SRI SIDDARTHA ACADEMY OF HIGHER EDUCATION

((Declared as Deemed to be University Under Section 3 of the UGC Act, 1956

Approved by AICTE, Accredited by NBA, NAAC 'A+' Grade)

AGALKOTE, TUMKURU-572107 KARNATAKA

Project Final Report On:

"HOW TO USE KALI LINUX FOR ETHICAL HACKING"

Submitted by

MOHAMMED MARDAN ALI	(21CS055)
NAMITH A	(21CS060)

in partial fulfillment of

BACHELOR OF ENGINEERING

in

Computer Science

DEPARTMENT OF COMPUTER SCIENCE ENGINEERINGS

SRI SIDDHARTHA INSTITUTE OF TECHNOLOGY

(A Constituent College of Sri Siddhartha Academy of Higher Education)

MARALUR, TUMKUR-572105 (2023-24)

SRI SIDDHARTHA INSTITUTE OF TECHNOLOGY,

TUMAKURU-572105

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the mini project work entitled ““HOW TO USE KALI LINUX FOR ETHICAL HACKING” is a bonafide work being carried out by MOHAMMED MARDAN ALI (21CS055), NAMITH A (21CS060) in partial fulfillment for the completion of VI Semester of Bachelor of Engineering in Department of Computer Science & Engineering from Sri Siddhartha Institute of Technology,A Constitute College of Sri Siddartha Academy of Higher Education during the academic year 2023-24. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the department library. The mini Project report has been approved as it satisfies the academic requirements in respect of mini project work prescribed for the Bachelor of Engineering degree.

11/7/24

Signature of the Guide
VEENA N D
Professor, Dept of CSE

Signature of the HOD
DR.RENUKALATHA S
Professor & Head, Dept of CSE

Names of the Examiners **Signature with date**

1. Dr. M Siddappa
2. Sowmyara.A

DECLARATION

MOHAMMED MARDAN ALI(21CS055) and **NAMITH A(21CS060)** of Sixth Semester, Department of Computer Science and Engineering of Sri Siddhartha Institute of Technology, Tumakuru, hereby declare that this Mini project titled, “HOW TO USE KALI LINUX FOR ETHICAL HACKING”, has been carried out by us under the supervision of VEENA N D Professor ,Department of CSE, Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru in partial fulfilment of the requirement for the completion of VI semester in Computer Science and Engineering.

MOHAMMED MARDAN ALI	(21CS055)
NAMITH A	(21CS060)

Contents

Abstract

Kali Linux, a Debian-based distribution, is the preferred choice for cybersecurity professionals, ethical hackers, and penetration testers. It is renowned for its extensive collection of tools specifically tailored for security testing, vulnerability analysis, and network examination. This powerful operating system offers over 600 tools, including Nmap for network mapping, Metasploit for exploitation, and Aircrack-ng for Wi-Fi security analysis, making it an indispensable toolkit for professionals in the field. Kali Linux is not only a resource for conducting security assessments but also serves as an educational platform for those looking to enter the cybersecurity domain. Its open-source nature allows for community-driven development and contribution, ensuring that it remains at the forefront of cybersecurity tools. Whether for professional use or educational purposes, Kali Linux stands out as a comprehensive solution for anyone serious about understanding and improving network security

Chapter 1

Introduction

Kali Linux, a powerful and versatile operating system, has gained immense popularity among ethical hackers, penetration testers, and security professionals. In this paper, we explore the fundamentals of Kali Linux, its development history, and its role in ethical hacking. We delve into the reasons why Kali Linux is the go-to choice for security experts and discuss its extensive toolkit. Additionally, we demonstrate the usage of some essential tools within Kali Linux for various hacking scenarios.

1. What is Kali Linux? Kali Linux is a Debian-based Linux distribution specifically designed for network analysts, penetration testers, and security researchers. It provides a comprehensive set of tools for ethical hacking, vulnerability assessment, and penetration testing. Unlike general-purpose Linux distributions, Kali Linux comes pre-installed with over 600 specialized tools, making it an indispensable resource for security professionals.

2. Development of Kali Linux Mati Aharoni and Devon Kearns are the core developers behind Kali Linux. It evolved from BackTrack Linux, another penetration testing-centric distribution. The development process adheres to Debian standards, with most of the code imported from Debian repositories. Kali Linux was officially released in 2013 and has since undergone several major updates.

