

Try Hack Me

Answer the questions below

What does SMB stand for?

Server Message Block

✓ Correct Answer

What type of protocol is SMB?

response-request

✓ Correct Answer

What protocol suite do clients use to connect to the server?

TCP/IP

✓ Correct Answer

What systems does Samba run on?

Unix

✓ Correct Answer

Target Machine Information

Title	Target IP Address	Expires
polosmb3	10.10.1.134	57min 5s

?

Add 1 hour

Terminate

Task 1 Get Connected

Task 2 Understanding SMB

Task 3 Enumerating SMB

Lets Get Started

▶ Start Machine

Before we begin, make sure to deploy the room and give it some time to boot. Please be aware, this can take up to five minutes so be patient!

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
) on Thu Oct 22 00:36:05 2025
```

```
=====
|   Target Information   |
=====
Target ..... 10.10.1.134
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.1.134 |
=====
[+] Got domain/workgroup name: WORKGROUP
```

```
root@srv543816:/var/opt/enum4linux# smbclient //10.10.1.134/profiles
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
```

```
smb: \>
root@srv543816:/var/opt# smbclient //10.10.1.134/profiles
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Tue Apr 21 11:08:23 2020
..               D           0   Tue Apr 21 10:49:56 2020
.cache           DH          0   Tue Apr 21 11:08:23 2020
.profile         H          807 Tue Apr 21 11:08:23 2020
.sudo_as_admin_successful H          0   Tue Apr 21 11:08:23 2020
.bash_logout     H          220 Tue Apr 21 11:08:23 2020
.viminfo         H          947 Tue Apr 21 11:08:23 2020
Working From Home Information.txt N          358 Tue Apr 21 11:08:23
2020
.ssh             DH          0   Tue Apr 21 11:08:23 2020
.bashrc          H         3771 Tue Apr 21 11:08:23 2020
.gnupg           DH          0   Tue Apr 21 11:08:23 2020

12316808 blocks of size 1024. 7584040 blocks available
smb: \> get "Working From Home Information.txt"
```

```
smb: \> get "Working From Home Information.txt"
getting file \Working From Home Information.txt of size 358 as Working
From Home Information.txt (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \> exit
```

```
root@srv543816:/var/opt# cat "Working From Home Information.txt"
John Cactus,
```

As you're well aware, due to the current pandemic most of POLO inc. has insisted that, wherever possible, employees should work from home. As such- your account has now been enabled with ssh access to the main server.

If there are any problems, please contact the IT department at it@polointernalcoms.uk

Regards,

James

Department Manager

```
root@srv543816:/var/opt#
```

Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?

John Cactus

✓ Correct Answer

What service has been configured to allow him to work from home?

ssh

✓ Correct Answer

```

root@srv543816:/var/opt# smbclient //10.10.1.134/profiles
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> cd .ssh
smb: \.ssh\> ls
.                  D            0   Tue Apr 21 11:08:23 2020
..                 D            0   Tue Apr 21 11:08:23 2020
id_rsa             A        1679   Tue Apr 21 11:08:23 2020
id_rsa.pub         N         396   Tue Apr 21 11:08:23 2020
authorized_keys    N            0   Tue Apr 21 11:08:23 2020

12316808 blocks of size 1024. 7584040 blocks available
smb: \.ssh\>

```

Okay! Now we know this, what directory on the share should we look in?

✓ Correct Answer

This directory contains authentication keys that allow a user to authenticate themselves on, and then access, a server. Which of these keys is most useful to us?

✓ Correct Answer

🔍 Hint

Download this file to your local machine, and change the permissions to "600" using "chmod 600 [file]"

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-96-generic x86_64)

```

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

```

System information as of Wed Oct 21 22:57:37 UTC 2020

```

System load:  0.0           Processes:            93
Usage of /:   33.3% of 11.75GB Users logged in:      0
Memory usage: 17%          IP address for eth0: 10.10.78.132
Swap usage:   0%

```

```

22 packages can be updated.
0 updates are security updates.

```

Last login: Tue Apr 21 11:19:15 2020 from 192.168.1.110

```

cactus@polosmb:~$ ls
smb.txt
cactus@polosmb:~$ cat smb.txt
THM{smb_is_fun_eh?}
cactus@polosmb:~$

```

Answer the questions below

What is Telnet?

application protocol

✓ Correct Answer

What has slowly replaced Telnet?

ssh

✓ Correct Answer

How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?

telnet 10.10.10.3 23

✓ Correct Answer

The lack of what, means that all Telnet communication is in plaintext?

encryption

✓ Correct Answer

🔍 Hint

