LAB FILE REPORT

Final Record

for

CSE3502-Information Security Management

Submitted by

Aryaman Mishra-19BCE1027

To

Dr.Ayesha SK

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

April 2022

Table of contents

Content Page no.

LAB 1

Aryaman Mishra

19BCE1027

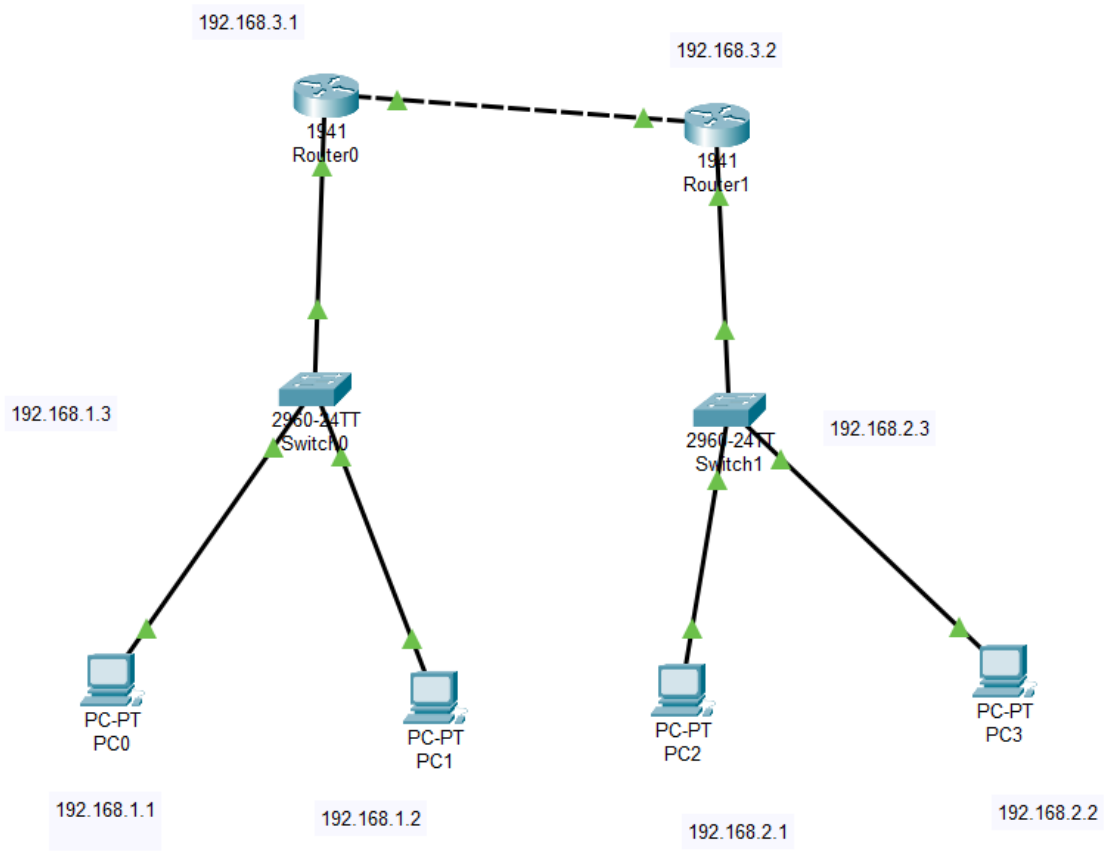
LAB 1

AIM: Create Topology in Cisco Packet Tracer and implement Static and RIP Protocol for Packet Transfer.

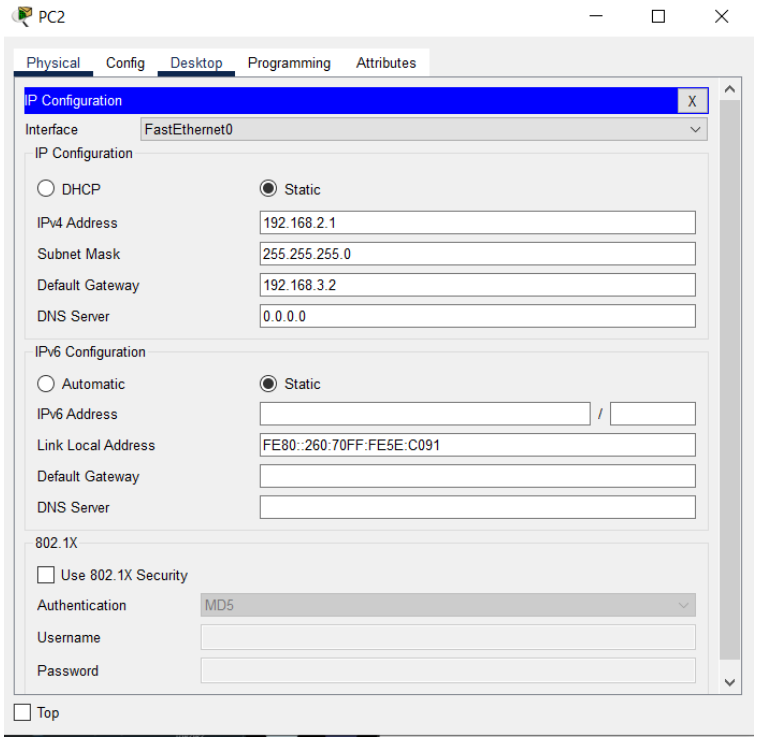
Tools Used:Cisco Packet Tracer.

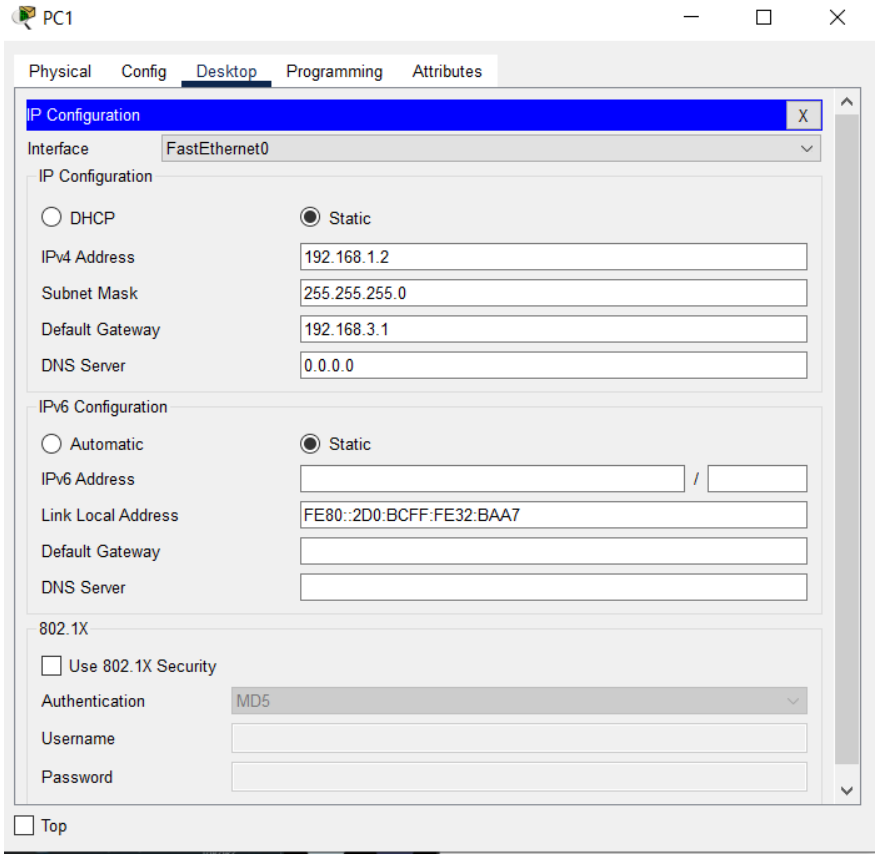
Experiment:

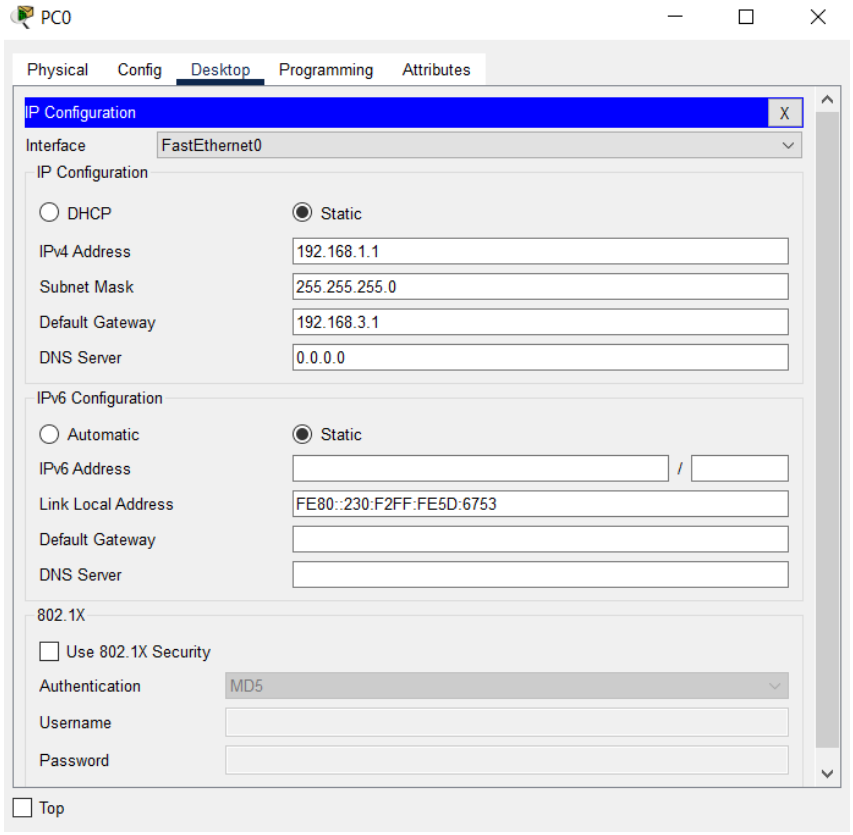
Create Topology.

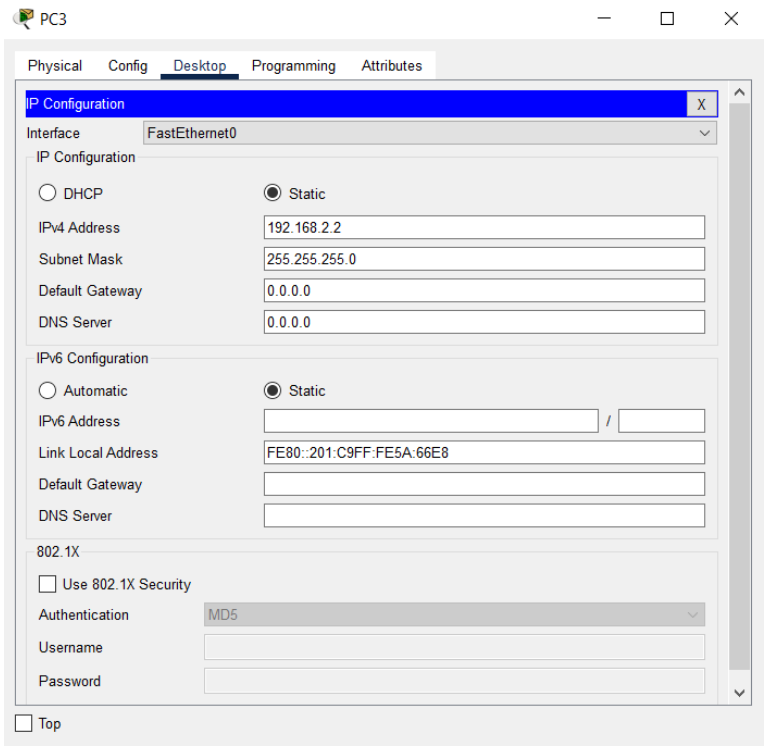


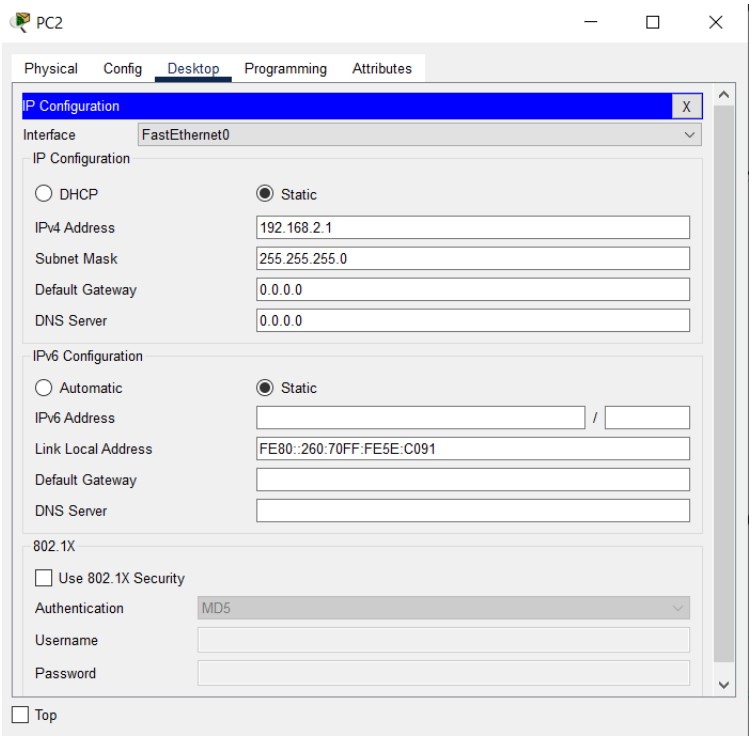
Configure IP Address and Default Gateway Configuration for the 4 PC Devices.

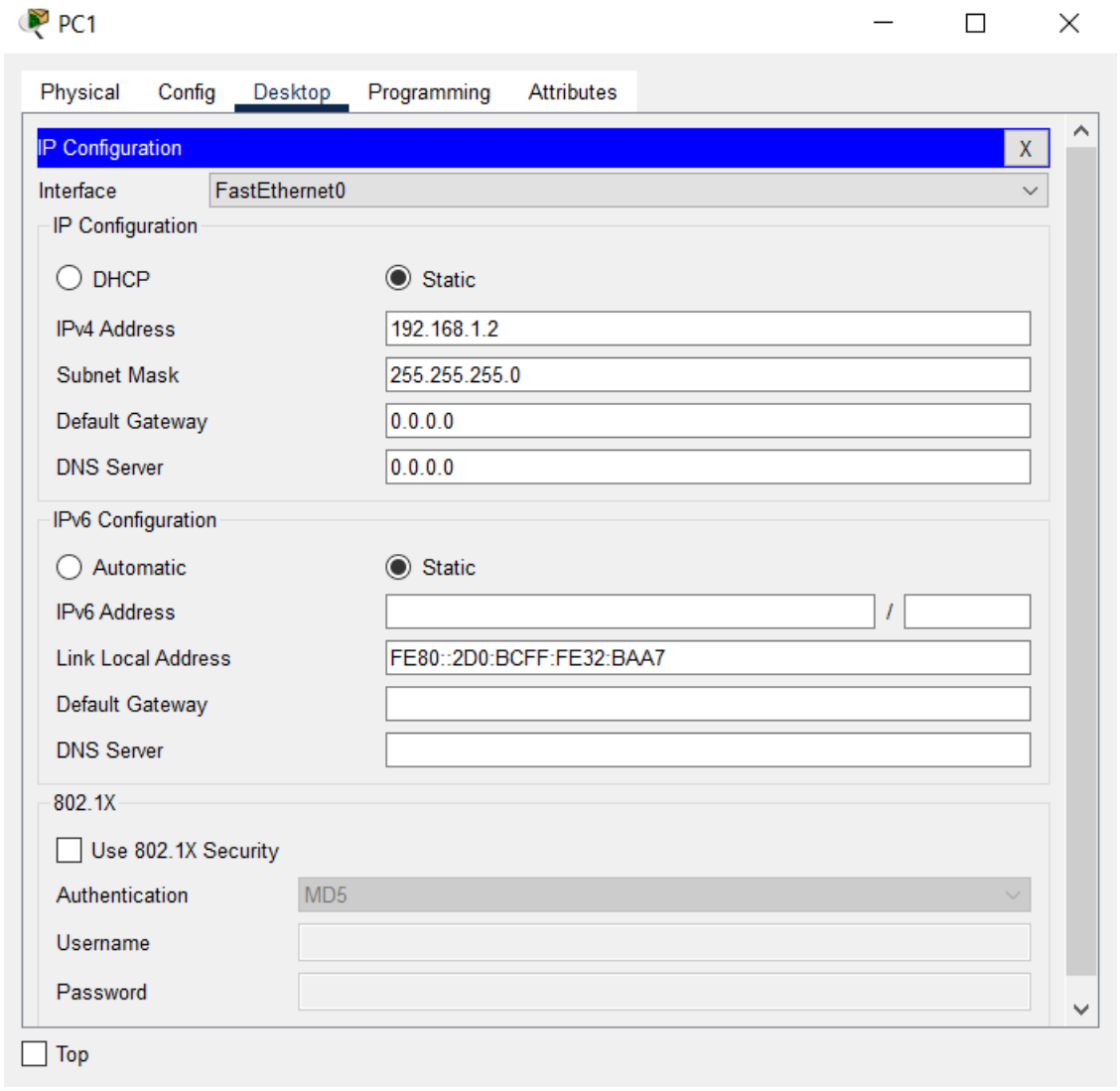

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.2
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:70FF:FE5E:C091
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

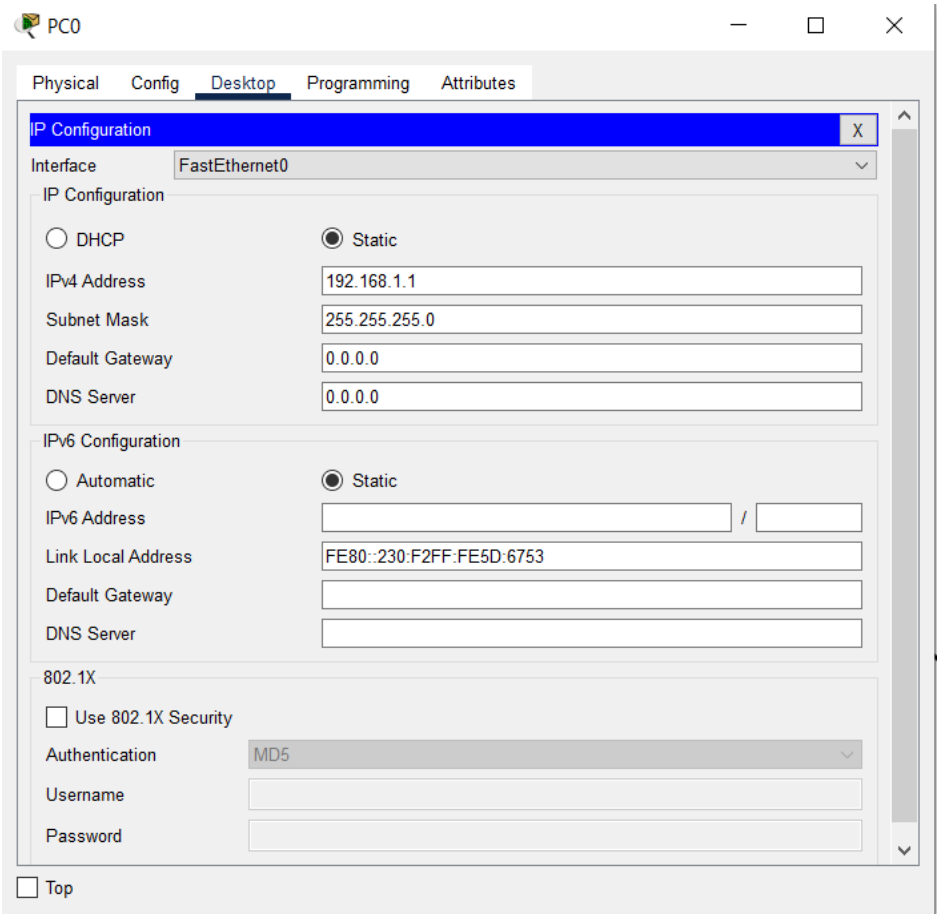

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE32:BAA7
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

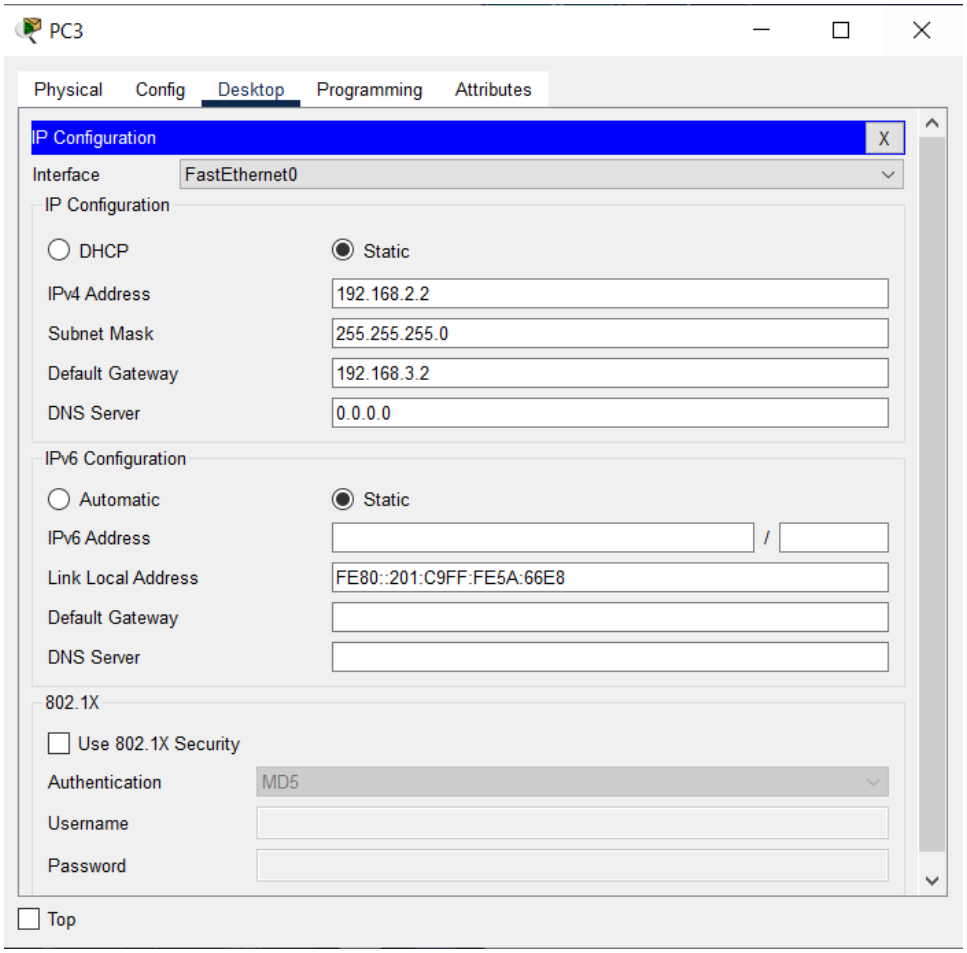

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::230:F2FF:FE5D:6753
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:C9FF:FE5A:66E8
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

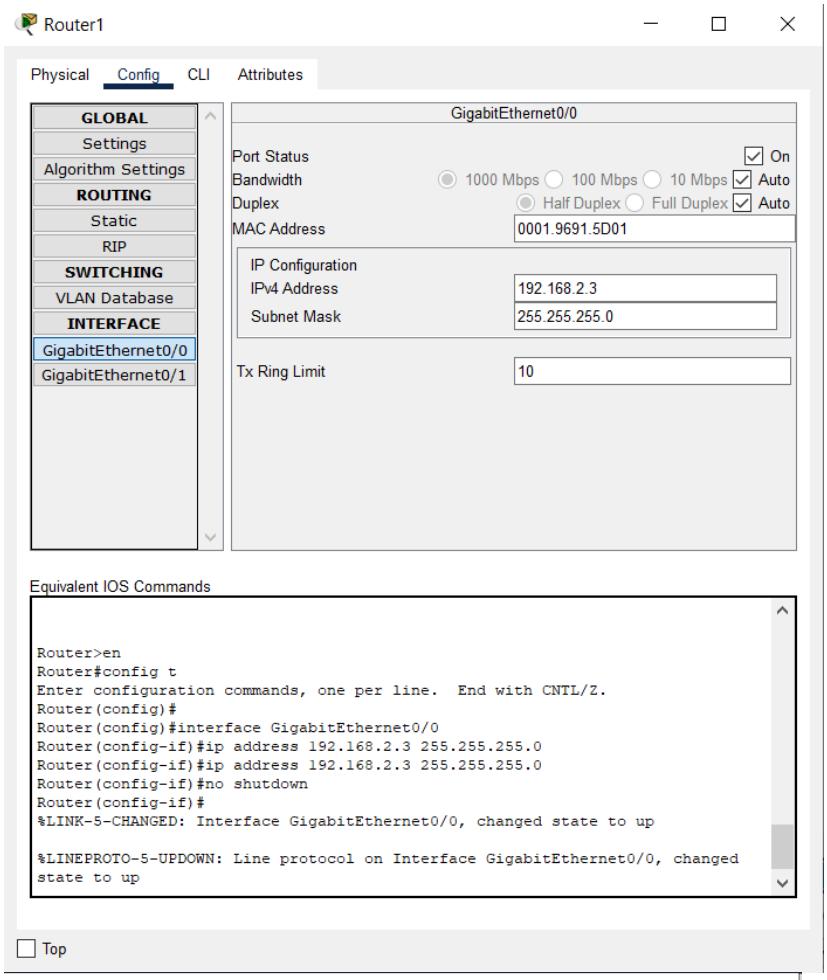

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:70FF:FE5E:C091
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

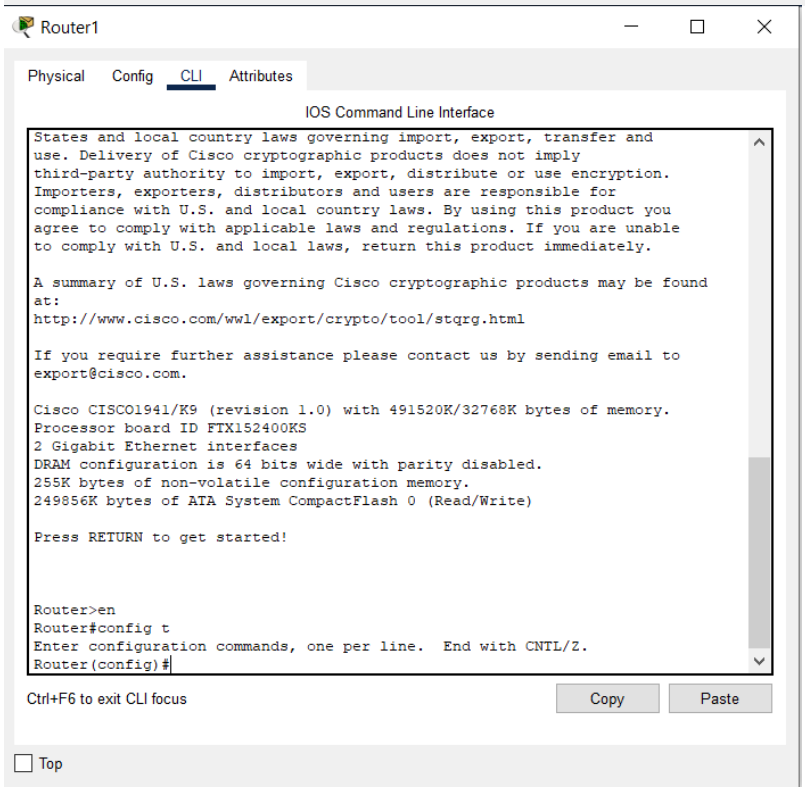

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE32:BAA7
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

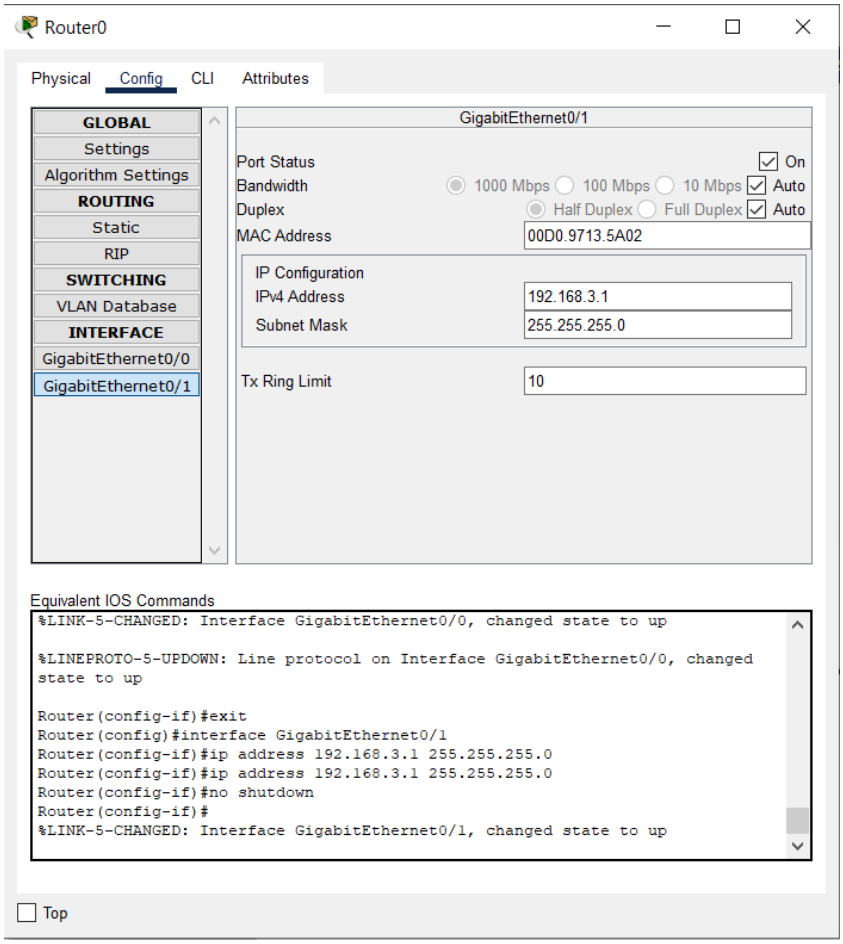

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::230:F2FF:FE5D:6753
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

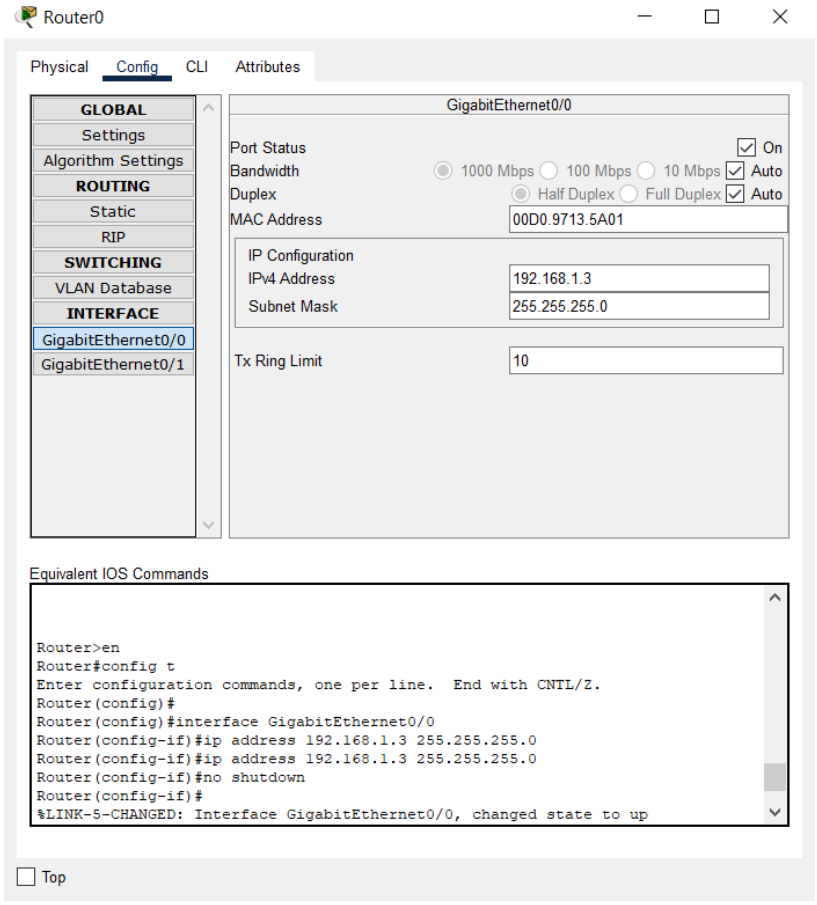


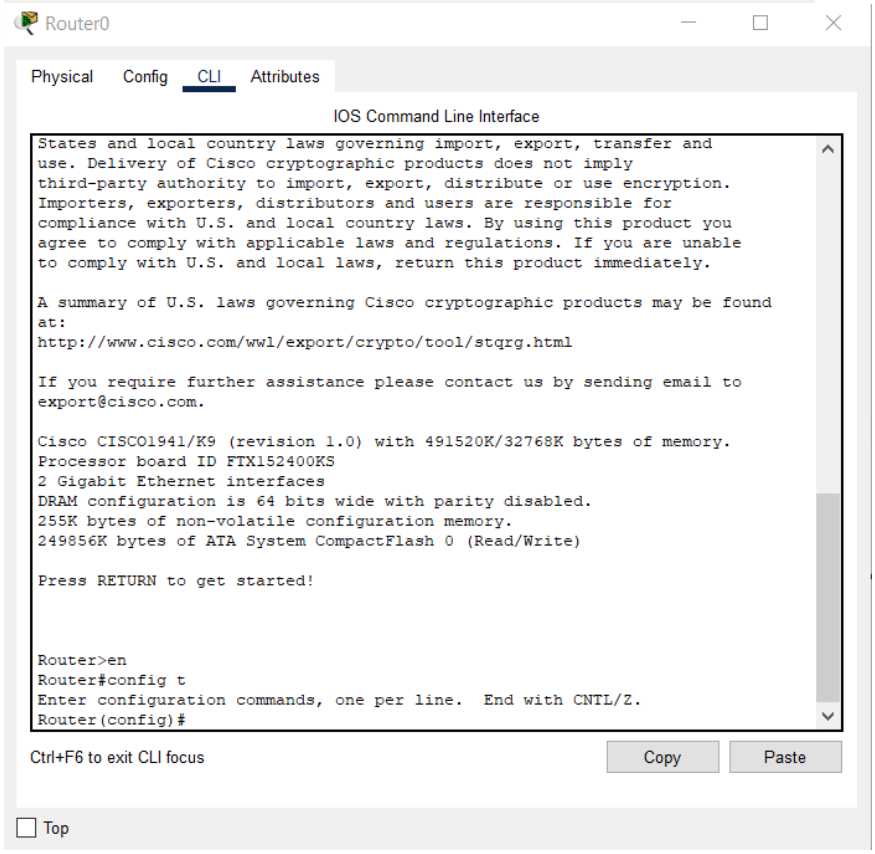
Assign IPv4 Address,Ports and Subnets of Routers.

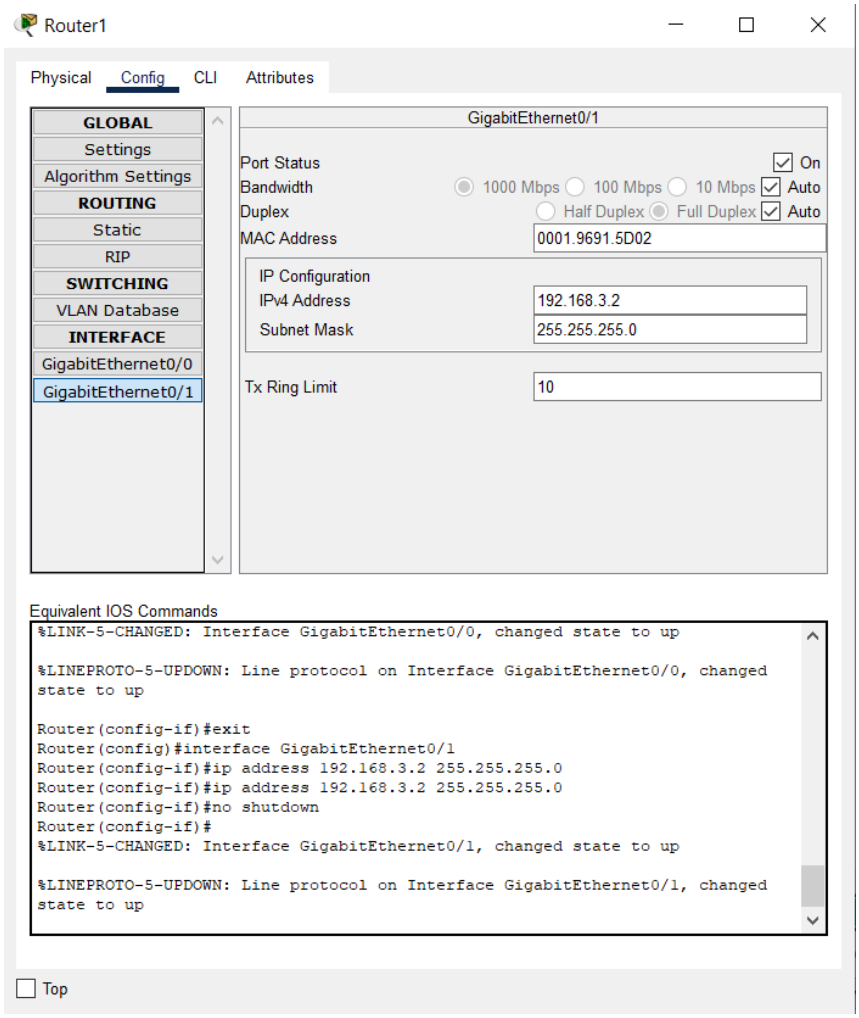

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.9691.5D01
IP Configuration
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.3 255.255.255.0
Router(config-if)#ip address 192.168.2.3 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Top


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

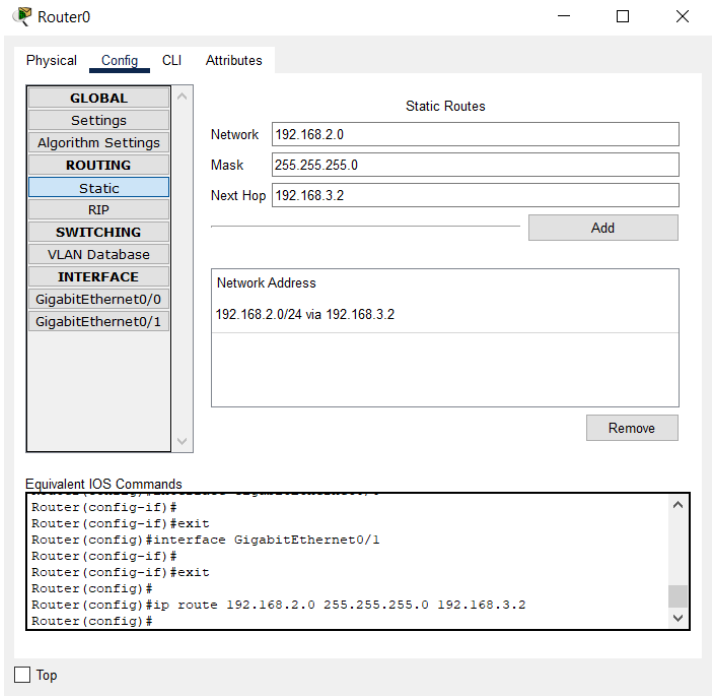

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.9713.5A02
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
Top

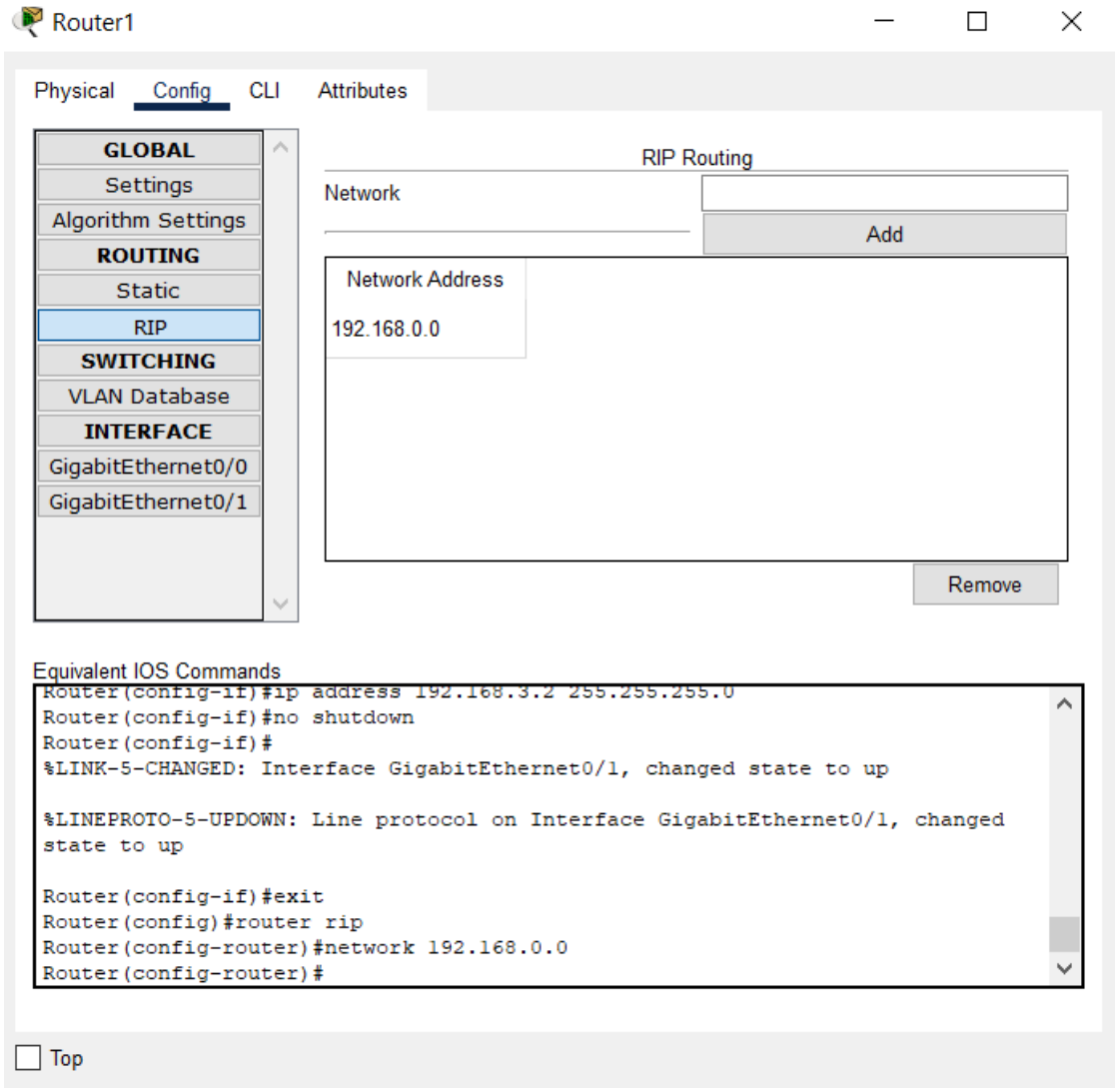

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.9713.5A01
IP Configuration
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.3 255.255.255.0
Router(config-if)#ip address 192.168.1.3 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
Top

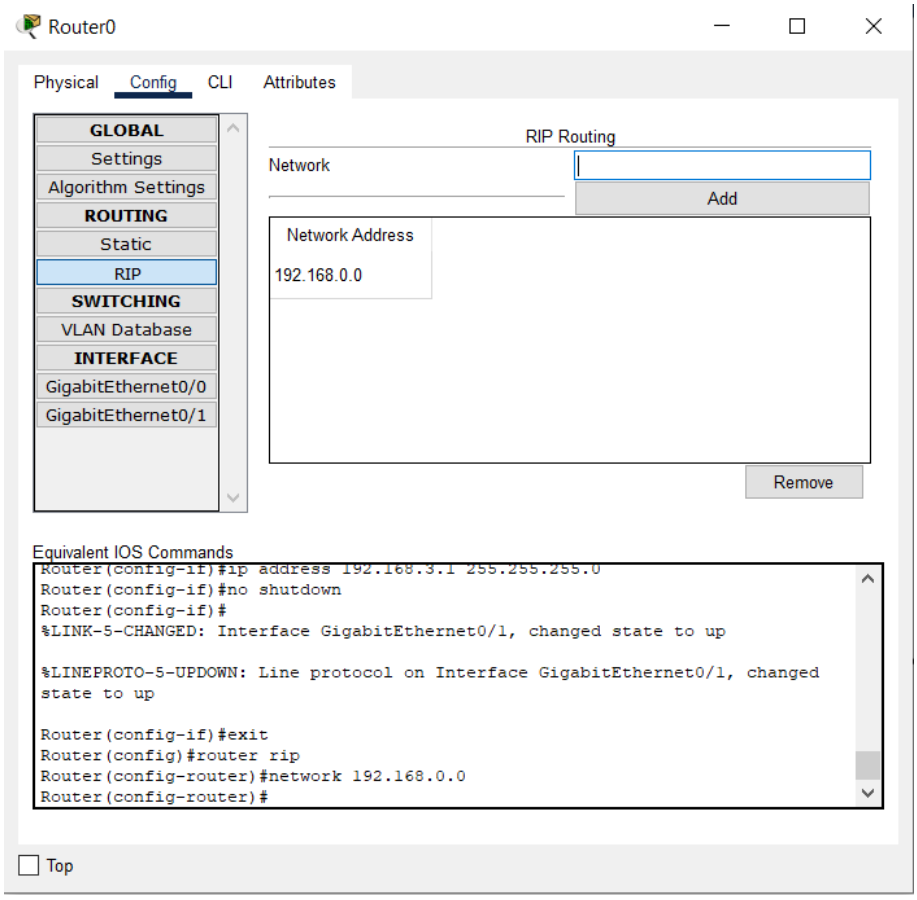

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

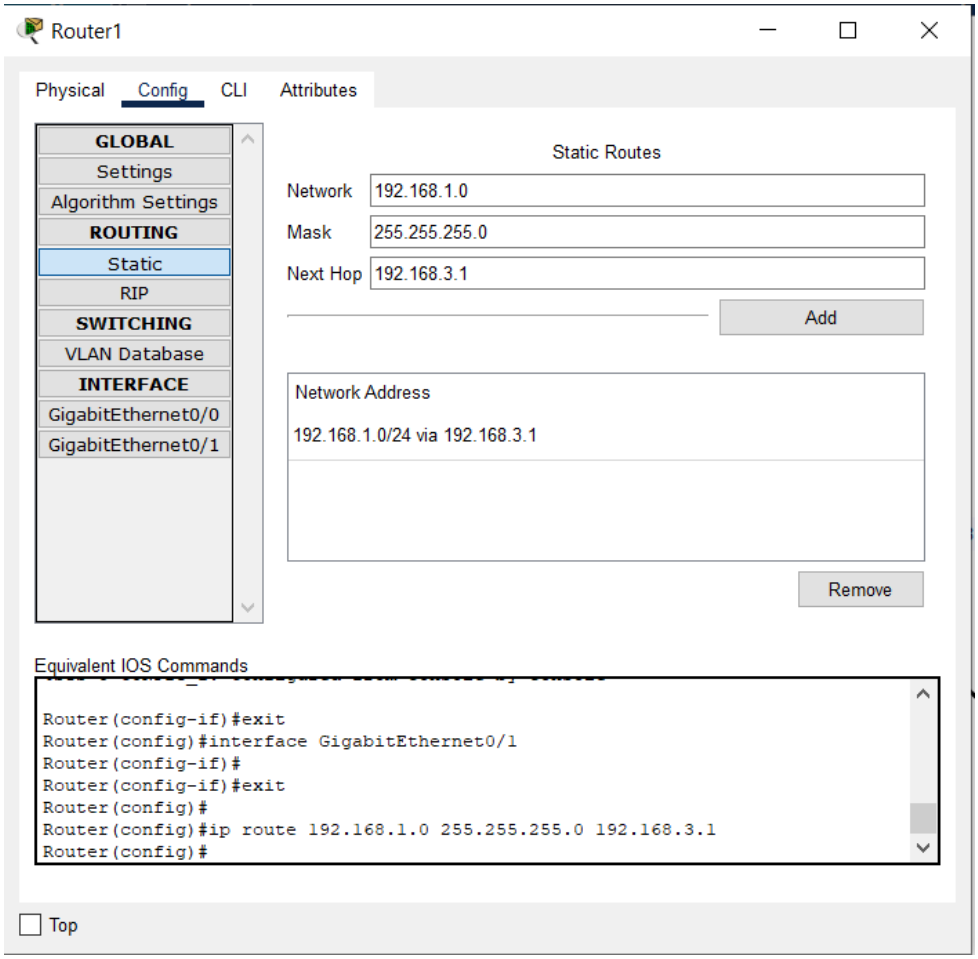


Assign Static and RIP routes for Router0 and Router1.


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Static Routes
Network 192.168.2.0
Mask 255.255.255.0
Next Hop 192.168.3.2
Add
Network Address
192.168.2.0/24 via 192.168.3.2
Remove
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
Router(config)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
RIP Routing
Network
Add
Network Address
192.168.0.0
Remove
Equivalent IOS Commands
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
RIP Routing
Network
Add
Network Address
192.168.0.0
Remove
Equivalent IOS Commands
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Static Routes
Network 192.168.1.0
Mask 255.255.255.0
Next Hop 192.168.3.1
Add
Network Address
192.168.1.0/24 via 192.168.3.1
Remove
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router(config)#
Top

Observation:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	Router0	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC0	Router1	ICMP		0.000	N	7	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	8	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	Router1	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC2	PC0	ICMP		0.000	N	5	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Router1	ICMP		0.000	N	2	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Router0	ICMP		0.000	N	9	(edit)	(delete)
	Successful	PC2	Router1	ICMP		0.000	N	10	(edit)	(delete)
	Successful	Router0	Router1	ICMP		0.000	N	11	(edit)	(delete)

Conclusion:Topology has been successfully created and executed.

LAB 2

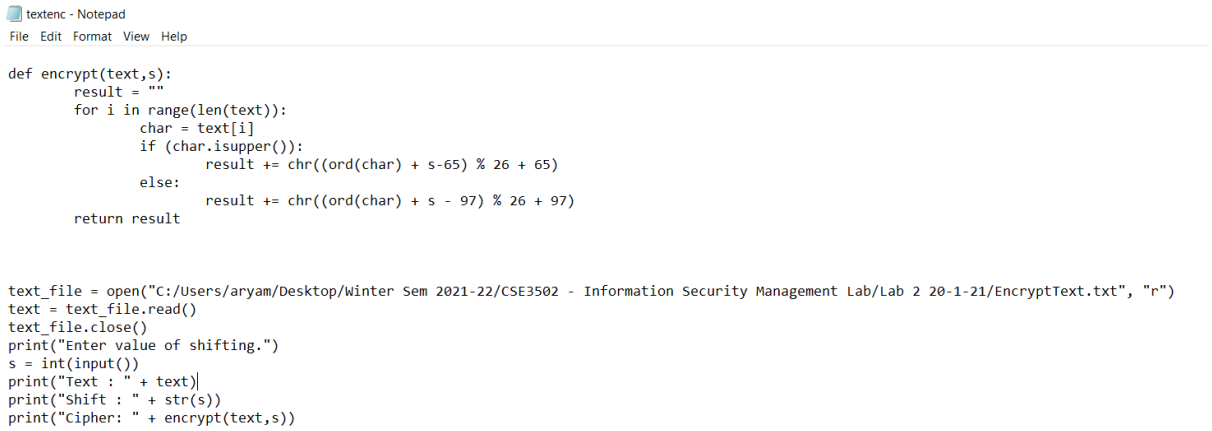
Aryaman Mishra

19BCE1027

Experiment 2

Aim: Implement caeser cipher encryption technique for a **text file** or audio file.

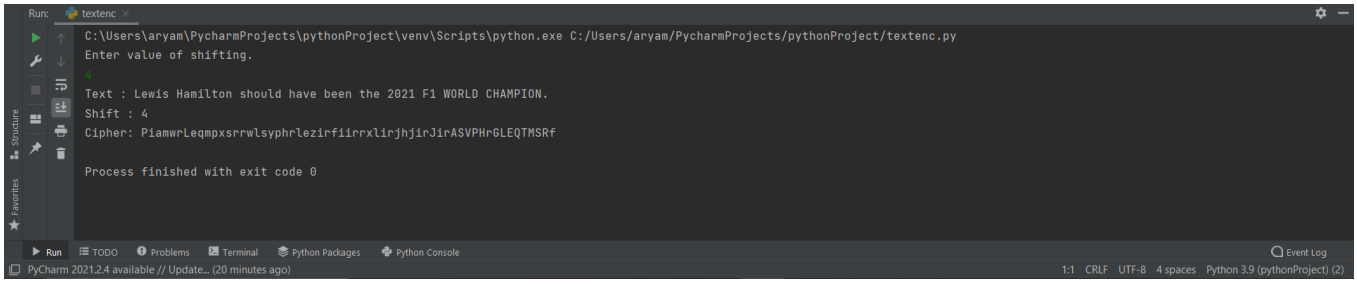
Code:




```
def encrypt(text,s):
        result = ""
        for i in range(len(text)):
                char = text[i]
                if (char.isupper()):
                        result += chr((ord(char) + s-65) % 26 + 65)
                else:
                        result += chr((ord(char) + s - 97) % 26 + 97)
        return result
```

```
text_file = open("C:/Users/aryam/Desktop/Winter Sem 2021-22/CSE3502 - Information Security Management Lab/Lab 2 20-1-21/EncryptText.txt", "r")

text = text_file.read()

text_file.close()

print("Enter value of shifting.")

s = int(input())

print("Text : " + text)

print("Shift : " + str(s))

print("Cipher: " + encrypt(text,s))
```

Output:



Conclusion:

Cipher for Text file has been successfully implemented for a text file and output for text file containing "Lewis Hamilton should have been the 2021 WORLD CHAMPION" is denoted in output screenshot.

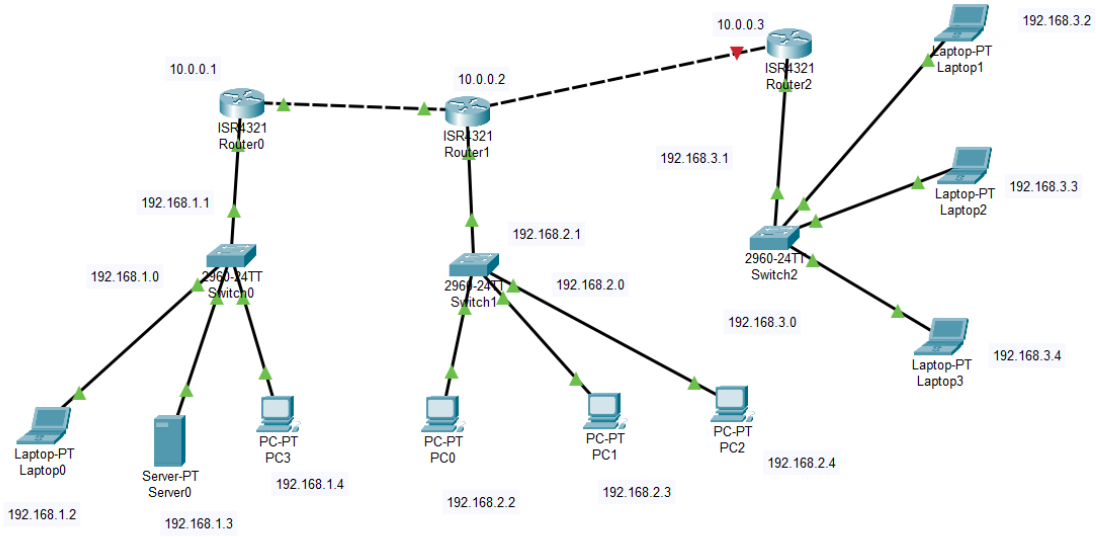
LAB 3

Aryaman Mishra

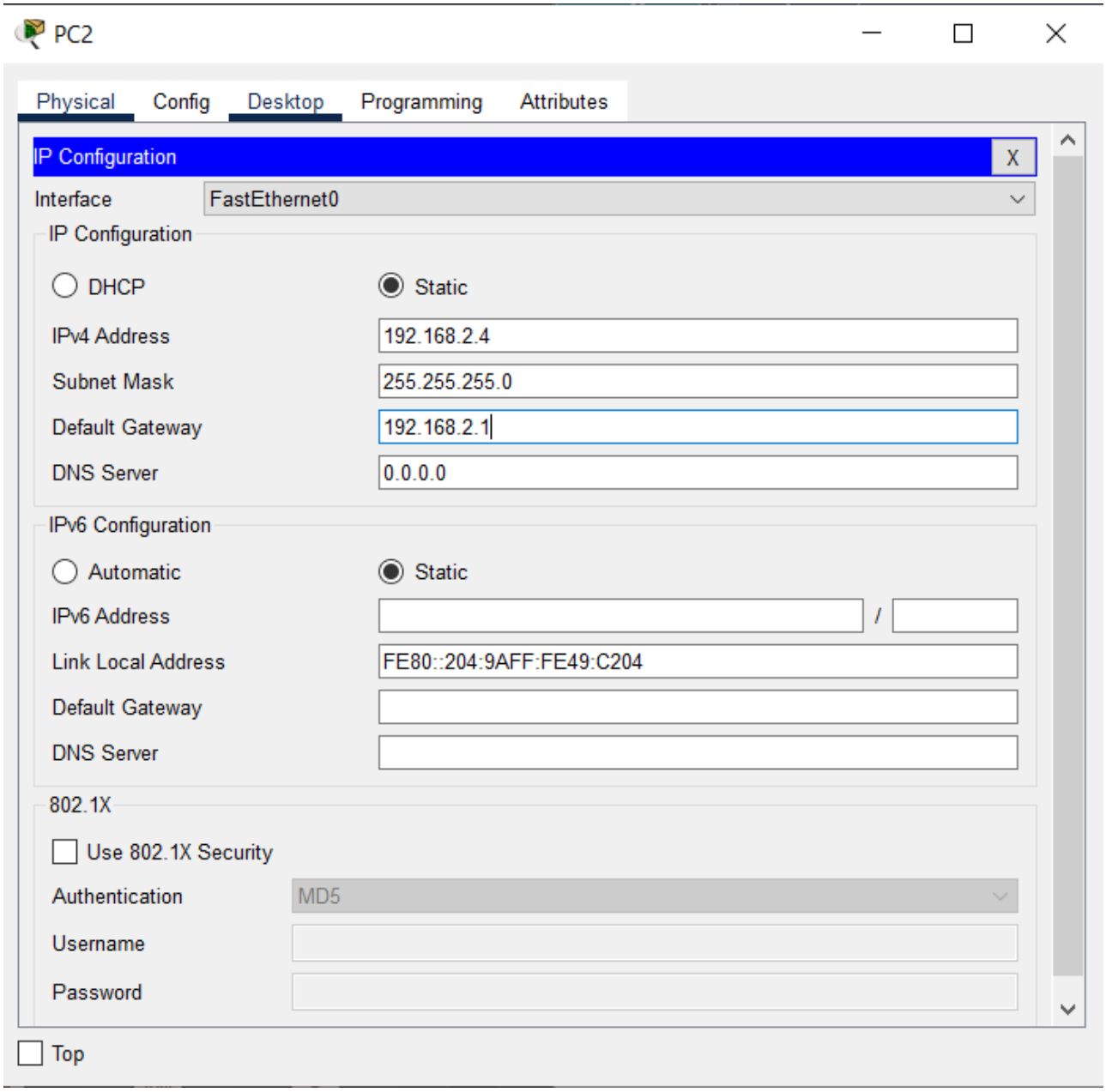
19BCE1027

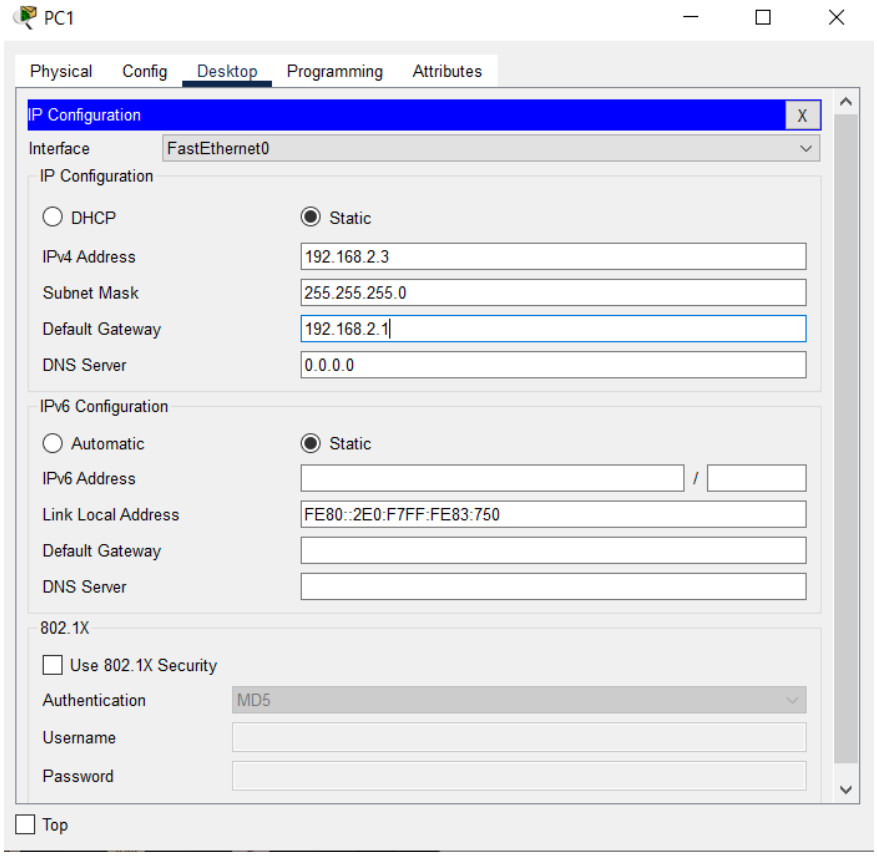
EXPERIMENT 3:ACCESS CONTROL LISTS

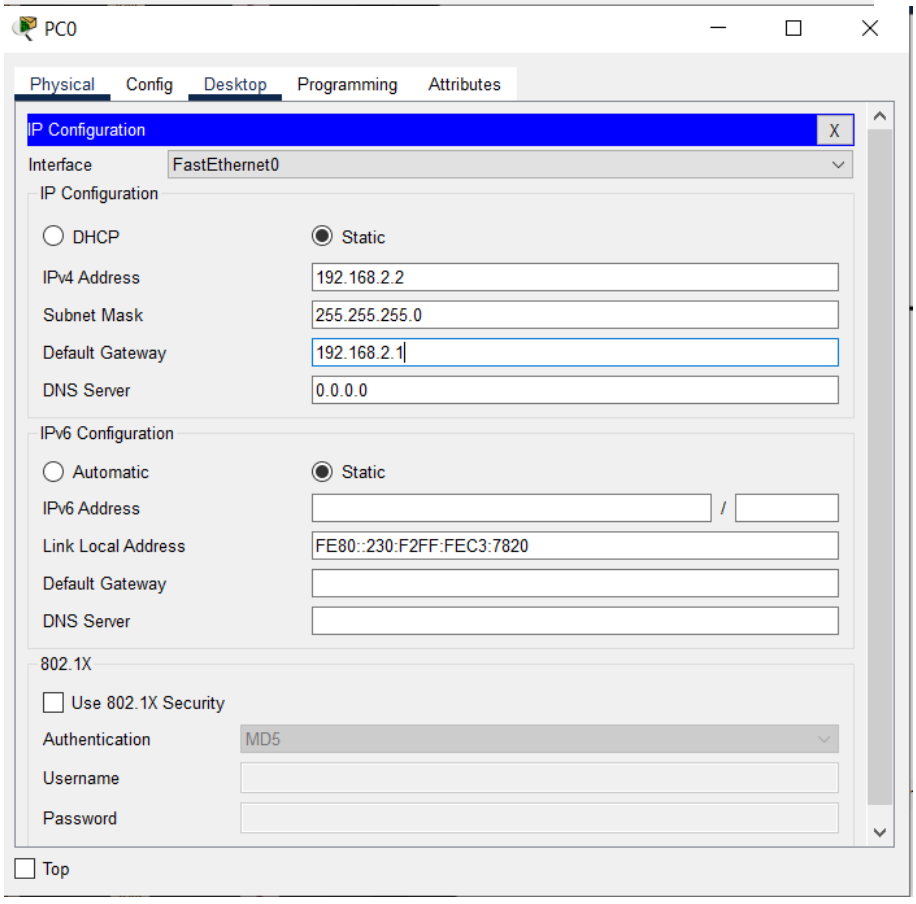
Topology

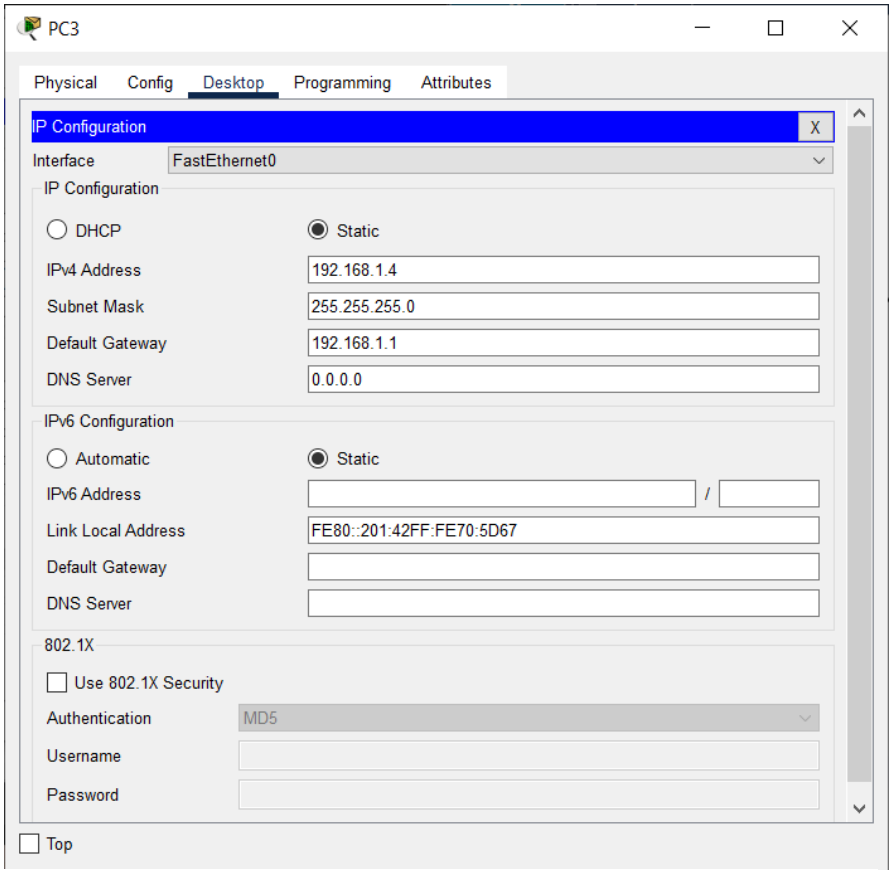


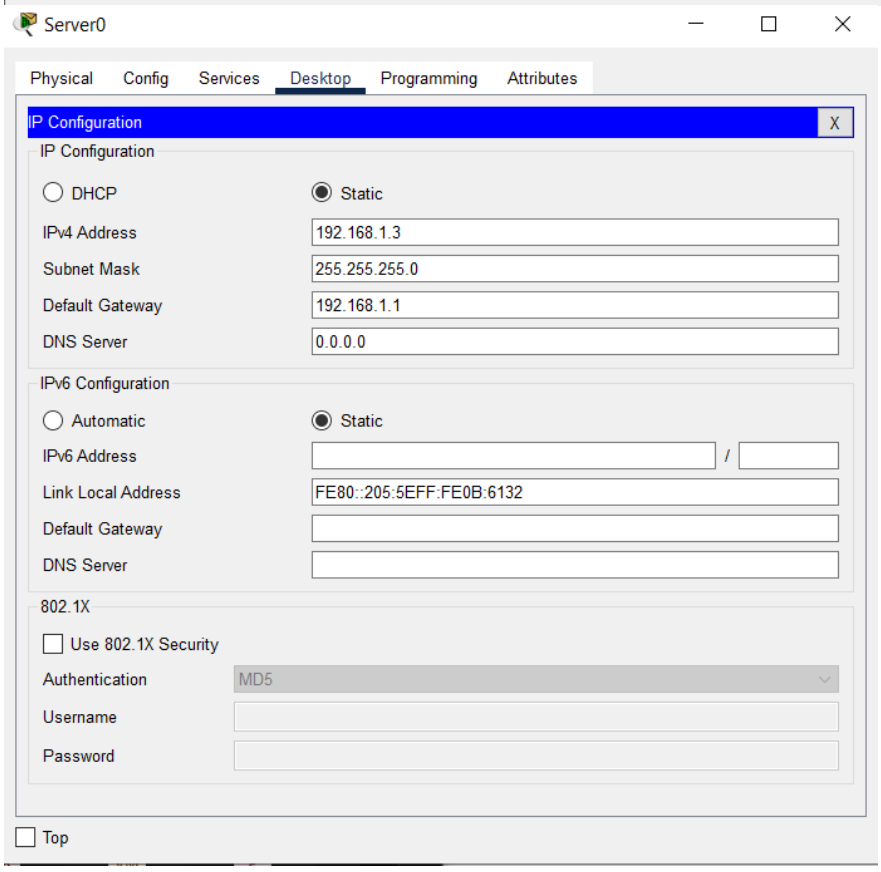
System Configurations

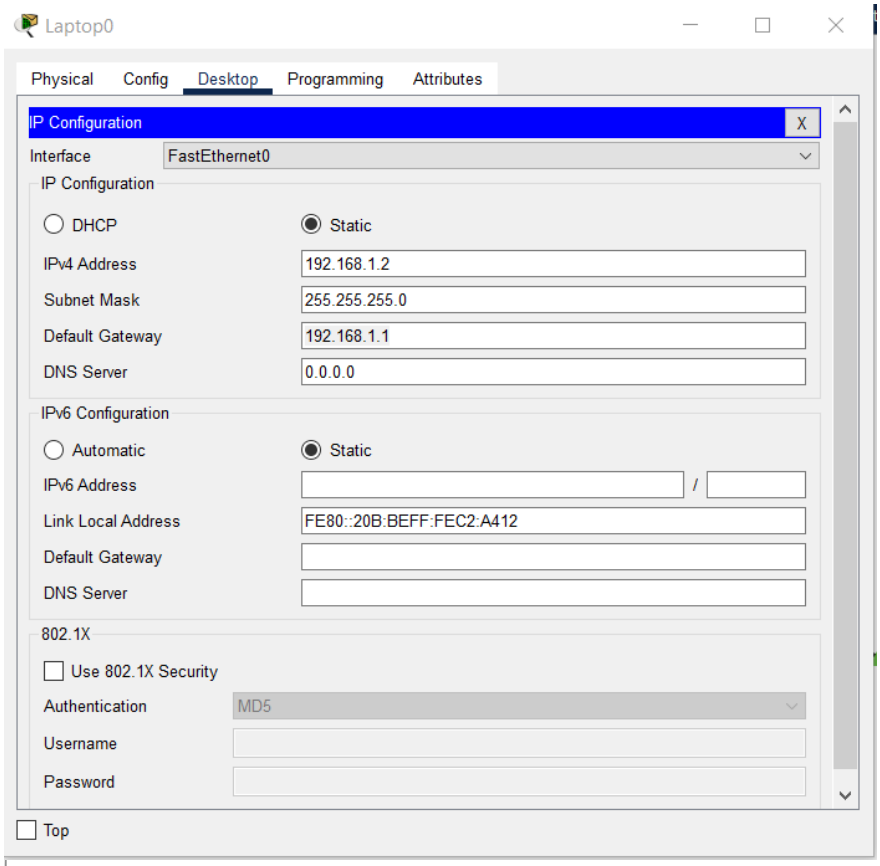


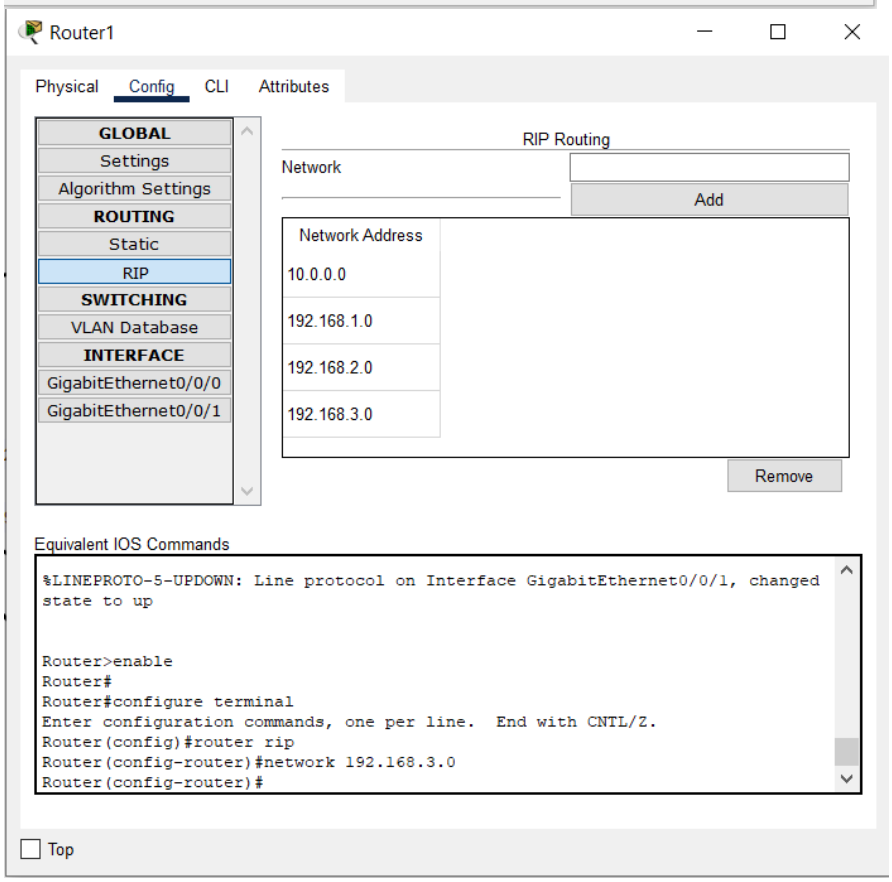

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:F7FF:FE83:750
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

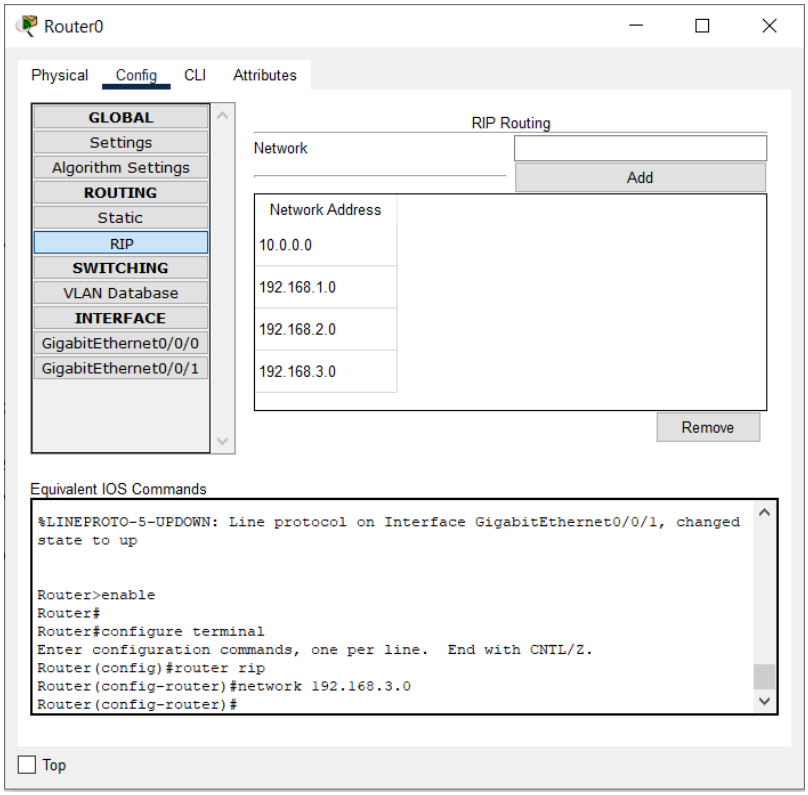

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::230:F2FF:FEC3:7820
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

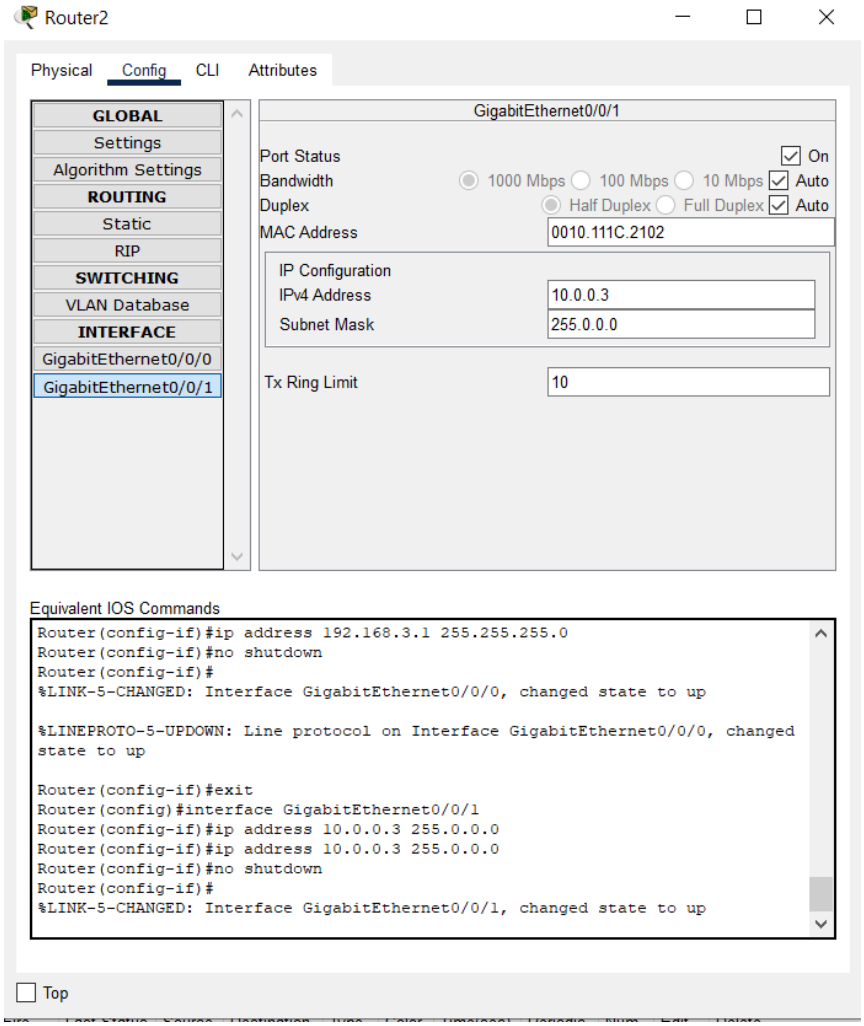

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:42FF:FE70:5D67
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

