

|  |  |  |  |
| --- | --- | --- | --- |
| **Penetration Testing** | | | |
| Lab Manual | | |
| **Department of Computer Science and Engineering**  **The NorthCap University, Gurugram** | | |
|  | |
|  | |
|  | |
|  | |
|  |

**Penetration Testing**

**Lab Manual**

**CSL282**

**Dr. Mehak Khurana**



Department of Computer Science and Engineering

The NorthCap University, Gurugram- 122001, India

Session 2019-20

*Published by:*

**School of Engineering and Technology**

**Department of Computer Science & Engineering**

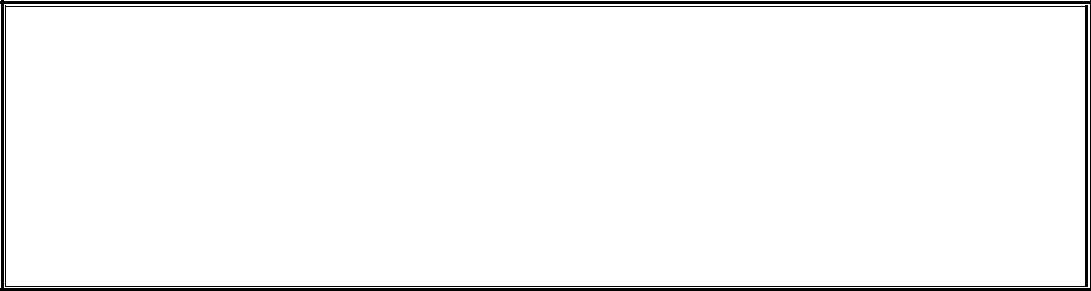
**The NorthCap University Gurugram**

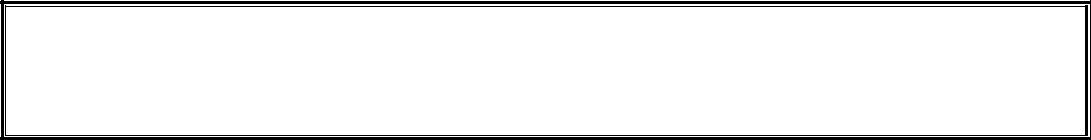
**• Laboratory Manual is for Internal Circulation only**

**© Copyright Reserved**

*No part of this Practical Record Book may be*

*reproduced, used, stored without prior permission of The NorthCap University*



Copying or facilitating copying of lab work comes under cheating and is considered as use of unfair means. Students indulging in copying or facilitating copying shall be awarded zero marks for that particular experiment. Frequent cases of copying may lead to disciplinary action. Attendance in lab classes is mandatory.

Labs are open up to 7 PM upon request. Students are encouraged to make full use of labs beyond normal lab hours.

**PREFACE**

Operating System Lab Manual is designed to meet the course and program requirements of NCU curriculum for B.Tech III year students of CSE branch. The concept of the lab work is to give brief practical experience for basic lab skills to students. It provides the space and scope for self-study so that students can come up with new and creative ideas.

The Lab manual is written on the basis of “teach yourself pattern” and expected that students who come with proper preparation should be able to perform the experiments without any difficulty. Brief introduction to each experiment with information about self-study material is provided. The laboratory exercises will include familiarization with LINUX system calls for process management and inter-process communication; Experiments on process scheduling and other operating system tasks through simulation/implementation. Students would require design process synchronization, CPU scheduling algorithms, memory management and disc management algorithms in high level languages like c, c++, python. Finally, the students would require applying the operating system concepts by experimenting on either xv6/minix operating systems. At the start of each experiment a question bank for preparation and practice is suggested which may be used to test the basic understanding of the students about the experiment. Students are expected to come thoroughly prepared for the lab. General disciplines, safety guidelines and report writing are also discussed.

The lab manual is a part of curriculum for the TheNorthCap University, Gurugram. Teacher’s copy of the experimental results and answer for the questions are available as sample guidelines.

We hope that lab manual would be useful to students of CSE, IT, ECE and BSc branches and author requests the readers to kindly forward their suggestions / constructive criticism for further improvement of the workbook.

Author expresses deep gratitude to Members, Governing Body-NCU for encouragement and motivation.