```
Last login: Thu May 1 11:52:38 2025 from 103.166.27.177
root@srv543816:~# nmap 10.10.191.181
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-01 11:58 UTC
Nmap scan report for 10.10.191.181
Host is up (0.13s latency).
All 1000 scanned ports on 10.10.191.181 are closed

Nmap done: 1 IP address (1 host up) scanned in 18.94 seconds
root@srv543816:~#
```

```
root@srv543816:~# nmap -p- -sS -sC -sV -Pn -O 10.10.191.181
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-01 12:01 UTC
Stats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.28% done; ETC: 12:11 (0:08:39 remaining)
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.82% done; ETC: 12:12 (0:08:20 remaining)
Stats: 0:05:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.87% done; ETC: 12:12 (0:06:54 remaining)
Stats: 0:07:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.39% done; ETC: 12:13 (0:04:51 remaining)
Stats: 0:09:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.93% done; ETC: 12:14 (0:03:17 remaining)
Stats: 0:13:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.47% done; ETC: 12:16 (0:01:27 remaining)
Stats: 0:14:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.63% done; ETC: 12:16 (0:00:50 remaining)
Stats: 0:15:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

```
SYN Stealth Scan Timing: About 98.03% done; ETC: 12:17 (0:00:19 remaining)
Stats: 0:16:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 0.00% done
Stats: 0:17:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 0.00% done
Stats: 0:17:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 0.00% done
Stats: 0:18:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 0.00% done
Stats: 0:18:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 0.00% done
Stats: 0:19:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:19:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.58% done; ETC: 12:20 (0:00:00 remaining)
Stats: 0:19:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.58% done; ETC: 12:20 (0:00:00 remaining)
Nmap scan report for 10.10.191.181
Host is up (0.13s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
8012/tcp  open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest,
GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC,
LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, RPCCheck, RTSPRequest,
SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer,
TerminalServerCookie, X11Probe:
|_   SKIDY'S BACKDOOR. Type .HELP to view commands
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8012-TCP:V=7.80%I=7%D=5/1%Time=68136661%P=x86_64-pc-linux-gnu%(NUL
SF:L,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x20view\x20commands
SF:\n")%r(GenericLines,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x
SF:20view\x20commands\n")%r(GetRequest,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x
SF:20\HELP\x20to\x20view\x20commands\n")%r(HTTPOptions,2E,"SKIDY'S\x20BAC
SF:KDOOR\.\x20Type\x20\HELP\x20to\x20view\x20commands\n")%r(RTSPRequest,2
SF:E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x20view\x20commands\n"
SF:)%r(RPCCheck,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x20view\
SF:x20commands\n")%r(DNSVersionBindReqTCP,2E,"SKIDY'S\x20BACKDOOR\.\x20Typ
SF:e\x20\HELP\x20to\x20view\x20commands\n")%r(DNSStatusRequestTCP,2E,"SKI
SF:DY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x20view\x20commands\n")%r(He
SF:lp,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to\x20view\x20command
SF:s\n")%r(SSLSessionReq,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\HELP\x20to
```

```
SF:\x20view\x20commands\n")%r(TerminalServerCookie,2E,"SKIDY'S\x20BACKDOOR
SF:\.\x20Type\x20\.\HELP\x20to\x20view\x20commands\n")%r(TLSSessionReq,2E,"
SF:SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20commands\n")%r
SF:(Kerberos,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20
SF:commands\n")%r(SMBProgNeg,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x
SF:20to\x20view\x20commands\n")%r(X11Probe,2E,"SKIDY'S\x20BACKDOOR\.\x20Ty
SF:pe\x20\.\HELP\x20to\x20view\x20commands\n")%r(FourOhFourRequest,2E,"SKID
SF:Y'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20commands\n")%r(LPD
SF:String,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20com
SF:mands\n")%r(LDAPSearchReq,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x
SF:20to\x20view\x20commands\n")%r(LDAPBindReq,2E,"SKIDY'S\x20BACKDOOR\.\x2
SF:0Type\x20\.\HELP\x20to\x20view\x20commands\n")%r(SIPOptions,2E,"SKIDY'S\
SF:x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20commands\n")%r(LANDesk
SF:-RC,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20to\x20view\x20comman
SF:ds\n")%r(TerminalServer,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\.\HELP\x20
SF:to\x20view\x20commands\n")%r(NCP,2E,"SKIDY'S\x20BACKDOOR\.\x20Type\x20\
SF:\.\HELP\x20to\x20view\x20commands\n");
```