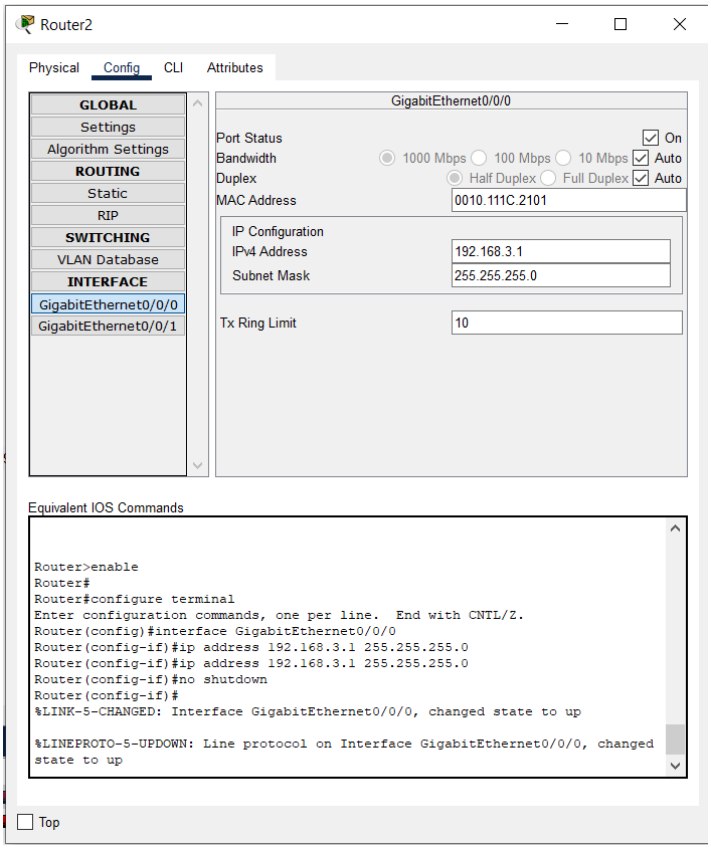

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::205:5EFF:FE0B:6132
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

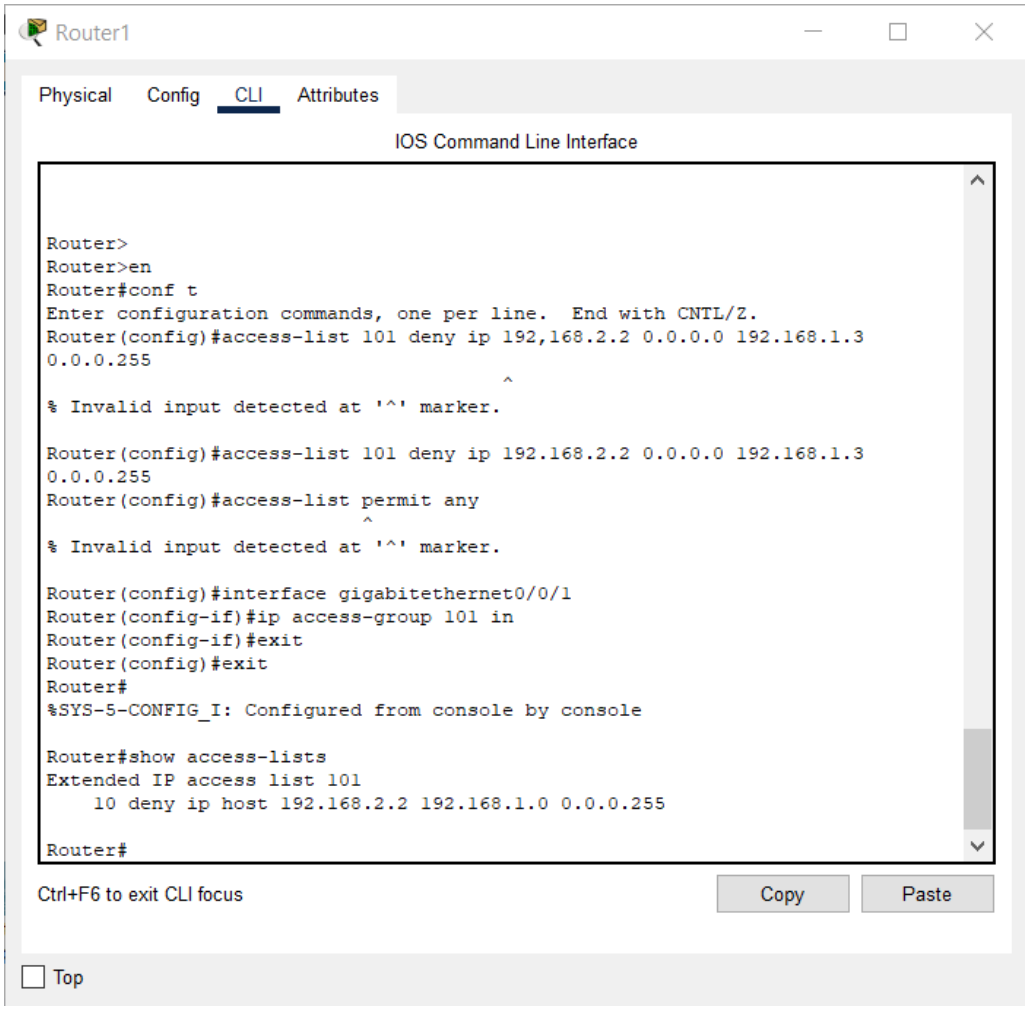

Laptop0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20B:BEFF:FEC2:A412
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

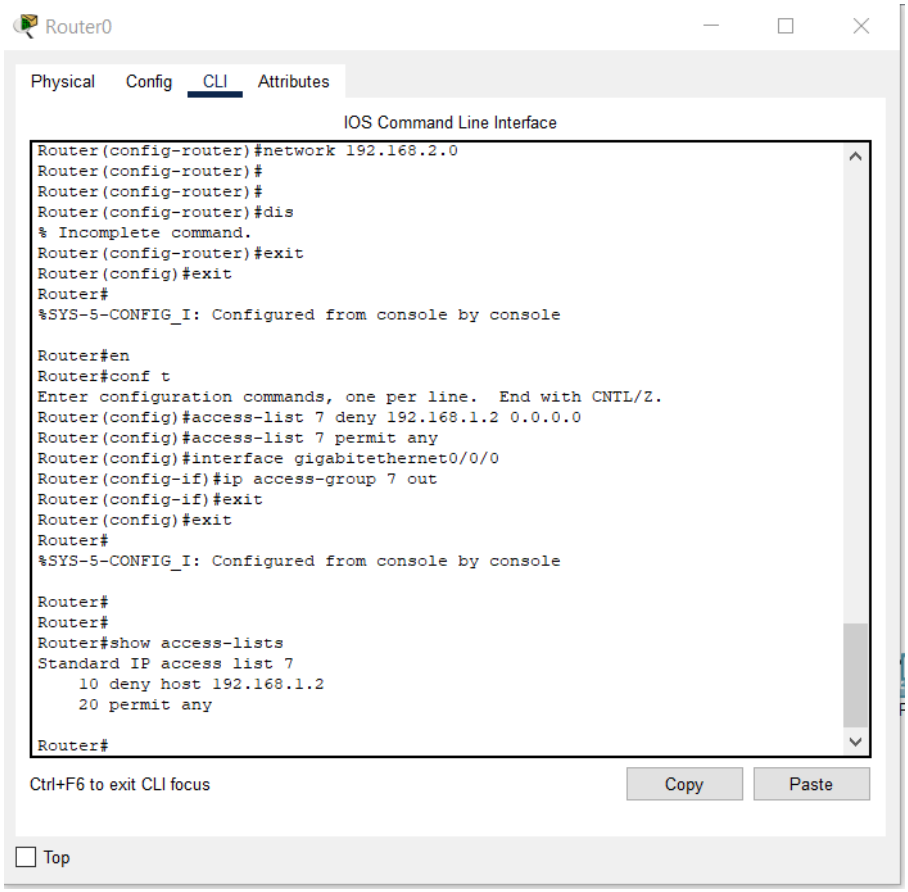

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
RIP Routing
Network
Add
Network Address
10.0.0.0
192.168.1.0
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#
Top

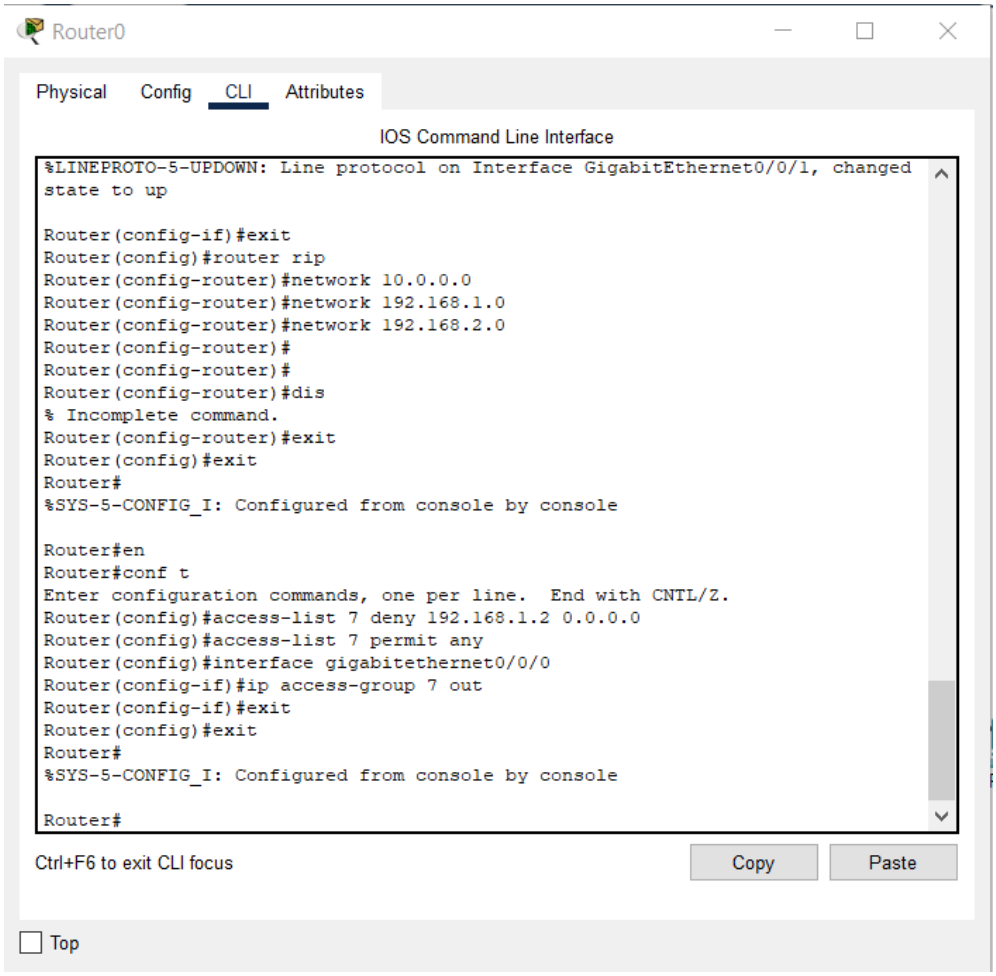

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
RIP Routing
Network
Add
Network Address
10.0.0.0
192.168.1.0
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#
Top

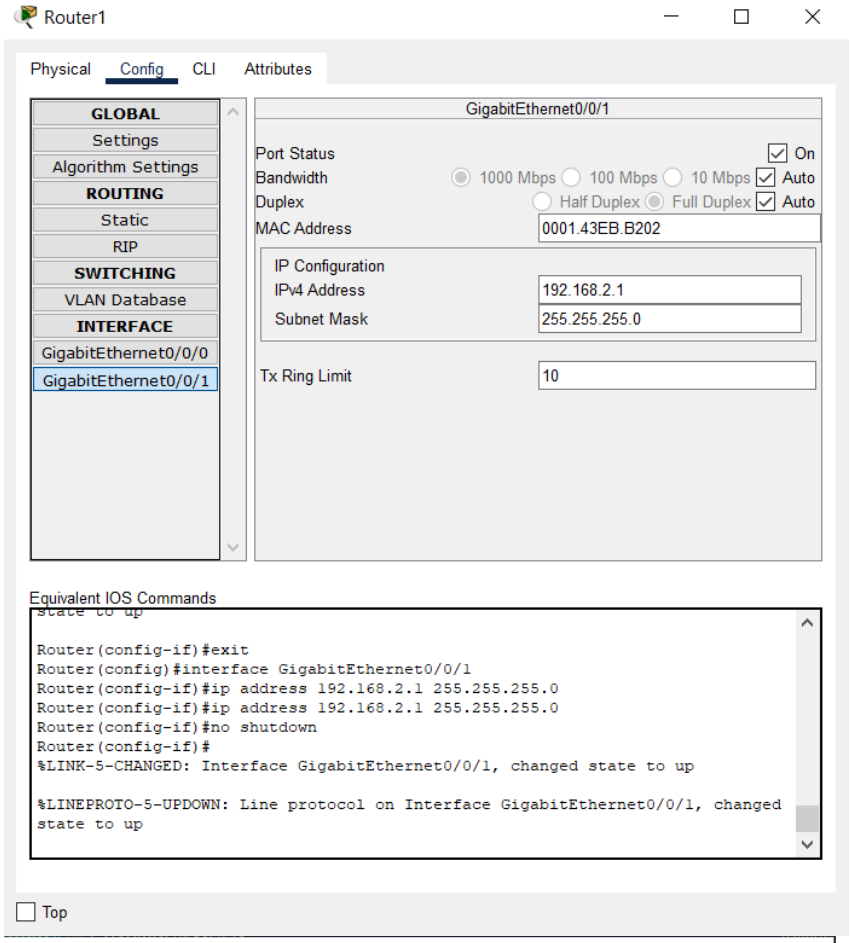

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0010.111C.2102
IP Configuration
IPv4 Address
10.0.0.3
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 10.0.0.3 255.0.0.0
Router(config-if)#ip address 10.0.0.3 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
Top

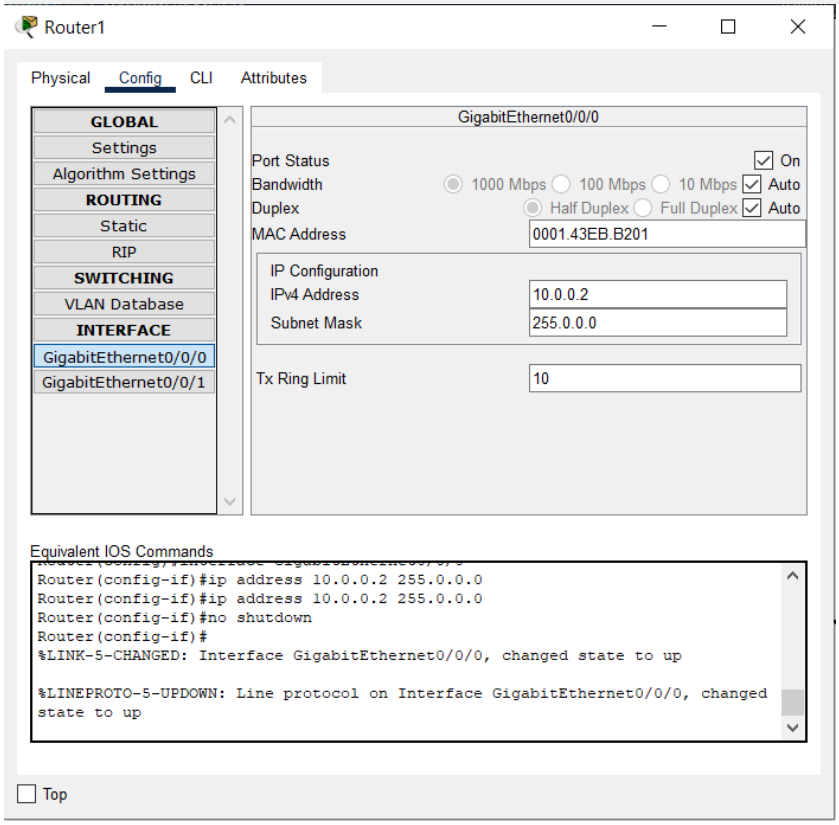

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0010.111C.2101
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Top

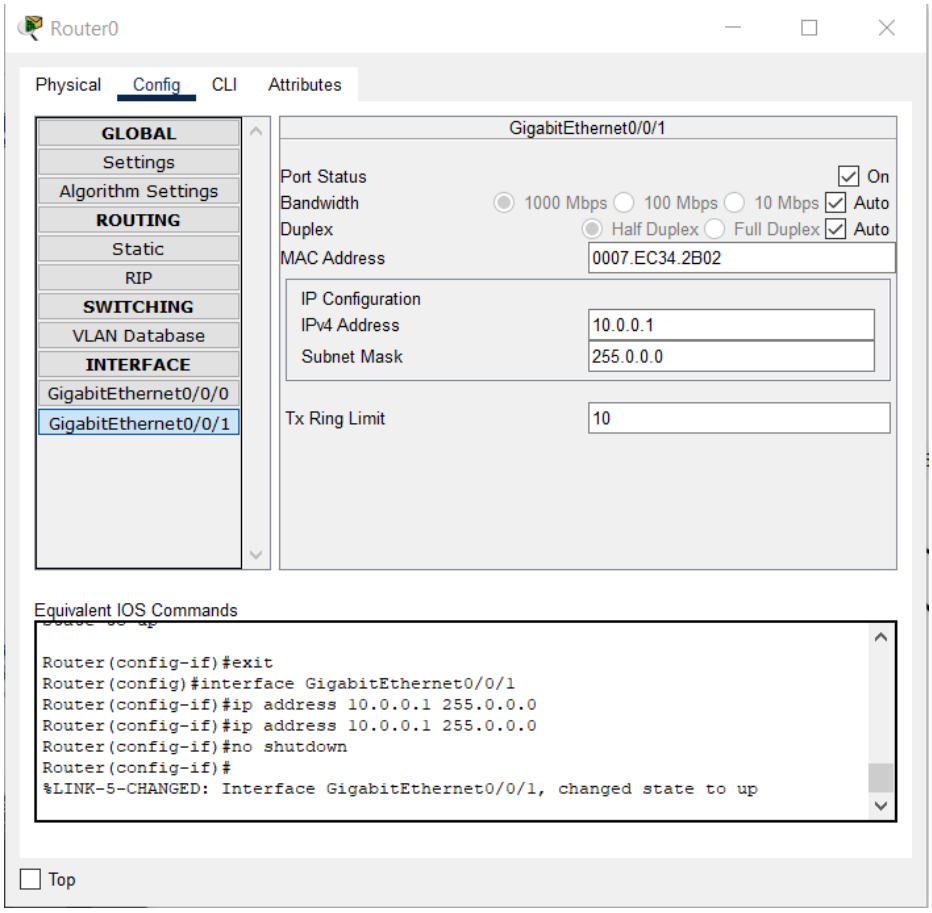

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 101 deny ip 192,168.2.2 0.0.0.0 192.168.1.3
0.0.0.255
^
% Invalid input detected at '^' marker.
Router(config)#access-list 101 deny ip 192.168.2.2 0.0.0.0 192.168.1.3
0.0.0.255
Router(config)#access-list permit any
^
% Invalid input detected at '^' marker.
Router(config)#interface gigabitethernet0/0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show access-lists
Extended IP access list 101
10 deny ip host 192.168.2.2 192.168.1.0 0.0.0.255
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

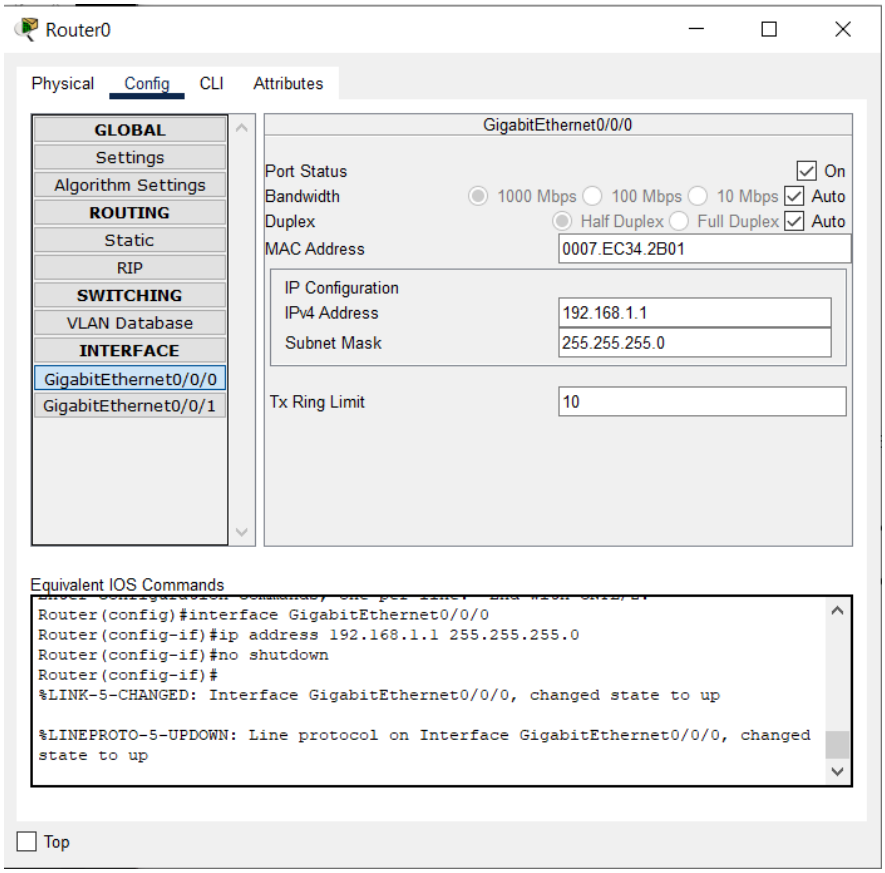

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#
Router(config-router)#dis
% Incomplete command.
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 7 deny 192.168.1.2 0.0.0.0
Router(config)#access-list 7 permit any
Router(config)#interface gigabitethernet0/0/0
Router(config-if)#ip access-group 7 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#
Router#show access-lists
Standard IP access list 7
10 deny host 192.168.1.2
20 permit any
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

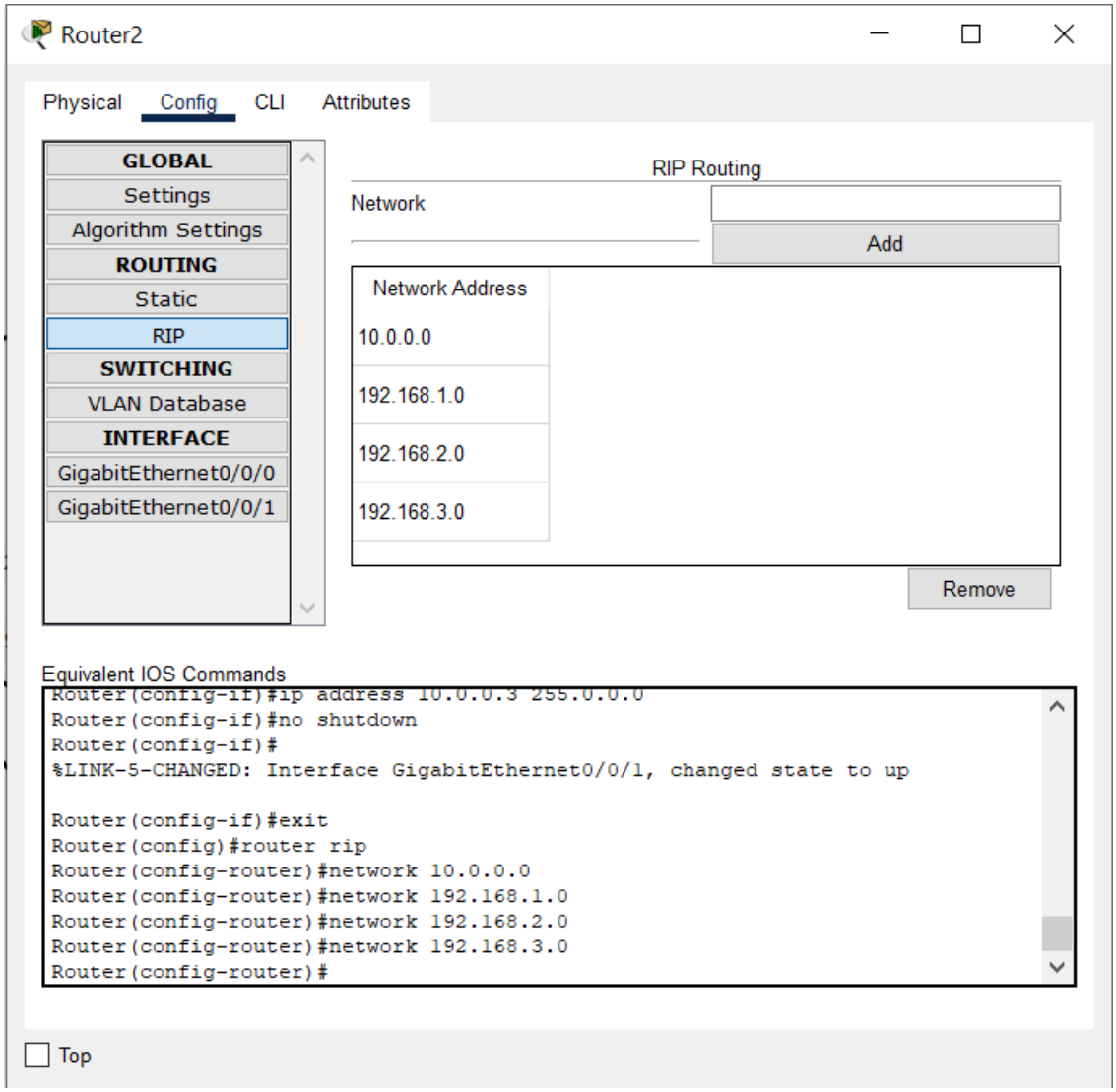

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#
Router(config-router)#dis
% Incomplete command.
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 7 deny 192.168.1.2 0.0.0.0
Router(config)#access-list 7 permit any
Router(config)#interface gigabitethernet0/0/0
Router(config-if)#ip access-group 7 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.43EB.B202
IP Configuration
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.43EB.B201
IP Configuration
IPv4 Address
10.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0007.EC34.2B02
IP Configuration
IPv4 Address
10.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
Top

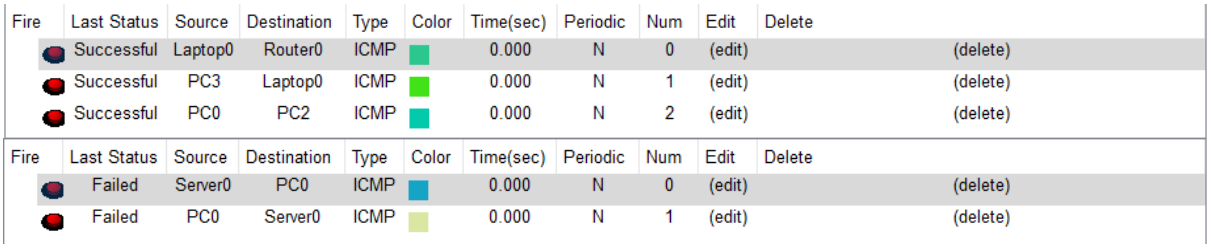

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0007.EC34.2B01
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Top



Results:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	PC3	ICMP		0.000	N	8	(edit)	(delete)
	Successful	Server0	Laptop0	ICMP		0.000	N	9	(edit)	(delete)
	Successful	PC3	Laptop0	ICMP		0.000	N	10	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC1	Laptop0	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC3	Laptop0	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Laptop0	PC3	ICMP		0.000	N	8	(edit)	(delete)
	Failed	PC0	Laptop0	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Server0	Router0	ICMP		0.000	N	3	(edit)	(delete)
	Successful	Laptop0	Router0	ICMP		0.000	N	4	(edit)	(delete)



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Router0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	Laptop0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC2	ICMP		0.000	N	2	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Server0	PC0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC0	Server0	ICMP		0.000	N	1	(edit)	(delete)

Inference:

Access Control Lists (ACL) are used to filter network traffic on Cisco routers. In order to filter network traffic, ACLs control if routed packets have to be forwarded or blocked at the ingress or egress router interface. The router checks each packet to determine whether to forward or drop the packet based on the criteria specified in the ACL applied to the interface.

IP ACL types

Two types of IP ACL can be configured in Cisco Packet Tracer 7.2 :

- Standard ACLs : This is the oldest ACL type which can be configured on Cisco routers. Traffic is filtered based on the source IP address of IP packets. The access-list number can be any number from 1 to 99. This kind of ACL has to be placed near the destination to avoid blocking legitimate trafic from the source.

```
access-list 1 permit 10.2.25.0 0.0.0.255
access-list 1 deny any
```

- Extended ACLs : Introduced in IOS version 8.3, the extended ACLs are more complex and allow filtering of the IP traffic based on a combination of multiple criterias : source IP address, destination IP address, TCP or UDP port, protocol, ... In numbered ACLs, the access-list number can be any number from 100 to 199 or 2000 to 2699 (available in IOS versions >12.0.1). Such ACLs can also be named access lists in which the ACL number is replaced by a keyword. This kind of ACL has to be placed near the source as it allows fine grained control to ressources accessed. Placing the ACL near the destination will make the trafic travel through the network before beeing blocked, resulting in bandwidth waste.

```
access-list 1 permit ip 10.2.25.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 101 permit icmp any 10.1.0.0 0.0.255.255 echo
access-list 1 deny ip any any
```

A wildcard mask is a mask of bits that indicates which parts of an IP address are available for examination. In the Cisco IOS, they are used in several places, for example:

- To indicate the size of a network or subnet for some routing protocols, such as OSPF.
- To indicate what IP addresses should be permitted or denied in access control lists (ACLs).

A wildcard mask can be thought of as an inverted subnet mask. For example, a subnet mask of 255.255.255.0 (binary equivalent = 11111111.11111111.11111111.00000000) inverts to a wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111).

A wild card mask is a matching rule.[2] The rule for a wildcard mask is:

- 0 means that the equivalent bit must match
- 1 means that the equivalent bit does not matter

Any wildcard bit-pattern can be masked for examination. For example, a wildcard mask of 0.0.0.254 (binary equivalent = 00000000.00000000.00000000.11111110) applied to IP address 10.10.10.2 (00001010.00001010.00001010.00000010) will match even-numbered IP addresses 10.10.10.0, 10.10.10.2, 10.10.10.4, 10.10.10.6 etc. Same mask applied to 10.10.10.1 (00001010.00001010.00001010.00000001) will match odd-numbered IP addresses 10.10.10.1, 10.10.10.3, 10.10.10.5 etc.

A network and wildcard mask combination of 1.1.1.1 0.0.0.0 would match an interface configured exactly with 1.1.1.1 only, and nothing else.

Wildcard masks are used in situations where subnet masks may not apply. For example, when two affected hosts fall in different subnets, the use of a wildcard mask will group them together.

CONCLUSION:

ACCESS CONTROL LOSTS HAVE BEEN SUCCESFULLY IMPLEMENTED IN CISCO PACKET TRACER.

LAB 4

Aryaman Mishra

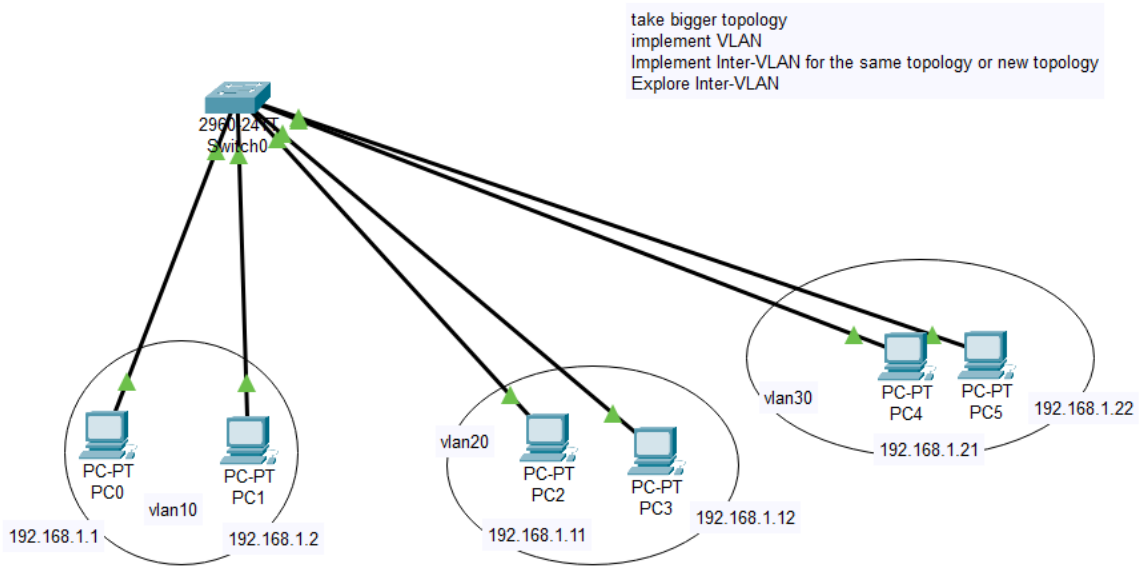
19BCE1027

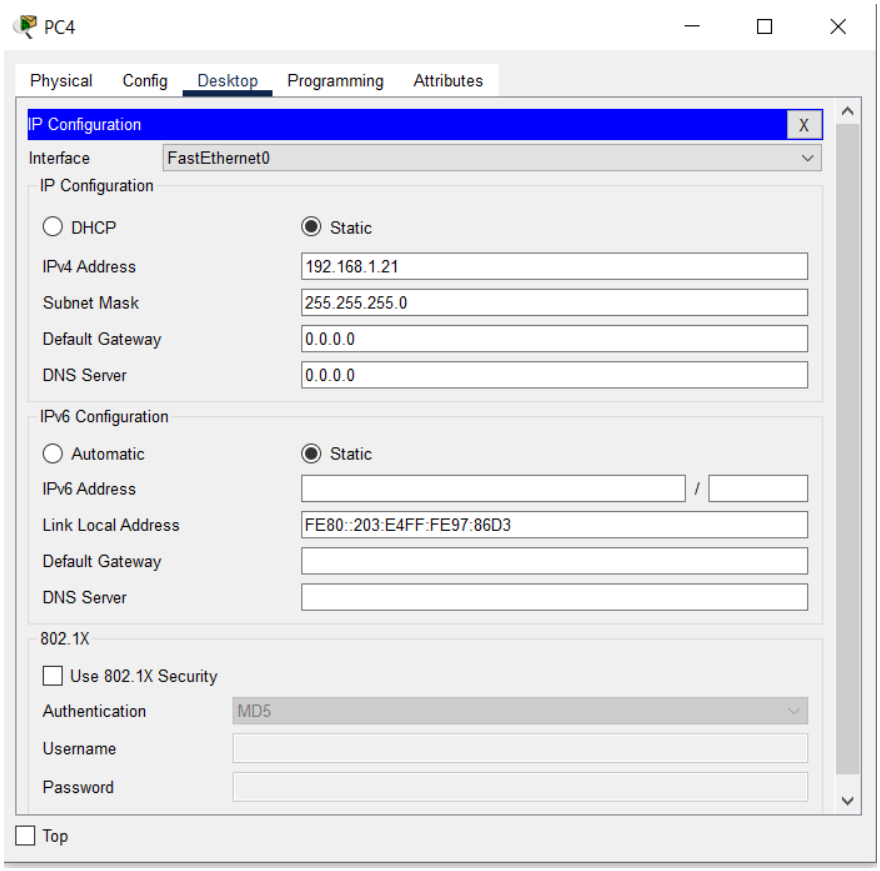
EXPERIMENT 4:VLANS AND INTER-VLANS(Class and Post-Lab Topology Included)

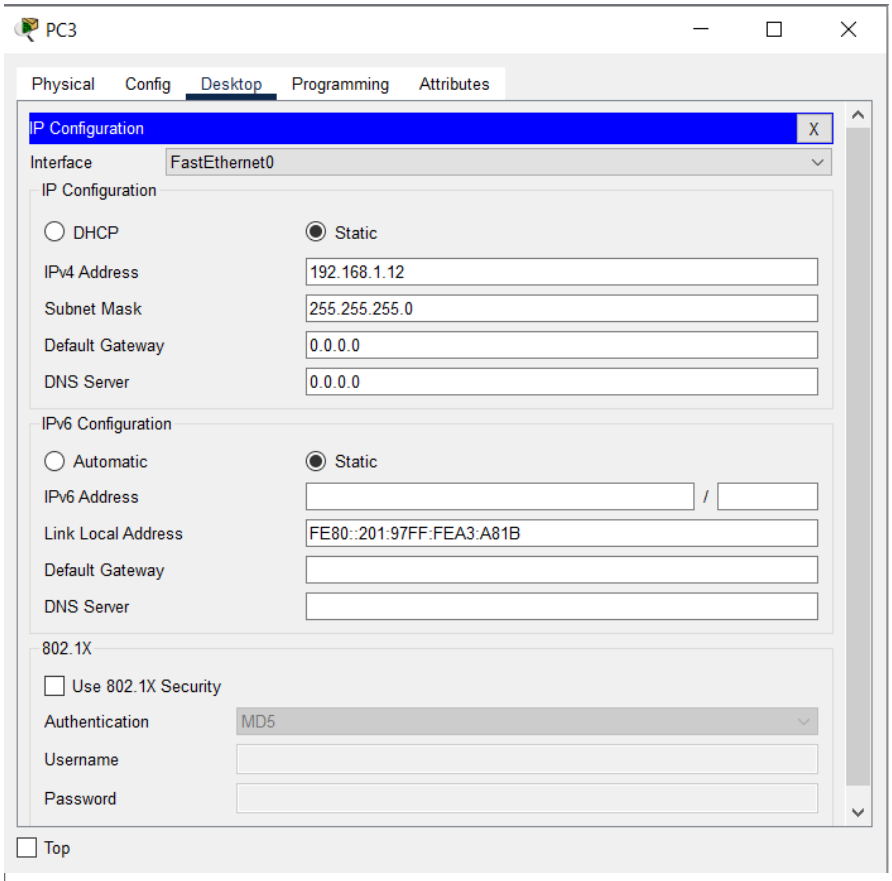
AIM:Implement VLAN and Inter-VLAN for same/new topology and explore Inter-VLAN.

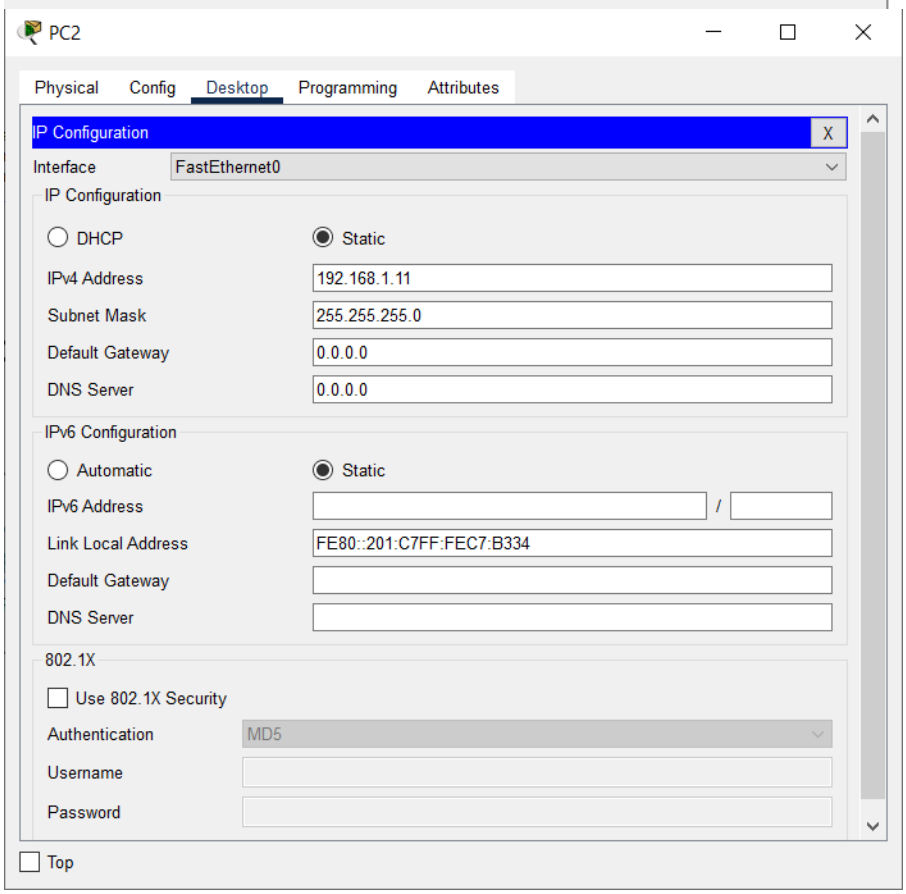
Topology:

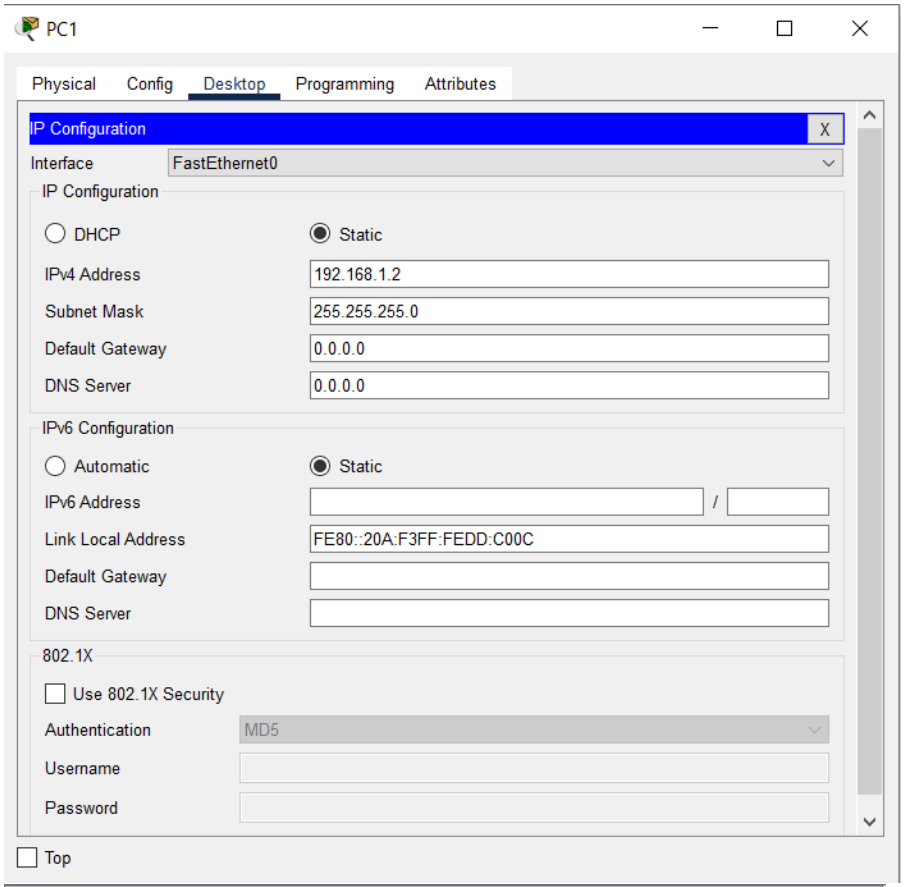
(CLASS)

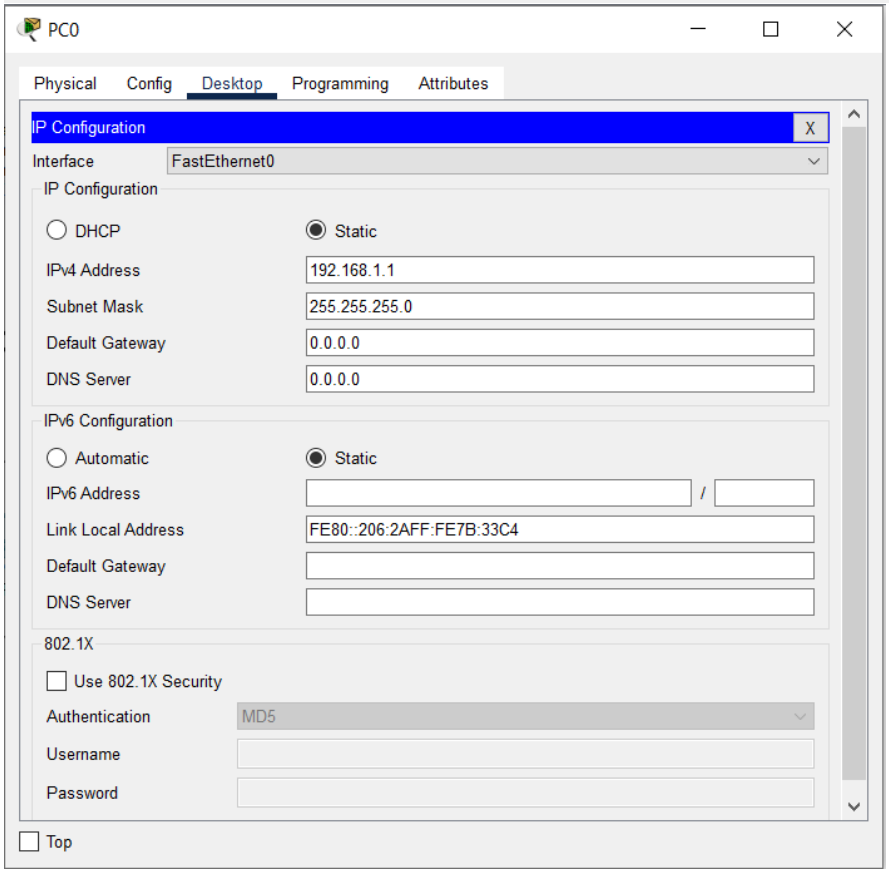


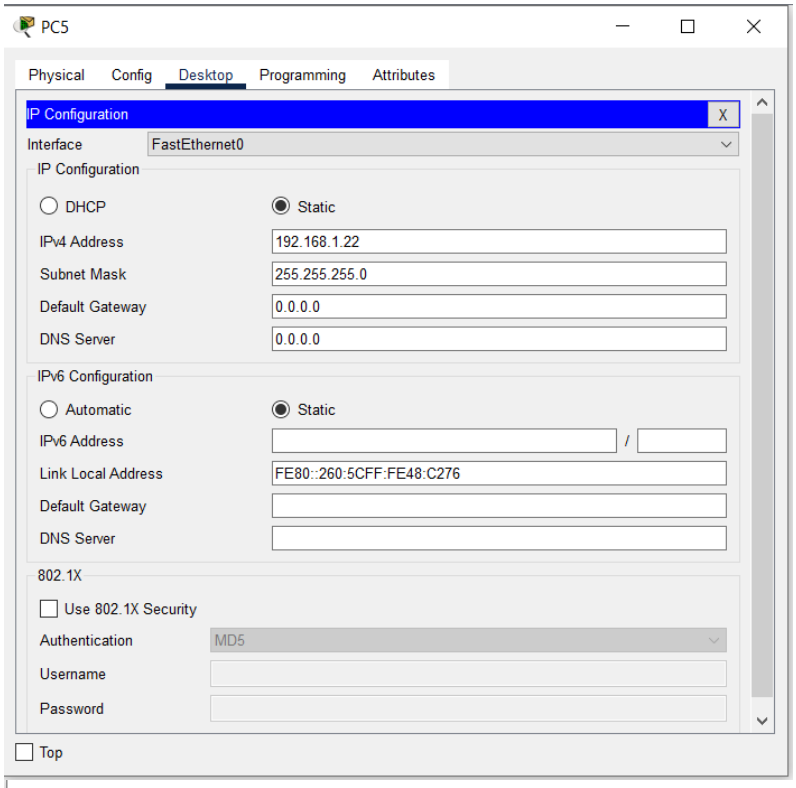

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.21
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::203:E4FF:FE97:86D3
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

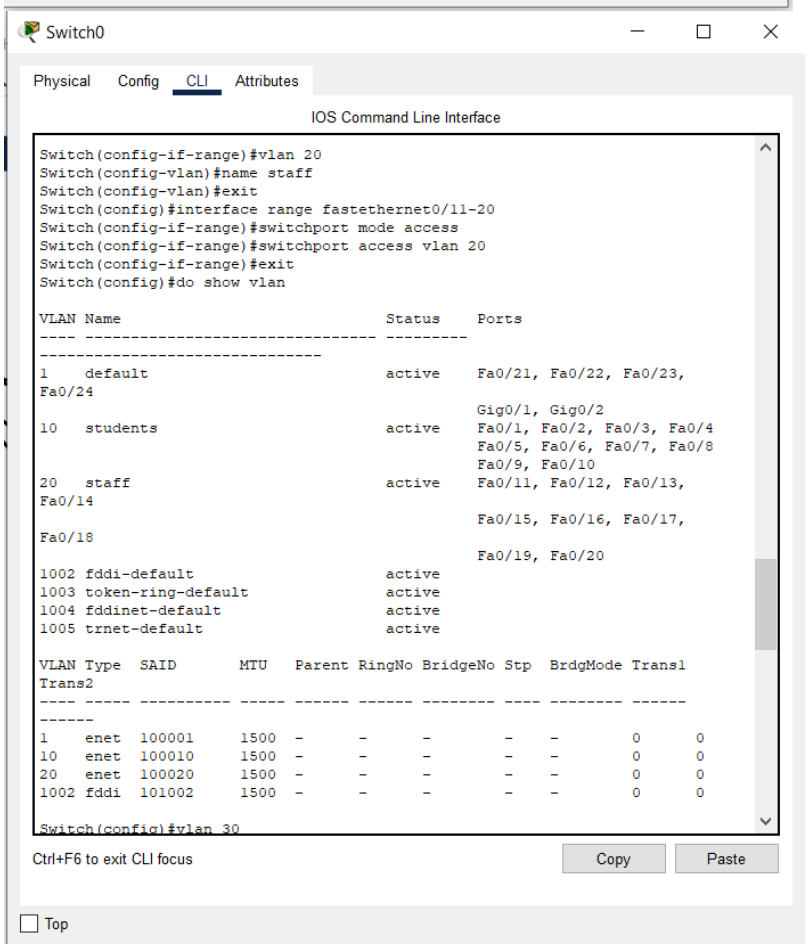

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.12
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FEA3:A81B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

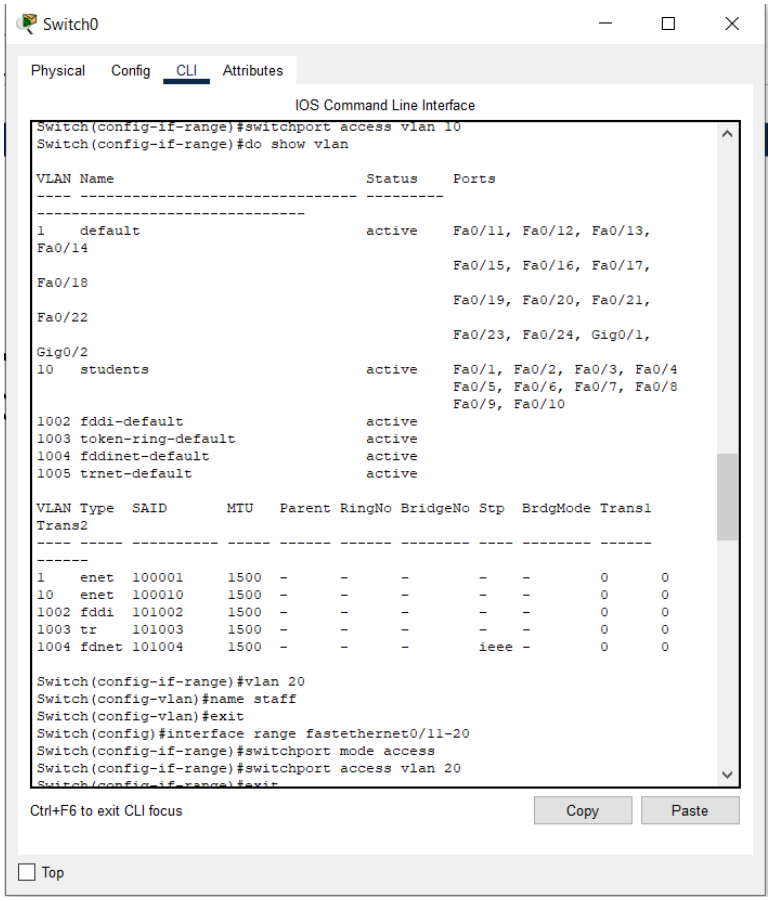

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:C7FF:FEC7:B334
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

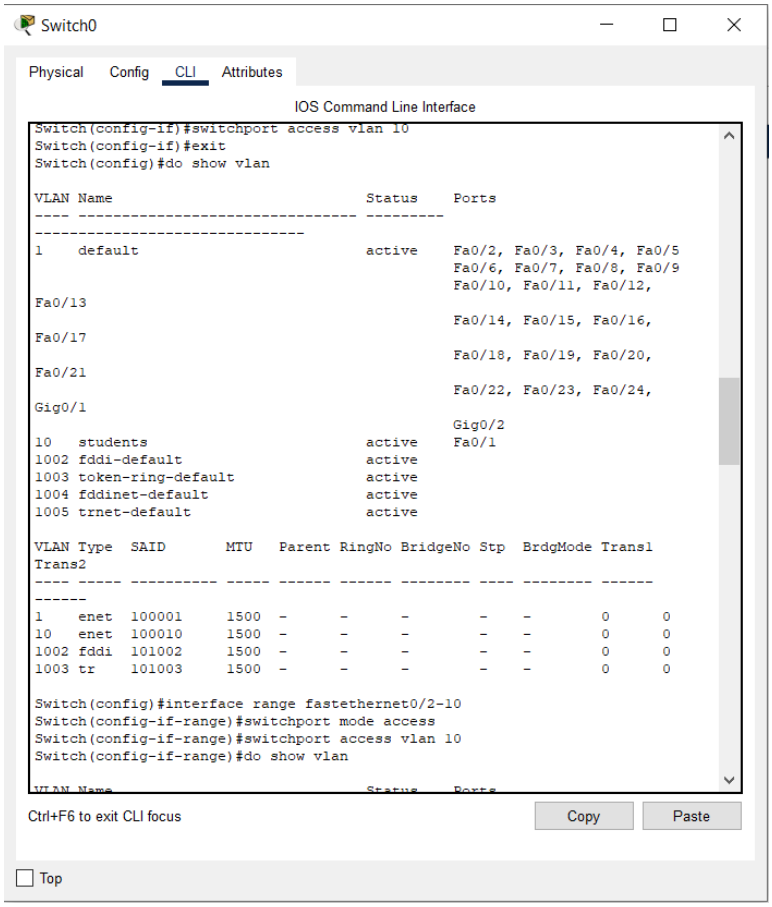

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20A:F3FF:FEDD:C00C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

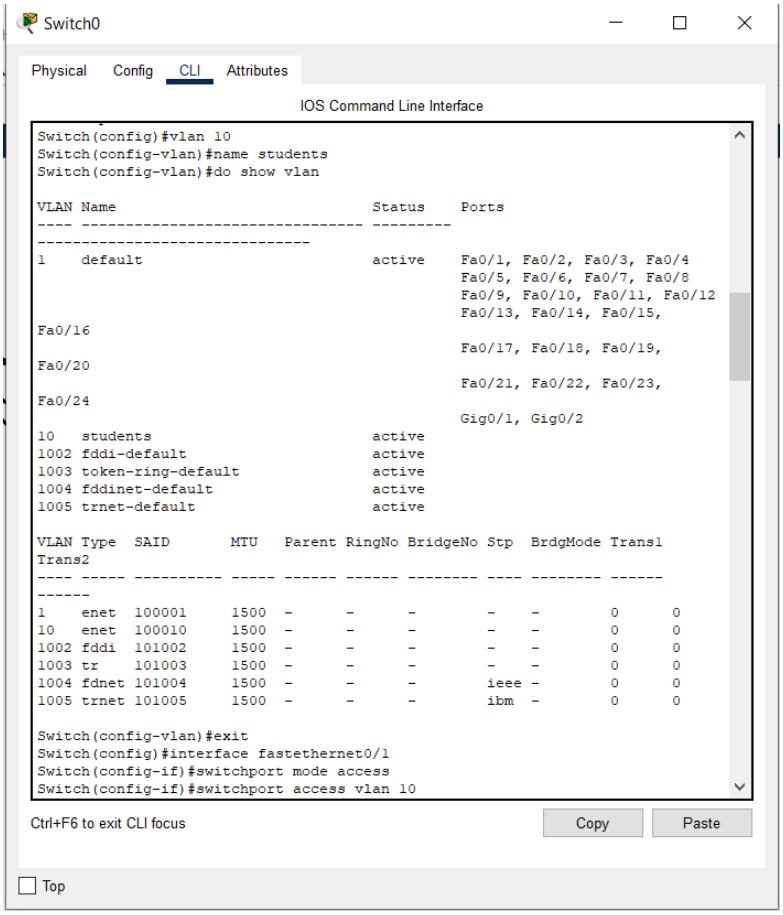

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::206:2AFF:FE7B:33C4
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

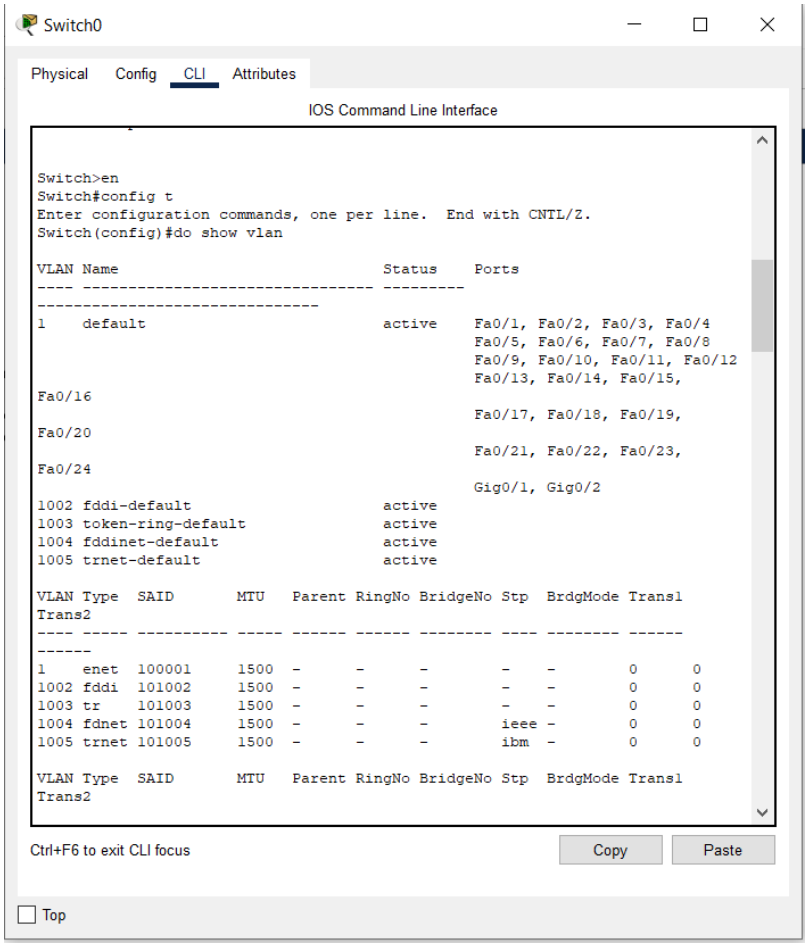

PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.22
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:5CFF:FE48:C276
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

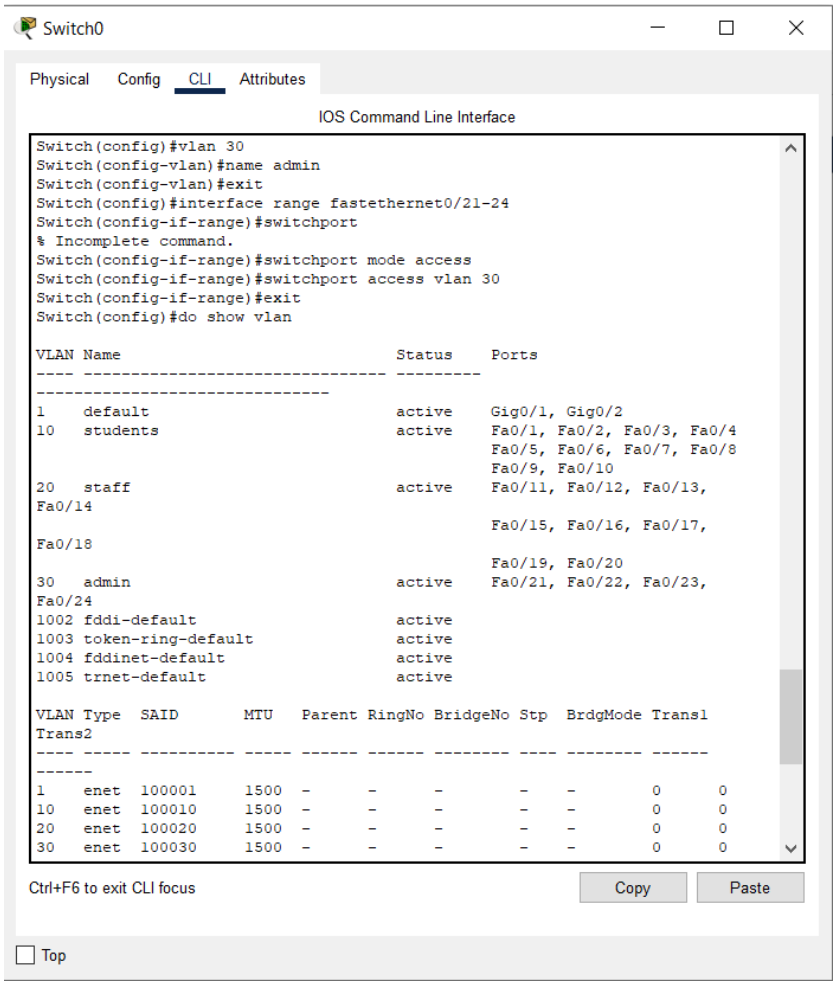

Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if-range)#vlan 20
Switch(config-vlan)#name staff
Switch(config-vlan)#exit
Switch(config)#interface range fastethernet0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#do show vlan
VLAN Name Status Ports
1 default active Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
10 students active Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
20 staff active Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
Switch(config)#vlan 30
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do show vlan
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 students active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
Switch(config-if-range)#vlan 20
Switch(config-vlan)#name staff
Switch(config-vlan)#exit
Switch(config)#interface range fastethernet0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

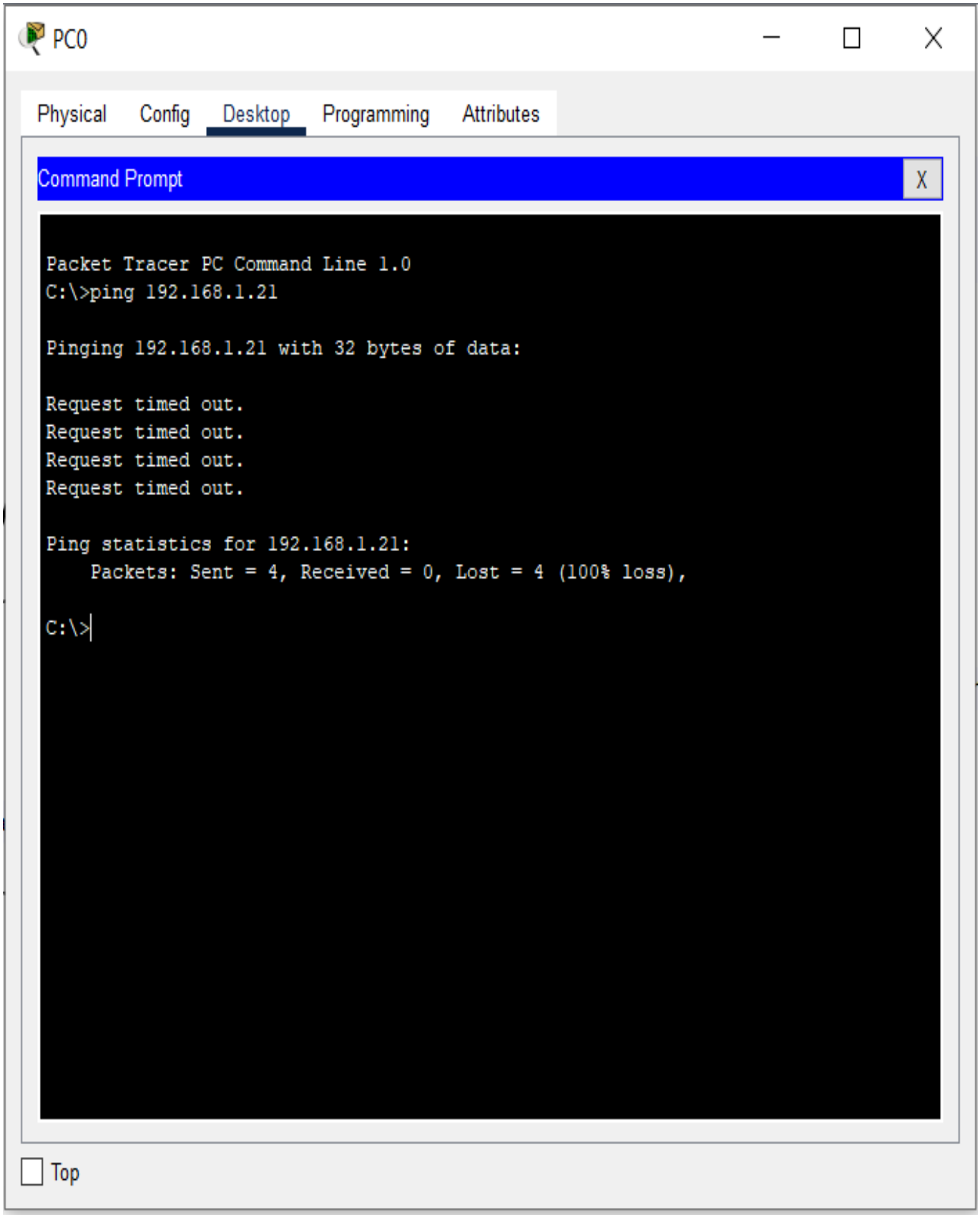

Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#do show vlan
VLAN Name Status Ports
---- -------------------------------- ---------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12,
Fa0/13
Fa0/14, Fa0/15, Fa0/16,
Fa0/17
Fa0/18, Fa0/19, Fa0/20,
Fa0/21
Fa0/22, Fa0/23, Fa0/24,
Gig0/1
Gig0/2
10 students active Fa0/1
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
Switch(config)#interface range fastethernet0/2-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do show vlan
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

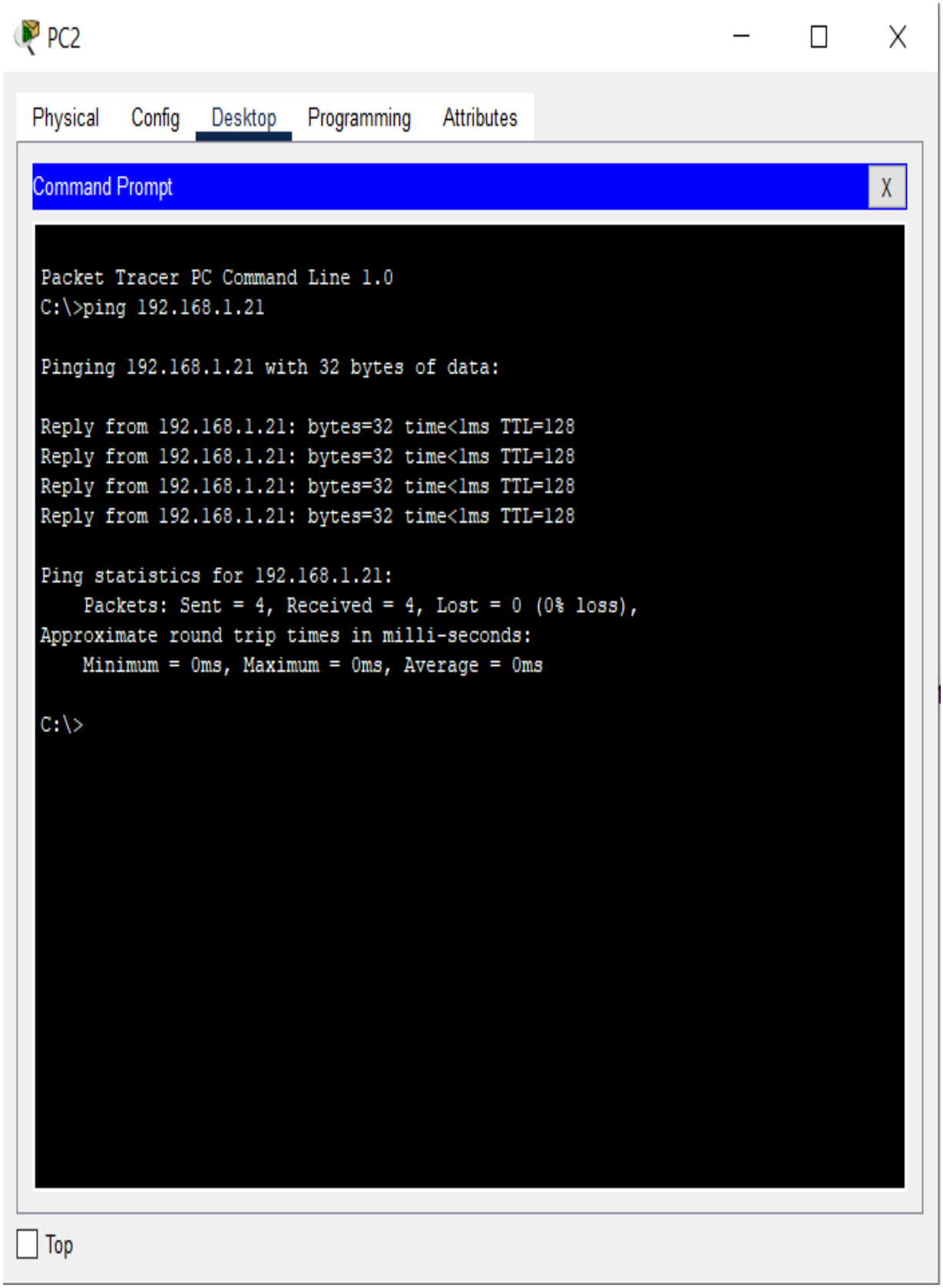

Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config)#vlan 10
Switch(config-vlan)#name students
Switch(config-vlan)#do show vlan
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15,
Fa0/16
Fa0/17, Fa0/18, Fa0/19,
Fa0/20
Fa0/21, Fa0/22, Fa0/23,
Fa0/24
Gig0/1, Gig0/2
10 students active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Switch(config-vlan)#exit
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#do show vlan
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15,
Fa0/16
Fa0/17, Fa0/18, Fa0/19,
Fa0/20
Fa0/21, Fa0/22, Fa0/23,
Fa0/24
Gig0/1, Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



Pinging other endpoint devices


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.21
Pinging 192.168.1.21 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.21:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.21
Pinging 192.168.1.21 with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.21:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

PC5

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=15ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

:

PC5

Physical Config Desktop Programming Attributes

Command Prompt

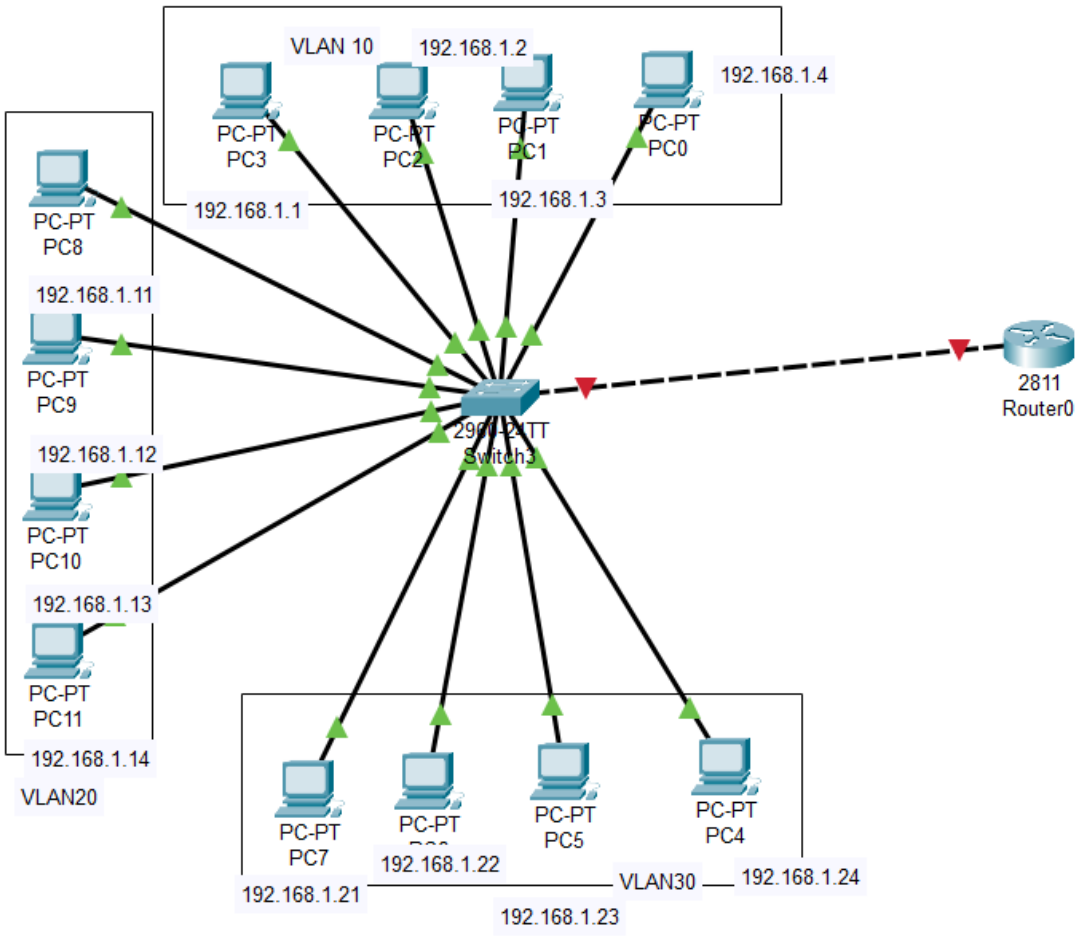
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=15ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms
```

Sending Packets from one VLAN to another:

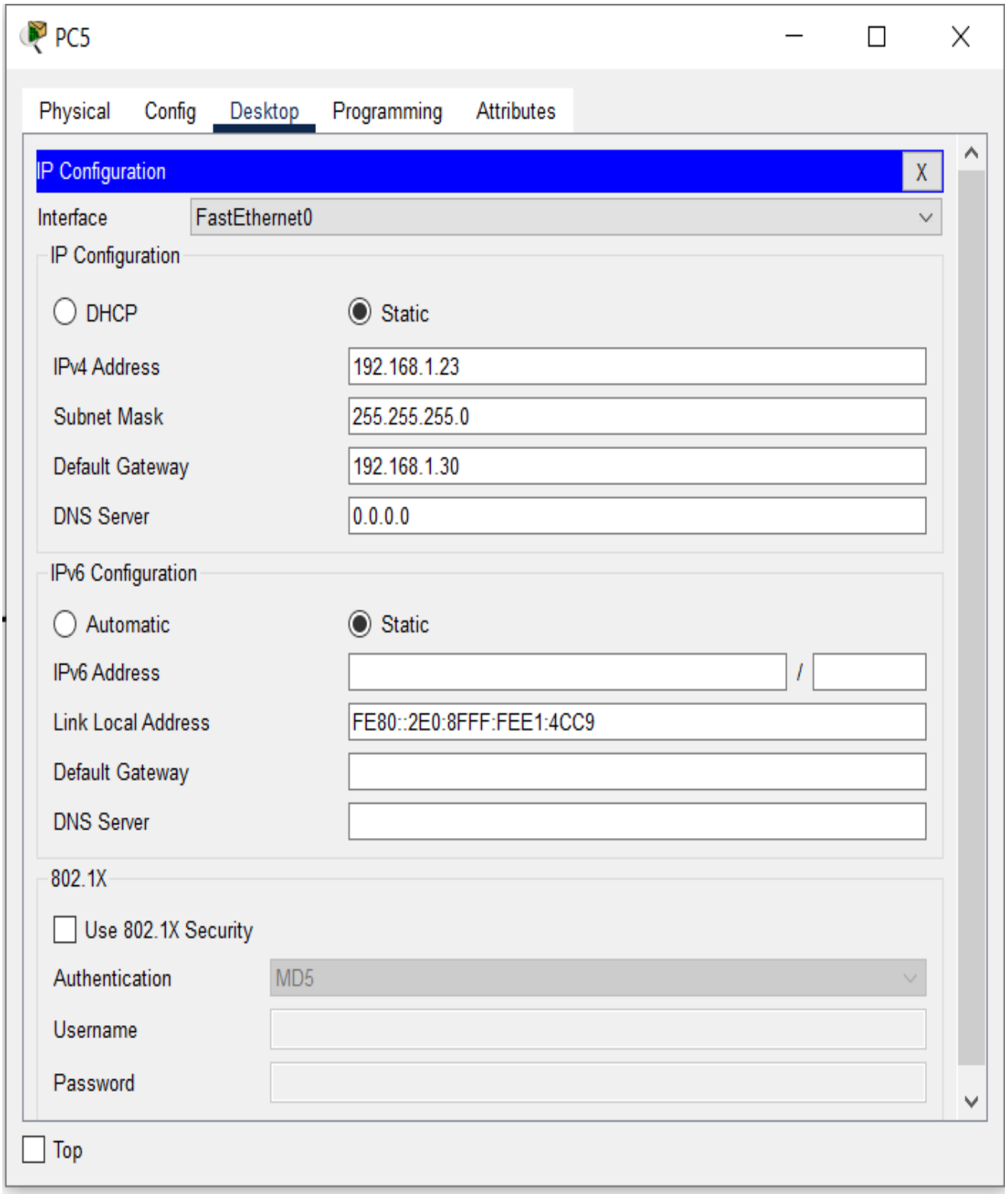
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC5	ICMP		0.000	N	0	(edit)	(delete)

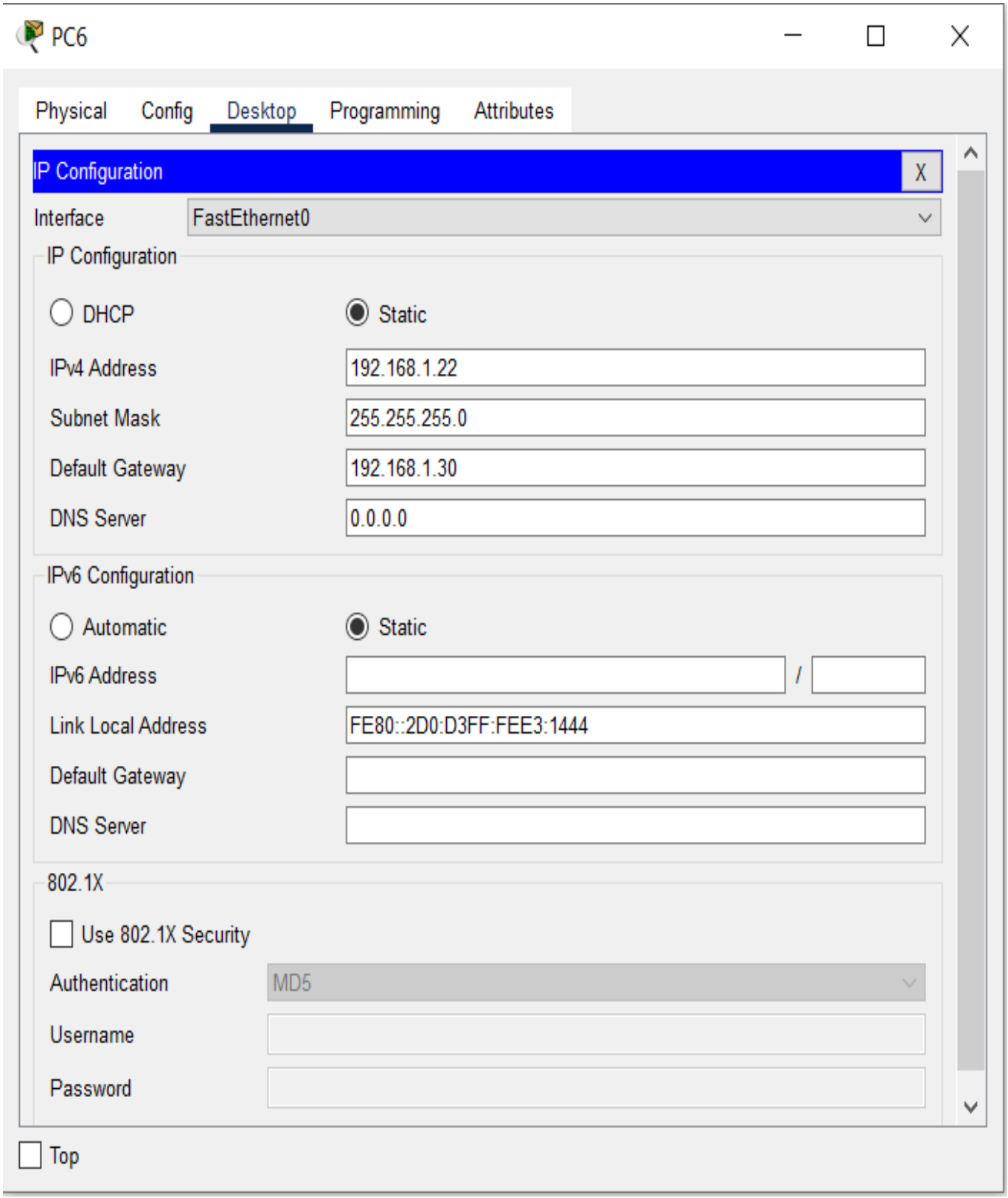
(POST-LAB)

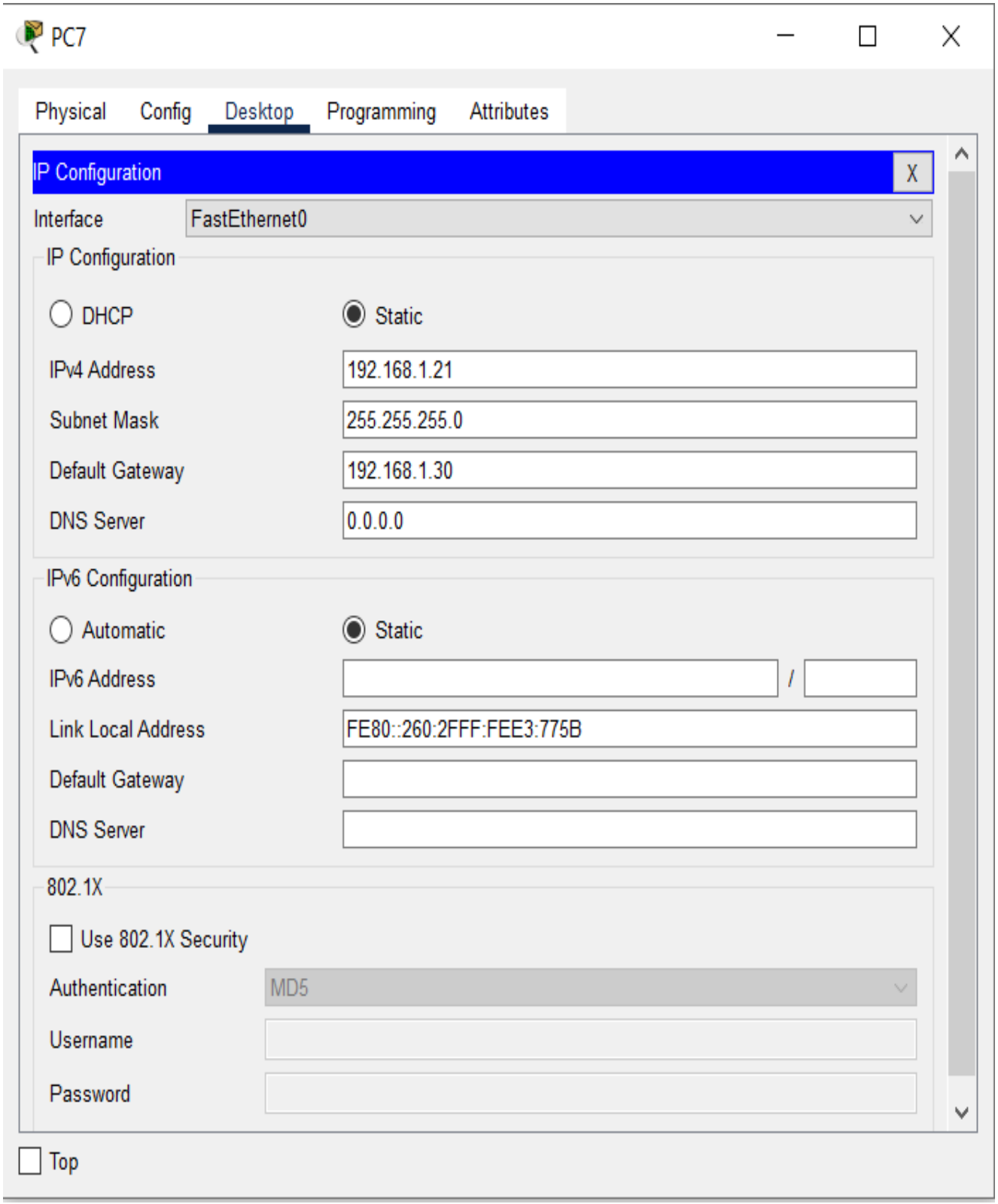
Topo;ogy

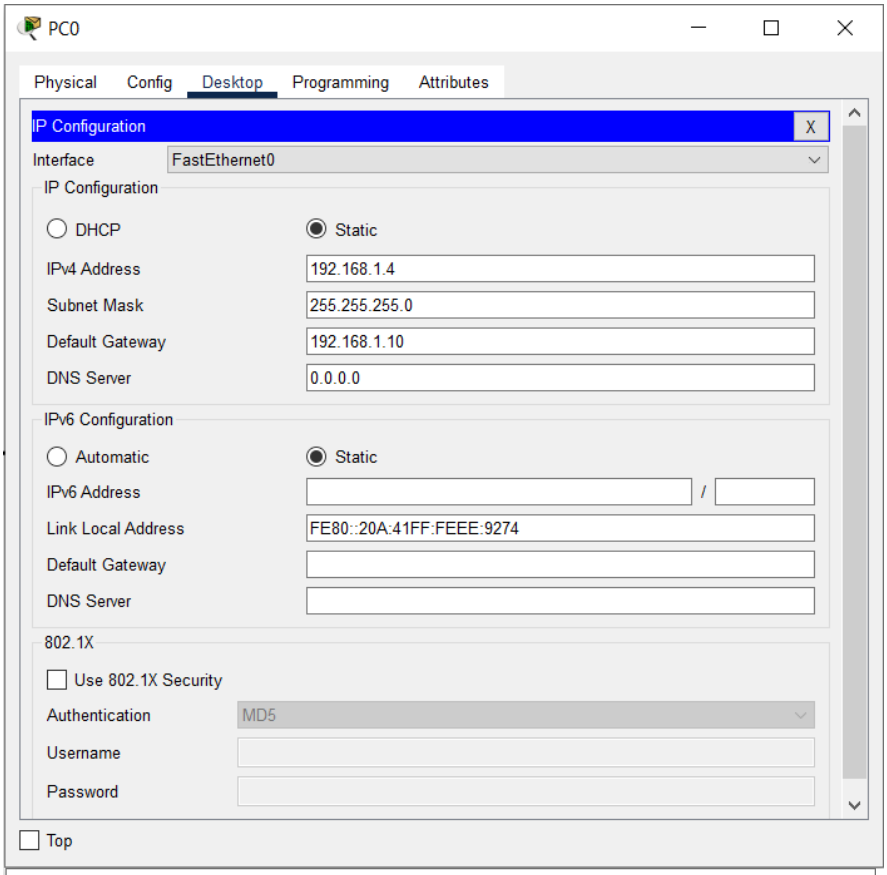


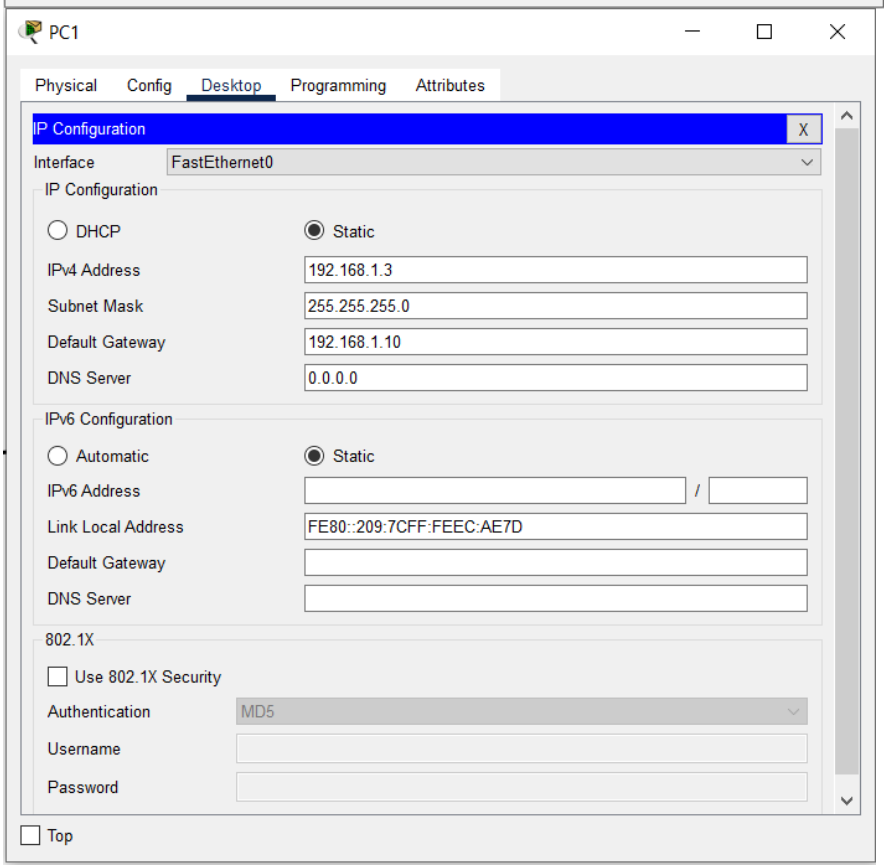
Configurations:

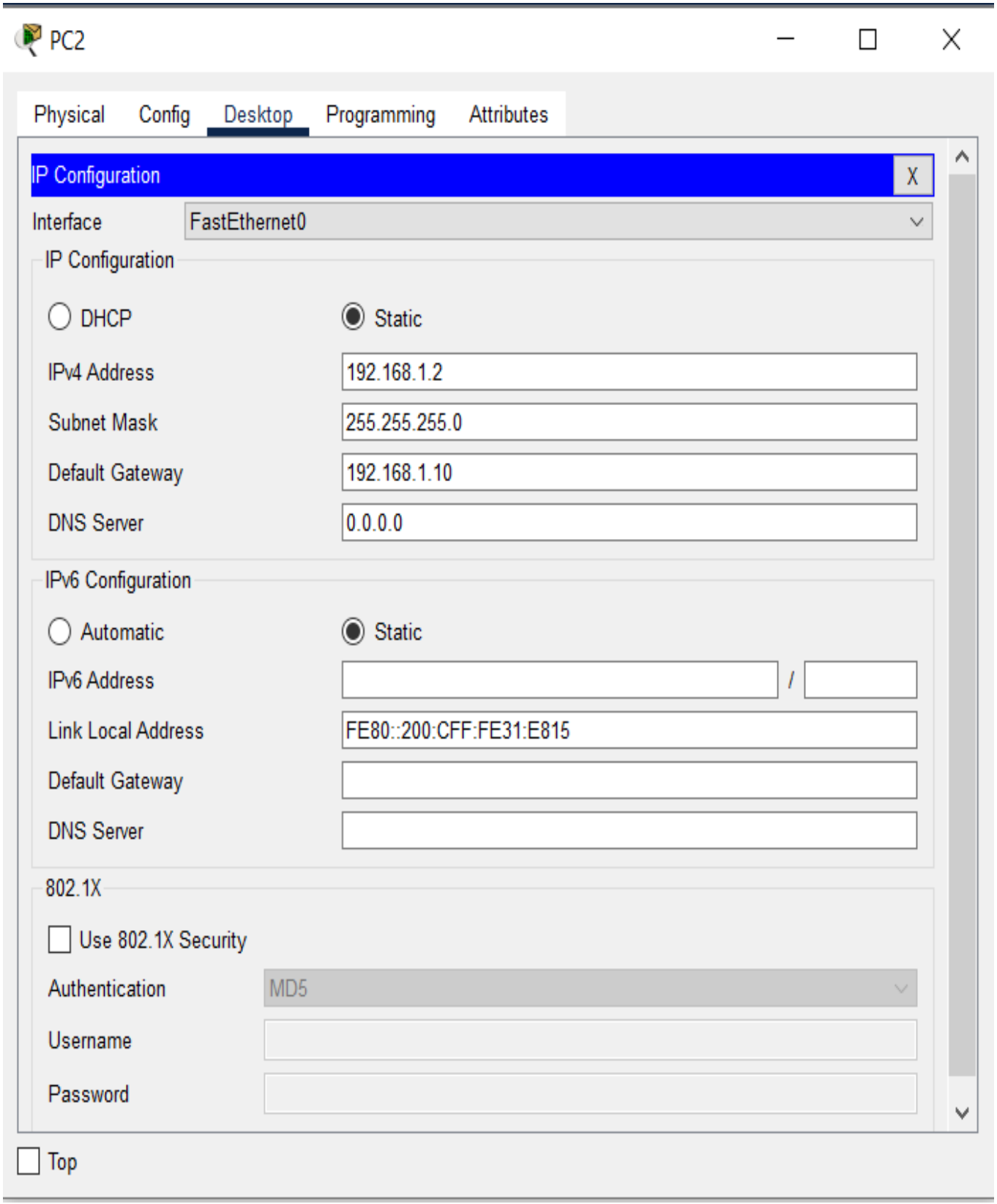

PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.23
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.30
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:8FFF:FEE1:4CC9
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

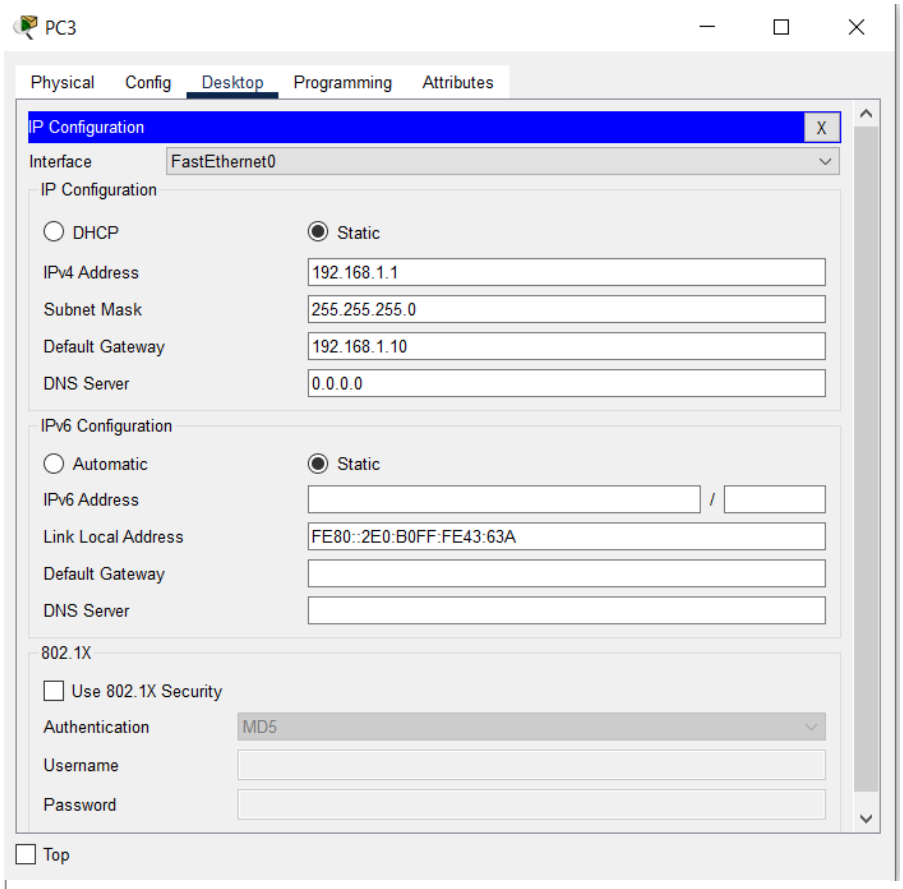

PC6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.22
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.30
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:D3FF:FEE3:1444
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

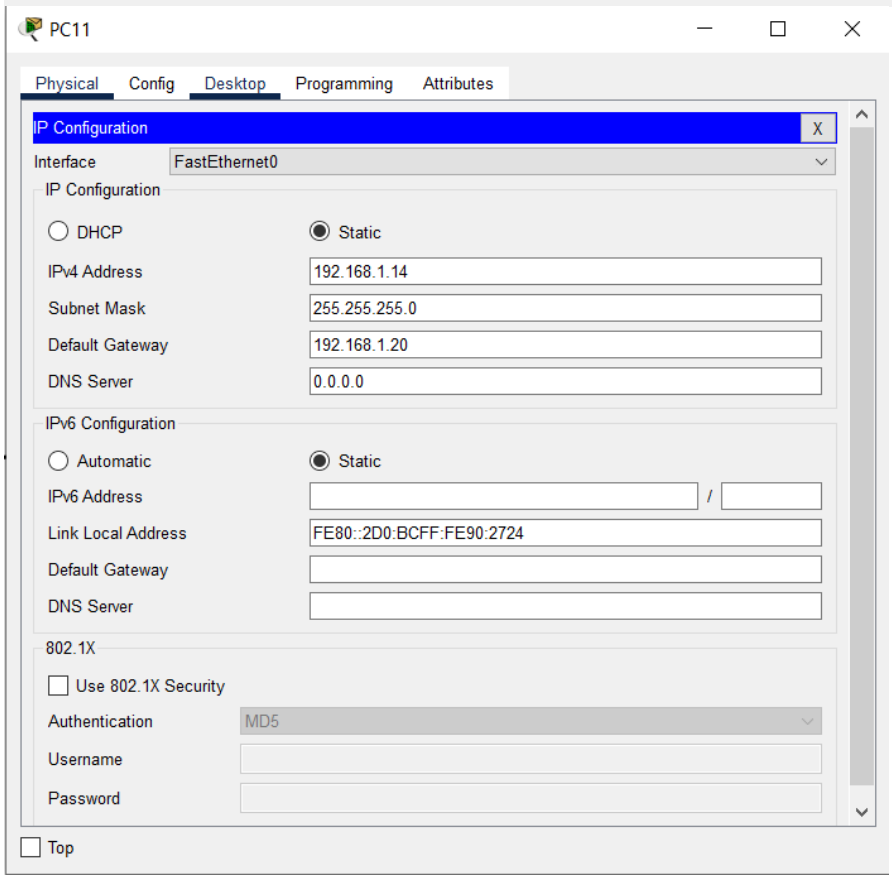

PC7
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.21
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.30
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:2FFF:FEE3:775B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

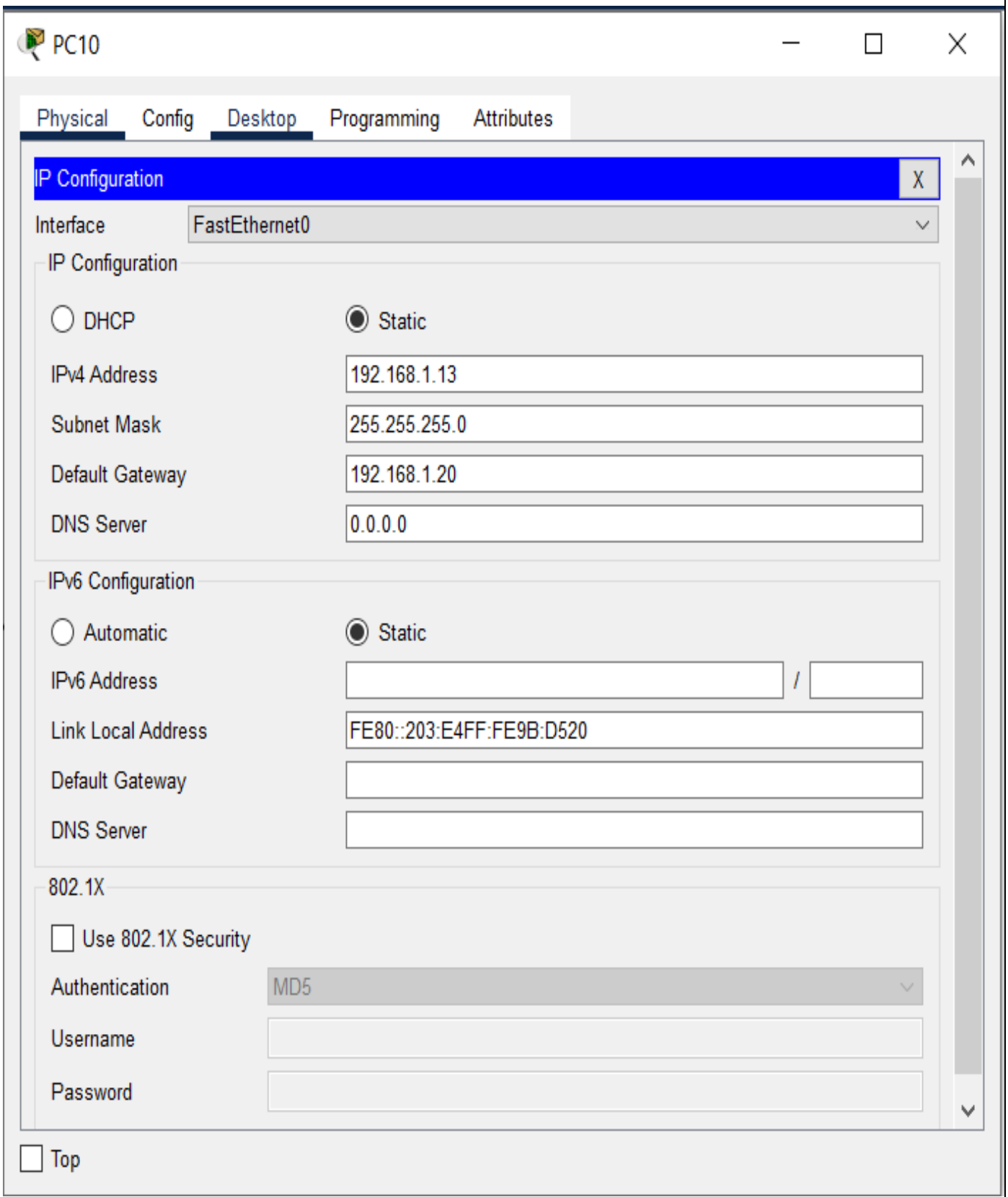

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20A:41FF:FEEE:9274
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

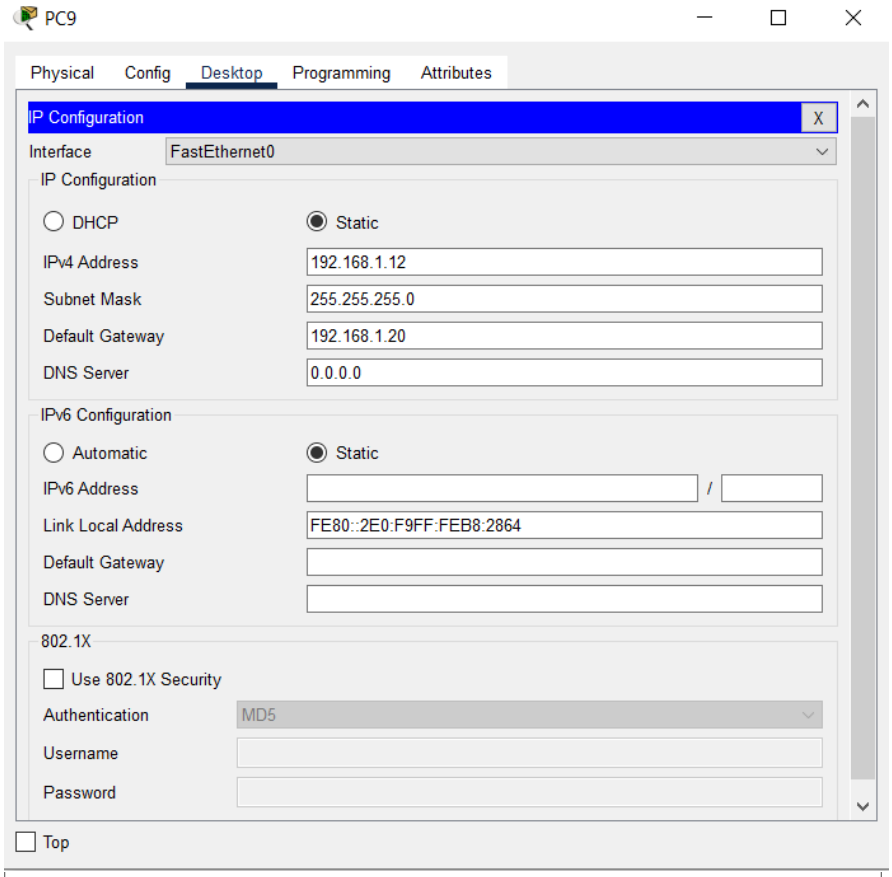

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::209:7CFF:FEEC:AE7D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

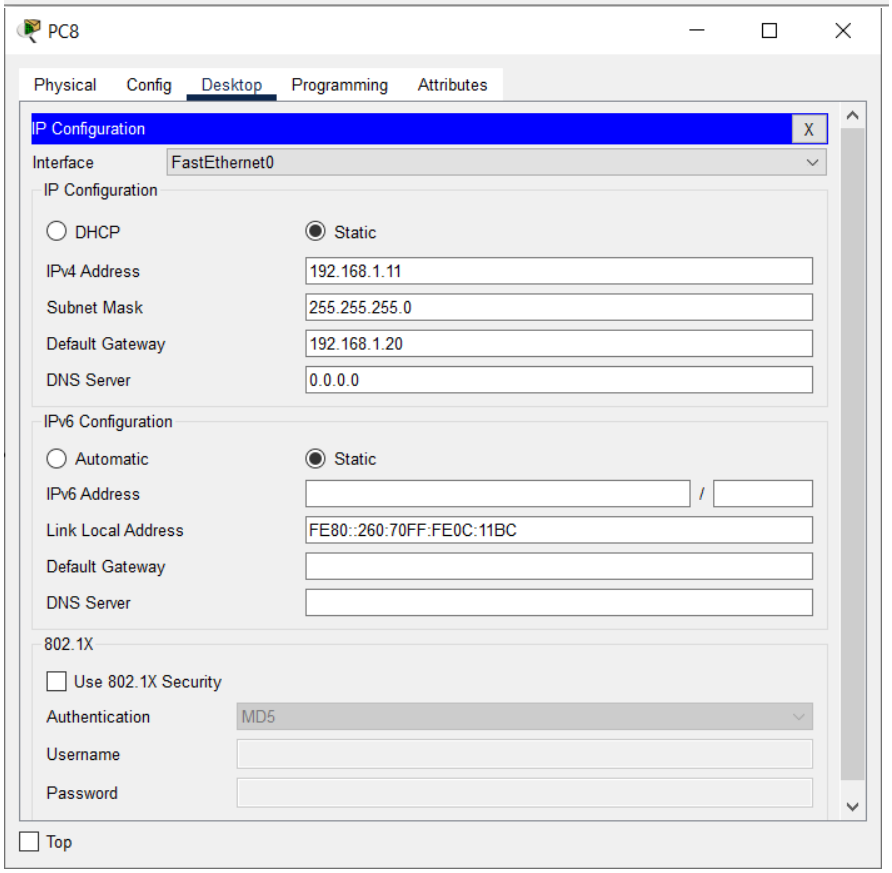

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::200:CFF:FE31:E815
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

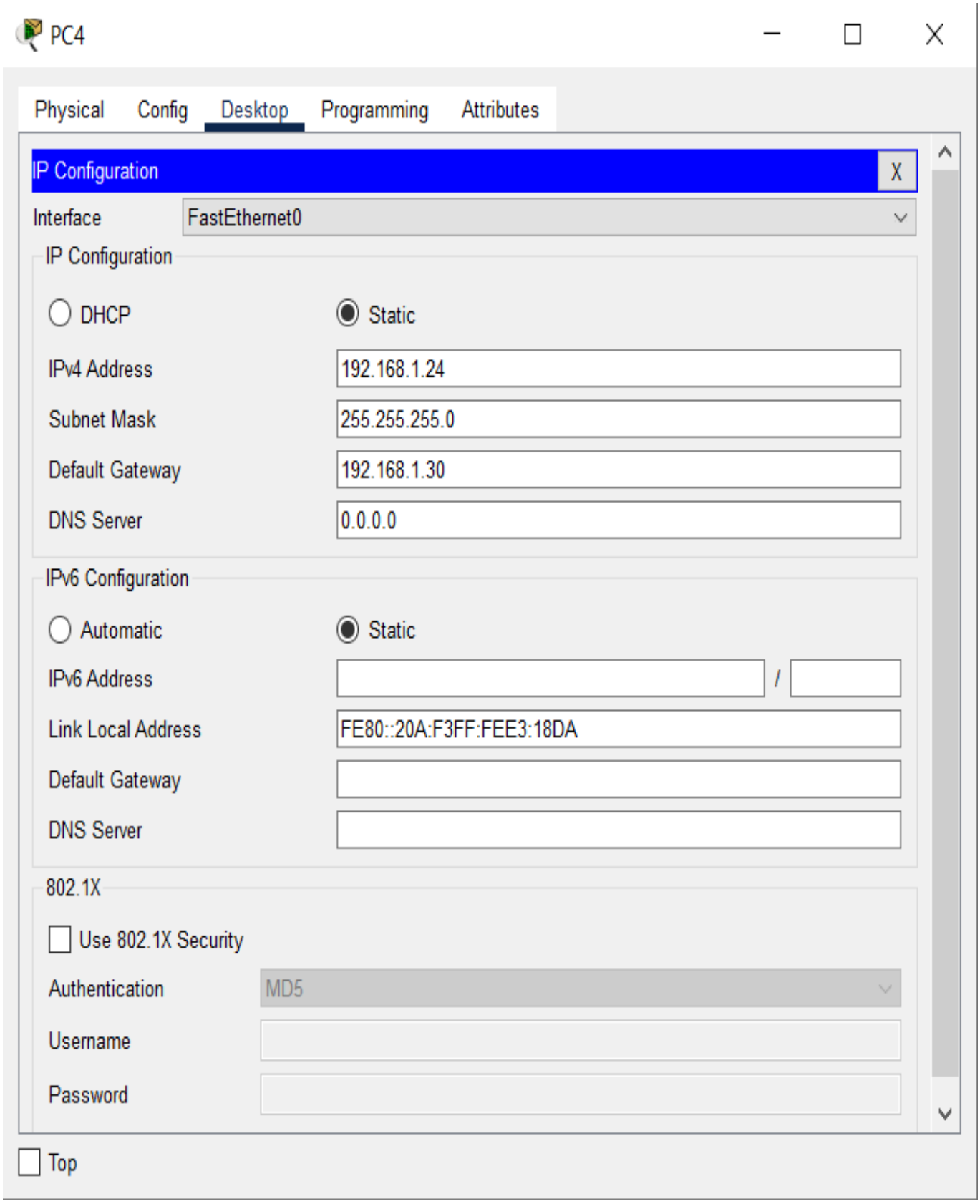

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:B0FF:FE43:63A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

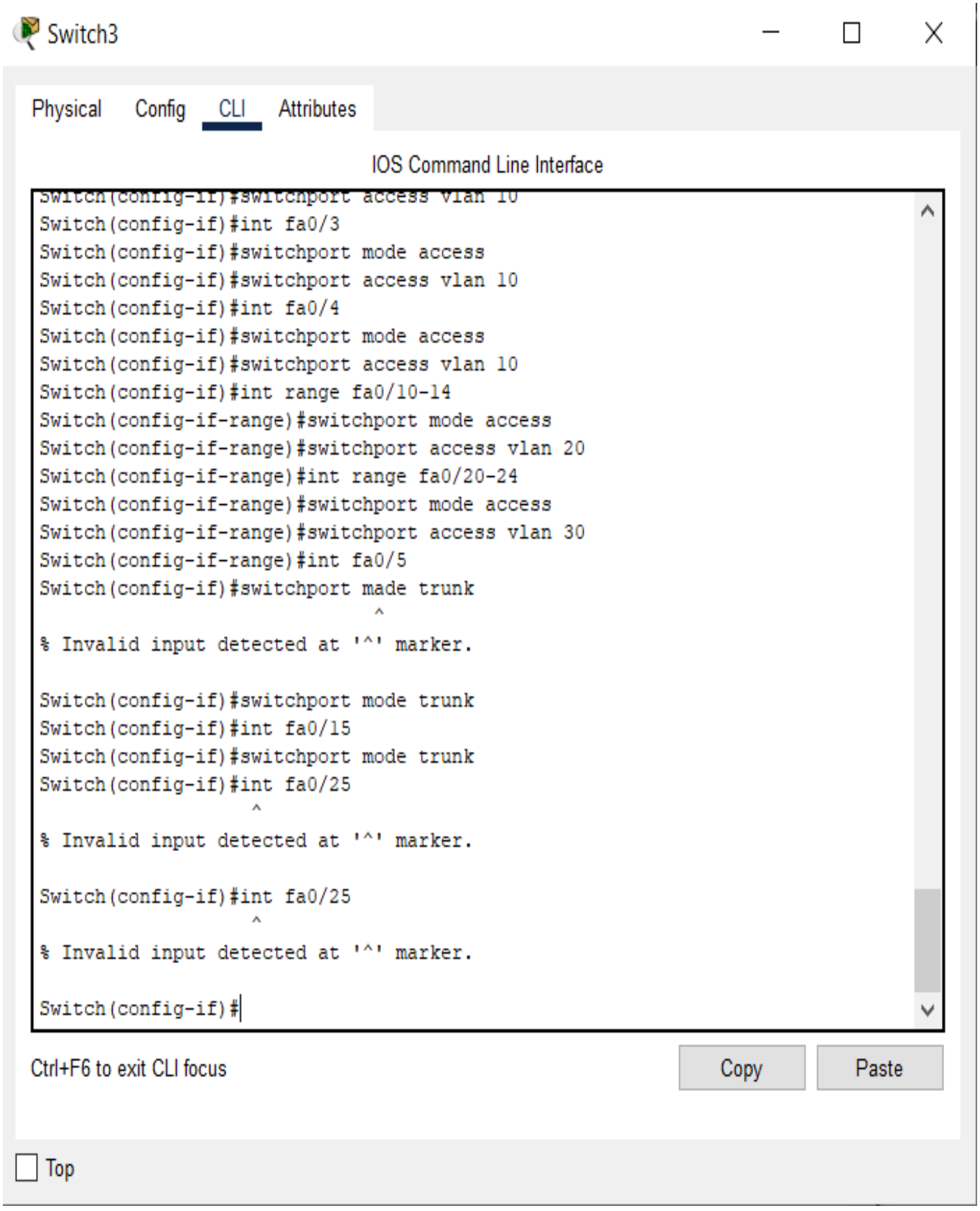

PC11
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.20
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FE90:2724
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

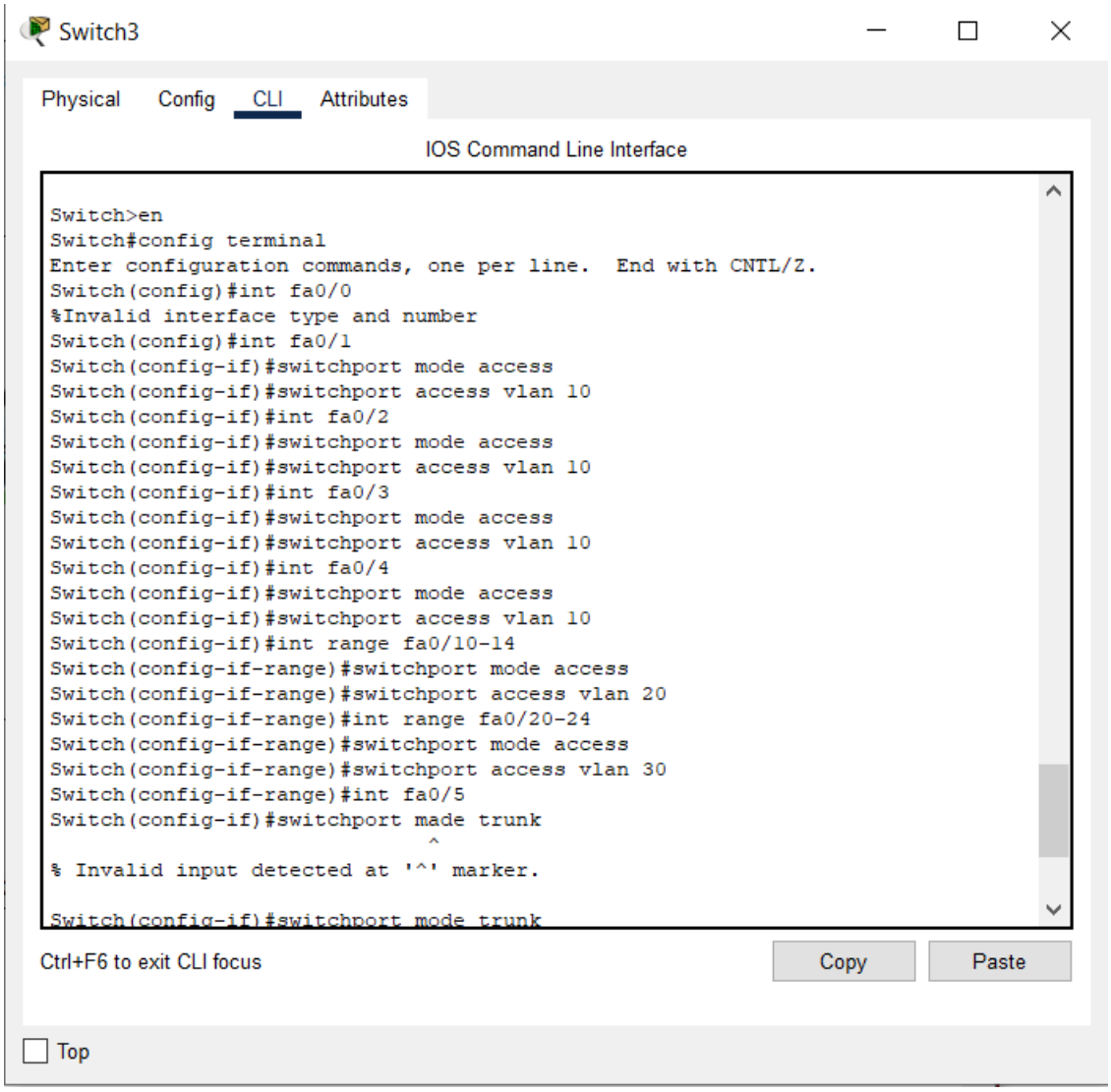

PC10
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.13
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.20
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::203:E4FF:FE9B:D520
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC9
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.20
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:F9FF:FEB8:2864
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC8
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.20
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:70FF:FE0C:11BC
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.24
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.30
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20A:F3FF:FEE3:18DA
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Switch3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int range fa0/10-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#int range fa0/20-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#int fa0/5
Switch(config-if)#switchport made trunk
^
% Invalid input detected at '^' marker.
Switch(config-if)#switchport mode trunk
Switch(config-if)#int fa0/15
Switch(config-if)#switchport mode trunk
Switch(config-if)#int fa0/25
^
% Invalid input detected at '^' marker.
Switch(config-if)#int fa0/25
^
% Invalid input detected at '^' marker.
Switch(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



SENDING PACKETS FROM ONE DEVICES TO ANOTHER:

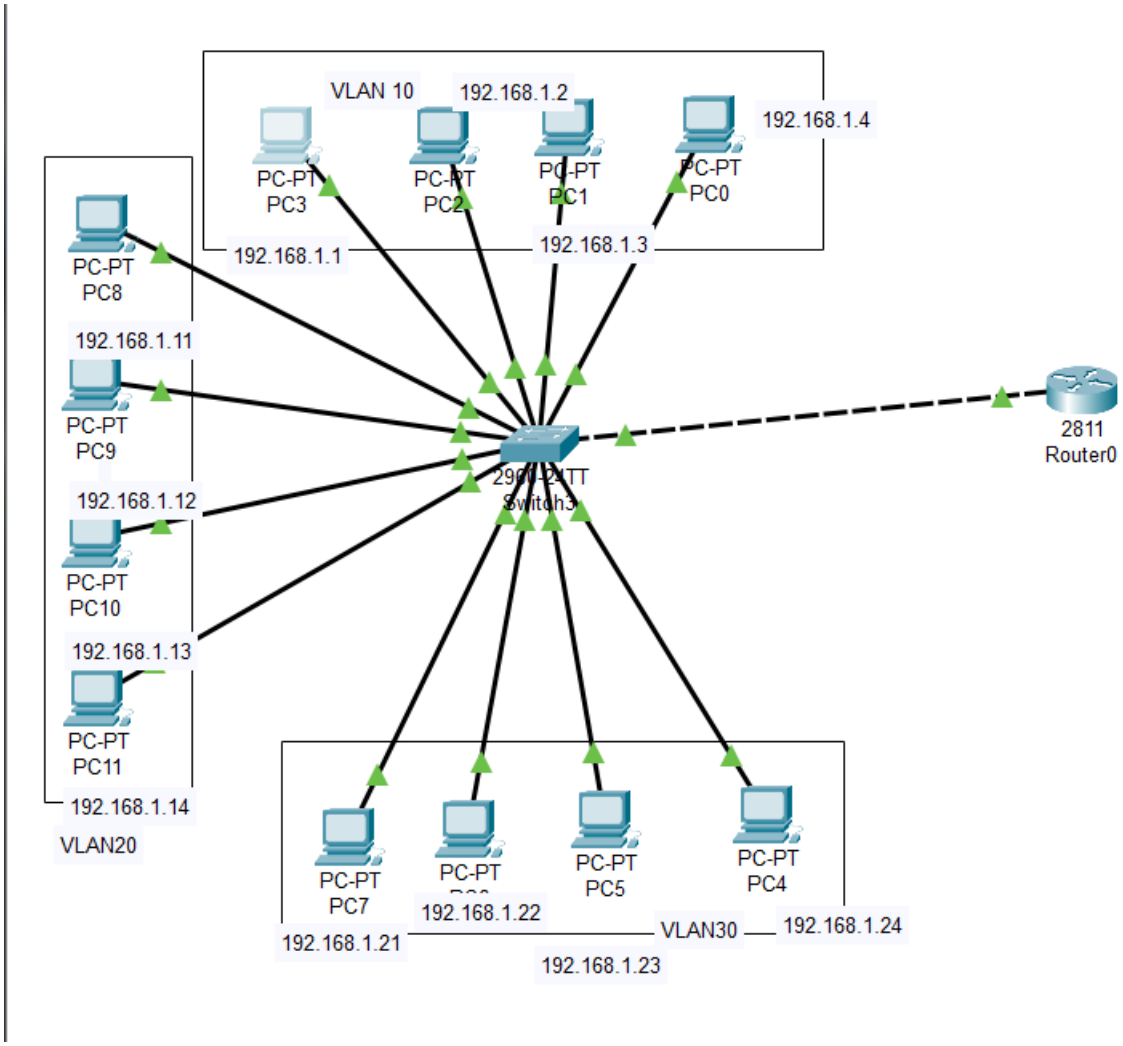
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC1	PC5	ICMP		0.000	N	3	(edit)	(delete)
	Failed	PC0	PC9	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC2	PC0	ICMP		0.000	N	5	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC4	PC10	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC7	PC4	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC3	ICMP		0.000	N	2	(edit)	(delete)

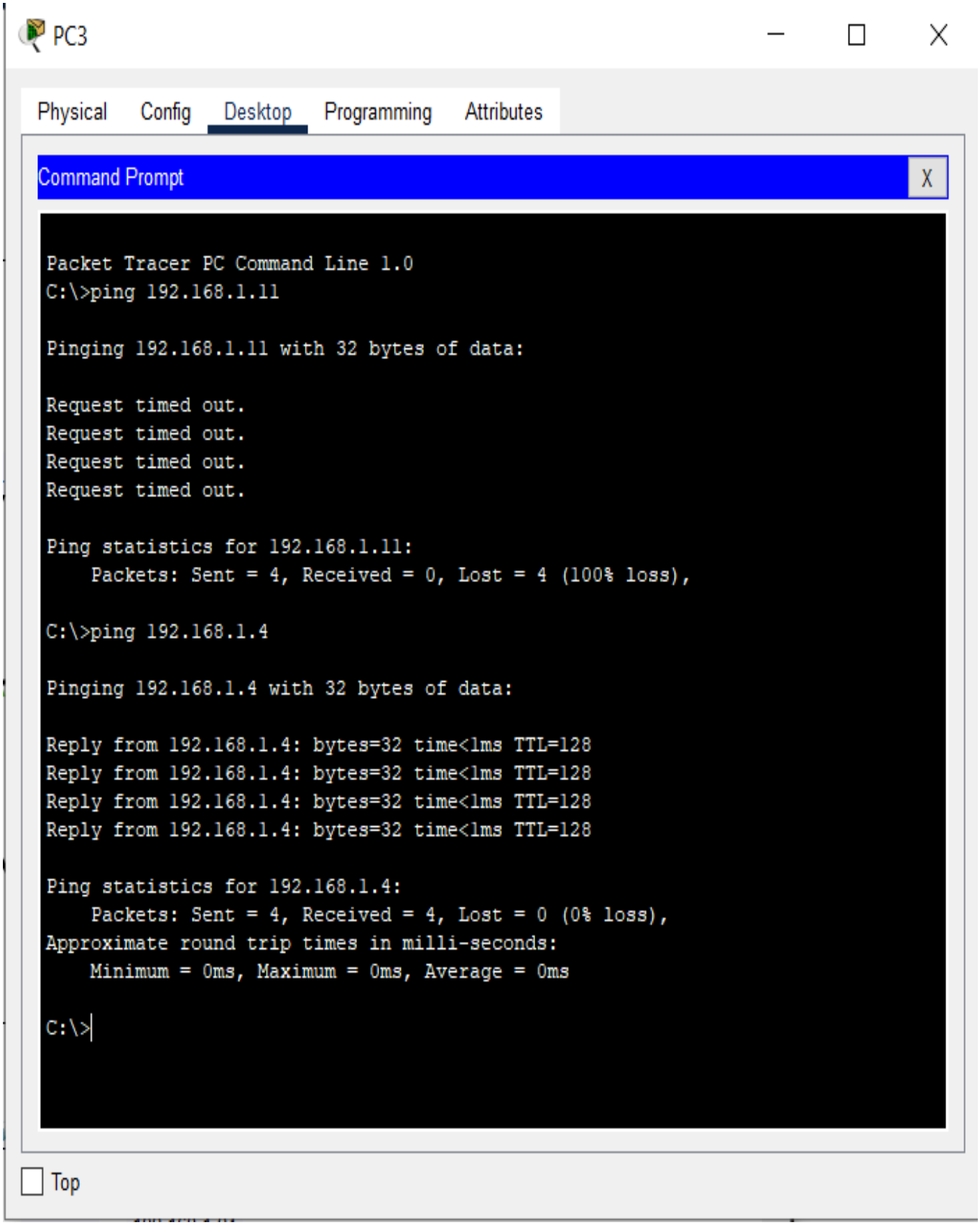
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC0	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC8	PC11	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC7	PC4	ICMP		0.000	N	7	(edit)	(delete)

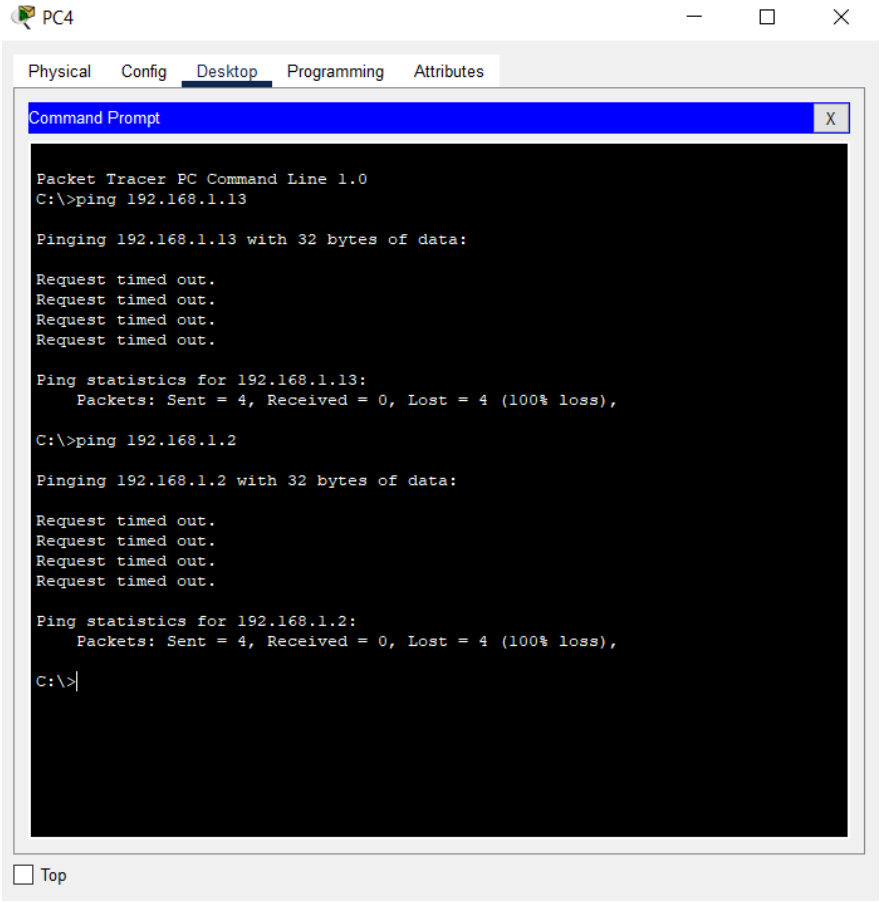
INTER-VLAN

Topology:



Router Configuration:


PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top



Inference

A Virtual LAN (**VLAN)** is simply a logical LAN, just as its name suggests. VLANs have similar characteristics with those of physical LANs, only that with VLANs, you can logically group hosts even if they are physically located on separate LAN segments.

We treat each VLAN as a separate subnet or broadcast domain. For this reason, to move packets from one VLAN to another, we have to use a router or a layer 3 switch.

VLANs are configured on switches by placing some interfaces into one broadcast domain and some interfaces into another.

An *access port* is assigned to a single VLAN . These ports are configured for switch ports that connect to devices with a normal network card, for example a PC in a network.

A *trunk port* on the other hand is a port that can be connected to another switch or router. This port can carry traffic of multiple VLANs.

Test inter-VLAN connectivity.

Here we'll test connectivity between computers in different VLANs . Don't forget that its the router that enables inter-VLAN routing.

Ping PC3 in VLAN 20 from PC1 in VLAN 10. If everything is well configured, then ping should work perfectly.

Conclusion:

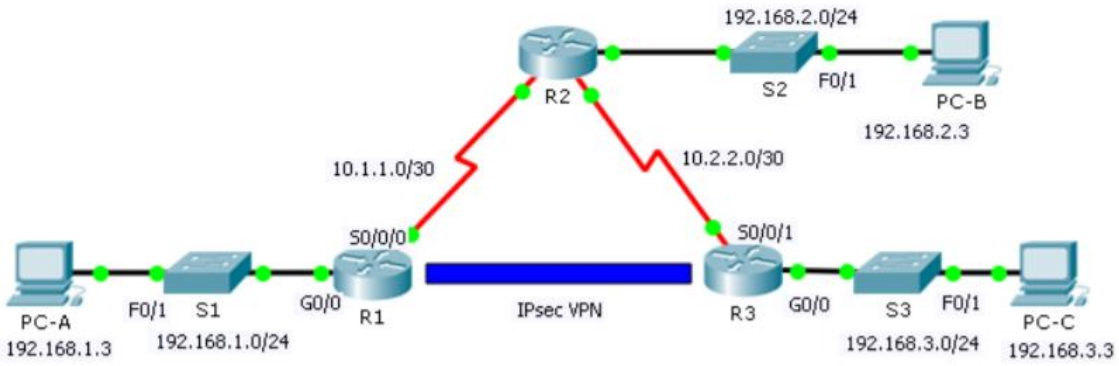
VLAN and inter-VLAN has been successfully implemented.

LAB 5

Aryaman Mishra

19BCE1027

VPN Configuration



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

1. Starting configurations for R1, ISP, and R3. Paste to global config mode :

hostname R1

interface g0/1

ip address 192.168.1.1 255.255.255.0

```
no shut
interface g0/0
ip address 209.165.100.1 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 209.165.100.2

hostname ISP
interface g0/1
ip address 209.165.200.2 255.255.255.0
no shut
interface g0/0
ip address 209.165.100.2 255.255.255.0
no shut
exit

hostname R3
interface g0/1
ip address 192.168.3.1 255.255.255.0
no shut
interface g0/0
ip address 209.165.200.1 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 209.165.200.2
```

2. Make sure routers have the security license enabled:

show version

license boot module c1900 technology-package securityk9

copy run start

reload

3. Configure IPsec on the routers at each end of the tunnel (R1 and R3)

!R1

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

!

crypto isakmp key secretkey address 209.165.200.1

!

crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac

!

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 209.165.200.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set R1-R3

match address 100

!

interface GigabitEthernet0/0

```
crypto map IPSEC-MAP
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255


!R3
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
!
crypto isakmp key secretkey address 209.165.100.1
!
crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 209.165.100.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set R3-R1
match address 100
!
interface GigabitEthernet0/0
crypto map IPSEC-MAP
!
R3
access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

R1

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Step 1: Test connectivity.

Ping from **PC-A** to **PC-C**.

Step 2: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on **R1** to the LAN on **R3** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between **R1** to **R3** LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny any, there is no need to add the statement to the list.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Step 3: Configure the ISAKMP Phase 1 properties on R1.

Configure the crypto ISAKMP policy **10** properties on **R1** along with the shared crypto key **cisco**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Step 4: Configure the ISAKMP Phase 2 properties on R1.

Create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Step 5: Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface. **Note:** This is not graded.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Part 3: Configure IPsec Parameters on R3

Step 1: Configure router R3 to support a site-to-site VPN with R1.

Now configure reciprocating parameters on **R3**. Configure ACL **110** identifying the traffic from the LAN on **R3** to the LAN on **R1** as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Step 2: Configure the ISAKMP Phase 1 properties on R3.

Configure the crypto ISAKMP policy **10** properties on **R3** along with the shared crypto key **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Step 3: Configure the ISAKMP Phase 2 properties on R1.

Like you did on **R1**, create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Step 4: Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/1 interface. **Note**: This is not graded.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on **R1**. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<output omitted>
```

Step 2: Create interesting traffic.

Ping **PC-C** from **PC-A**.

Step 3: Verify the tunnel after interesting traffic.

On **R1**, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<output omitted>
```

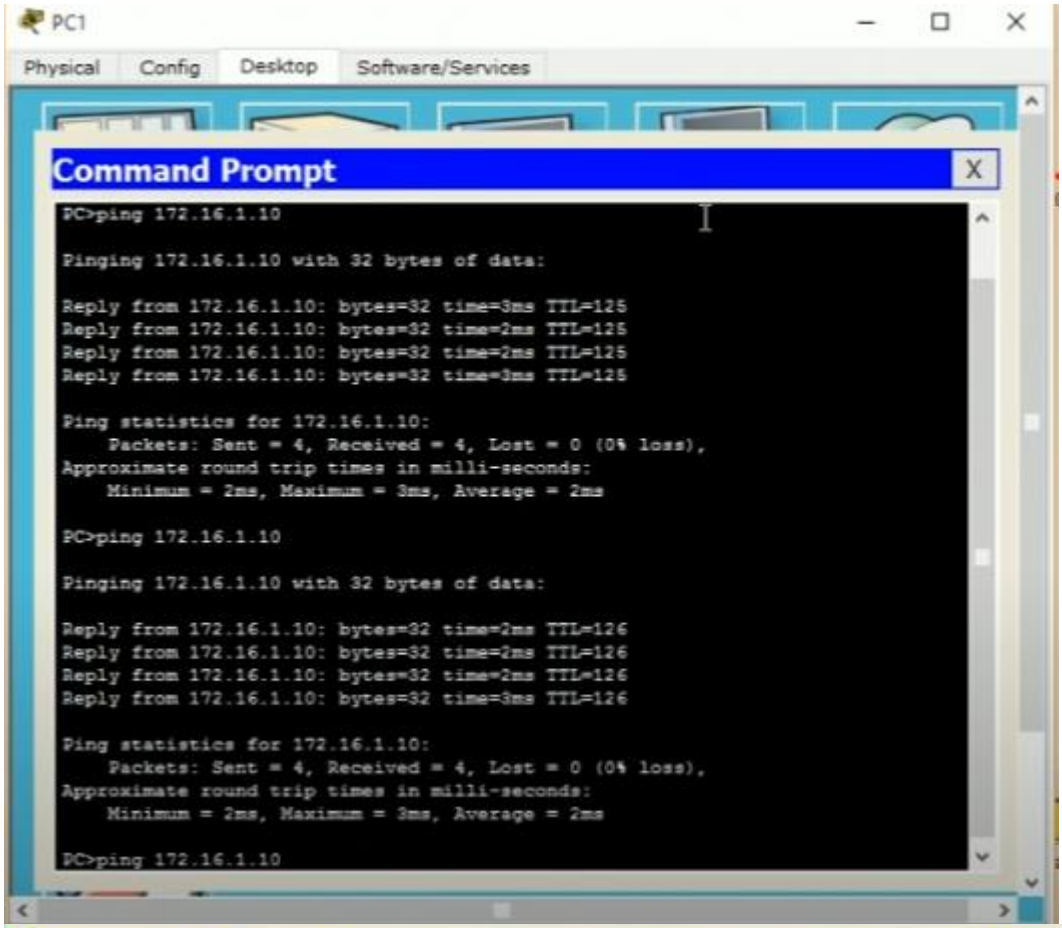
Step 4: Create uninteresting traffic.

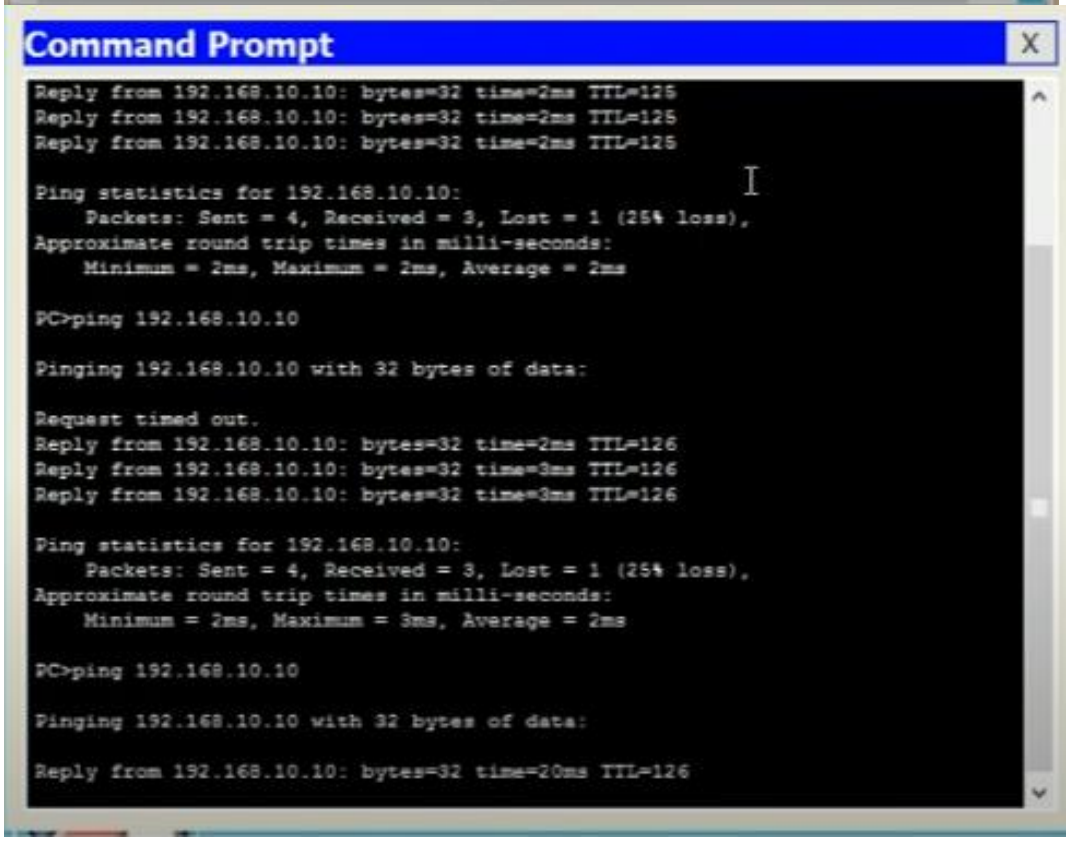
Ping **PC-B** from **PC-A**.

Step 5: Verify the tunnel.

On **R1**, re-issue the **show crypto ipsec sa** command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted.

Output on next Page:


PC1
Physical
Config
Desktop
Software/Services
Command Prompt
PC>ping 172.16.1.10
Pinging 172.16.1.10 with 32 bytes of data:
Reply from 172.16.1.10: bytes=32 time=3ms TTL=125
Reply from 172.16.1.10: bytes=32 time=2ms TTL=125
Reply from 172.16.1.10: bytes=32 time=2ms TTL=125
Reply from 172.16.1.10: bytes=32 time=3ms TTL=125
Ping statistics for 172.16.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
PC>ping 172.16.1.10
Pinging 172.16.1.10 with 32 bytes of data:
Reply from 172.16.1.10: bytes=32 time=2ms TTL=126
Reply from 172.16.1.10: bytes=32 time=2ms TTL=126
Reply from 172.16.1.10: bytes=32 time=2ms TTL=126
Reply from 172.16.1.10: bytes=32 time=3ms TTL=126
Ping statistics for 172.16.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
PC>ping 172.16.1.10

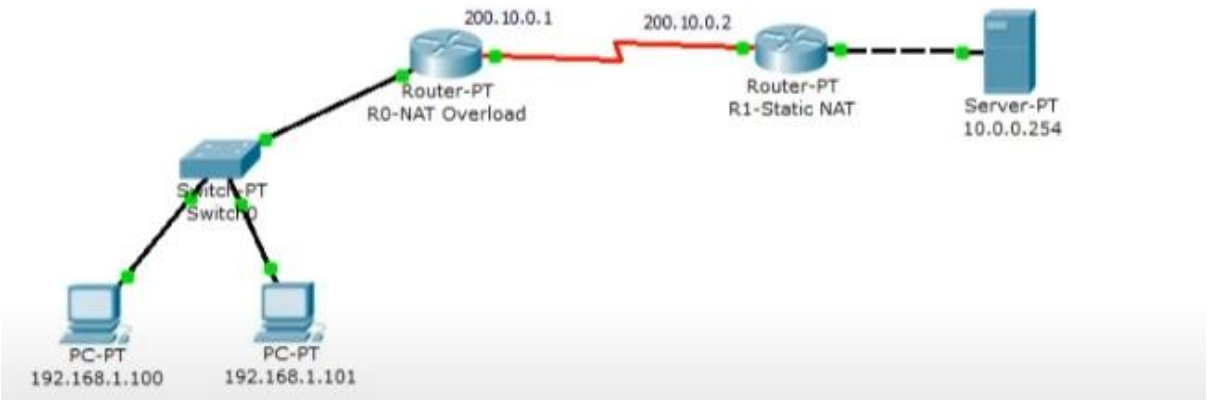

Command Prompt
Reply from 192.168.10.10: bytes=32 time=2ms TTL=125
Reply from 192.168.10.10: bytes=32 time=2ms TTL=125
Reply from 192.168.10.10: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms
PC>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.10: bytes=32 time=2ms TTL=126
Reply from 192.168.10.10: bytes=32 time=3ms TTL=126
Reply from 192.168.10.10: bytes=32 time=3ms TTL=126
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
PC>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=20ms TTL=126

LAB 6

ARYAMAN MISHRA

19BCE1027

NAT AND PAT



To assign IP address in Laptop click Laptop and click Desktop and IP configuration and Select Static and set IP address.

Two interfaces of Router1 are used in topology; FastEthernet0/0 and Serial 0/0/0.

By default interfaces on router are remain administratively down during the start up. We need to configure IP address and other parameters on interfaces before we could actually use them for routing. Interface mode is used to assign the IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

Router>enable

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Before we configure IP address in interfaces let's assign a unique descriptive name to router.

Router(config)#hostname R1

R1#

Now execute the following commands to set IP address in FastEthernet 0/0 interface.

R1(config)#interface FastEthernet0/0

R1(config-if)#ip address 10.0.0.1 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit

interface FastEthernet 0/0 command is used to enter in interface mode.

ip address 10.0.0.1 255.0.0.0 command assigns IP address to interface.

no shutdown command is used to bring the interface up.

exit command is used to return in global configuration mode.

Serial interface needs two additional parameters clock rate and bandwidth. Every serial cable has two ends DTE and DCE. These parameters are always configured at DCE end.

We can use show controllers interface command from privilege mode to check the cable's end.

R1(config)#exit

R1#show controllers serial 0/0/0

Interface Serial0/0/0

Hardware is PowerQUICC MPC860

DCE V.35, clock rate 2000000

[Output omitted]

Fourth line of output confirms that DCE end of serial cable is attached. If you see DTE here instead of DCE skip these parameters.

Now we have necessary information let's assign IP address to serial interface.

R1#configure terminal

R1(config)#interface Serial0/0/0

R1(config-if)#ip address 100.0.0.1 255.0.0.0

R1(config-if)#clock rate 64000

R1(config-if)#bandwidth 64

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#

Router#configure terminal Command is used to enter in global configuration mode.

Router(config)#interface serial 0/0/0 Command is used to enter in interface mode.

Router(config-if)#ip address 100.0.0.1 255.0.0.0 Command assigns IP address to interface.

Router(config-if)#clock rate 64000

In real life environment this parameter controls the data flow between serial links and need to be set at service provider's end. In lab environment we need not to worry about this value. We can use any valid rate here.

Router(config-if)#bandwidth 64

Bandwidth works as an influencer. It is used to influence the metric calculation of EIGRP or any other routing protocol which uses bandwidth parameter in route selection process.

Router(config-if)#no shutdown Command brings interface up.

Router(config-if)#exit Command is used to return in global configuration mode.

We will use same commands to assign IP addresses on interfaces of Router2. We need to provided clock rate and bandwidth only on DCE side of serial interface. Following command will assign IP addresses on interface of Router2.

Initial IP configuration in R2

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#interface FastEthernet0/0

R2(config-if)#ip address 192.168.1.1 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface Serial0/0/0

R2(config-if)#ip address 100.0.0.2 255.0.0.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#

That's all initial IP configuration we need. Now this topology is ready for the practice of static nat.

Configure Static NAT

Static NAT configuration requires three steps: -

Define IP address mapping

Define inside local interface

Define inside global interface

Since static NAT use manual translation, we have to map each inside local IP address (which needs a translation) with inside global IP address. Following command is used to map the inside local IP address with inside global IP address.

Router(config)#ip nat inside source static [inside local ip address] [inside global IP address]

For example in our lab Laptop1 is configured with IP address 10.0.0.10. To map it with 50.0.0.10 IP address we will use following command

Router(config)#ip nat inside source static 10.0.0.10 50.0.0.10

In second step we have to define which interface is connected with local the network. On both routers interface Fa0/0 is connected with the local network which need IP translation.

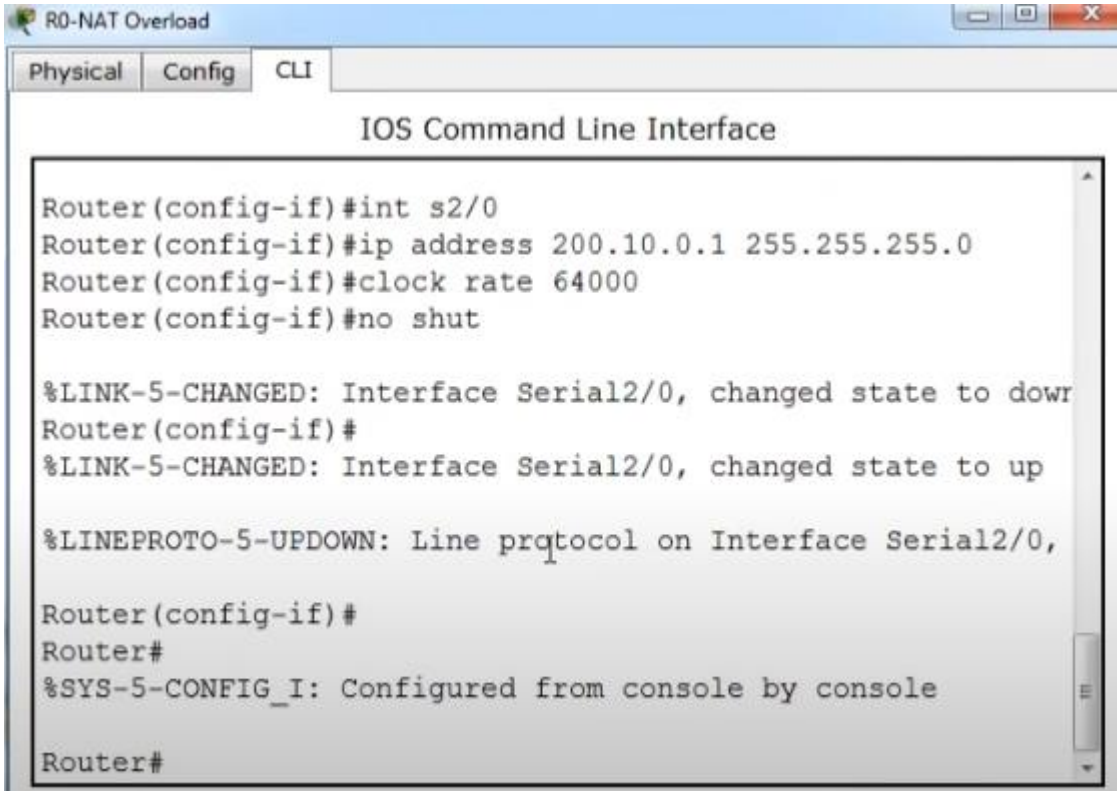
Following command will define interface Fa0/0 as inside local.

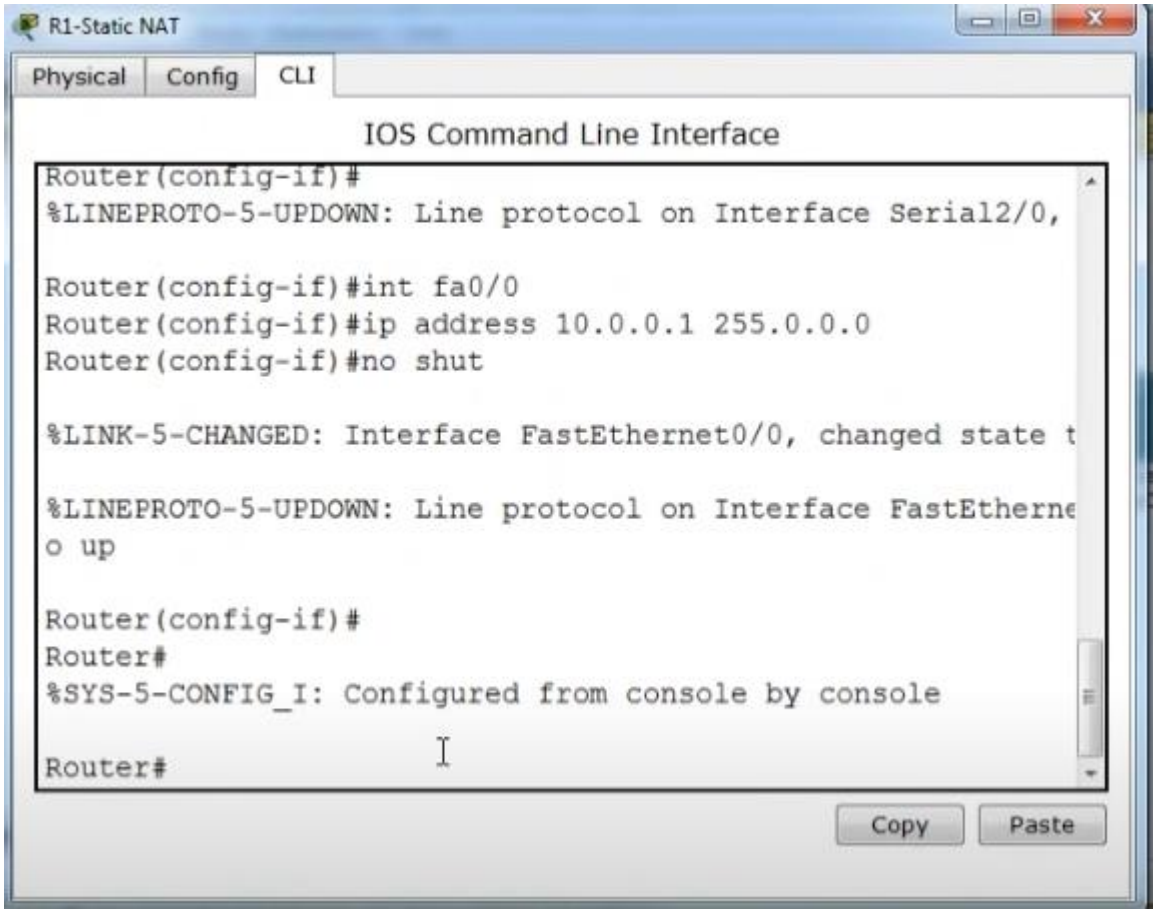
Router(config-if)#ip nat inside

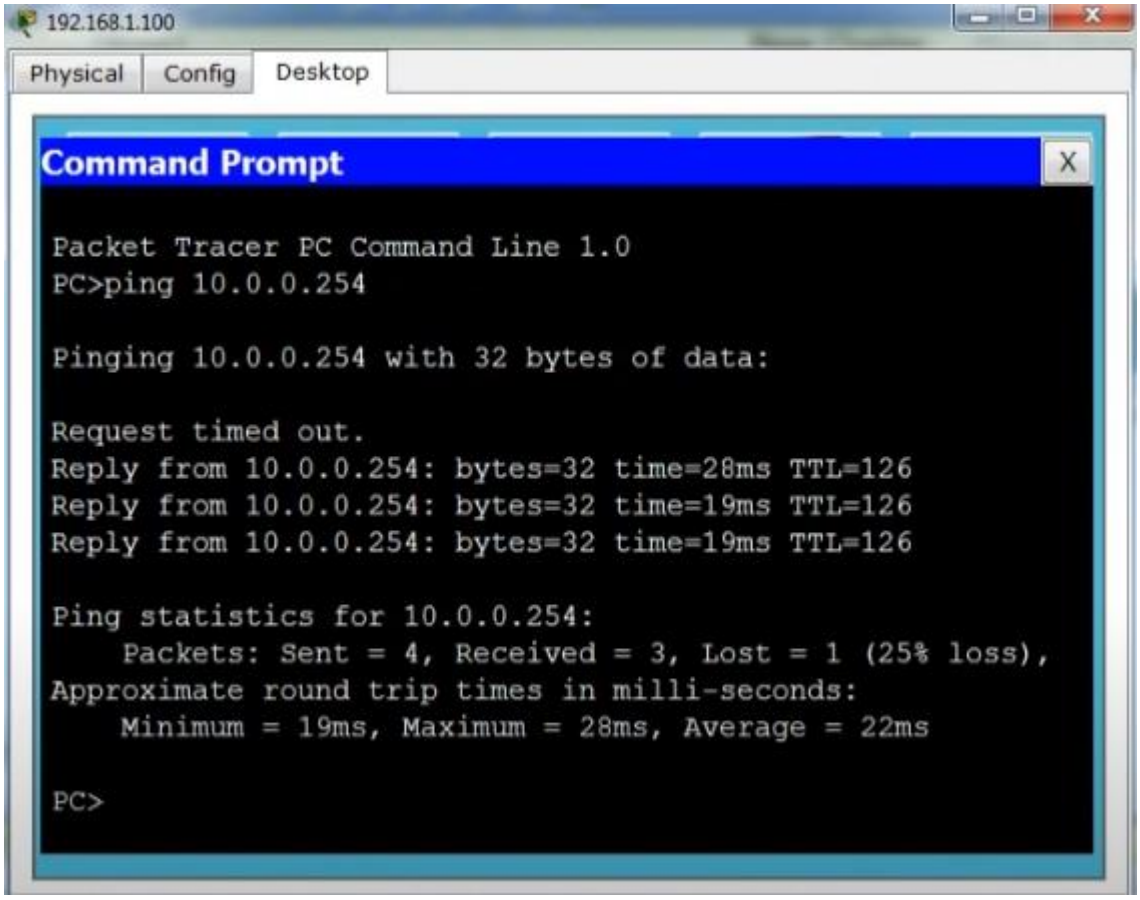
In third step we have to define which interface is connected with the global network. On both routers serial 0/0/0 interface is connected with the global network. Following command will define interface Serial0/0/0 as inside global.

