HackerFrogs Afterschool
Network Hacking – Session 2

Class:
Network Hacking

Workshop Number:
AS-NET-02

Document Version:
1.75

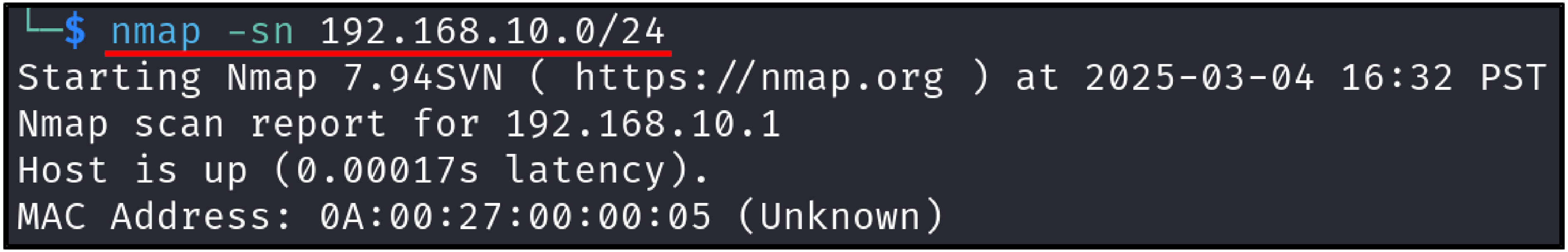
Special Requirements:
Registered account
at tryhackme.com

Welcome to HackerFrogs Afterschool!

This is the second session for network hacking!

Let's go over the concepts we covered in the previous session!

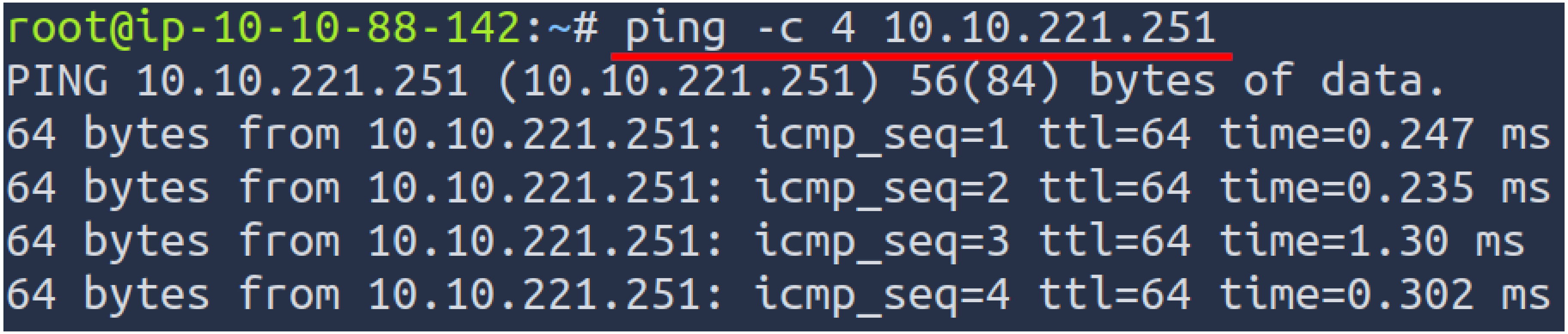
Ping Sweeping



```
└─$ nmap -sn 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 16:32 PST
Nmap scan report for 192.168.10.1
Host is up (0.00017s latency).
MAC Address: 0A:00:27:00:00:05 (Unknown)
```

Ping sweeping is the act of sending ping packets to each address on a network range for the purpose of determining which IP addresses are online

