ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

(A Unit of Alva's Education Foundation)

MOODBIDRI , DAKSHINA KANNADA-574225

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(IoT & Cyber Security including Blockchain)

IV SEMESTER

NOTES

ON

CYBER SECURITY LAB

Subject Code:BICL404

UNDER THE GUIDANCE OF

Ms. K Swathi / Mr. Anveeksh Rao

2023-2024

Cyber Security lab		Semester	IV
Course Code	**BICL 404**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		

Course objectives:

- To get Practical exposure of Cyber security threats
- To get Practical exposure on Forensics Tools

Sl.NO	Experiments
1	Install Kali Linux and explore basic Linux commands and tools.
2	Perform basic network scanning using the Nmap tool (Zenmap on Windows). Identify services, open ports, active hosts, operating systems, and vulnerabilities.
3	Phishing simulations (Google, LUCY and GoPhish).
4	Packet analysis using Wireshark.
5	Ransomware tabletop exercise on insider threat.
6	Perform SQL injection using BurpSuite
7	Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram
8	Installation of rootkits and study about the variety of options
9	Perform an Experiment to Sniff Traffic using ARP Poisoning
10	Demonstrate intrusion detection system using snort

Course outcomes (Course Skill Set):

At the end of the course the student will be able to:

- Demonstrate the usage of tools to identify cyber threats/attacks
- Use Autopsy tools for digital forensic.
- Demonstrate Network analysis using Network miner tools.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

Continuous Internal Evaluation (CIE):

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.

- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.
- General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)
- Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.
- The minimum duration of SEE is 02 hours

Suggested Learning Resources:

- Real digital Forensics for Handheld Devices, E.P Dorothy, Auerback Publications, 2013
- The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012
- Handbook of Digital Forensics and Investigation, E. Casey , Academic Press, 2010
- Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C.H Malin, E. Casey and J M Aquilina, Syngress, 2012
- The Best Damn Cybercrime and digital forensics Book Period, J Wiles and A Reyes, Syngress, 2007

Experiment 1

Install Kali Linux and explore basic Linux commands and tools:

Objective:

The objective of this lab is to introduce students to Kali Linux, a powerful Linux distribution widely used for penetration testing, digital forensics, and security auditing. By the end of this lab, students should be familiar with the installation process of Kali Linux and have a basic understanding of Linux commands and tools.

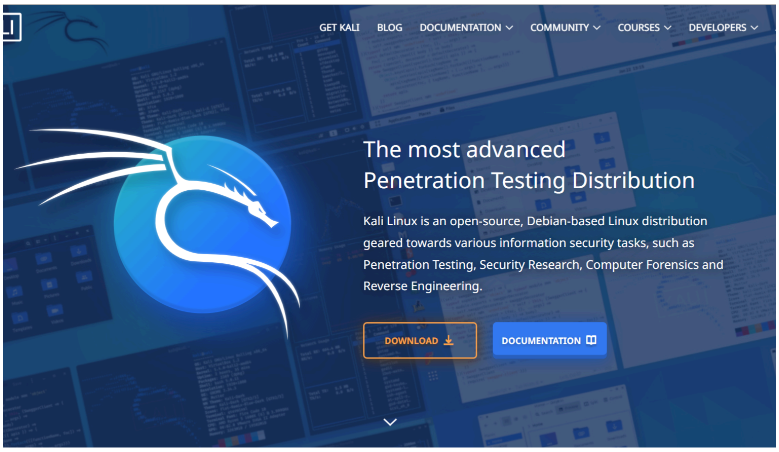
Materials Required:

1. A computer with at least 4GB of RAM and 20GB of free disk space
2. Kali Linux ISO file (available for download from the official Kali Linux website)
3. Virtualization software such as VirtualBox or VMware

Procedure:

Step 1: Download Kali Linux ISO:

- Visit the official Kali Linux website (https://www.kali.org/) and navigate to the "Downloads" section.
- Download the appropriate ISO image for your system (e.g., 64-bit ISO for most modern systems).