3. Why Use Kali Linux? Several compelling reasons make Kali Linux the preferred choice for ethical hacking:

1. Free and Open Source Kali Linux is free to use and follows the open-source model. Its development tree is publicly viewable on Git, allowing users to customize and contribute to the codebase.

2. Extensive Toolkit Kali Linux includes over 600 pre-installed penetration testing and security analytics tools. These tools cover various aspects of security testing, including

network scanning, vulnerability assessment, password cracking, and forensics.

3. Multilingual Support Kali Linux ensures true multilingual support, allowing users to operate in their native language and access the necessary tools for their tasks.

Chapter 2

Literature Survey

Kali Linux is widely used by professionals and companies for cybersecurity purposes. Here are some examples:

1. AuraSec GmbH: A German company specializing in information technology and services1.

2. Institute of Data: An Australian educational institution focusing on data science and cybersecurity1.

3. Harbor Labs: A U.S.-based company providing IT and security services1. Millennium Corporation: An American company offering IT and cybersecurity solutions1.

4. Thentia: A Canadian firm specializing in regulatory and compliance software1. RSM US LLP: One of the largest accounting firms in the United States, providing various services including cybersecurity1.

5. X8 LLC: A U.S. defense and space company1.

6. Aerstone: An American IT service provider known for its cybersecurity expertise1.

7. TIME Systems: A U.S. management consulting firm with a focus on IT solutions1

. 8. GreyCastle Security: A U.S. company specializing in computer and network security1

. 9. ValueMentor: A cybersecurity company based in the United Arab Emirates1. Office of Management and Enterprise

10. Services: A U.S. government administration entity that utilizes Kali Linux for various security tasks

Chapter 3

Existing System

1. Nmap (Network Mapper): Nmap is a powerful network scanner used for host discovery, OS detection, and port scanning. It provides insights into hosts, open ports, and services running on a network.

2. Burp Suite: Burp Suite is a web application security testing tool. It acts as a proxy, allowing users to intercept and modify requests. Security professionals use it for testing vulnerabilities like XSS and SQL injection.

3. Wireshark: Wireshark is a network protocol analyzer that captures and analyzes network traffic. It helps identify security issues, monitor network behavior, and troubleshoot network problems.

4. Metasploit Framework: Metasploit is a powerful framework for developing, testing, and executing exploits. It simplifies penetration testing by providing a wide range of pre-built exploits and payloads.

5. Aircrack-ng: Aircrack-ng is a collection of tools for assessing Wi-Fi network security. It includes features for monitoring, compromising networks (WEP, WPA, WPA2), and recovering Wi-Fi passwords.

6.Seeker: Seeker is a collection of tools for accessing a phone location.It includes featues like phone location ,service provider,ip adress and location pinned at google maps.

7.John the ripper: It is the tool used for crackinh hash passwords that are very difficult to crack and is one of the best tool.

Chapter 4

Requirements

4.0.1 Hardware Requirements

1.Laptop or PC system with intel core i3 or AMD E1 processor for good performance.

2.A minimum 20GB space in the system hard disk for installation.

3.A bootable USB or CD-DVD to flash the drive with kali iso file.

4.0.2 Software Requirements

1.Latest version of Kali linux provided in https://kali.org/get-kali is an open website with different versions of kali linux for laptop,virtualbox,rasberry-pie and mobile phoens.

2.For hacking we need to install any seeker and ngrok as they are not pre installed with the kali linux.

Chapter 5

Hacking

5.0.1 Seeker

It is mainly used for tracking a phone location.It has various interfaces for phone tracking:

1.Near you

2.Whatsapp

3.Telegram

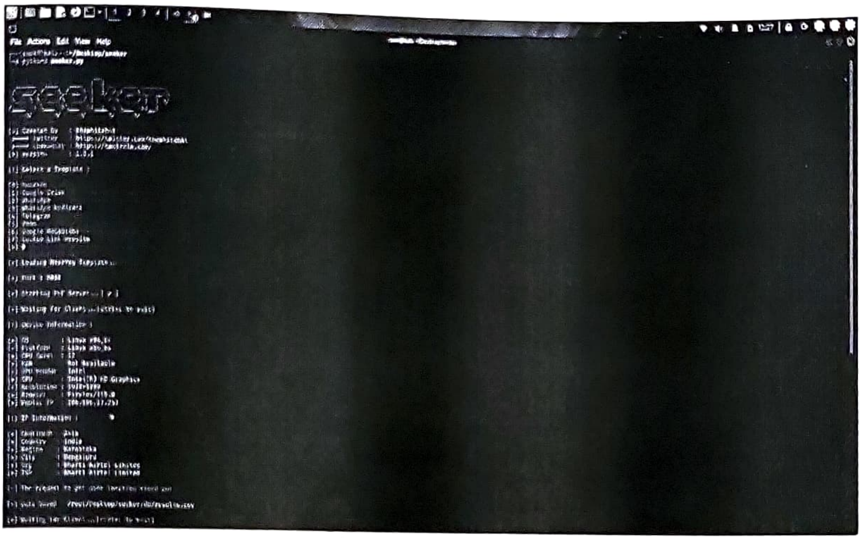
4.Whatsapp Redirect

5.Google drive

6.Google Recaptcha

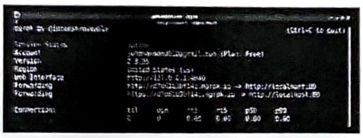
7.Custom links

We will be using the first method for phone tracking,as it is easy to apply and accurate.



```
File Actions Edit View Help
[illegible] ~/Desktop/seeker
python3 seeker.py

[+] Created By   : thewhiteh4t
 |---> Twitter   : https://twitter.com/thewhiteh4t
 |---> Community : https://twc1rcle.com/
[>] Version      : 1.3.1

[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] WhatsApp Redirect
[4] Telegram
[5] Zoom
[6] Google Recaptcha
[7] Custom Link Preview
[>] 0

[+] Loading NearYou Template...

[+] Port : 8080

[+] Starting PHP Server......[ ✓ ]

[+] Waiting for Client...[ctrl+c to exit]

[!] Device Information :

[+] OS         : Linux x86_64
[+] Platform   : Linux x86_64
[+] CPU Cores  : 12
[+] RAM        : Not Available
[+] GPU Vendor : Intel
[+] GPU        : Intel(R) HD Graphics
[+] Resolution : 1920x1080
[+] Browser    : Firefox/115.0
[+] Public IP  : 106.195.17.251

[!] IP Information :

[+] Continent : Asia
[+] Country   : India
[+] Region    : Karnataka
[+] City      : Bengaluru
[+] Org       : Bharti Airtel Limited
[+] ISP       : Bharti Airtel Limited

[-] The request to get your location timed out

[+] Data Saved : /root/Desktop/seeker/db/results.csv

[+] Waiting for Client...[ctrl+c to exit]
```

We will also need to host the network and control traffic so we have used ngrok.



```
ngrok by @inconshreveable                                   (Ctrl+C to quit)

Session Status        online
Account               [illegible] (Plan: Free)
Version               2.3.35
Region                United States (us)
Web Interface         http://127.0.0.1:4040
Forwarding            http://[illegible].ngrok.io -> http://localhost:80
Forwarding            https://[illegible].ngrok.io -> http://localhost:80

Connections           ttl     opn     rt1     rt5     p50     p90
                      0       0       0.00    0.00    0.00    0.00
```

Step 1:We need to open the terminal where the seeker folder is located.

Step 2:We have to run the seeker.py file with python3 command, by which the seeker interface is displayed with options.

Step 3:Select the option 0 that is Near you option.

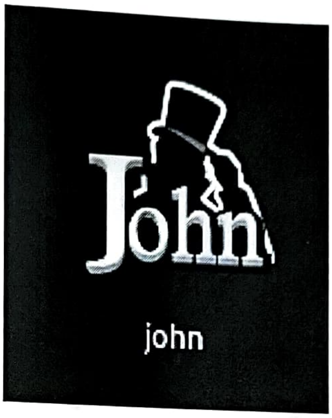
Step 4:It automatically generates the link and the port number.

Step 5:As the port number is visible but the link is not visible, for open a new a new terminal and run "ngrok http 8080" by the ngrok starts to monitor the web interface. The link is present in the forwarding row.

Step 6:Send the link to the target via whatsapp or telegram.

5.0.2 Linux password cracking

As all the passwords of linux are stored in shadows folder and are hash format we will be using john the ripper for cracking the password.