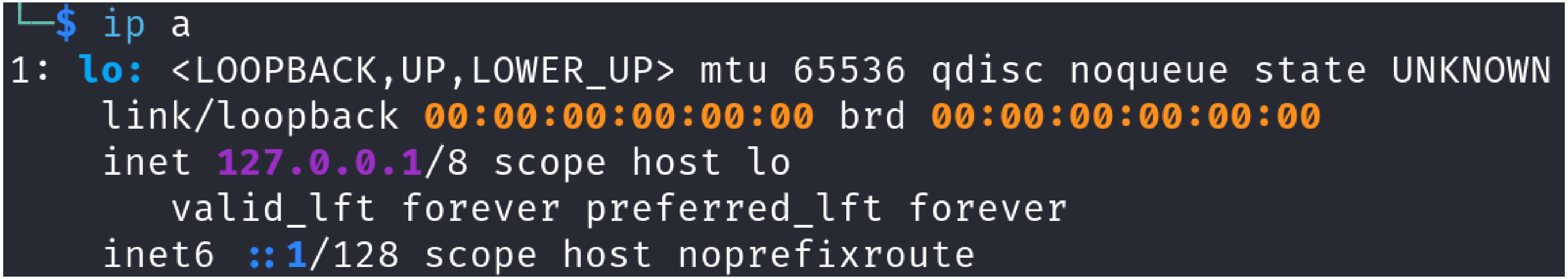
Ping Command



```
root@ip-10-10-88-142:~# ping -c 4 10.10.221.251
PING 10.10.221.251 (10.10.221.251) 56(84) bytes of data.
64 bytes from 10.10.221.251: icmp_seq=1 ttl=64 time=0.247 ms
64 bytes from 10.10.221.251: icmp_seq=2 ttl=64 time=0.235 ms
64 bytes from 10.10.221.251: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 10.10.221.251: icmp_seq=4 ttl=64 time=0.302 ms
```

The Ping command is the most common way we determine connectivity between two network devices

Looking Up Your Networking Info
Ip and Ifconfig commands

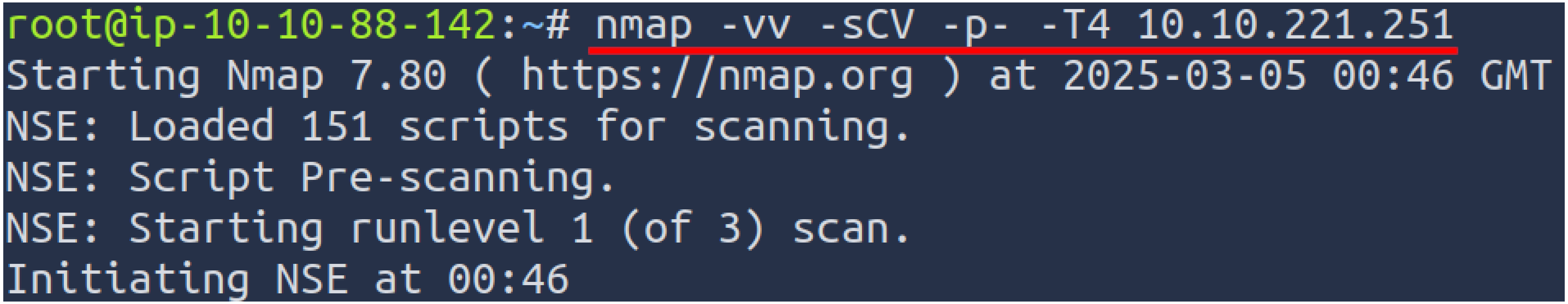


```
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
```

We'll also need to get our own networking info, which we can do with the Ip command. Ip command syntax:

```
ip a
```

Enumerating Open Ports /w Nmap



```
root@ip-10-10-88-142:~# nmap -vv -sCV -p- -T4 10.10.221.251
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-05 00:46 GMT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:46
```

Nmap is very common network security tool that can be used to determine which networking ports and services are open on remote servers

