Jawaharlal Nehru Engineering College

Cyber Security
Laboratory Manual

For

MCA Students

15, Aug 20 15– Rev 00 – Comp Sc – ISO 9000 Tech Document

Author JNEC, Aurangabad

FORWARD

It is my great pleasure to present this laboratory manual for Third year MCA students for the subject of Cyber Security keeping in view the vast coverage required for visualization of concepts of Cyber Security using Linux / Wire shark coding with examples.

As a student, many of you may be wondering with some of the questions in your mind regarding the subject and exactly what has been tried is to answer through this manual.

As you may be aware that MGM has already been awarded with ISO 9000 certification and it is our endure to technically equip our students taking the advantage of the procedural aspects of ISO 9000 Certification.

Faculty members are also advised that covering these aspects in initial stage itself, will greatly relieved them in future as much of the load will be taken care by the enthusiasm energies of the students once they are conceptually clear.

Dr. Sudhir Deshmukh
Principal

LABORATORY MANNUAL CONTENTS

This manual is intended for the Third year students of MCA branch in the subject of Cyber Security. This manual typically contains practical/Lab Sessions related to Cyber Security covering various aspects related the subject to enhanced understanding.

Although, as per the syllabus, Linux commands and Wireshark tool are prescribed, we have made the efforts to cover various aspects of Cyber Security and communication.

Students are advised to thoroughly go through this manual rather than only topics mentioned in the syllabus as practical aspects are the key to understanding and conceptual visualization of theoretical aspects covered in the books.

Good Luck for your Enjoyable Laboratory Sessions

G.R.Agarwal
MCA Department

SUBJECT INDEX

Assignment 1

1. Which command is used for finding host/domain name and IP address ?
2. Which command will display the assigned IP address of ETHERNET adapter?
3. Which command is used for checking the network connectivity ?
4. Which command is used for finding all the ip addresses of a given domain name ?
5. Which command is used for finding connection to and from the host ?
6. Which command is used to view user information, user's login name, real name, terminal name and write status ?
7. Which command is used for mapping name to IP addresses?
8. Which command is used for connecting to a host on a particular port ?
9. Which command is used to make a connection to a remote machine and execute
10. Programs as if one were physically present ?
11. What are the text based web browsers available through command line ?

Assignment 2

1. Which command is used for downloading a website for off-line view ?
2. Which command is used for displaying or manipulating the ARP (Address Resolution Protocol) information on a network device or computer. ?
3. Which command is used for checking/starting/stopping networking services, users, messaging, configuration and so on... ?
4. Which command is a packet filtering configuration program used for manipulating netfilter kernel based firewall ?
5. Which command is used for showing network statistics ?
6. Which command is used for displaying and manipulating routing table ?
7. Which command is used to monitor access control for supported services ?
8. Which command is used to view network traffic ?
9. Which command is used to change your hostname ?
10. Which command is used for an interface IP address ?

Assignment 3

1. Which command is used for controls access to daemons at the application level, rather than at the IP level?
2. Which command is used for connecting to a host with encryption?
3. In which file, we can find the local look up server used by the browser.
4. Command used to find out the intermediate nodes between the host and the server is.
5. Which command used to find out the intermediate domain name nodes between the host and the server?
6. Command used to follow all the information a DNS server has about a particular domain
7. The command is get documents/files from or send documents to a server

8. How to check if a particular interface is up and running?
9. This command is used to list info about machines that respond to SMB name queries (for example windows based machines sharing their hard disk's).
10. This command is used to look up the contact information from the "whois" databases, the servers are only likely to hold major sites. Note that contact information is likely to be hidden or restricted as it is often abused by crackers and others looking for a way to cause malicious damage to organizations.
11. It allows you to send and receive files between two computers.
12. Another part of the ssh package. This command is similar to ftp but uses an encrypted tunnel to connect to an ftp server and is therefore more secure than just plain ftp.
13. Part of the ssh package. Allows you to copy files from one computer to another computer.
14. nfs - nfs fstab format and options
15. where to look to find out the services which are available to the system .
16.where to look to find out the list of protocols which are available to the system along with their port numbers .
17. To listing the iptables of your linux system.
18. How to know if a service is running or not.
19. How to Enable IP Forwarding in Linux.

Assignment 4

1. Study of Wireshark Manual.

Assignment 5

Perform the following using Wireshark

1. Identify the first 2 packets (i.e. their packet numbers) containing HTTP GET request.
2. What webpage was visited in the above 2 packets?
3. What version of HTTP was used?
4. What is the destination IP address in the above packets?
5. List the source and destination ports of the packets travelling from the client to the server in the above packets?
6. In the HTTP server's response, look at the information sent about the server. What server software was used?
7. What are the IP addresses of the server?

Assignment 6

Perform the following using Wireshark.

1. What are the MAC addresses of the client and server?
2. How many WebPages (not websites) have been opened?
3. What is the time difference between first HTTP GET and the first HTTP response (OK)?
4. Count the total number of HTTP GET requests.
5. What is the time difference between the first and last HTTP GET requests? Hint: Follow a similar procedure as mentioned previously.
6. How may packets were exchanged between the server (corresponding to the both IP ad- dresses) and the client? (Note: Their sum must be equal to the total no. of packets)
7. Find the total no. of HTTP requests sent by the host spongebob.wikia.com.

