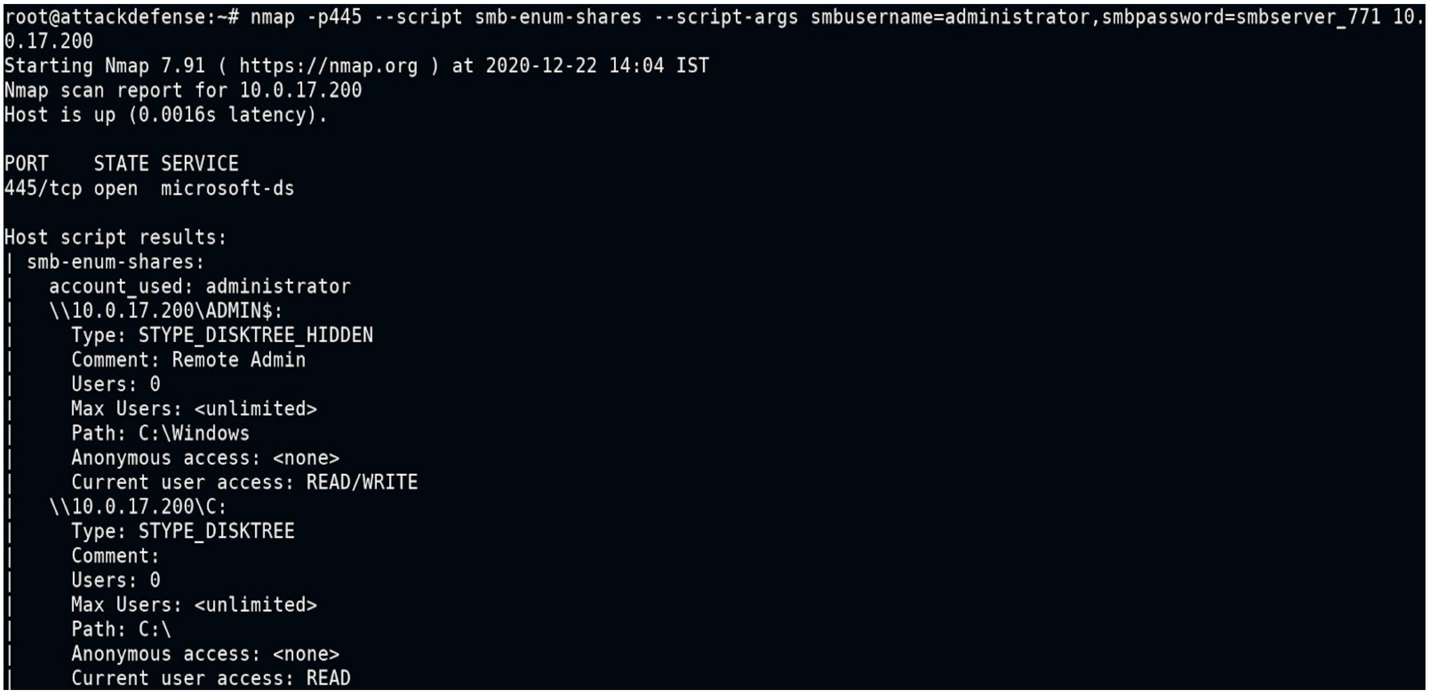
Also, we can notice that **IPC$** share has read and write permissions.

About IPC$ share

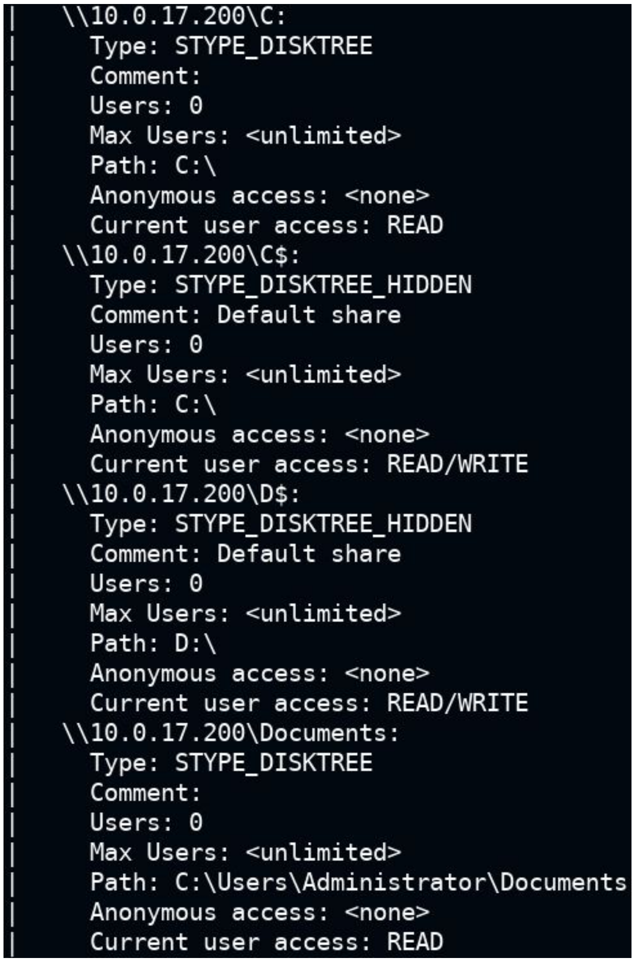
“The IPC$ share is also known as a null session connection. By using this session, Windows lets anonymous users perform certain activities, such as enumerating the names of domain accounts and network shares.”

Scanning all shares using valid credentials to check the permissions.