This Session's Topics

- common networking services

- FTP service

- SMB service

- Telnet service

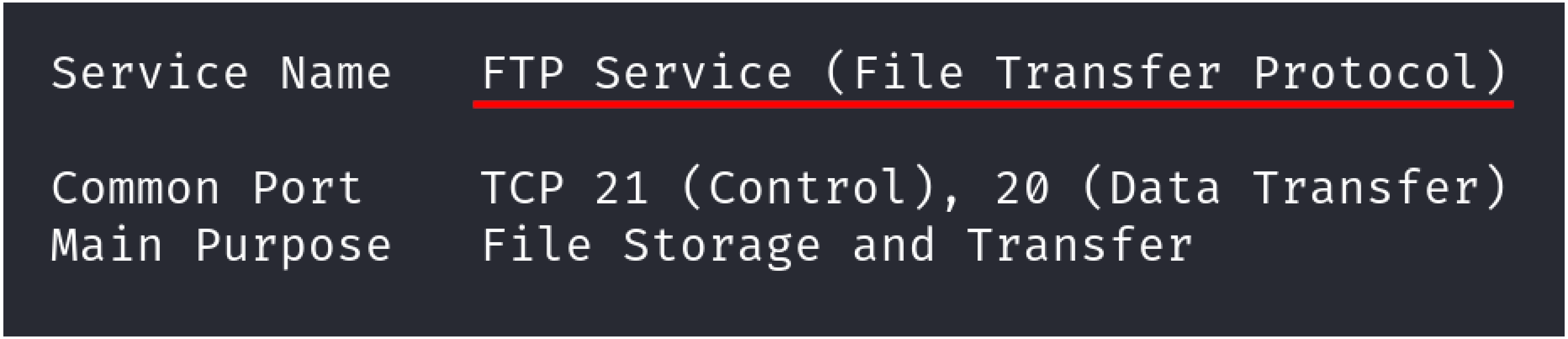
Accessing TryHackMe

Let's access this TryHackMe room to learn about common networking services:

https://tryhackme.com/room/learncyberin25days

The first part of this session is in Task 11 on this webpage

FTP Service (File Transfer Protocol)

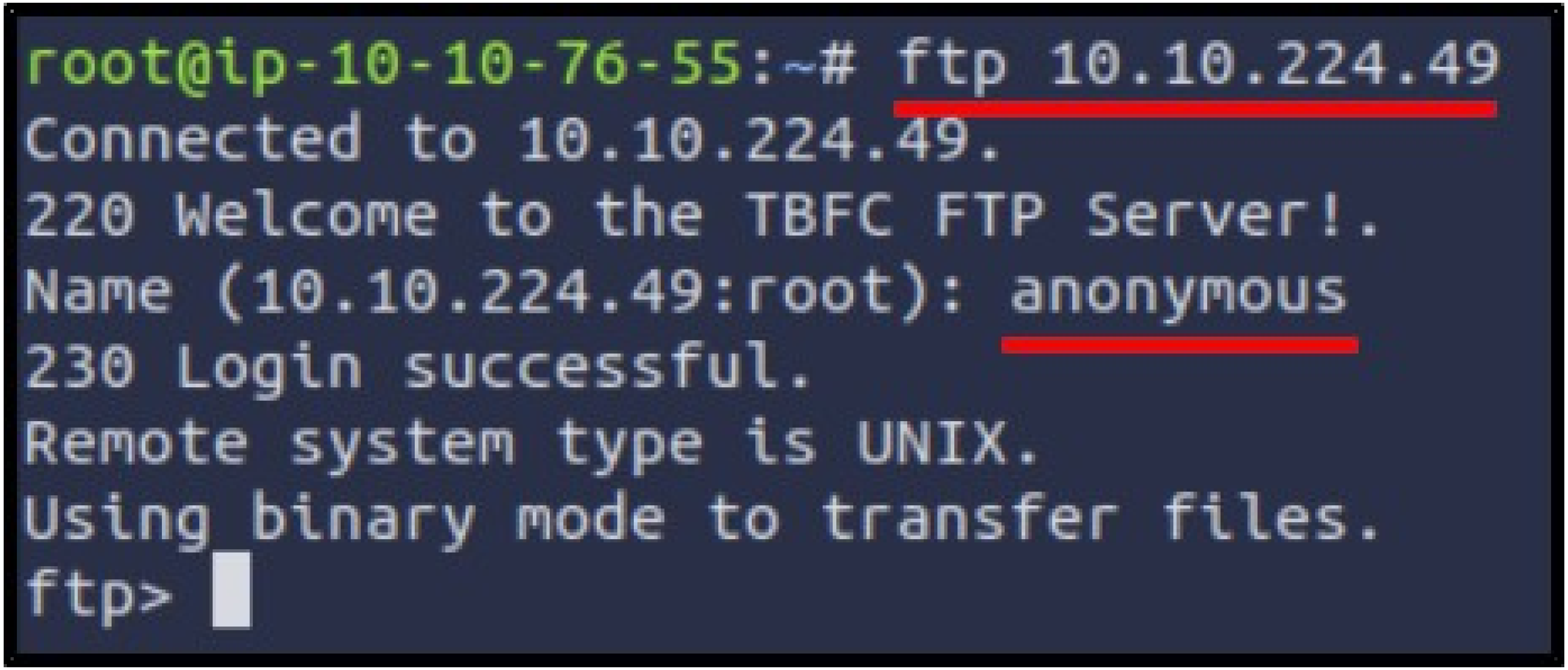


```
Service Name   FTP Service (File Transfer Protocol)

Common Port    TCP 21 (Control), 20 (Data Transfer)
Main Purpose   File Storage and Transfer
```

