Indira Gandhi Delhi Technical University for Women

(Established by Govt. of Delhi vide Act 09 of 2012)

(Formerly Indira Gandhi Institute of Technology)

Kashmere Gate, Delhi - 110006

LABORATORY MANUAL
[2013-2014]

For

OS Hardening

MIS-528

TABLE OF CONTENTS

1. Objectives of the Lab…….……3
2. Rules to be followed in the Lab…….....4
3. Syllabus…….……...5
4. Guidelines……..….....7
5. List of Experiments……8
6. Evaluation Policy……9
7. Project……10

OBJECTIVES OF THE LAB

This manual is intended for the Second Semester students of M.Tech in the subject of OS Hardening.

This manual typically contains exercises for the practical/lab sessions related to the subject so as to help the students in enhancing their understanding of the course and implement the concepts learnt in theory sessions.

RULES TO BE FOLLOWED IN LAB

1. Plagiarism in any form will not be tolerated in the lab work and project.

2. The students must submit the files for checking strictly as advised by the instructor in the lab without fail.

3. The students are supposed to mandatorily appear for the internal assessment on the day as announced in the lab.

4. Any student found indulged in malpractices, disobedience will be debarred from the lab without any warning for a part/whole semester.

5. It is expected and strongly encouraged that students utilize their Lab hours efficiently.

6. Every effort should be made to complete the lab work in the assigned lab only.

7. Every student work on assigned system only. Any problem in the system must be reported to the lab in charge in advance. Reporting and ensuring the physical condition of the system is the responsibility of the students. No exercise in this regard will be entertained.

SYLLABUS

Paper Code: MIS-504	L	P	C
Paper: OS Hardening	4	0	4

INSTRUCTIONS TO PAPER SETTERS:
Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks.
Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks

UNIT 1

Overview of Linux and Windows Operating system, Linux Kernel, Windows kernel, Networking , Secure booting, Boot loaders and Boot time services, Securing Virtual Terminals, Securing log in Screens, Users and Groups, Shadow Password, Groups, adding groups, Deleting Unnecessary users and Groups, Passwords, Password Aging, Process Accounting, Plugable Authentication Modules, , Hardening Kernel in Linux

(10 Hrs)

UNIT 2

Working of Linux Firewall, Tabls, Chains, Policies, Filtering Criteria, IP table Commands, Securing Connections and Remote Administrations, Public key encryptions, SSL,TLS, Open SSL, Remote administration, ssh, scp,sftp, ssh-agent, Agent forwarding, The sshd Daemon, Securing Files and File system, Access Permission, Imutable Files, Encrypting Files, Securely Mounting Files, Secring removal devices, Understanding Logging and log Monitoring, Syslog, Syslog-NG, Log anaysis and correlation, Hardening remote access to Email, Securing FTP server

(10 Hrs)

UNIT 3

Understanding Windows Kernel, Windows attacks, Automated Vs dedicated attackers, Virus, Trojan, Directory traversal, Password Cracking, Social engineering, Adware, spyware, spam, phishing and Farming, Conventional Defense mechanism, Unconventional defenses, Host based firewall, Use of Anti -virus , Anti-Spam software, and anti-spam softwares, Hardening TCP/IP stack, Securing Files and File system in Windows, NTFS permissions, Best practice recommendations. (10 Hrs)

UNIT 4

Windows password authentication, Unicode password, Password Complexities, Strong Password, Windows password Hashes, Password Attacks, tools and techniques, Defense mechanism against password attacks, Disable LM password Hashes, Disable LM and NTLM authentication, Hardening File System, Protection of High Risk files, High risk windows files, File Defenses, Methods to prevent unauthorised execution, Securing internet explorer

(10 Hrs)

References:

1. R A Grimes, "Professional Windows Desktop and server Hardening ", 1st edition, 2006, Wiley India Edition
2. James Turnbull, " Hardening Linux", 1st edition , 2005, Apress publication
3. Scambray, Shema, and Sima, "Hacking Exposed Web Applications", 3rd edition , 2010, McGraw Hill.
4. Sander Van Vugt, " Red Hat Enterprise Linux 6 Administration", 1st edition, 2010, Wiley Interscience

GUIDELINES

1. In file, every lab experiment will consist of the objectives, methods, tools (if any), source code and output, observations and results.

2. The students also have to save their programs in a directory on the machine they are assigned in the lab (details will be given in lab).

3. The students must ensure that the schedule for completion of the lab experiments is strictly adhered to. Delay in performing practical assignments or submission of file as per the stipulated schedule will suggest underperformance by the student and will inevitably lead to penalty in marks.

4. Students are expected to read the lab manual carefully and come prepared with the theoretical concepts of the experiment they are going to perform in the lab so as to ensure effective utilization of lab hours to finish the experiment timely and allow students to work on more complicated cases based on the experiment which will be discussed in lab once the students have completed the basic experiment.

5. It must be noted that the every lab experiment once completed will be followed by implementing the same on complex data sets and problems. The same will be announced in lab in detail.

LIST OF EXPERIMENTS

1. Install Linux & Windows operating systems.
2. Implement the basic and advanced DOS and Linux commands.
3. Secure boot loader config files in Linux (*LILO & Grub*) using passwords and encryption.
4. Control the boot sequencing and start up services *init* and *inittab* scripts.
5. Implement *vlock* for securing virtual terminals in Linux.
6. Manage the ACL (users & groups) of a Linux based system.
7. Implement authentication framework based on module stacking using Pluggable Authentication Module in Linux.
8. Analyze the password management and its aging rules in Linux based systems.
9. Implement process accounting at startup for machine with Linux operating system.
10. Implement the Password security and Access control in Windows.
11. Install the Linux kernel hardening patch Openwall.
12. Execute Openwall for kernel analysis and hardening.
13. Analyse Linux basedNetfilter firewall and its rules.
14. Create a set of iptables rules for INPUT, OUTPUT and FORWARD chains.
15. Perform system hardening using the Microsoft Baseline Analyzer Assessment (MBSA) tool.
16. Implement the Group Policies, Security Templates and Configuration Baselines in a Windows OS.
17. Perform the application of the updates, hot fixes and patch management in Windows and Linux.
18. Implement the File System security in Windows and Linux
19. Implement the Service security in Windows and Linux
20. Perform the log analysis in Windows based systems.

Evaluation Policy

1. The will be regular supervision and assessment of the students during the labhours throughout the semester.

2. The student must complete the lab work and get the files submitted and checkedas advised in the lab by the instructor.

3. Internal Assessment will be done as per the academic calendar which will includeviva, practical and project status report.

4. The students are expected to come up with novice approaches in problem solvingespecially while working on the project which will earn them marks accordingly.

Project

The students will be required to work in group of n (2<n<6) students for the projectwork which is primarily going to be designed to evaluate the student's understandingof the subject and also inculcate the qualities of applying the theoretical knowledge tothe practical real world applications. The students are expected to not only implementthe use of subject knowledge but also think out of the box and look for proposing newissues, problems and their solutions in the subject domain.

The details of the same will be discussed in the lab. The projects will be assignedbefore Minor I and evaluated throughout the semester in the lab for progress. Finalevaluation will be done 1 week after the Minor II.

The students are allowed and encouraged to refer the study material in books,references, internet etc but Plagiarism from any possible source is strictly prohibited.