**Authors**

**The NorthCap University**

**Gurugram, India**

|  |  |  |  |
| --- | --- | --- | --- |
| **CONTENTS** | | | |
| S.N. | **Details** | Page No. | |
|  | **Syllabus** |  | |
| 1 | **Introduction** |  | |
| 2 | **Lab Requirement** |  |
| 3 | **General Instructions** |  |
| 4 | **List of Experiments** |  |
| 8 | **Annexure 1 (Format of Lab Report)** |  |
| 9 | **Annexure 2 (Format of Lab Certificate)** |  |

**SYLLABUS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Department:** | | **Department of Computer Science and Engineering** | | | | | |
| 1. **Course Name:** Penetration Testing | | | | 1. **Course Code** | 1. **L-P** | | 1. **Credits** |
| CSL282 | 3-4 | | 4 |
| 1. **Type of Course (Check one):** | | Programme Core **✓**  Programme Elective Open Elective | | | | | |
| 1. **Pre-requisite(s), if any:** | | | | | | | |
| 1. **Frequency of offering (check one):** Odd Even **✓** Either semester Every semester | | | | | | | |
| 1. **Brief Syllabus:**   This course is focused on the practical side of penetration testing whilst including necessary theoretical details. It will make students learn how to protect users from cyber attackers by becoming an ethical hacker. It takes students from a beginner to a more advanced level, by the time course finishes students will be able to launch attacks and test the security of computers. It commences with different ways of gathering information about the target and consequently discusses various ways to discover and exploit large number of vulnerabilities to gain access. Thereafter, it includes what you can do with the access you gained from exploiting the above vulnerabilities and ways to maintain that access. | | | | | | | |
| **Total lecture, Tutorial and Practical Hours for this course (Take 15 teaching weeks per semester): 90** | | | | | | | |
| **Lectures: 40 hours** | | | **Practice** | | | | |
| **Tutorials : 5 hours** | | | **Lab Work: 45 hours** | |
| 1. **Course Outcomes (COs)**   Possible usefulness of this course after its completion i.e. how this course will be practically useful to him once it is completed | | | | | | | |
| **CO 1** | Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment. | | | | | | |
| **CO 2** | Utilize scanning tools to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments. | | | | | | |
| **CO 3** | Recognize security vulnerabilities, such as weak configurations, unpatched systems. | | | | | | |
| **CO 4** | Apply penetration testing tools to exploit and investigate vulnerable systems. | | | | | | |
| **CO 5** | Implementing on web application-based attacks | | | | | | |
| 1. **UNIT WISE DETAILS No. of Units: 45** | | | | | | | |
| **Unit Number: 1 Title:** Introduction **No. of hours: 5**  **Content Summary:**  What is Data, Information, places of data, Security Triangle, key terms, Types of Information, Cyber Terrorism, Defacement, Cyber laws, Network Terminologies, Introduction to network, Network Protocols, IP address, IP subnet, classes, NAT, DHCP Server, Types of network, Ports, Proxy Servers, Introduction to Malwares | | | | | | | |
| **Unit Number: 2 Title:** Information Gathering/Footprinting  **No. of hours: 8**  **Content Summary:**  Introduction to Information gathering, Web VAPT, Network VAPT, IMSM, Information gathering Domain Name Services, targeting email and Maltego, Recon-ng and google operators, digital footprinting, shared web servers, dedicated web servers | | | | | | | |
| **Unit Number: 3 Title:** Scanningand its types **No. of hours: 10**  **Content Summary:**  Introduction, Nmap and Port Scanning, Vulnerability Scanner, OS Fingerprinting, Banner Grabbing, Enumeration Tools, Vulnerabilities and levels of vulnerabilities, tools to generate report, Linux basics, Penetration testing OS, Wordlist generator, Crunch tool. | | | | | | | |
| **Unit Number: 4 Title:** Gaining Access and Maintaining Access **No. of hours: 12**  **Content Summary:**  Direct Exploitation, Password Attacks-Online Offline, Exploitation-Client-side Attack, Social Engineering exploitation, OS login bypass, online, offline method, Keyloggers (Ardamax), Malwares, Trojan, Dark comet, Remote Connections  . | | | | | | | |
| **Unit Number: 5 Title:** Post Exploitation and Web application attacks **No. of hours: 5**  **Content Summary:**  Introduction to Post exploitation, Power-hub tool File Transfer Without interactive Shell, Exploit Development, Pivoting, setting up domain controller | | | | | | | |
| 1. **Brief Description of Self-learning components by students (through books/resource material etc.):** | | | | | | | |
| 1. **Books Recommended:**   **Text Books**:   * Stuart McClure,‎ Joel Scam bray,‎ George Kurtz, “Hacking Exposed 7: Network Security Secrets and Solutions”, Tata McGraw Hill, 1st edition, 2012   **Reference Books**:   * Cyber Security Essentials, James Graham, Richard Howard, Ryan Olson, CRC Taylor and Francis, 1st edition, 2010   **Reference websites: (nptel, swayam, coursera, edx, udemy, lms, official documentation weblink)**   * <https://www.cybrary.it/course/web-application-pen-testing/> * <https://www.cybrary.it/course/advanced-penetration-testing/> * https://www.cybrary.it/course/ethical-hacking/ | | | | | | | |