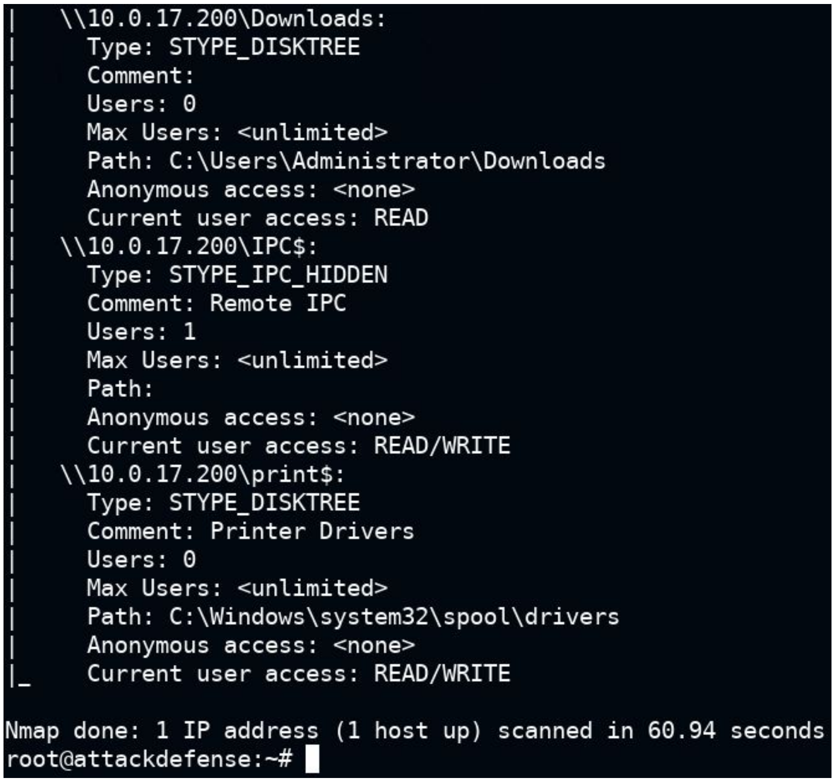
Command: nmap -p445 --script smb-enum-shares --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



```
root@attackdefense:~# nmap -p445 --script smb-enum-shares --script-args smbusername=administrator,smbpassword=smbserver_771 10.
0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:04 IST
Nmap scan report for 10.0.17.200
Host is up (0.0016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: administrator
|   \\10.0.17.200\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Windows
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.17.200\C:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\
|     Anonymous access: <none>
|     Current user access: READ
```



```
|     \\10.0.17.200\C:
|       Type: STYPE_DISKTREE
|       Comment:
|       Users: 0
|       Max Users: <unlimited>
|       Path: C:\
|       Anonymous access: <none>
|       Current user access: READ
|     \\10.0.17.200\C$:
|       Type: STYPE_DISKTREE_HIDDEN
|       Comment: Default share
|       Users: 0
|       Max Users: <unlimited>
|       Path: C:\
|       Anonymous access: <none>
|       Current user access: READ/WRITE
|     \\10.0.17.200\D$:
|       Type: STYPE_DISKTREE_HIDDEN
|       Comment: Default share
|       Users: 0
|       Max Users: <unlimited>
|       Path: D:\
|       Anonymous access: <none>
|       Current user access: READ/WRITE
|     \\10.0.17.200\Documents:
|       Type: STYPE_DISKTREE
|       Comment:
|       Users: 0
|       Max Users: <unlimited>
|       Path: C:\Users\Administrator\Documents
|       Anonymous access: <none>
|       Current user access: READ
```

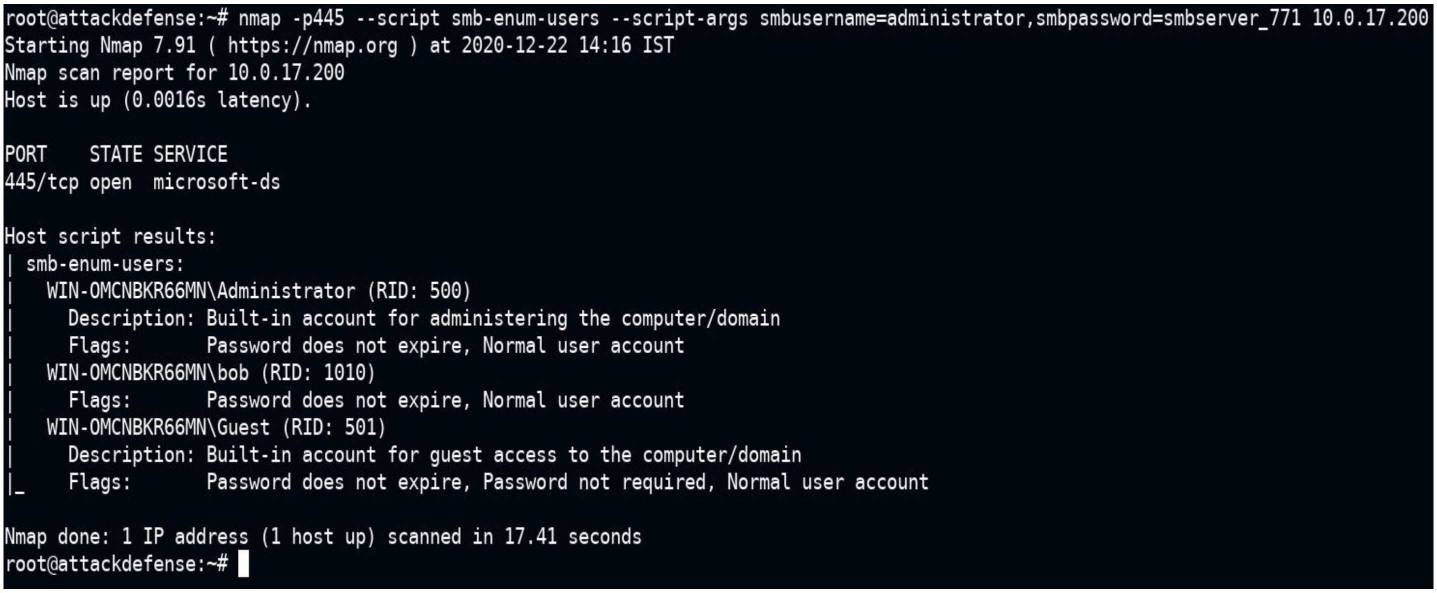


```
|   \\10.0.17.200\Downloads:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Users\Administrator\Downloads
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.0.17.200\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Users: 1
|     Max Users: <unlimited>
|     Path:
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.17.200\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Windows\system32\spool\drivers
|     Anonymous access: <none>
|_    Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 60.94 seconds
root@attackdefense:~#
```

We can observe that the administrator user has read and write privilege to the entire **C$**. i.e **C:\**

Step 8: Enumerate the windows users on a target machine.

Command: nmap -p445 --script smb-enum-users --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200

