Cyber Security

(CSL 422)

Lab Workbook

Faculty name:

Student name:

Roll No.:

Semester:

Group:

Department of Computer Science and Engineering

The NorthCap University, Gurugram- 122001, India

Session 2024-25

INDEX

S.No	Experiment	Page No.	Date of Experiment	Date of Submission	Marks	CO Covered	Sign
1	Perform reconnaissance to find all the relevant information on selected websites using 10 network information gathering tools.						
2	Gather information using Social Networking sites and google Dorks						
3	Perform Network Scanning using NMAP and ZENMAP						
4	Use Nessus tool to find all the vulnerabilities with its level and generate a report for an organization						
5	Install Wireshark and apply filters to gather different information Perform Session hijacking/ find credentials of unsecure real time website using Wireshark						
6	Create Trojan and Exploit victim's machine by taking its complete access						

7	Track keystrokes of victim machine using Keylogger						
8	Execute basic commands of Linux. Use CHMOD command to change the privileges and permissions Generate Word list from using wordlist generator ZAP						
9	Perform Windows Login Bypass in virtual machine						
10	Perform Kali Linux Login Bypass in virtual machine						
11	Exploit windows to gain access of victim's machine using Metasploit framework						
12	Exploit Windows 7 using Metasploit						

EXPERIMENT NO. 1

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective(s):

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

Outcome:

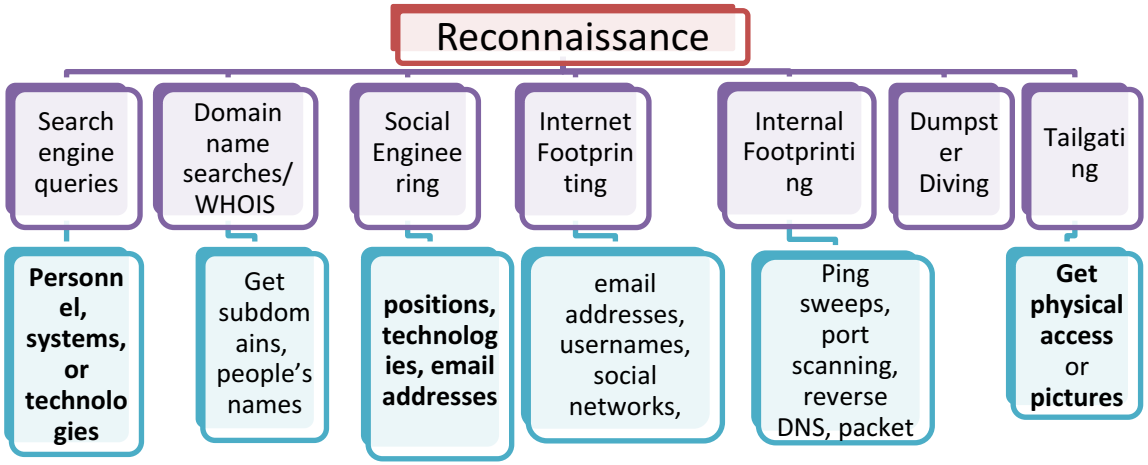
The students will understand which type of passive information can be gathered to exploit the target machine

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.



Question Bank:

1. In which topology there is a central controller or hub?
2. Which topology covers security, robust and eliminating traffic factor?
3. Video streaming is done through which protocol??
4. Which command is used to find the IP address of your system?
5. Why are systems vulnerable?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 2

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

Outcome:

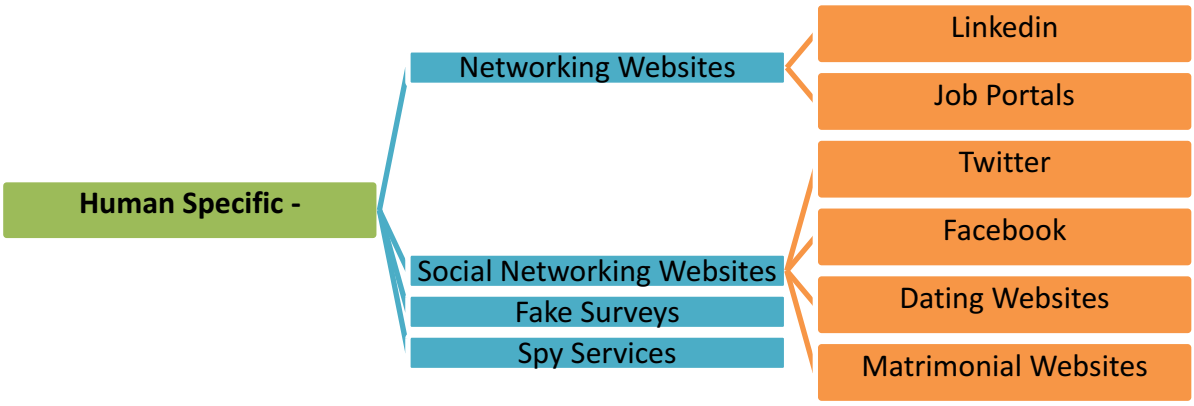
The students will understand how to gather information available on google freely using google dorks