**Practice (Tutorial/Case Studies/ Industry Visit/Field Work) Content**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Topic** | **Unit covered** |
|  | 1. Add proxy server as an extension in google chrome and check the IP address before and after changing the proxy. 2. Add Virtual Private Network as an extension in google chrome and check the IP address before and after changing the proxy. | 1 |
|  | Case study on VAPT | 2 |
|  | Study and analysis of various Security tools | 2 |

|  |
| --- |
| **Project (To be done as individual/in group): No** |

**Evaluation Scheme (Choose one related to the course)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **TYPE OF COURSE** | **PARTICULAR** | **ALLOTTED RANGE OF MARKS** | **PASS CRITERIA** |
| 1. | Theory+ Practical  (L-T-P/L-0-P) | Minor Test | 15% | Must Secure 30% Marks Out of Combined Marks of Major Test Plus Minor Test with Overall 40% Marks in Total. |
| Major Test | 35% |
| Continuous Evaluation Through Class Tests/Practice/Assignments/Presentation/Quiz | 10% |
| Online Quiz | 5% |
| Lab Work | 35% |

1. **INTRODUCTION**

That ‘learning is a continuous process’ cannot be over emphasized. The theoretical knowledge gained during lecture sessions need to be strengthened through practical experimentation. Thus, practical makes an integral part of a learning process.

The purpose of conducting experiments can be stated as follows:

* To familiarize the students with the basic concepts, of secure programming and the take home laboratory assignments mainly implementation-oriented which includes threats, mitigation and detection techniques. The lab sessions will be based on exploring the concepts discussed in class.
* Observing Security problems in Software Programs
* Reporting and analysing the security threats and exploits in programs.
* Hands on experience on mitigation techniques

1. **LAB REQUIREMENTS**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Requirements** | **Details** |
| **1** | **Software Requirements** | Virtual Machine, Trojan, Keylogger, Wireshark, Nmap, ZenMap, Nessus |
| **2** | **Operating System** | Kali Linux, Window XP (SP0, SP1), Windows 7, windows 10 |
| **3** | **Hardware Requirements** | Windows and Linux: Intel 64/32 or AMD Athlon 64/32, or AMD Opteron processor  16 GB RAM  256 GB hard disk space |
| **4** | **Required Bandwidth** | NA |

1. **GENERAL INSTRUCTIONS** 
   1. **General discipline in the lab**
   * Students must turn up in time and contact concerned faculty for the experiment they are supposed to perform.
   * Students will not be allowed to enter late in the lab.
   * Students will not leave the class till the period is over.
   * Students should come prepared for their experiment.
   * Experimental results should be entered in the lab report format and certified/signed by concerned faculty/ lab Instructor.
   * Students must get the connection of the hardware setup verified before switching on the power supply.
   * Students should maintain silence while performing the experiments. If any necessity arises for discussion amongst them, they should discuss with a very low pitch without disturbing the adjacent groups.
   * Violating the above code of conduct may attract disciplinary action.
   * Damaging lab equipment or removing any component from the lab may invite penalties and strict disciplinary action.
   1. **Attendance**

* Attendance in the lab class is compulsory.
* Students should not attend a different lab group/section other than the one assigned at the beginning of the session.
* On account of illness or some family problems, if a student misses his/her lab classes, he/she may be assigned a different group to make up the losses in consultation with the concerned faculty / lab instructor. Or he/she may work in the lab during spare/extra hours to complete the experiment. No attendance will be granted for such case**.**
  1. **Preparation and Performance**
* Students should come to the lab thoroughly prepared on the experiments they are assigned to perform on that day. Brief introduction to each experiment with information about self study reference is provided on LMS.
* Students must bring the lab report during each practical class with written records of the last experiments performed complete in all respect.
* Each student is required to write a complete report of the experiment he has performed and bring to lab class for evaluation in the next working lab. Sufficient space in work book is provided for independent writing of theory, observation, calculation and conclusion.
* Students should follow the Zero tolerance policy for copying / plagiarism. Zero marks will be awarded if found copied. If caught further, it will lead to disciplinary action.
* Refer **Annexure 1** for Lab Report Format