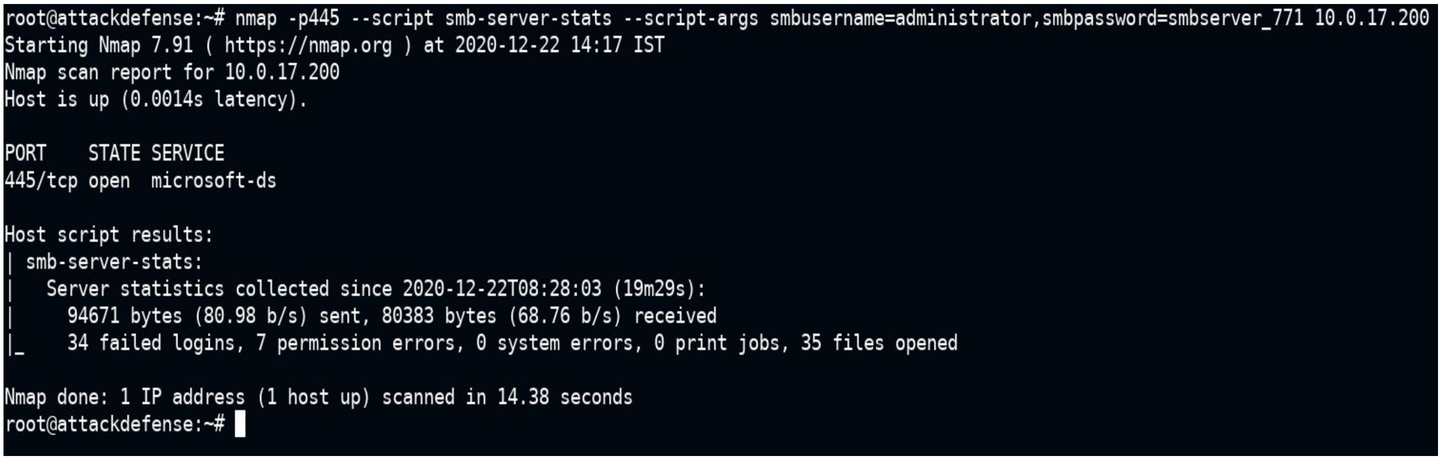


```
root@attackdefense:~# nmap -p445 --script smb-enum-users --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:16 IST
Nmap scan report for 10.0.17.200
Host is up (0.0016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   WIN-OMCNBKR66MN\Administrator (RID: 500)
|     Description: Built-in account for administering the computer/domain
|     Flags:       Password does not expire, Normal user account
|   WIN-OMCNBKR66MN\bob (RID: 1010)
|     Flags:       Password does not expire, Normal user account
|   WIN-OMCNBKR66MN\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|_    Flags:       Password does not expire, Password not required, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 17.41 seconds
root@attackdefense:~# 
```

We can observe that there are three users present on the target machine. i.e Administrator, bob, Guest

Step 9: Get information about the server statistics. It uses port 445 and port 139 to fetch the details.

Command: nmap -p445 --script smb-server-stats --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



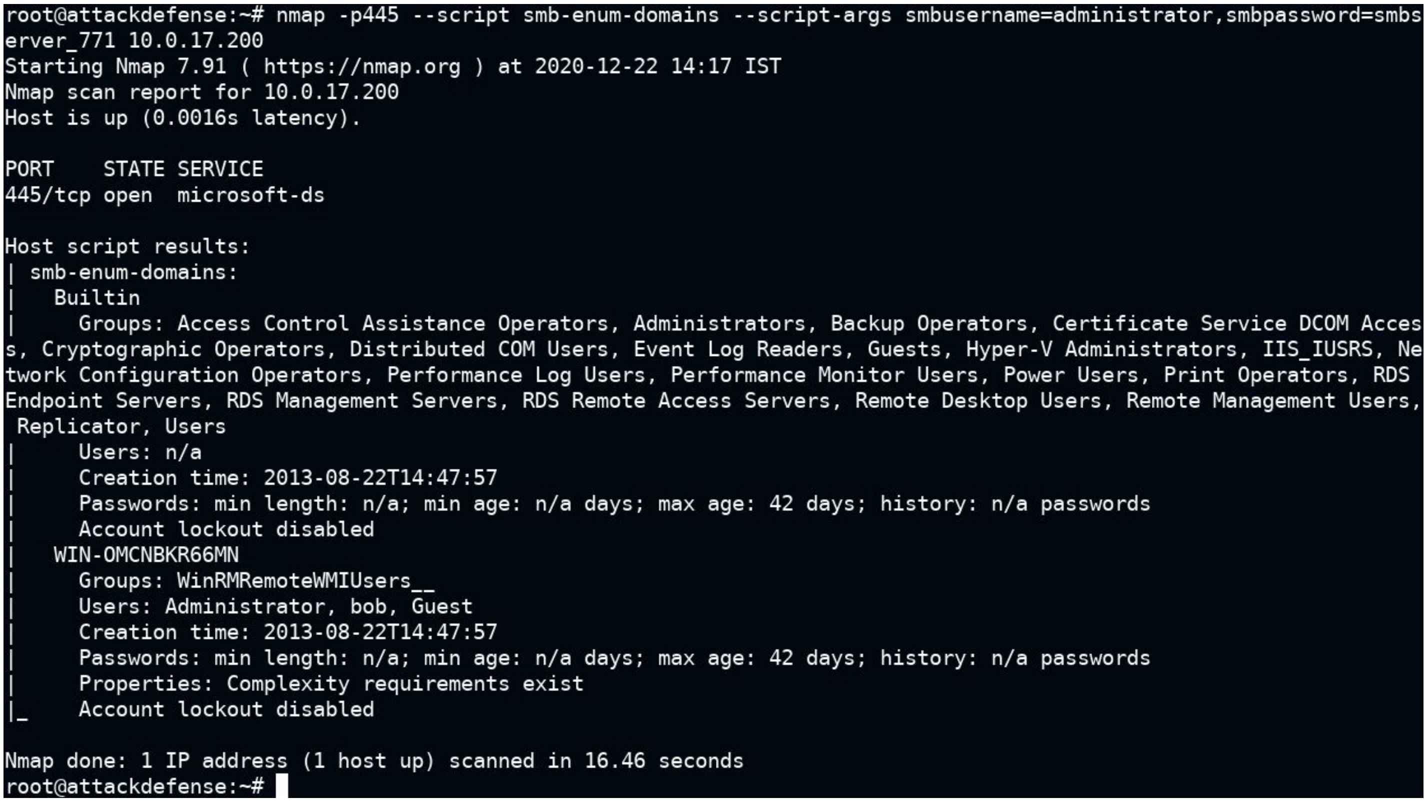
```
root@attackdefense:~# nmap -p445 --script smb-server-stats --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:17 IST
Nmap scan report for 10.0.17.200
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-server-stats:
|   Server statistics collected since 2020-12-22T08:28:03 (19m29s):
|     94671 bytes (80.98 b/s) sent, 80383 bytes (68.76 b/s) received
|_    34 failed logins, 7 permission errors, 0 system errors, 0 print jobs, 35 files opened

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
root@attackdefense:~# 
```

We can notice that we have received failed logins, permission & system errors, and opened files and print jobs.

Please note: There is a possibility that the above output would be different in your case which is completely okay.

Step 10: Enumerating available domains on a target machine.