Problem Statement:

Gather information using Social Networking sites and google Dorks

Background Study:

- D 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)

Question Bank:

1. What is digital footprinting?
2. How to use information from GHDB and FSDB?
3. Google search: Is it possible to search sites by value of tag attribute?
4. What Data Can We Find Using Google Dorks?
5. What is the following command used for: filetype:txt inurl:"email.txt" ?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 3

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

Outcome:

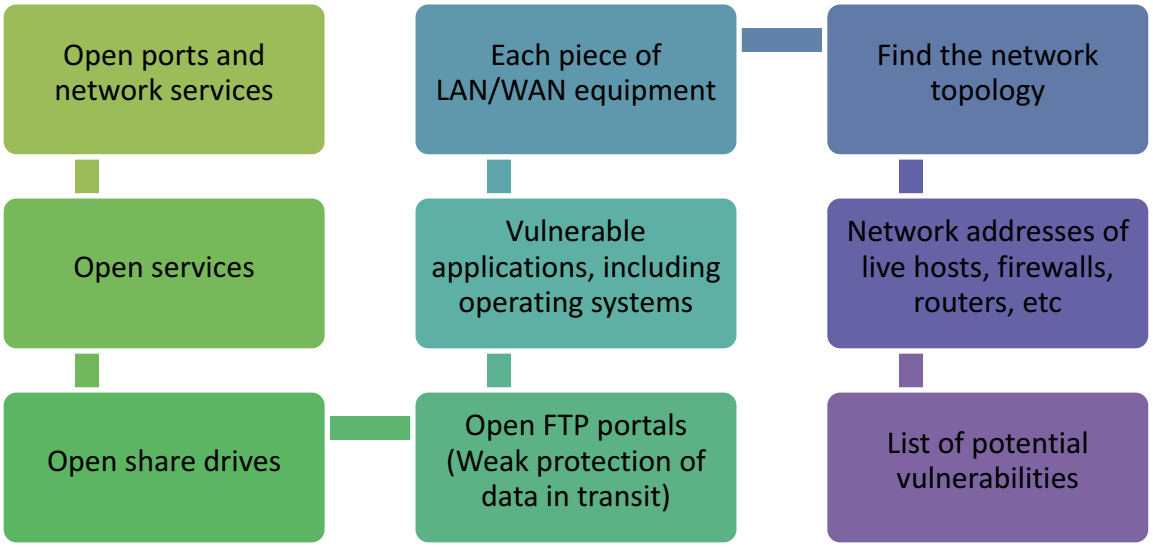
- The students will understand difference between active and passive reconnaissance.
- The students will be able to gather the information of the target machine by interacting with it.
- The students will understand Nmap Tool.

Problem Statement:

- Perform Network Scanning using NMAP and ZENMAP

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



Question Bank:

1. How to find the network addresses of live hosts, firewalls, routers, etc
2. In which phase where attacker will interact with the target with an aim to identify the vulnerabilities.
3. Differentiate between static and dynamic analysis.
4. Explain the different types of scanning.
5. Differentiate between filtered and unfiltered ports.

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 4

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

Outcome:

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

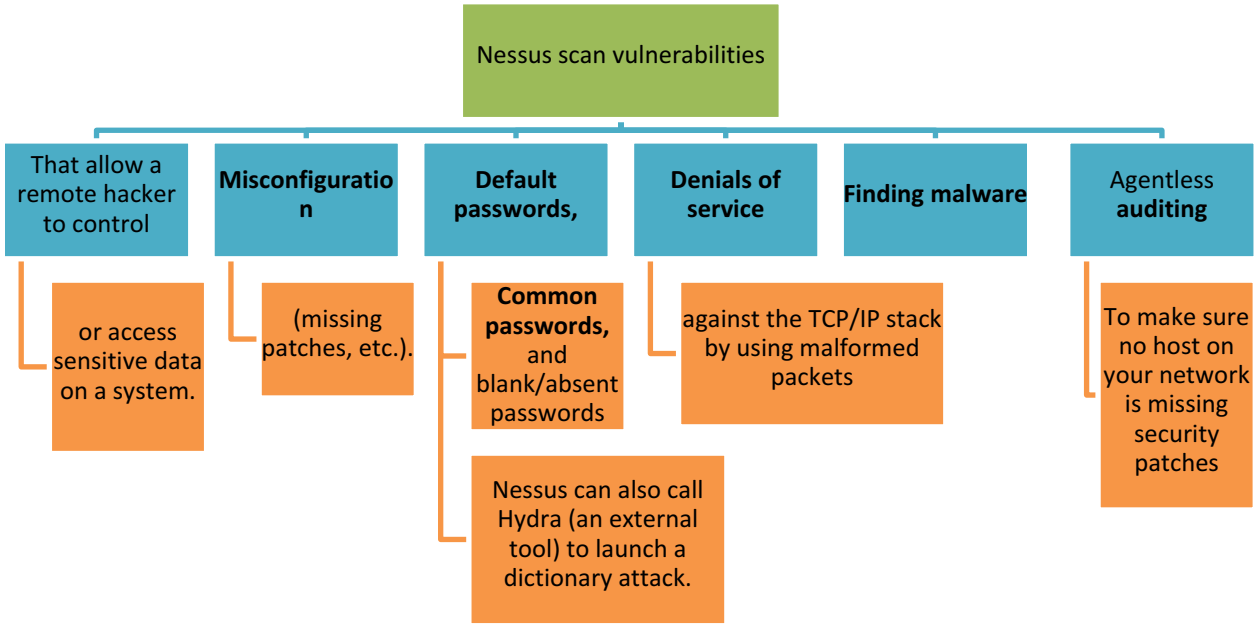
Problem Statement:

Use NIKTO & 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.



Question Bank:

1. What are the features of popular Vulnerability scanning tools?
2. Differentiate between NESSUS and NMAP.
3. List the top Vulnerability scanner tools.
4. List 4 applications of NESSUS tool.
5. What is a Plugin?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 5

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

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:

- Install Wireshark on any network and apply filters to gather different information of the target machine
- Perform Session hijacking/ find credentials of unsecure real time website 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.

Question Bank:

1. Differentiate between RST and FIN flag.
2. What information can be retrieved from a sniffer?
3. Is Wireshark an active or passive network scanning tool and why?
4. What is a pcap file?

5. How to combine filters in Wireshark to check the traffic from a particular IP and for http then.

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 6

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

To familiarize the students with the concept of exploitation

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
- ways of remote connection
    - Forward Connection
    - Reverse connection

Question Bank:

1. What are the different types of Exploitation.
2. Write a short note on RAT.
3. Differentiate between socket and stub.
4. Which folder is created when the victim click on a dark comet?
5. Find an application which can see the "Established" and "Listening" connection of a machine just like "netstat".

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 7

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

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

Question Bank:

1. Differentiate between software and hardware keyloggers.
2. What are the different methods of installing a keylogger?

3. List 5 open source keyloggers.
4. Can Ardamax keylogger record audio of a victim's machine?
5. What is the use of Crypter software?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 8

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

Outcome:

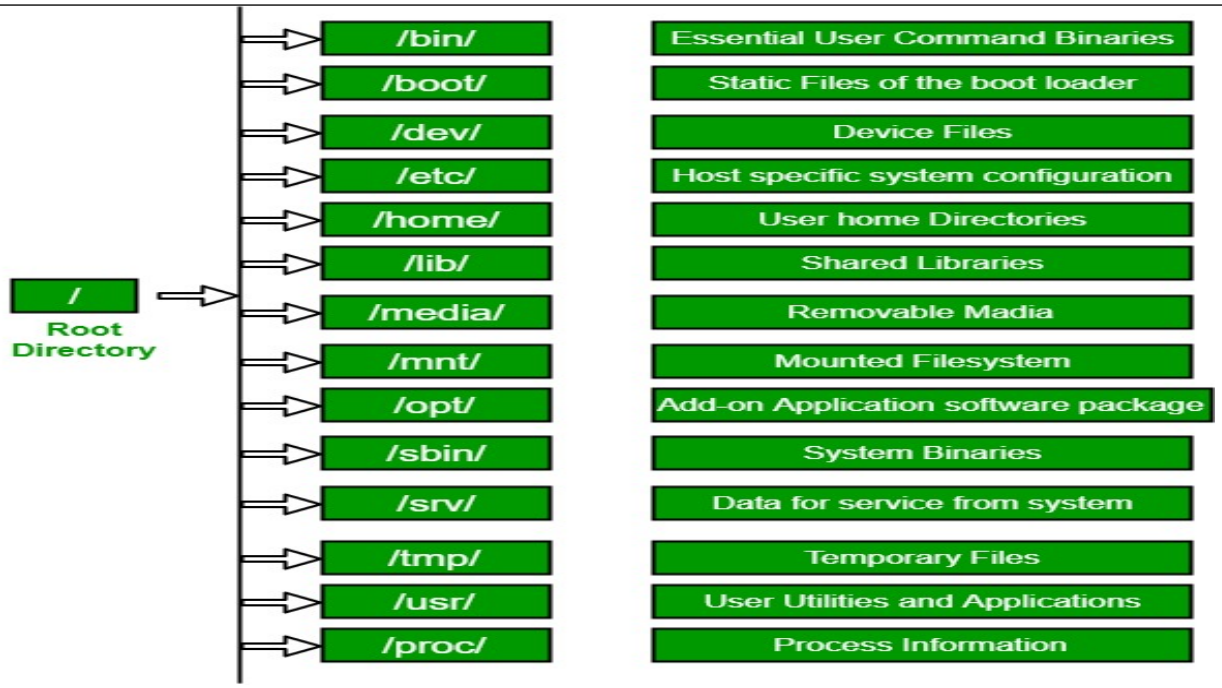
- The students will be able to learn commands of Linux required for exploitation
- Student will be able to change permissions of the Files and Folders

Problem Statement:

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

Background Study:

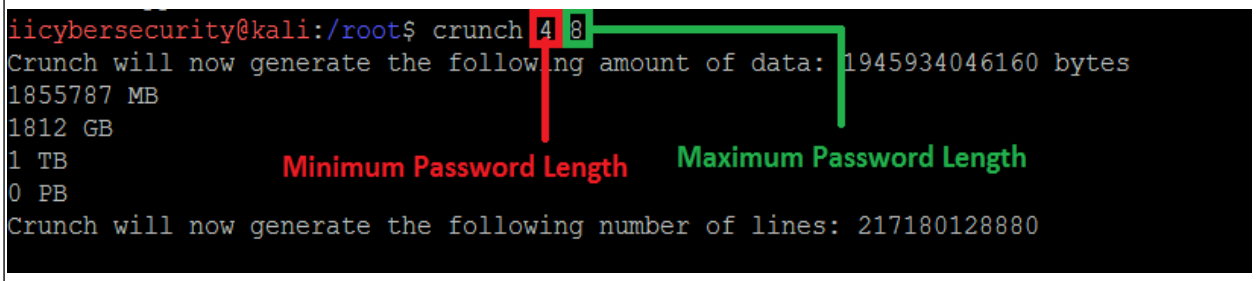
- Linux word derived and evolved from UNIX.
- Unix was the first operating system came to existence with CLI environment and mainly used for server side working as per today's requirements.
- It is the most flexible and customizable OS used by skilled individuals.
- It is an open source



Crunch Min.Value Max.Value Characters

Example –

crunch 4 4 0123456789



Question Bank:

1. Which command is used to make a directory in LINUX?
2. What is the use of grep command?
3. Which command is used to find out all the information about the OS?
4. Explain the following syntax: "chmod 754 filename".
5. Elaborate on the different privileges and permissions in LINUX.

Use **–b option** for wordlist fragmentation that split a single wordlist into multi wordlist

6. crunch 5 7 raj@123 -b 3mb -o START

   Crunch let you generate compress wordlist with **option –z** and other parameters are gzip, bzip2, lzma, and 7z

7. crunch 5 7 raj@123 –z gzip -o START

   -p option is used for generating wordlist with help of permutation, here can ignore min and max length of the character string

8. crunch 3 6 -p raj chandel hackingarticles
9. crunch 5 5 IGNITE -c 25 -o /root/Desktop/8.txt

   use –d option to set the filter for repetition.

10. crunch 6 6 -t raj%%% -d 2% -o /root/Desktop/6.1.txt

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 9

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

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 windows Login Bypass using netuser and John the Ripper Tool

Background Study:

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

Question Bank:

1. Which command is used to create new user after Windows Login bypass?
2. How to remove the password of a victim's Window machine?
3. How to change the password of a victim's Window machine?
4. What is the purpose of the following command: net user gg /delete
5. Write a short note on **RainbowCrack** tool.