1. **LIST OF EXPERIMENTS**

|  |  |  |
| --- | --- | --- |
| Exp. No. | Division of Experiments | List of Experiments |
| 1 | Reconnaissance | Perform reconnaissance to find all the relevant information on selected website  using 10 network information gathering tools. |
| Gather information using Social Networking sites and google Dorks |
| 2 | Scanning | 1. Perform active reconnaissance using AngryIPScanner, Softperfect Network Scanner, Cain&Able   Perform Network Scanning using NMAP in windows and ZENMAP in kali Linux |
| 1. Install Wireshark and apply filters to gather different information   Find the link accessed by the victim using Wireshark |
| Perform Session hijacking/ find credentials of unsecure real time website using Wireshark |
| Use Nessus tool to find all the vulnerabilities with its level and generate a report for an organization |
| 1. Perform active reconnaissance using AngryIPScanner, Softperfect Network Scanner, Cain&Able   Perform Network Scanning using NMAP in windows and ZENMAP in kali Linux |
| 3 | Password Generation | * Execute basic commands of Linux   Use CHMOD command to change the privileges and permissions |
| Generate Word list from using wordlist generator Crunch |
| Generate and password list and exploit using Hydra |
| 4 | Gaining and Maintaining Access | 1. Install Hiren Boot in bootable pen drive 2. Perform windows Login Bypass Hiren Boot or active password changer |
| Perform Kali Linux Login Bypass in virtual machine |
| Perform MAC Login Bypass in virtual machine |
| Create Trojan and Exploit victim’s machine by taking its complete access |
| Track keystrokes of victim machine using Ardamax Keylogger |
| Exploit Windows XP using Metasploit |
| Exploit Windows7 using Metasploit |
| Exploit Windows using Eternal Blue and Eternal Romance using Metasploit |
| Exploitation by creating a payload in pdf File using metasploit |
| Exploit windows using metasploitable2 |
| 5 | Covering Tracks | Perform steps to remove the tracks in windows and kali Linux |
| Temper the time and date of the files to cover tracks |

1. **LIST OF PROJECTS**
   * + 1. Generating KeyLogger
       2. Exploitation of Windows 10 using Metasploit
       3. Creating Trojan for windows 7
2. **RUBRICS**

|  |  |
| --- | --- |
| **Marks Distribution** | |
| **Continuous Evaluation(50 Marks)** | **End Semester Exam (20 Marks)** |
| Each experiment shall be evaluated for 10 marks and at the end of the semester proportional marks shall be awarded out of 50. | End semester practical evaluation including Mini project (if any) carries 20 marks. |
| Following is the breakup of 10 marks for each  **4 Marks**: Observation & conduct of experiment. Teacher may ask questions about experiment.  **3 Marks:** For report writing  **3 Marks:** For the 15 minutes quiz to be conducted in every lab. |

**Annexure 1**

**Penetration Testing**

**(CSL 282)**

Lab Practical Report



Faculty name Student name

Roll No.:

Semester:

Group:

Department of Computer Science and Engineering

The NorthCap University, Gurugram- 122001, India

Session 2019-20

**INDEX**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Experiment** | **Page No.** | **Date of Experiment** | **Date of Submission** | **Marks** | **CO Covered** | **Signature** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Experiment No: 1**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the first phase of Penetration Testing.

**Program Outcome**

* The students will understand which type of passive information can be gathered to exploit the target machine

**Problem Statement**

Perform reconnaissance to find all the relevant information on selected website using 10 information gathering tools.(Including 4 Kali Linux Tools)

**Background Study:**

* OSINT gathering is an important first step in penetration testing.
* Gathering as much intelligence on your organization and the potential targets for exploit.
* Clear understanding of the client’s systems and operations before you begin exploiting.
* (how a target works and its potential vulnerabilities.)

**Code**

**Output: Screenshots**

**Experiment No: 2**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students about the first phase of Penetration Testing.

**Program Outcome**

* The students will understand how to gather information available on google freely using google dorks

**Problem Statement**

* Gather information using Social Networking sites and google Dorks

**Background Study:**

* Google is an Attacker's Ally
* Lot of information freely available via Internet on public platform
* Personal information on company website or a social media site, that give hints to user account password.
* Names can be entered in a search engine to reveal home addresses and telephone numbers.
* Saves patches between sessions, writes them back to executable file and updates fixups
* Open architecture - many third-party plugins are available
* No installation - no trash in registry or system directories

Here, some google search syntax to crawl the password:   
  
1. "Login: \*" "password =\*" filetype: xls (searching data command to the system files that are stored in Microsoft Excel)   
  
2. allinurl: auth\_user\_file.txt (to find files auth\_user\_file.txt containing password on server).   
  