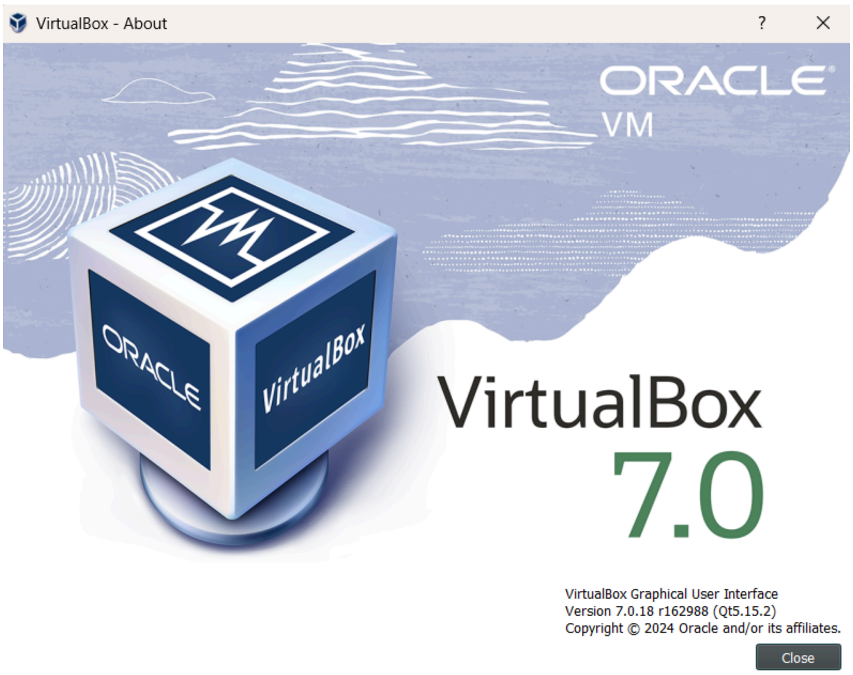


The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

Step 2: Install Virtualization Software:

- If not already installed, download and install virtualization software such as VirtualBox or VMware on your host machine.
- Follow the installation instructions provided by the virtualization software.



VirtualBox Graphical User Interface
Version 7.0.18 r162988 (Qt5.15.2)
Copyright © 2024 Oracle and/or its affiliates.

Step 3: Create a New Virtual Machine:

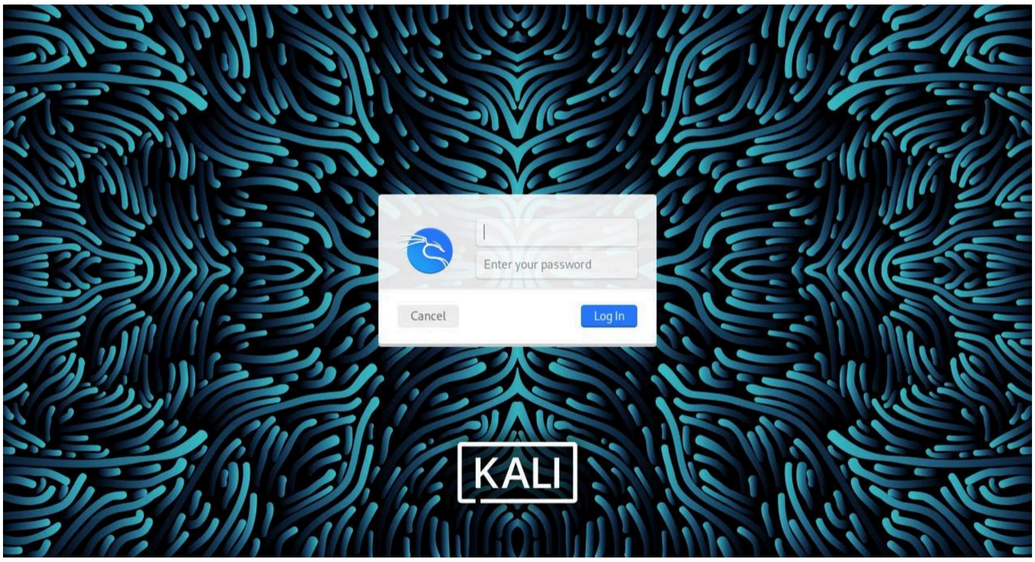
- Open VirtualBox or VMware and create a new virtual machine.
- Choose "Linux" as the operating system type and "Debian (64-bit)" as the version.
- Allocate at least 2GB of RAM and 20GB of disk space for the virtual machine.

Step 4: Install Kali Linux:

- Start the virtual machine and select the Kali Linux ISO file as the bootable media.
- Follow the on-screen instructions to install Kali Linux.
- Choose the appropriate options such as language, timezone, keyboard layout, and disk partitioning.
- Set up a username, password, and hostname for the Kali Linux installation.
- Wait for the installation process to complete.