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.80%E=4%D=5/1%OT=8012%CT=1%CU=39710%PV=Y%DS=5%DC=I%G=Y%TM=681367

OS:0C%P=x86_64-pc-linux-

gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)SE

OS:Q(SP=105%GCD=1%ISR=105%TI=Z%CI=Z%TS=A)OPS(O1=M508ST11NW7%O2=M508ST11NW7%

OS:O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=F4B3%W2

OS:=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NN

OS:NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%

OS:DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%

OS:O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%

OS:W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%

OS:RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 5 hops

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 1166.76 seconds

root@srv543816:~#

```

root@srv543816:~# nmap -p- -sS -sC -sV -O 10.10.104.185
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-01 12:50 UTC
Stats: 0:08:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.64% done; ETC: 13:07 (0:08:50 remaining)
Stats: 0:17:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.92% done; ETC: 13:11 (0:04:04 remaining)
Stats: 0:18:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.01% done; ETC: 13:11 (0:03:14 remaining)
Stats: 0:21:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.11% done; ETC: 13:12 (0:00:12 remaining)
Stats: 0:22:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.10.104.185
Host is up (0.16s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0      0          353 Apr 24  2020
PUBLIC_NOTICE.txt
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.17.48.117
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/1%OT=21%CT=1%CU=32117%PV=Y%DS=5%DC=I%G=Y%TM=6813736
7
OS:%P=x86_64-pc-linux-
gnu)SEQ(SP=FE%GCD=1%ISR=109%TI=Z%CI=I%II=I%TS=A)SEQ(S
OS:P=FE%GCD=1%ISR=109%TI=Z%II=I%TS=A)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=
M
OS:508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)WIN(W1=68DF%W2=68
D

```

```
OS:F%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6
%
OS:CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y
Y
OS:%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
R
OS:D=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0
%
OS:S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
C
OS:K=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 5 hops

Service Info: Host: Welcome

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

:/nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1382.32 seconds

root@srv543816:~#

10.10.104.185


```
3306/tcp open  mysql
```

```

root@srv543816:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .
      '   dB'                BBP
dB'dB'dB'dB' dBBP      dBP      dBP BB
dB'dB'dB'dB' dBP      dBP      dBP BB
dB'dB'dB'dB' dBBBBP    dBP      dBBBBBBB

                                dBBBBBP dBBBBBb dBP      dBBBBBP dBP dBBBBBBB
                                dB' dBP      dB'.BP
                                |      dBP      dBBBB' dBP      dB'.BP dBP      dBP
--o--      dBP      dBP      dBP      dB'.BP dBP      dBP
                                |      dBBBBP dBP      dBBBBP dBBBBP dBP      dBP

      o                                To boldly go where no
                                      shell has gone before

      =[ metasploit v6.4.54-dev-                                ]
+ -- --=[ 2500 exploits - 1288 auxiliary - 431 post                ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops                  ]
+ -- --=[ 9 evasion                                                ]

Metasploit Documentation: https://docs.metasploit.com/

```



Congratulations on completing Network Services 2!!! 🎉

Points earned 🔑 440	Completed tasks ✅ 11	Room type 👤 Walkthrough	Difficulty 📶 Easy	Streak 🔥 2
------------------------	-------------------------	----------------------------	----------------------	---------------

💬 Leave Feedback

Next

Room progress (13%)

What is HTTPS? (HyperText Transfer Protocol Secure)

HTTPS is the secure version of HTTP. HTTPS data is encrypted so it not only stops people from seeing the data you are receiving and sending, but it also gives you assurances that you're talking to the correct web server and not something impersonating it.

Answer the questions below

What does HTTP stand for?

HyperText Transfer Protocol ✓ Correct Answer

What does the S in HTTPS stand for?

secure ✓ Correct Answer

On the mock webpage on the right there is an issue, once you've found it, click on it. What is the challenge flag?

THM{INVALID_HTTP_CERT} ✓ Correct Answer

http://tryhackme.com/

TryHackMe

Welcome To TryHackMe



What is Networking?



Info

Room



Network Services



Easy

Room



Network Services 2



Easy

Room



HTTP in Detail



Easy

Room