3. filetype: xls inurl: "password.xls" (looking for username and password in ms excel format). This command can change with admin.xls)   
  
4. intitle: login password (get link to the login page with the login words on the title and password words anywhere. If you want to the query index more pages, type allintitle)   
  
5. intitle: "Index of" master.passwd (index the master password page)   
  
6. index of / backup (will search the index backup file on server)   
  
7. intitle: index.of people.lst (will find web pages that contain user list).   
  
8. intitle: index.of passwd.bak ( will search the index backup password files)

**Code**

**Output: Screenshots**

**Experiment No: 3a**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Second phase of penetration testing

**Program Outcome**

* The students will understand difference between active and passive reconnaissance.
* The students will be able to gather the information of the target machine by interacting with it.
* The students will understand Nmap Tool

**Problem Statement**

Perform active reconnaissance, Network Scanning using NMAP in windows

**Background Study:**

* Active reconnaissance is commonly referred to as *scanning*.
* Taking the information discovered during reconnaissance and using it to examine the network.
* The process of scanning perimeter and internal network devices for weaknesses.
* Looking for information that can help to perpetrate attack

**Code/steps**

**Output: Screenshots**

**Experiment No: 4**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Second phase of penetration testing

**Program Outcome**

* The students will understand difference between active and passive reconnaissance.
* The students will be able to gather the information of open and closed ports of the target machine by interacting with it.
* The students will understand Zen map inbuilt Tool of Kali Linux

**Problem Statement**

Perform active reconnaissance, Network Scanning using Zenmap in windows

**Background Study:**

* It uses DNS lookup- It matches name with IP address
* It pings the remote target with 0 byte packets to each port
* Sends different packets with different timing to determine filtered/unfiltered, version, etc.

**Code/steps**

**Output: Screenshots**

**Experiment No: 5**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Second phase of penetration testing

**Program Outcome**

* The students will be able to gather the information of the network by analyzing the traffic moving in and out from target machine
* The students will understand Wireshark inbuilt Tool of Kali Linux

**Problem Statement**

* Run Wireshark on any network and apply filters to gather different information of the target machine
* Find the link accessed by the victim using Wireshark

**Background Study:**

* World’s foremost and widely-used network protocol analyzer.
* Tells what’s happening on your network at a microscopic level
* Standard across many commercial and non-profit enterprises, government agencies, and educational institutions.
* got famous in black hat.
* observes the messages exchanged.
* Passive and Preinstalled in Kali Linux, for windows [http://www.wireshark.org](http://www.wireshark.org/).

**Code/steps**

**Output: Screenshots**

**Experiment No: 6**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Second phase of penetration testing

**Program Outcome**

* The students will be able to gather the information of the network by analyzing the traffic moving in and out from target machine
* The students will understand Wireshark inbuilt Tool of Kali Linux

**Problem Statement**

Perform Session hijacking/ find credentials of unsecure real time website using Wireshark

**Background Study:**

**Packet sniffer:**

* To monitor the data transmitted over a network
* used for diagnostic or troubleshooting purposes
* To steal data transmitted over the network.
* Applicable to both wired and wireless networks
* Can be passive or active

**Code/steps**

**Output: Screenshots**

**Experiment No: 7**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Second phase of penetration testing

**Program Outcome**

* The students will be able to find all the vulnerabilites present in the target machine
* Will also understand the Nessus Vulnerability scanner tool

**Problem Statement**

Install Nessus, Use Nessus tool to find all the vulnerabilities with its level and generate a report for an organization

**Background Study:**

**Packet sniffer:**

* It has a database of vulnerabilities based on which it performs the check on the remote host.
* Its database contains all the information required (service, port, packet type, a potential path to exploit, etc.) to check the security issue.
* They can scan the network and websites against thousands of vulnerabilities, provide the list of issues based on the risk and suggest the remediation as well.