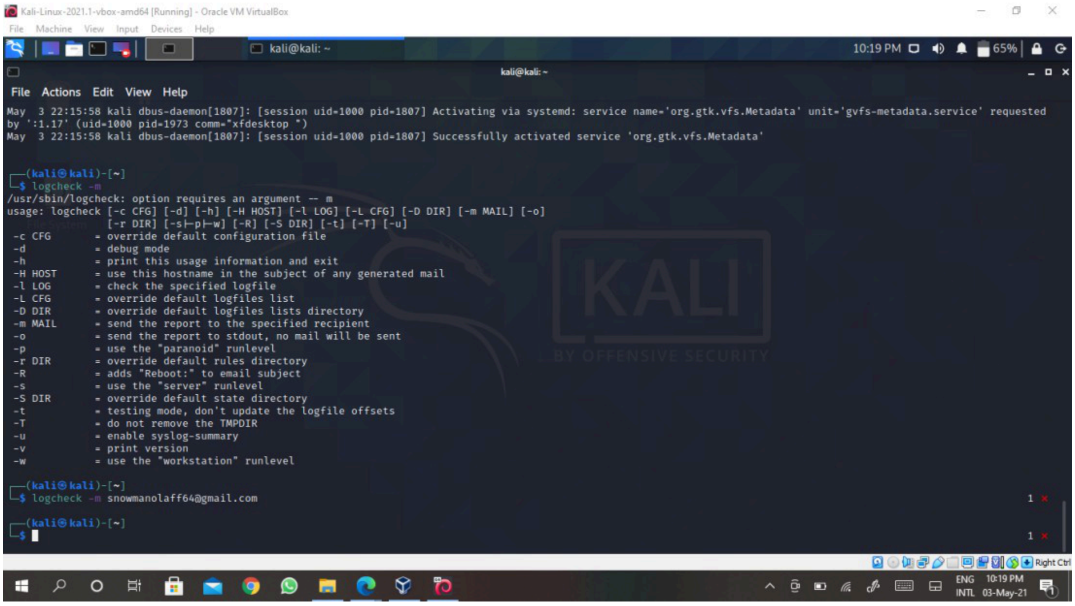
Step 5: Log in to Kali Linux:

- Once the installation is complete, restart the virtual machine.
- Log in using the username and password created during the installation process.



Step 6: Explore Basic Linux Commands and Tools:

- Once logged in, open the terminal emulator.
- Familiarize yourself with basic Linux commands such as **ls**, **cd**, **mkdir**, **rm**, **cp**, **mv**, etc.
- Explore system information commands like **uname**, **hostname**, **ifconfig**, **df**, **free**, etc.
- Experiment with package management commands such as **apt** or **apt-get** to install, update, and remove software packages.
- Discover some basic Kali Linux tools such as **nmap**, **metasploit**, **wireshark**, **hydra**, **john**, etc. (Note: Due to the nature of these tools, exercise caution and use them responsibly in a controlled environment.)


Kali-Linux-2021.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
10:19 PM
65%
kali@kali: ~
File Actions Edit View Help
Right Ctrl
ENG INTL 10:19 PM 03-May-21

```
May  3 22:15:58 kali dbus-daemon[1807]: [session uid=1000 pid=1807] Activating via systemd: service name='org.gtk.vfs.Metadata' unit='gvfs-metadata.service' requested
by ':1.17' (uid=1000 pid=1973 comm="xfdesktop ")
May  3 22:15:58 kali dbus-daemon[1807]: [session uid=1000 pid=1807] Successfully activated service 'org.gtk.vfs.Metadata'


┌──(kali㉿kali)-[~]
└─$ logcheck -m
/usr/sbin/logcheck: option requires an argument -- m
usage: logcheck [-c CFG] [-d] [-h] [-H HOST] [-l LOG] [-L CFG] [-D DIR] [-m MAIL] [-o]
                [-r DIR] [-s|-p|-w] [-R] [-S DIR] [-t] [-T] [-u]
 -c CFG       = override default configuration file
 -d           = debug mode
 -h           = print this usage information and exit
 -H HOST      = use this hostname in the subject of any generated mail
 -l LOG       = check the specified logfile
 -L CFG       = override default logfiles list
 -D DIR       = override default logfiles lists directory
 -m MAIL      = send the report to the specified recipient
 -o           = send the report to stdout, no mail will be sent
 -p           = use the "paranoid" runlevel
 -r DIR       = override default rules directory
 -R           = adds "Reboot:" to email subject
 -s           = use the "server" runlevel
 -S DIR       = override default state directory
 -t           = testing mode, don't update the logfile offsets
 -T           = do not remove the TMPDIR
 -u           = enable syslog-summary
 -v           = print version
 -w           = use the "workstation" runlevel

┌──(kali㉿kali)-[~]
└─$ logcheck -m snowmanolaff64@gmail.com                                          1 ×

┌──(kali㉿kali)-[~]
└─$ █                                                                             1 ×
```

Step 7: Conclusion:

- Congratulations! You have successfully installed Kali Linux and explored basic Linux commands and tools.
- Experiment further with the Linux environment and tools to deepen your understanding and proficiency.