Router(config-if)#ip nat outside

Following figure illustrates these terms.




R1-Static NAT
Physical
Config
CLI
IOS Command Line Interface
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0,
Router(config-if)#int fa0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state t
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
o up
Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Copy
Paste



Let's implement all these commands together and configure the static NAT.

R1 Static NAT Configuration

R1(config)#ip nat inside source static 10.0.0.10 50.0.0.10

R1(config)#interface FastEthernet 0/0

R1(config-if)#ip nat inside

R1(config-if)#exit

R1(config)#

R1(config)#interface Serial 0/0/0

R1(config-if)#ip nat outside

R1(config-if)#exit

For testing purpose I configured only one static translation. You may use following commands to configure the translation for remaining address.

R1(config)#ip nat inside source static 10.0.0.20 50.0.0.20

R1(config)#ip nat inside source static 10.0.0.30 50.0.0.30

R2 Static NAT Configuration

R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10

R2(config)#interface FastEthernet 0/0

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#

R2(config)#interface Serial 0/0/0

R2(config-if)#ip nat outside

R2(config-if)#exit

Before we test this lab we need to configure the IP routing. IP routing is the process which allows router to route the packet between different networks. Following tutorial explain routing in detail with examples

Routing concepts Explained with Examples

Configure static routing in R1

R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2

Configure static routing in R2

R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1

Testing Static NAT Configuration

In this lab we configured static NAT on R1 and R2. On R1 we mapped inside local IP address 10.0.0.10 with inside global address 50.0.0.10 while on R2 we mapped inside local IP address 192.168.1.10 with inside global IP address 200.0.0.10.

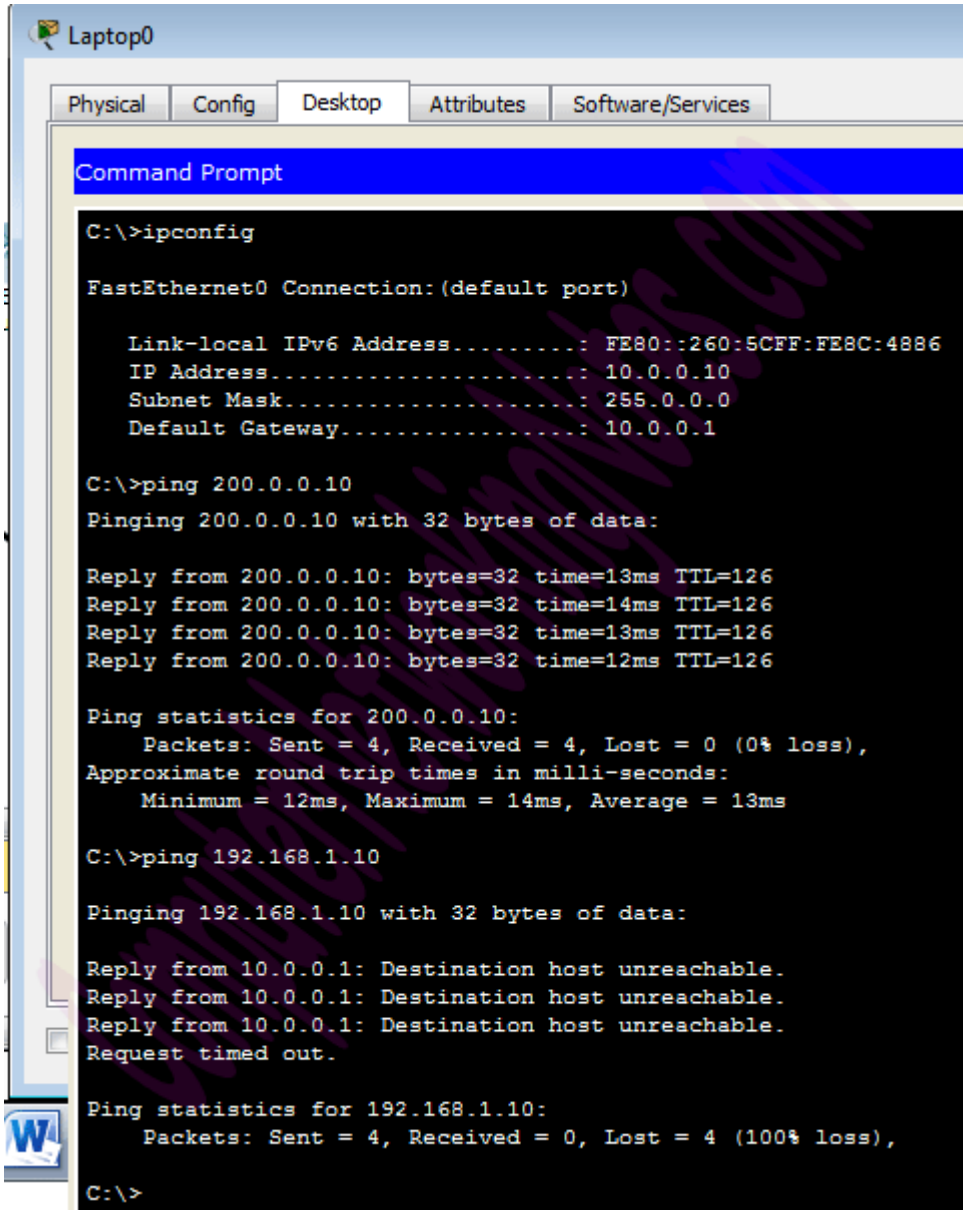
Device	Inside Local IP Address	Inside Global IP Ad
Laptop0	10.0.0.10	50.0.0.10
Server	192.168.1.10	200.0.0.10

To test this setup click Laptop0 and Desktop and click Command Prompt.

Run **ipconfig** command.

Run **ping 200.0.0.10** command.

Run **ping 192.168.1.10** command.

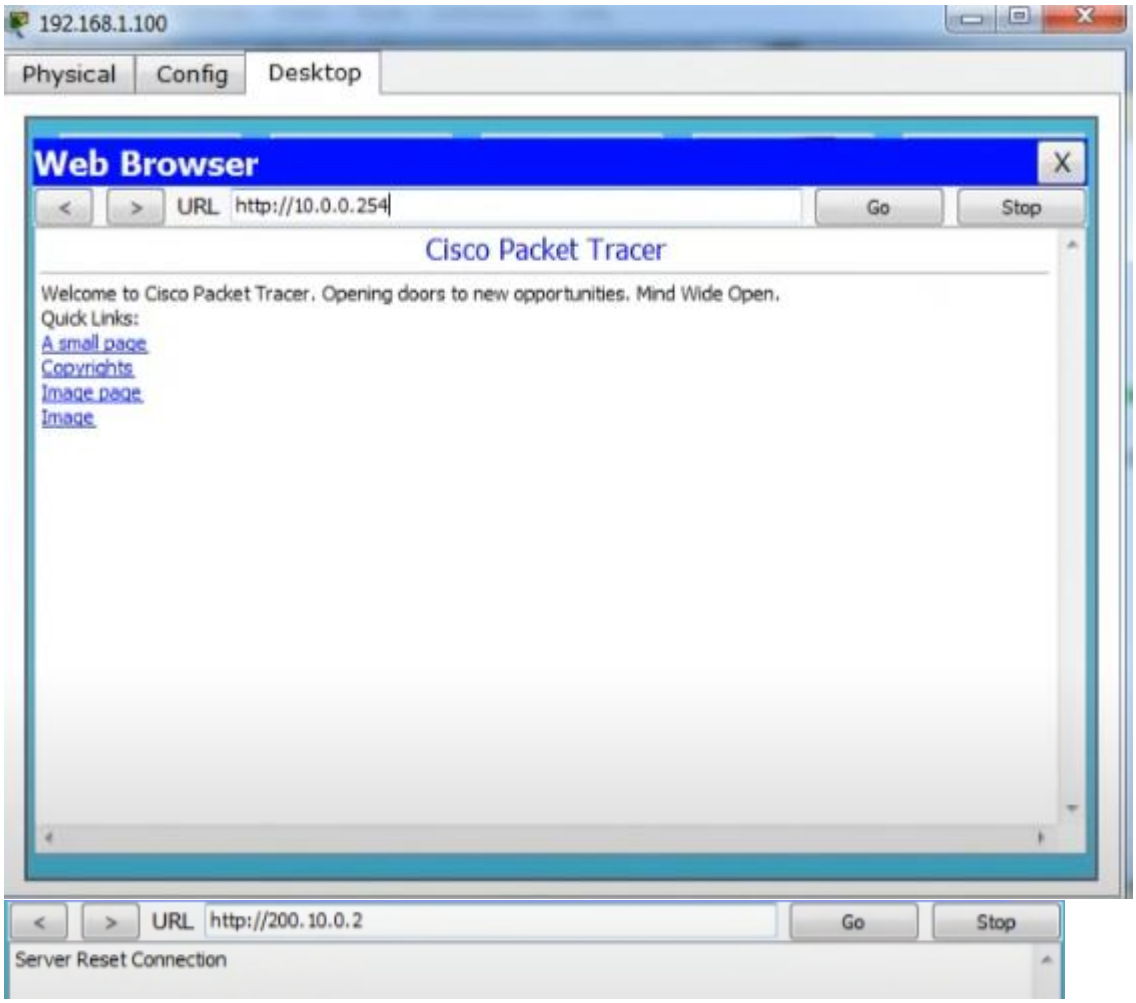


First command verifies that we are testing from correct NAT device.

Second command checks whether we are able to access the remote device or not. A ping reply confirms that we are able to connect with remote device on this IP address.

Third command checks whether we are able to access the remote device on its actual IP address or not. A ping error confirms that we are not able to connect with remote device on this IP address.

Let's do one more testing. Click **Laptop0** and click **Desktop** and click **Web Browser** and access 200.0.0.10.



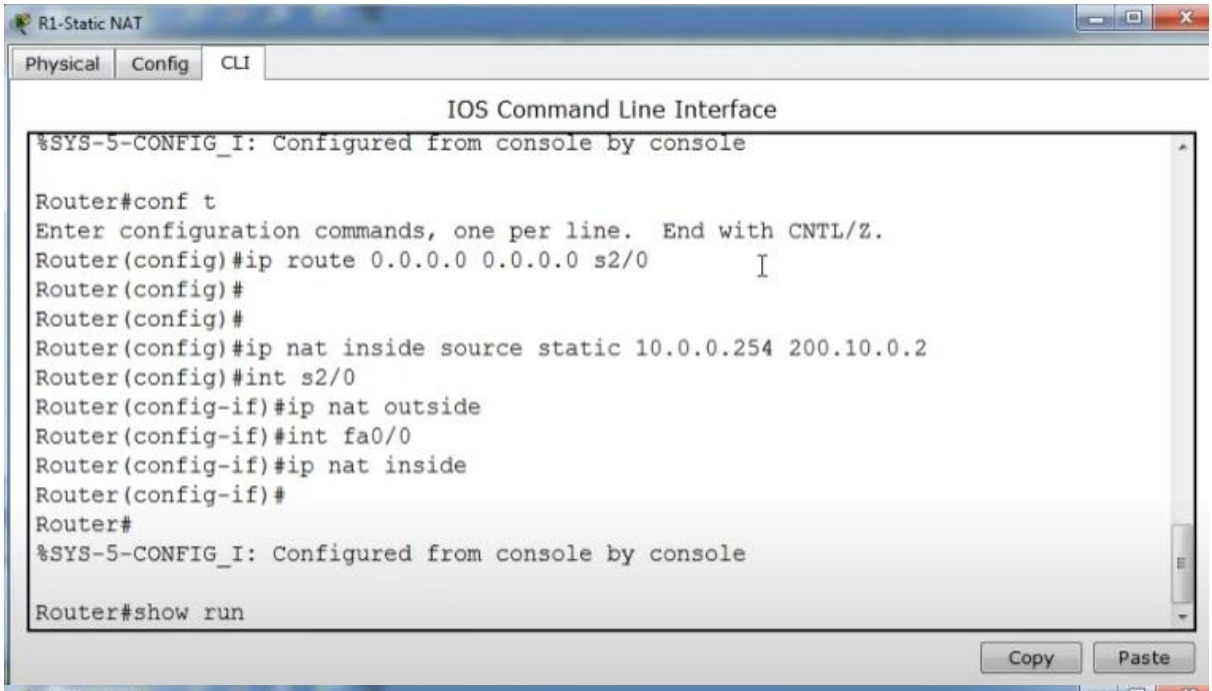
We can also verify this translation on router with **show ip nat translation** command.

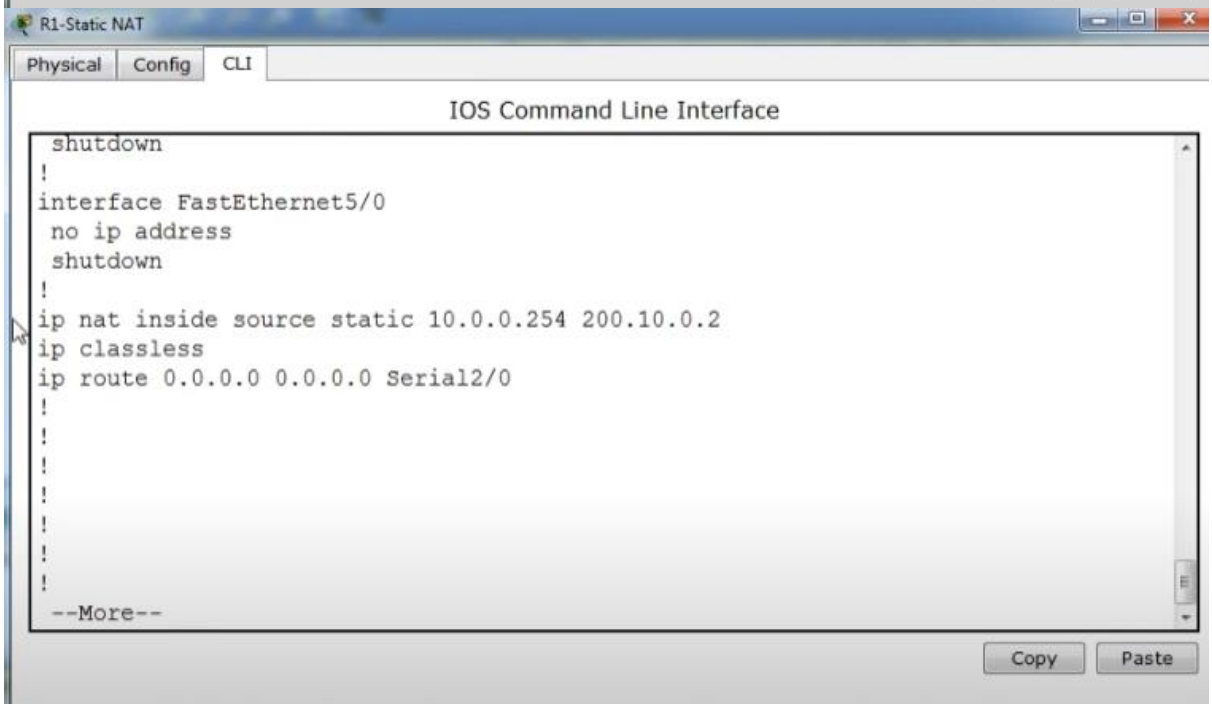
Following figure illustrate this translation on router R1.

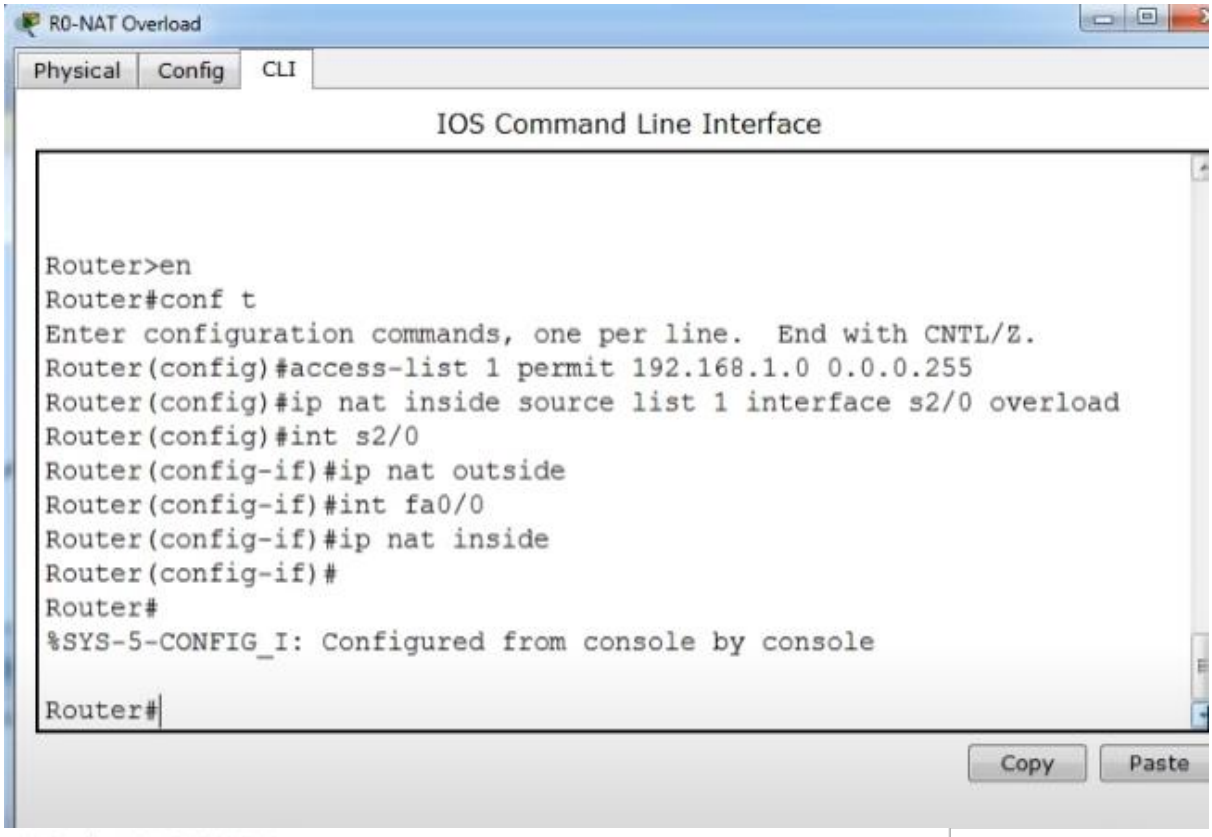
```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 50.0.0.10:13      10.0.0.10:13       200.0.0.10:13      200.0.0.10:13
icmp 50.0.0.10:14      10.0.0.10:14       200.0.0.10:14      200.0.0.10:14
icmp 50.0.0.10:15      10.0.0.10:15       200.0.0.10:15      200.0.0.10:15
icmp 50.0.0.10:16      10.0.0.10:16       200.0.0.10:16      200.0.0.10:16
tcp 50.0.0.10:1030     10.0.0.10:1030     200.0.0.10:80      200.0.0.10:80
tcp 50.0.0.10:1031     10.0.0.10:1031     200.0.0.10:80      200.0.0.10:80

R1#
```

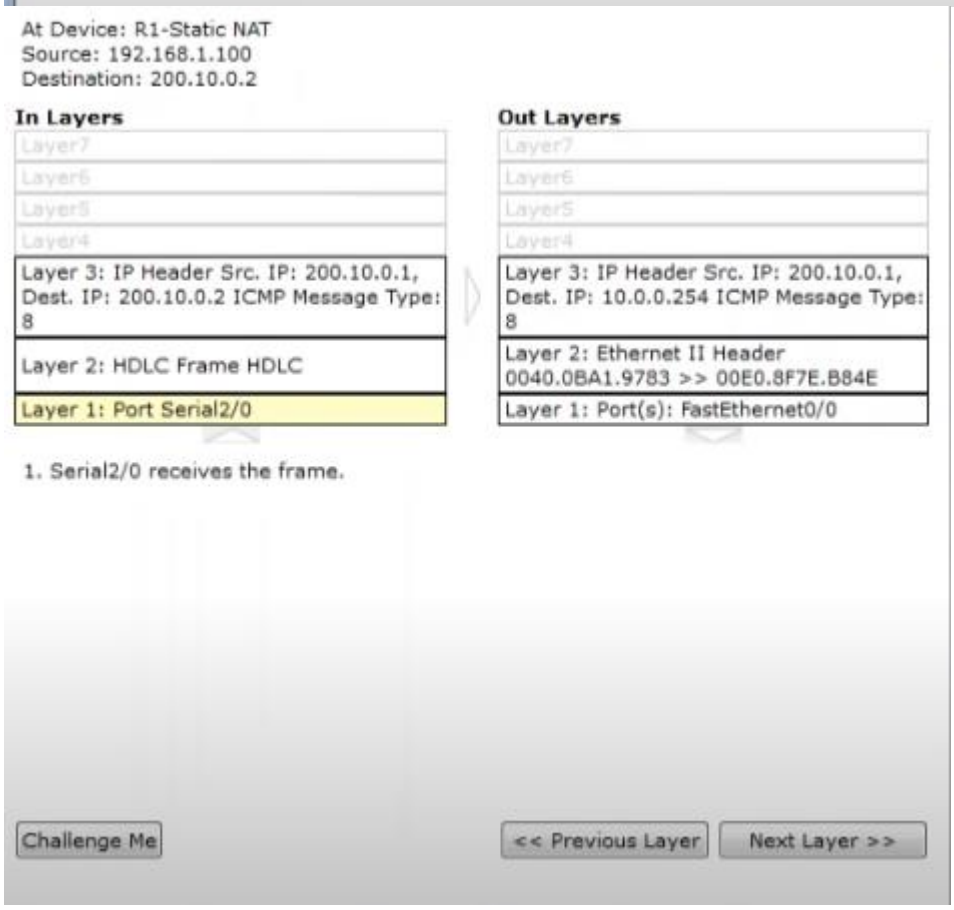
Following figure illustrate this translation on router R2

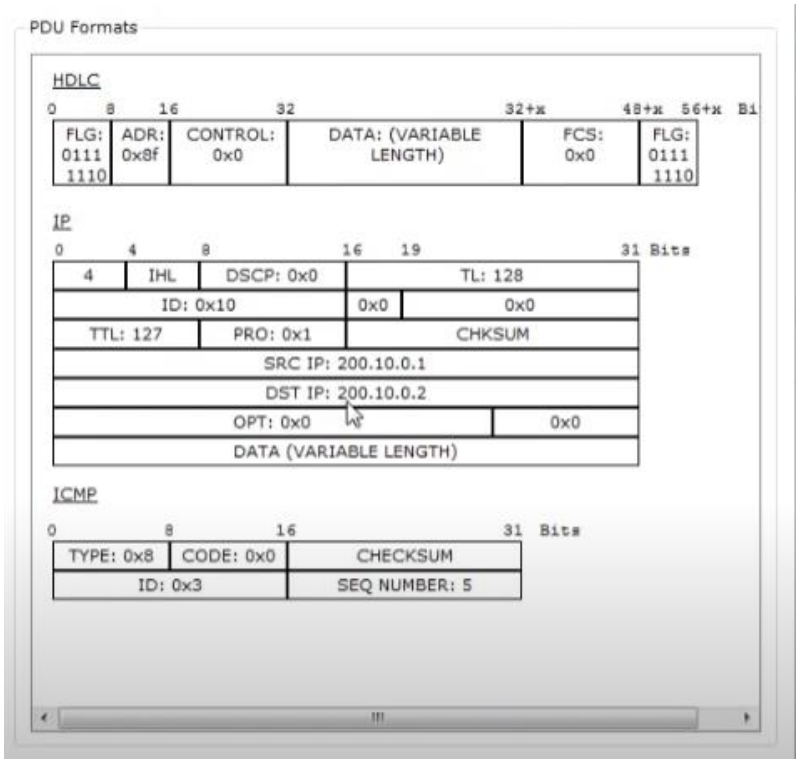
```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.0.0.10:13     192.168.1.10:13    50.0.0.10:13       50.0.0.10:13
icmp 200.0.0.10:14     192.168.1.10:14    50.0.0.10:14       50.0.0.10:14
icmp 200.0.0.10:15     192.168.1.10:15    50.0.0.10:15       50.0.0.10:15
icmp 200.0.0.10:16     192.168.1.10:16    50.0.0.10:16       50.0.0.10:16
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.10:1030     50.0.0.10:1030
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.10:1031     50.0.0.10:1031

R2#
```

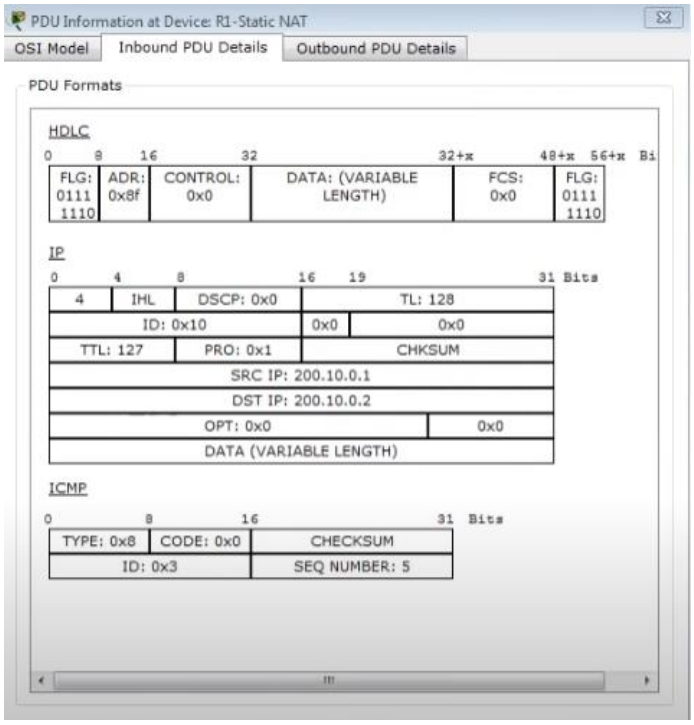





R0-NAT Overload
Physical
Config
CLI
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface s2/0 overload
Router(config)#int s2/0
Router(config-if)#ip nat outside
Router(config-if)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Copy
Paste

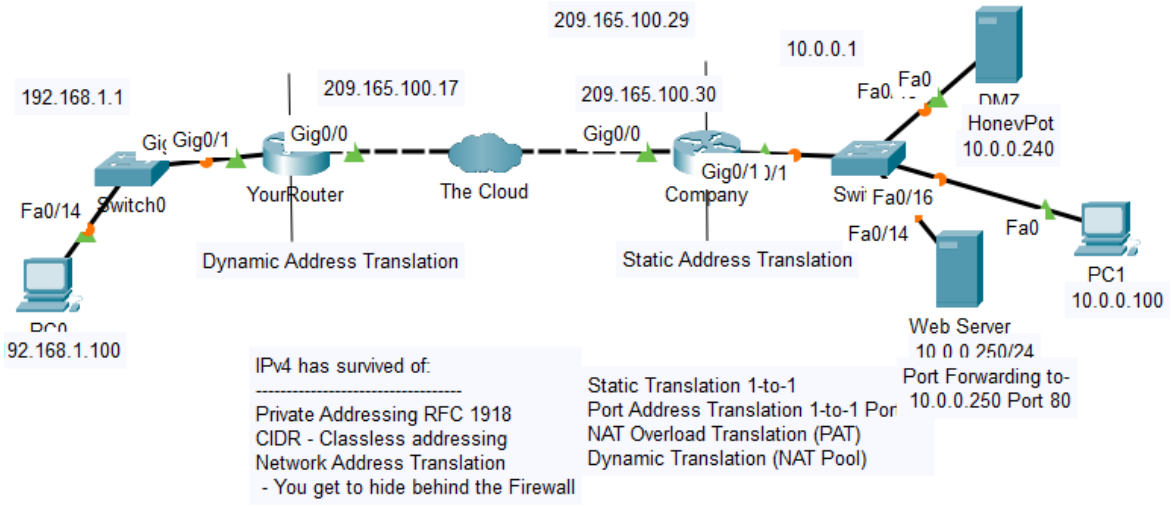

At Device: R1-Static NAT
Source: 192.168.1.100
Destination: 200.10.0.2
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 200.10.0.1, Dest. IP: 200.10.0.2 ICMP Message Type: 8
Layer 2: HDLC Frame HDLC
Layer 1: Port Serial2/0
Layer 3: IP Header Src. IP: 200.10.0.1, Dest. IP: 10.0.0.254 ICMP Message Type: 8
Layer 2: Ethernet II Header 0040.0BA1.9783 >> 00E0.8F7E.B84E
Layer 1: Port(s): FastEthernet0/0
1. Serial2/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>



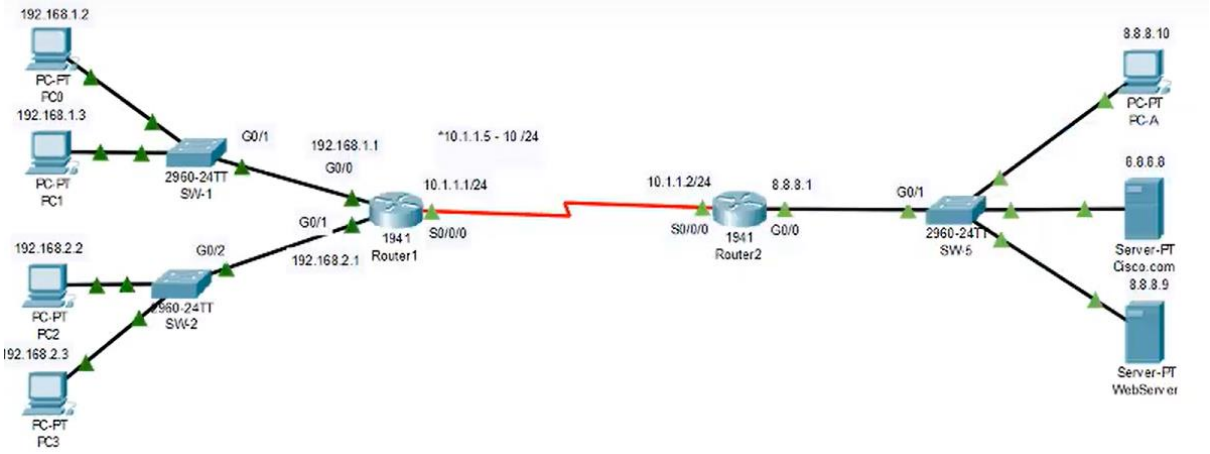


The actual IP address is not listed here because router is receiving packets after the translation. From R1's point of view remote device's IP address is 200.0.0.10 while from R2's point of view end device's IP address is 50.0.0.10.

This way if NAT is enabled we would not be able to trace the actual end device.

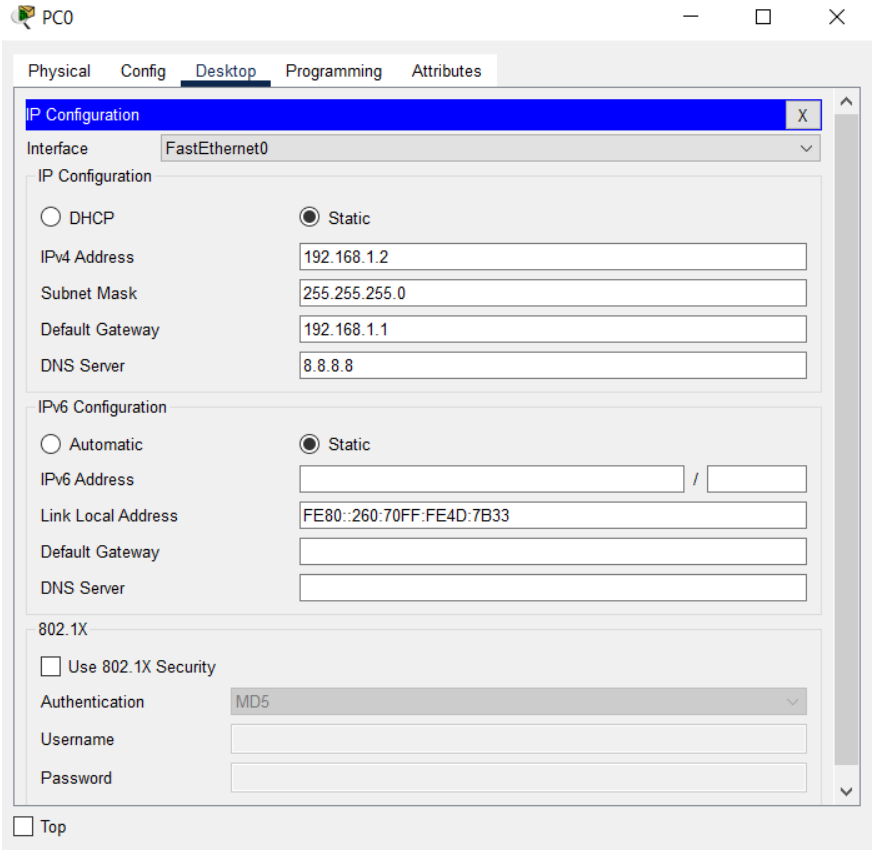


NEW TOPOLOGY

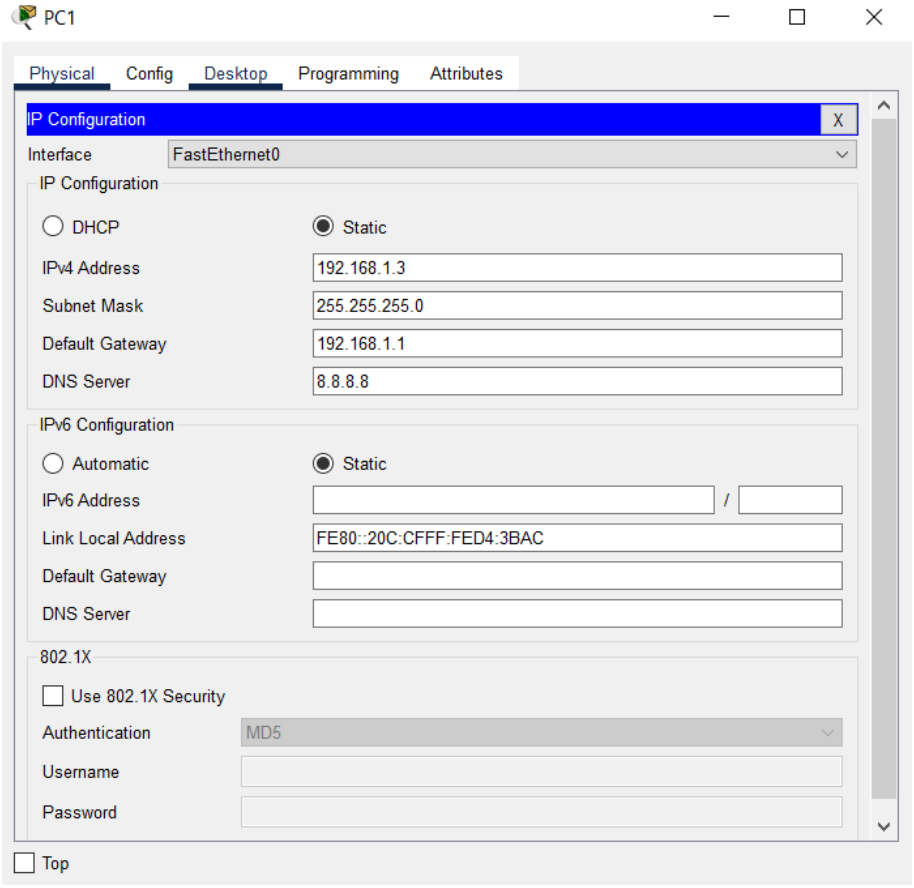


PC configuration

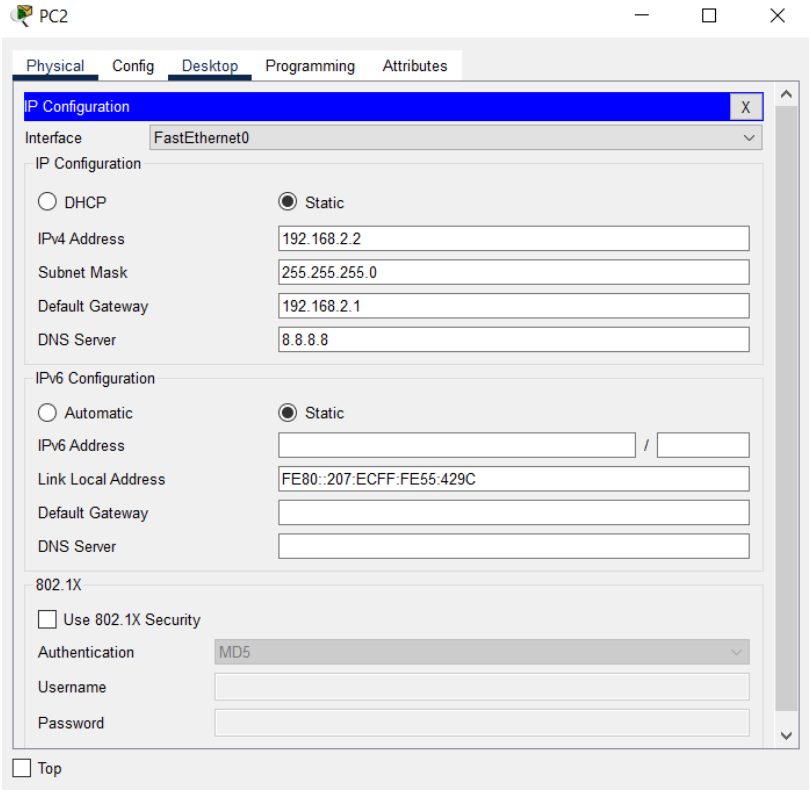
PC0


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:70FF:FE4D:7B33
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

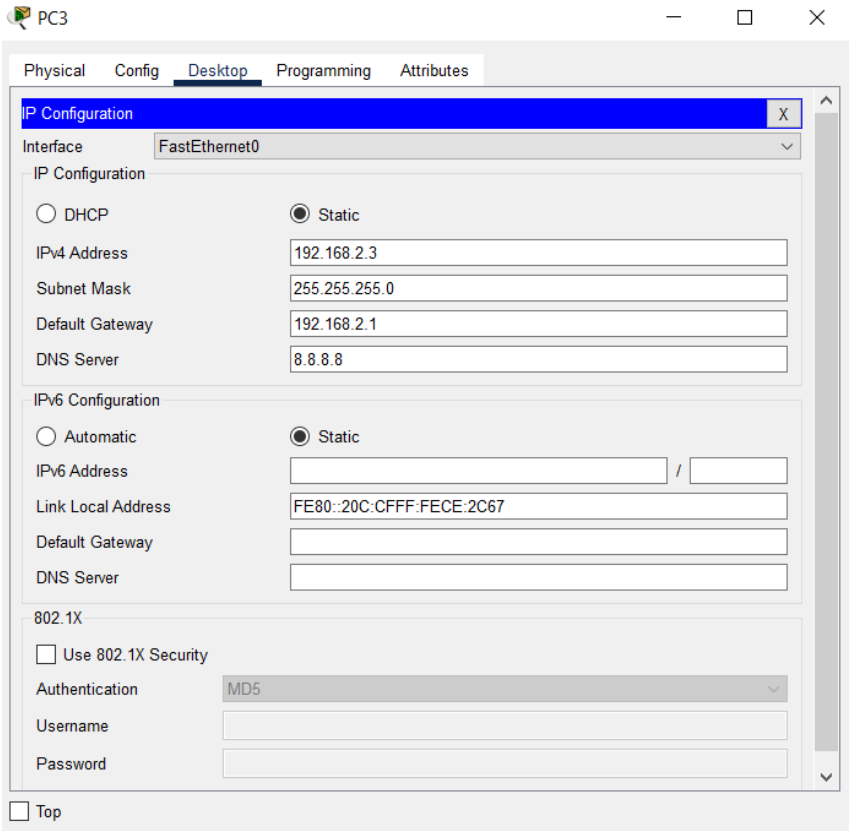
PC1


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20C:CFFF:FED4:3BAC
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

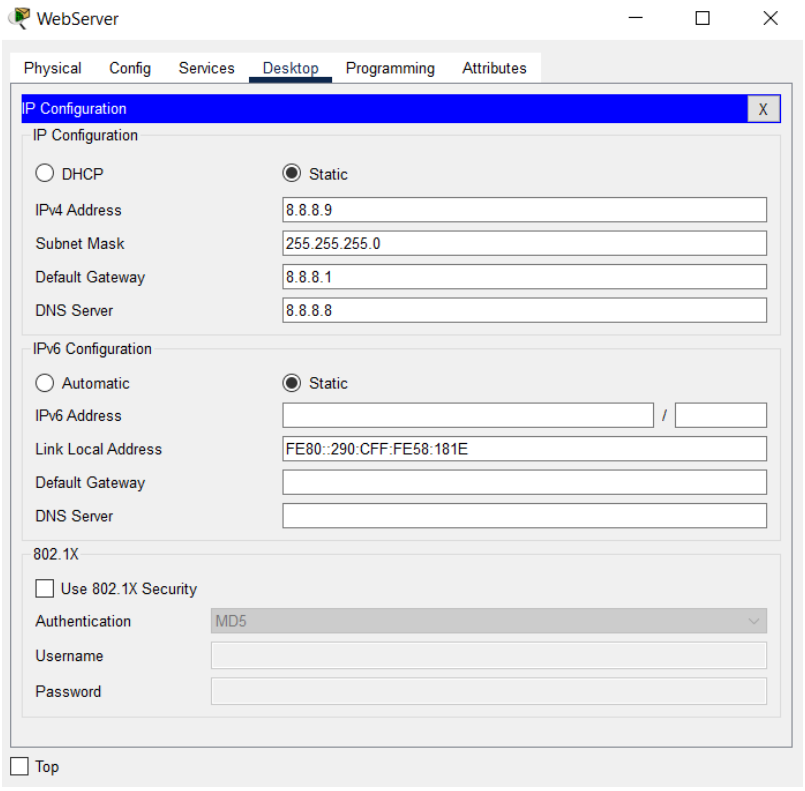
PC2


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::207:ECFF:FE55:429C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

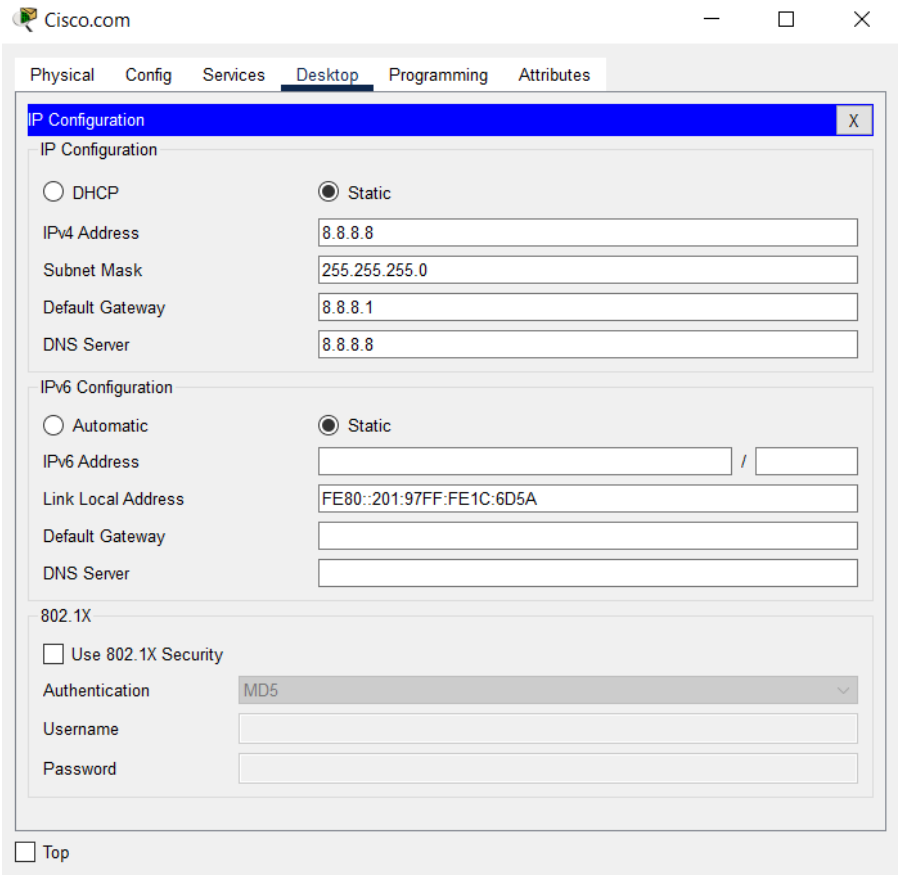
PC3


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20C:CFFF:FECE:2C67
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

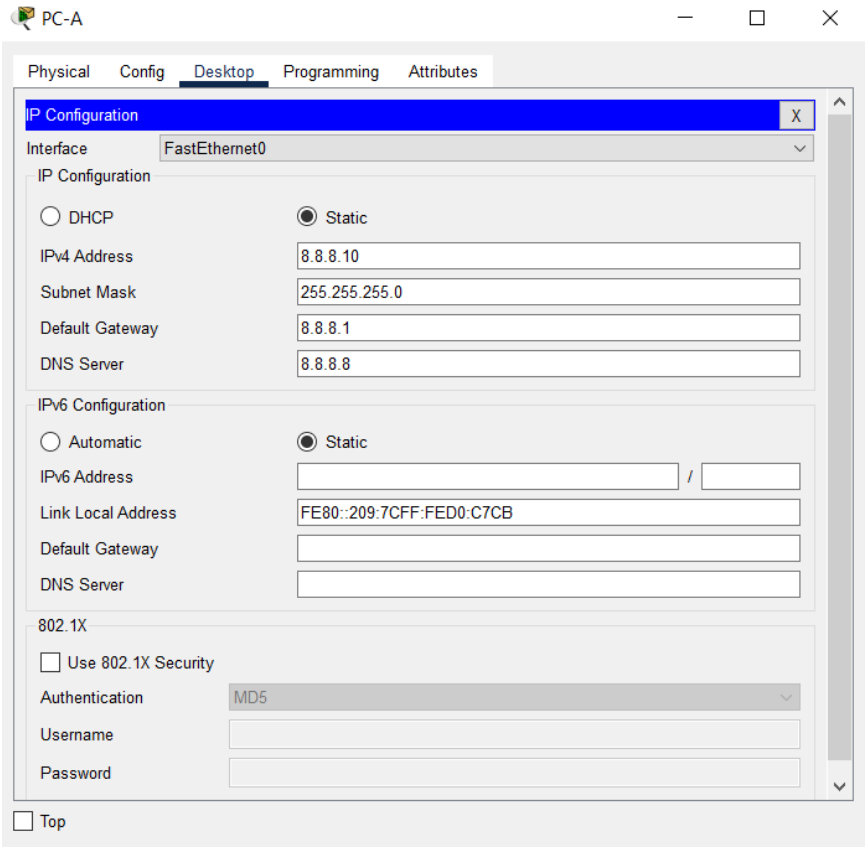
WEB SERVER



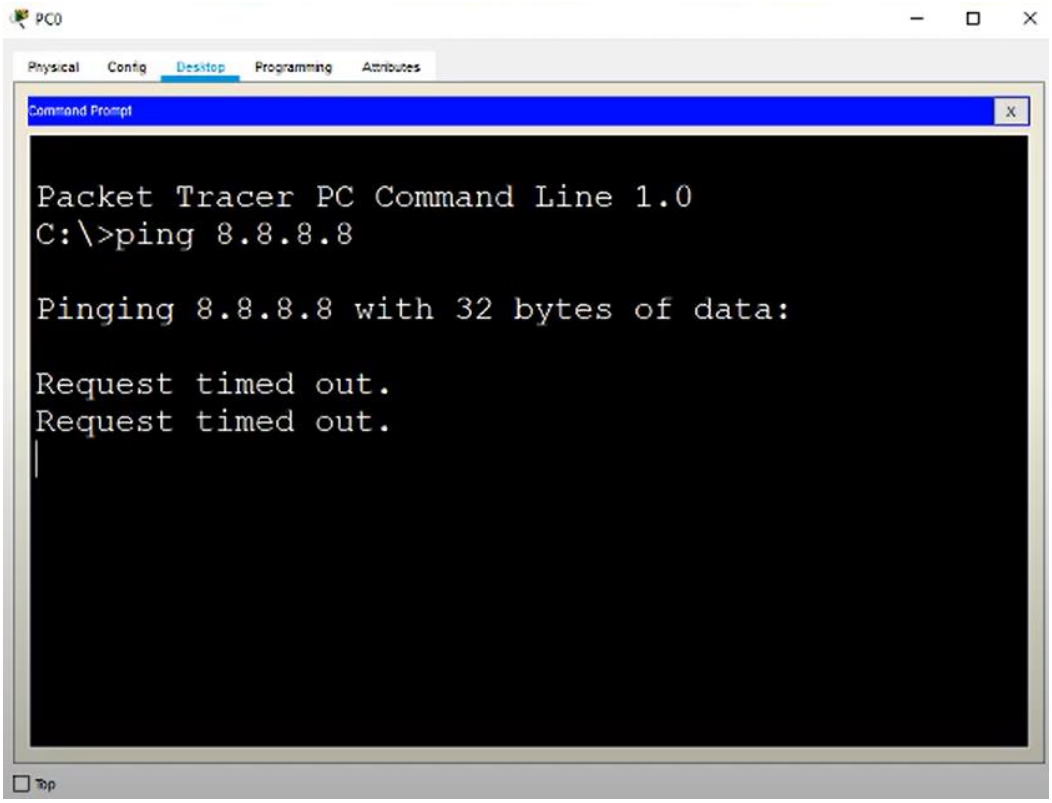
CISCO.COM


Cisco.com
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
8.8.8.8
Subnet Mask
255.255.255.0
Default Gateway
8.8.8.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE1C:6D5A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC-A

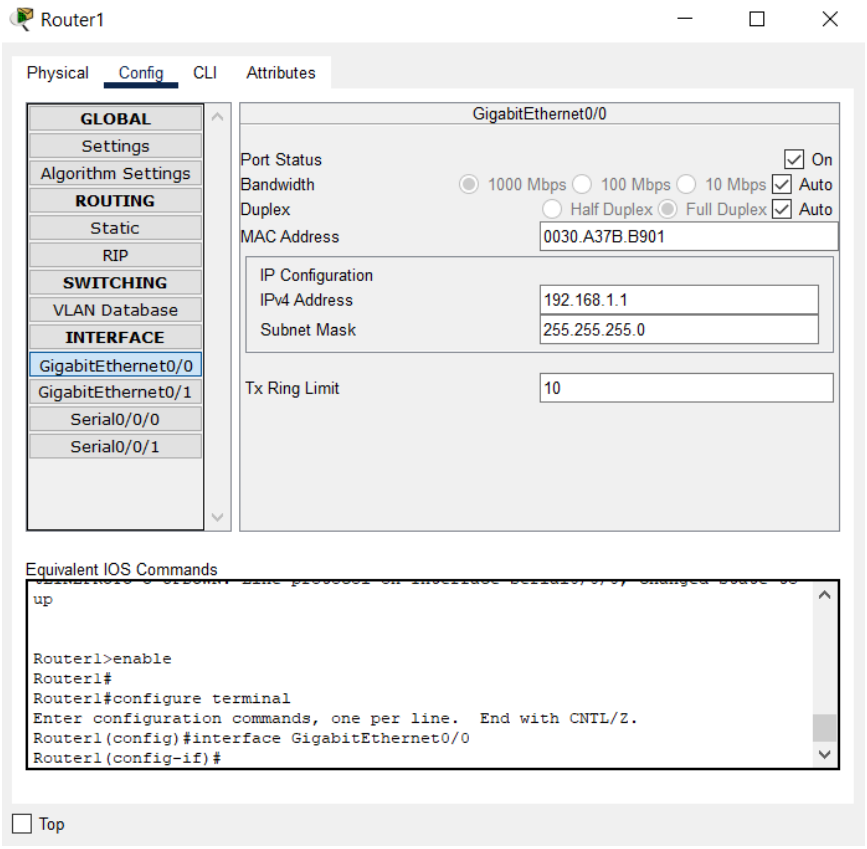


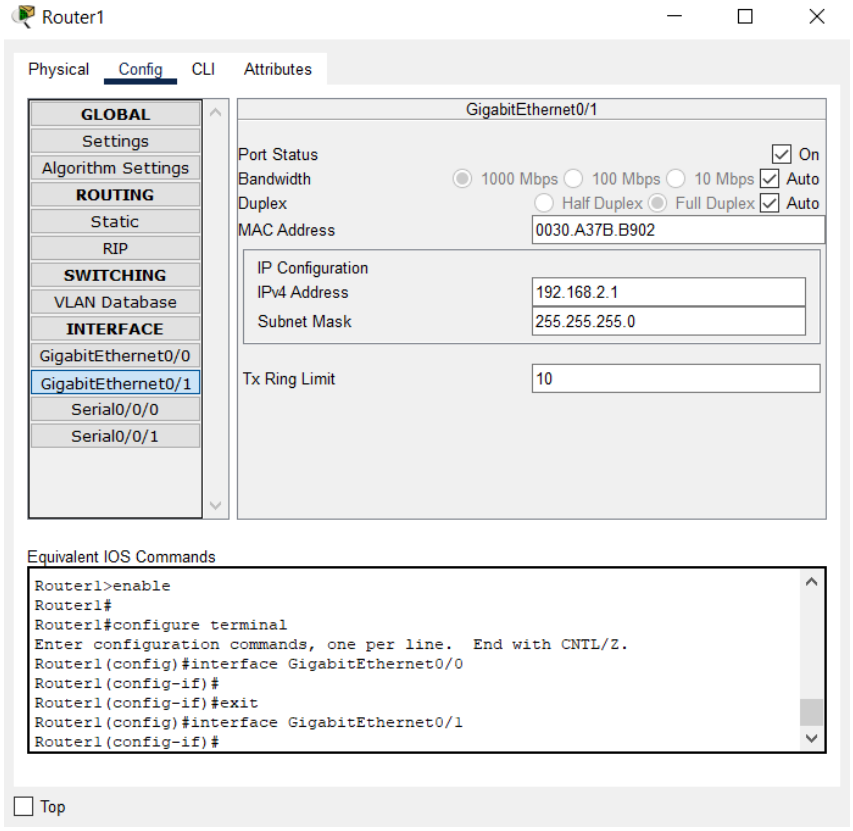
CHECKING THE PING REQUEST

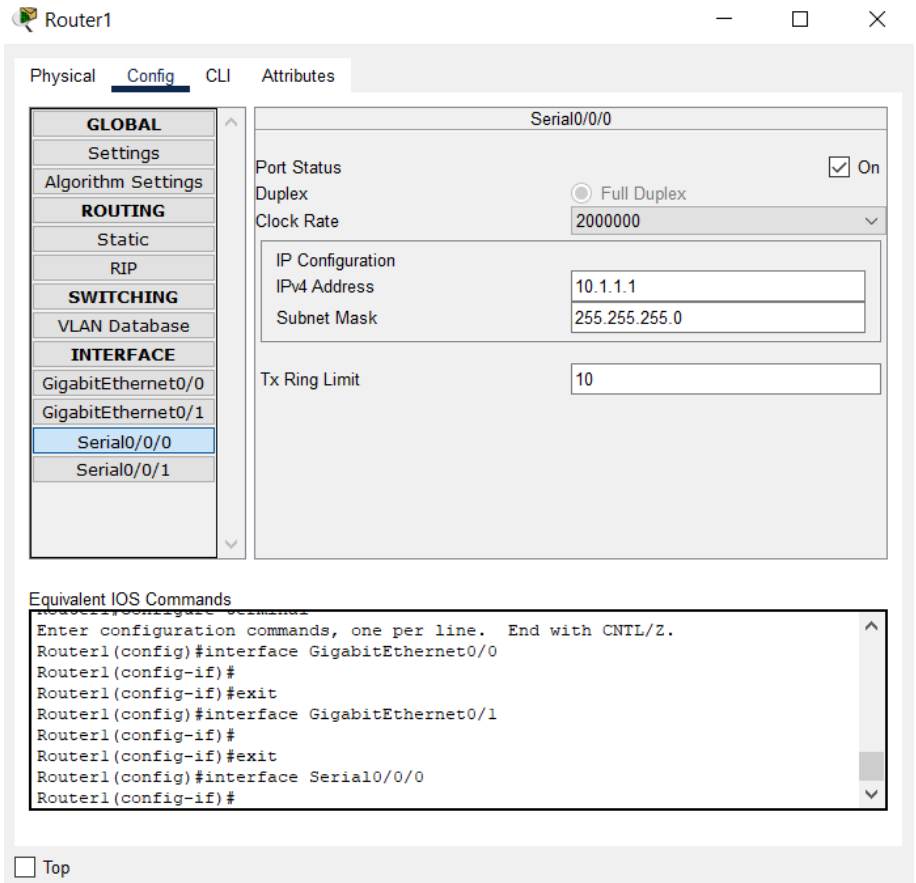


Router 1941(for more switches) configurations

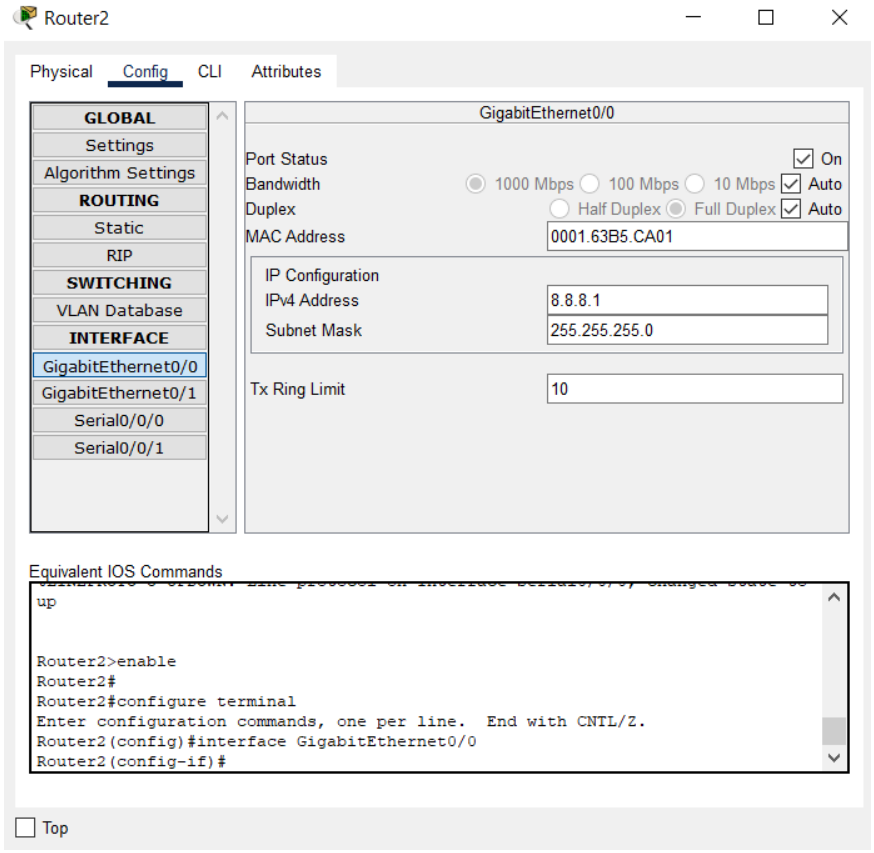
ROUTER 1

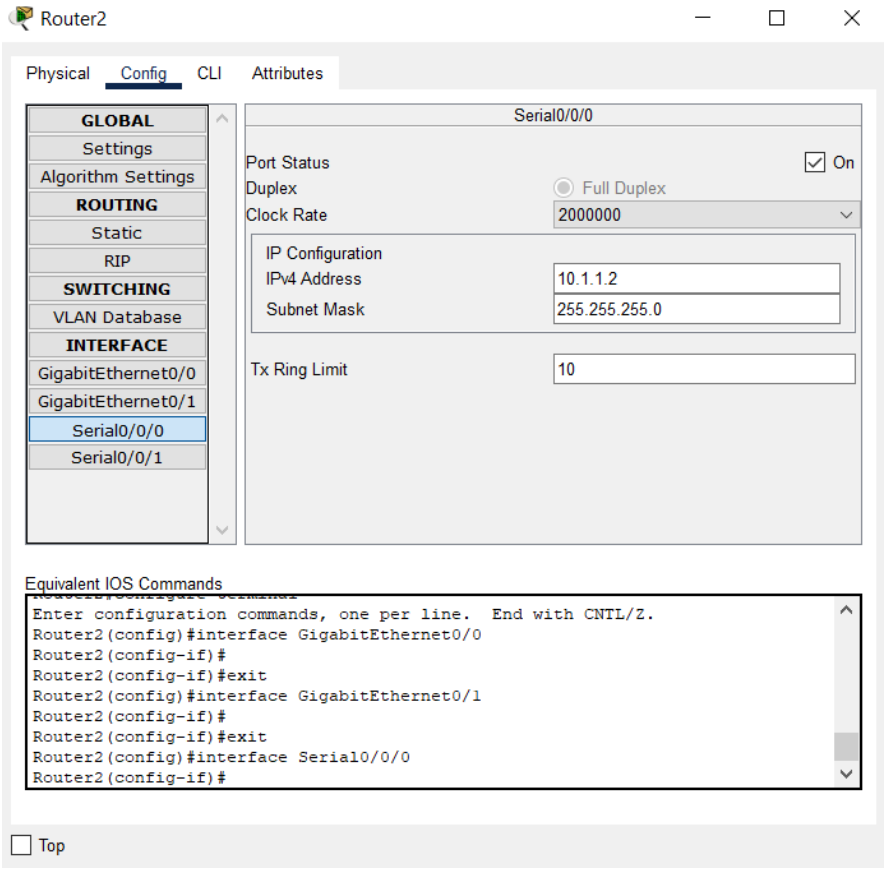



Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0030.A37B.B902
IP Configuration
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router1>enable
Router1#
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.1.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/0/0
Router1(config-if)#
Top

ROUTER 2


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.63B5.CA01
IP Configuration
IPv4 Address
8.8.8.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
up
Router2>enable
Router2#
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#interface GigabitEthernet0/0
Router2(config-if)#
Top



STATIC NAT

NAT of cisco.com device using IP address of 10.1.1.3

Static translation

Commands for static translation

First we mark interfaces as nat outside or nat inside and then using ip nat command to translate public ip address into a private ip address in our case for honeypot.

en

conf t

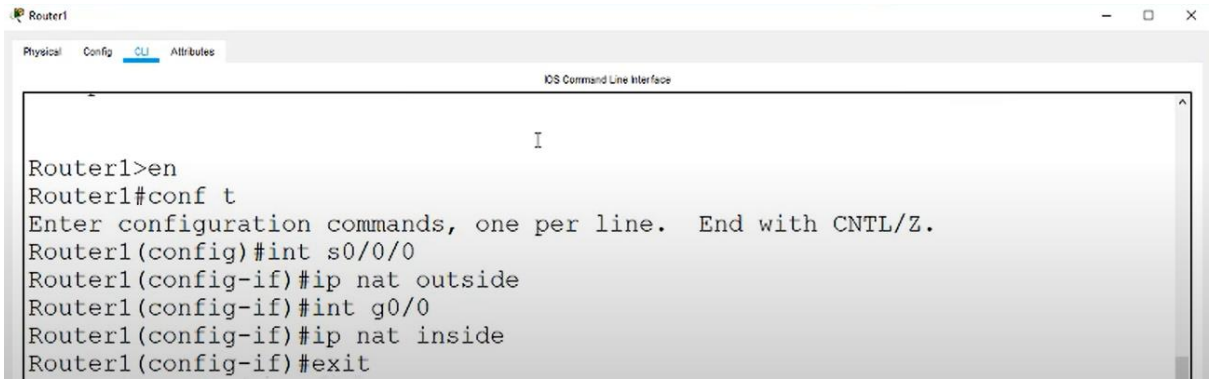
int g0/0

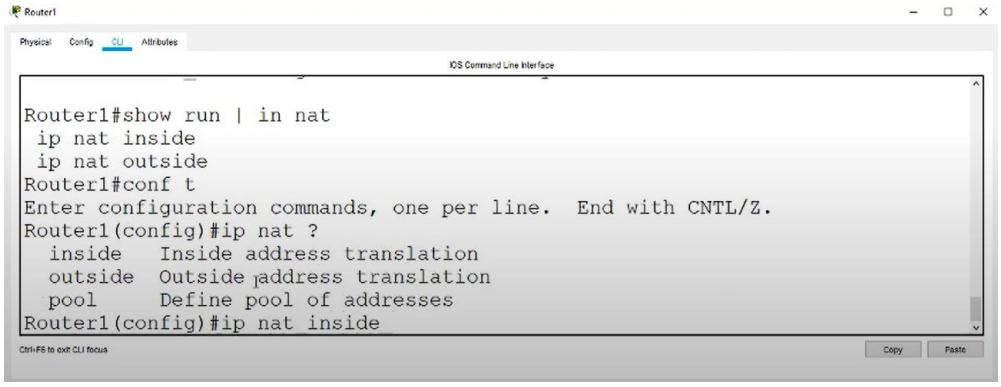
ip nat out

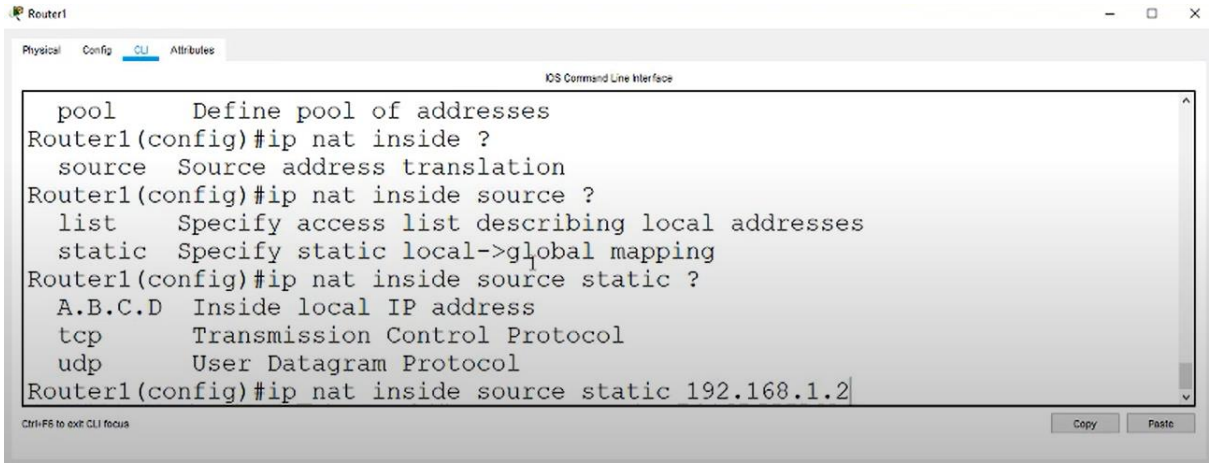
int g0/1

ip nat inside

ip nat inside source static 192.168.1.2 10.1.1.3

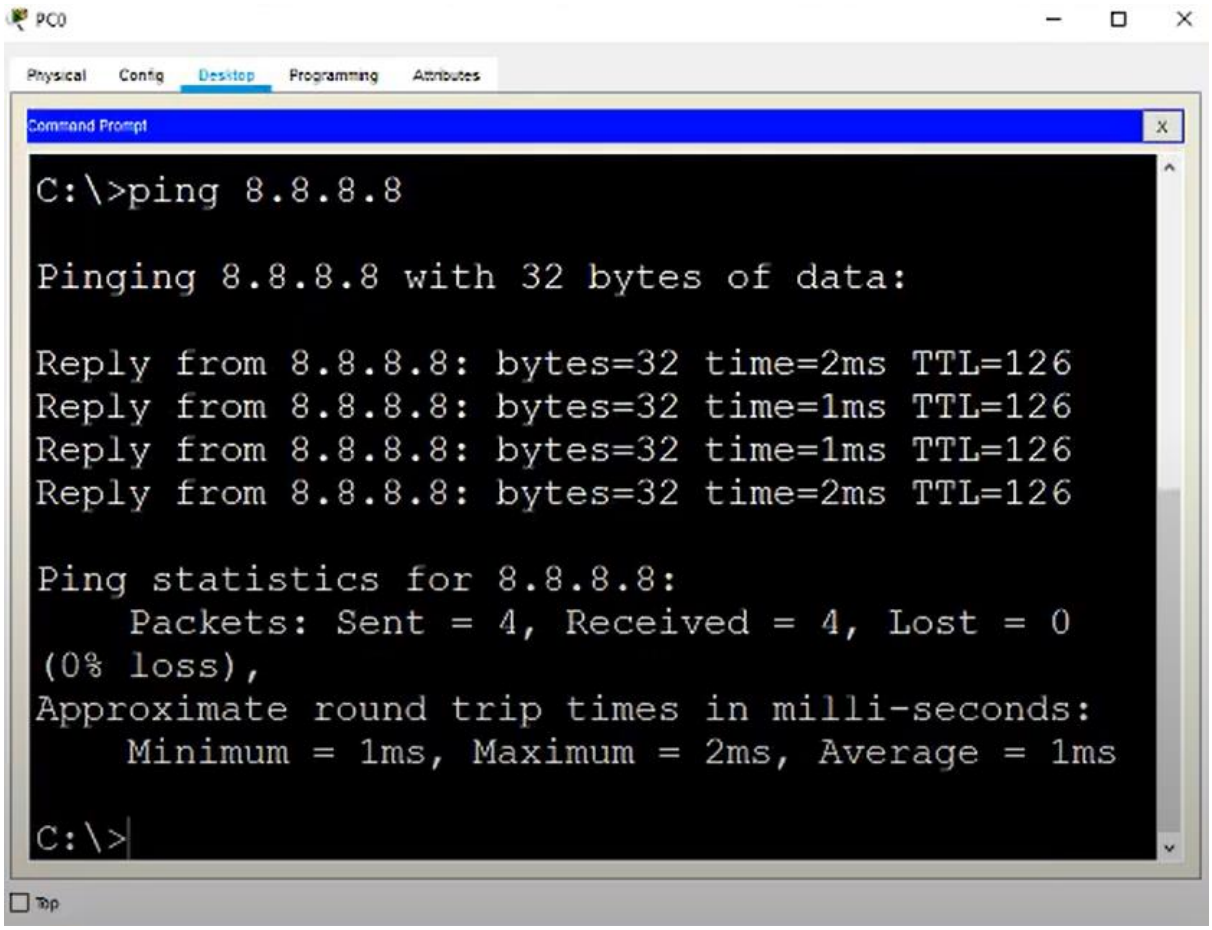




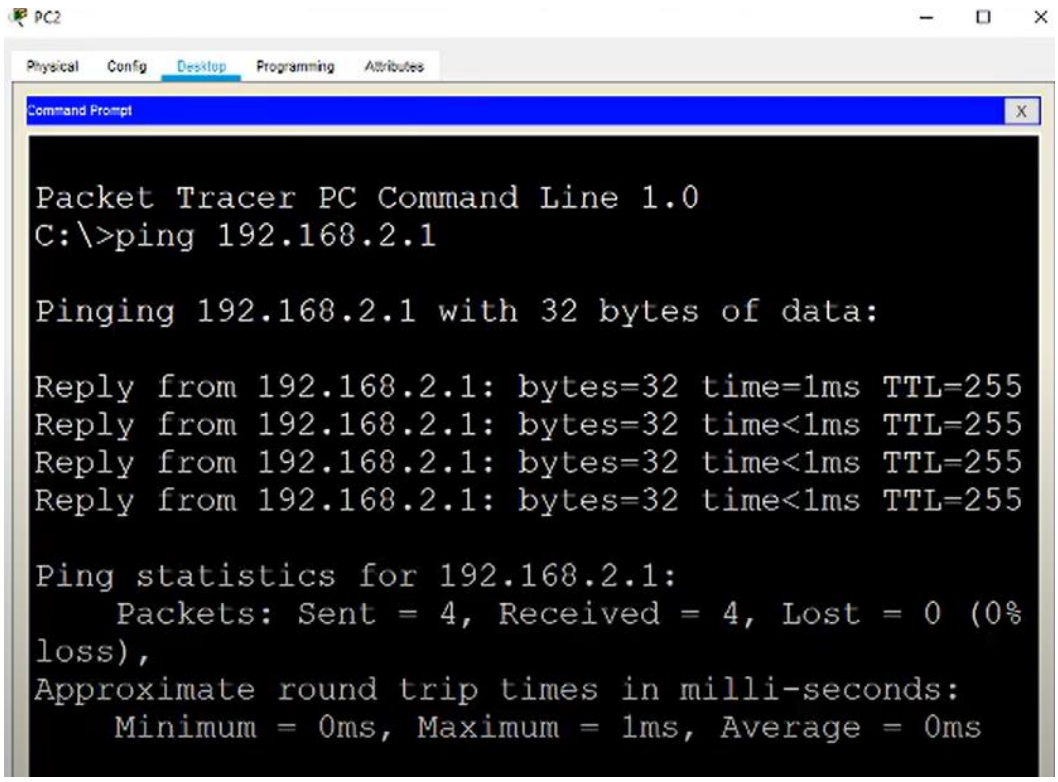


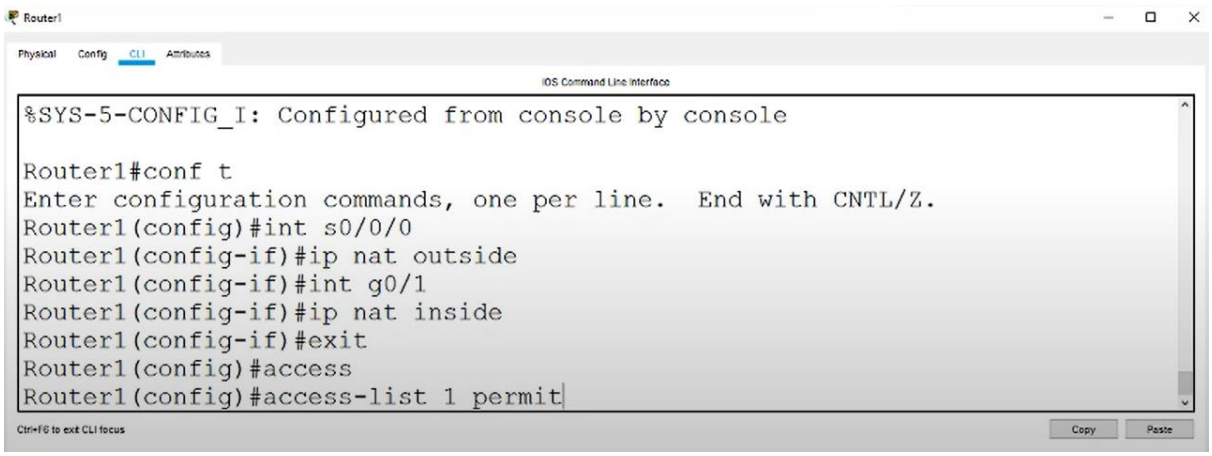
```
Router1(config)#ip nat inside source static 192.168.1.2 ?
  A.B.C.D  Inside global IP address
Router1(config)#ip nat inside source static 192.168.1.2 10.1.1.3
Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#
```

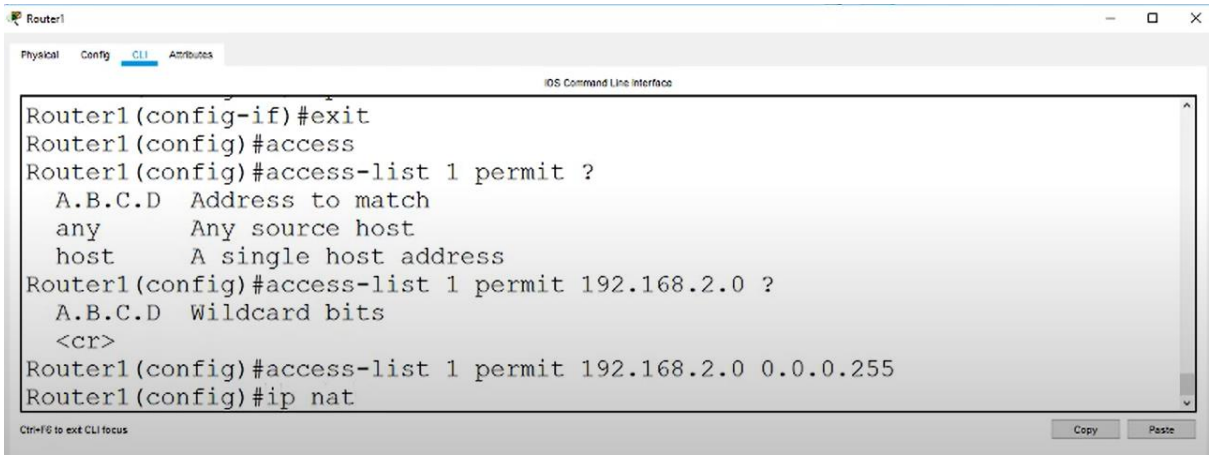
Ctrl+F6 to exit CLI focus | Copy | Paste

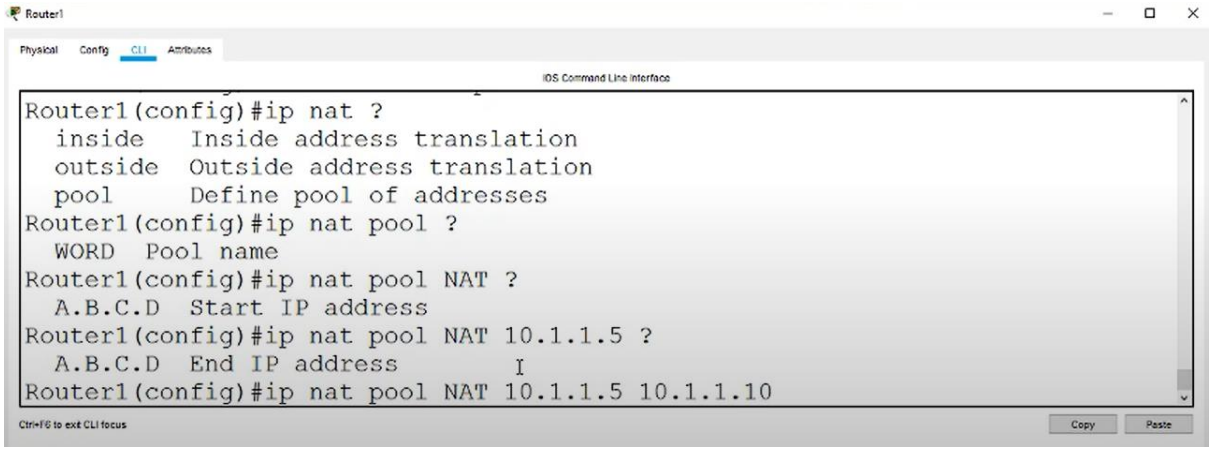


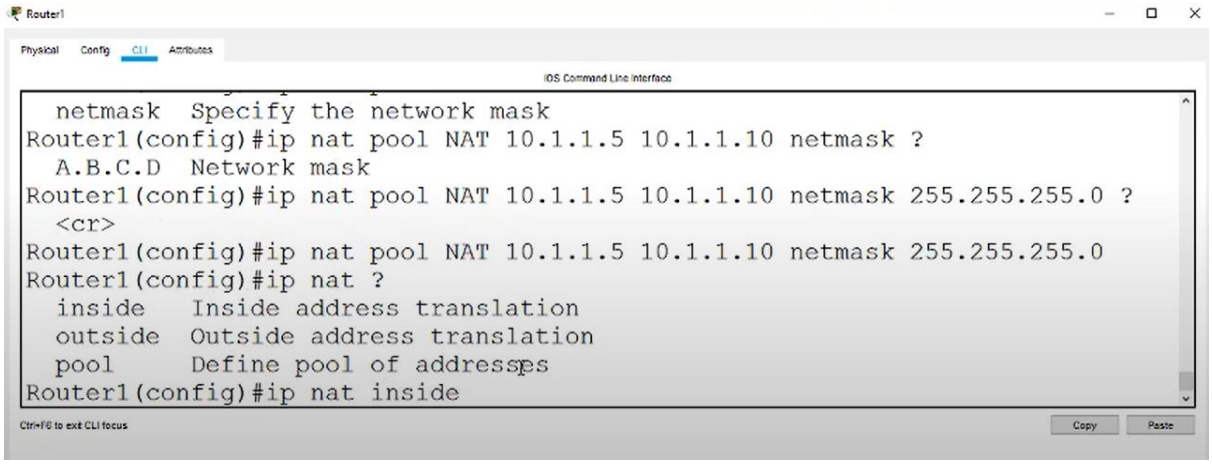
DYNAMIC NAT

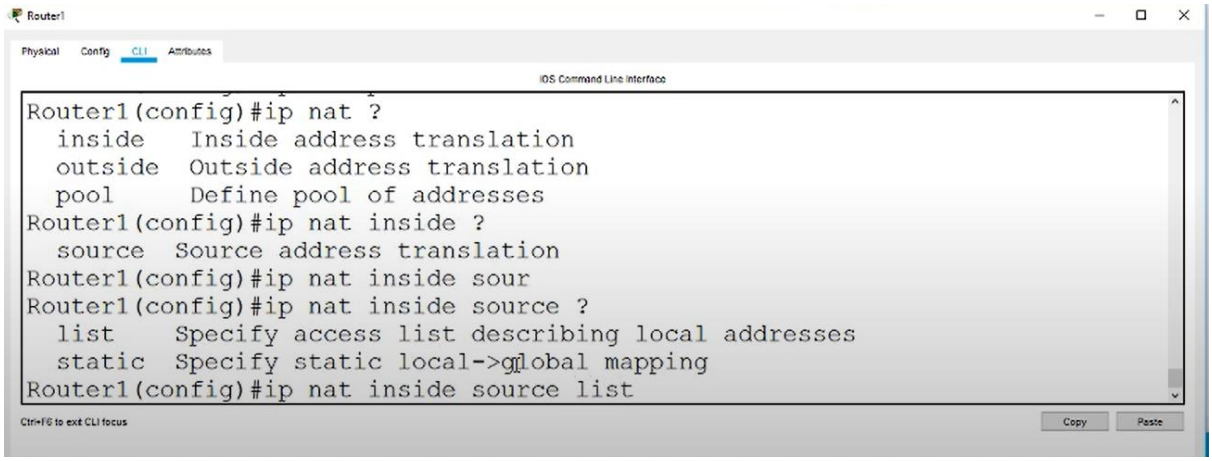

PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

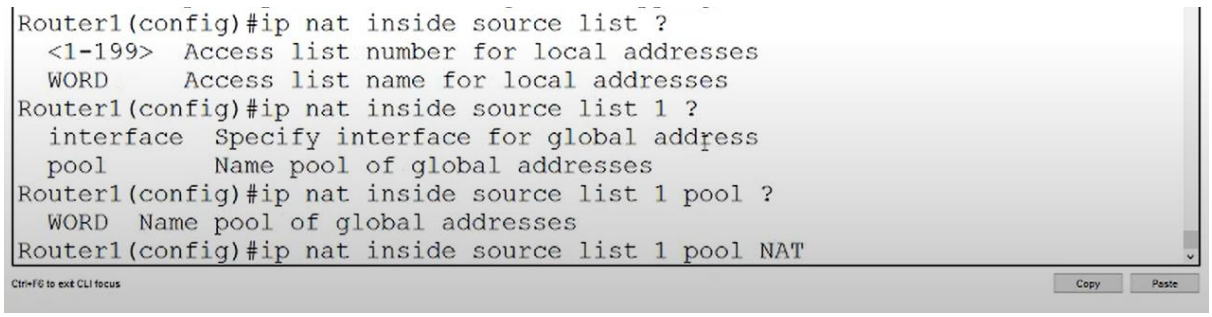

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#int s0/0/0
Router1(config-if)#ip nat outside
Router1(config-if)#int g0/1
Router1(config-if)#ip nat inside
Router1(config-if)#exit
Router1(config)#access
Router1(config)#access-list 1 permit
Ctrl+F6 to exit CLI focus
Copy
Paste


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router1(config-if)#exit
Router1(config)#access
Router1(config)#access-list 1 permit ?
A.B.C.D Address to match
any Any source host
host A single host address
Router1(config)#access-list 1 permit 192.168.2.0 ?
A.B.C.D Wildcard bits
<cr>
Router1(config)#access-list 1 permit 192.168.2.0 0.0.0.255
Router1(config)#ip nat
Ctrl+F6 to exit CLI focus
Copy
Paste

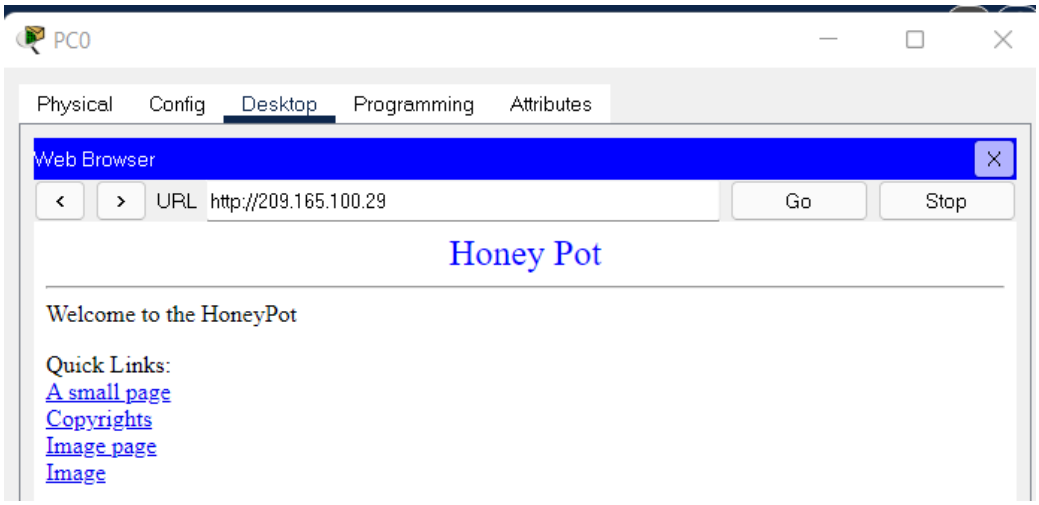

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router1(config)#ip nat ?
inside Inside address translation
outside Outside address translation
pool Define pool of addresses
Router1(config)#ip nat pool ?
WORD Pool name
Router1(config)#ip nat pool NAT ?
A.B.C.D Start IP address
Router1(config)#ip nat pool NAT 10.1.1.5 ?
A.B.C.D End IP address
Router1(config)#ip nat pool NAT 10.1.1.5 10.1.1.10
Ctrl+F6 to exit CLI focus
Copy
Paste

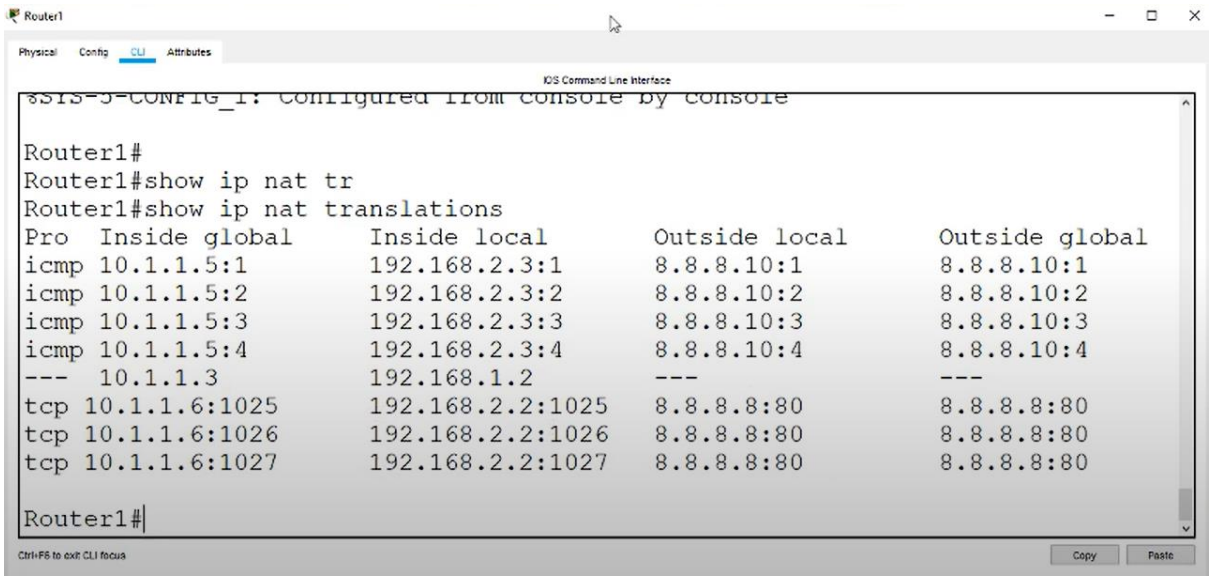

Router1
Physical Config CLI Attributes
IOS Command Line Interface
netmask Specify the network mask
Router1(config)#ip nat pool NAT 10.1.1.5 10.1.1.10 netmask ?
A.B.C.D Network mask
Router1(config)#ip nat pool NAT 10.1.1.5 10.1.1.10 netmask 255.255.255.0 ?
<cr>
Router1(config)#ip nat pool NAT 10.1.1.5 10.1.1.10 netmask 255.255.255.0
Router1(config)#ip nat ?
inside Inside address translation
outside Outside address translation
pool Define pool of addresses
Router1(config)#ip nat inside
Ctrl+F6 to exit CLI focus
Copy
Paste


Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router1(config)#ip nat ?
inside Inside address translation
outside Outside address translation
pool Define pool of addresses
Router1(config)#ip nat inside ?
source Source address translation
Router1(config)#ip nat inside sour
Router1(config)#ip nat inside source ?
list Specify access list describing local addresses
static Specify static local->global mapping
Router1(config)#ip nat inside source list
Ctrl+F6 to exit CLI focus
Copy
Paste


Router1(config)#ip nat inside source list ?
<1-199> Access list number for local addresses
WORD Access list name for local addresses
Router1(config)#ip nat inside source list 1 ?
interface Specify interface for global address
pool Name pool of global addresses
Router1(config)#ip nat inside source list 1 pool ?
WORD Name pool of global addresses
Router1(config)#ip nat inside source list 1 pool NAT
Ctrl+F6 to exit CLI focus
Copy
Paste

When we put public address from pc0 it gets translated and displays honeypot





PAT (Network Overload Translation)

To translate any computer's ip address across the network of 192.168.1.0

We use PAT.