The FTP service is a common networking service which allows users to upload and download files

Accessing FTP



```
root@ip-10-10-76-55:~# ftp 10.10.224.49
Connected to 10.10.224.49.
220 Welcome to the TBFC FTP Server!.
Name (10.10.224.49:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

We can access the FTP service through the FTP client program, which can sometimes accept anonymous login

Common FTP Commands

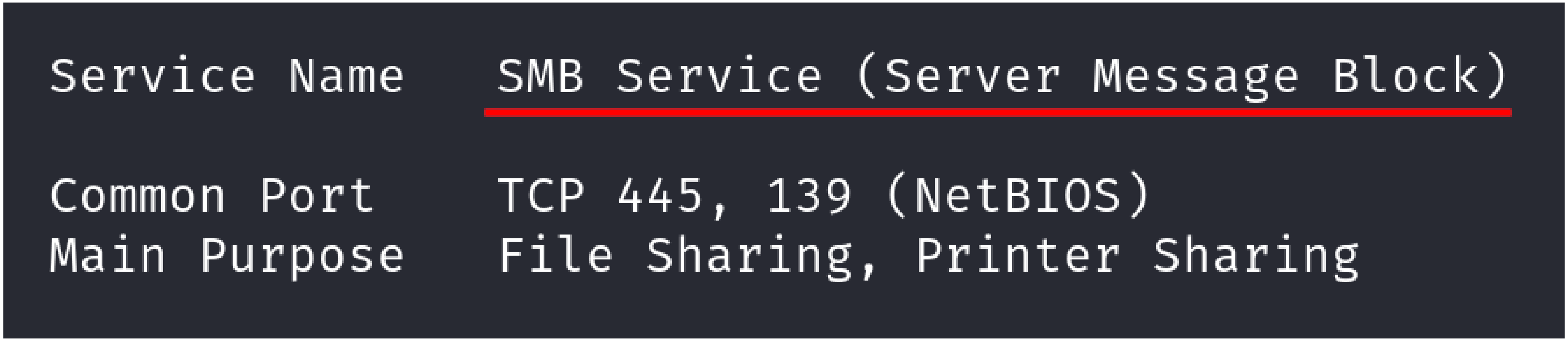
`ls`	<--- list out directory contents
`cd <directory>`	<--- change directory
`get <filename>`	<--- download file
`put <filename>`	<--- upload file
`quit`	<--- exit the program

Here's a list of common FTP commands

Next Service – SMB (Task 12)

Let's move on to another Task in the TryHackMe room to learn about the next networking service: SMB. Let's switch to Task 12 now

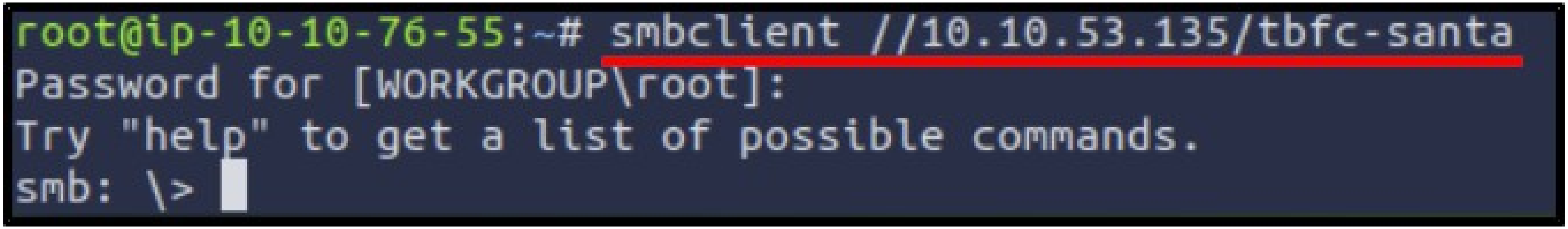
SMB Service (Server Message Block)



Service Name	SMB Service (Server Message Block)
Common Port	TCP 445, 139 (NetBIOS)
Main Purpose	File Sharing, Printer Sharing

The SMB service is a file and printer sharing service that is most commonly associated with the Windows OS

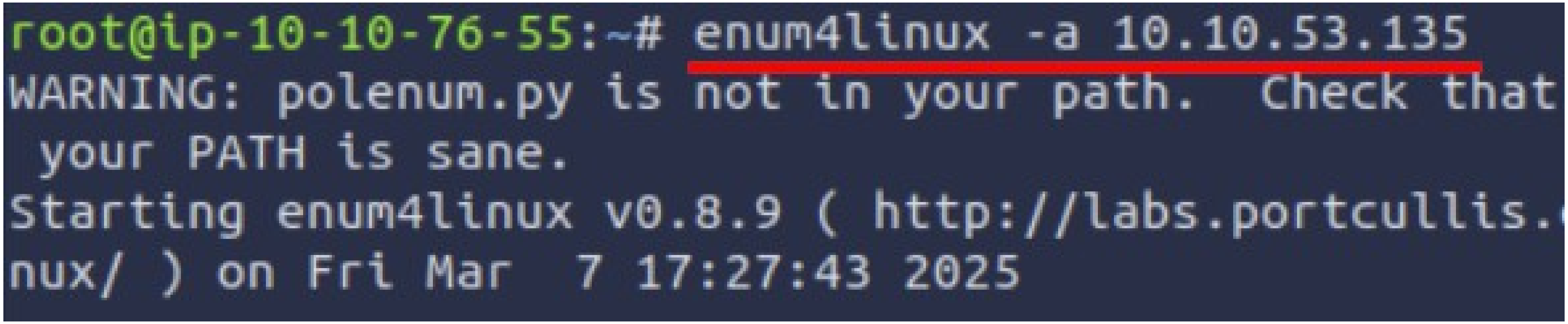
Accessing SMB