Assignment 7

1. SQL Injection Implementation and Execution.

Assignment 8

1. Give a short note on OSSEC?
2. What are the components of OSSEC
3. List the few key features of OSSEC.
4. What are the types of agent in OSSEC?
5. What are the roles of Manager (server) and an Agent in OSSEC?
6. What is Syscheck in OSSEC?
7. What is LIDS and HIDS?

Assignment 9

1. Which type of log is used by pflogsumm.
2. Which type of log is used by webalizer.
3. What are the different types of log is/are used by AWStats
4. pflogsumm analyzes is a mail/weblog or both ?
5. webalizer analyzes is a mail/weblog or both ?
6. command line option used for increment log analysis, mention domain name and squid log file with webalizer.
7. AWStats tools written in which language?

Assignment 10

1. Steps for setting up Cyber Security in organization.

References for All Assignments:

1. http://www.ossec.net/
2. www.linuxmanpages.com/man1/pflogsumm.1.php
3. www.webalizer.org/
4. http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/

DO's and Don'ts in Laboratory:

1. Do not handle any equipment before reading the instructions/Instruction manuals

2. Read carefully the power ratings of the equipment before it is switched on whether
Ratings 230 V/50 Hz or 115V/60 Hz. For Indian equipments, the power ratings are
Normally 230V/50Hz. If You have equipment with 115/60 Hz ratings, do not insert
Power plug, as our normal supply is 230V/50 Hz, which will damage the equipment.

3. Observe type of sockets of equipment power to avoid mechanical damage

4. Do not forcefully place connectors to avoid the damage

5. Strictly observe the instructions given by the teacher/Lab Instructor

Instruction for Laboratory Teachers::

1. Submission related to whatever lab work has been completed should be done during the next lab session. The immediate arrangements for printouts related to submission on the day of practical assignments.

2. Students should be taught for taking the printouts under the observation of lab teacher.

3. The promptness of submission should be encouraged by way of marking and evaluation patterns that will benefit the sincere students.

1. LAB EXCERCISES:

[Purpose these exercises is to make familiar the students to Redhat Linux Networking Commands]

- *Exercise No1: (2 Hours) : Theory & Practical Assignment Submission .*

- *Students are required to study the aspects of Linux Networking understand and execute all the networking commands.*

Refer to Solution Manual Document for detailed study and examples.

2. Lab Exercises:

[Purpose of these exercises to make familiar students to Redhat Linux Networking]

- *Exercise No2: (2 Hours) : Practical & Theory Assignment Submission .*

- *Students are required to study the aspects of Linux Networking understand and execute all the networking commands.*

Refer to Solution Manual Document for detailed study and examples.

3. Lab Exercises:

Exercise No3: (2 Hours) – 1 Practical.

[Purpose of these exercises to make familiar students with Traditional Linux Networking and their Implementations]

- *Exercise No3: (2 Hours) : Practical & Theory Assignment Submission .*

- *Students are required to study the aspects of Linux Networking understand and execute all the networking commands.*

Refer to Solution Manual Document for detailed study and examples.

4. Lab Exercises:

[Purpose of this exercise is to Study Wireshark Packet Monitoring software Manual]

Exercise No 4: (2 Hours) – 1 Theory Assignment.

This assignment requires the students to study the monitoring of data packets and packet headers using wireshark freeware. Specifically HTTP,FTP, SMTP type of packet traffic need to be studied.

Refer to Solution Manual Document for detailed study and examples.

5. Lab Exercises:

[Purpose of these exercises to monitor network traffic using wire shark tool]

Exercise No 5: (2 Hours) – 1 Practical.

- *Students are required to Monitor Network Traffic by Monitoring HTTP and other protocol generated Traffic. Wireshark is freeware can be down loaded for the purpose.*

Refer to Solution Manual Document for detailed study and examples.

6. Lab Exercises:

[Purpose of these exercises to monitor network traffic using wire shark tool]

Exercise No 6: (2 Hours) – 1 Practical

- *Students are required to Monitor Network Traffic by Monitoring HTTP and other protocol generated Traffic using Wireshark.*

Refer to Solution Manual Document for detailed study and examples.

7. Lab Exercises:

[Purpose of these exercises to study and Execute SQL Injection queries]

Exercise No 7: (2 Hours) – 1 Practical

Oracle Server session to be used for the purpose to execute and understand SQL query Anomalies.

Oracle Server Login : system password : manager

Refer to Solution Manual Document for detailed study and examples.

8. Lab Exercises:

[Purpose of these exercises to study and understand, use and monitor open source security tool]

Exercise No 8: (2 Hours) – 1 Practical

OSSEC is a freeware for Open source host based Intrusion detection system. Student can reach www.ossec.net for documentation and software download from the site.

Refer to Solution Manual Document for detailed study and examples.

9. Lab Exercises:

[Purpose of these exercises to study and understand, use and record readings of pflogsum log analyzer and summarizer and also to understand webalizer]

Exercise No 9: (4 Hours) – 2 Practical

Pflogsum is a log analyzer and summarizer program. Webalizer is a fast ,free webserver log file analysis program.
Student can visit www.webalizer.org home site for documentation and download of the software.

Refer to Solution Manual Document for detailed study and examples.

10.Lab Exercises:

[Purpose of these exercises to study and understand and write a theory assignment for setting up security in an organization]

Exercise No 10: (4 Hours) – 2 Theory Assignment.

Refer to Solution Manual Document for detailed study and examples.