Commands

access-list 1 permit 192.168.1.0 0.0.0.255

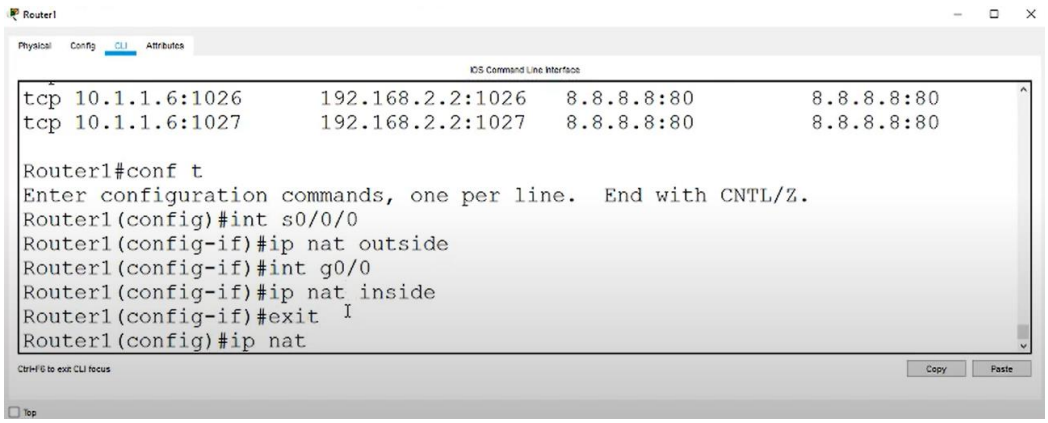
ip nat inside source list 10 interface g0/0 overload

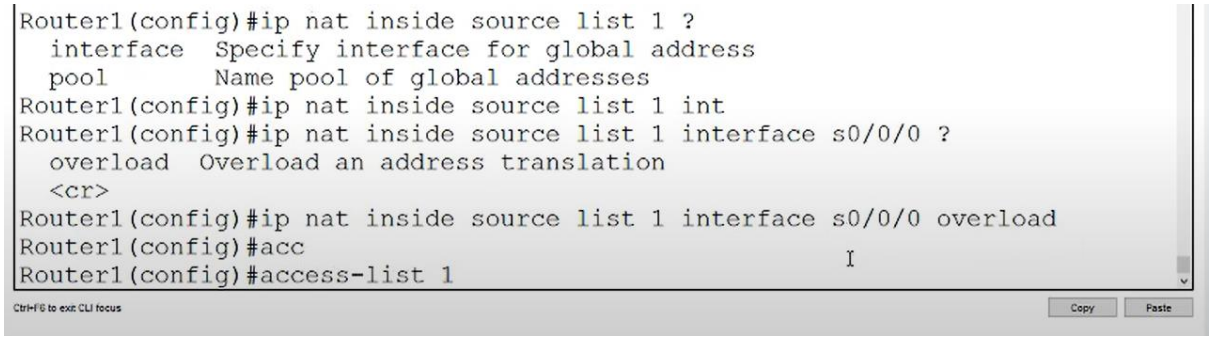
Port Address Translation

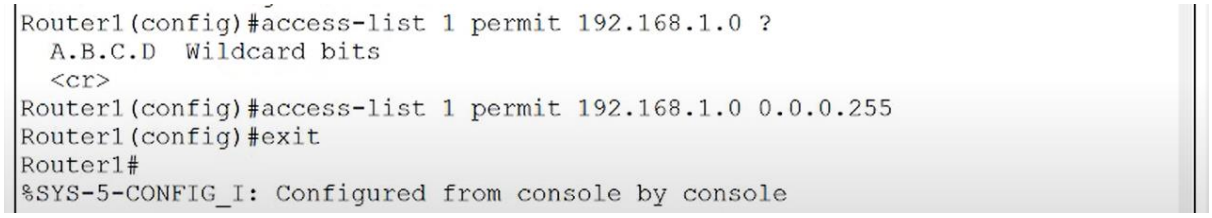
Now we want the server to be only available for port 80.

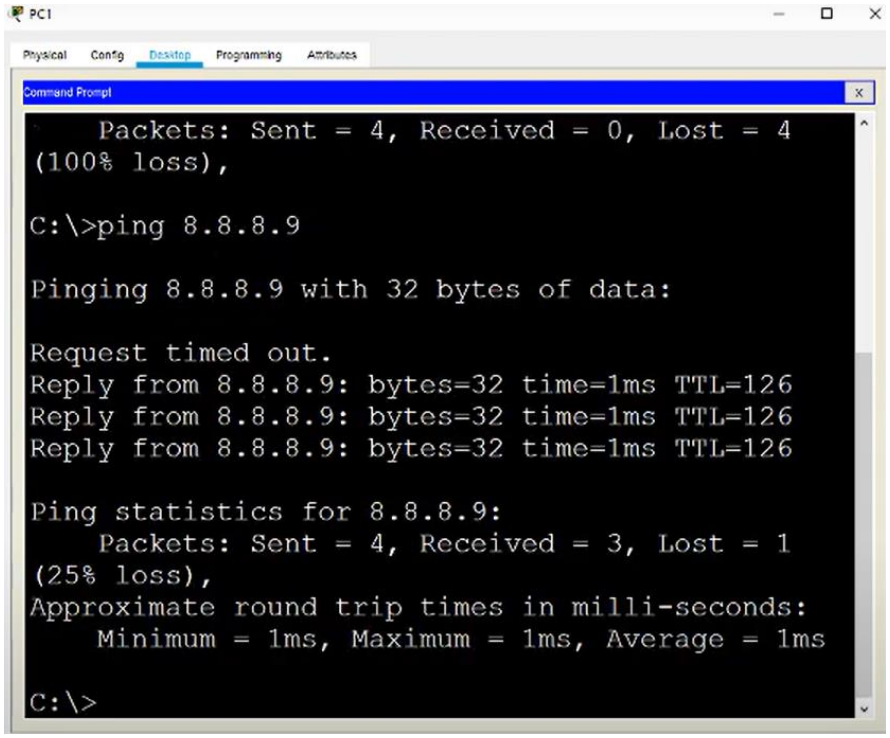
Earlier there was just static translation over all ports but now we will restrict it to only port 80.

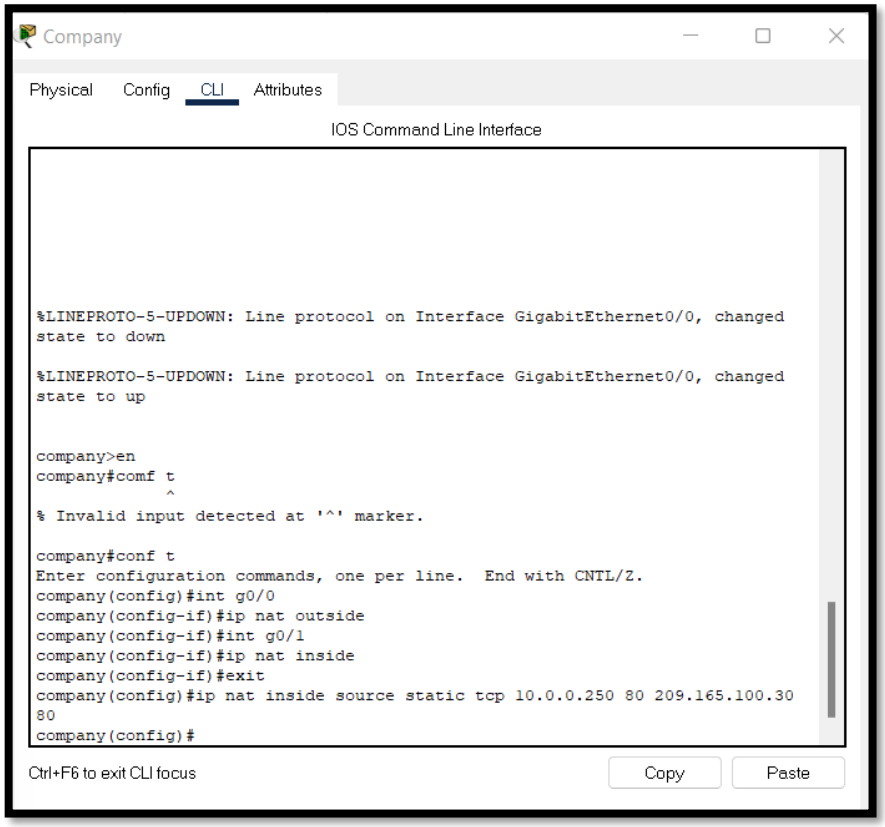
Commands











On typing ip address it hits other web server and displays output

This was the port forwarding to 10.0.0.250 port 80

Conclusion:Static NAT,dynamic NAT and PAT have been successfully implemented.

LAB 7

ARYAMAN MISHRA

19BCE1027

LAB 7

AIM: Create a network topology with a CISCO ASA Firewall, Router, Switch, 3 PCs and a Server. Here, a PC is to be connected with ASA Firewall and two PCs are to be connected with switch. Do the following:

1. Create two VLANs

2. Configure the Router, Server and Firewall.

3. Ensure the firewall functionality by demonstrating the packet transmission between the PCs and Server.

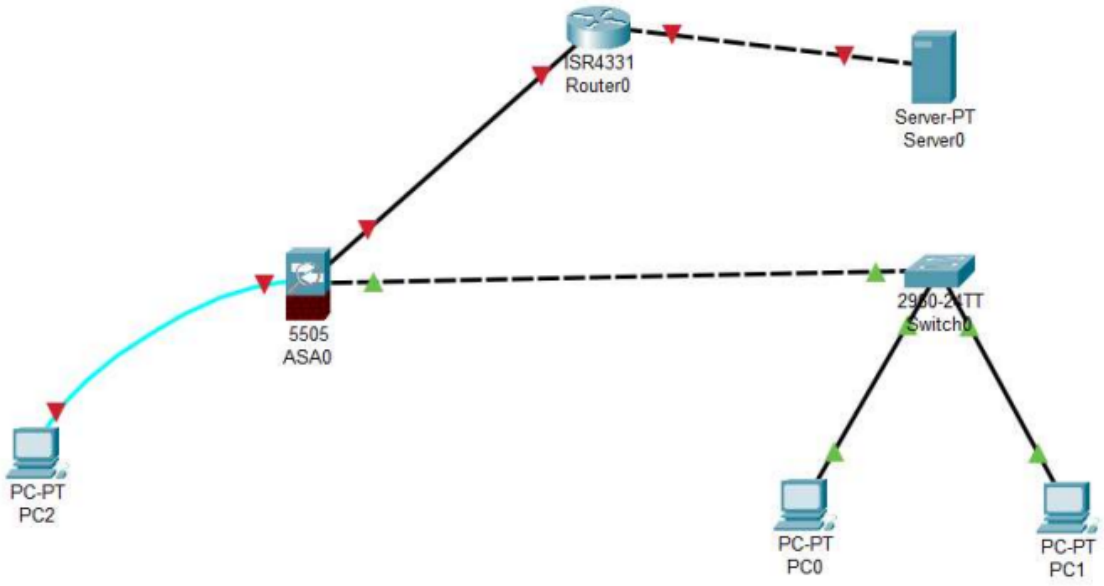
4. Apply NAT

5. Use DHCP and ICMP protocols

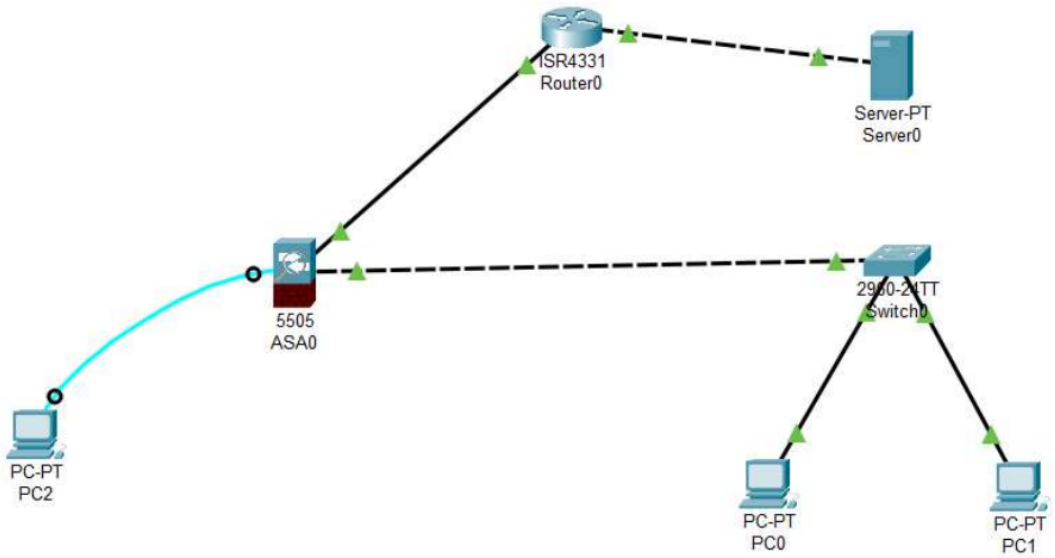
6. Ping the connected PCs

Experiment:

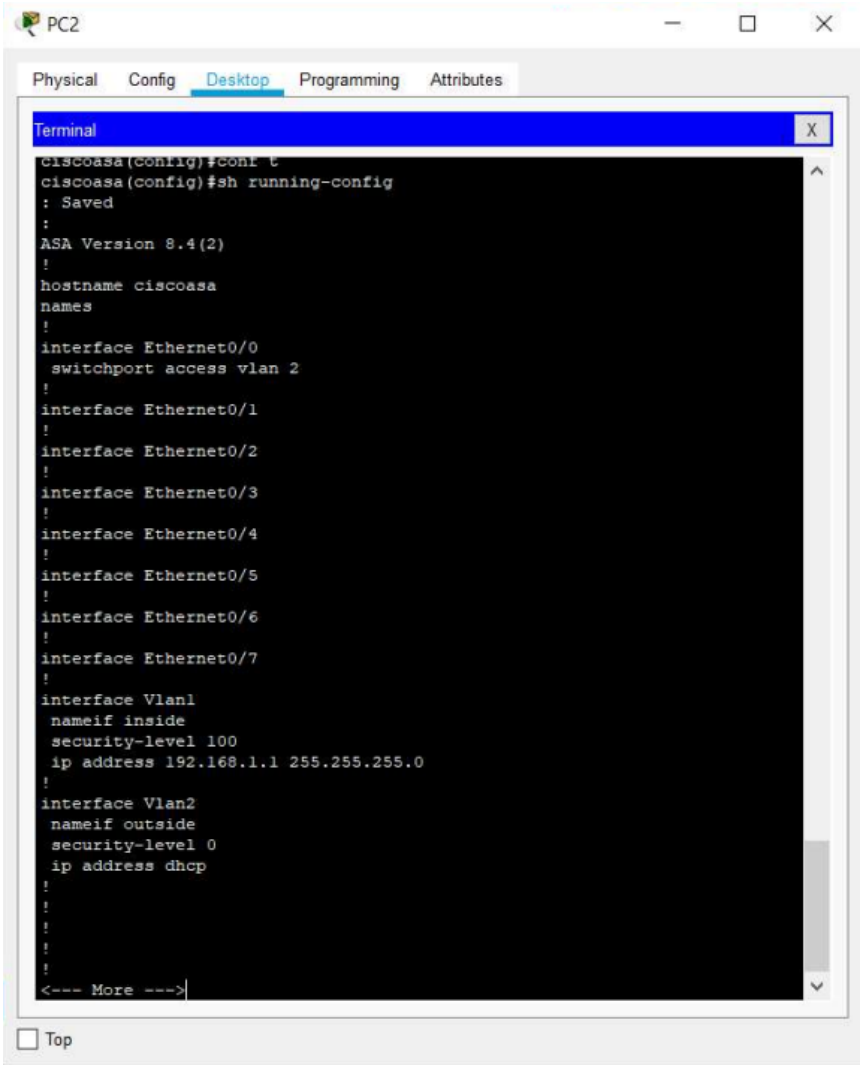
Create a Topology



Turn on the routers.



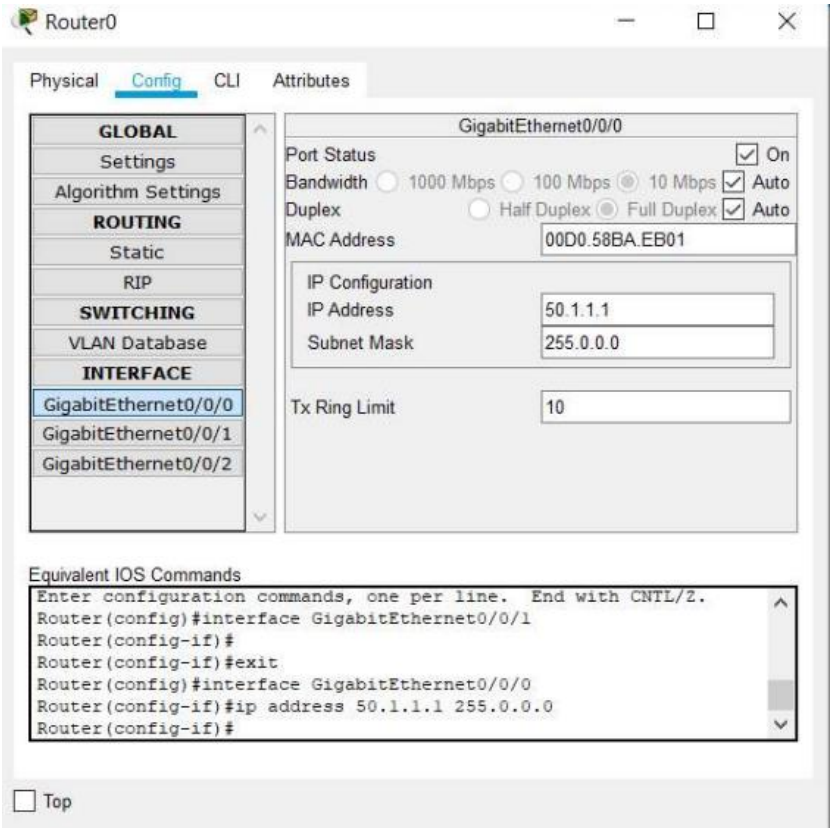
Configuring 1 st VLAN with firewall.

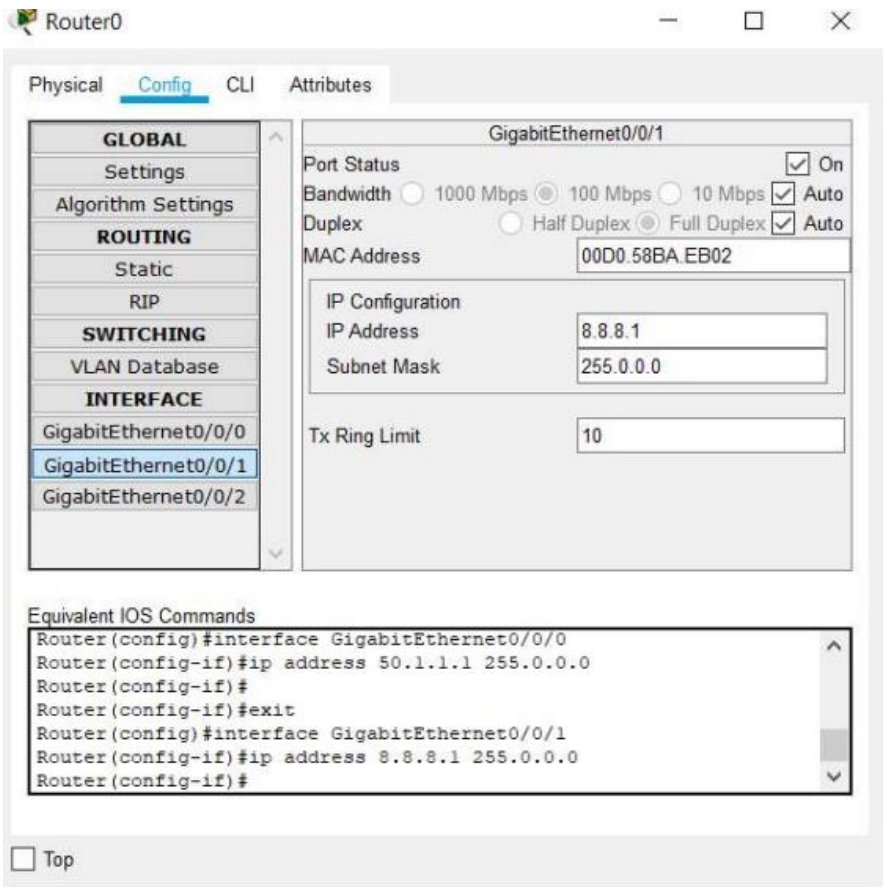

PC2
Physical
Config
Desktop
Programming
Attributes
Terminal
X
ciscoasa(config)#conf t
ciscoasa(config)#sh running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address dhcp
!
!
!
!
!
<--- More --->
Top

```
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip add 10.1.1.1 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#
```

Setting the IP Address on Router

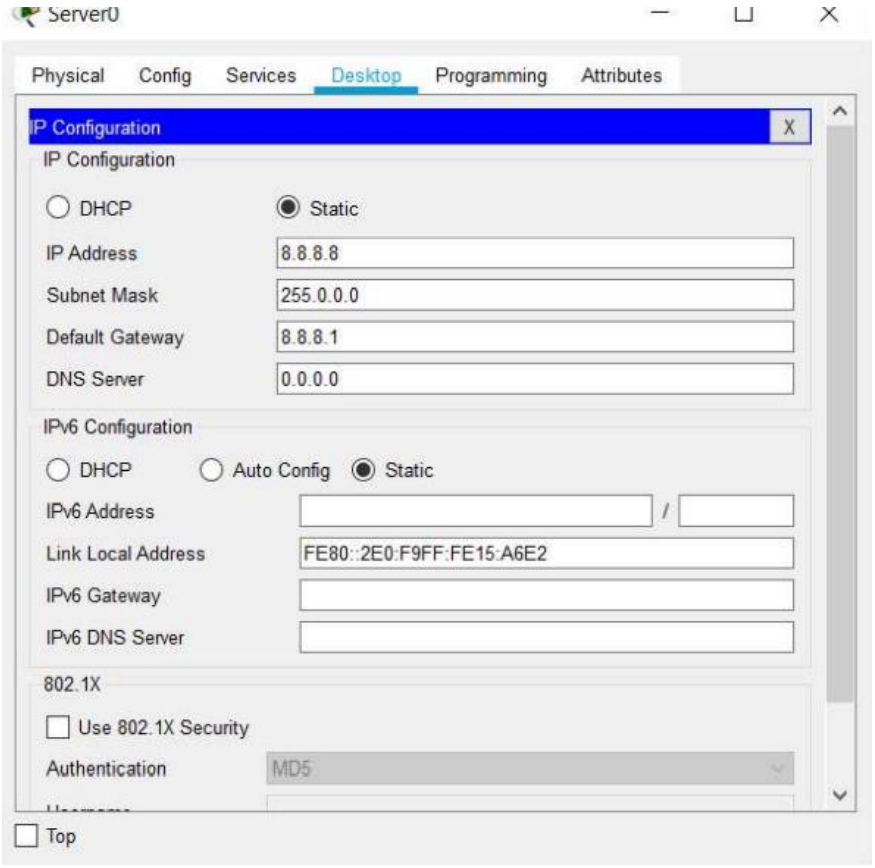
```
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit
ciscoasa(config)#v
                 ^
% Invalid input detected at '^' marker.

ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 50.1.1.2 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#intint e0/0
                   ^
% Invalid input detected at '^' marker.

ciscoasa(config)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#
```



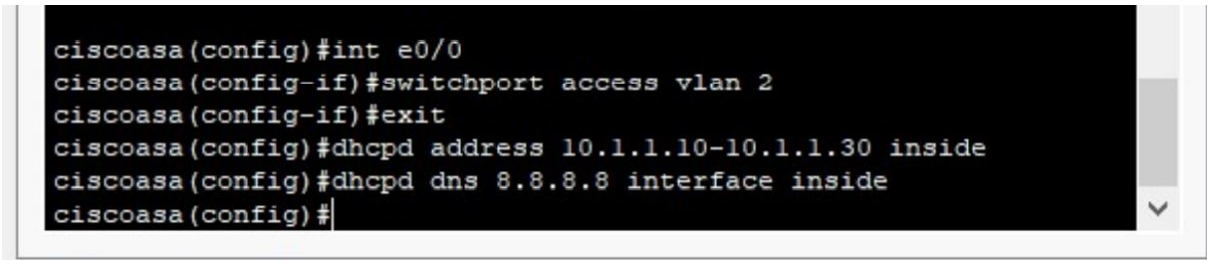


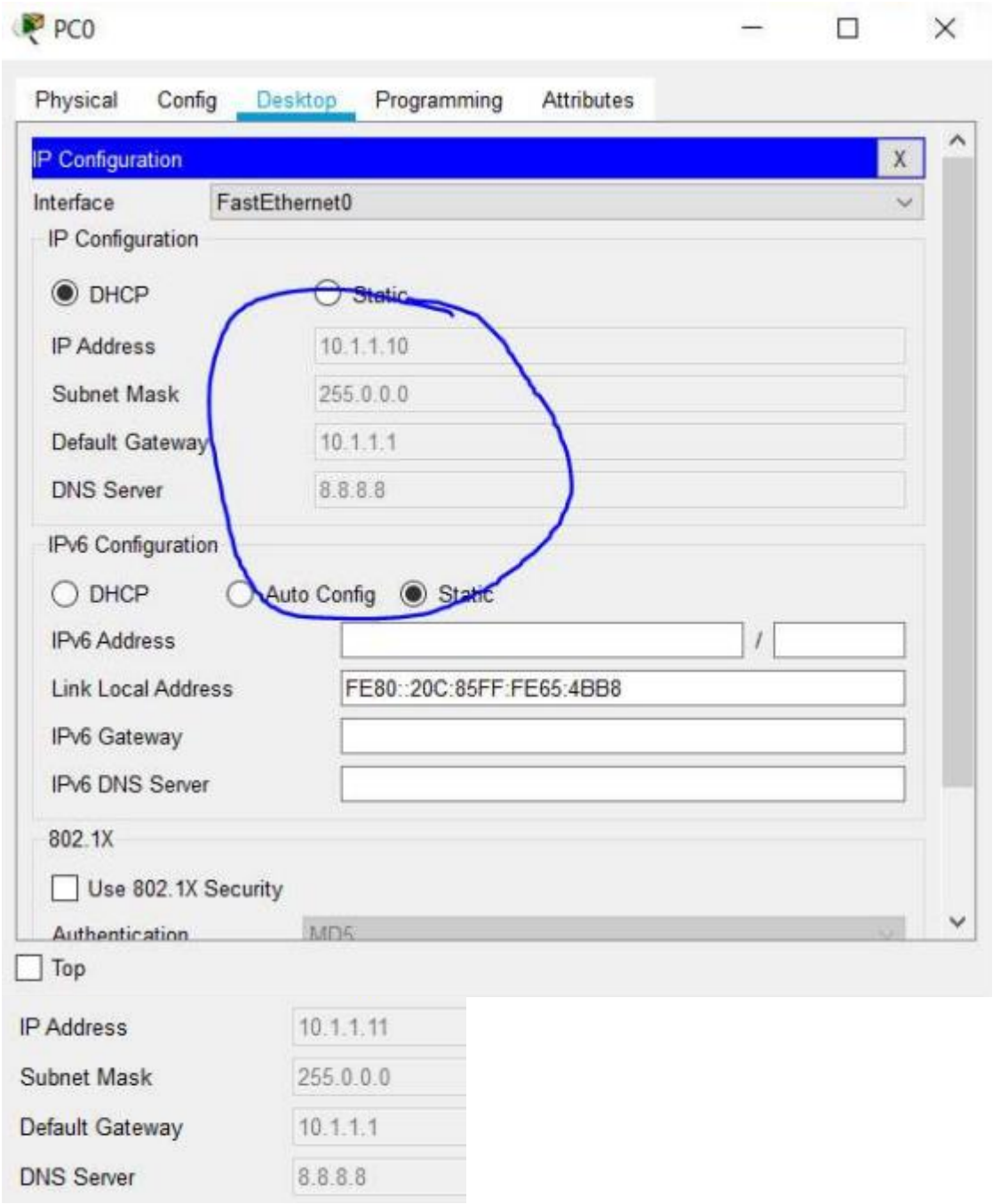
Setting the IP Address on Router

Setting the IP Address on the Server



Setting DHCPD range for Firewall via the PC-2 and the DNS IP





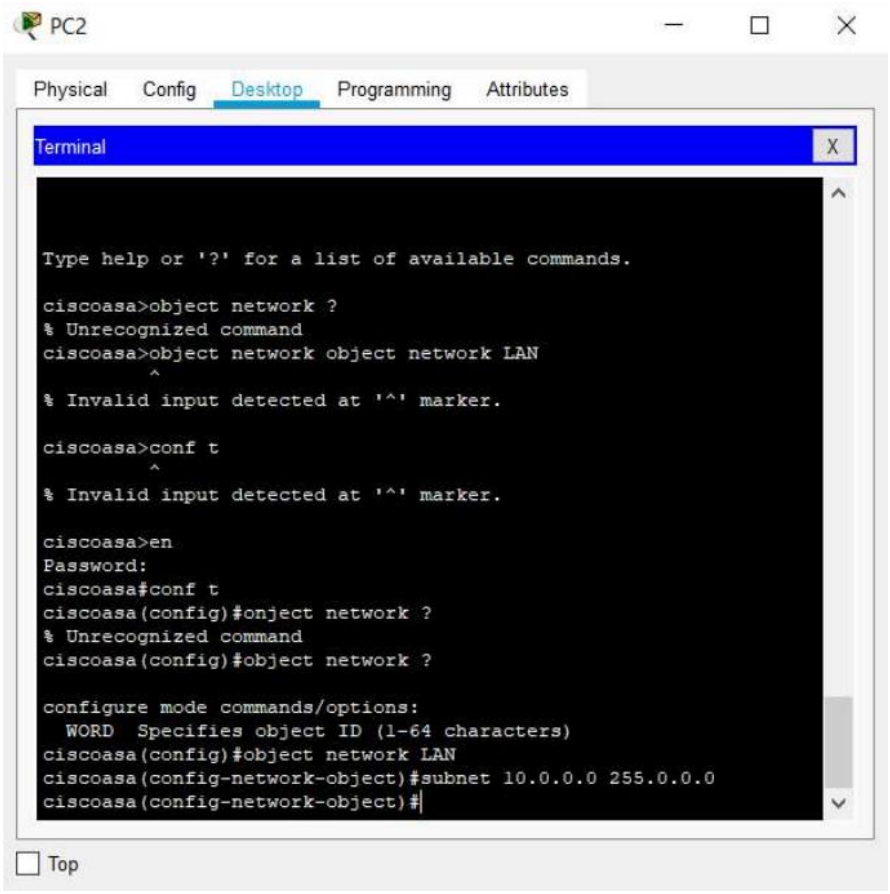
Setting up OSPF on the Router

```
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1
```

Setting up OSPF on the Router

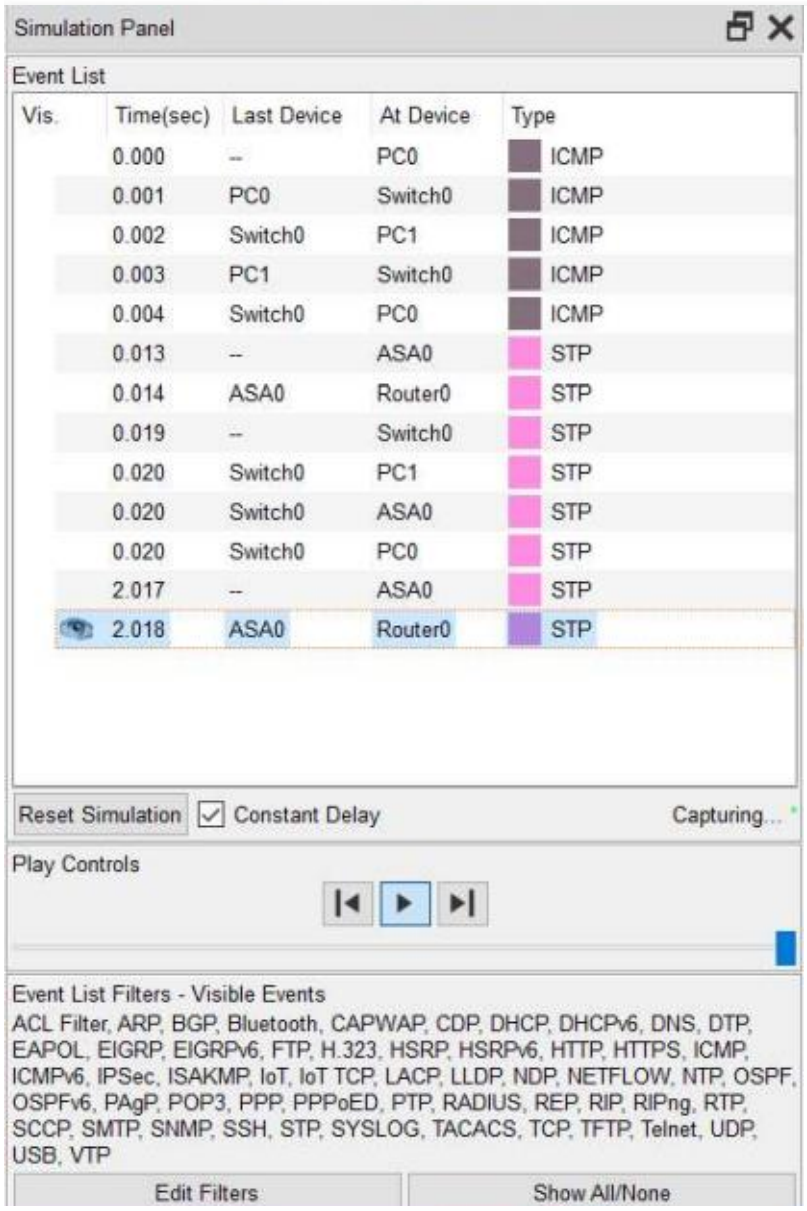
```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#exit
Router(config)#router ospf ?
  <1-65535>  Process ID
Router(config)#router ospf
% Incomplete command.
Router(config)#router ospf ?
  <1-65535>  Process ID
Router(config)#router ospf 1
Router(config-router)#net 50.0.0.0 ?
  A.B.C.D  OSPF wild card bits
Router(config-router)#net 50.0.0.0 0.255.255.255 area 0
Router(config-router)#net 8.0.0.0 0.255.255.255 area 0
Router(config-router)#
```

Enable NAT on ASA


PC2
Physical
Config
Desktop
Programming
Attributes
Terminal
X
Type help or '?' for a list of available commands.
ciscoasa>object network ?
% Unrecognized command
ciscoasa>object network object network LAN
^
% Invalid input detected at '^' marker.
ciscoasa>conf t
^
% Invalid input detected at '^' marker.
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#onject network ?
% Unrecognized command
ciscoasa(config)#object network ?
configure mode commands/options:
WORD Specifies object ID (1-64 characters)
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#
Top

Enable NAT on ASA

```
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#nat ?

network-object mode commands/options:
  (  Open parenthesis for (<internal_if_name>,<external_if_name>)
pair
ciscoasa(config-network-object)#nat (inside, Outside) dynamic
interface
ciscoasa(config-network-object)#
```



All steps have been successfully implemented and executed.

LAB 8

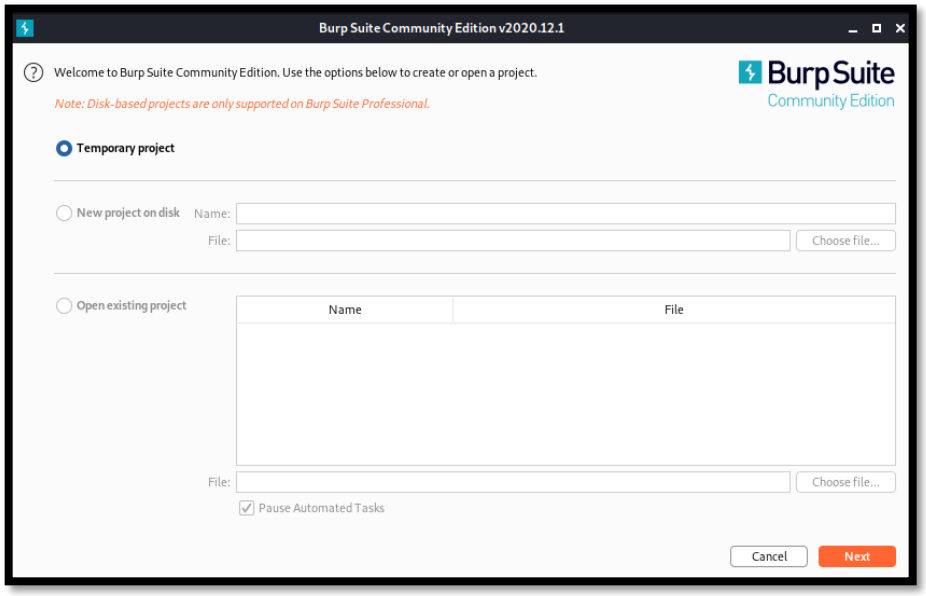
Aryaman Mishra

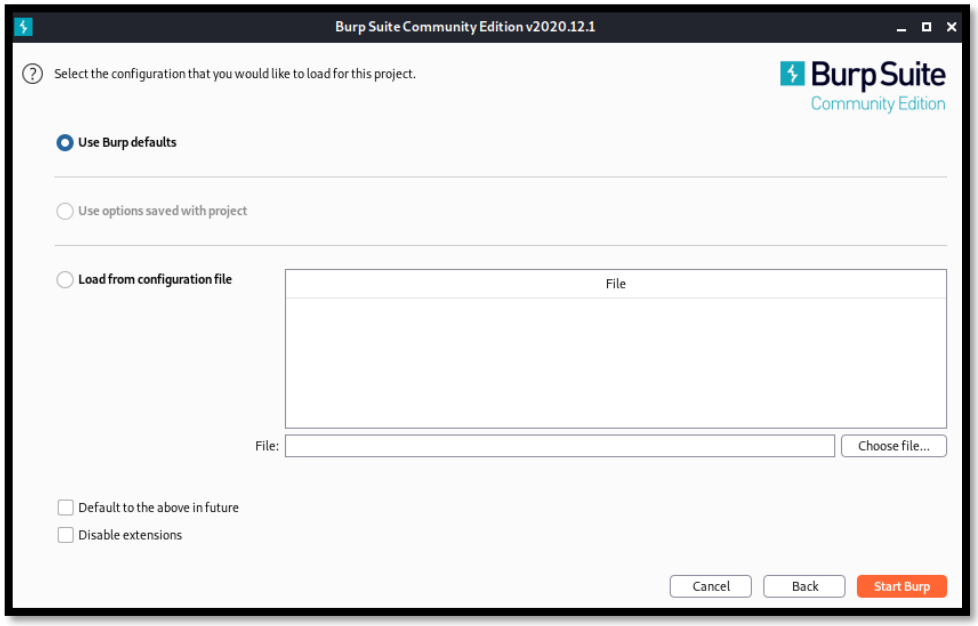
19BCE1027

LAB 8-CA CERTIFICATE IN BURP SUITE

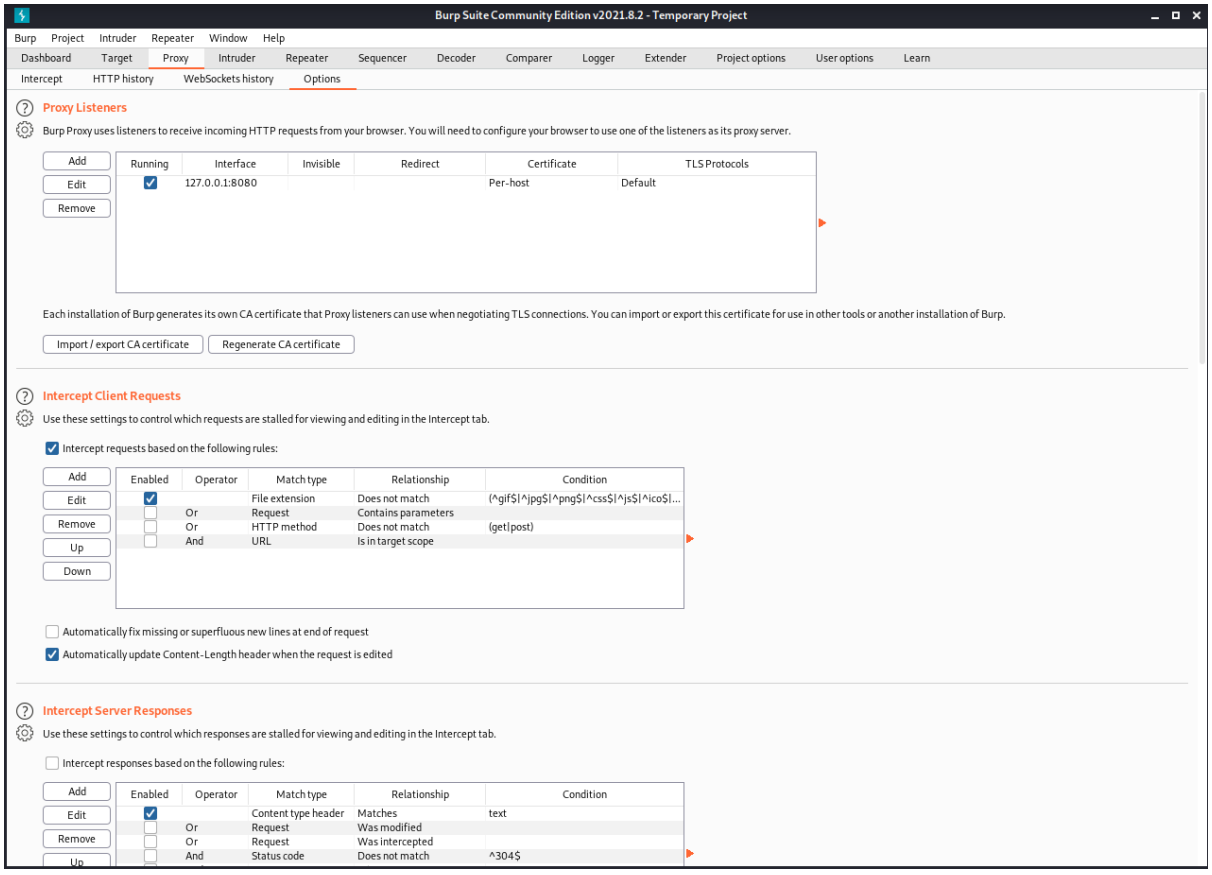
Launch Burp suite from command line.

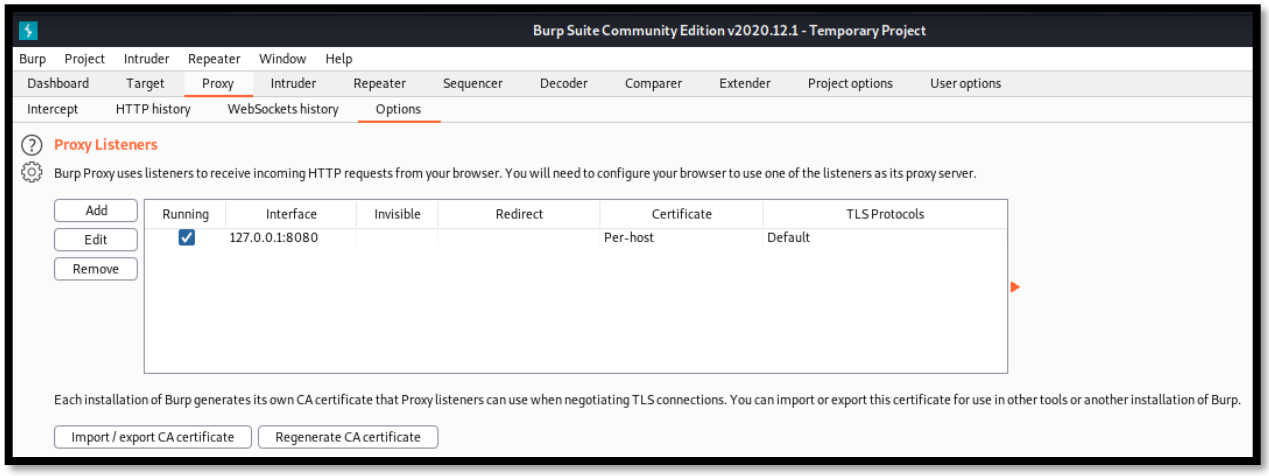
Select temporary Project and choose Burp default settings..





Go to Proxy tab and then to options.





Burp is listening on this port and this interface.

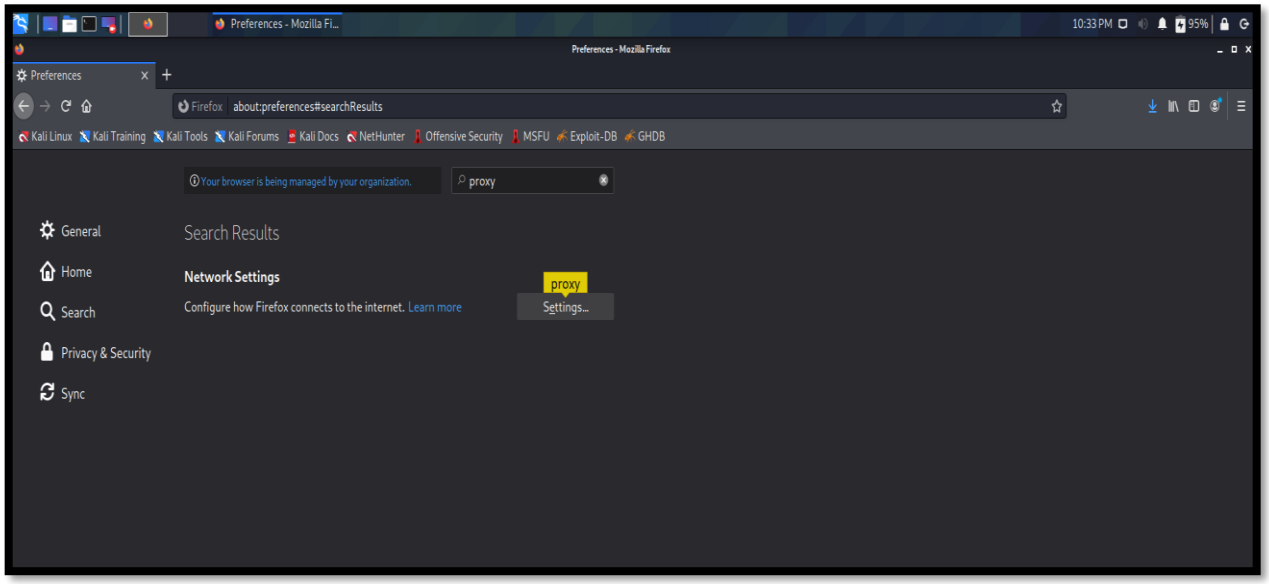
The socket is 127.0.0.1:8080(loopback interface).Any request on this specific loopback interface will be captured by Burp.

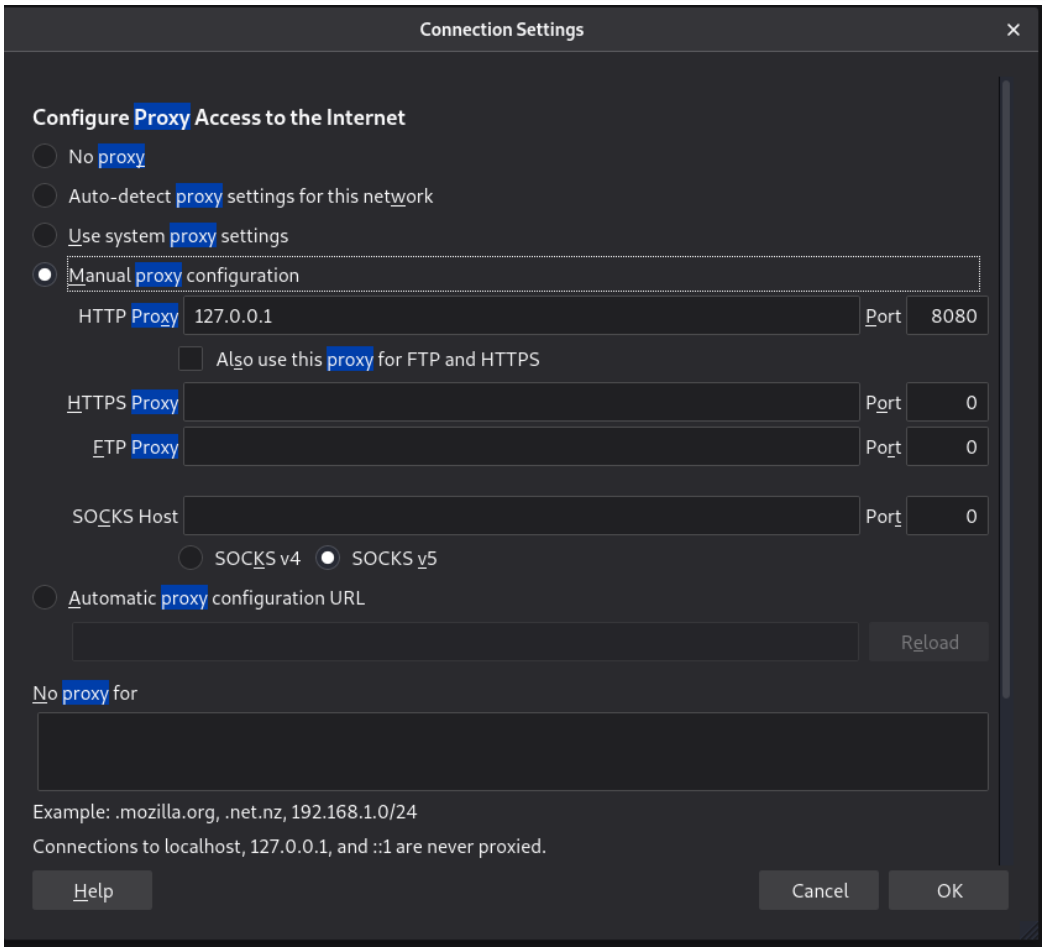
We cannot send any request on the loopback interface so we will open Firefox browser.

Now Burp is ready to see requests from the browser.

To redirect requests on the proxy and not server,we will have to configure our Browser.

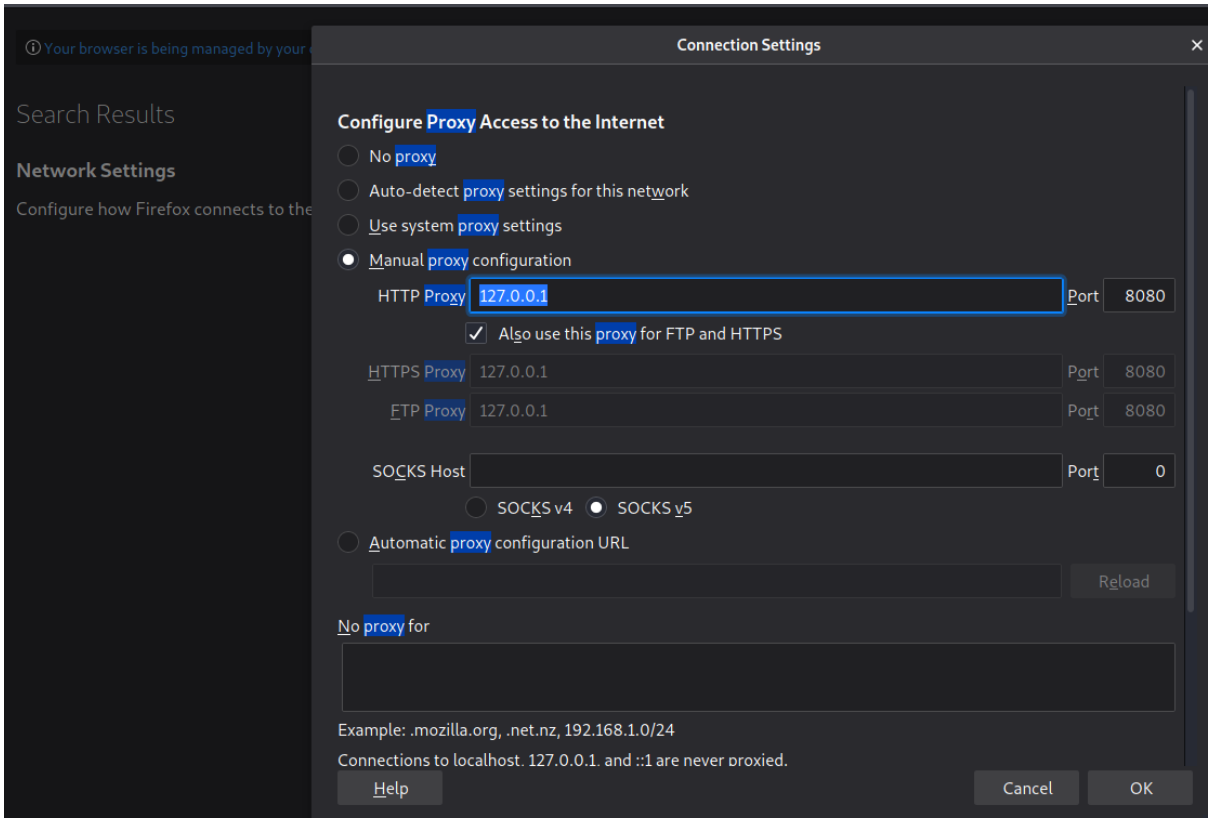
Mention target IP address on Manual settings.





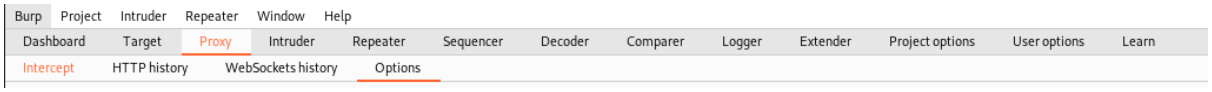
Any request will go through our Proxy.

Select Manual proxy option and type proxy ip same as that on burpsuite i.e. 127.0.0.1:8080.

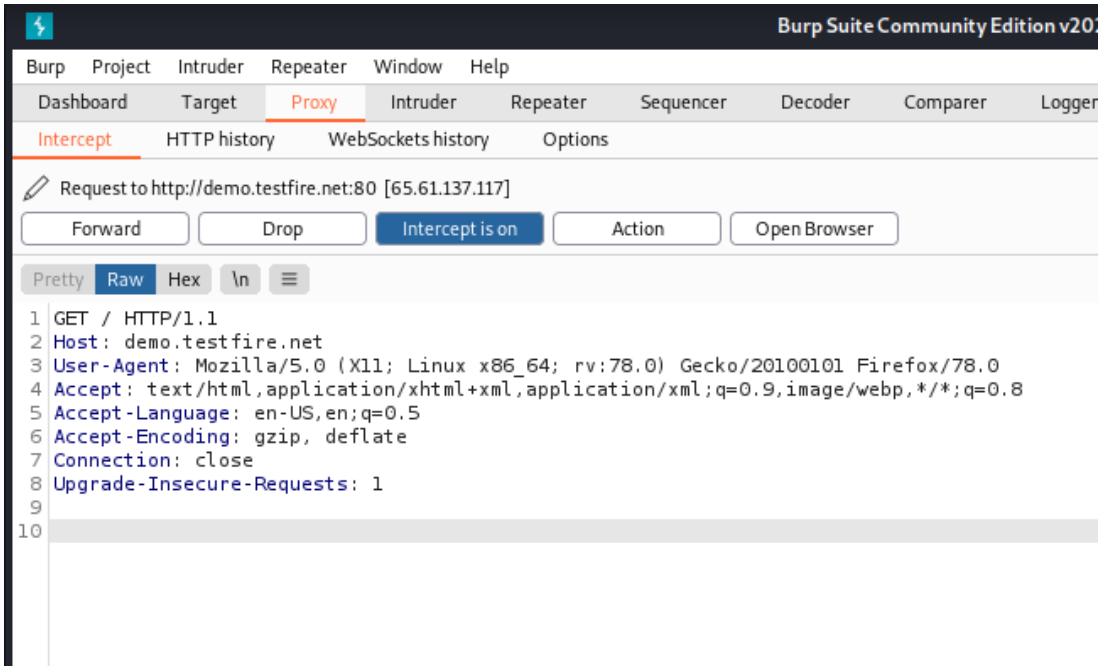


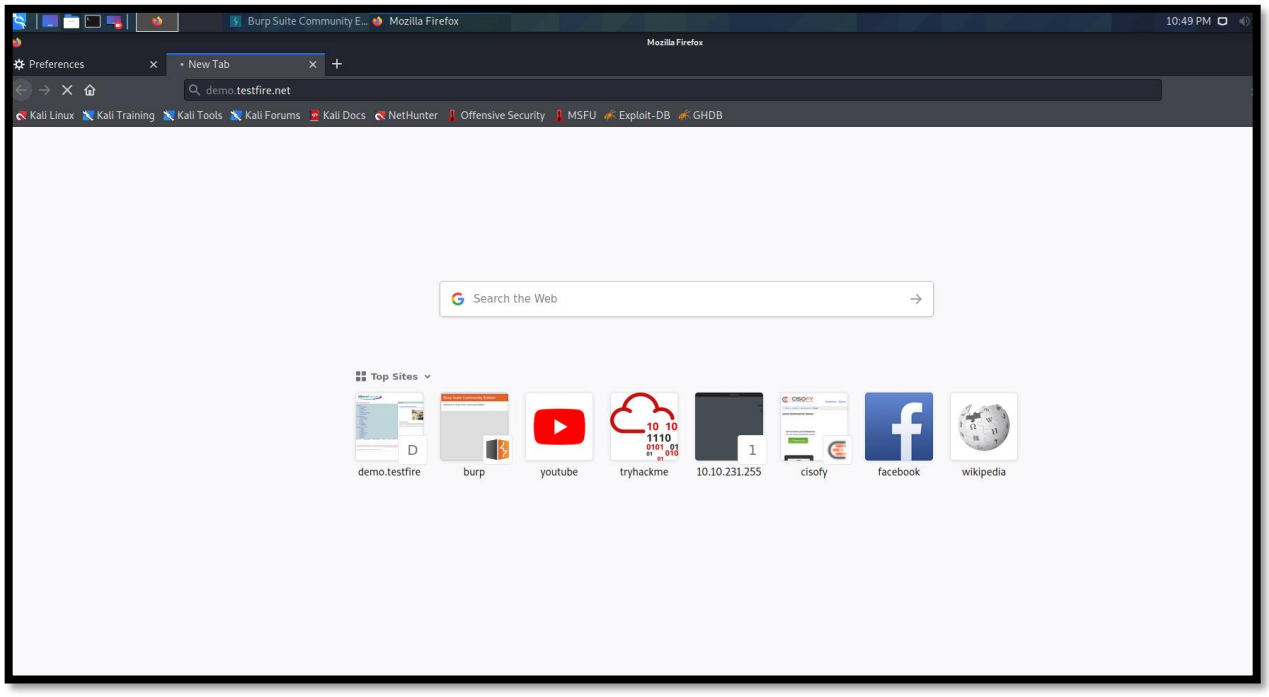
Now we will try to open a demo test website at **http://demo.testfire.net.**

Test site not loading when intercept is on for proxy as request reaches the proxy.

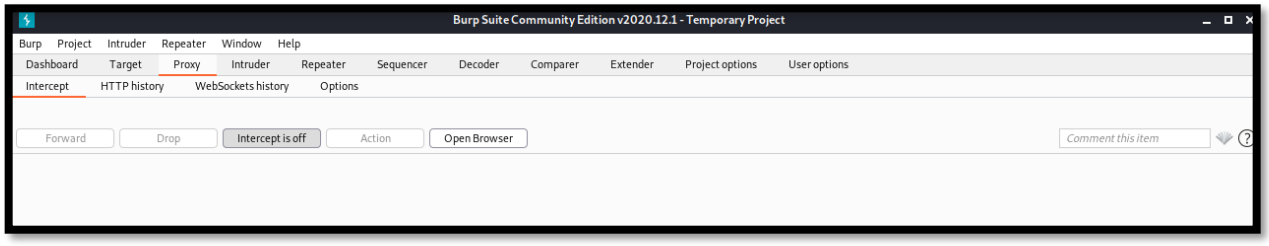


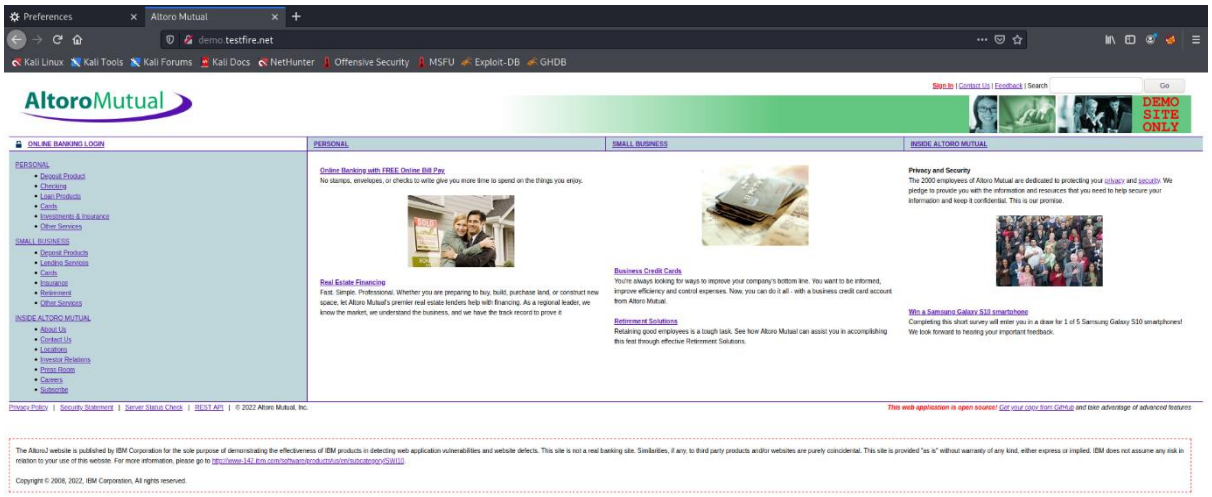
Intercept is highlighted orange.





When intercept is off it will allow them to pass through.

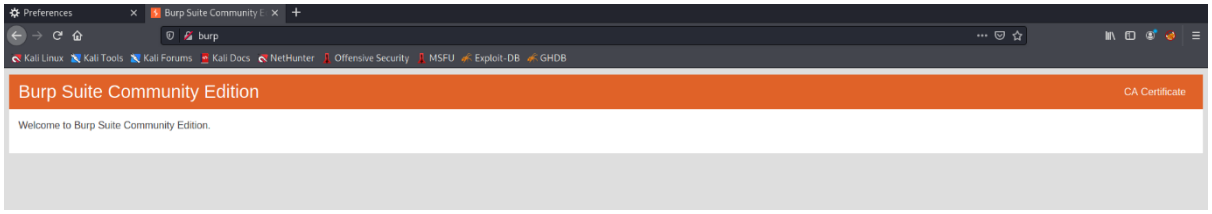




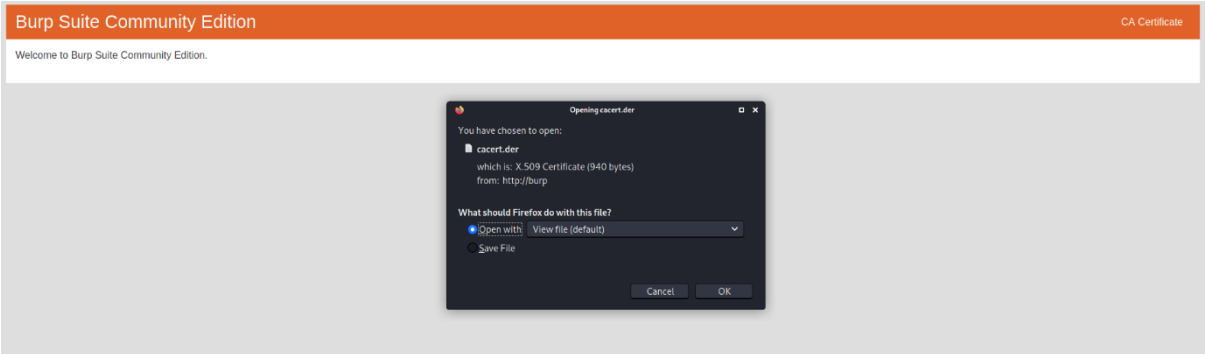
Download some CA certificates for burp in our browser so that the sites run.

Download certificate

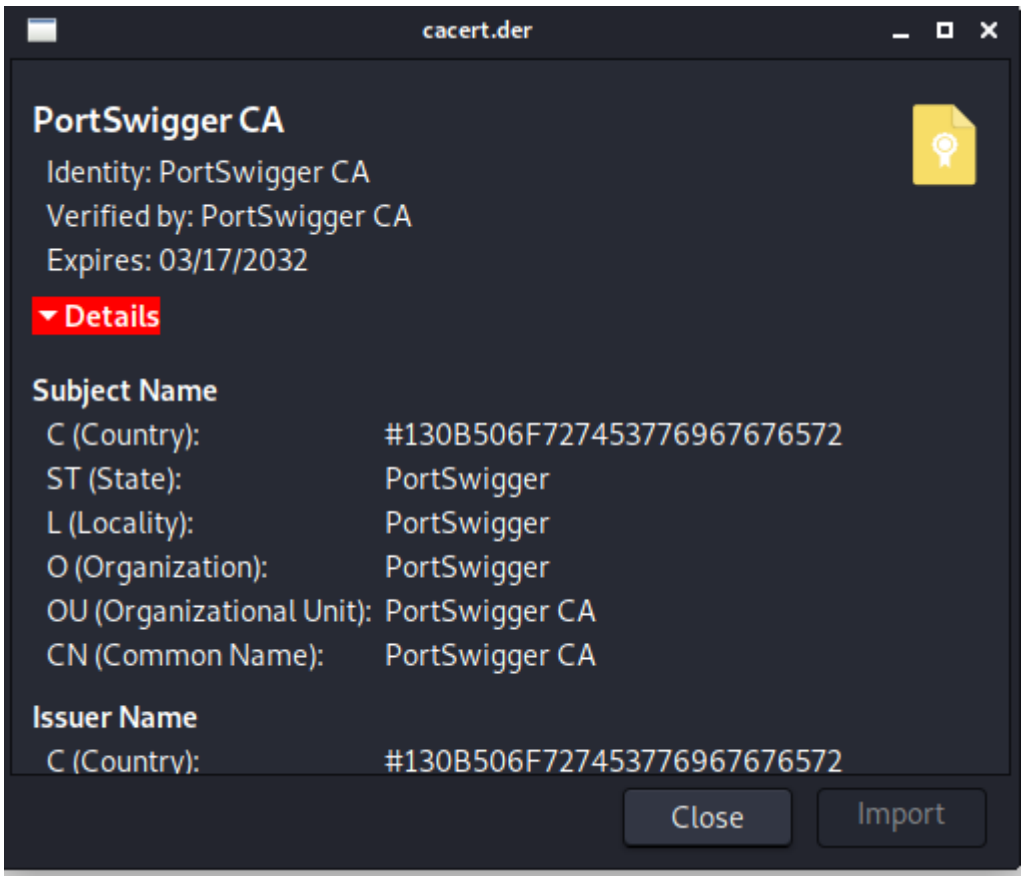
Go to site http://burp



Click on CA certificate

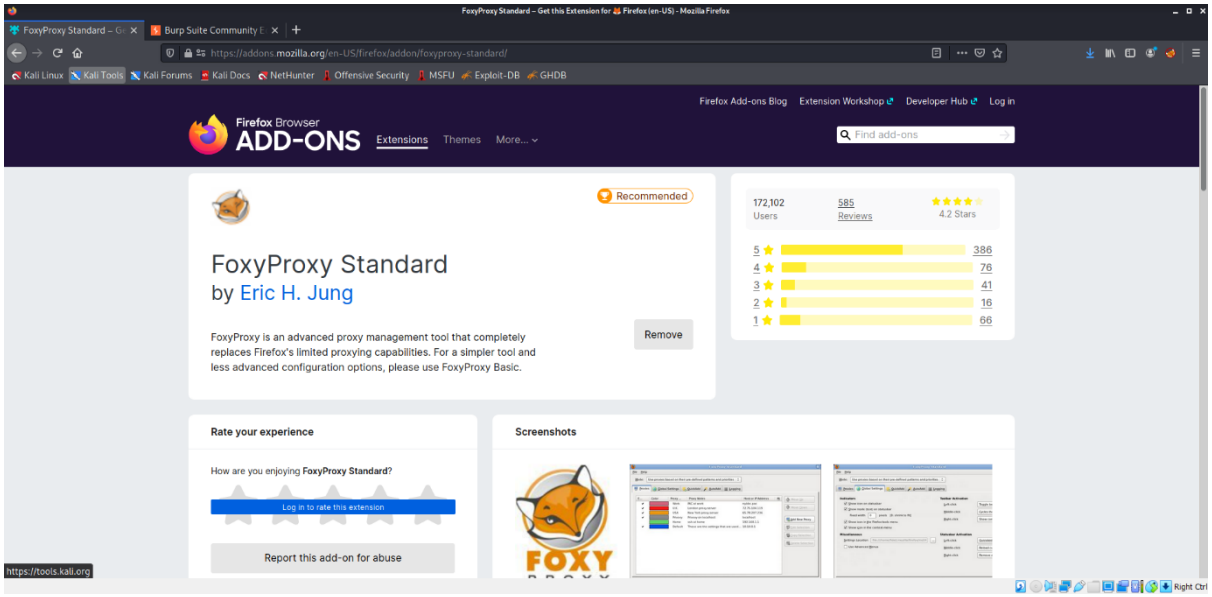


Download the certificate.