```
root@ip-10-10-76-55:~# smbclient //10.10.53.135/tbfc-santa
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

On Linux we can access SMB shares through the SMBclient program

SMB Enumeration (Enum4Linux)



```
root@ip-10-10-76-55:~# enum4linux -a 10.10.53.135
WARNING: polenum.py is not in your path.  Check that
 your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.
nux/ ) on Fri Mar  7 17:27:43 2025
```

But when we connect to SMB, we have to specify a share to connect to. We can use another program, Enum4Linux, to figure out which shares are available

Common SMB Commands

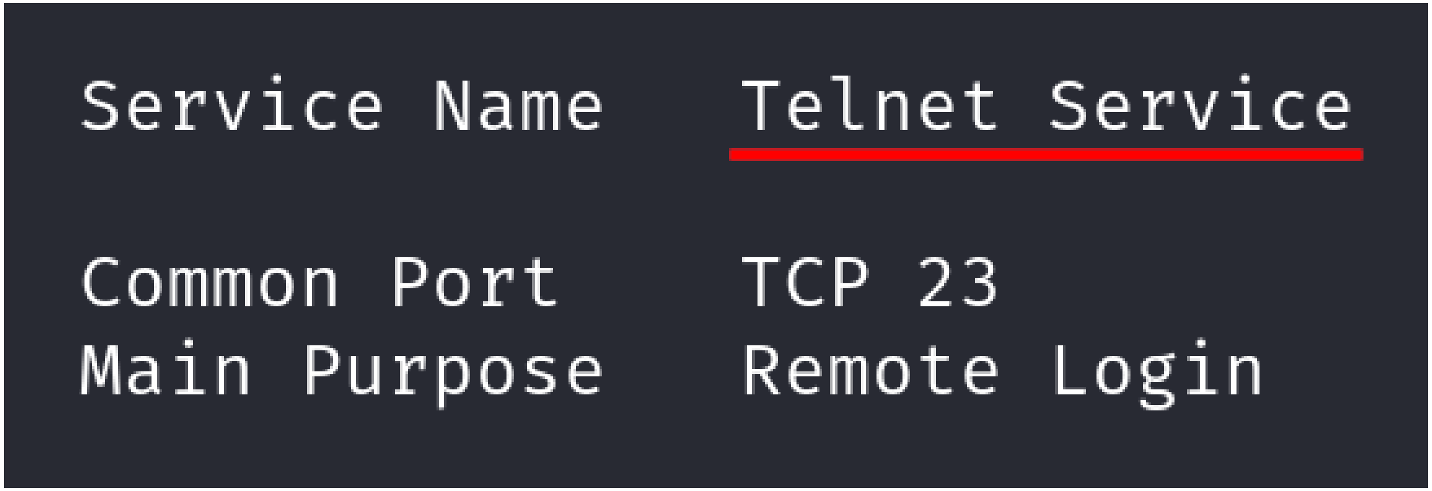
```
dir                 <--- list out directory contents
cd <directory>      <--- change directory
get <filename>      <--- download file
put <filename>      <--- upload file
exit                <--- exit the program
```