Command: nmap -p445 --script smb-enum-domains --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200

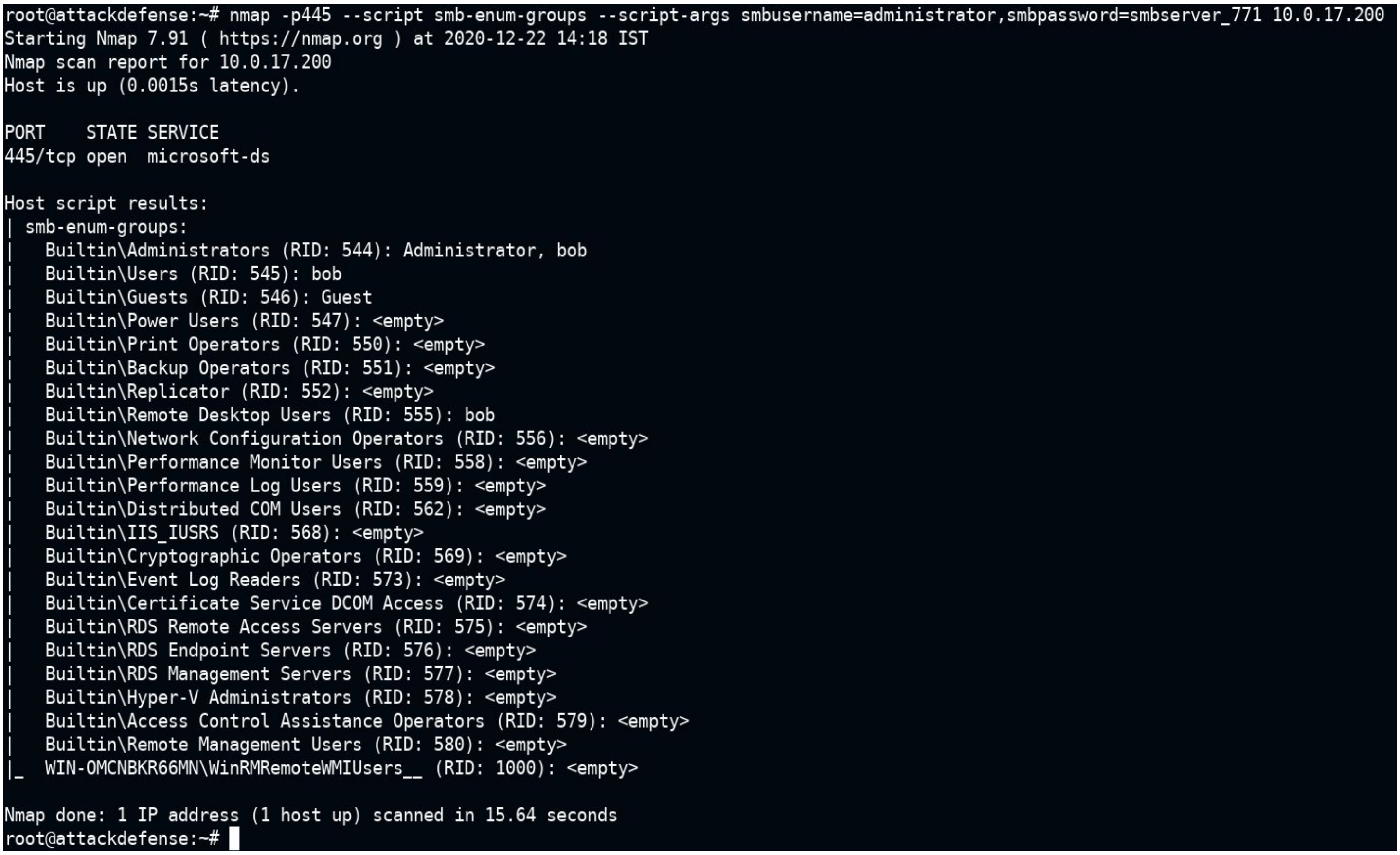


```
root@attackdefense:~# nmap -p445 --script smb-enum-domains --script-args smbusername=administrator,smbpassword=smbs
erver_771 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:17 IST
Nmap scan report for 10.0.17.200
Host is up (0.0016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: Access Control Assistance Operators, Administrators, Backup Operators, Certificate Service DCOM Acces
s, Cryptographic Operators, Distributed COM Users, Event Log Readers, Guests, Hyper-V Administrators, IIS_IUSRS, Ne
twork Configuration Operators, Performance Log Users, Performance Monitor Users, Power Users, Print Operators, RDS
Endpoint Servers, RDS Management Servers, RDS Remote Access Servers, Remote Desktop Users, Remote Management Users,
 Replicator, Users
|     Users: n/a
|     Creation time: 2013-08-22T14:47:57
|     Passwords: min length: n/a; min age: n/a days; max age: 42 days; history: n/a passwords
|     Account lockout disabled
|   WIN-OMCNBKR66MN
|     Groups: WinRMRemoteWMIUsers__
|     Users: Administrator, bob, Guest
|     Creation time: 2013-08-22T14:47:57
|     Passwords: min length: n/a; min age: n/a days; max age: 42 days; history: n/a passwords
|     Properties: Complexity requirements exist
|_    Account lockout disabled

Nmap done: 1 IP address (1 host up) scanned in 16.46 seconds
root@attackdefense:~#
```

We have received the information about the built-in domain on the target machine.

Step 11: Enumerating available user groups on a target machine.

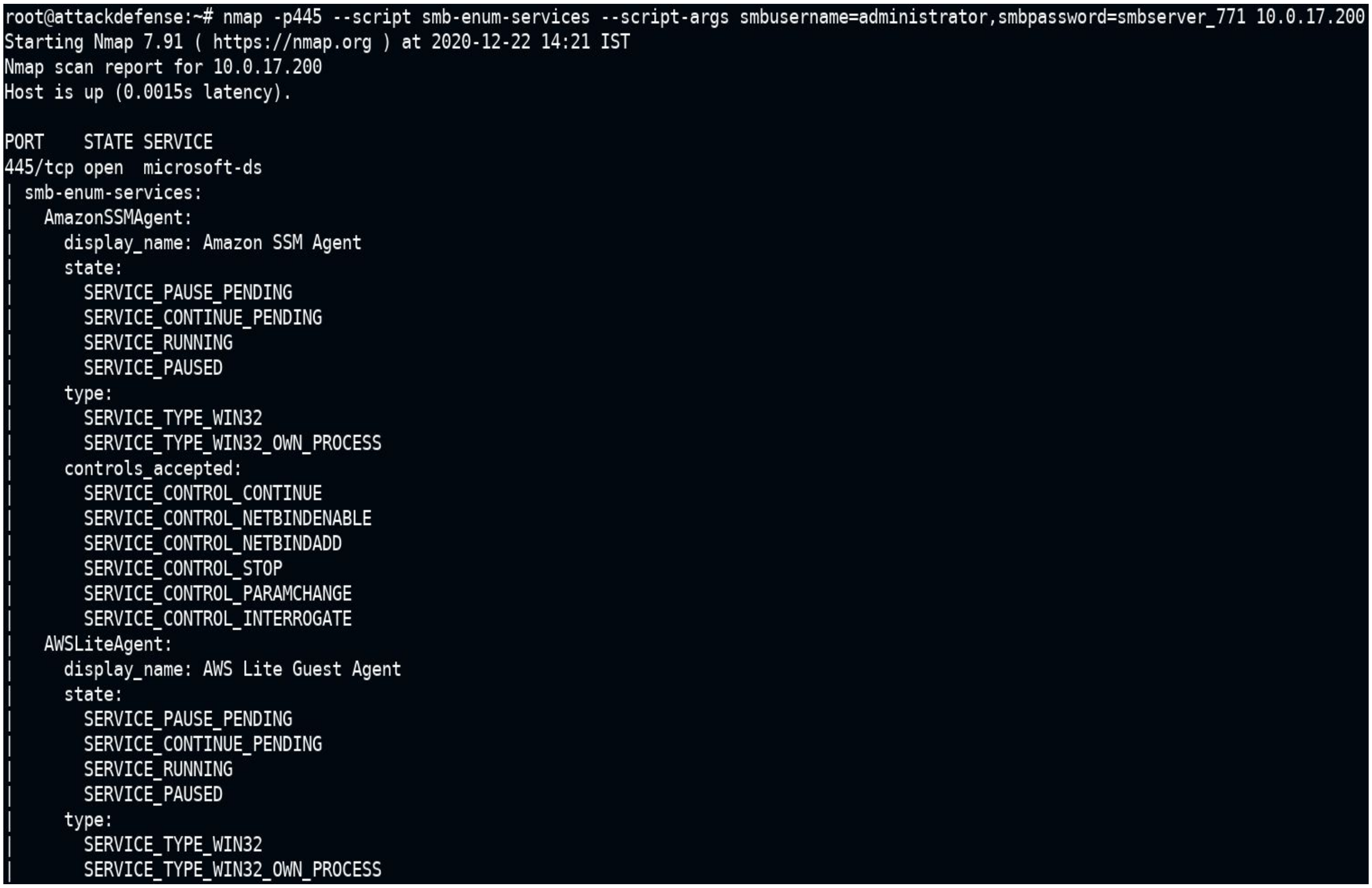
Command: nmap -p445 --script smb-enum-groups --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



