Hack the box - Netmon

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)
| 02-03-19  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

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**

ftp 10.10.10.152
anonymous
anonymous

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

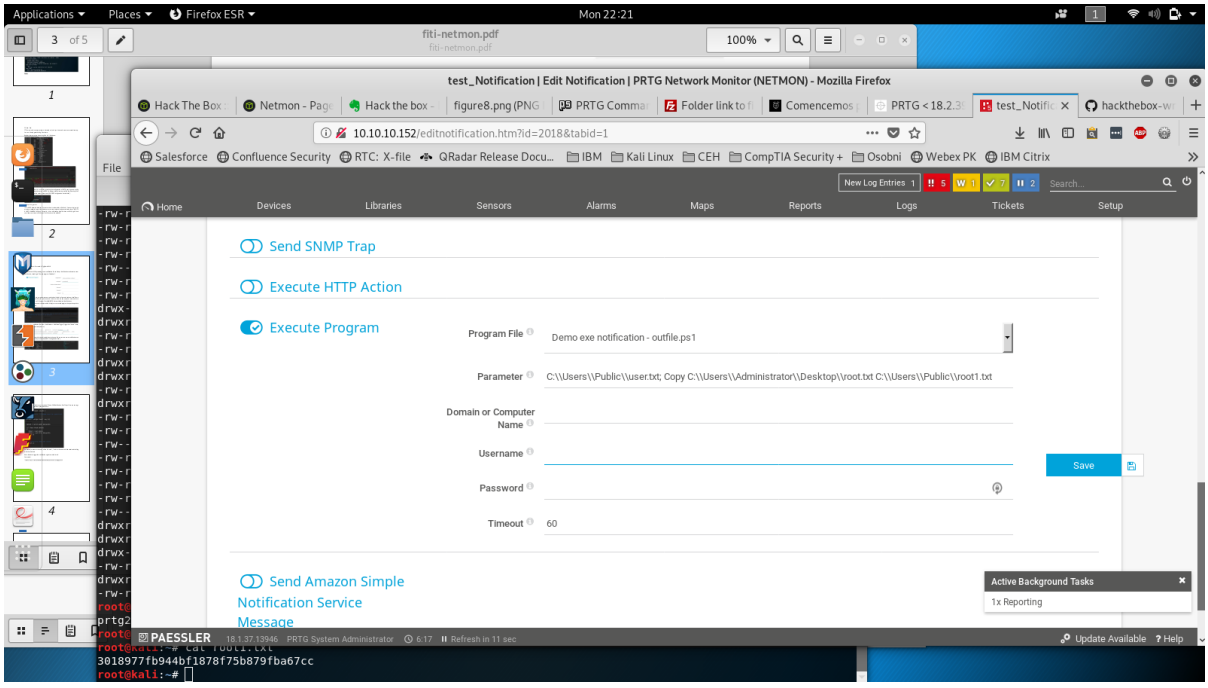
We can see that port 80 is opened, so navigate to the browser and go to http://10.10.10.152 . A login screen is shown:

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!**



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.

If this does not work, then your injection command is probably incorrect. You can check Logs menu for more information, if nothing happens !