Here's a list of common SMB commands

Next Service – Telnet (Task 15)

Let's move on to another Task in the TryHackMe room to learn about the next networking service: Telnet. Let's switch to Task 15 now

Telnet (Telecommunications Network)

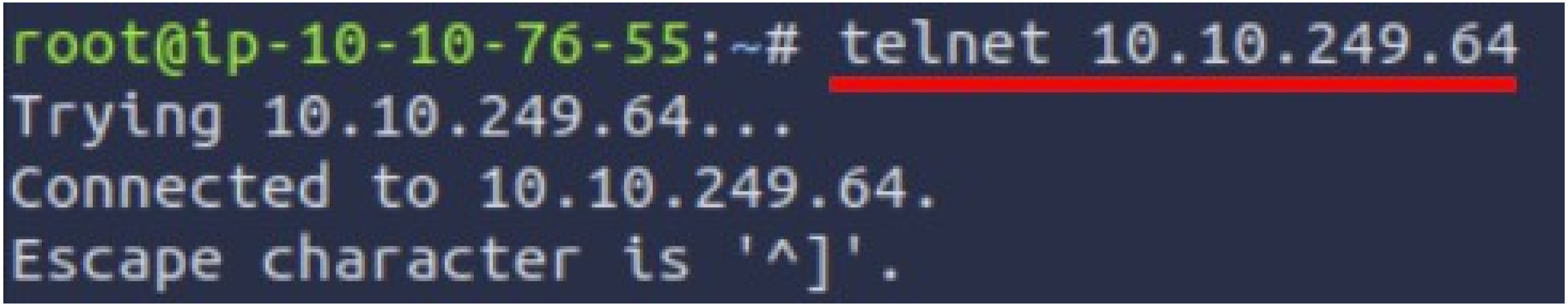


```
Service Name    Telnet Service

Common Port     TCP 23
Main Purpose    Remote Login
```

Telnet is a service that allows remote terminal login, and it is the predecessor to the SSH service

Accessing Telnet



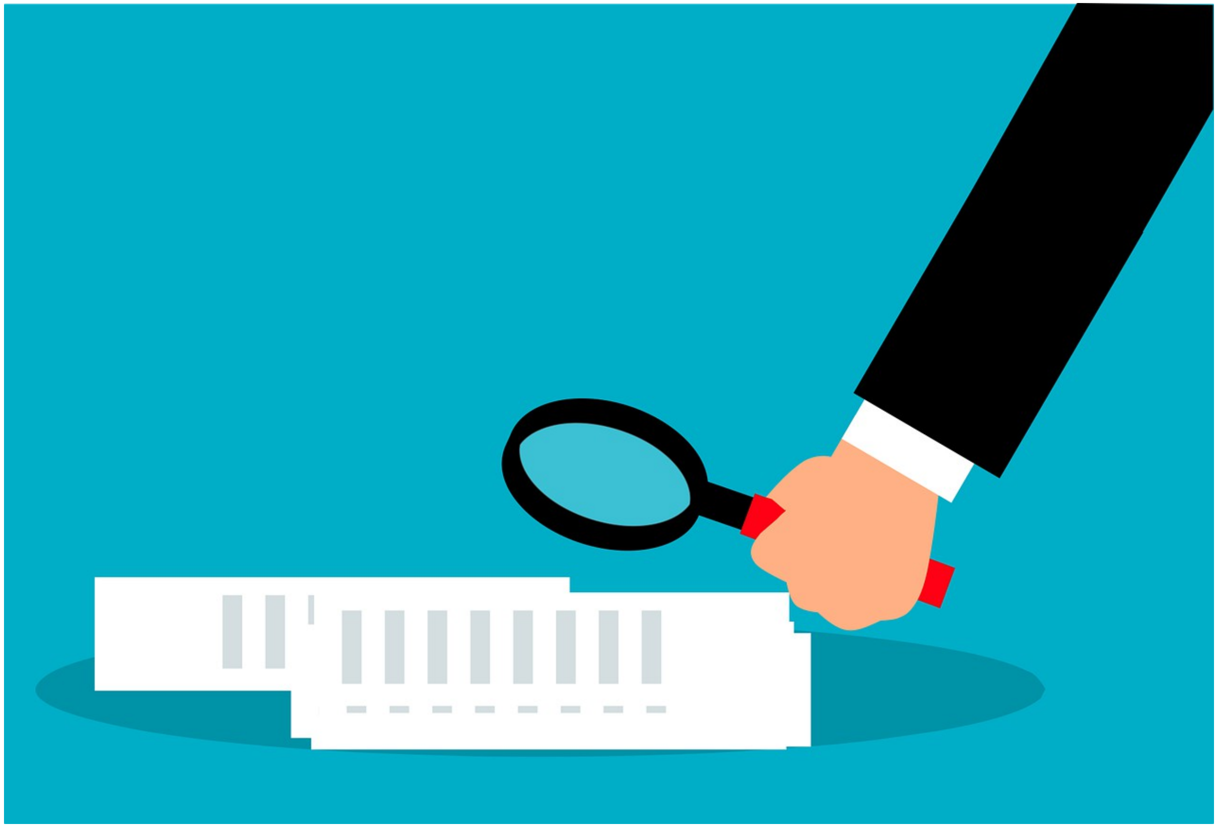
```
root@ip-10-10-76-55:~# telnet 10.10.249.64
Trying 10.10.249.64...
Connected to 10.10.249.64.
Escape character is '^]'.
```