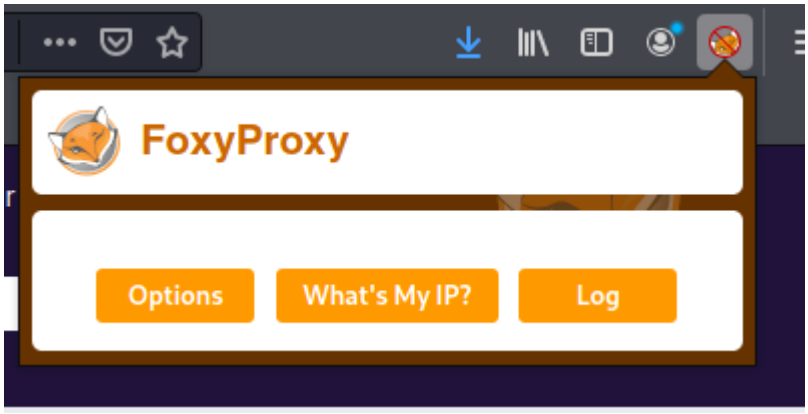


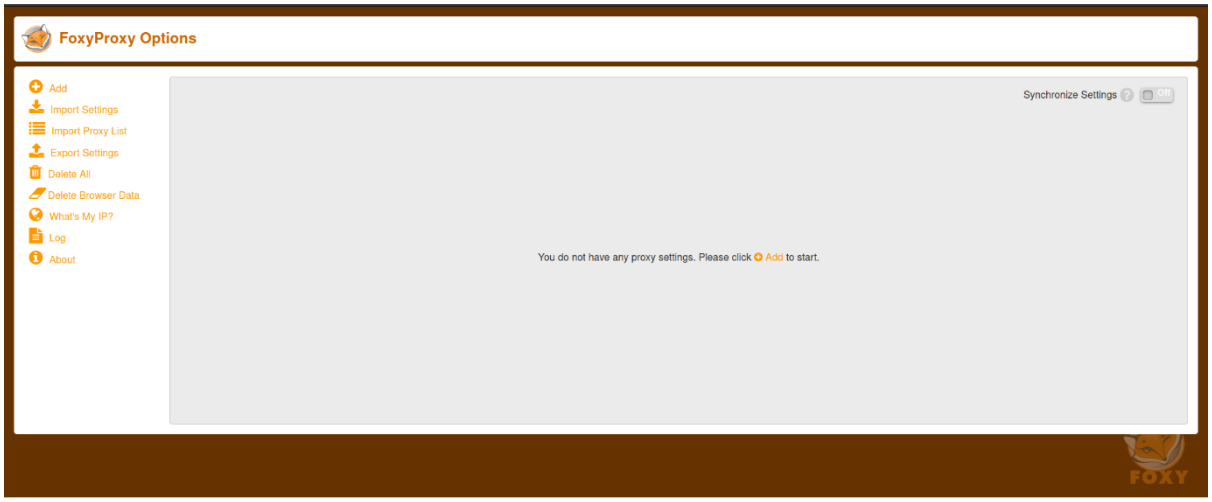
Import the certificates.

Download FoxyProxy add-on in Firefox.

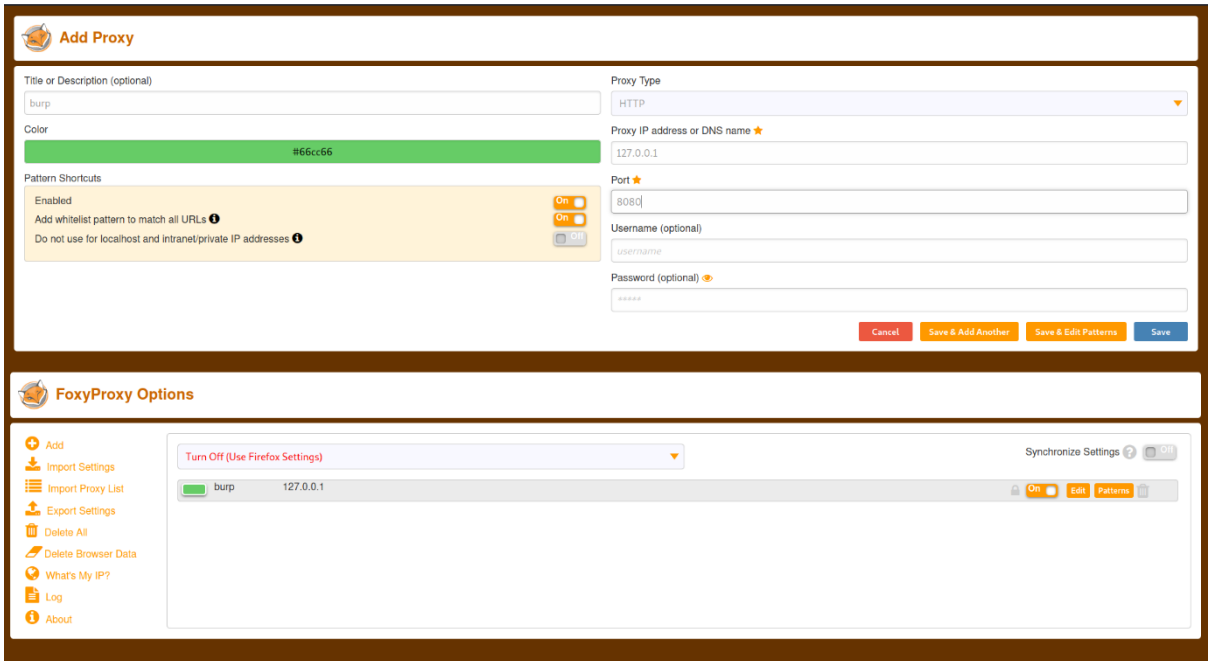


Click on options.

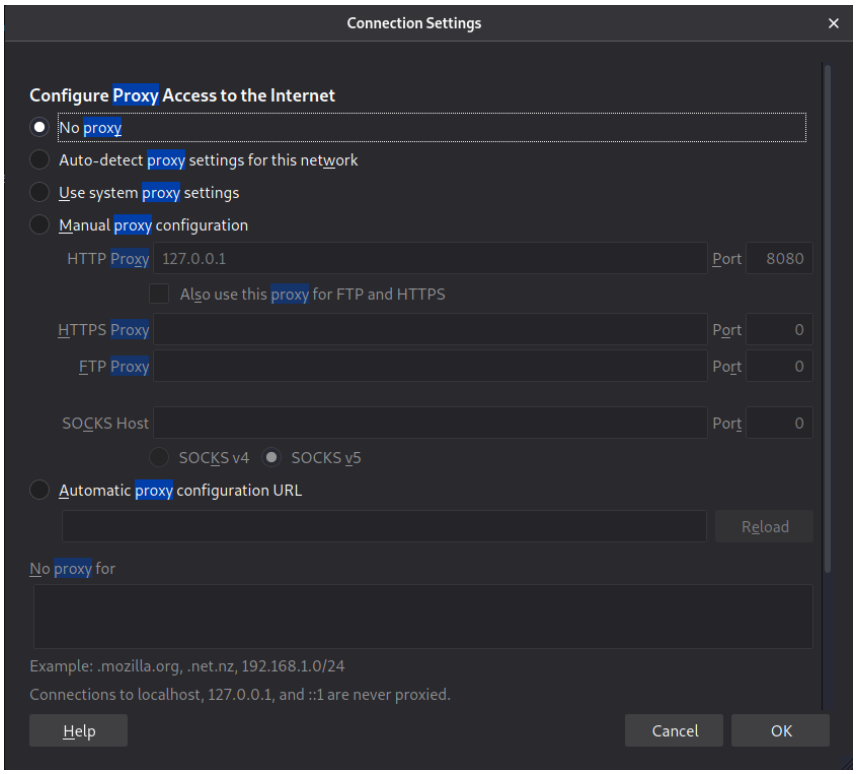




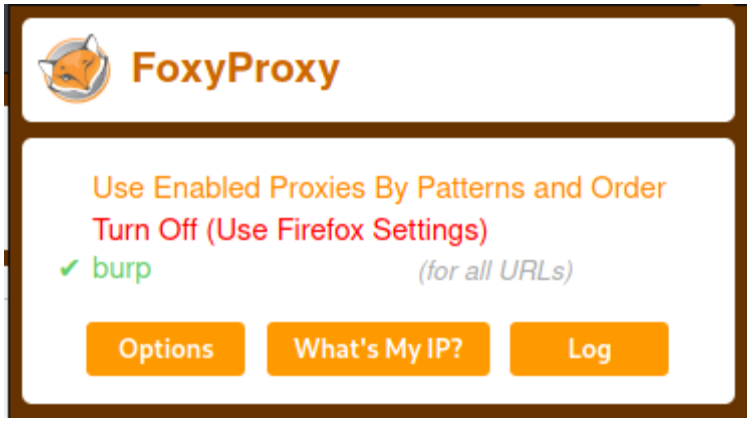
Fill proxy details and hit ‘save.’

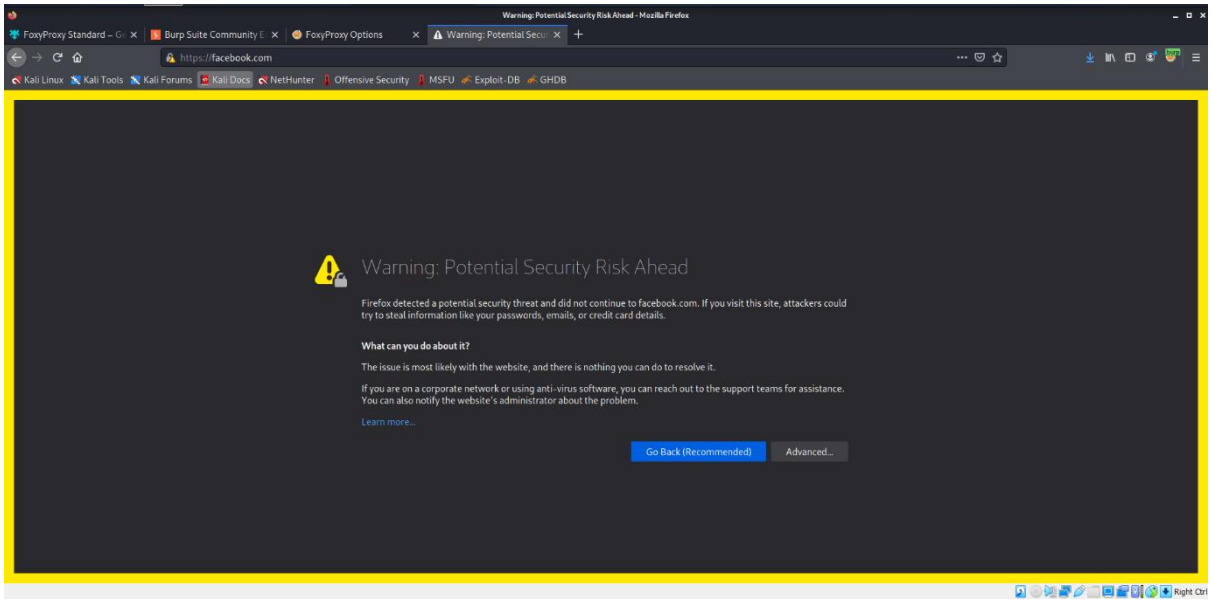


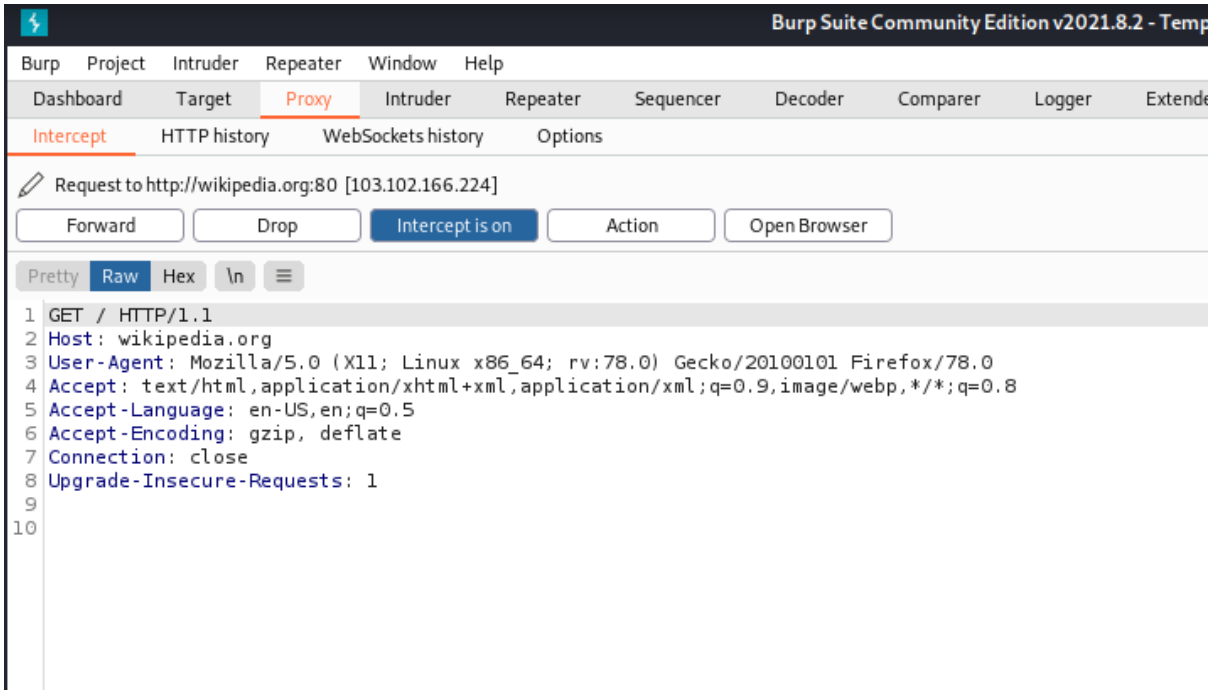
Revert to default settings in browser preferences.



Enable burp proxy option in plugin.







All requests will go through Proxy by Foxyproxy and not browser settings now.

Conclusion:Burp suite and Proxy settings have been successfully implemented with their respective operations.

LAB 9

Aryaman Mishra

19BCE1027

Sniper (Single payload attack)

This uses a single set of payloads. It targets each payload position in turn, and places each payload into that position in turn. Positions that are not targeted for a given request are not affected - the position markers are removed and any enclosed text that appears between them in the template remains unchanged. This attack type is useful for fuzzing a number of request parameters individually for common vulnerabilities. The total number of requests generated in the attack is the product of the number of positions and the number of payloads in the payload set.

Battering ram (Single payload attack)

This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once. This attack type is useful where an attack requires the same input to be inserted in multiple places within the request (e.g. a username within a Cookie and a body parameter). The total number of requests generated in the attack is the number of payloads in the payload set.

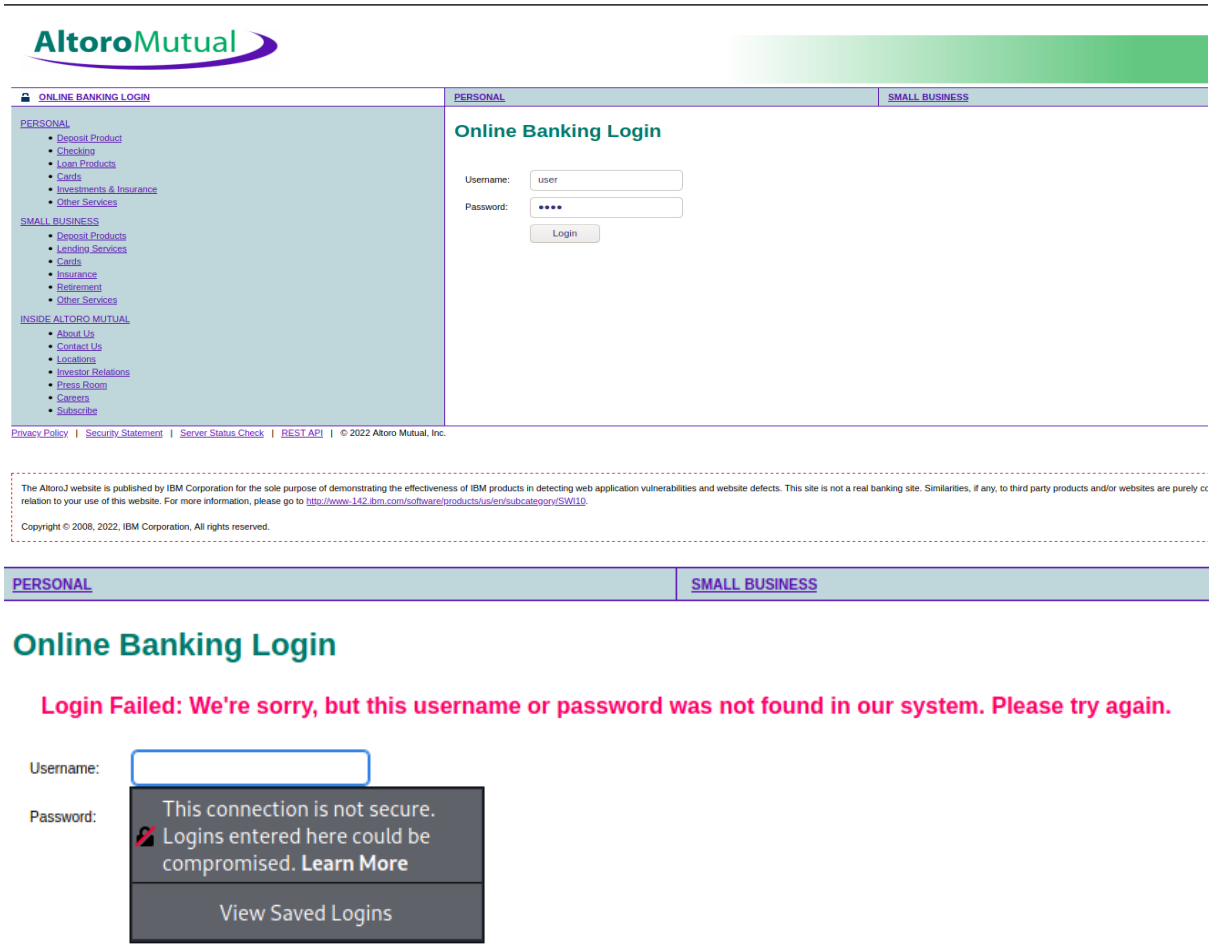
Pitchfork

This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, and places one payload into each defined position. In other words, the first request will place the first payload from payload set 1 into position 1 and

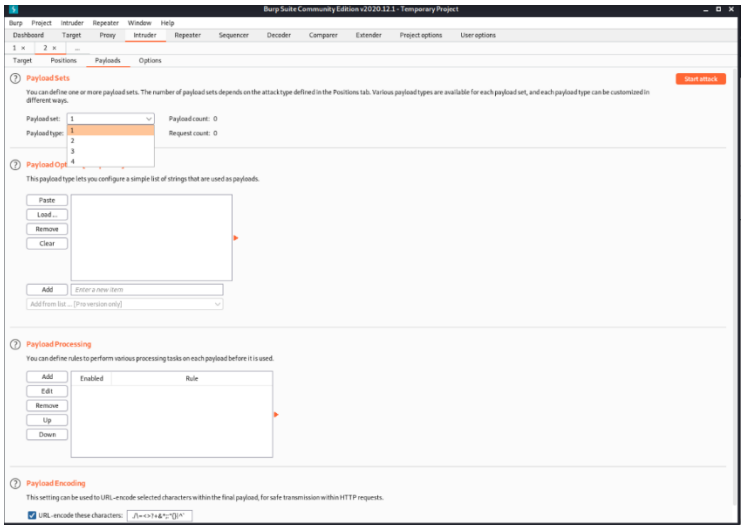
the first payload from payload set 2 into position 2; the second request will place the second payload from payload set 1 into position 1 and the second payload from payload set 2 into position 2, etc. This attack type is useful where an attack requires different but related input to be inserted in multiple places within the request (e.g. a username in one parameter, and a known ID number corresponding to that username in another parameter). The total number of requests generated in the attack is the number of payloads in the smallest payload set.

Cluster bomb

This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested. I.e., if there are two payload positions, the attack will place the first payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1. This attack type is useful where an attack requires different and unrelated or unknown input to be inserted in multiple places within the request (e.g. when guessing credentials, a username in one parameter, and a password in another parameter). The total number of requests generated in the attack is the product of the number of payloads in all defined payload sets - this may be extremely large.

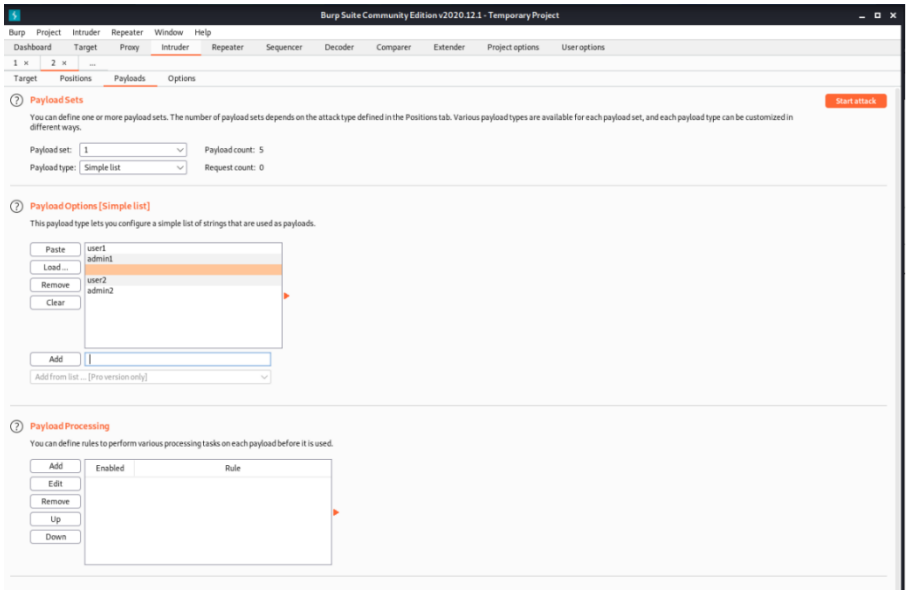


Pitchfork



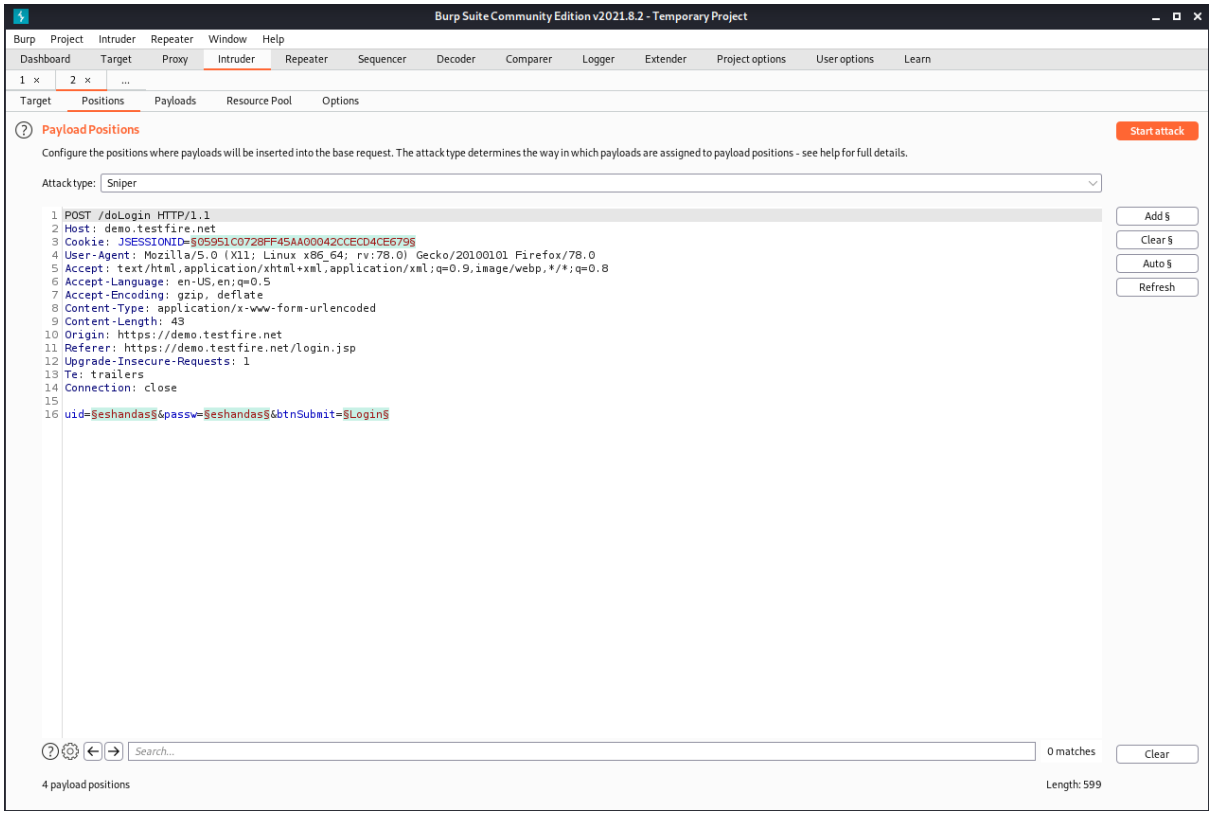
Cluster Bomb

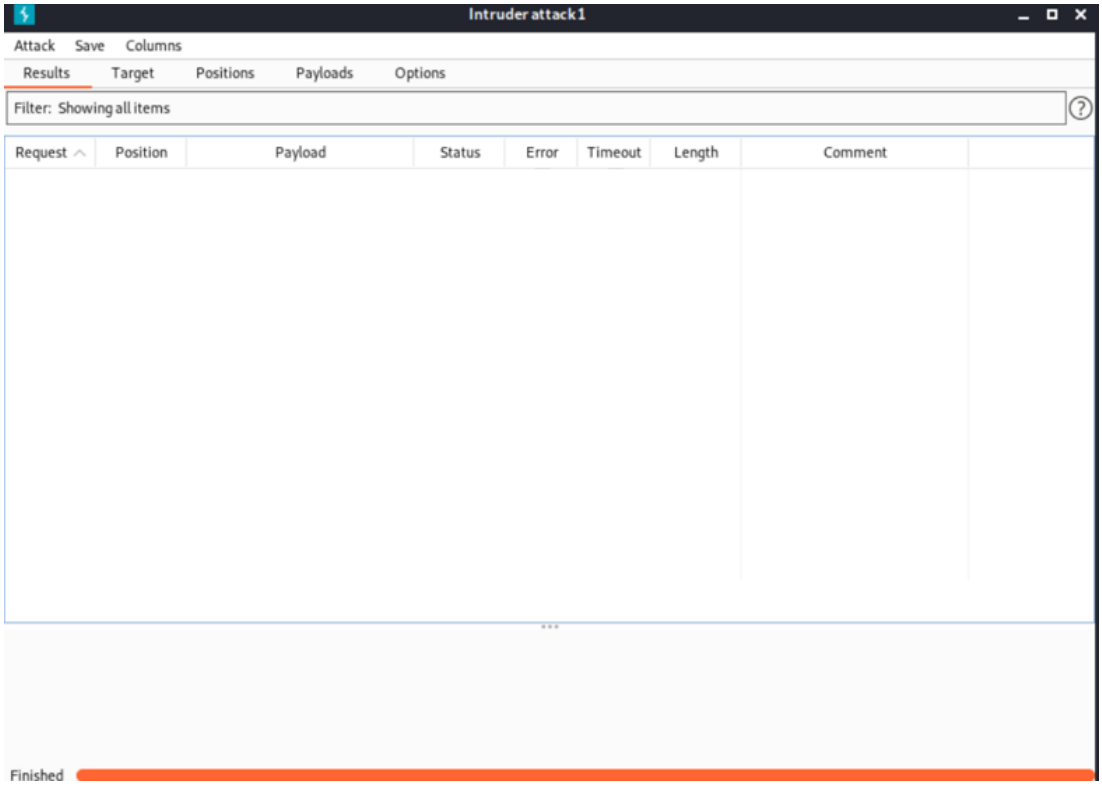
Payload

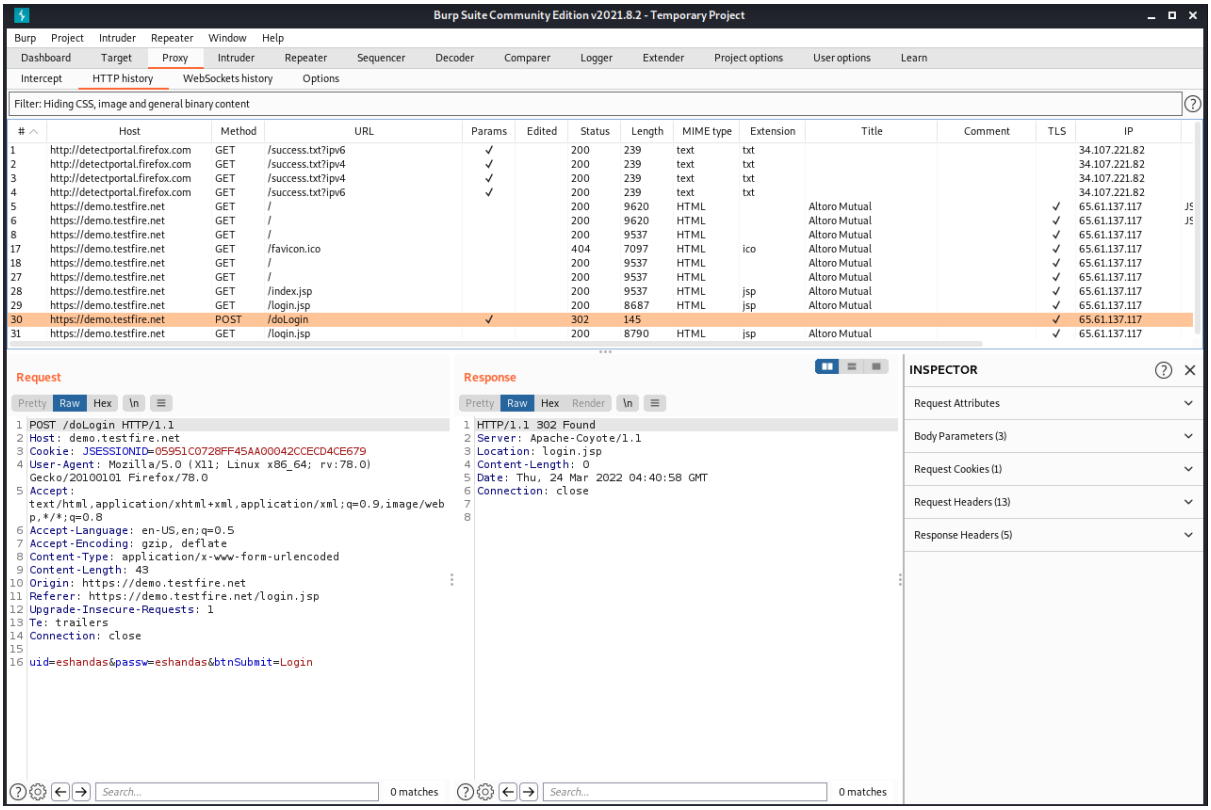


For sniper attack

Start attack

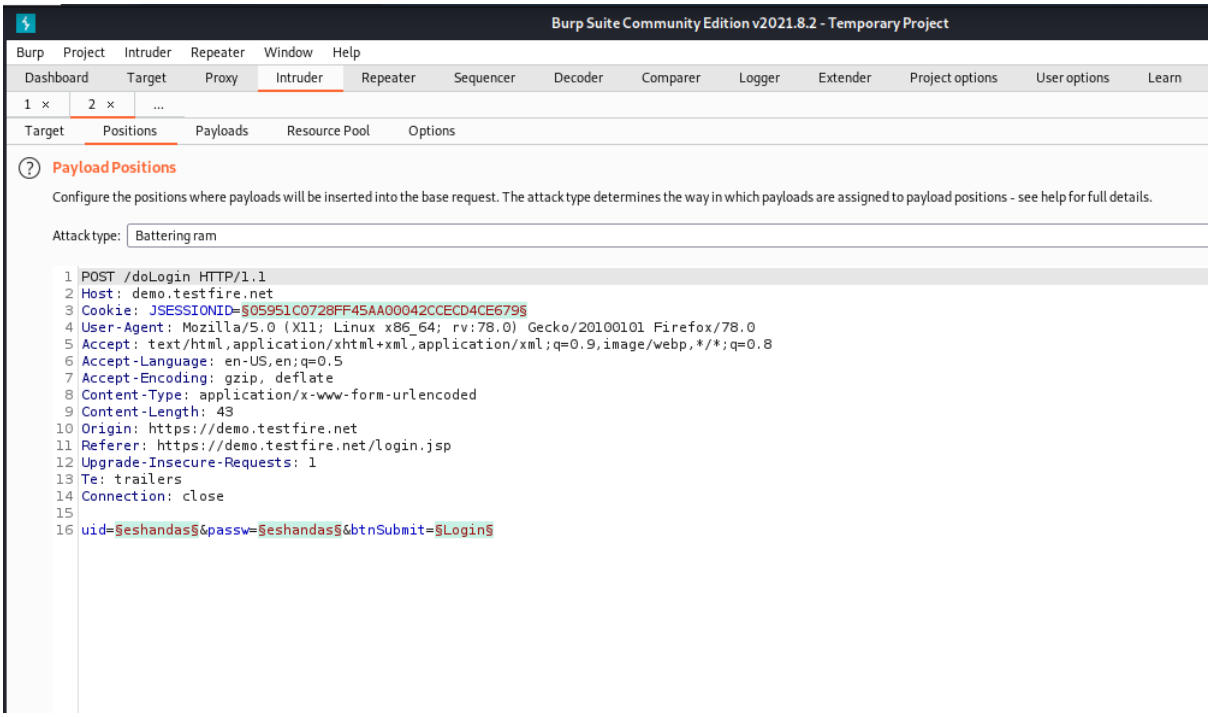


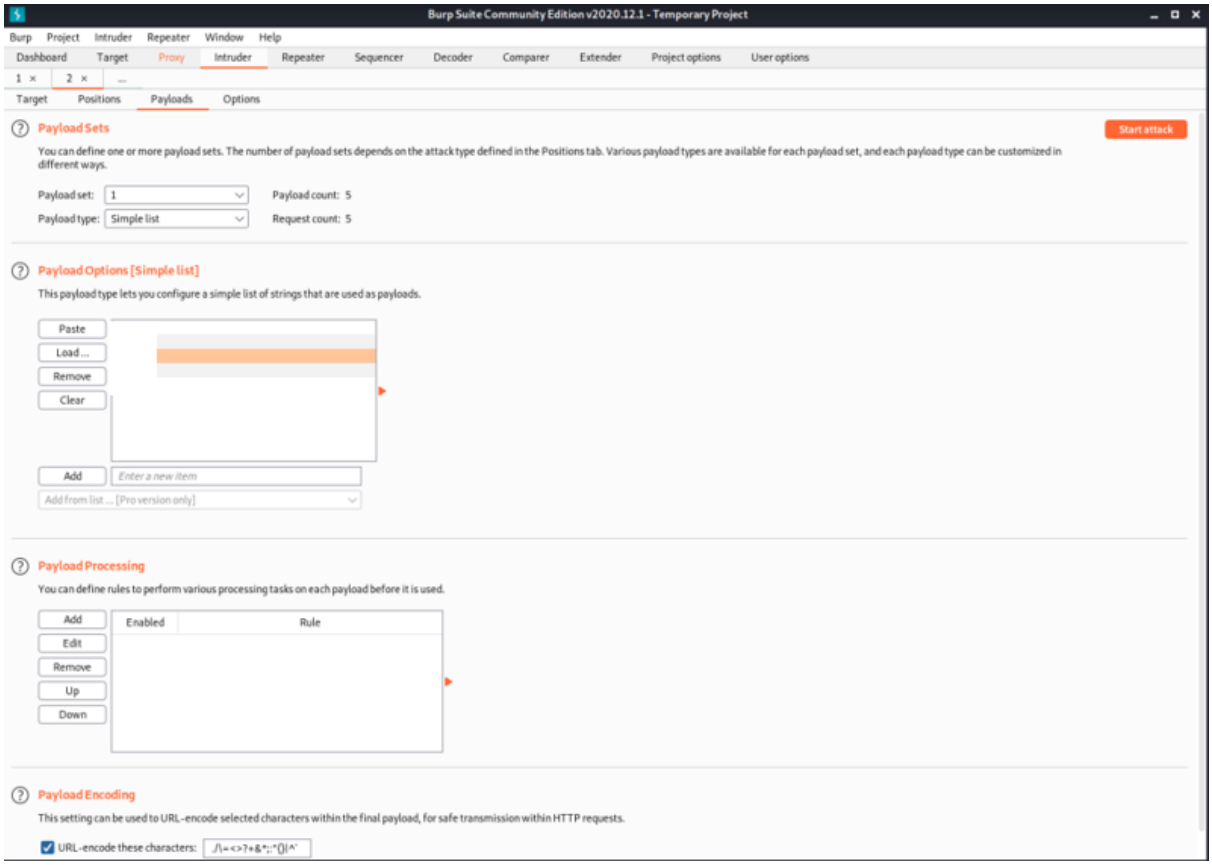

Intruder attack 1
Attack
Save
Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Position
Payload
Status
Error
Timeout
Length
Comment
Finished

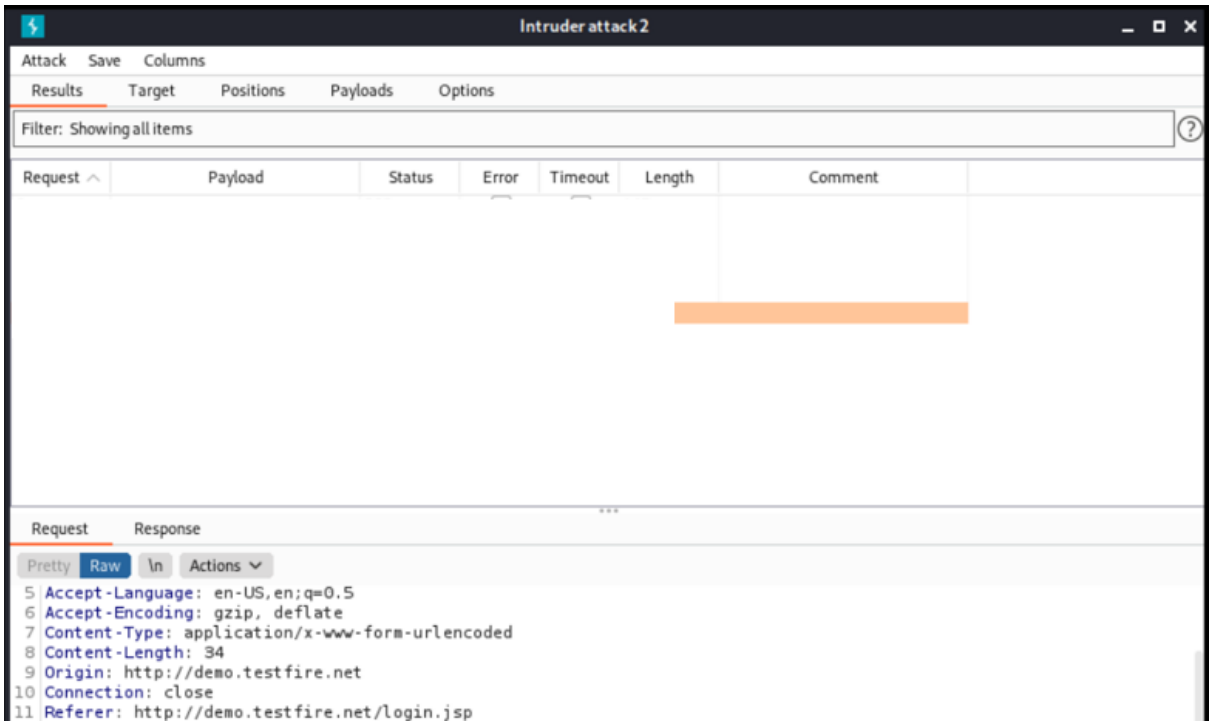

Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Request
Response
INSPECTOR
Request Attributes
Body Parameters (3)
Request Cookies (1)
Request Headers (13)
Response Headers (5)
0 matches
0 matches

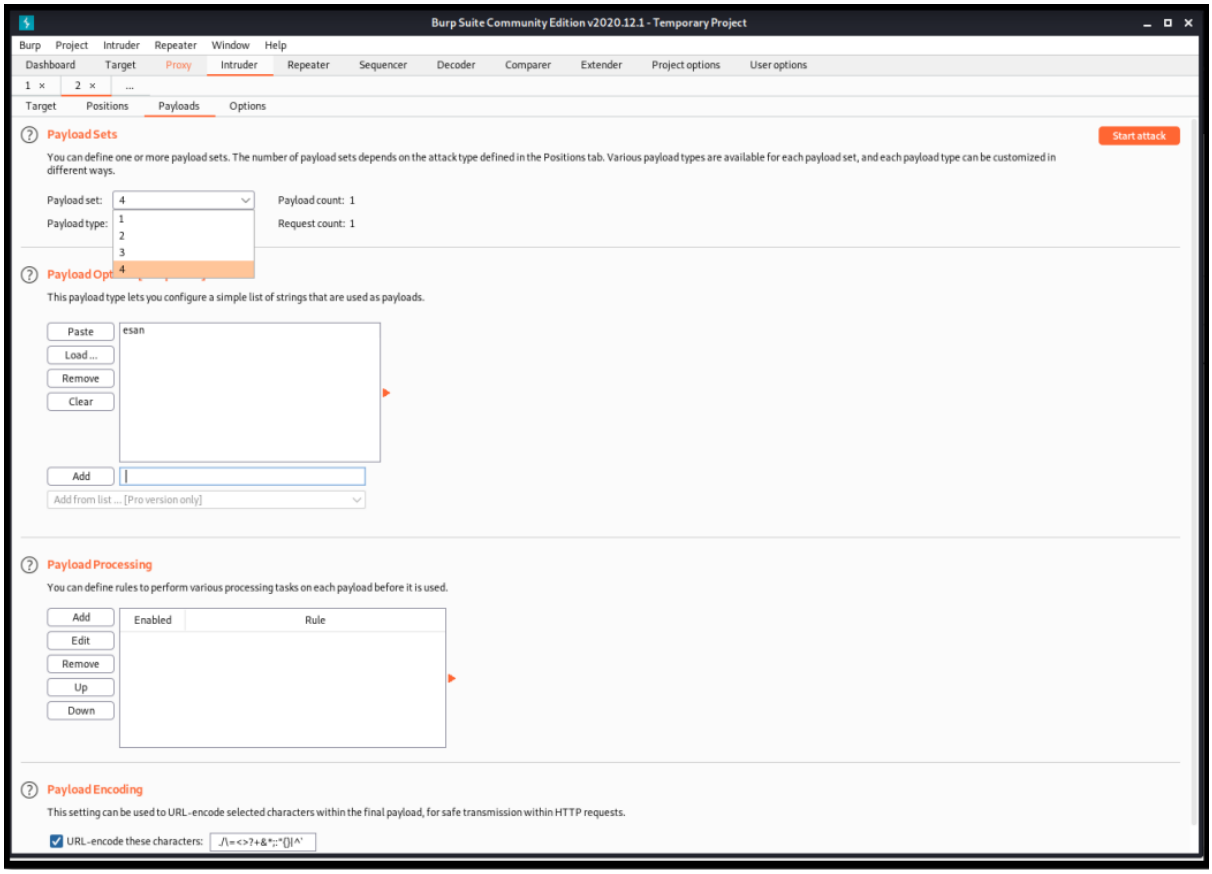
Demo website 4 attacks and Own website 4 attacks

Battering ram attack

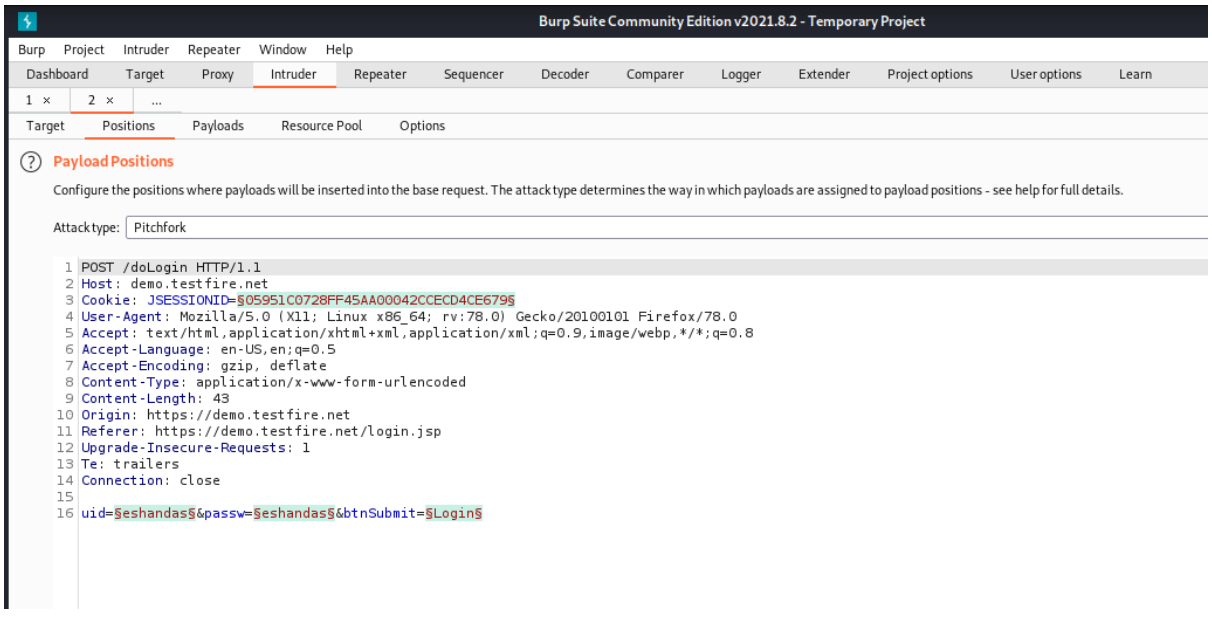


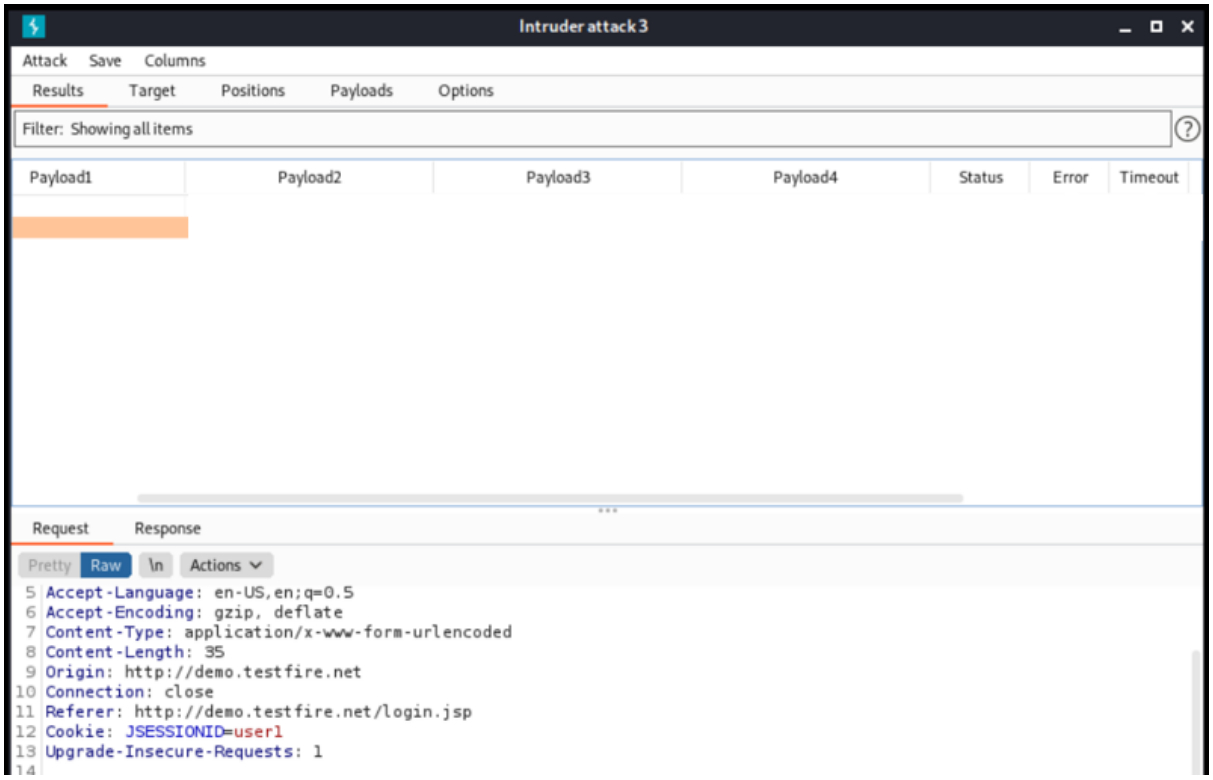

Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 5
Payload type: Simple list
Request count: 5
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:


Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
Request Response
Pretty Raw \n Actions
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp

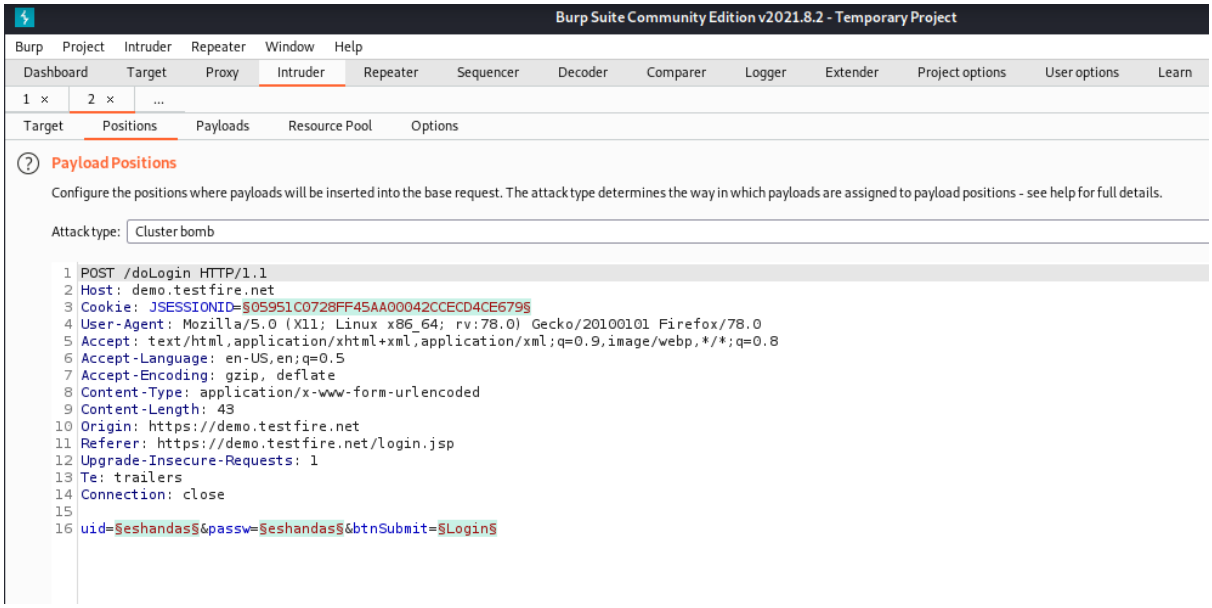


Pitchfork attack ()

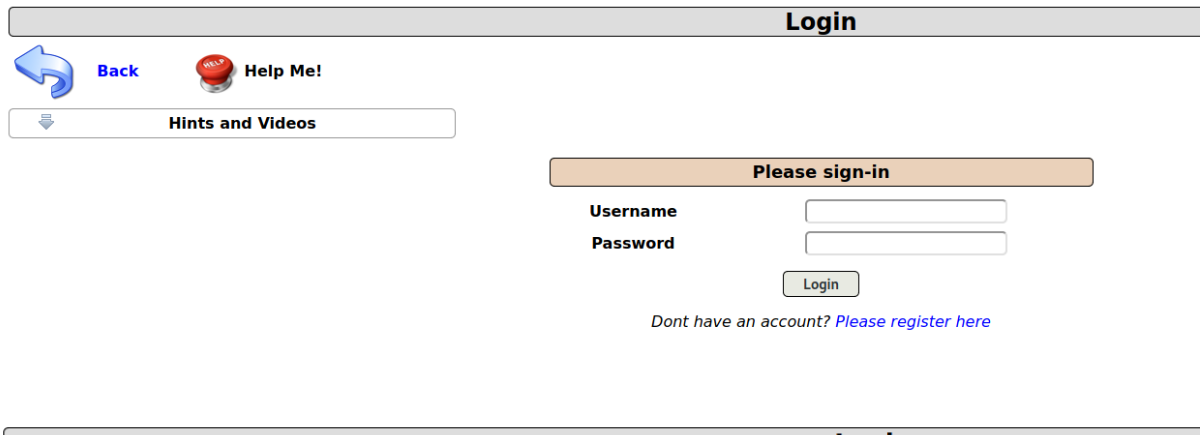


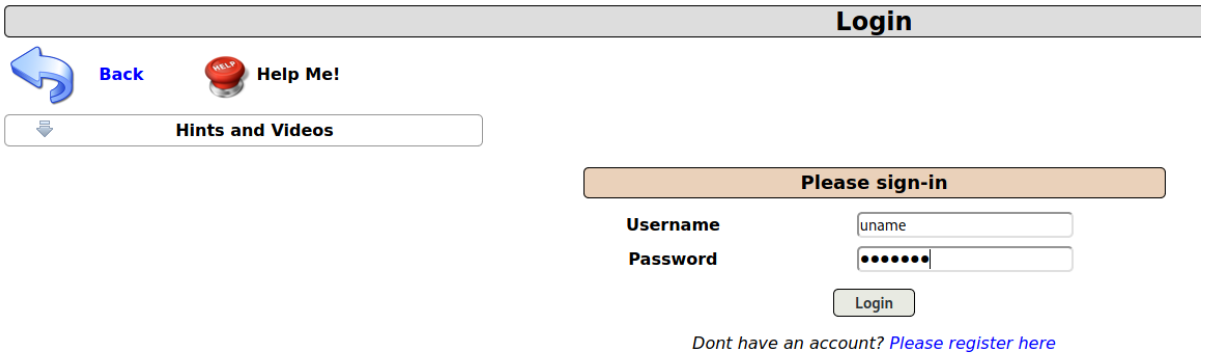


Clustering Bomb Attack



OWN website experiments





Username:uname

Password:pass123

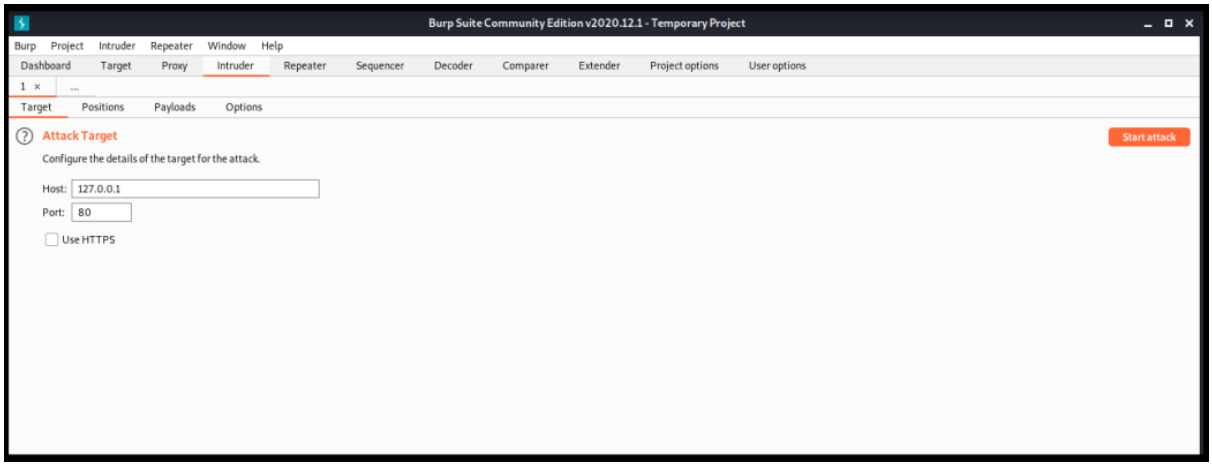
Click on ‘send to intruder.’ And turn intercept off.

Login the website Quickstore Admin Portal (Self-made website)

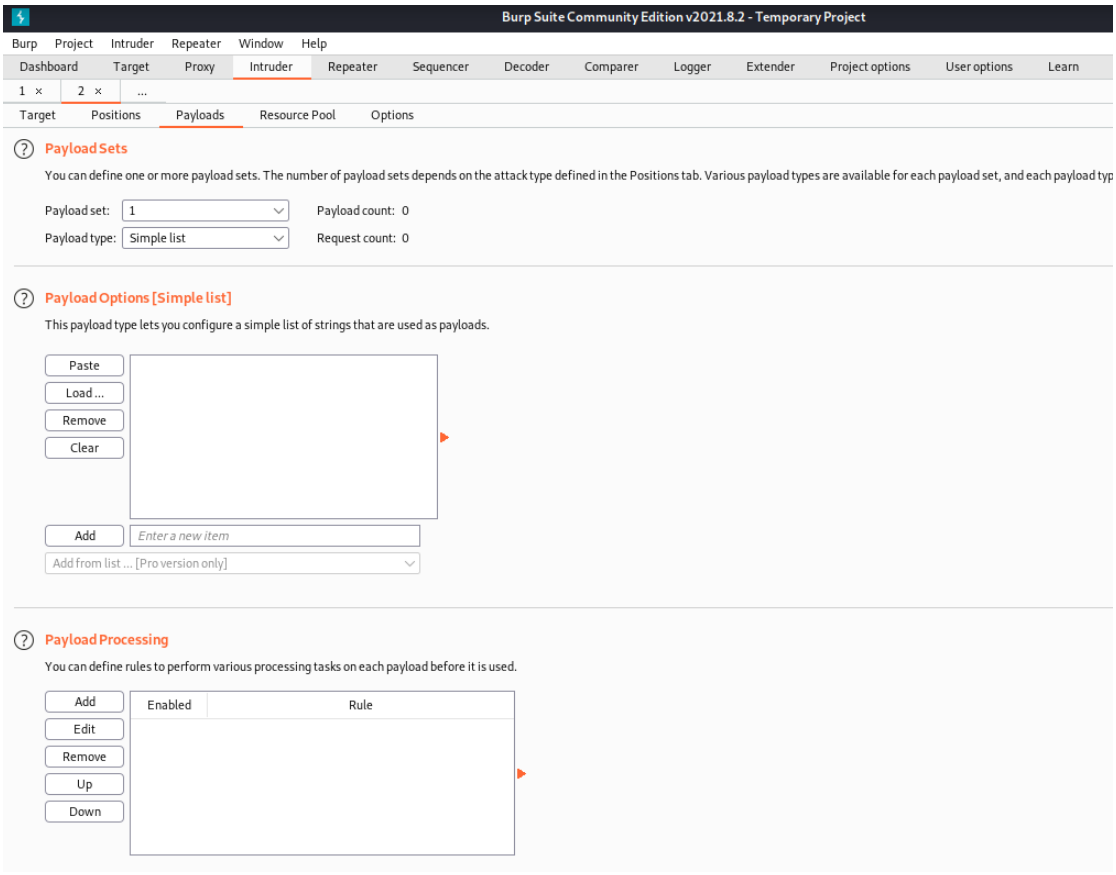
Go to burpsuite then choose Intruder and then select target

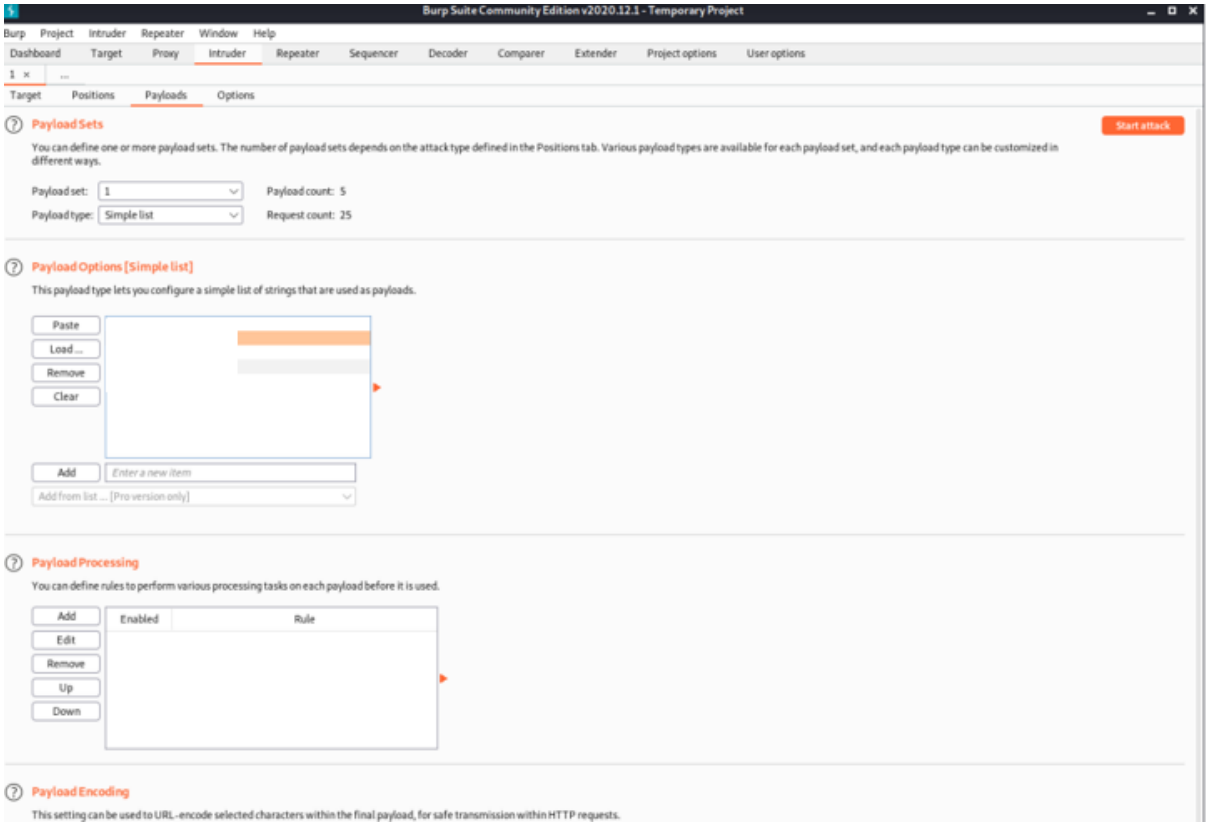
Again set target host as 127.0.0.1

Port :80

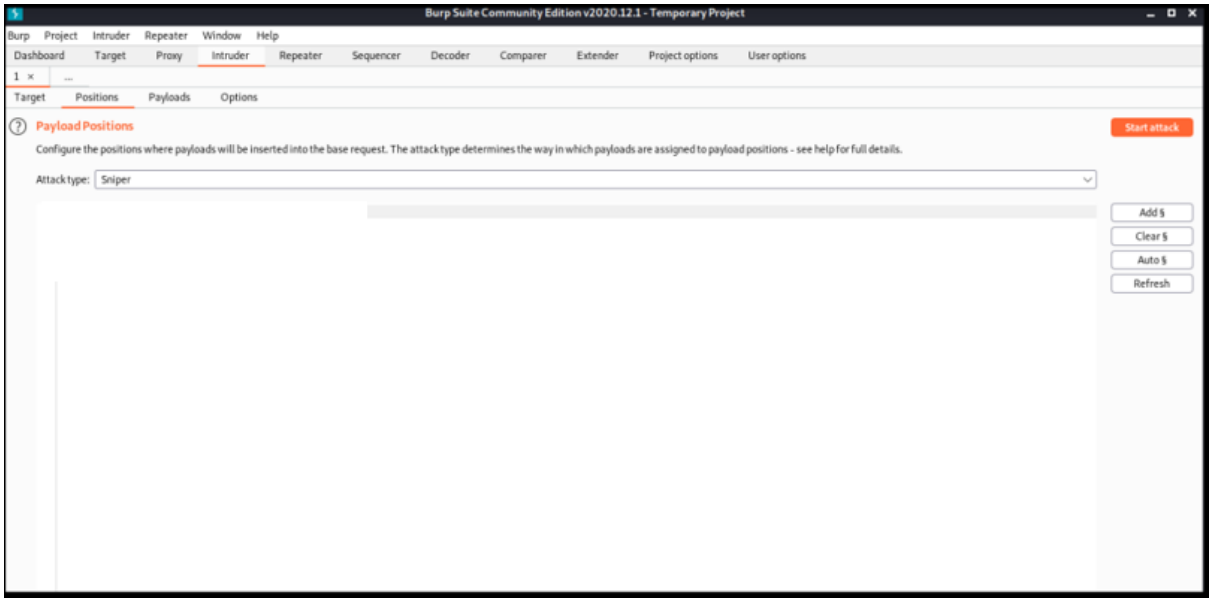


Go to payloads section and payloads as per attack type

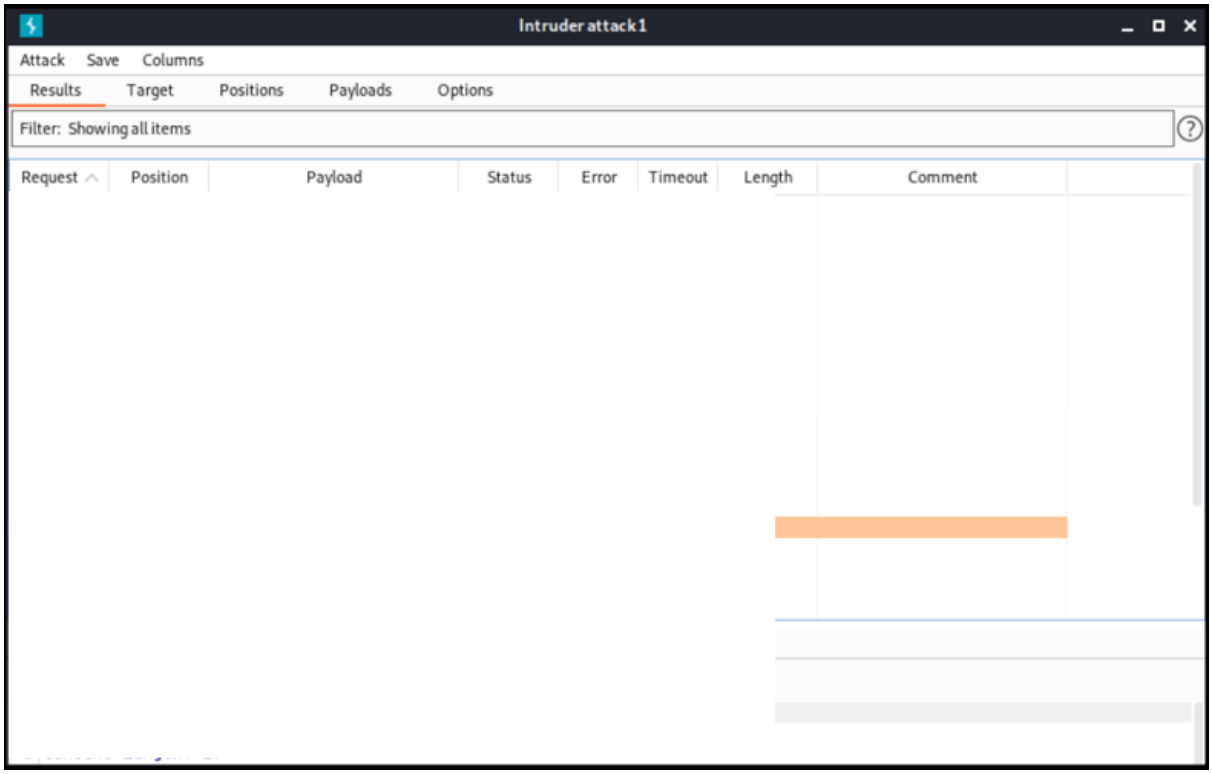




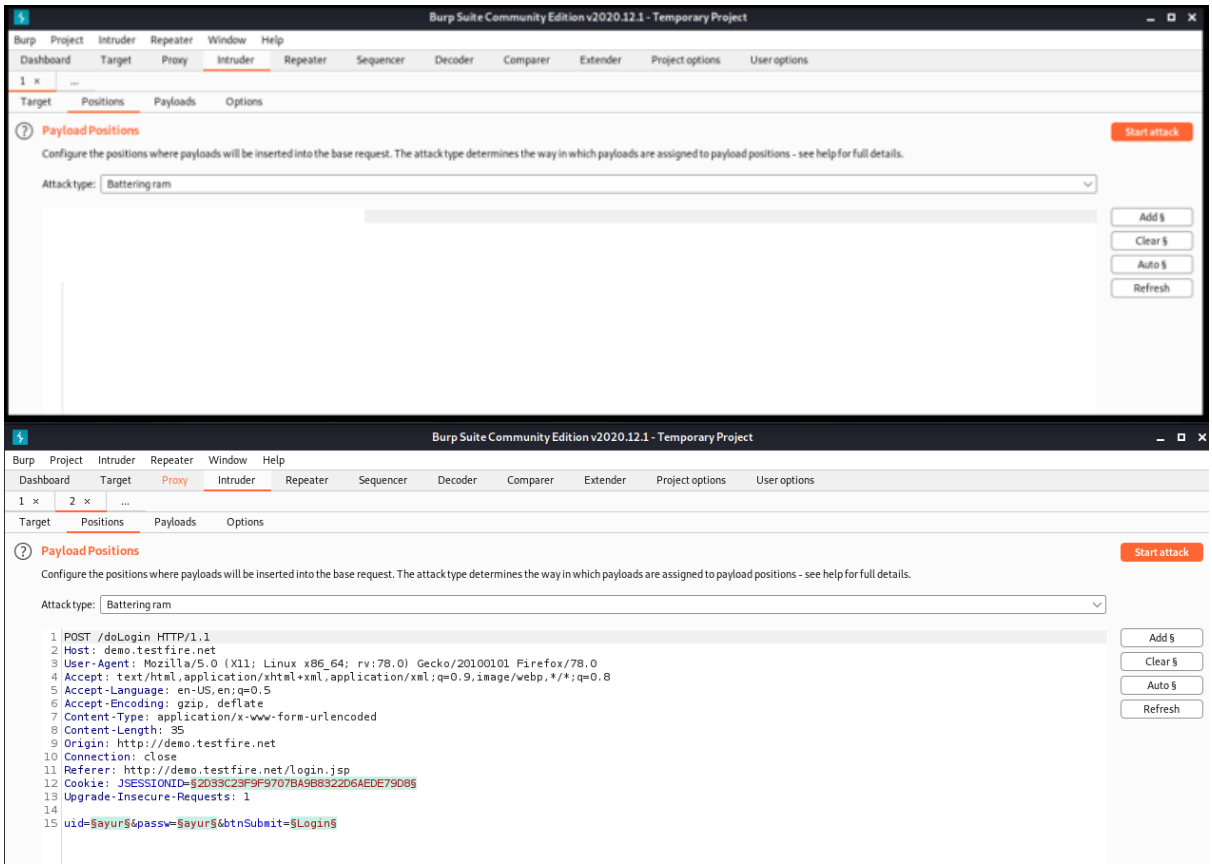
Set attack type: sniper

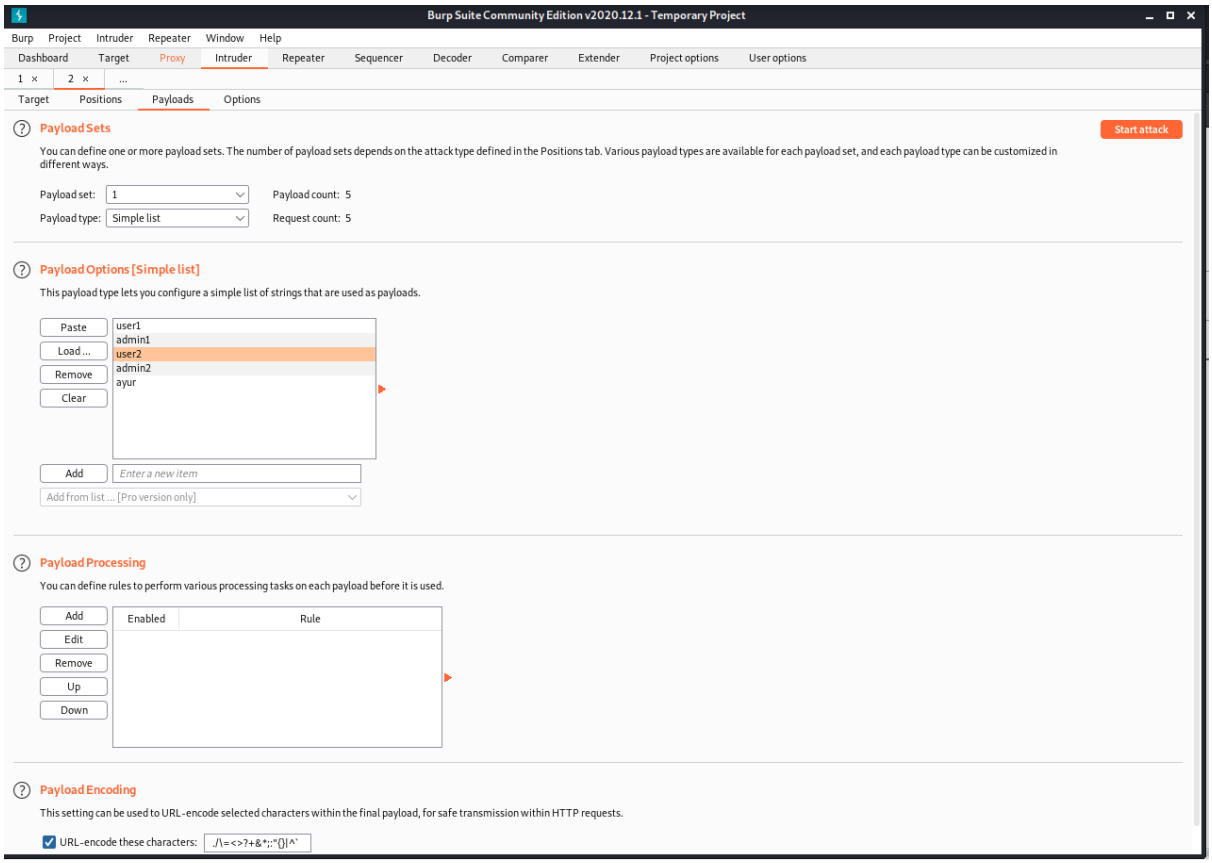


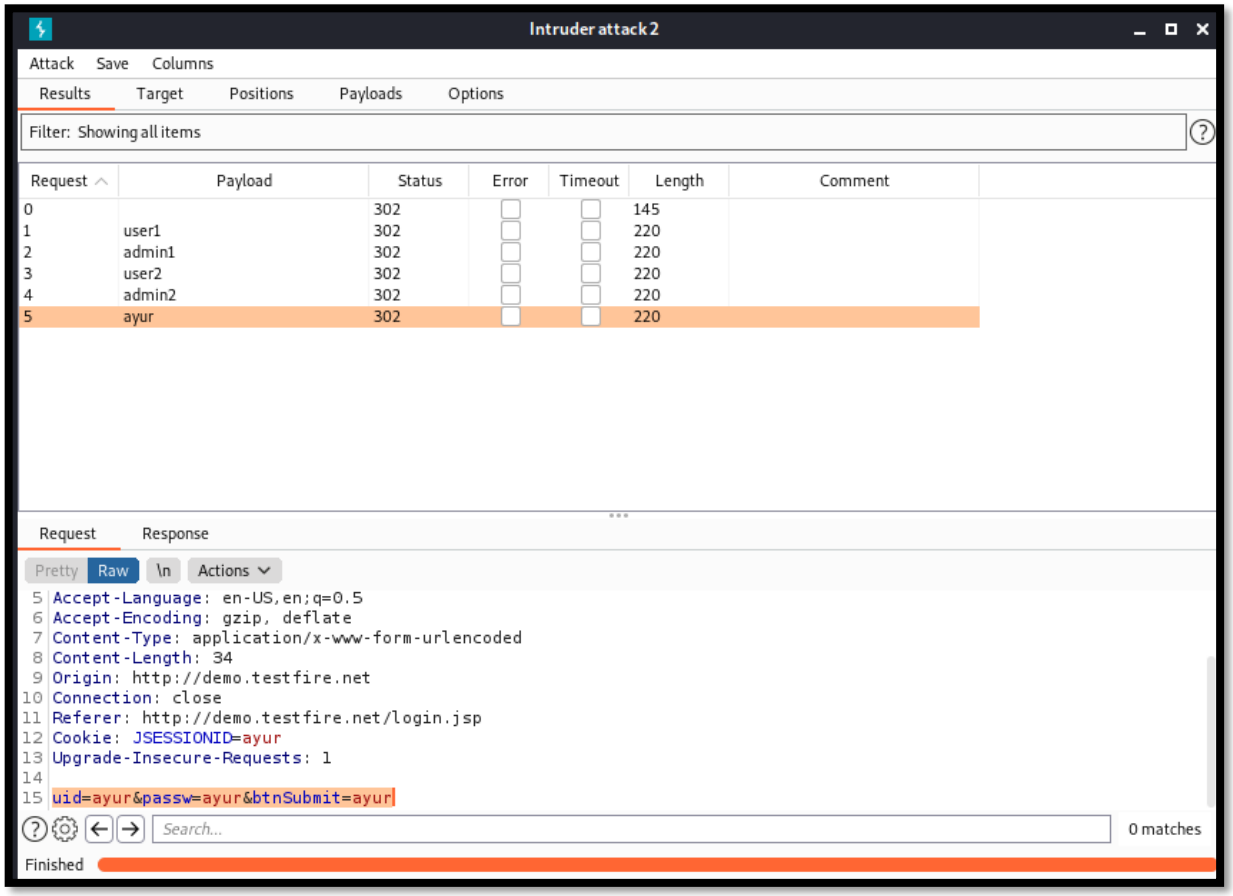
Start Attack

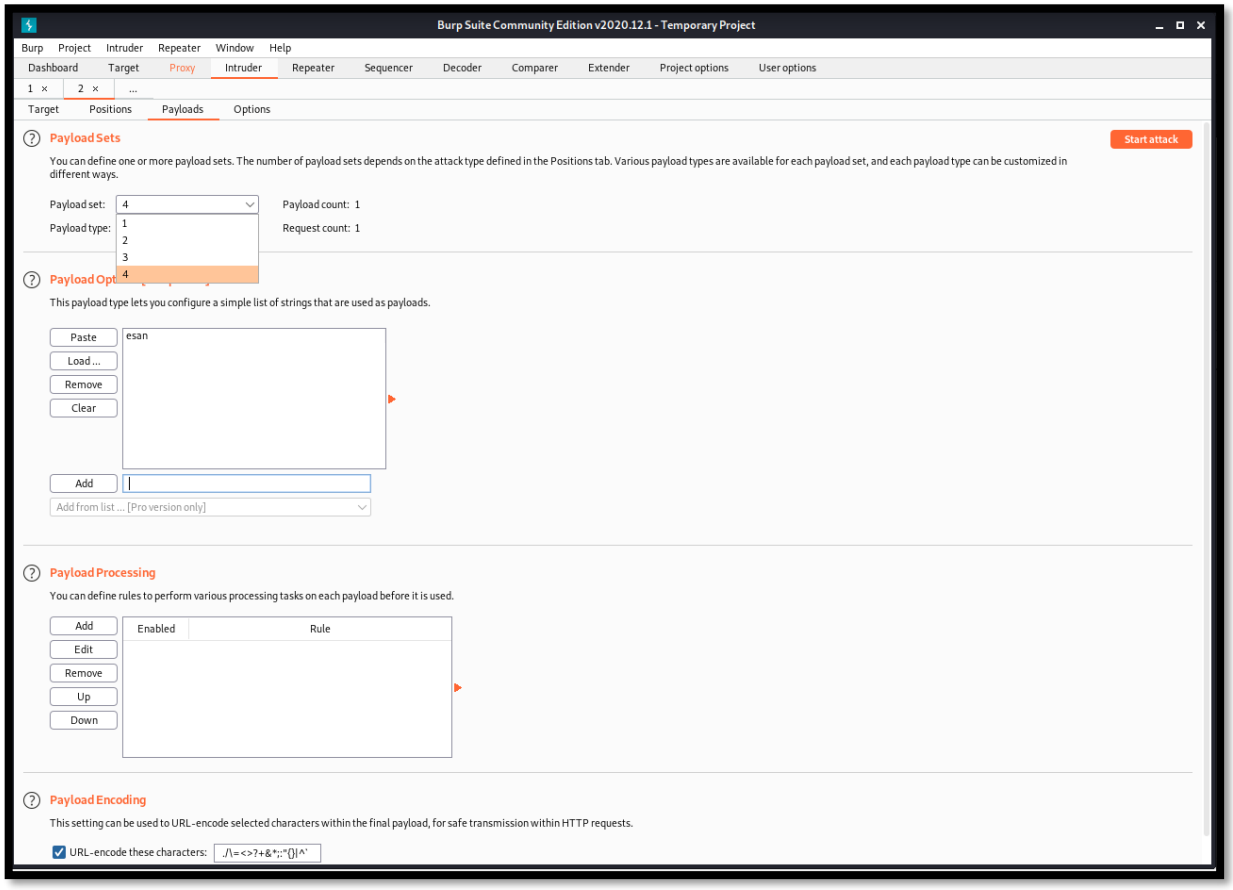


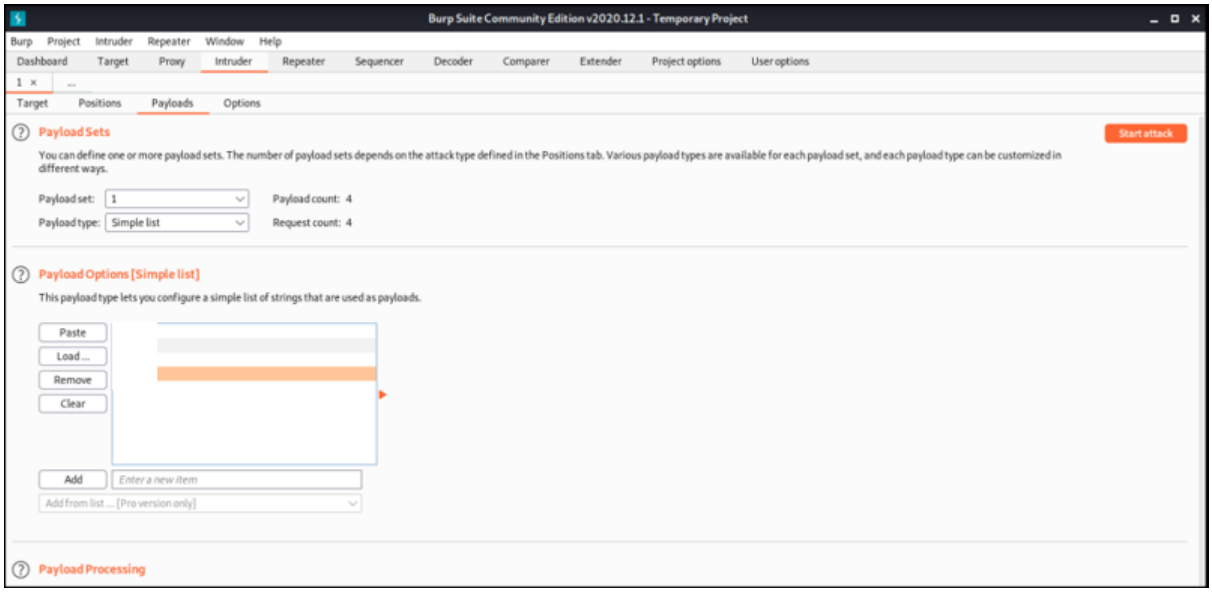
Battering ram attack




Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 5
Payload type: Simple list
Request count: 5
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
user1
admin1
user2
admin2
ayur
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`