**Code/steps**

**Output: Screenshots**

**Experiment No: 8**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Linux to extract information

**Program Outcome**

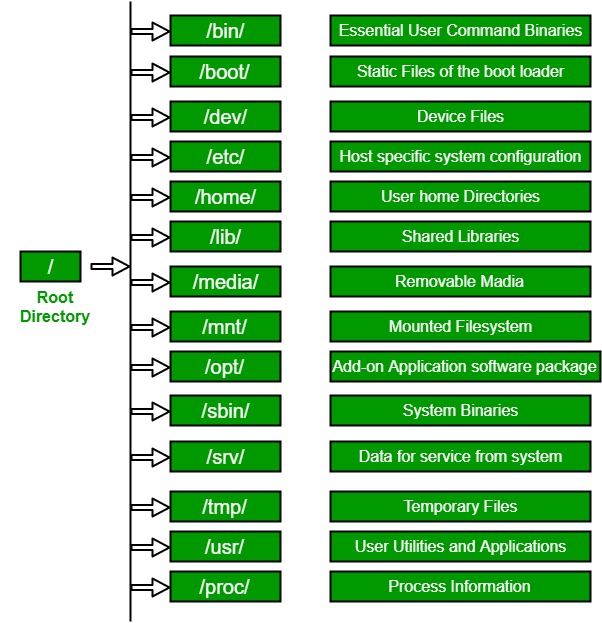
* The students will be able to learn commands of Linux required for exploitation
* Student will be able to change permissions of the Files and Folders

**Problem Statement**

* Execute basic commands of Linux
* Use CHMOD command to change the privileges and permissions

**Background Study:**

* Linux word derived and evolved from UNIX.
* Unix was the first operating system came to existence with CLI environment and mainly used for server side working as per today's requirements.
* It is the most flexible and customizable OS used by skilled individuals.
* It is an open source
* Like INDIA has its own Linux based operating system i.e. BOSS.



**Code/steps**

**Output: Screenshots**

**Experiment No: 9**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Linux Commands

**Program Outcome**

* The students will understand Crunch Word generator for password generation inbuilt Tool of Kali Linux

**Problem Statement**

Generate Word list from using wordlist generator Crunch

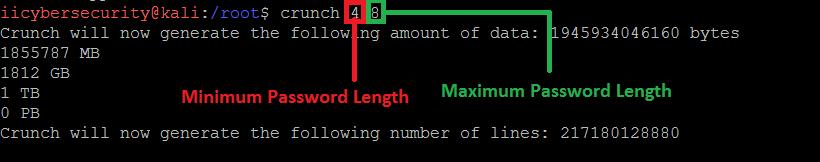
**Background Study:**

**Usage Syntax -**

**Crunch Min.Value Max.Value Characters**

**Example –**

**crunch 4 4 0123456789**



**Code/steps**

**Output: Screenshots**

**Experiment No: 10**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Password cracking

**Program Outcome**

* The students will be able to exploit password using tool

**Problem Statement**

* Generate and password list and exploit using Hydra

**Background Study:**

Brute-force search (exhaustive search) is a mathematical method, which difficulty depends on a number of all possible solutions. The definition «brute-force» is usually used in the context of hackers attacks when the intruder tries to find valid login/password to an account or service.

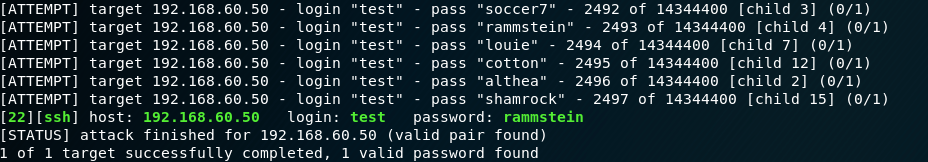
Examine tools are possible to use for brute-force attacks on SSH and web services, which are available in Kali Linux (Patator, Medusa, THC Hydra, Metasploit) and BurpSuite.

For password mining using THC Hydra run the command:

hydra -V -f -t 4 -l test -P /root/wordlist ssh://192.168.60.50

where:

* -V — to display a couple login+password while the password mining;
* -f — is a stop as soon as the password for specified login will be found;
* -P — is a path to the password dictionary;
* ssh://192.168.60.50 — is a service and victim IP address.



**Code/steps**

**Output: Screenshots**

**Experiment No: 11**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Bypass the Login of Windows

**Program Outcome**

* The students will be able to Bypass the login details of target in active and passive mode on all type of operating system

**Problem Statement**

* Install Hiren Boot in bootable pen drive,
* Perform windows Login Bypass Hiren Boot or active password changer

**Background Study:**

* Login Bypass
  + Online Method
    - System Unlocked
  + Offline Method
    - System locked