We can access the Telnet service through the Telnet client program

Common Telnet Commands

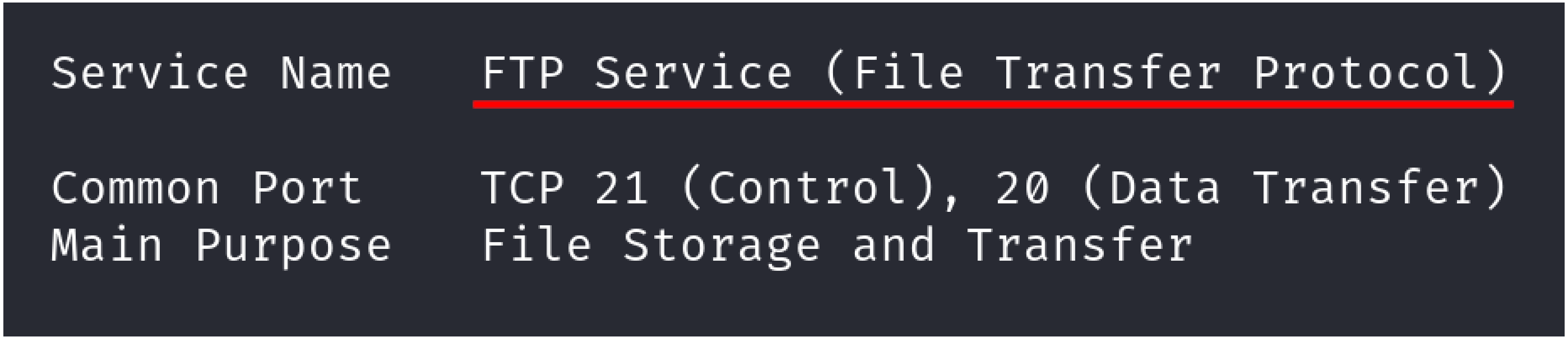
Typical Telnet access provides terminal access to the server, and you use the terminal commands associated with the server's OS (Linux, Windows, etc..) while using the Telnet client

Summary



Let's review the network hacking concepts we learned in this workshop:

FTP Service (File Transfer Protocol)