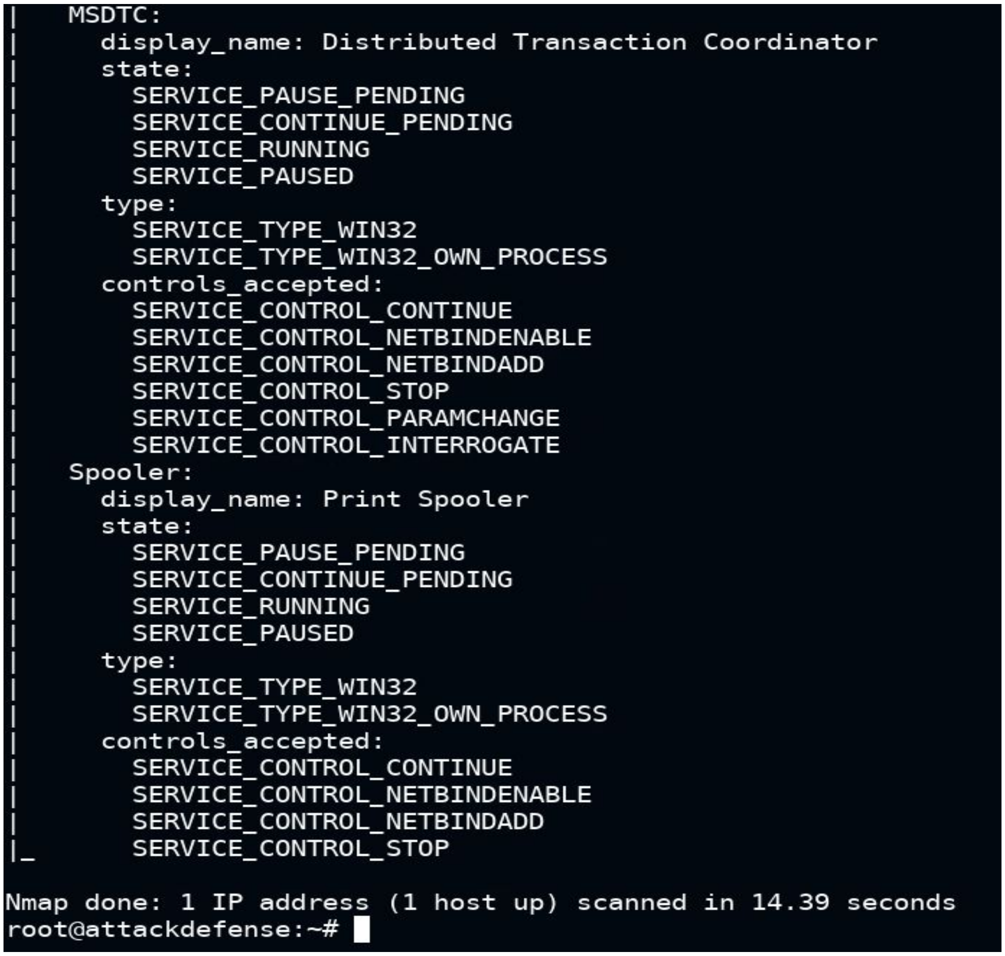
```
root@attackdefense:~# nmap -p445 --script smb-enum-groups --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:18 IST
Nmap scan report for 10.0.17.200
Host is up (0.0015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-groups:
|   Builtin\Administrators (RID: 544): Administrator, bob
|   Builtin\Users (RID: 545): bob
|   Builtin\Guests (RID: 546): Guest
|   Builtin\Power Users (RID: 547): <empty>
|   Builtin\Print Operators (RID: 550): <empty>
|   Builtin\Backup Operators (RID: 551): <empty>
|   Builtin\Replicator (RID: 552): <empty>
|   Builtin\Remote Desktop Users (RID: 555): bob
|   Builtin\Network Configuration Operators (RID: 556): <empty>
|   Builtin\Performance Monitor Users (RID: 558): <empty>
|   Builtin\Performance Log Users (RID: 559): <empty>
|   Builtin\Distributed COM Users (RID: 562): <empty>
|   Builtin\IIS_IUSRS (RID: 568): <empty>
|   Builtin\Cryptographic Operators (RID: 569): <empty>
|   Builtin\Event Log Readers (RID: 573): <empty>
|   Builtin\Certificate Service DCOM Access (RID: 574): <empty>
|   Builtin\RDS Remote Access Servers (RID: 575): <empty>
|   Builtin\RDS Endpoint Servers (RID: 576): <empty>
|   Builtin\RDS Management Servers (RID: 577): <empty>
|   Builtin\Hyper-V Administrators (RID: 578): <empty>
|   Builtin\Access Control Assistance Operators (RID: 579): <empty>
|   Builtin\Remote Management Users (RID: 580): <empty>
|_  WIN-OMCNBKR66MN\WinRMRemoteWMIUsers__ (RID: 1000): <empty>

Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
root@attackdefense:~# 
```

Step 12: Enumerating services on a target machine.