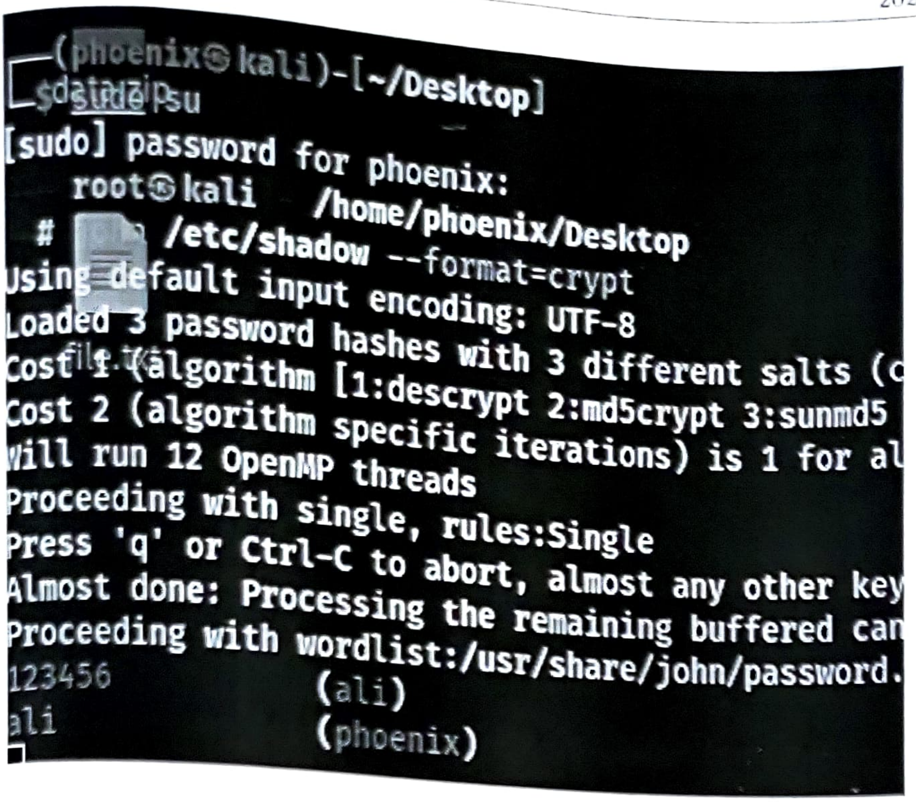


john the ripper has its very own password file using which it cracks the password.If the password is present in the file it is good to go or it cannot crack the password.We will be now performing the cracking the password using John.

Step 1:We will be opening the terminal with root id as sudo su.

Step 2:We will specifying the location of shadow file with john command as john location.

Step 3:After hitting the enter button we will be now getting the passwords with the user name of the kali linux users.



```
┌──(phoenix㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for phoenix:
    root㉿kali   /home/phoenix/Desktop
  # [illegible] /etc/shadow --format=crypt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (c
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5
Cost 2 (algorithm specific iterations) is 1 for al
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key
Almost done: Processing the remaining buffered can
Proceeding with wordlist:/usr/share/john/password.
123456           (ali)
ali              (phoenix)
```

Chapter 6

Conclusion

In conclusion, Kali Linux stands as a pivotal asset in the realm of ethical hacking, providing an arsenal of specialized tools that cater to various aspects of cybersecurity. Its comprehensive suite of applications enables ethical hackers to conduct thorough penetration tests, vulnerability assessments, and security audits. Kali Linux's commitment to the open-source community and its continuous evolution with the cybersecurity landscape ensures that it remains an invaluable resource for professionals and enthusiasts alike. By leveraging Kali Linux, ethical hackers can simulate sophisticated cyber attacks, identify system vulnerabilities, and implement robust security measures to protect against malicious threats. It is a testament to the power of open-source software in advancing the field of information security and fostering a proactive approach to digital defense. Whether for educational purposes or professional deployments, Kali Linux is a testament to the synergy between technology and expertise in securing our digital world.

Chapter 7

References

1.YouTube contains many videos and courses for the topic and many you tubers are certified hackers who teach about cyber security and ethical hacking.

2.Infosys learning app provides free courses for students who are interested in learning about cybersecurity and ethical hacking.