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 10

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

Outcome:

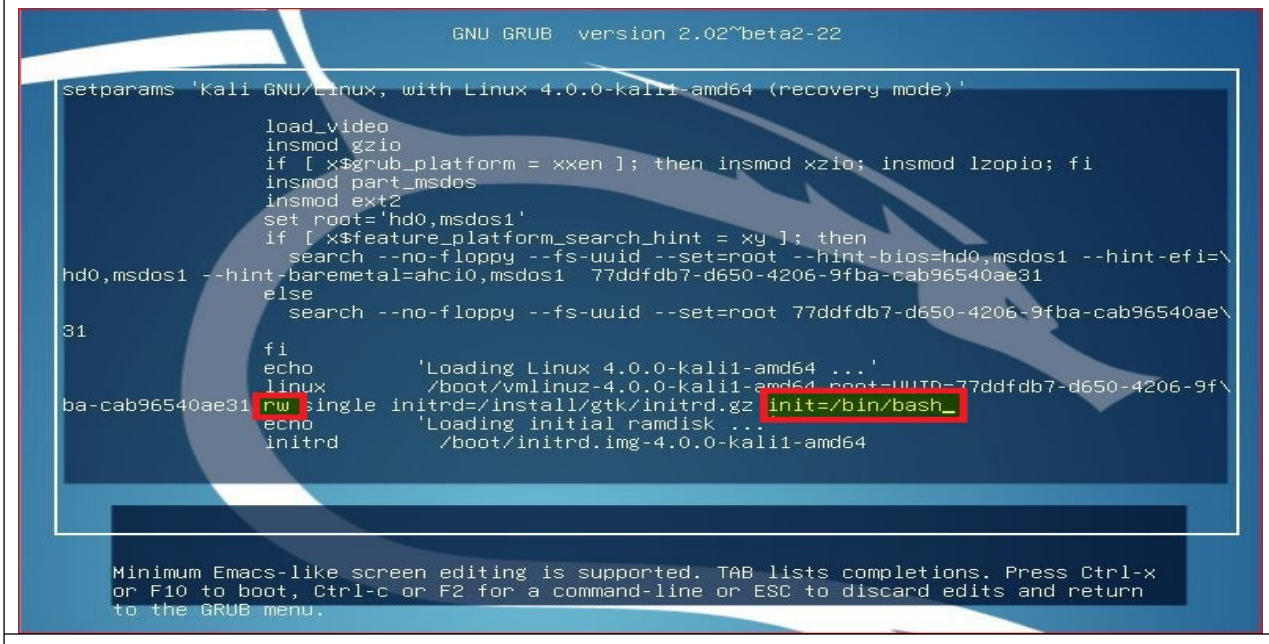
- The students will be able to Bypass the login details of target in active and passive mode on all type of operating system

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:



Question Bank:

1. Write a short note on **John the Ripper** tool.
2. Can **THC Hydra** tool be used for cracking LINUX machine password?
3. Which file allows the hacker to see user information such as full name, phone number etc. in LINUX?
4. Which permission value in LINUX allows to read and execute?
5. What is the UID of root user in LINUX?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 12

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective: To familiarize the students with the concept of Third and Fourth phase of penetration testing
Outcome: • The students will be able to gain and maintain access of the target machine using pdf file
Problem Statement: Exploit Windows to gain access of victim's machine using Metasploit framework
Background Study: • Exploit Windows 7 using Metasploit framework
Question Bank: 1. What are the different methods to gain access of a system? 2. Explain the functionality of Auxiliary modules in Metasploit. 3. What is the use of grep command in Metasploit? 4. Which command is used to set global variables within msfconsole? 5. How is reverse shell different from bind shell?

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 13

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective: To familiarize the students with the concept of Third and Fourth phase of penetration testing
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** o This module provides all of the features of the Metasploit payload system on different platforms and architectures.
Question Bank: 1. What is a meterpreter? 2. Explain the Msfvenom commands required to generate payload. 3. Write the command to start key scanner on victim's machine. 4. What is the output of following command - keyscan_dump. 5. Write the command to upload a file in window's F drive after getting meterpreter access.

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs

EXPERIMENT NO. 14 (VALUE ADDED EXPERIMENT)

Student Name and Roll Number:
Semester /Section:
Link to Code:
Date:
Faculty Signature:
Marks:

Objective:

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

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

Question Bank:

1. What is pivoting?
2. What is the use of getsystem command in Meterpreter script.
3. Write the command for taking screenshots of victim's machine after getting meterpreter access.
4. Write the command to clear event logs for clearing hacker's tracks.
5. What is the outcome of the follwoing command: **shred -zu root/.bash_history**

Student Work Area

Algorithm/Flowchart/Code/Sample Outputs