Command: nmap -p445 --script smb-enum-services --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



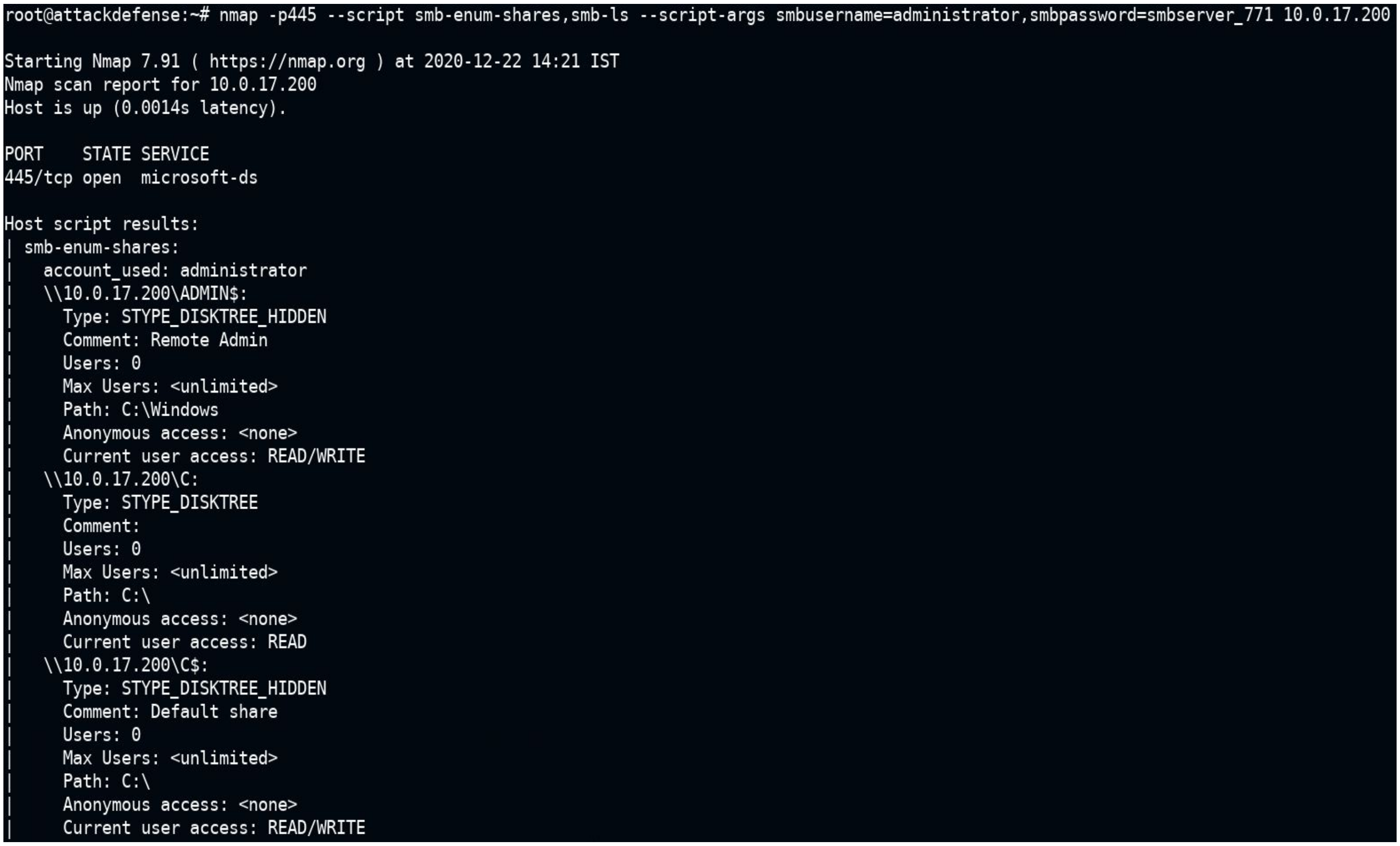
```
root@attackdefense:~# nmap -p445 --script smb-enum-services --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:21 IST
Nmap scan report for 10.0.17.200
Host is up (0.0015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
| smb-enum-services:
|   AmazonSSMAgent:
|     display_name: Amazon SSM Agent
|     state:
|       SERVICE_PAUSE_PENDING
|       SERVICE_CONTINUE_PENDING
|       SERVICE_RUNNING
|       SERVICE_PAUSED
|     type:
|       SERVICE_TYPE_WIN32
|       SERVICE_TYPE_WIN32_OWN_PROCESS
|     controls_accepted:
|       SERVICE_CONTROL_CONTINUE
|       SERVICE_CONTROL_NETBINDENABLE
|       SERVICE_CONTROL_NETBINDADD
|       SERVICE_CONTROL_STOP
|       SERVICE_CONTROL_PARAMCHANGE
|       SERVICE_CONTROL_INTERROGATE
|   AWSLiteAgent:
|     display_name: AWS Lite Guest Agent
|     state:
|       SERVICE_PAUSE_PENDING
|       SERVICE_CONTINUE_PENDING
|       SERVICE_RUNNING
|       SERVICE_PAUSED
|     type:
|       SERVICE_TYPE_WIN32
|       SERVICE_TYPE_WIN32_OWN_PROCESS
```