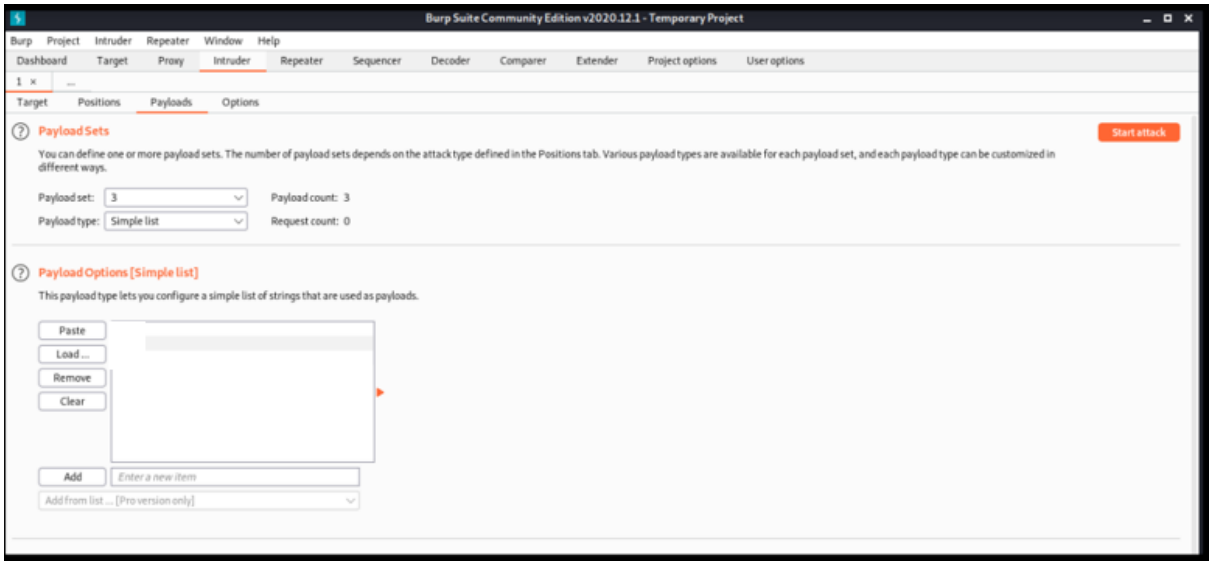

Intruder attack 2
Attack
Save
Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
0 302 145
1 user1 302 220
2 admin1 302 220
3 user2 302 220
4 admin2 302 220
5 ayur 302 220
Request
Response
Pretty
Raw
\n
Actions
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp
12 Cookie: JSESSIONID=ayur
13 Upgrade-Insecure-Requests: 1
14
15 uid=ayur&passw=ayur&btnSubmit=ayur
Search...
0 matches
Finished

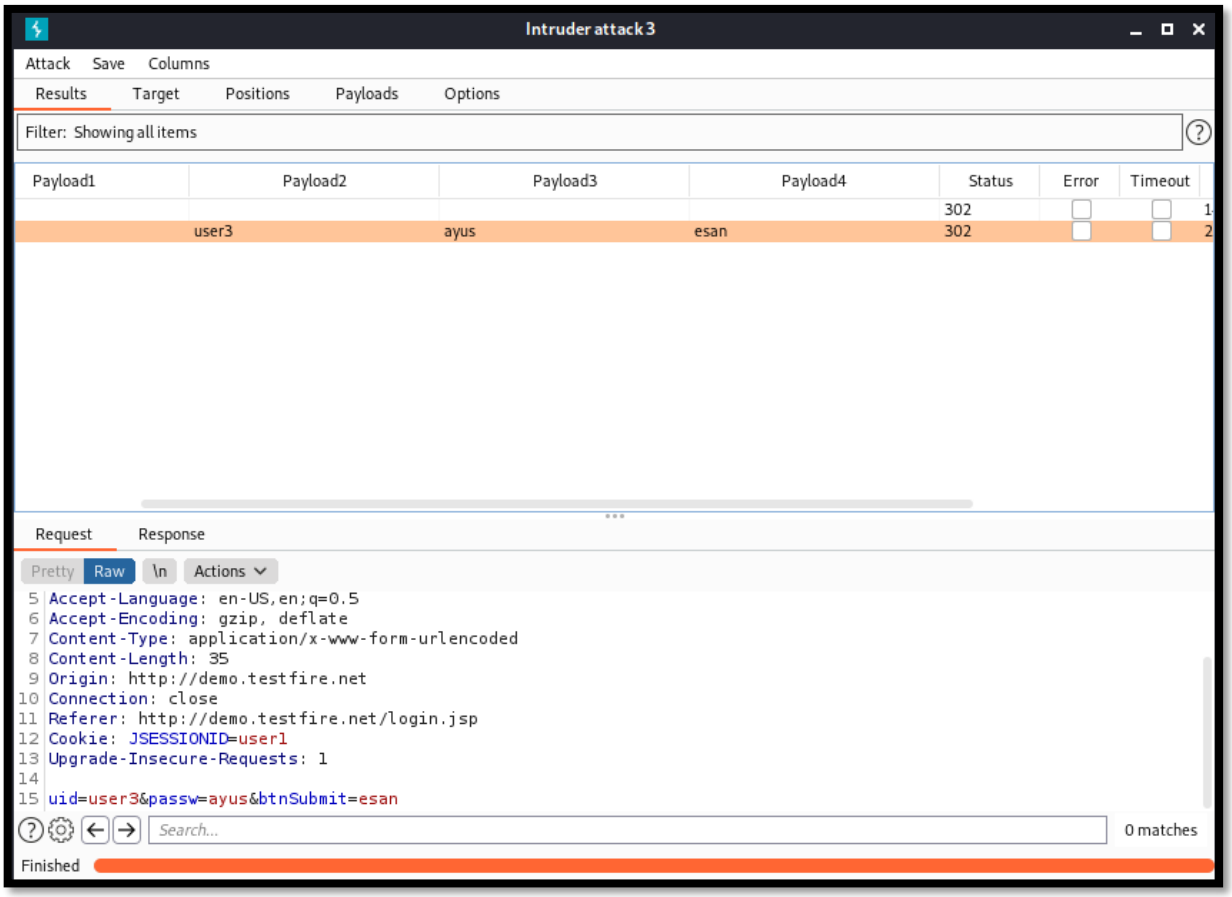


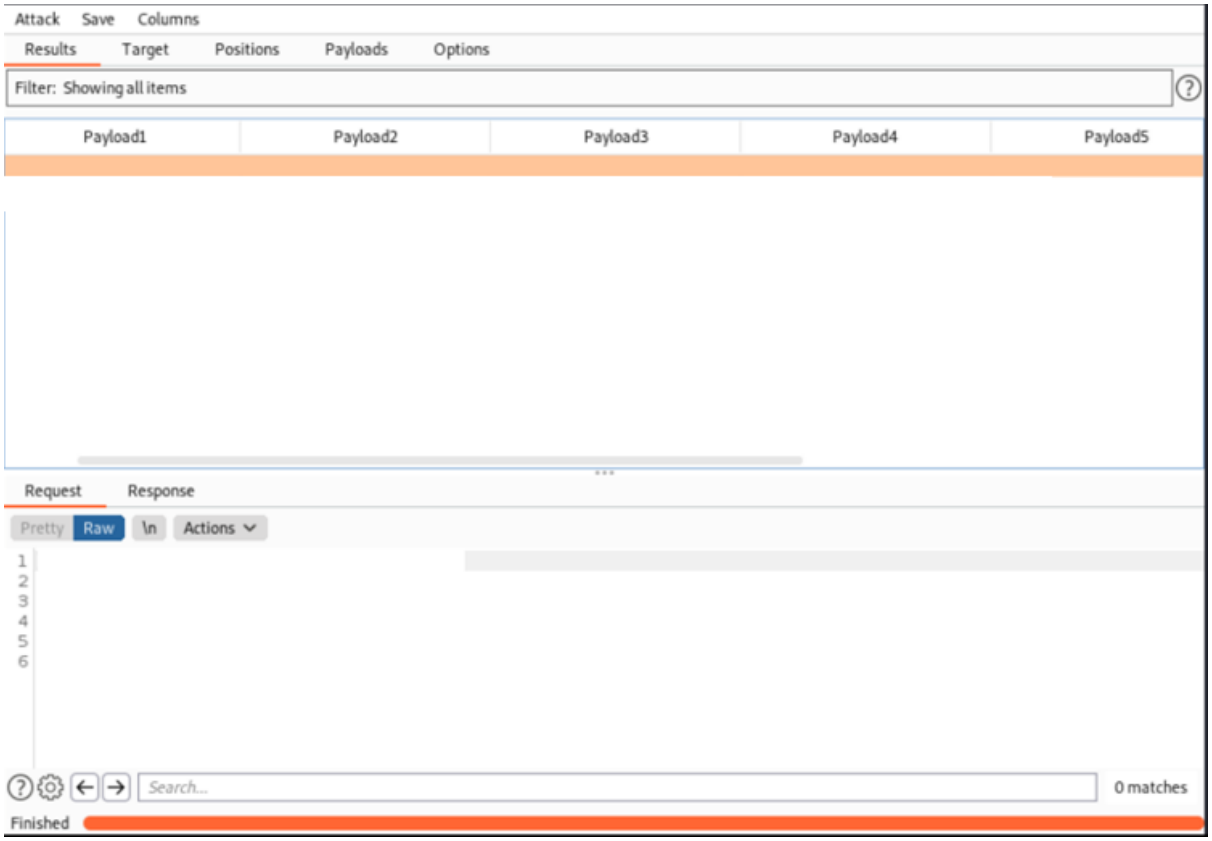


Pitchfork attack

Provide different values for payloads and click on start attack

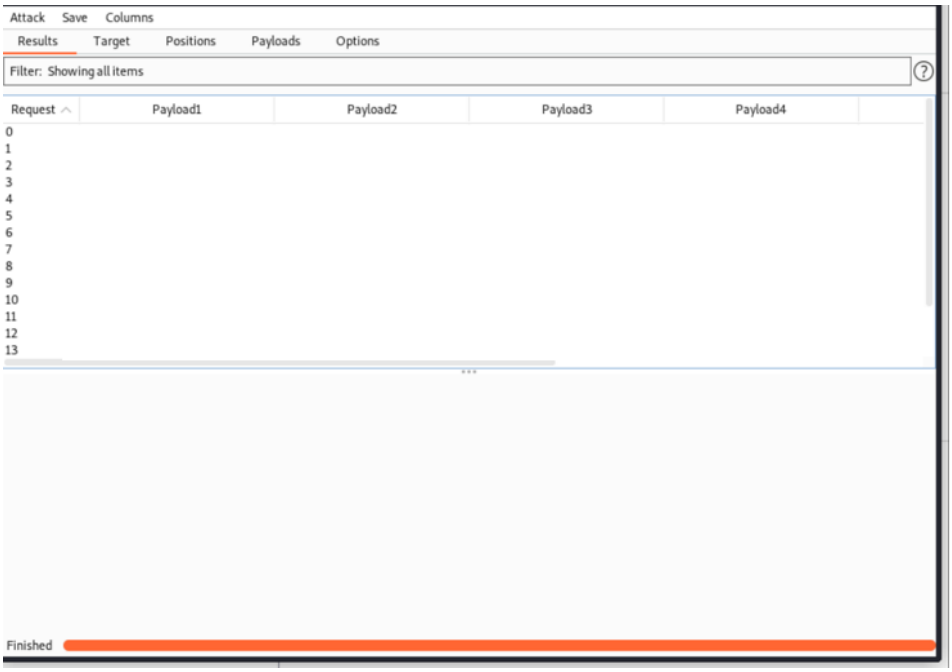


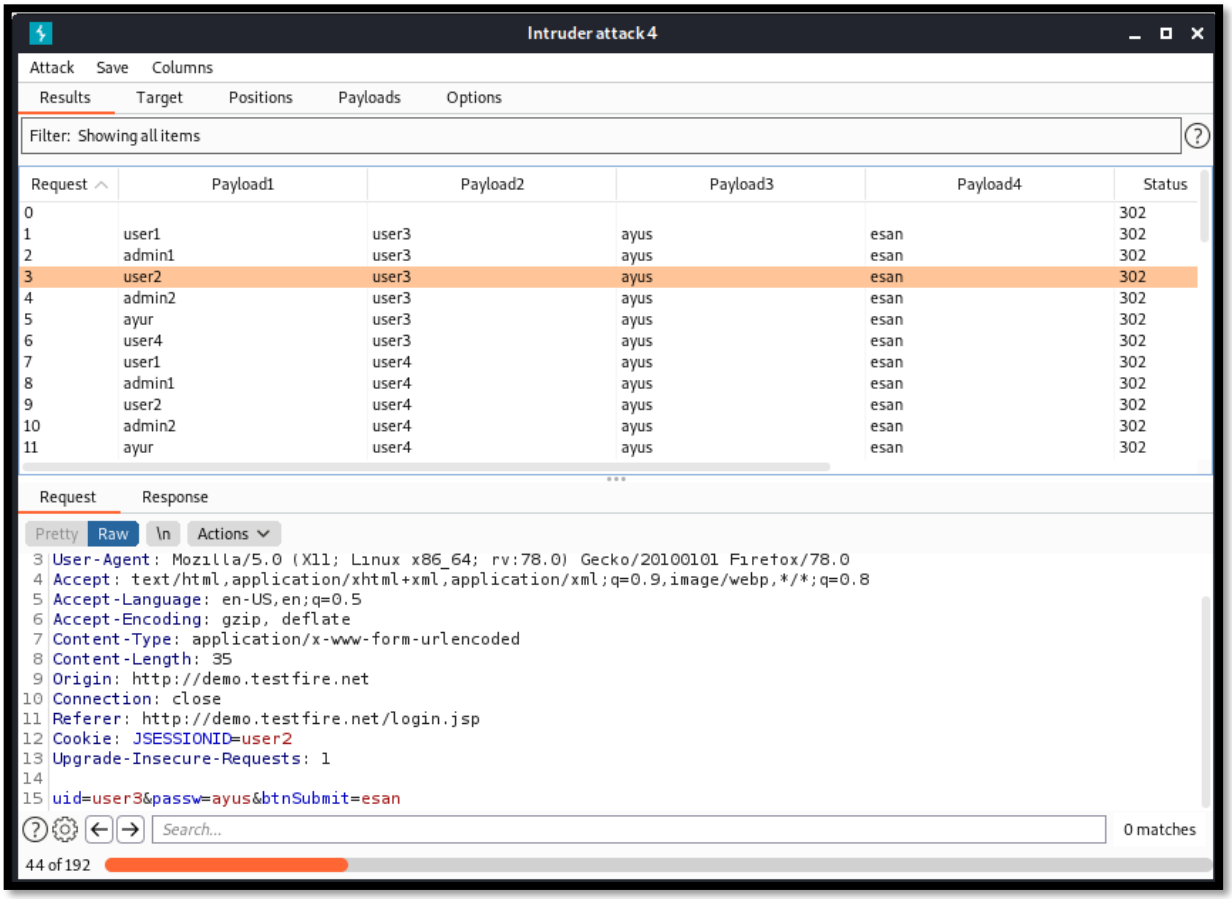




Clustering Bomb attack

Provide different values for payloads and click on start attack





Result: **All the attacks were successfully executed on a demo website and a self- made demo website used for login.**

LAB 10

Aryaman Mishra

19BCE1027

DVWA is made with PHP and MySQL for security professionals or aspiring security professionals to discover as many issues as possible and exploit some of the most commons vulnerabilities of web platforms like **SQL injection**, **Cross Site Scripting** (*XSS*), **Cross Site Request Forgery** (*CSRF*), and more.

https://github.com/digininja/DVWA.git

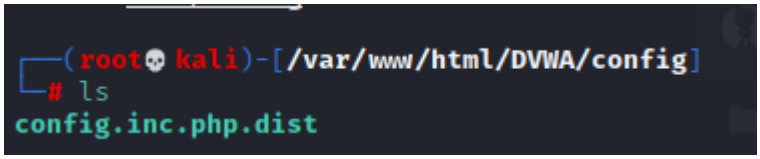
```
┌──(root💀kali)-[~]
└─# cd /var/www/html/
```

```
┌──(root💀kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 3798, done.
remote: Counting objects: 100% (905/905), done.
remote: Compressing objects: 100% (342/342), done.
remote: Total 3798 (delta 612), reused 590 (delta 552), pack-reused 2893
Receiving objects: 100% (3798/3798), 1.64 MiB | 377.00 KiB/s, done.
Resolving deltas: 100% (1824/1824), done.
```

```
┌──(root💀kali)-[/var/www/html]
└─# ls
DVWA  index.html  index.nginx-debian.html
```

```
┌──(root💀kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
```

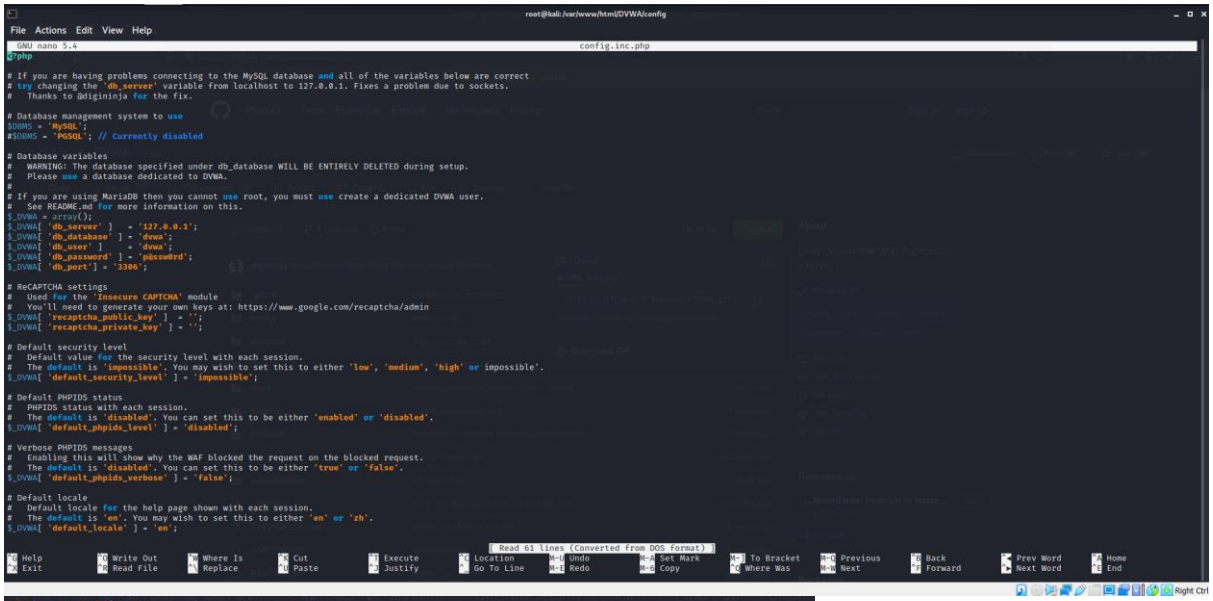
```
┌──(root💀kali)-[/var/www/html]
└─# cd DVWA/config
```



We will use the text editor to edit the configuration typing the following command:

sudo vim /var/www/html/dvwa/config/config.inc.php.dist

Change username and password as required by you.




```
┌──(root💀kali)-[~]
└─# cd /var/www/html/DVWA/config

┌──(root💀kali)-[/var/www/html/DVWA/config]
└─# ls
config.inc.php  config.inc.php.dist  config.inc.php.save  config.inc.php.save.1

┌──(root💀kali)-[/var/www/html/DVWA/config]
└─# cat config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ 'db_port'] = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
```

```
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ 'db_port'] = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
#   Enabling this will show why the WAF blocked the request on the blocked request.
#   The default is 'disabled'. You can set this to be either 'true' or 'false'.
$_DVWA[ 'default_phpids_verbose' ] = 'false';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

define ("MYSQL", "mysql");
define ("SQLITE", "sqlite");

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
#   This does not affect the backend for any other services, just these two labs.
#   If you do not understand what this means, do not change it.
$_DVWA["SQLI_DB"] = MYSQL;
#$_DVWA["SQLI_DB"] = SQLITE;
#$_DVWA["SQLITE_DB"] = "sqli.db";

?>

┌──(root💀kali)-[/var/www/html/DVWA/config]
└─#
```

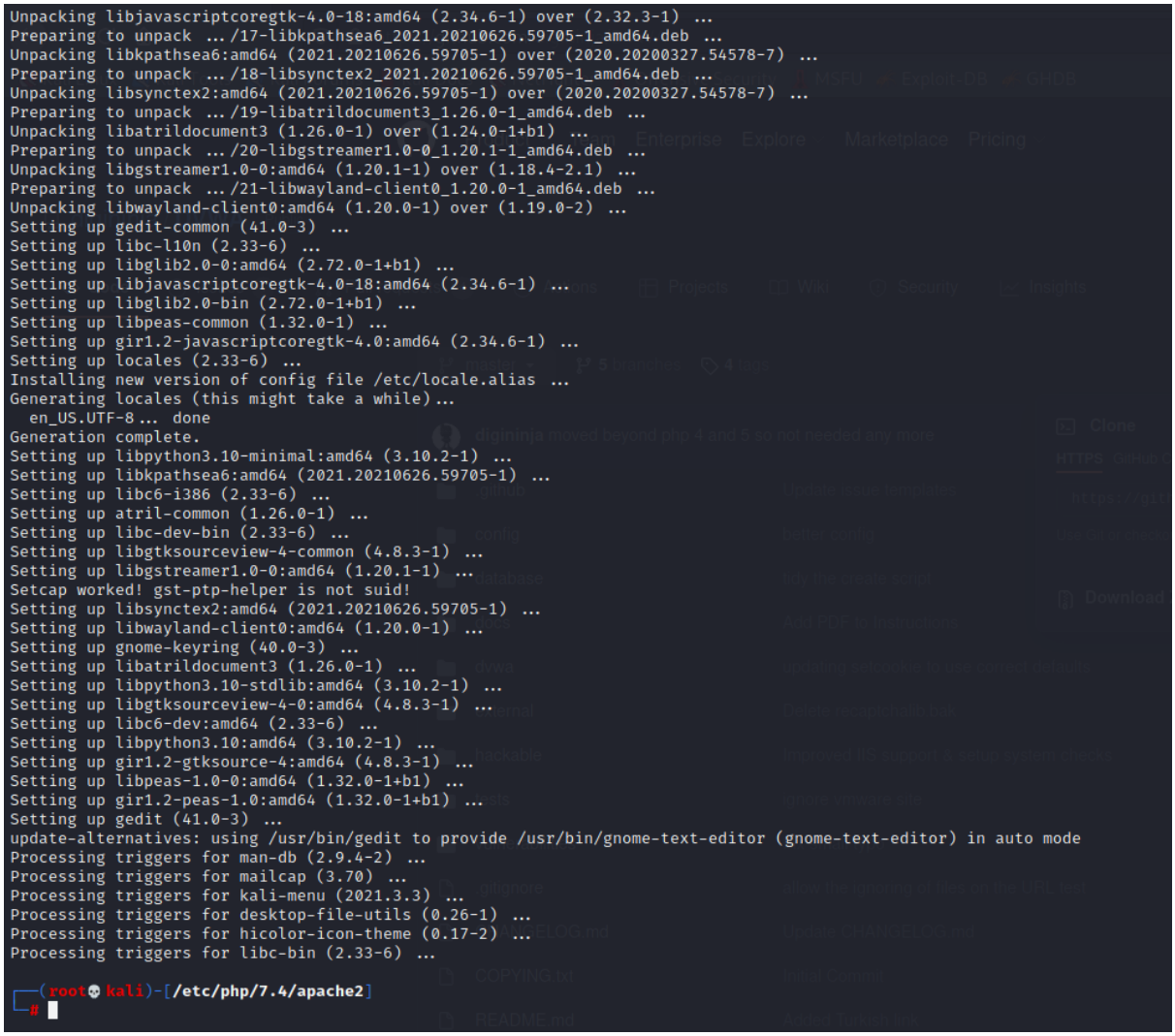
Start Mysql server.

```
┌──(root💀kali)-[~]
└─# service mysql start

┌──(root💀kali)-[~]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Create a user in MariaBD and grant all priviledges to ‘user’@127.0.0.1

```
┌──(root㉿kali)-[~]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'user'@'127.0.0.1' identify by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'identify by 'pass'' at line 1
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified  by 'pass';
Query OK, 0 rows affected (0.053 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@127.0.0.1 identified by 'pass';
Query OK, 0 rows affected (0.054 sec)

MariaDB [(none)]>
```

```
┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
7.4

┌──(root㉿kali)-[/etc/php]
└─# cd 7.4

┌──(root㉿kali)-[/etc/php/7.4]
└─# cd apache2

┌──(root㉿kali)-[/etc/php/7.4/apache2]
└─# ls
conf.d  php.ini

┌──(root㉿kali)-[/etc/php/7.4/apache2]
└─# gedit php.ini
Command 'gedit' not found, but can be installed with:
apt install gedit
Do you want to install it? (N/y)y
apt install gedit
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  atril-common bubblewrap fonts-mathjax fonts-roboto-slab gdal-data gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gnome-desktop3-data gobject-introspection libarmadillo10 libarpack2 libatrildocument3 libcfitsio9
  libcharls2 libdap27 libdapclient6v5 libdjvulibre-text libdjvulibre21 libepsilon1 libfreexl1 libfyba0 libgdal28 libgeos-3.9.1 libgeos-c1v5 libgeotiff5 libgnome-desktop-3-19 libgs9 libgs9-common libgxps2 libharfbuzz-icu0 libhdf4-0-alt
  libhdf5-hl-100 libheif1 libijs-0.35 libjavascriptcoregtk-4.0-18 libjbig2dec0 libjs-mathjax libkmlbase1 libkmldom1 libkmlengine1 libkpathsea6 libmanette-0.2-0 libnetcdf18 libodbc1 libogdi4.1 libpaper-utils libpaper1 libpipewire-0.3-0
  libpipewire-0.3-common libpipewire-0.3-modules libproj19 libqhull8.0 librttopo1 libsoup-gnome2.4-1 libspa-0.2-modules libspatialite7 libspectre1 libsuperlu5 libsynctex2 liburiparser1 libwpe-1.0-1 libwpebackend-fdo-1.0-1
  libxerces-c3.2 libxkbregistry0 odbcinst odbcinst1debian2 pipewire pipewire-bin pipewire-media-session proj-data pwgen python-mpltoolkits.basemap-data python3-adblockparser python3-advancedhttpserver python3-boltons python3-cairo-dev
  python3-docx python3-ecdsa python3-exif python3-exifread python3-gdal python3-geoip2 python3-geojson python3-graphene-sqlalchemy python3-icalendar python3-ipwhois python3-maxminddb python3-mpltoolkits.basemap python3-networkx
  python3-phonenumbers python3-pptx python3-pygraphviz python3-pypdf2 python3-pyproj python3-pyshp python3-requests-file python3-rule-engine python3-secure python3-singledispatch python3-smoke-zephyr python3-stem xdg-dbus-proxy
  xdg-desktop-portal xdg-desktop-portal-gtk zenity-common
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  atril-common gcc-12-base gedit-common gir1.2-gtksource-4 gir1.2-javascriptcoregtk-4.0 gir1.2-peas-1.0 gnome-keyring libatrildocument3 libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libglib2.0-0 libglib2.0-bin
  libgstreamer1.0-0 libgtksourceview-4-0 libgtksourceview-4-common libjavascriptcoregtk-4.0-18 libkpathsea6 libpeas-1.0-0 libpeas-common libpython3.10 libpython3.10-minimal libpython3.10-stdlib libstdc++6 libsynctex2 libwayland-client0
  locales
Suggested packages:
  gedit-plugins glibc-doc libnss-nis libnss-nisplus manpages-dev gstreamer1.0-tools
Recommended packages:
  yelp zenity manpages-dev libc-devtools
The following packages will be REMOVED:
  atril gir1.2-webkit2-4.0 kali-desktop-xfce kali-hidpi-mode king-phisher libatrilview3 libwebkit2gtk-4.0-37 zenity
The following NEW packages will be installed:
  gcc-12-base gedit gedit-common gir1.2-gtksource-4 gir1.2-peas-1.0 libgtksourceview-4-0 libgtksourceview-4-common libpeas-1.0-0 libpeas-common libpython3.10 libpython3.10-minimal libpython3.10-stdlib
The following packages will be upgraded:
```

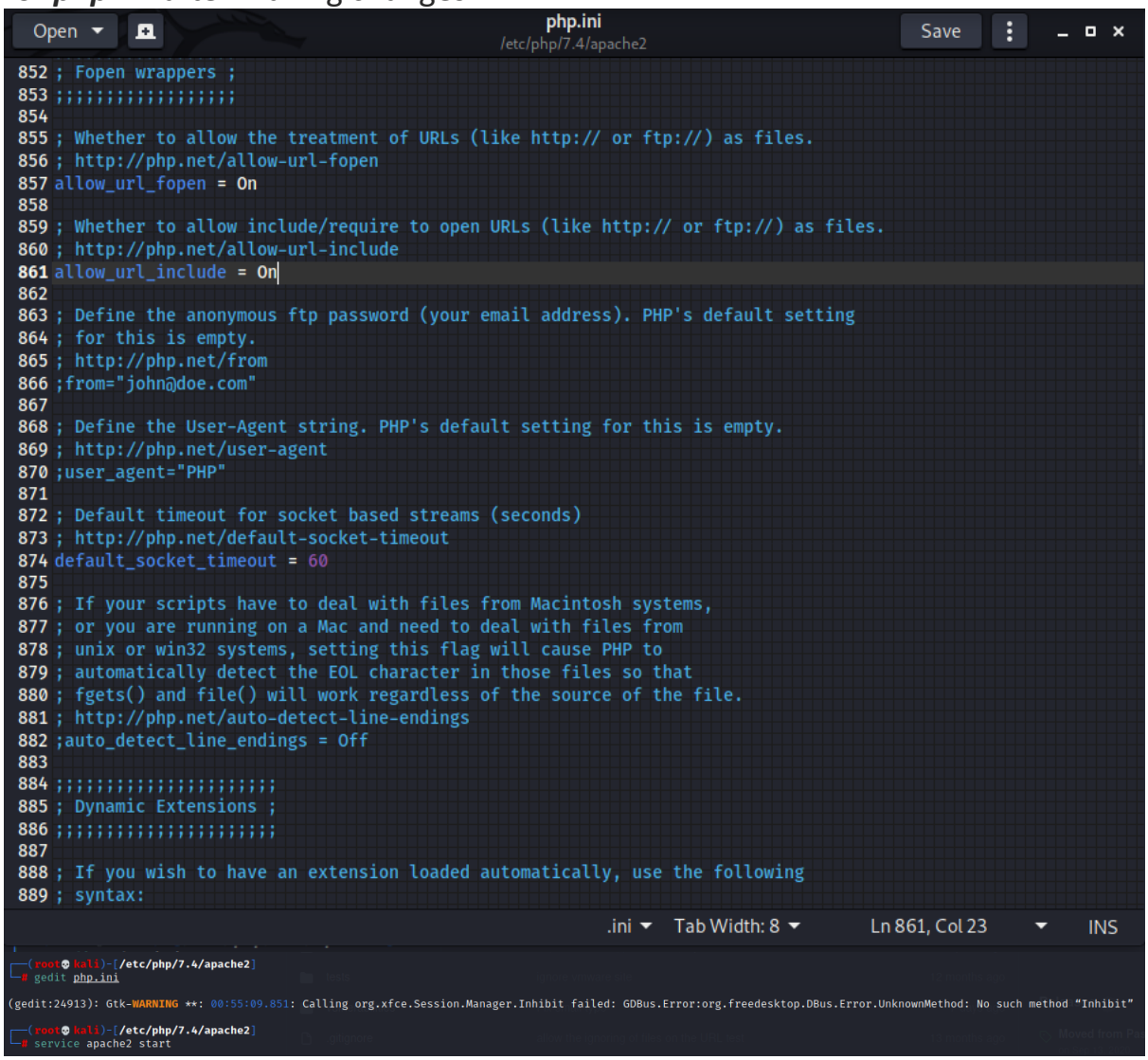


Once done, we need to edit the main config (***php.ini***) file for apache2, which is not correctly overridden for **DVWA** by default.

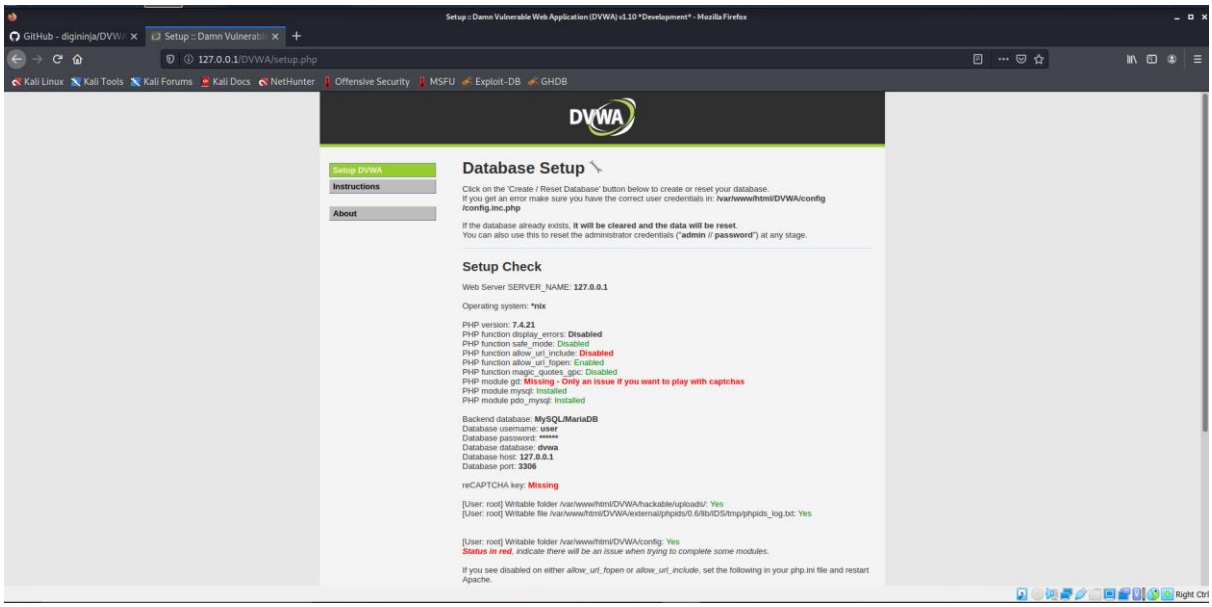
sudo vim /etc/php5/apache2/php.ini

- Enable Allow_url_fopen
- Enable Allow_url_include

This is necessary to exploit the file upload vulnerability. Here's a screenshot for ***php.ini*** after making changes.



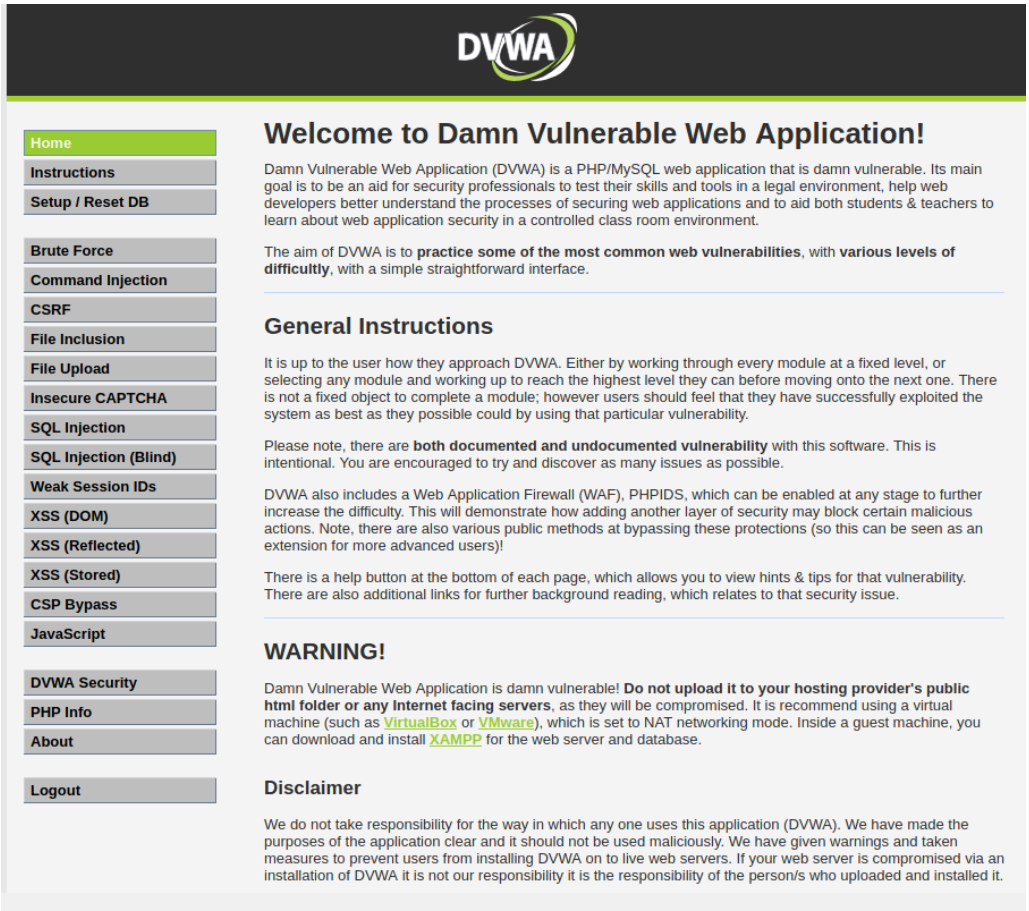
Access localhost/DVWA and work with DVWA Application.



Scroll and click ‘recreate database’ option and you will be redirected to login page.

Username:**admin**

Password:**password**

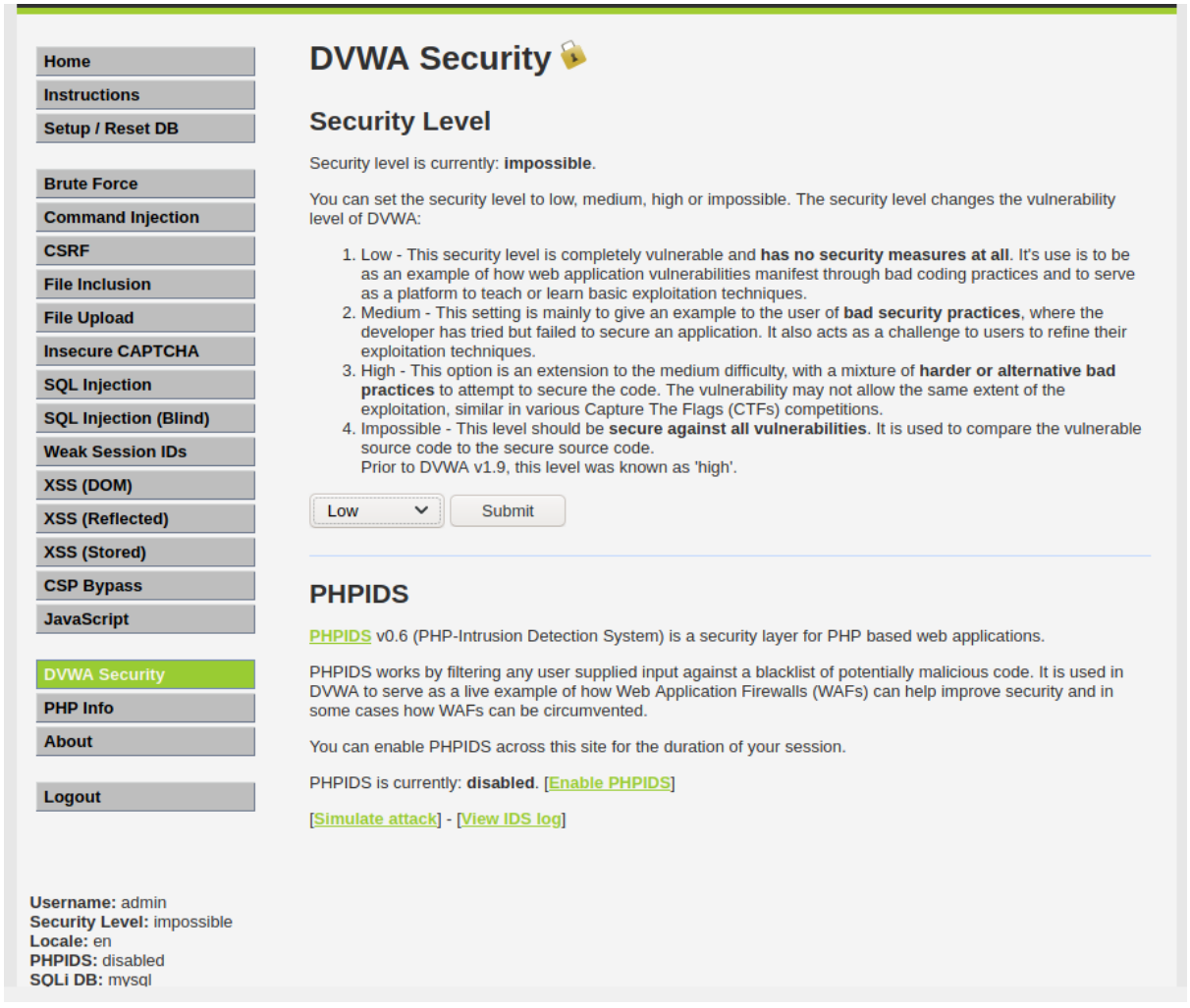


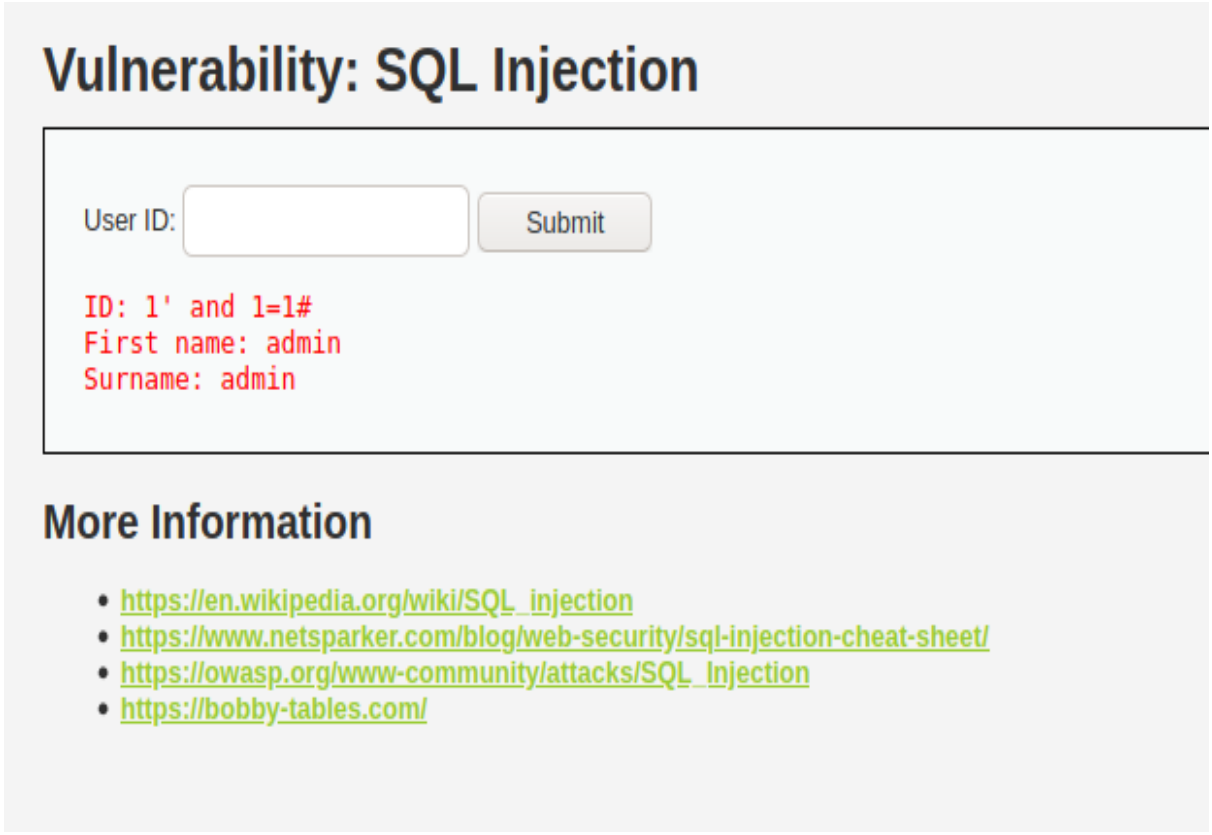
Now, login to change the strength of vulnerabilities by clicking on “DVWA Security”.

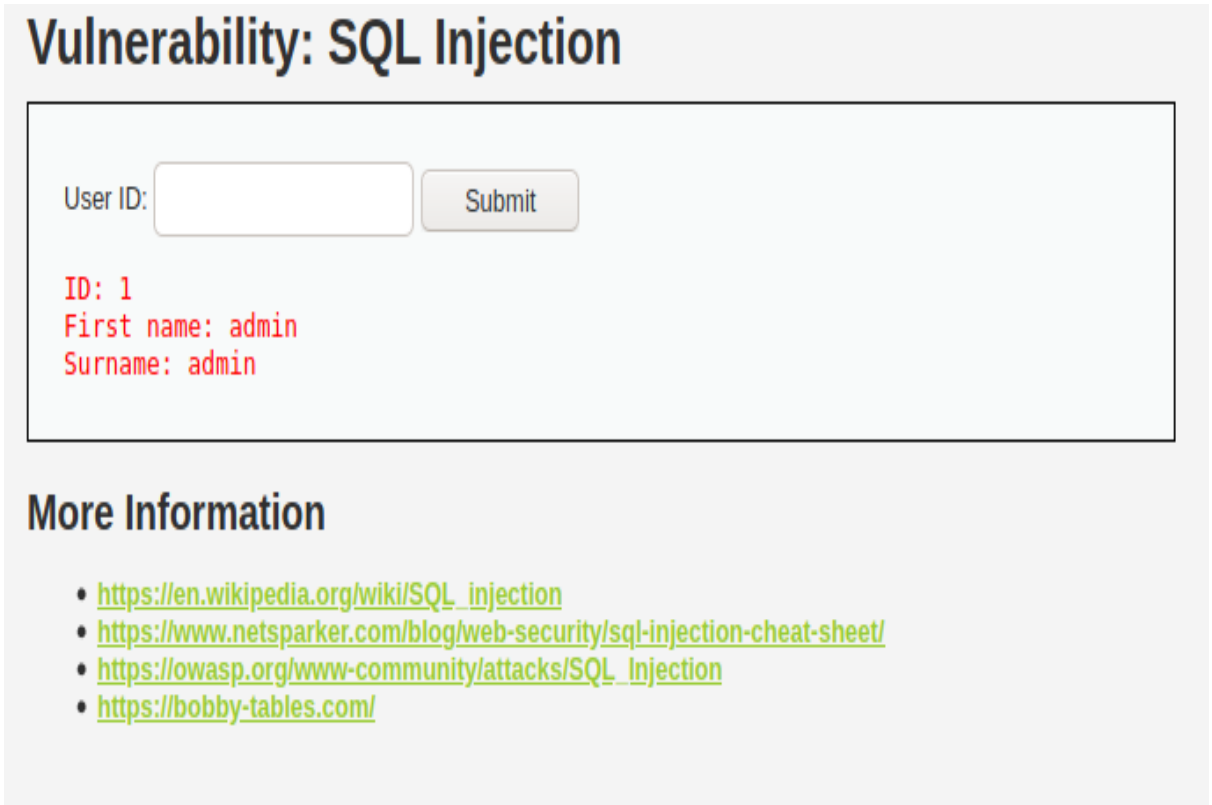
Low Level: Low-Level Security gives you the freedom to exploit all known vulnerabilities means there will be no security in a given framework and hence you can try all attacks if you are using it first Time.

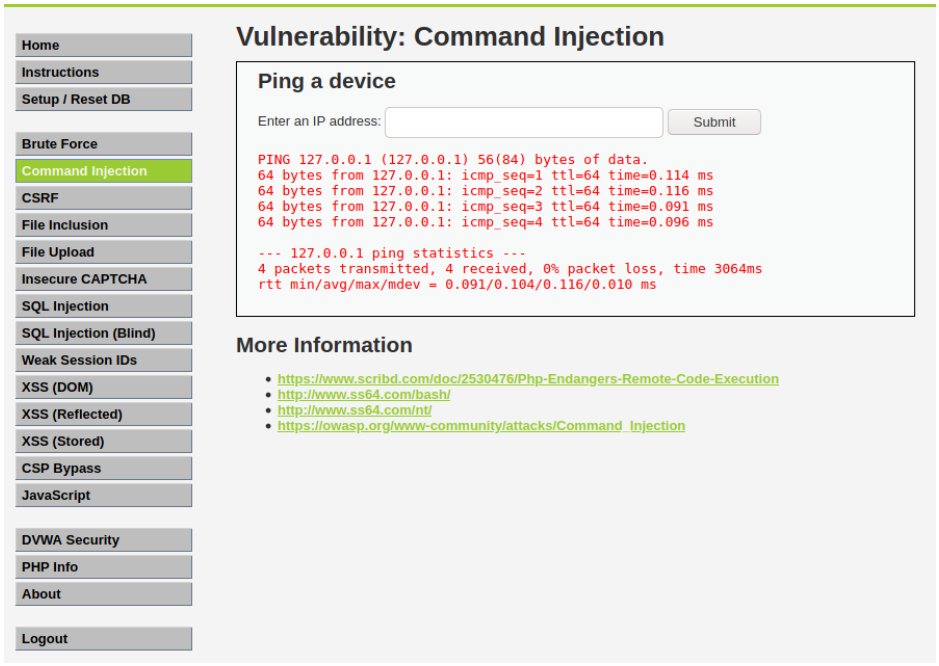
Medium Level: Medium security will have all entry-level validations and filtration which can stop any script kiddie to get the benefit of available vulnerabilities.

High Level: High Level is kind of Zero Day environment and if you can breach it then that means you are on the right track to becoming a VAPT Expert.


Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Username: admin
Security Level: impossible
Locale: en
PHPIDS: disabled
SQLi DB: mysql
DVWA Security
Security Level
Security level is currently: impossible.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Low
Submit
PHPIDS
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently: disabled. [Enable PHPIDS]
[Simulate attack] - [View IDS log]


Vulnerability: SQL Injection
User ID:
Submit
ID: 1' and 1=1#
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/


Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/



Conclusion:DVWA has been successfully configured and SQL and Command Injection can be implemented using the web tool.

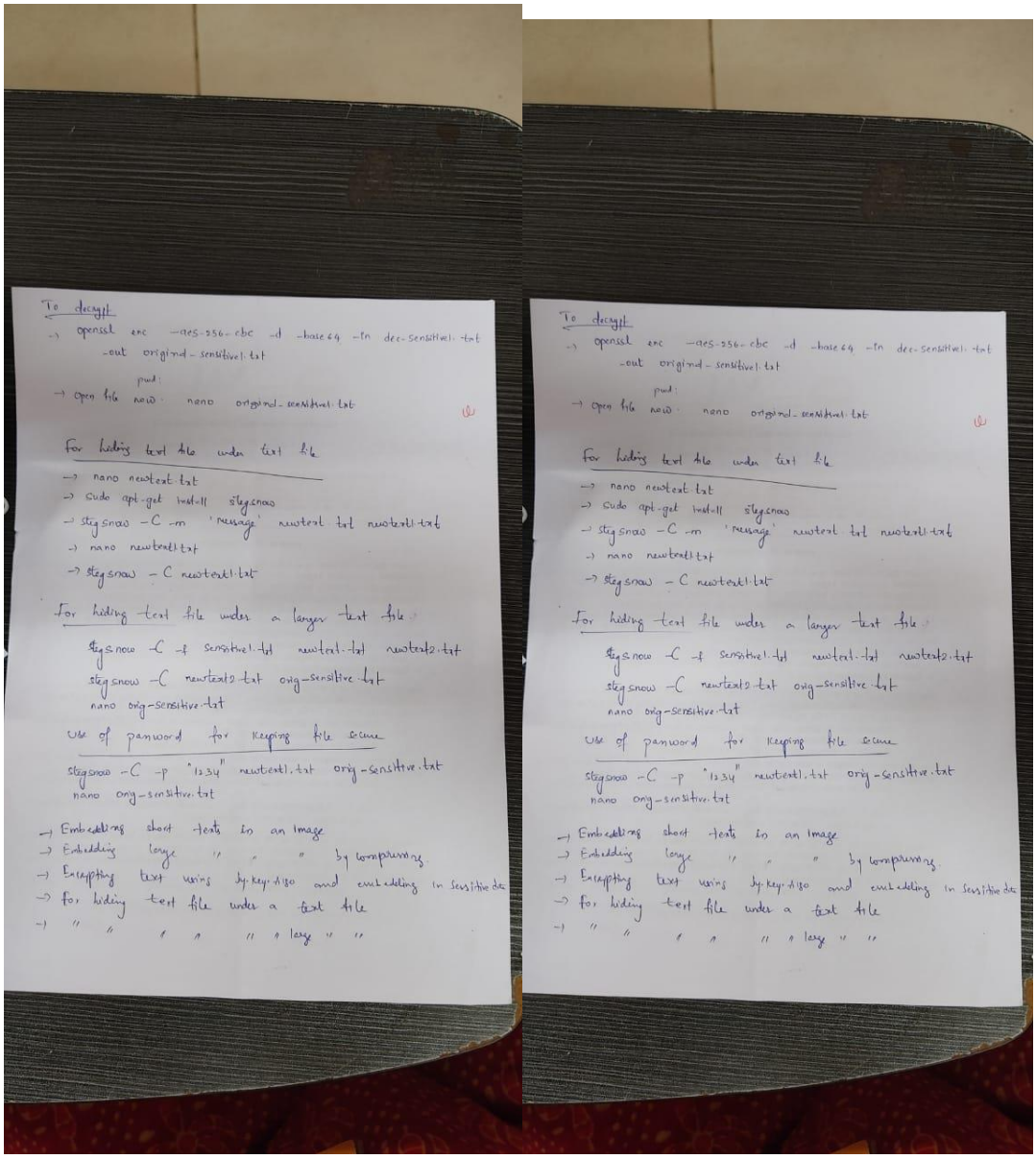
LAB 11

ARYAMAN MISHRA

19BCE1027

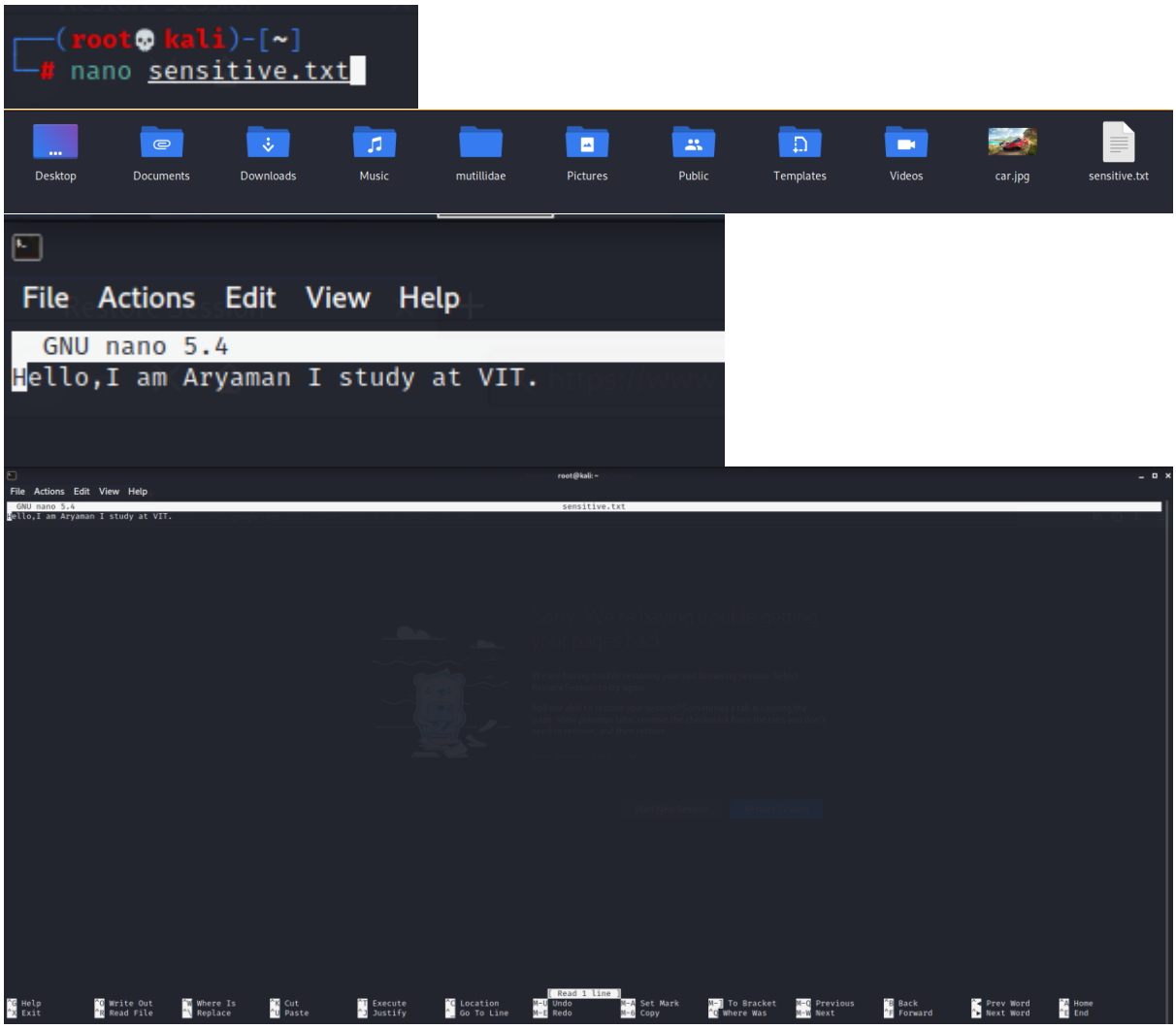
Information hiding using Steghide and Stegsnow

Commands to execute



Steghide is a steganography tool that allows you to cover confidential records inside a

picture or sound record with a passphrase. Bolsters BMP and JPEG picture group, AU and WAV sound group. This device has its advantages and disadvantages. One upside is that it is much better at covering and can extend a lot without any type of document. It does this by using a propelled calculation to shroud it inside a picture (or sound) record without changing the form (or sound) of the document. This is additionally without using Steghide (or if there is not the same scientific method as Steghide) then it is difficult to remove the hidden documents from the picture.



Install steghide

```
┌──(root💀kali)-[~]
└─# steghide --help
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

embedding options:
 -ef, --embedfile        select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed ... 9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

extracting options:
 -sf, --stegofile        select stego file
   -sf <filename>        extract data from <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to extract data
 -xf, --extractfile      select file name for extracted data
   -xf <filename>        write the extracted data to <filename>
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

options for the info command:
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg
```

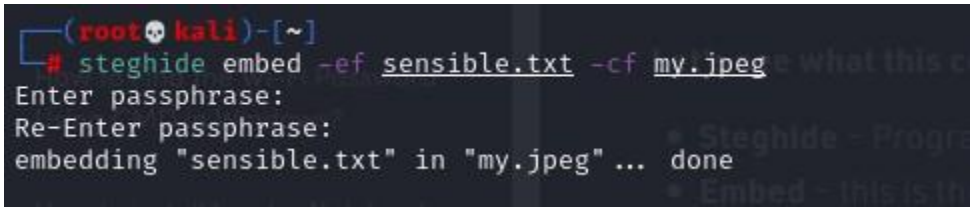
```
┌──(root💀kali)-[~]
└─# steghide embed -cf car.jpg -ef sensitive.txt
Enter passphrase:
Re-Enter passphrase:
embedding "sensitive.txt" in "car.jpg"... done
```

```
┌──(root💀kali)-[~]
└─# steghide embed -cf car.jpg -ef sensitive.txt -sf car.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "sensitive.txt" in "car.jpg"... done
the file "car.jpg" does already exist. overwrite ? (y/n) y
```

```
┌──(root💀kali)-[~]
└─# steghide extract -sf car.jpg -xf sensitive2.txt
Enter passphrase:
wrote extracted data to "sensitive2.txt".
```

Embedding data in the image:

We hide the data in the image using the Steghide so that only the person who accepts it can read it. Therefore, we created a text file named “sensible.txt”, in which we wrote our confidential data and images. JPEG is the file in which we are embedding our data.



Here, ef and cf are termed as embedded files and cover files, respectively.

Let’s see what this command is doing:

Steghide – Program Name
Embed – this is the command
-cf – This flag is for the cover file (the file used to embed the data)
filename – this is the name of the cover file
-ef – This flag is for the embed file (the file that will be embedded)
Filename – This is the name of the embedded file

Extraction of Data From Image Via Steghide:

Using Steghide adds an extra layer of security by allowing us to use a password for it. As long as you know the passphrase, it is quite easy to extract data from the image.

```
┌──(root💀kali)-[~]
└─# steghide extract -sf my.jpeg
Enter passphrase:
the file "sensible.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "sensible.txt".
```

Password Protect Files:

Now, we can also extract files using the following command. This command is different in that it specifies a password in the command itself, therefore, we do not need to specify it separately.

```
┌──(root💀kali)-[~]
└─# steghide embed -ef sensible.txt -cf my.jpeg -p 1289
embedding "sensible.txt" in "my.jpeg" ... done
```

```
┌──(root💀kali)-[~]
└─# sudo steghide extract -sf my.jpeg -p 1289
the file "sensible.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "sensible.txt".
```

Retrieve Information of Embedded File:

If we have an image in which the data is suspected to be hidden and if so, what algorithm is used to encrypt the data in the file?

```
┌──(root💀kali)-[~]
└─# steghide info my.jpeg
"my.jpeg":
  format: jpeg
  capacity: 19.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "sensible.txt":
    size: 21.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Verbose Mode

To obtain every information of a file during extraction, we can use verbose mode. The verbose mode gives you detailed information.

```
┌──(root💀kali)-[~]
└─# steghide embed  -v -ef sensible.txt -cf my.jpeg
Enter passphrase:
Re-Enter passphrase:
reading secret file "sensible.txt" ... done
reading cover file "my.jpeg" ... done
creating the graph ... 113 sample values, 344 vertices, 54287 edges
executing Static Minimum Degree Construction Heuristic ... 100.0% (1.0) done
```

Encrypting Algorithms:

We can encrypt the data we are hiding using encryption techniques.

```
┌──(root💀kali)-[~]
└─# steghide embed -ef sensible.txt -cf my.jpeg -e des
Enter passphrase:
Re-Enter passphrase:
embedding "sensible.txt" in "my.jpeg" ... done
```

Hiding text file under text file

Creating a new text file

```
┌──(root💀kali)-[~]
└─# nano newtext.txt
```

```
root@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.4                                    newtext.txt
hello frends how are you this is a text file
```

This command encodes the message inside newtext.txt and saves the resulting file that contains the message in newtext1.txt.

```
┌──(root💀kali)-[~]
└─# stegsnow -C -m 'secreat message' newtext.txt newtext1.txt
Compressed by 45.00%
Message exceeded available space by approximately 450.00%.
An extra 2 lines were added.
```

Checking newtext1 file

```
┌──(root💀kali)-[~]
└─# nano newtext1.txt
```

```
File  Actions  Edit  View  Help
  GNU nano 5.4                                                newtext1.txt
hello frends how are you this is a text file
```

Checking using stegsnow

```
┌──(root💀kali)-[~]
└─# stegsnow -C newtext1.txt
secreat message
```

Creating sensitive1 file

```
┌──(root💀kali)-[~]
└─# nano sensitive1.txt
```

```
                                                            root@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.4                                              sensitive1.txt *
this is a hidden message
```

Hiding text file under a layer text file

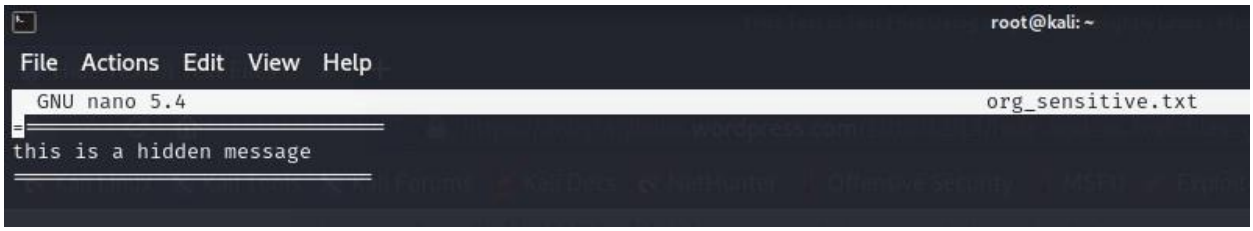
```
┌──(root💀kali)-[~]
└─# stegsnow -C -f sensitive1.txt newtext.txt newtext2.txt
Compressed by 2681212801411272192.00%
Message exceeded available space by approximately 6291.67%.
An extra 26 lines were added.
```

Encode newtext2 file inside org_sensitive file

```
┌──(root💀kali)-[~]
└─# stegsnow -C newtext2.txt org_sensitive.txt
```

Checking org_sensitive file

```
┌──(root💀kali)-[~]
└─# nano org_sensitive.txt
```

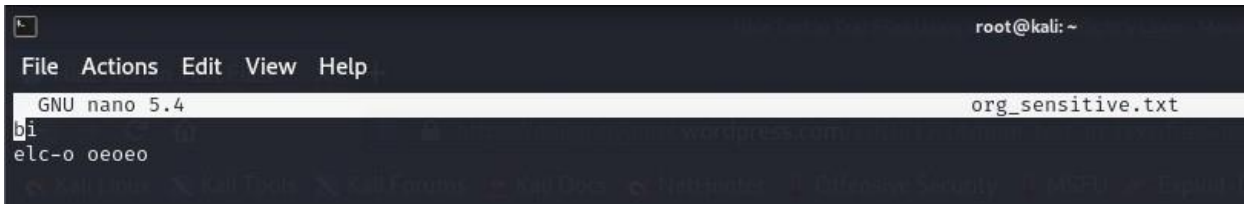


Encoding using password for keeping file secure

```
┌──(root💀kali)-[~]
└─# stegsnow -C -p "1234" newtext1.txt org_sensitive.txt
```

Checking org_sensitive file

```
┌──(root💀kali)-[~]
└─# nano org_sensitive.txt
```



LAB 12

ARYAMAN MISHRA

19BCE1027

LAB 12-Exploring Information Auditing Tool

Tool:Lynis

Lynis is an open source security tool. It helps with auditing systems running UNIX-alike systems (Linux, macOS, BSD), and providing guidance for system hardening and compliance testing. This document contains the basics to use the software.

By running 'lynis' the program is started and will provide the basic parameters available. If you manually extracted Lynis (or used Git), then use './lynis' to start the program from the local directory.

The most common command to start Lynis is using **audit system** command. This still start the security scan.

To run Lynis you should meet one requirement: have write access to **/tmp** (temporary files)

The Lynis tool requires a minimum amount of parameters to run. If you are using it for the first time, just run lynis and see what output it provides.

```
$ ./lynis
```

Without any commands, Lynis will display its status, together with suggestions on how to start.

Audit

The *audit* command tells Lynis to perform an audit.

Targets include:

- **system** - audit the host system
- **dockerfile** - audit a dockerfile

Show

The *show* command informs Lynis to share information, like help or the value of something.

Examples:

- **help** - show help and tips
- **profiles** - show discovered audit profiles
- **settings** - show active settings
- **version** - show Lynis version

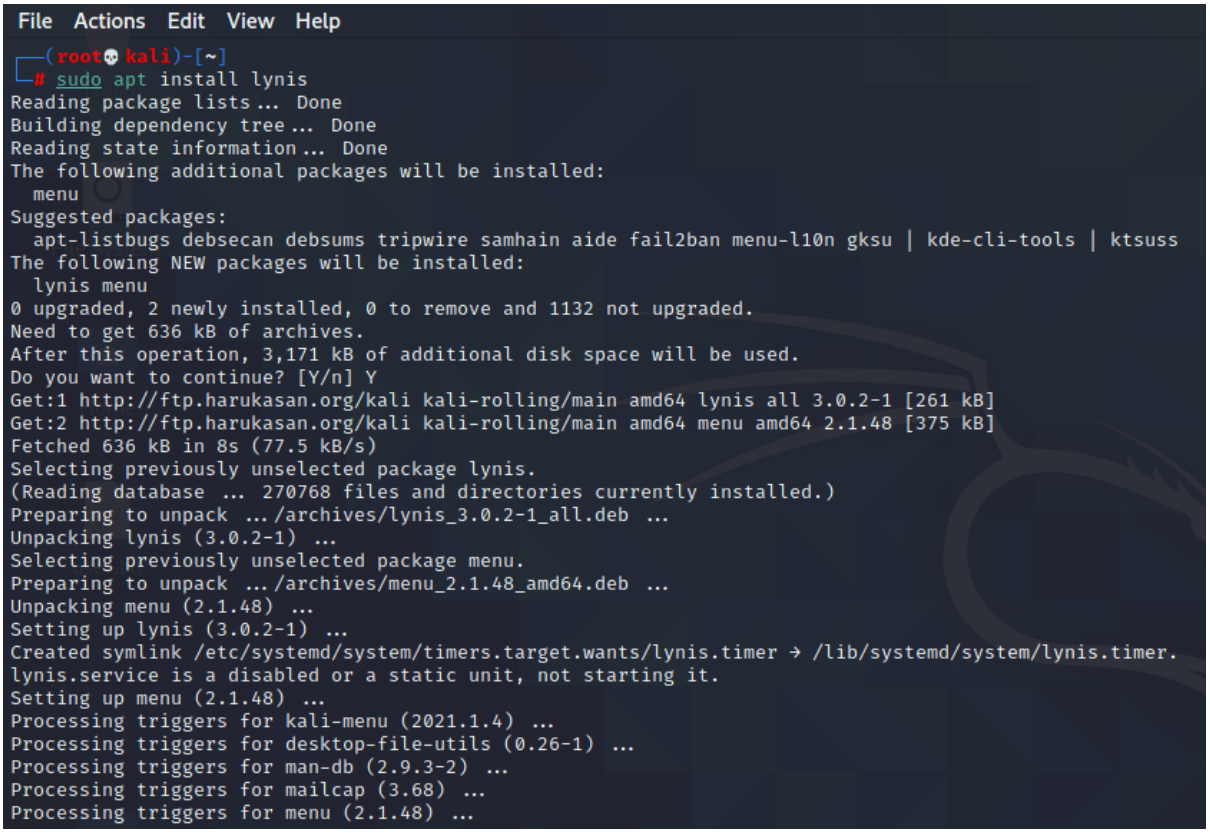
Parameters

In the table below, the most commonly used parameters are listed.

Parameter	Abbreviated	Description
--auditor "Name"		Assign an auditor name to the audit (report)
--checkall	-c	Start the check
--check-update		Check if Lynis is up-to-date
--cronjob		Run Lynis as cronjob (includes -c -Q)
--help	-h	Shows valid parameters
--manpage		View man page
--nocolors		Do not use any colors
--pentest		Perform a penetration test scan (non-privileged)
--quick	-Q	Don't wait for user input, except on errors
--quiet		Only show warnings (includes --quick, but doesn't wait)

Parameter	Abbreviated	Description
--reverse-colors		Use a different color scheme for light backgrounds
--version	-V	Check program version (and quit)

Installing Lynis on Kali Linux.