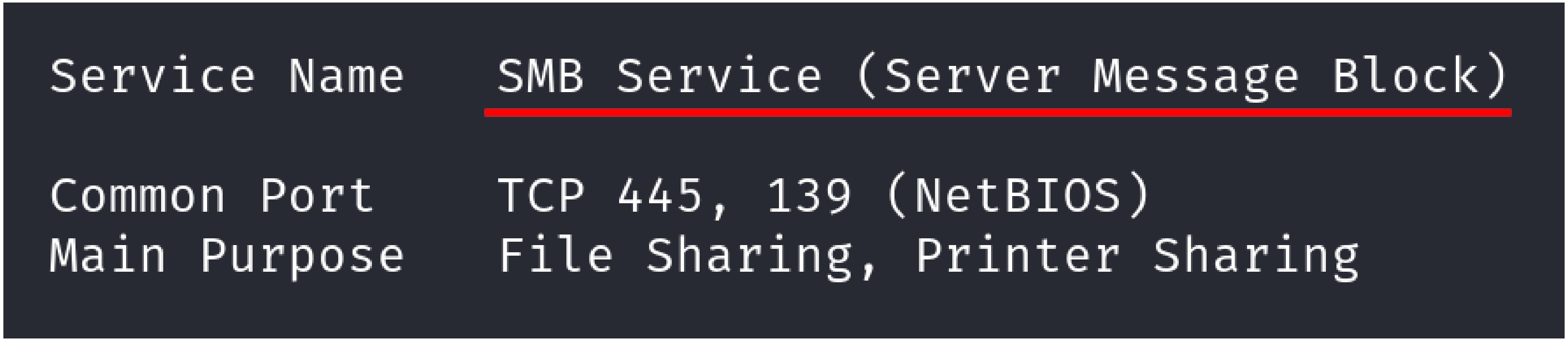


```
Service Name   FTP Service (File Transfer Protocol)

Common Port    TCP 21 (Control), 20 (Data Transfer)
Main Purpose   File Storage and Transfer
```

The FTP service is a common networking service which allows users to upload and download files

SMB Service (Server Message Block)

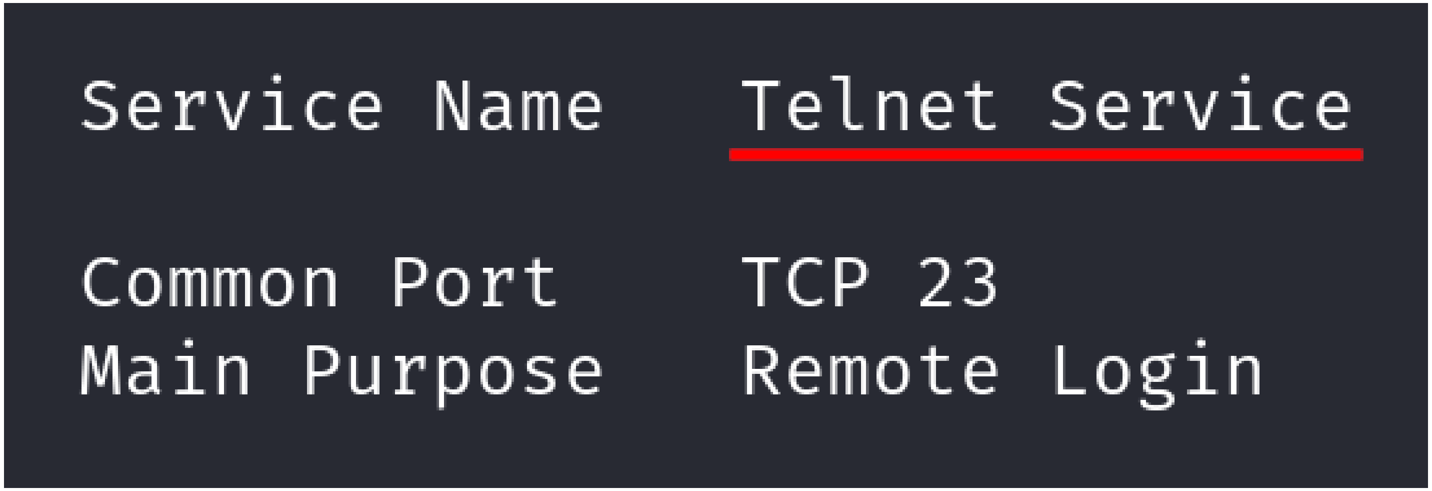


```
Service Name    SMB Service (Server Message Block)

Common Port     TCP 445, 139 (NetBIOS)
Main Purpose    File Sharing, Printer Sharing
```

The SMB service is a file and printer sharing service that is most commonly associated with the Windows OS

Telnet (Telecommunications Network)



```
Service Name    Telnet Service

Common Port     TCP 23
Main Purpose    Remote Login
```

Telnet is a service that allows remote terminal login, and it is the predecessor to the SSH service

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning about how to perform web app enumeration with a number of different tools!