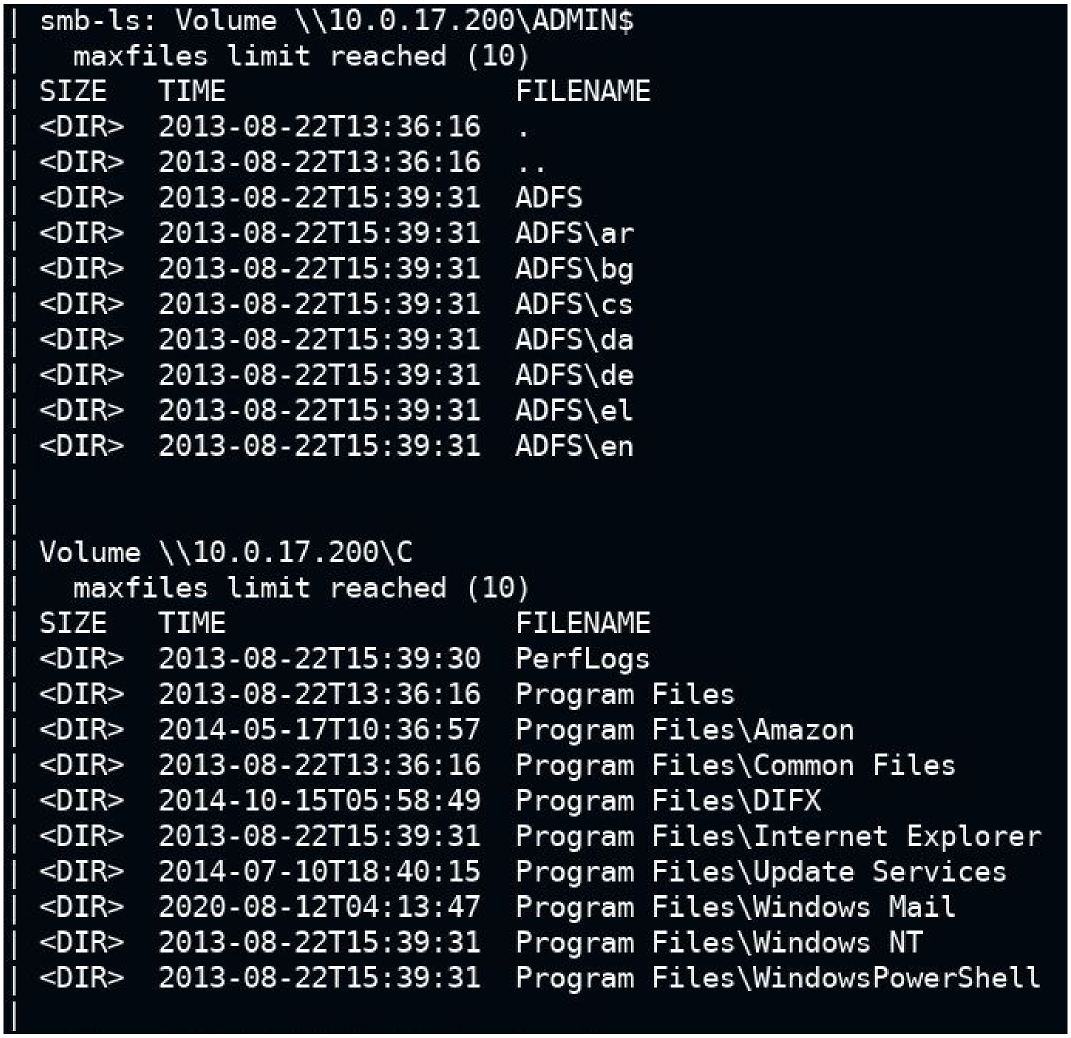
```
|   MSDTC:
|     display_name: Distributed Transaction Coordinator
|     state:
|       SERVICE_PAUSE_PENDING
|       SERVICE_CONTINUE_PENDING
|       SERVICE_RUNNING
|       SERVICE_PAUSED
|     type:
|       SERVICE_TYPE_WIN32
|       SERVICE_TYPE_WIN32_OWN_PROCESS
|     controls_accepted:
|       SERVICE_CONTROL_CONTINUE
|       SERVICE_CONTROL_NETBINDENABLE
|       SERVICE_CONTROL_NETBINDADD
|       SERVICE_CONTROL_STOP
|       SERVICE_CONTROL_PARAMCHANGE
|       SERVICE_CONTROL_INTERROGATE
|   Spooler:
|     display_name: Print Spooler
|     state:
|       SERVICE_PAUSE_PENDING
|       SERVICE_CONTINUE_PENDING
|       SERVICE_RUNNING
|       SERVICE_PAUSED
|     type:
|       SERVICE_TYPE_WIN32
|       SERVICE_TYPE_WIN32_OWN_PROCESS
|     controls_accepted:
|       SERVICE_CONTROL_CONTINUE
|       SERVICE_CONTROL_NETBINDENABLE
|       SERVICE_CONTROL_NETBINDADD
|_      SERVICE_CONTROL_STOP

Nmap done: 1 IP address (1 host up) scanned in 14.39 seconds
root@attackdefense:~# 
```

Step 12: Enumerating all the shared folders and drives then running the **ls** command (The **ls** command is used to list files or directories, similarly **dir** in windows) on all the shared folders.

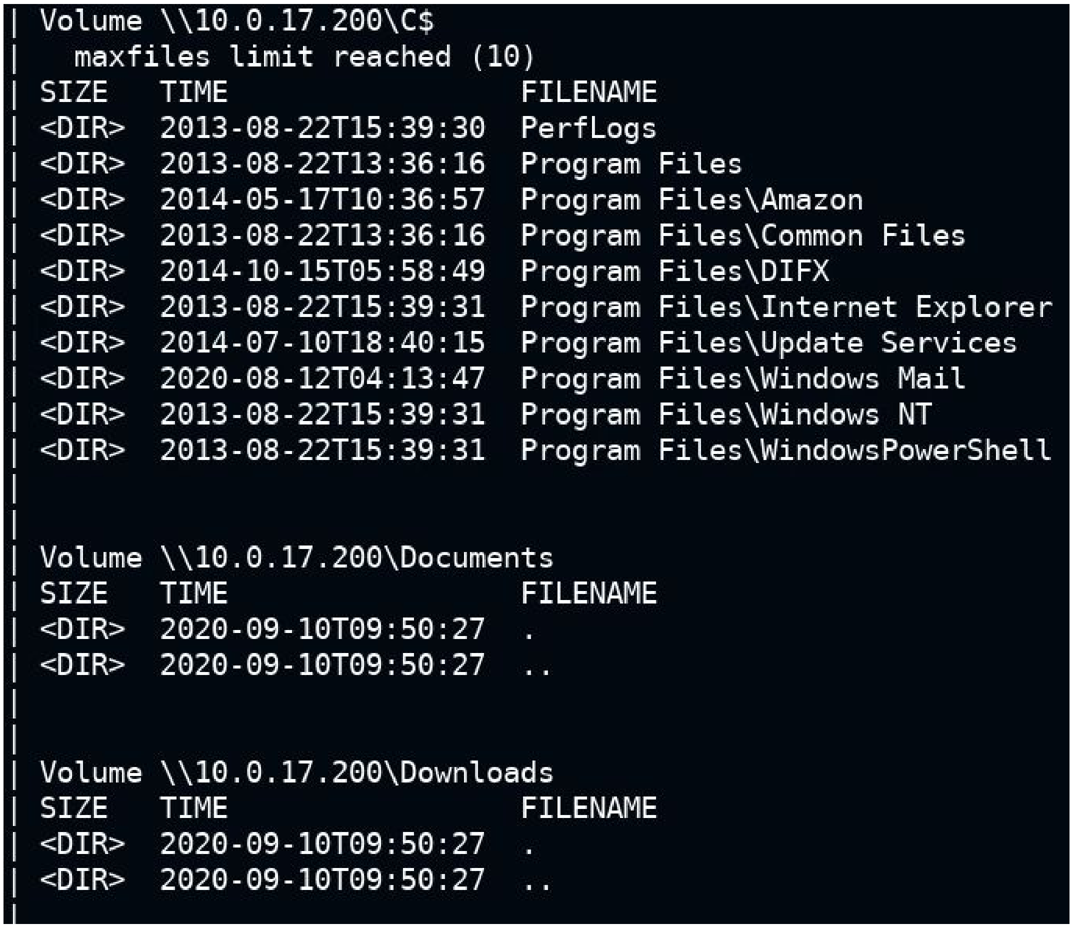
Command: nmap -p445 --script smb-enum-shares,smb-ls --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200