Execute Lynis -h for command details

```
┌──(root💀kali)-[~]
└─# lynis -h

[ Lynis 3.0.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                : Perform local security scan
        audit system remote <host>  : Remote security scan
        audit dockerfile <file>     : Analyze Dockerfile

    show
        show                        : Show all commands
        show version                : Show Lynis version
        show help                   : Show help

    update
        update info                 : Show update details


  Options:

    Alternative system audit modes
    --forensics                     : Perform forensics on a running or mounted system
    --pentest                       : Non-privileged, show points of interest for pentesting

    Layout options
    --no-colors                     : Don't use colors in output
    --quiet (-q)                    : No output
    --reverse-colors                : Optimize color display for light backgrounds
    --reverse-colours               : Optimize colour display for light backgrounds
```

```
    Misc options
    --debug                         : Debug logging to screen
    --no-log                        : Don't create a log file
    --profile <profile>             : Scan the system with the given profile file
    --view-manpage (--man)          : View man page
    --verbose                       : Show more details on screen
    --version (-V)                  : Display version number and quit
    --wait                          : Wait between a set of tests
    --slow-warning <seconds>  : Threshold for slow test warning in seconds (default 10)

    Enterprise options
    --plugindir <path>              : Define path of available plugins
    --upload                        : Upload data to central node

    More options available. Run '/usr/sbin/lynis show options', or use the man page.



┌──(root💀kali)-[~]
└─#
```

Lynis Audit System command execution:


(root kali)-[~]
lynis audit system
[Lynis 3.0.2]
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[+] Initializing program
- Detecting OS ... [DONE]
- Checking profiles ... [DONE]
Program version: 3.0.2
Operating system: Linux
Operating system name: Kali Linux
Operating system version: kali-rolling
Kernel version: 5.10.0
Hardware platform: x86_64
Hostname: kali
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
- Program update status ... [NO UPDATE]
[+] System tools
- Scanning available tools ...
- Checking system binaries ...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
- Plugin: debian
[


[+] Debian Tests
- Checking for system binaries that are required by Debian Tests ...
- Checking /bin ... [FOUND]
- Checking /sbin ... [FOUND]
- Checking /usr/bin ... [FOUND]
- Checking /usr/sbin ... [FOUND]
- Checking /usr/local/bin ... [FOUND]
- Checking /usr/local/sbin ... [FOUND]
- Authentication:
- PAM (Pluggable Authentication Modules):
- libpam-tmpdir [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
- Software:
- apt-listbugs [Not Installed]
- apt-listchanges [Not Installed]
- needrestart [Not Installed]
- debsecan [Not Installed]
- debsums [Not Installed]
- fail2ban [Not Installed]
]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 20 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 19 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- ModemManager.service: [MEDIUM]
- NetworkManager.service: [EXPOSED]
- colord.service: [EXPOSED]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- haveged.service: [OK]
- inetutils-inetd.service: [UNSAFE]
- libvirtd.service: [UNSAFE]
- lightdm.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]
- lynis.service: [UNSAFE]
- mlocate.service: [EXPOSED]


- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 20 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 19 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- ModemManager.service: [MEDIUM]
- NetworkManager.service: [EXPOSED]
- colord.service: [EXPOSED]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- haveged.service: [OK]
- inetutils-inetd.service: [UNSAFE]
- libvirtd.service: [UNSAFE]
- lightdm.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]
- lynis.service: [UNSAFE]
- mlocate.service: [EXPOSED]
- plymouth-start.service: [UNSAFE]
- polkit.service: [UNSAFE]
- rc-local.service: [UNSAFE]
- rescue.service: [UNSAFE]
- rpc-gssd.service: [UNSAFE]
- rpc-svcgssd.service: [UNSAFE]
- rsync.service: [EXPOSED]
- rsyslog.service: [UNSAFE]
- rtkit-daemon.service: [MEDIUM]
- smartmontools.service: [UNSAFE]
- stunnel4.service: [UNSAFE]
- systemd-ask-password-console.service: [UNSAFE]
- systemd-ask-password-plymouth.service: [UNSAFE]
- systemd-ask-password-wall.service: [UNSAFE]
- systemd-fsckd.service: [UNSAFE]
- systemd-initctl.service: [UNSAFE]
- systemd-journald.service: [OK]
- systemd-logind.service: [OK]
- systemd-machined.service: [MEDIUM]
- systemd-networkd.service: [OK]
- systemd-rfkill.service: [UNSAFE]
- systemd-udevd.service: [EXPOSED]
- udisks2.service: [UNSAFE]
- upower.service: [OK]
- user@0.service: [UNSAFE]
- virtlockd.service: [UNSAFE]
- virtlogd.service: [UNSAFE]


[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 77 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration
- configuration in systemd conf files [DEFAULT]
- configuration in etc/profile [DEFAULT]
- 'hard' configuration in security/limits.conf [DEFAULT]
- 'soft' configuration in security/limits.conf [DEFAULT]
- Checking setuid core dumps configuration [DISABLED]
- Check if reboot is needed [NO]
[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [NOT FOUND]
- Searching for IO waiting processes [NOT FOUND]
- Search prelink tooling [NOT FOUND]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Password hashing methods [OK]
- Checking password hashing rounds [DISABLED]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- Sudoers file(s) [FOUND]
- Permissions for directory: /etc/sudoers.d [WARNING]
- Permissions for: /etc/sudoers [OK]
- Permissions for: /etc/sudoers.d/kali-grant-root [OK]
- Permissions for: /etc/sudoers.d/README [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [SUGGESTION]
- Accounts without password [OK]


- Locked accounts [FOUND]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Mount options of /dev [HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED
- Mount options of /run [HARDENED]
- Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [NOT DISABLED]


[+] NFS
- Query rpc registered programs [DONE]
- Query NFS versions [DONE]
- Query NFS protocols [DONE]
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [UNKNOWN]
- Checking /etc/hosts
- Duplicate entries in hosts file [NONE]
- Presence of configured hostname in /etc/hosts [FOUND]
- Hostname mapped to localhost [NOT FOUND]
- Localhost mapping to IP address [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [FOUND]
- Checking security repository in sources.list file or directory [WARNING]
- Checking vulnerable packages (apt-get only) [DONE]
[WARNING]: Test PKGS-7392 had a long execution: 1702.208100 seconds
- Checking package audit tool [INSTALLED]
Found: apt-get
- Toolkit for automatic upgrades [NOT FOUND]
[+] Networking
- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 192.168.29.1 [OK]
Nameserver: 2405:201:6008:30e3::c0a8:1d01 [OK]
- Minimal of 2 responsive nameservers [OK]
- DNSSEC supported (systemd-resolved) [UNKNOWN]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [SKIPPED]
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client
- Checking for ARP monitoring software [NOT FOUND]
- Uncommon network protocols [0]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]


[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]
[+] Software: e-mail and messaging
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [FOUND (118)]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [FOUND]
- Checking PHP disabled functions [FOUND]
- Checking expose_php option [OFF]
- Checking enable_dl option [OFF]
- Checking allow_url_fopen option [ON]

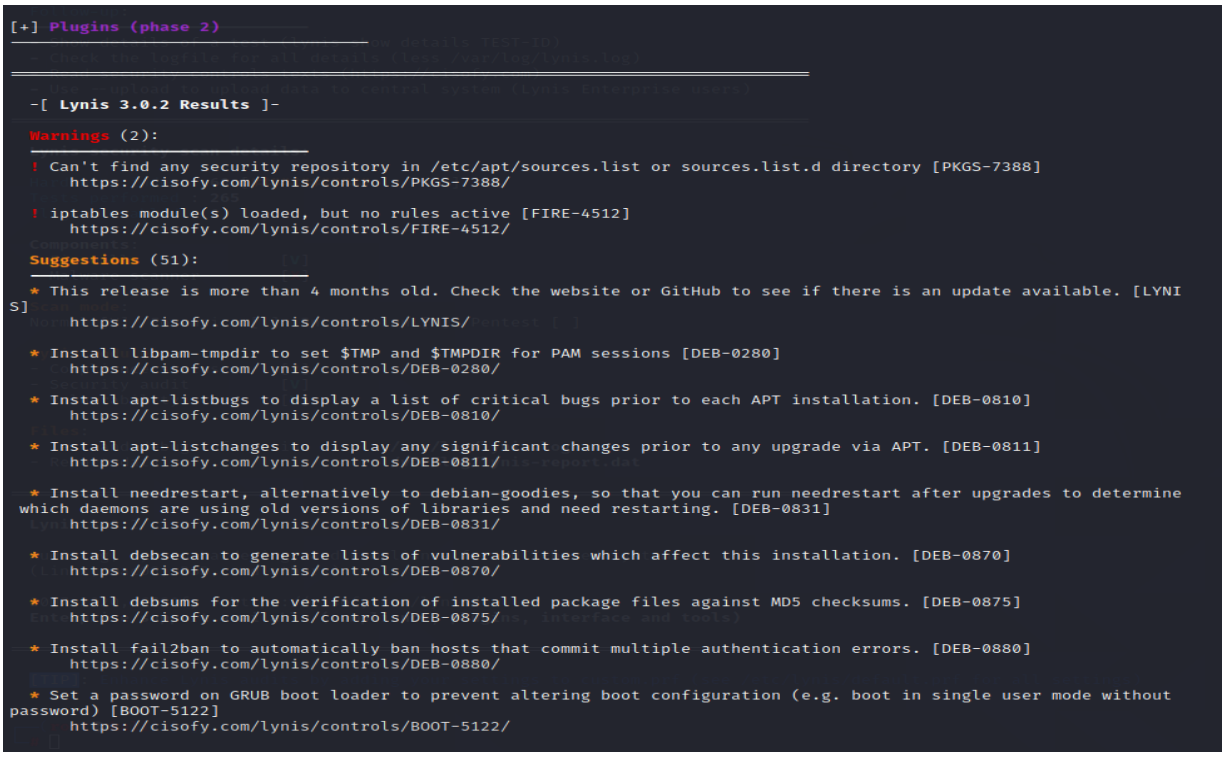

[+] PHP
- Checking PHP [FOUND]
- Checking PHP disabled functions [FOUND]
- Checking expose_php option [OFF]
- Checking enable_dl option [OFF]
- Checking allow_url_fopen option [ON]
- Checking allow_url_include option [OFF]
- Checking listen option [OK]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking remote logging [NOT ENABLED]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]
[+] Insecure services
- Installed inetd package [NOT FOUND]
- Checking enabled inetd services [OK]
- Installed xinetd package [OK]
- xinetd status
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [SUGGESTION]
- Checking TFTP server installation [SUGGESTION]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]

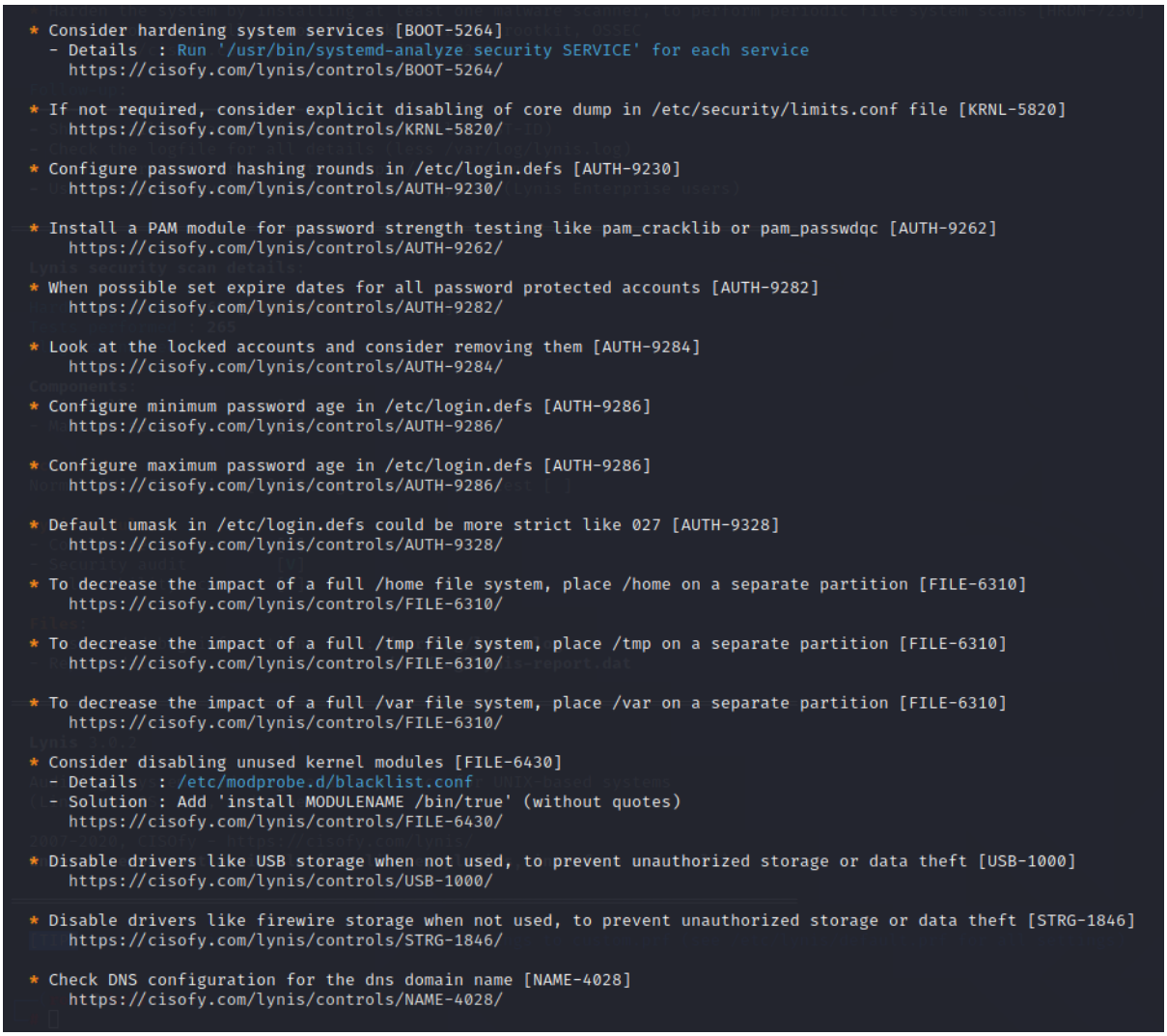

* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
Lynis security scan details:
Hardening index : 60 [############]
Tests performed : 265
Plugins enabled : 1
Components:
- Firewall [V]
- Malware scanner [X]
Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]
Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
Lynis 3.0.2
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)
2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
(root kali)-[~]
#

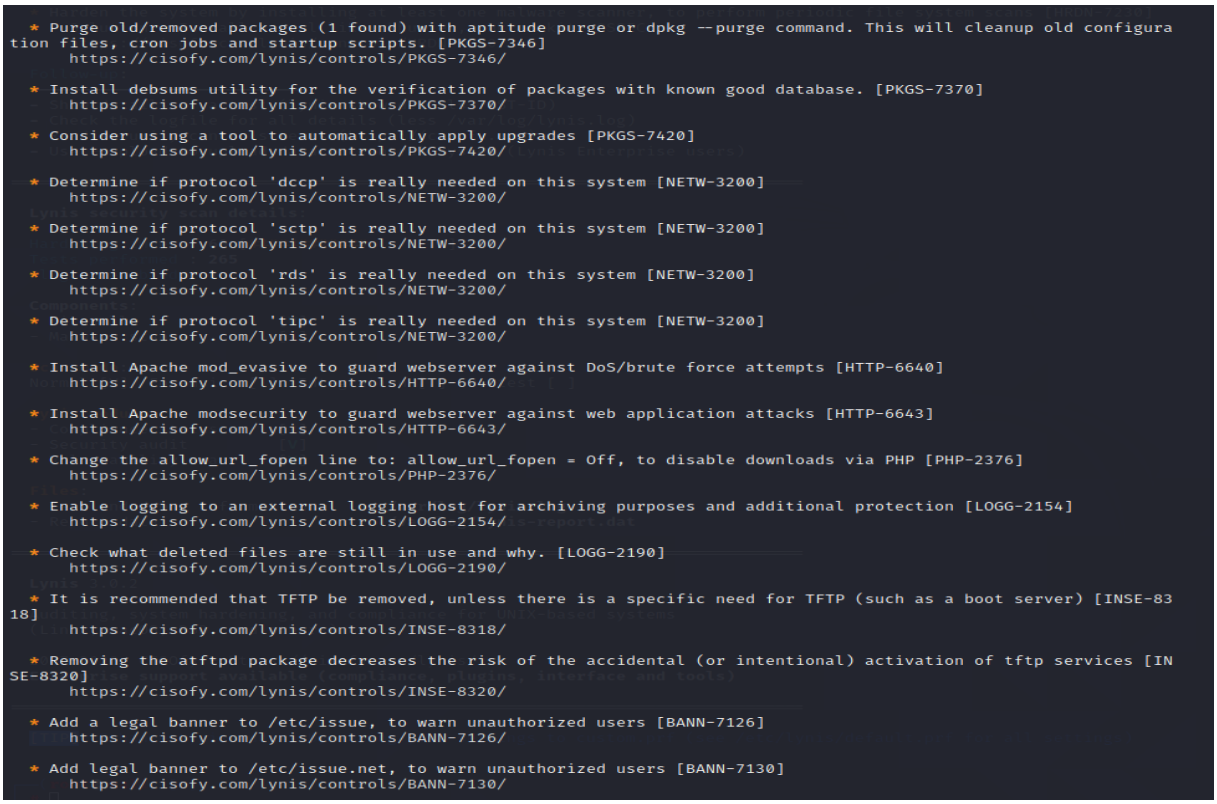
Executing lynis audit system --forensics

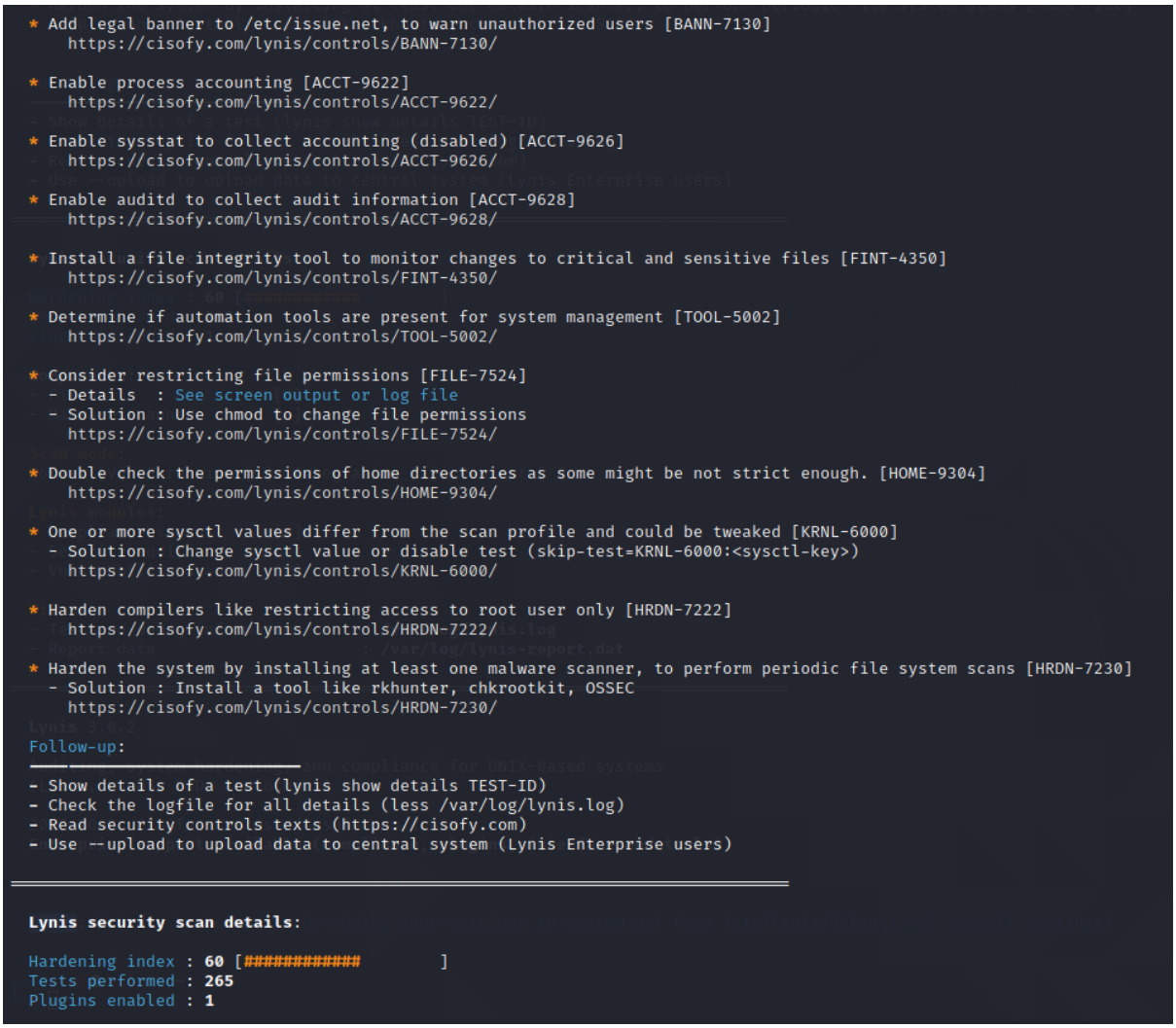

- Plugin: debian
[
[+] Debian Tests
- Checking for system binaries that are required by Debian Tests ...
- Checking /bin ... [FOUND]
- Checking /sbin ... [FOUND]
- Checking /usr/bin ... [FOUND]
- Checking /usr/sbin ... [FOUND]
- Checking /usr/local/bin ... [FOUND]
- Checking /usr/local/sbin ... [FOUND]
- Authentication:
- PAM (Pluggable Authentication Modules):
- libpam-tmpdir [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
- Software:
- apt-listbugs [Not Installed]
- apt-listchanges [Not Installed]
- needrestart [Not Installed]
- debsecan [Not Installed]
- debsums [Not Installed]
- fail2ban [Not Installed]
]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 20 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 19 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- ModemManager.service: [MEDIUM]
- NetworkManager.service: [EXPOSED]
- colord.service: [EXPOSED]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- haveged.service: [OK]
- inetutils-inetd.service: [UNSAFE]
- libvirtd.service: [UNSAFE]
- lightdm.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]

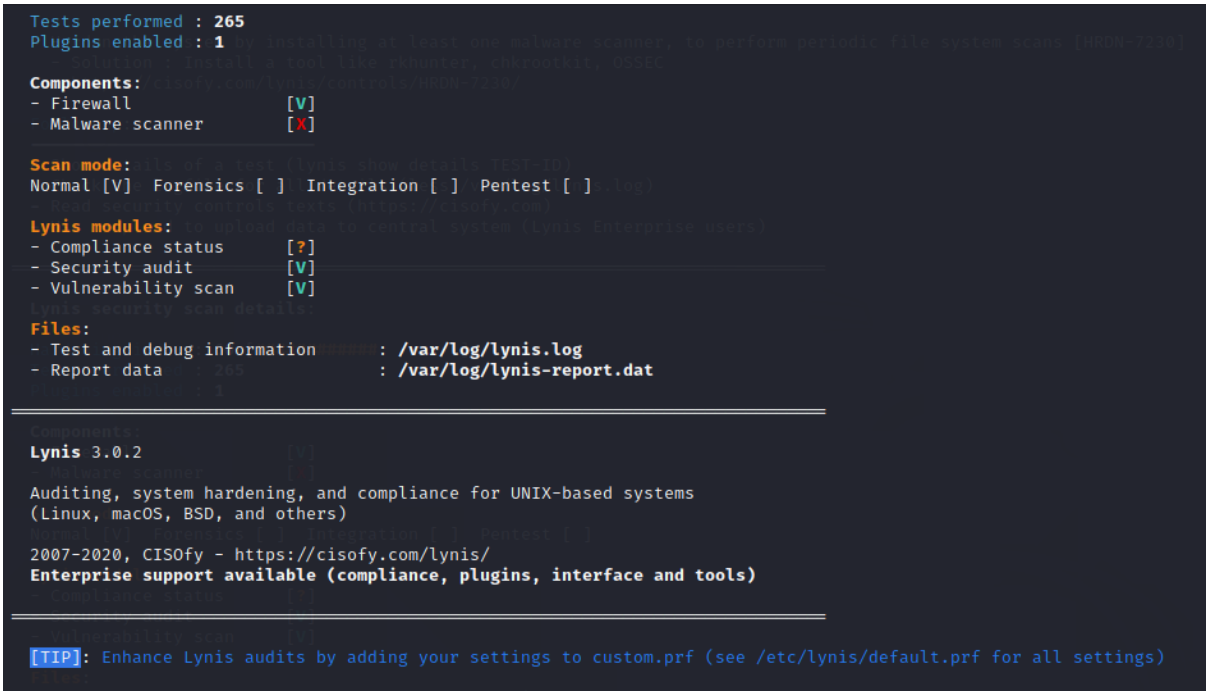

- lynis.service: [UNSAFE]
- mlocate.service: [EXPOSED]
- plymouth-start.service: [UNSAFE]
- polkit.service: [UNSAFE]
- rc-local.service: [UNSAFE]
- rescue.service: [UNSAFE]
- rpc-gssd.service: [UNSAFE]
- rpc-svcgssd.service: [UNSAFE]
- rsync.service: [EXPOSED]
- rsyslog.service: [UNSAFE]
- rtkit-daemon.service: [MEDIUM]
- smartmontools.service: [UNSAFE]
- stunnel4.service: [UNSAFE]
- systemd-ask-password-console.service: [UNSAFE]
- systemd-ask-password-plymouth.service: [UNSAFE]
- systemd-ask-password-wall.service: [UNSAFE]
- systemd-fsckd.service: [UNSAFE]
- systemd-initctl.service: [UNSAFE]
- systemd-journald.service: [OK]
- systemd-logind.service: [OK]
- systemd-machined.service: [MEDIUM]
- systemd-networkd.service: [OK]
- systemd-rfkill.service: [UNSAFE]
- systemd-udevd.service: [EXPOSED]
- udisks2.service: [UNSAFE]
- upower.service: [OK]
- user@0.service: [UNSAFE]
- virtlockd.service: [UNSAFE]
- virtlogd.service: [UNSAFE]
- virtualbox-guest-utils.service: [UNSAFE]
[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 82 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration
- configuration in systemd conf files [DEFAULT]
- configuration in etc/profile [DEFAULT]
- 'hard' configuration in security/limits.conf [DEFAULT]
- 'soft' configuration in security/limits.conf [DEFAULT]
- Checking setuid core dumps configuration [DISABLED]
- Check if reboot is needed [NO]


[+] Plugins (phase 2)
-[Lynis 3.0.2 Results]-
Warnings (2):
! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
https://cisofy.com/lynis/controls/PKGS-7388/
! iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/lynis/controls/FIRE-4512/
Suggestions (51):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
https://cisofy.com/lynis/controls/DEB-0811/
* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]
https://cisofy.com/lynis/controls/DEB-0831/
* Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
https://cisofy.com/lynis/controls/DEB-0870/
* Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
https://cisofy.com/lynis/controls/DEB-0875/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/lynis/controls/DEB-0880/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/lynis/controls/BOOT-5122/

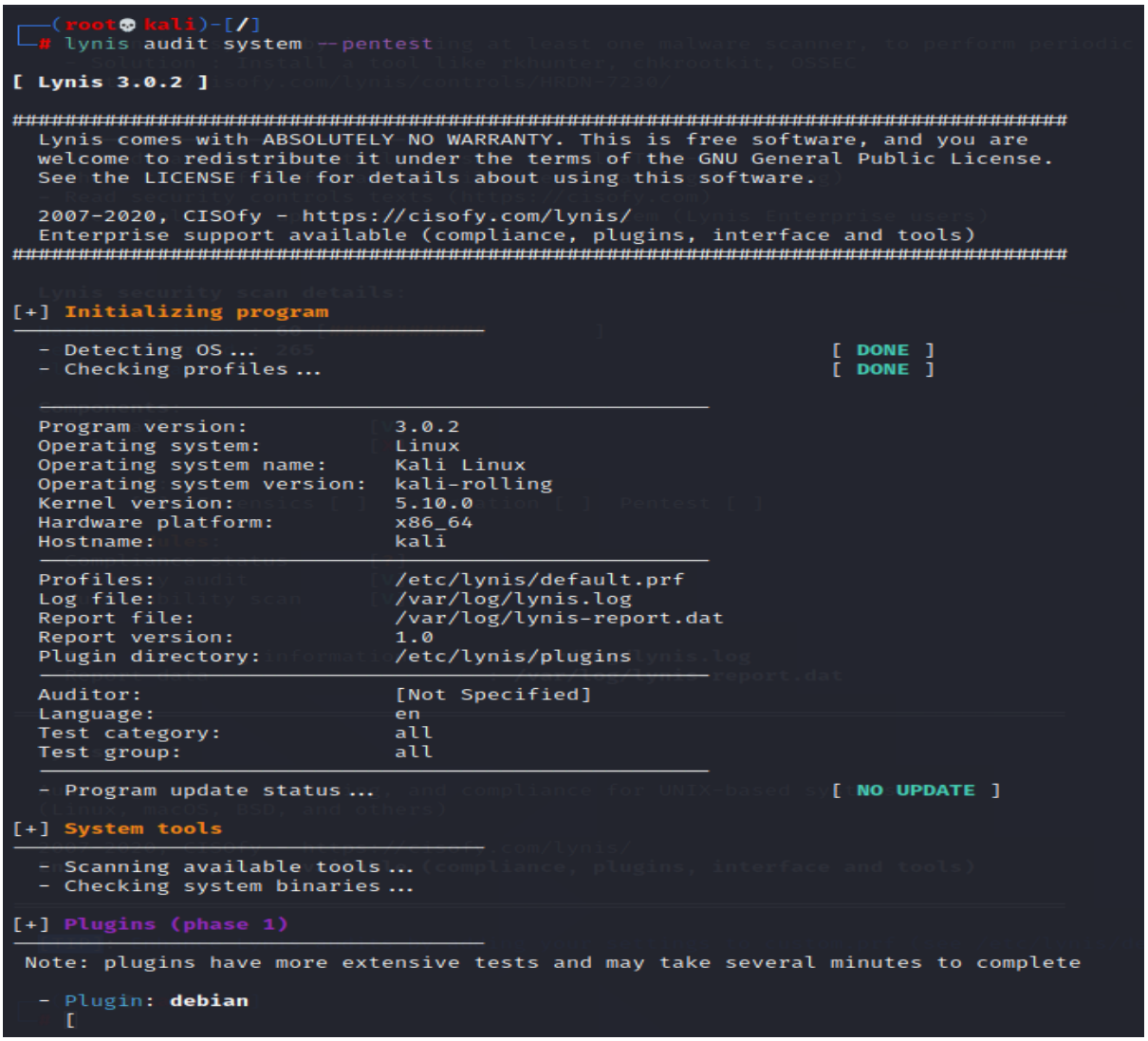

* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
https://cisofy.com/lynis/controls/BOOT-5264/
* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
https://cisofy.com/lynis/controls/KRNL-5820/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
https://cisofy.com/lynis/controls/AUTH-9262/
* When possible set expire dates for all password protected accounts [AUTH-9282]
https://cisofy.com/lynis/controls/AUTH-9282/
* Look at the locked accounts and consider removing them [AUTH-9284]
https://cisofy.com/lynis/controls/AUTH-9284/
* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
https://cisofy.com/lynis/controls/AUTH-9328/
* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/
* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/
* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
https://cisofy.com/lynis/controls/FILE-6310/
* Consider disabling unused kernel modules [FILE-6430]
- Details : /etc/modprobe.d/blacklist.conf
- Solution : Add 'install MODULENAME /bin/true' (without quotes)
https://cisofy.com/lynis/controls/FILE-6430/
* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
https://cisofy.com/lynis/controls/USB-1000/
* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
https://cisofy.com/lynis/controls/STRG-1846/
* Check DNS configuration for the dns domain name [NAME-4028]
https://cisofy.com/lynis/controls/NAME-4028/


* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configura
tion files, cron jobs and startup scripts. [PKGS-7346]
https://cisofy.com/lynis/controls/PKGS-7346/
* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
https://cisofy.com/lynis/controls/PKGS-7370/
* Consider using a tool to automatically apply upgrades [PKGS-7420]
https://cisofy.com/lynis/controls/PKGS-7420/
* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'rds' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/lynis/controls/HTTP-6640/
* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/lynis/controls/HTTP-6643/
* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
https://cisofy.com/lynis/controls/PHP-2376/
* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
https://cisofy.com/lynis/controls/LOGG-2154/
* Check what deleted files are still in use and why. [LOGG-2190]
https://cisofy.com/lynis/controls/LOGG-2190/
* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-83
18]
https://cisofy.com/lynis/controls/INSE-8318/
* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [IN
SE-8320]
https://cisofy.com/lynis/controls/INSE-8320/
* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
https://cisofy.com/lynis/controls/BANN-7126/
* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/lynis/controls/BANN-7130/


* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/lynis/controls/BANN-7130/
* Enable process accounting [ACCT-9622]
https://cisofy.com/lynis/controls/ACCT-9622/
* Enable sysstat to collect accounting (disabled) [ACCT-9626]
https://cisofy.com/lynis/controls/ACCT-9626/
* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/lynis/controls/ACCT-9628/
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/lynis/controls/FINT-4350/
* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/lynis/controls/TOOL-5002/
* Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
https://cisofy.com/lynis/controls/FILE-7524/
* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
https://cisofy.com/lynis/controls/HOME-9304/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/lynis/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
Lynis security scan details:
Hardening index : 60 [############]
Tests performed : 265
Plugins enabled : 1



Executing Lynis Audit system –pentest command:


┌──(root💀kali)-[/]
└─# lynis audit system --pentest
[Lynis 3.0.2]
##
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
##
[+] Initializing program
- Detecting OS ... [DONE]
- Checking profiles ... [DONE]
Program version: 3.0.2
Operating system: Linux
Operating system name: Kali Linux
Operating system version: kali-rolling
Kernel version: 5.10.0
Hardware platform: x86_64
Hostname: kali
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
- Program update status ... [NO UPDATE]
[+] System tools
- Scanning available tools ...
- Checking system binaries ...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
- Plugin: debian
[


[+] Debian Tests
- Checking for system binaries that are required by Debian Tests ...
- Checking /bin ... [FOUND]
- Checking /sbin ... [FOUND]
- Checking /usr/bin ... [FOUND]
- Checking /usr/sbin ... [FOUND]
- Checking /usr/local/bin ... [FOUND]
- Checking /usr/local/sbin ... [FOUND]
- Authentication:
- PAM (Pluggable Authentication Modules):
- libpam-tmpdir [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/sda1 [NOT ENCRYPTED]
- Software:
- apt-listbugs [Not Installed]
- apt-listchanges [Not Installed]
- needrestart [Not Installed]
- debsecan [Not Installed]
- debsums [Not Installed]
- fail2ban [Not Installed]
[+] Boot and services
- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
- Checking for password protection [NONE]
- Check running services (systemctl) [DONE]
Result: found 20 running services
- Check enabled services at boot (systemctl) [DONE]
Result: found 19 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- ModemManager.service: [MEDIUM]
- NetworkManager.service: [EXPOSED]
- colord.service: [EXPOSED]
- cron.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- haveged.service: [OK]
- inetutils-inetd.service: [UNSAFE]
- libvirtd.service: [UNSAFE]
- lightdm.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]
- lynis.service: [UNSAFE]
- mlocate.service: [EXPOSED]


- plymouth-start.service: [UNSAFE]
- polkit.service: [UNSAFE]
- rc-local.service: [UNSAFE]
- rescue.service: [UNSAFE]
- rpc-gssd.service: [UNSAFE]
- rpc-svcgssd.service: [UNSAFE]
- rsync.service: [EXPOSED]
- rsyslog.service: [UNSAFE]
- rtkit-daemon.service: [MEDIUM]
- smartmontools.service: [UNSAFE]
- stunnel4.service: [UNSAFE]
- systemd-ask-password-console.service: [UNSAFE]
- systemd-ask-password-plymouth.service: [UNSAFE]
- systemd-ask-password-wall.service: [UNSAFE]
- systemd-fsckd.service: [UNSAFE]
- systemd-initctl.service: [UNSAFE]
- systemd-journald.service: [OK]
- systemd-logind.service: [OK]
- systemd-machined.service: [MEDIUM]
- systemd-networkd.service: [OK]
- systemd-rfkill.service: [UNSAFE]
- systemd-udevd.service: [EXPOSED]
- udisks2.service: [UNSAFE]
- upower.service: [OK]
- user@0.service: [UNSAFE]
- virtlockd.service: [UNSAFE]
- virtlogd.service: [UNSAFE]
- virtualbox-guest-utils.service: [UNSAFE]
[+] Kernel
- Checking default run level [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [FOUND]
- Checking kernel version and release [DONE]
- Checking kernel type [DONE]
- Checking loaded kernel modules [DONE]
Found 82 active modules
- Checking Linux kernel configuration file [FOUND]
- Checking default I/O kernel scheduler [NOT FOUND]
- Checking for available kernel update [OK]
- Checking core dumps configuration
- configuration in systemd conf files [DEFAULT]
- configuration in etc/profile [DEFAULT]
- 'hard' configuration in security/limits.conf [DEFAULT]
- 'soft' configuration in security/limits.conf [DEFAULT]
- Checking setuid core dumps configuration [DISABLED]
- Check if reboot is needed [NO]
[+] Memory and Processes


[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [NOT FOUND]
- Searching for IO waiting processes [NOT FOUND]
- Search prelink tooling [NOT FOUND]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Password hashing methods [OK]
- Checking password hashing rounds [DISABLED]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- Sudoers file(s) [FOUND]
- Permissions for directory: /etc/sudoers.d [WARNING]
- Permissions for: /etc/sudoers [OK]
- Permissions for: /etc/sudoers.d/kali-grant-root [OK]
- Permissions for: /etc/sudoers.d/README [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [SUGGESTION]
- Accounts without password [OK]
- Locked accounts [FOUND]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]
[+] File systems


[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Mount options of /dev [HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED]
- Mount options of /run [HARDENED]
- Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [NOT DISABLED]
[+] NFS
- Query rpc registered programs [DONE]
- Query NFS versions [DONE]
- Query NFS protocols [DONE]
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [UNKNOWN]
- Checking /etc/hosts
- Duplicate entries in hosts file [NONE]
- Presence of configured hostname in /etc/hosts [FOUND]
- Hostname mapped to localhost [NOT FOUND]
- Localhost mapping to IP address [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]

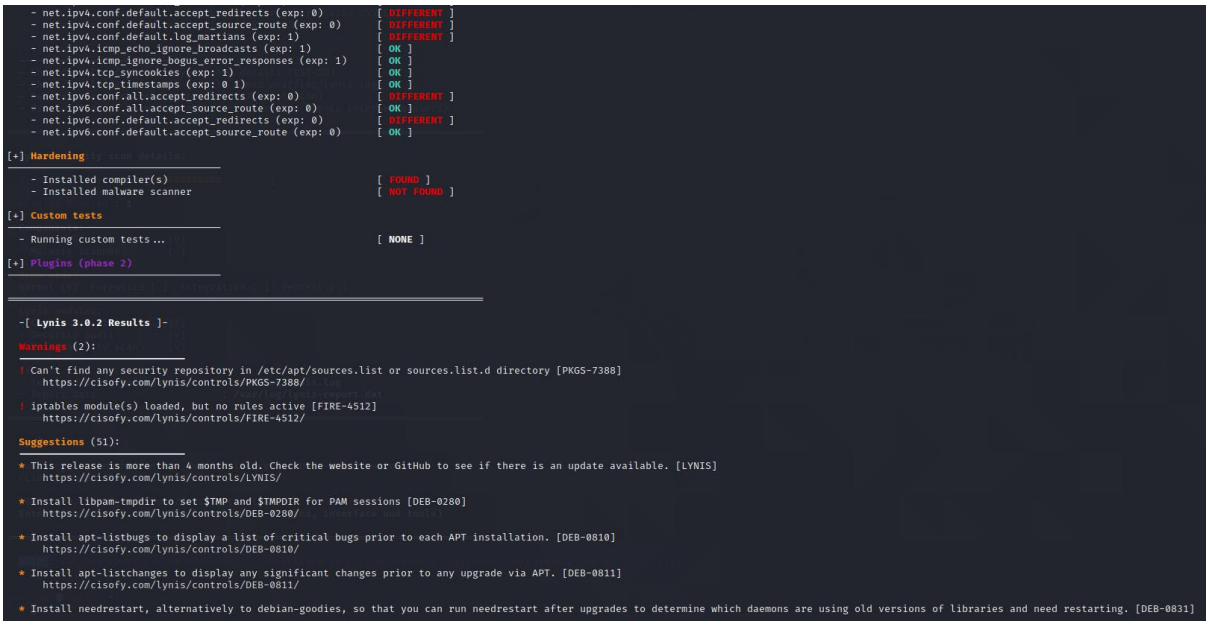

[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [FOUND]
- Checking security repository in sources.list file or directory [WARNING]
- Checking vulnerable packages (apt-get only) [DONE]
[WARNING]: Test PKGS-7392 had a long execution: 11.672215 seconds
- Checking package audit tool [INSTALLED]
Found: apt-get
- Toolkit for automatic upgrades [NOT FOUND]
[+] Networking
- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 192.168.29.1 [OK]
Nameserver: 2405:201:6008:30e3::c0a8:1d01 [OK]
- Minimal of 2 responsive nameservers [OK]
- DNSSEC supported (systemd-resolved) [UNKNOWN]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [SKIPPED]
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client
- Checking for ARP monitoring software [NOT FOUND]
- Uncommon network protocols [0]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]
[+] Software: e-mail and messaging
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]


[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)
Info: No virtual hosts found
* Loadable modules [FOUND (118)]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [FOUND]
- Checking PHP disabled functions [FOUND]
- Checking expose_php option [OFF]
- Checking enable_dl option [OFF]
- Checking allow_url_fopen option [ON]
- Checking allow_url_include option [OFF]
- Checking listen option [OK]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]


[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking remote logging [NOT ENABLED]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]
[+] Insecure services
- Installed inetd package [NOT FOUND]
- Checking enabled inetd services [OK]
- Installed xinetd package [OK]
- xinetd status
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [SUGGESTION]
- Checking TFTP server installation [SUGGESTION]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab and cronjob files [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]


[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/132] [NONE]
[WARNING]: Test CRYP-7902 had a long execution: 19.277655 seconds
- Found 0 encrypted and 1 unencrypted swap devices in use. [OK]
- Kernel entropy is sufficient [YES]
- HW RNG & rngd [NO]
- SW prng [YES]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [DISABLED]
- Checking presence SELinux [NOT FOUND]
- Checking presence TOMOYO Linux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [NONE]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [DISABLED]
- dm-verity (status) [DISABLED]
- Checking presence integrity tool [NOT FOUND]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NOT FOUND]
- Checking for IDS/IPS tooling [NONE]
[+] Software: Malware
[+] File Permissions
- Starting file permissions check
File: /boot/grub/grub.cfg [OK]
File: /etc/crontab [SUGGESTION]
File: /etc/group [OK]

```
    File: /etc/crontab                                          [ SUGGESTION ]
    File: /etc/group                                            [ OK ]
    File: /etc/group-                                           [ OK ]
    File: /etc/hosts.allow                                      [ OK ]
    File: /etc/hosts.deny                                       [ OK ]
    File: /etc/issue                                            [ OK ]
    File: /etc/issue.net                                        [ OK ]
    File: /etc/motd                                             [ OK ]
    File: /etc/passwd                                           [ OK ]
    File: /etc/passwd-                                          [ OK ]
    File: /etc/ssh/sshd_config                                  [ SUGGESTION ]
    Directory: /root/.ssh                                       [ OK ]
    Directory: /etc/cron.d                                      [ SUGGESTION ]
    Directory: /etc/cron.daily                                  [ SUGGESTION ]
    Directory: /etc/cron.hourly                                 [ SUGGESTION ]
    Directory: /etc/cron.weekly                                 [ SUGGESTION ]
    Directory: /etc/cron.monthly                                [ SUGGESTION ]

[+] Home directories
------------------------------------

  - Permissions of home directories                             [ WARNING ]
  - Ownership of home directories                               [ OK ]
  - Checking shell history files                                [ OK ]

[+] Kernel Hardening
------------------------------------

  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                           [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                               [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                           [ OK ]
    - fs.protected_regular (exp: 2)                             [ OK ]
    - fs.protected_symlinks (exp: 1)                            [ OK ]
    - fs.suid_dumpable (exp: 0)                                 [ OK ]
    - kernel.core_uses_pid (exp: 1)                             [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                              [ OK ]
    - kernel.dmesg_restrict (exp: 1)                            [ OK ]
    - kernel.kptr_restrict (exp: 2)                             [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                          [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                       [ OK ]
    - kernel.randomize_va_space (exp: 2)                        [ OK ]
    - kernel.sysrq (exp: 0)                                     [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)                 [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                     [ DIFFERENT ]
    - net.core.bpf_jit_harden (exp: 2)                          [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)            [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                     [ OK ]
    - net.ipv4.conf.all.log_martians (exp: 1)                   [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                      [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                      [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)                 [ DIFFERENT ]
```


- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Hardening
- Installed compiler(s) [FOUND]
- Installed malware scanner [NOT FOUND]
[+] Custom tests
- Running custom tests... [NONE]
[+] Plugins (phase 2)
-[Lynis 3.0.2 Results]-
Warnings (2):
! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
https://cisofy.com/lynis/controls/PKGS-7388/
! iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/lynis/controls/FIRE-4512/
Suggestions (51):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
https://cisofy.com/lynis/controls/DEB-0811/
* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]

```
    https://cisofy.com/lynis/controls/DEB-0831/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
    https://cisofy.com/lynis/controls/DEB-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
    https://cisofy.com/lynis/controls/DEB-0875/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
    https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    https://cisofy.com/lynis/controls/BOOT-5122/

* Consider hardening system services [BOOT-5264]
  - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
    https://cisofy.com/lynis/controls/KRNL-5820/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
    https://cisofy.com/lynis/controls/AUTH-9230/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
    https://cisofy.com/lynis/controls/AUTH-9262/
* When possible set expire dates for all password protected accounts [AUTH-9282]
    https://cisofy.com/lynis/controls/AUTH-9282/

* Look at the locked accounts and consider removing them [AUTH-9284]
    https://cisofy.com/lynis/controls/AUTH-9284/
* Configure minimum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/lynis/controls/AUTH-9328/
* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/
```

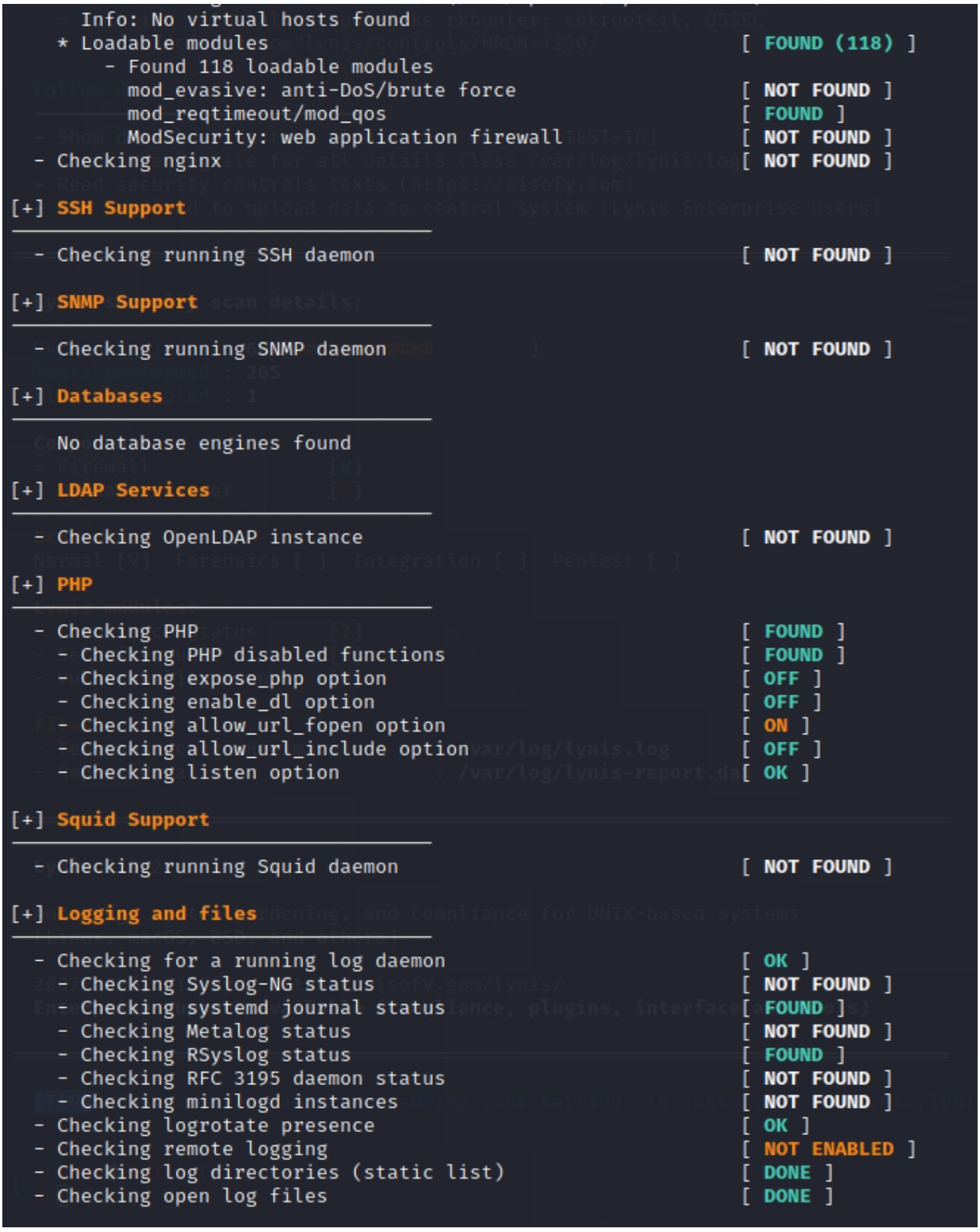

* Consider disabling unused kernel modules [FILE-6430]
- Details : /etc/modprobe.d/blacklist.conf
- Solution : Add 'install MODULENAME /bin/true' (without quotes)
https://cisofy.com/lynis/controls/FILE-6430/
* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
https://cisofy.com/lynis/controls/USB-1000/
* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
https://cisofy.com/lynis/controls/STRG-1846/
* Check DNS configuration for the dns domain name [NAME-4028]
https://cisofy.com/lynis/controls/NAME-4028/
* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
https://cisofy.com/lynis/controls/PKGS-7346/
* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
https://cisofy.com/lynis/controls/PKGS-7370/
* Consider using a tool to automatically apply upgrades [PKGS-7420]
https://cisofy.com/lynis/controls/PKGS-7420/
* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'rds' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/lynis/controls/HTTP-6640/
* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/lynis/controls/HTTP-6643/
* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
https://cisofy.com/lynis/controls/PHP-2376/
* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
https://cisofy.com/lynis/controls/LOGG-2154/
* Check what deleted files are still in use and why. [LOGG-2190]
https://cisofy.com/lynis/controls/LOGG-2190/
* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]
* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]
https://cisofy.com/lynis/controls/INSE-8318/
* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]
https://cisofy.com/lynis/controls/INSE-8320/
* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
https://cisofy.com/lynis/controls/BANN-7126/
* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/lynis/controls/BANN-7130/
* Enable process accounting [ACCT-9622]
https://cisofy.com/lynis/controls/ACCT-9622/
* Enable sysstat to collect accounting (disabled) [ACCT-9626]
https://cisofy.com/lynis/controls/ACCT-9626/
* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/lynis/controls/ACCT-9628/
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/lynis/controls/FINT-4350/
* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/lynis/controls/TOOL-5002/
* Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
https://cisofy.com/lynis/controls/FILE-7524/
* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
https://cisofy.com/lynis/controls/HOME-9304/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/lynis/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)


* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
Lynis security scan details:
Hardening index : 60 [############]
Tests performed : 265
Plugins enabled : 1
Components:
- Firewall [V]
- Malware scanner [X]
Scan mode:
Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running privileged)
Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
Lynis 3.0.2
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)
2007-2020, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)


[+] Memory and Processes
- Checking /proc/meminfo [FOUND]
- Searching for dead/zombie processes [NOT FOUND]
- Searching for IO waiting processes [NOT FOUND]
- Search prelink tooling [NOT FOUND]
[+] Users, Groups and Authentication
- Administrator accounts [OK]
- Unique UIDs [OK]
- Consistency of group files (grpck) [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [OK]
- Password hashing methods [OK]
- Checking password hashing rounds [DISABLED]
- Query system users (non daemons) [DONE]
- NIS+ authentication support [NOT ENABLED]
- NIS authentication support [NOT ENABLED]
- Sudoers file(s) [FOUND]
- Permissions for directory: /etc/sudoers.d [WARNING]
- Permissions for: /etc/sudoers [OK]
- Permissions for: /etc/sudoers.d/kali-grant-root [OK]
- Permissions for: /etc/sudoers.d/README [OK]
- PAM password strength tools [SUGGESTION]
- PAM configuration files (pam.conf) [FOUND]
- PAM configuration files (pam.d) [FOUND]
- PAM modules [FOUND]
- LDAP module in PAM [NOT FOUND]
- Accounts without expire date [SUGGESTION]
- Accounts without password [OK]
- Locked accounts [FOUND]
- Checking user password aging (minimum) [DISABLED]
- User password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NOT FOUND]
- umask (/etc/login.defs) [SUGGESTION]
- LDAP authentication support [NOT ENABLED]
- Logging failed login attempts [ENABLED]
[+] Shells
- Checking shells from /etc/shells
Result: found 11 shells (valid shells: 11).
- Session timeout settings/tools [NONE]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NONE]
- Checking default umask in /etc/profile [NONE]

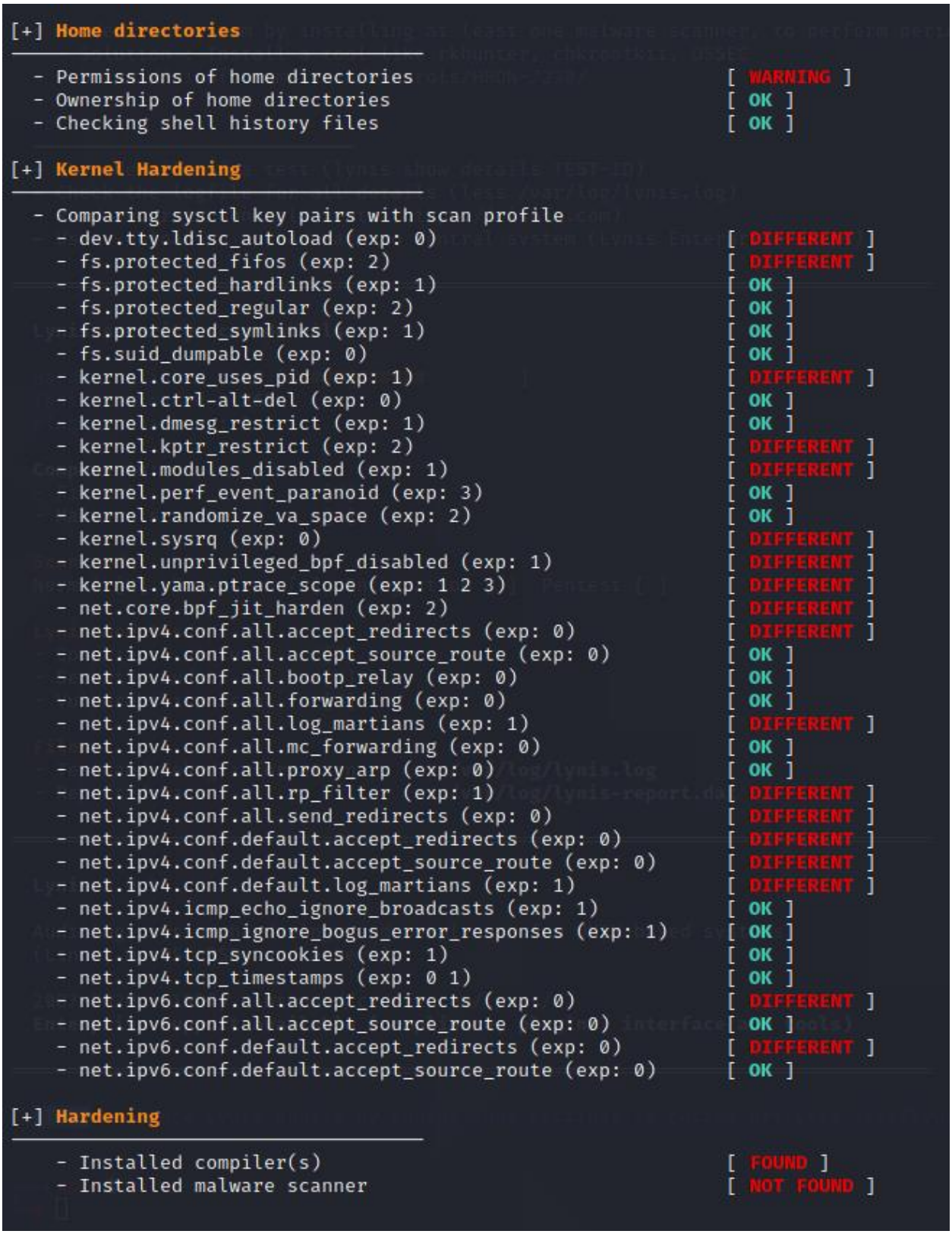

[+] File systems
- Checking mount points
- Checking /home mount point [SUGGESTION]
- Checking /tmp mount point [SUGGESTION]
- Checking /var mount point [SUGGESTION]
- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGGESTION]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- ACL support root file system [ENABLED]
- Mount options of / [NON DEFAULT]
- Mount options of /dev [HARDENED]
- Mount options of /dev/shm [PARTIALLY HARDENED]
- Mount options of /run [HARDENED]
- Total without nodev:6 noexec:7 nosuid:4 ro or noexec (W^X): 7 of total 23
- Checking Locate database [FOUND]
- Disable kernel support of some filesystems
- Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf
[+] USB Devices
- Checking usb-storage driver (modprobe config) [NOT DISABLED]
- Checking USB devices authorization [ENABLED]
- Checking USBGuard [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config) [NOT DISABLED]
[+] NFS
- Query rpc registered programs [DONE]
- Query NFS versions [DONE]
- Query NFS protocols [DONE]
- Check running NFS daemon [NOT FOUND]
[+] Name services
- Searching DNS domain name [UNKNOWN]
- Checking /etc/hosts
- Duplicate entries in hosts file [NONE]
- Presence of configured hostname in /etc/hosts [FOUND]
- Hostname mapped to localhost [NOT FOUND]
- Localhost mapping to IP address [OK]
[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager


[+] Ports and packages
- Searching package managers
- Searching dpkg package manager [FOUND]
- Querying package manager
- Query unpurged packages [FOUND]
- Checking security repository in sources.list file or directory [WARNING]
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 38820 (apt-get)
E: Unable to lock directory /var/lib/apt/lists/
- Checking vulnerable packages (apt-get only) [DONE]
- Checking package audit tool [INSTALLED]
Found: apt-get
- Toolkit for automatic upgrades [NOT FOUND]
[+] Networking
- Checking IPv6 configuration [ENABLED]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 192.168.29.1 [OK]
Nameserver: 2405:201:6008:30e3::c0a8:1d01 [OK]
- Minimal of 2 responsive nameservers [OK]
- DNSSEC supported (systemd-resolved) [UNKNOWN]
- Checking default gateway [DONE]
- Getting listening ports (TCP/UDP) [SKIPPED]
- Checking promiscuous interfaces [OK]
- Checking waiting connections [OK]
- Checking status DHCP client
- Checking for ARP monitoring software [NOT FOUND]
- Uncommon network protocols [0]
[+] Printers and Spools
- Checking cups daemon [NOT FOUND]
- Checking lp daemon [NOT RUNNING]
[+] Software: e-mail and messaging
[+] Software: firewalls
- Checking iptables kernel module [FOUND]
- Checking iptables policies of chains [FOUND]
- Checking for empty ruleset [WARNING]
- Checking for unused rules [OK]
- Checking host based firewall [ACTIVE]
[+] Software: webserver
- Checking Apache (binary /usr/sbin/apache2) [FOUND]
Info: Configuration file found (/etc/apache2/apache2.conf)


Info: No virtual hosts found
* Loadable modules [FOUND (118)]
- Found 118 loadable modules
mod_evasive: anti-DoS/brute force [NOT FOUND]
mod_reqtimeout/mod_qos [FOUND]
ModSecurity: web application firewall [NOT FOUND]
- Checking nginx [NOT FOUND]
[+] SSH Support
- Checking running SSH daemon [NOT FOUND]
[+] SNMP Support
- Checking running SNMP daemon [NOT FOUND]
[+] Databases
No database engines found
[+] LDAP Services
- Checking OpenLDAP instance [NOT FOUND]
[+] PHP
- Checking PHP [FOUND]
- Checking PHP disabled functions [FOUND]
- Checking expose_php option [OFF]
- Checking enable_dl option [OFF]
- Checking allow_url_fopen option [ON]
- Checking allow_url_include option [OFF]
- Checking listen option [OK]
[+] Squid Support
- Checking running Squid daemon [NOT FOUND]
[+] Logging and files
- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NOT FOUND]
- Checking systemd journal status [FOUND]
- Checking Metalog status [NOT FOUND]
- Checking RSyslog status [FOUND]
- Checking RFC 3195 daemon status [NOT FOUND]
- Checking minilogd instances [NOT FOUND]
- Checking logrotate presence [OK]
- Checking remote logging [NOT ENABLED]
- Checking log directories (static list) [DONE]
- Checking open log files [DONE]


- Checking log directories (static list) [DONE]
- Checking open log files [DONE]
- Checking deleted files in use [FILES FOUND]
[+] Insecure services
- Installed inetd package [NOT FOUND]
- Checking enabled inetd services [OK]
- Installed xinetd package [OK]
- xinetd status
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NOT FOUND]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [SUGGESTION]
- Checking TFTP server installation [SUGGESTION]
[+] Banners and identification
- /etc/issue [FOUND]
- /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
- /etc/issue.net contents [WEAK]
[+] Scheduled tasks
- Checking crontab and cronjob files [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/132] [NONE]
[WARNING]: Test CRYP-7902 had a long execution: 19.769443 seconds
- Found 0 encrypted and 1 unencrypted swap devices in use. [OK]
- Kernel entropy is sufficient [YES]
- HW RNG & rngd [NO]
- SW prng [YES]
[+] Virtualization


[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [DISABLED]
- Checking presence SELinux [NOT FOUND]
- Checking presence TOMOYO Linux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [NONE]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [DISABLED]
- dm-verity (status) [DISABLED]
- Checking presence integrity tool [NOT FOUND]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NOT FOUND]
- Checking for IDS/IPS tooling [NONE]
[+] Software: Malware
[+] File Permissions
- Starting file permissions check
File: /boot/grub/grub.cfg [OK]
File: /etc/crontab [SUGGESTION]
File: /etc/group [OK]
File: /etc/group- [OK]
File: /etc/hosts.allow [OK]
File: /etc/hosts.deny [OK]
File: /etc/issue [OK]
File: /etc/issue.net [OK]
File: /etc/motd [OK]
File: /etc/passwd [OK]
File: /etc/passwd- [OK]
File: /etc/ssh/sshd_config [SUGGESTION]
Directory: /root/.ssh [OK]
Directory: /etc/cron.d [SUGGESTION]
Directory: /etc/cron.daily [SUGGESTION]
Directory: /etc/cron.hourly [SUGGESTION]
Directory: /etc/cron.weekly [SUGGESTION]


[+] Home directories
- Permissions of home directories [WARNING]
- Ownership of home directories [OK]
- Checking shell history files [OK]
[+] Kernel Hardening
- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFFERENT]
- fs.protected_fifos (exp: 2) [DIFFERENT]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [OK]
- kernel.core_uses_pid (exp: 1) [DIFFERENT]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.modules_disabled (exp: 1) [DIFFERENT]
- kernel.perf_event_paranoid (exp: 3) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFFERENT]
- kernel.yama.ptrace_scope (exp: 1 2 3) [DIFFERENT]
- net.core.bpf_jit_harden (exp: 2) [DIFFERENT]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Hardening
- Installed compiler(s) [FOUND]
- Installed malware scanner [NOT FOUND]


* Enable sysstat to collect accounting (disabled) [ACCT-9626]
https://cisofy.com/lynis/controls/ACCT-9626/
* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/lynis/controls/ACCT-9628/
* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/lynis/controls/FINT-4350/
* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/lynis/controls/TOOL-5002/
* Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
https://cisofy.com/lynis/controls/FILE-7524/
* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
https://cisofy.com/lynis/controls/HOME-9304/
* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/lynis/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/lynis/controls/HRDN-7230/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
Lynis security scan details:
Hardening index : 60 [##########]
Tests performed : 265
Plugins enabled : 1
Components:
- Firewall [V]
- Malware scanner [X]
Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]


[+] Scheduled tasks
- Checking crontab and cronjob files [DONE]
[+] Accounting
- Checking accounting information [NOT FOUND]
- Checking sysstat accounting data [DISABLED]
- Checking auditd [NOT FOUND]
[+] Time and Synchronization
[+] Cryptography
- Checking for expired SSL certificates [0/132] [NONE]
[WARNING]: Test CRYP-7902 had a long execution: 20.065627 seconds
- Found 0 encrypted and 1 unencrypted swap devices in use. [OK]
- Kernel entropy is sufficient [YES]
- HW RNG & rngd [NO]
- SW prng [YES]
[+] Virtualization
[+] Containers
[+] Security frameworks
- Checking presence AppArmor [FOUND]
- Checking AppArmor status [DISABLED]
- Checking presence SELinux [NOT FOUND]
- Checking presence TOMOYO Linux [NOT FOUND]
- Checking presence grsecurity [NOT FOUND]
- Checking for implemented MAC framework [NONE]
[+] Software: file integrity
- Checking file integrity tools
- dm-integrity (status) [DISABLED]
- dm-verity (status) [DISABLED]
- Checking presence integrity tool [NOT FOUND]
[+] Software: System tooling
- Checking automation tooling
- Automation tooling [NOT FOUND]
- Checking for IDS/IPS tooling [NONE]

```
[+] Software: Malware
------------------------------------

[+] File Permissions
------------------------------------

  - Starting file permissions check
    File: /boot/grub/grub.cfg                               [ OK ]
    File: /etc/crontab                                      [ SUGGESTION ]
    File: /etc/group                                        [ OK ]
    File: /etc/group-                                       [ OK ]
    File: /etc/hosts.allow                                  [ OK ]
    File: /etc/hosts.deny                                   [ OK ]
    File: /etc/issue                                        [ OK ]
    File: /etc/issue.net                                    [ OK ]
    File: /etc/motd                                         [ OK ]
    File: /etc/passwd                                       [ OK ]
    File: /etc/passwd-                                      [ OK ]
    File: /etc/ssh/sshd_config                              [ SUGGESTION ]
    Directory: /root/.ssh                                   [ OK ]
    Directory: /etc/cron.d                                  [ SUGGESTION ]
    Directory: /etc/cron.daily                              [ SUGGESTION ]
    Directory: /etc/cron.hourly                             [ SUGGESTION ]
    Directory: /etc/cron.weekly                             [ SUGGESTION ]
    Directory: /etc/cron.monthly                            [ SUGGESTION ]

[+] Home directories
------------------------------------

  - Permissions of home directories                         [ WARNING ]
  - Ownership of home directories                           [ OK ]
  - Checking shell history files                            [ OK ]

[+] Kernel Hardening
------------------------------------

  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                       [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                           [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                       [ OK ]
    - fs.protected_regular (exp: 2)                         [ OK ]
    - fs.protected_symlinks (exp: 1)                        [ OK ]
    - fs.suid_dumpable (exp: 0)                             [ OK ]
    - kernel.core_uses_pid (exp: 1)                         [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                          [ OK ]
    - kernel.dmesg_restrict (exp: 1)                        [ OK ]
    - kernel.kptr_restrict (exp: 2)                         [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                      [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 3)                   [ OK ]
    - kernel.randomize_va_space (exp: 2)                    [ OK ]
    - kernel.sysrq (exp: 0)                                 [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)             [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                 [ DIFFERENT ]
    - net.core.bpf_jit_harden (exp: 2)                      [ DIFFERENT ]
```


- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFFERENT]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFFERENT]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFFERENT]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFFERENT]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Hardening
- Installed compiler(s) [FOUND]
- Installed malware scanner [NOT FOUND]
[+] Custom tests
- Running custom tests... [NONE]
[+] Plugins (phase 2)
-[Lynis 3.0.2 Results]-
Warnings (2):
! iptables module(s) loaded, but no rules active [FIRE-4512]
https://cisofy.com/lynis/controls/FIRE-4512/
Suggestions (51):
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
https://cisofy.com/lynis/controls/LYNIS/
* Consider using a tool to automatically apply upgrades [PKGS-7420]
https://cisofy.com/lynis/controls/PKGS-7420/
* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'sctp' is really needed on this system [NETW-3200]

```
Suggestions (51):
-----------------

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

* Consider using a tool to automatically apply upgrades [PKGS-7420]
    https://cisofy.com/lynis/controls/PKGS-7420/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
    https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
    https://cisofy.com/lynis/controls/HTTP-6643/

* Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
    https://cisofy.com/lynis/controls/PHP-2376/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
    https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]
    https://cisofy.com/lynis/controls/LOGG-2190/

* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]
    https://cisofy.com/lynis/controls/INSE-8318/

* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]
    https://cisofy.com/lynis/controls/INSE-8320/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
    https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
    https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
    https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]
```

Remotely trying to access contents of phone on same network:

```
┌──(root💀kali)-[~]
└─# lynis audit system remote 192.168.29.142

How to perform a remote scan:
=============================
Target  : 192.168.29.142
Command : ./lynis audit system

* Step 1: Create tarball
  mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis

* Step 2: Copy tarball to target 192.168.29.142
  scp -q ./files/lynis-remote.tar.gz 192.168.29.142:~/tmp-lynis-remote.tgz

* Step 3: Execute audit command
  ssh 192.168.29.142 "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system"

* Step 4: Clean up directory
  ssh 192.168.29.142 "rm -rf ~/tmp-lynis"

* Step 5: Retrieve log and report
  scp -q 192.168.29.142:/tmp/lynis.log ./files/192.168.29.142-lynis.log
  scp -q 192.168.29.142:/tmp/lynis-report.dat ./files/192.168.29.142-lynis-report.dat

* Step 6: Clean up tmp files (when using non-privileged account)
  ssh 192.168.29.142 "rm /tmp/lynis.log /tmp/lynis-report.dat"
```

```
┌──(root💀kali)-[~]
└─# sudo apt install apt-listbugs
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
apt-listbugs is already the newest version (0.1.35).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.

┌──(root💀kali)-[~]
└─# sudo apt install needrestart
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
needrestart is already the newest version (3.5-5).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.

┌──(root💀kali)-[~]
└─# sudo apt install apt-listchanges
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
apt-listchanges is already the newest version (3.24).
0 upgraded, 0 newly installed, 0 to remove and 1160 not upgraded.
```

Executing suggestions:

```
┌──(root💀kali)-[/lynis]
└─# sudo apt-get install -y libpam-tmpdir
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  libpam-tmpdir
0 upgraded, 1 newly installed, 0 to remove and 1162 not upgraded.
Need to get 11.9 kB of archives.
After this operation, 54.3 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libpam-tmpdir amd64 0.09+b2 [11.9 kB]
Fetched 11.9 kB in 2s (5,106 B/s)
Selecting previously unselected package libpam-tmpdir.
(Reading database ... 271070 files and directories currently installed.)
Preparing to unpack .../libpam-tmpdir_0.09+b2_amd64.deb ...
Unpacking libpam-tmpdir (0.09+b2) ...
Setting up libpam-tmpdir (0.09+b2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install fail2ban
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  python3-systemd
Suggested packages:
  mailx monit
The following NEW packages will be installed:
  fail2ban python3-systemd
0 upgraded, 2 newly installed, 0 to remove and 1160 not upgraded.
Need to get 487 kB of archives.
After this operation, 2,337 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 fail2ban all 0.11.2-2 [451 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-systemd amd64 234-3+b4 [36.4 kB]
Fetched 487 kB in 15s (31.6 kB/s)
Retrieving bug reports ... Done
Parsing Found/Fixed information ... Done
serious bugs of fail2ban (→ 0.11.2-2) <Forwarded>
 b1 - #991449 - fix for CVE-2021-32749 breaks systems with mail from bsd-mailx
Summary:
 fail2ban(1 bug)
Are you sure you want to install/upgrade the above packages? [Y/n/?/...] Y
Selecting previously unselected package fail2ban.
(Reading database ... 273242 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.11.2-2_all.deb ...
Unpacking fail2ban (0.11.2-2) ...
Selecting previously unselected package python3-systemd.
Preparing to unpack .../python3-systemd_234-3+b4_amd64.deb ...
Unpacking python3-systemd (234-3+b4) ...
Setting up fail2ban (0.11.2-2) ...
update-rc.d: We have no instructions for the fail2ban init script.
update-rc.d: It looks like a network service, we disable it.
fail2ban.service is a disabled or a static unit, not starting it.
Setting up python3-systemd (234-3+b4) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install debsecan
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  bsd-mailx exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libidn12 liblockfile1 libunbound8
Suggested packages:
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl
The following NEW packages will be installed:
  bsd-mailx debsecan exim4-base exim4-config exim4-daemon-light libgnutls-dane0 libidn12 liblockfile1 libunbound8
0 upgraded, 9 newly installed, 0 to remove and 1160 not upgraded.
Need to get 3,327 kB of archives.
After this operation, 6,648 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 exim4-config all 4.95-2 [335 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-base amd64 4.95-2 [1,187 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libunbound8 amd64 1.13.1-1 [504 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libgnutls-dane0 amd64 3.7.2-2 [404 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 libidn12 amd64 1.38-3 [83.3 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 exim4-daemon-light amd64 4.95-2 [674 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 liblockfile1 amd64 1.17-1+b1 [17.0 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 bsd-mailx amd64 8.1.2-0.20180807cvs-2 [88.6 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 debsecan all 0.4.20.1 [33.2 kB]
Fetched 3,327 kB in 1min 14s (45.2 kB/s)
Retrieving bug reports ... Done
Parsing Found/Fixed information ... Done
Preconfiguring packages ...
Selecting previously unselected package exim4-config.
(Reading database ... 273712 files and directories currently installed.)
Preparing to unpack .../0-exim4-config_4.95-2_all.deb ...
Unpacking exim4-config (4.95-2) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../1-exim4-base_4.95-2_amd64.deb ...
Unpacking exim4-base (4.95-2) ...
Selecting previously unselected package libunbound8:amd64.
Preparing to unpack .../2-libunbound8_1.13.1-1_amd64.deb ...
Unpacking libunbound8:amd64 (1.13.1-1) ...
Selecting previously unselected package libgnutls-dane0:amd64.
Preparing to unpack .../3-libgnutls-dane0_3.7.2-2_amd64.deb ...
Unpacking libgnutls-dane0:amd64 (3.7.2-2) ...
Selecting previously unselected package libidn12:amd64.
Preparing to unpack .../4-libidn12_1.38-3_amd64.deb ...
Unpacking libidn12:amd64 (1.38-3) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../5-exim4-daemon-light_4.95-2_amd64.deb ...
Unpacking exim4-daemon-light (4.95-2) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack .../6-liblockfile1_1.17-1+b1_amd64.deb ...
Unpacking liblockfile1:amd64 (1.17-1+b1) ...
Selecting previously unselected package bsd-mailx.
```

```
Unpacking exim4-config (4.95-2) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../1-exim4-base_4.95-2_amd64.deb ...
Unpacking exim4-base (4.95-2) ...
Selecting previously unselected package libunbound8:amd64.
Preparing to unpack .../2-libunbound8_1.13.1-1_amd64.deb ...
Unpacking libunbound8:amd64 (1.13.1-1) ...
Selecting previously unselected package libgnutls-dane0:amd64.
Preparing to unpack .../3-libgnutls-dane0_3.7.2-2_amd64.deb ...
Unpacking libgnutls-dane0:amd64 (3.7.2-2) ...
Selecting previously unselected package libidn12:amd64.
Preparing to unpack .../4-libidn12_1.38-3_amd64.deb ...
Unpacking libidn12:amd64 (1.38-3) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../5-exim4-daemon-light_4.95-2_amd64.deb ...
Unpacking exim4-daemon-light (4.95-2) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack .../6-liblockfile1_1.17-1+b1_amd64.deb ...
Unpacking liblockfile1:amd64 (1.17-1+b1) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack .../7-bsd-mailx_8.1.2-0.20180807cvs-2_amd64.deb ...
Unpacking bsd-mailx (8.1.2-0.20180807cvs-2) ...
Selecting previously unselected package debsecan.
Preparing to unpack .../8-debsecan_0.4.20.1_all.deb ...
Unpacking debsecan (0.4.20.1) ...
Setting up libunbound8:amd64 (1.13.1-1) ...
Setting up libidn12:amd64 (1.38-3) ...
Setting up debsecan (0.4.20.1) ...
Setting up exim4-config (4.95-2) ...
Adding system-user for exim (v4)
Setting up liblockfile1:amd64 (1.17-1+b1) ...
Setting up libgnutls-dane0:amd64 (3.7.2-2) ...
Setting up exim4-base (4.95-2) ...
exim: DB upgrade, deleting hints-db
update-rc.d: As per Kali policy, exim4 init script is left disabled.
Created symlink /etc/systemd/system/timers.target.wants/exim4-base.timer → /lib/systemd/system/exim4-base.timer.
exim4-base.service is a disabled or a static unit not running, not starting it.
Setting up exim4-daemon-light (4.95-2) ...
Setting up bsd-mailx (8.1.2-0.20180807cvs-2) ...
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Processing triggers for libc-bin (2.31-9) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
┌──(root💀kali)-[~/lynis]
└─# sudo apt install debsums
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libfile-fnmatch-perl
The following NEW packages will be installed:
  debsums libfile-fnmatch-perl
0 upgraded, 2 newly installed, 0 to remove and 1160 not upgraded.
Need to get 55.7 kB of archives.
After this operation, 155 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 libfile-fnmatch-perl amd64 0.02-2+b8 [10.4 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 debsums all 3.0.2 [45.3 kB]
Fetched 55.7 kB in 3s (18.4 kB/s)
Retrieving bug reports ... Done
Parsing Found/Fixed information ... Done
Selecting previously unselected package libfile-fnmatch-perl.
(Reading database ... 273948 files and directories currently installed.)
Preparing to unpack .../libfile-fnmatch-perl_0.02-2+b8_amd64.deb ...
Unpacking libfile-fnmatch-perl (0.02-2+b8) ...
Selecting previously unselected package debsums.
Preparing to unpack .../archives/debsums_3.0.2_all.deb ...
Unpacking debsums (3.0.2) ...
Setting up libfile-fnmatch-perl (0.02-2+b8) ...
Setting up debsums (3.0.2) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

After installing all dependancies and installations,we will see this difference along with normal execution of all above executed commands:

```
[+] Debian Tests
------------------------------------

  - Checking for system binaries that are required by Debian Tests ...
    - Checking /bin ...                                  [ FOUND ]
    - Checking /sbin ...                                 [ FOUND ]
    - Checking /usr/bin ...                              [ FOUND ]
    - Checking /usr/sbin ...                             [ FOUND ]
    - Checking /usr/local/bin ...                        [ FOUND ]
    - Checking /usr/local/sbin ...                       [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                    [ Installed and Enabled ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                          [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                       [ Installed and enabled for apt ]
    - apt-listchanges                                    [ Installed and enabled for apt ]
    - needrestart                                        [ Installed ]
    - debsecan                                           [ Installed and enabled for cron ]
    - debsums                                            [ Installed and enabled for cron ]
    - fail2ban                                           [ Installed with jail.conf ]
]
```

Conclusion:All the experiments pertaining to Information Security Management has been successfully executed and recorded.