**Code/steps**

**Output: Screenshots**

**Experiment No: 12**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Bypass the Login of Linux and MAC

**Program Outcome**

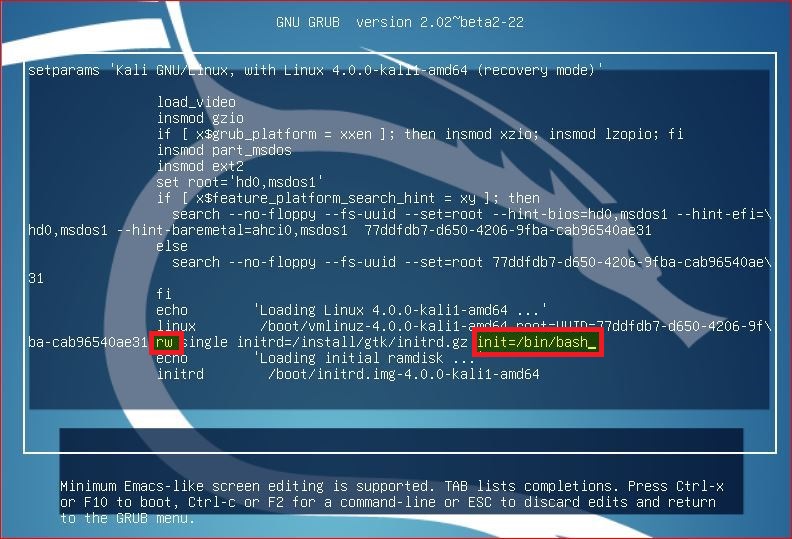
* The students will be able to Bypass the login details of target in active and passive mode on all type of operating system

**Problem Statement**

* Perform Kali Linux Login Bypass in virtual machine
* Perform MAC Login Bypass in virtual machine

**Background Study:**

Bypassing Login of Kali Linux and MAC:



**Code/steps**

**Output: Screenshots**

**Experiment No: 13**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of exploitation

**Program Outcome**

* The students will be able to gain access of target machine using Malware

**Problem Statement**

Create Trojan and Exploit victim’s machine by taking its complete access

**Background Study:**

* Trojans are the malicious applications or programs which looks like a normal application but is harmful in nature as it can give the whole remote access of the Target's Machine to the Attacker's Machine.
* E.g. Poke and take remote control of your machine
* 2 ways of remote connection
  + Forward Connection
  + Reverse connection

**Code/steps**

**Output: Screenshots**

**Experiment No: 14**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third phase of penetration testing

**Program Outcome**

* The students will be able to gather the keystrokes of target machine

**Problem Statement**

* Track keystrokes of victim machine using Ardamax Keylogger

**Background Study:**

* Installed on a Victims computer.
* records these keystrokes and stores them in the logs.
* Starts operating in the background (stealth mode) and captures every keystroke of the target computer.
* silent, does not show up in the start-menu, windows startup, program files, add/remove programs or the task manager.

Ardamax Keylogger

* <https://www.ardamax.com/keylogger>
* Username: ardamax
* Password: ardamax
* After install you can delete but it is working (can check in task manager or triangle yellow icon on taskbar)
* **Open and view logs**
* It works on everything notepad, start, online accounts etc
* **Hidden mode:** attacker can hide also (right click)- ctrl + H
* **Invisibility option:** from task manager. It auto starts

**Code/steps**

**Output: Screenshots**

**Experiment No: 15**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third and Fourth phase of penetration testing

**Program Outcome**

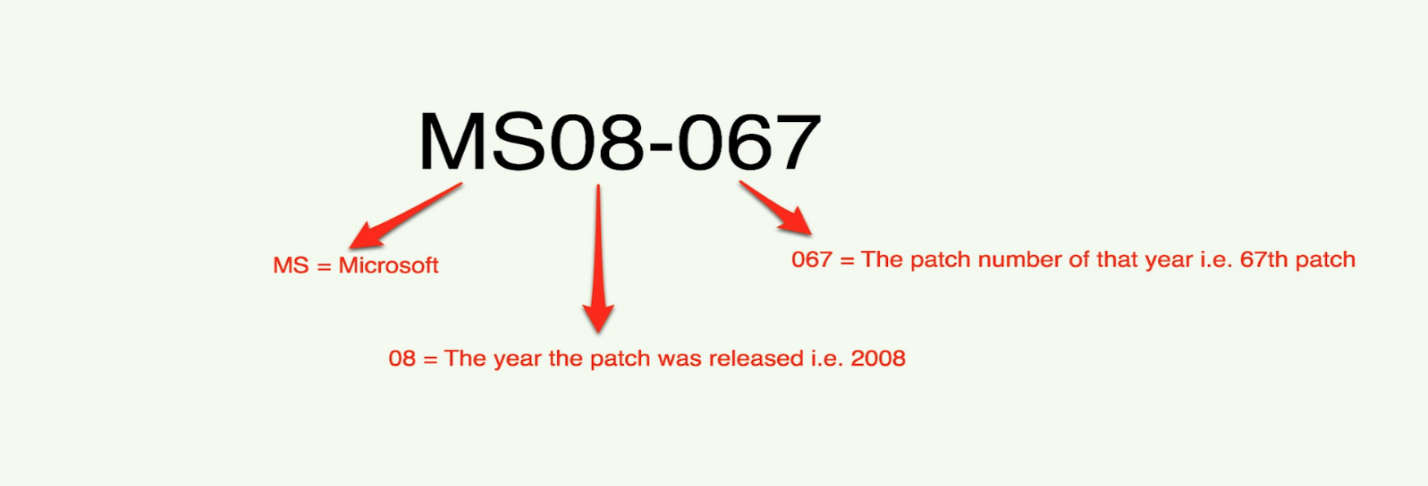
* The students will be able to gain and maintain access of the target machine