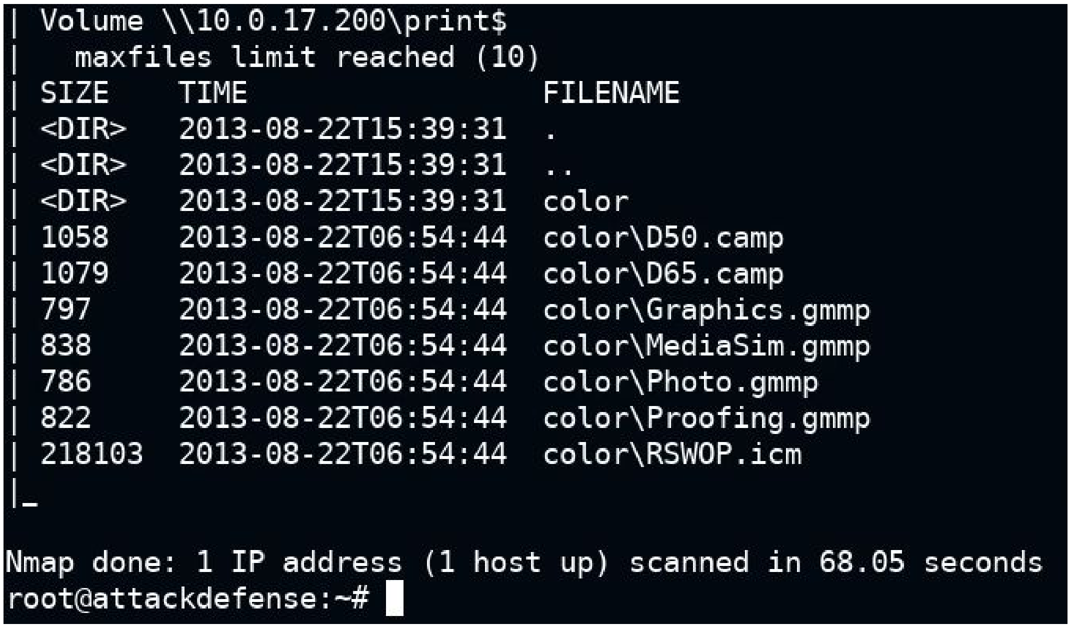
```
root@attackdefense:~# nmap -p445 --script smb-enum-shares,smb-ls --script-args smbusername=administrator,smbpassword=smbserver_771 10.0.17.200

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 14:21 IST
Nmap scan report for 10.0.17.200
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: administrator
|   \\10.0.17.200\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Windows
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.17.200\C:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.0.17.200\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\
|     Anonymous access: <none>
|     Current user access: READ/WRITE
```



```
| smb-ls: Volume \\10.0.17.200\ADMIN$
|   maxfiles limit reached (10)
| SIZE   TIME                 FILENAME
| <DIR>  2013-08-22T13:36:16  .
| <DIR>  2013-08-22T13:36:16  ..
| <DIR>  2013-08-22T15:39:31  ADFS
| <DIR>  2013-08-22T15:39:31  ADFS\ar
| <DIR>  2013-08-22T15:39:31  ADFS\bg
| <DIR>  2013-08-22T15:39:31  ADFS\cs
| <DIR>  2013-08-22T15:39:31  ADFS\da
| <DIR>  2013-08-22T15:39:31  ADFS\de
| <DIR>  2013-08-22T15:39:31  ADFS\el
| <DIR>  2013-08-22T15:39:31  ADFS\en
|
|
| Volume \\10.0.17.200\C
|   maxfiles limit reached (10)
| SIZE   TIME                 FILENAME
| <DIR>  2013-08-22T15:39:30  PerfLogs
| <DIR>  2013-08-22T13:36:16  Program Files
| <DIR>  2014-05-17T10:36:57  Program Files\Amazon
| <DIR>  2013-08-22T13:36:16  Program Files\Common Files
| <DIR>  2014-10-15T05:58:49  Program Files\DIFX
| <DIR>  2013-08-22T15:39:31  Program Files\Internet Explorer
| <DIR>  2014-07-10T18:40:15  Program Files\Update Services
| <DIR>  2020-08-12T04:13:47  Program Files\Windows Mail
| <DIR>  2013-08-22T15:39:31  Program Files\Windows NT
| <DIR>  2013-08-22T15:39:31  Program Files\WindowsPowerShell
|
```



```
|  Volume \\10.0.17.200\C$
|    maxfiles limit reached (10)
|  SIZE   TIME                 FILENAME
|  <DIR>  2013-08-22T15:39:30  PerfLogs
|  <DIR>  2013-08-22T13:36:16  Program Files
|  <DIR>  2014-05-17T10:36:57  Program Files\Amazon
|  <DIR>  2013-08-22T13:36:16  Program Files\Common Files
|  <DIR>  2014-10-15T05:58:49  Program Files\DIFX
|  <DIR>  2013-08-22T15:39:31  Program Files\Internet Explorer
|  <DIR>  2014-07-10T18:40:15  Program Files\Update Services
|  <DIR>  2020-08-12T04:13:47  Program Files\Windows Mail
|  <DIR>  2013-08-22T15:39:31  Program Files\Windows NT
|  <DIR>  2013-08-22T15:39:31  Program Files\WindowsPowerShell
|
|
|  Volume \\10.0.17.200\Documents
|  SIZE   TIME                 FILENAME
|  <DIR>  2020-09-10T09:50:27  .
|  <DIR>  2020-09-10T09:50:27  ..
|
|
|  Volume \\10.0.17.200\Downloads
|  SIZE   TIME                 FILENAME
|  <DIR>  2020-09-10T09:50:27  .
|  <DIR>  2020-09-10T09:50:27  ..
|
```



```
| Volume \\10.0.17.200\print$
|   maxfiles limit reached (10)
| SIZE    TIME                 FILENAME
| <DIR>   2013-08-22T15:39:31  .
| <DIR>   2013-08-22T15:39:31  ..
| <DIR>   2013-08-22T15:39:31  color
| 1058    2013-08-22T06:54:44  color\D50.camp
| 1079    2013-08-22T06:54:44  color\D65.camp
| 797     2013-08-22T06:54:44  color\Graphics.gmmp
| 838     2013-08-22T06:54:44  color\MediaSim.gmmp
| 786     2013-08-22T06:54:44  color\Photo.gmmp
| 822     2013-08-22T06:54:44  color\Proofing.gmmp
| 218103  2013-08-22T06:54:44  color\RSWOP.icm
|_

Nmap done: 1 IP address (1 host up) scanned in 68.05 seconds
root@attackdefense:~# 
```

References:

1. Nmap (https://nmap.org/)
2. Nmap Scripts (https://nmap.org/nsedoc/scripts)