Safety Precautions:

- Use Kali Linux and its tools responsibly and legally.
- Exercise caution when running commands or using tools that could potentially harm systems or networks.
- Ensure that you are using Kali Linux in a controlled environment, such as a virtual machine, for educational purposes only.

Note: This lab manual is intended for educational purposes only. It is important to respect the laws and regulations governing the use of penetration testing tools and techniques.

BASIC COMMANDS IN LINUX :

- **date :** Display the current date and time in Linux.
- **cal :** Shows current month calendar as output.
- **pwd:** Displays the current directory. The current directory is nothing but the directory in which you are currently operating.
- **whoami:** command used to identify the current logged in user. clear : clear the terminal.
- **ls:** command to list computer files.
- **mkdir:** Command allows the user to create directories.
- **cd :** command used to change the current working directory.
- **touch :** Create an empty file.
- **nano:** It is a text editor. Nano text editor is used to create and edit files, included in most Linux distributions.
- **vi:** vi is one of the most commonly used editor program and included by default with every UNIX and linux system.
- **vim:** It is a text editor. Vim is an improved version of the vi editor. cat: It prints the content of a file.
- **head:** By default, without any option, the head command will display the first 10 lines from the file.

- **tail:** By default, it displays the last ten lines of a file.
- **wc:** wc stands for word count. It is used to find out number of lines, word count, byte and characters count in the files specified in the file arguments.
- **man:** It provides a detailed view of the command which includes NAME, SYNOPSIS, DESCRIPTION, OPTIONS, EXIT STATUS, RETURN VALUES, ERRORS, FILES, VERSIONS, EXAMPLES and AUTHORS.
- **pinfo:** Pinfo is an info file viewer or a script for viewing info files.
- **find:** find is a command-line utility that locates files based on some user-specified criteria.
- **history:** history command in Linux is a utility with the purpose of keeping track of previously used commands in the command line. cp: The cp command has a simple purpose to copy files and folders from one place to another.
- **mv:** mv stands for move and is essentially used for moving files or directories from one location to another.
- **rm:** The rm command is used to remove files and directories in Linux.
- **reboot:** reboot command is used restart or reboot the system. shutdown: The shutdown command in Linux is used to power down the system in a safe way

Experiment 2

Perform basic network scanning using the Nmap tool (Zenmap on Windows). Identify services, open ports,active hosts, operating systems, and vulnerabilities.

Objective: To perform basic network scanning using the Nmap tool (Zenmap on Windows) to identify services, open ports, active hosts, operating systems, and vulnerabilities.

Equipment Required:

1. Computer with Nmap tool installed (Zenmap for Windows users)
2. Access to a network (either local or remote) for scanning

Procedure:

1. Launch Nmap/Zenmap:
    - Open the Nmap application or Zenmap if you are using Windows.
    - If Nmap is not installed, download and install it from the official website.
2. Identify Target Network:
    - Determine the target network you wish to scan. This could be a local network or a remote network.
3. Choose Scan Type:
    - Select the appropriate scan type based on your objectives. Common scan types include:
        - Quick Scan (Scan the most common 1,000 ports)
        - Full TCP Scan (Scan all TCP ports)
        - Intense Scan (Scan top 1000 ports with OS detection and version detection)
        - Custom Scan (Specify ports, timing options, etc.)
4. Specify Target(s):
    - Enter the IP address range or hostname of the target network. For example:

      For Example 192.168.1.1-255

    - You can also specify individual IP addresses or subnets.
5. Initiate Scan:
    - Click on the "Scan" button to initiate the scan process.

  - Depending on the scan type and network size, the scan may take some time to complete. Be patient.

6. Review Results:
    - Once the scan is complete, review the results displayed by Nmap/Zenmap.
    - Look for information such as:
        - Open ports: Ports that are accessible and can potentially be used to access services.
        - Active hosts: Devices that are online and responsive on the network.
        - Services: Information about the services running on each open port.
        - Operating systems: Nmap/Zenmap may attempt to identify the operating system of each host.
        - Vulnerabilities: Nmap/Zenmap may detect known vulnerabilities in services or operating systems.
7. Interpret Results:
    - Analyze the results to understand the network topology, identify potential security risks, and gather information about the network and its devices.
8. Document Findings:
    - Document your findings in a clear and organized manner. Include details such as IP addresses, open ports, identified services, operating systems, and any vulnerabilities discovered.

Safety Precautions:

- Ensure that you have proper authorization before scanning any network.
- Avoid performing scans on networks or devices without permission, as it may violate ethical and legal guidelines.

Conclusion:

Congratulations! You have successfully performed basic network scanning using the Nmap tool (Zenmap on Windows). By analyzing the results, you gained valuable insights into the target network's topology, services, operating systems, and potential vulnerabilities.