**Problem Statement**

* Exploit Windows XP with SP0 and SP1 using Metasploit

**Background Study:**

* Number of ways that you can bind your shell to a port
* There are two popular types of shells:
  1. Bind Shell and
  2. Reverse Shell
* A bind shell is the kind that opens up a new service on the victim machine and requires the attacker to connect to it in order to get a session.



**Code/steps**

**Output: Screenshots**

**Experiment No: 16**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third and Fourth phase of penetration testing

**Program Outcome**

* The students will be able to gain and maintain access of the target machine

**Problem Statement**

Exploit Windows7 using Metasploit

**Background Study:**

* **Exploit/multi/handler**
  + This module provides all of the features of the Metasploit payload system on different platforms and architectures.

**Code/steps**

**Output: Screenshots**

**Experiment No: 17**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third and Fourth phase of penetration testing

**Program Outcome**

* The students will be able to gain and maintain access of the target machine using the exploit

**Problem Statement**

Exploit Windows using Eternal Blue and Eternal Romance using Metasploit

**Background Study:**

* This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive.
* This will then be used to overwrite the connection session information with as an Administrator session.
* The normal psexec payload code execution is done.
* Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits.
* This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.

**Code/steps**

**Output: Screenshots**

**Experiment No: 18**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third and Fourth phase of penetration testing

**Program Outcome**

* The students will be able to gain and maintain access of the target machine using pdf file

**Problem Statement**

Exploitation by creating a payload in pdf File using Metasploit

**Background Study:**

* Infected PDFs have always been a privileged way to infect users because this document format is very common and used by almost everyone.
* It exists many ways to exploit Acrobat Reader vulnerabilities and it’s very stealth and elegant way to launch a malware.
* How easy it is to craft a malicious PDF with custom shellcode and trigger a vulnerability to execute a payload.
* Analyse the malicious PDF to learn how the payload is stored, and how to extract it.

**Code/steps**

**Output: Screenshots**

**Experiment No: 19**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Third and Fourth phase of penetration testing

**Program Outcome**

* The students will be able to gain and maintain access of the target machine

**Problem Statement**

Exploit windows using metasploitable2

**Background Study:**

Simple attack against the target Linux-based operating system Metasploitable2.

* It is available online at <http://sourceforge.net/projects/metasploitable/files/Metasploitable2>
* Metasploitable2 was designed to be vulnerable to attack.

**Code/steps**

**Output: Screenshots**

**Experiment No: 20**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Fifth phase of penetration testing

**Program Outcome**

* The students will be able to Cover tracks and post exploit the target machine

**Problem Statement**

Perform steps to remove the tracks in windows and kali Linux

**Background Study:**

* In the phases previous to this one the pen tester successfully managed to avoid detection by firewalls and intrusion detection systems,
* the purpose of this phase is to cover up all the little clues that would give away the nature of his deeds.
* There are few ways that we can cover our tracks, making it VERY difficult to track our malicious activities.
  + Clear the File, events logs or clear history
  + Hide the Files

**Code/steps**

**Output: Screenshots**

**Experiment No: 21**

Student Name and Roll Number:

Semester /Section:

Link to Code:

Date:

Faculty Signature:

Remarks:

**Objective**

To familiarize the students with the concept of Fifth phase of the penetration testing

**Program Outcome**

* The students will be able to understand how to delete or remove the data from the target machine after the exploitation

**Problem Statement**

Temper the time and date of the files to cover tracks

**Background Study:**

* All the traces of attack such as log files, intrusion detection system alarms are removed to cover the tracks.
* Removes all files and folders created, modify logs and registry once the hacker leaves the system.
* Using of reverse Http shells and ICMP tunnels also helps to cover tracks.

**Code/steps**

**Output: Screenshots**