

**EVALUATION OF INTERNSHIP REPORT**

## B.TECH: III Year

**Department of Computer Science & Information Technology**

**Name of the Student: KRATIK PANDEY**

**Branch & section: CSIT 2**

**Roll No: 0827CI201095**

**Year: 2022**

## Department of Computer Science & Information Technology

**AITR, Indore**

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**Certificate**

Certified that training work entitled “*Cyber security*” is a bonafied work carried out in fifth semester by “*KRATIK PANDEY*” in partial fulfillment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from “*Prof. Nidhi Nigam /Assistant professor CSIT department”* of Acropolis Institute of Technology and Research during the academic year 2022-23.

*Prof. Praveen Gupta Prof. Nidhi Nigam*

**ACKNOWLEDGEMENT**

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training "Prof. Nidhi Nigam /Assistant professor CSIT department”, CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

*KRATIK PANDEY*

*0827CI201095*

### ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

### INDEX

S.no CONTENTS

1. Introduction to technology Undertaken

2. Objectives

3. Project undertaken

4. Screenshots of Project

5. Conclusion

6 References

**Cyber Security Introduction - Cyber Security Basics:**

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing.  Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms  whether IT or non-IT firms have understood the importance of Cyber Security and focusing  on adopting all possible measures to deal with cyber threats.

**What is cyber security?**

"Cyber security is primarily about people, processes, and technologies working together to  encompass the full range of threat reduction, vulnerability reduction, deterrence, international  engagement, incident response, resiliency, and recovery policies and activities, including  computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect  networks, computers, programs and data from attack, damage or unauthorized access.

∙ The term cyber security refers to techniques and practices designed to protect digital  data.

∙ The data that is stored, transmitted or used on an information system.

**Why is cyber security important?**

Listed below are the reasons why cyber security is so important in what’s become a  predominant digital world:

∙ Cyber-attacks can be extremely expensive for businesses to endure.

∙ In addition to financial damage suffered by the business, a data breach can also inflict  untold reputational damage.

∙ Cyber-attacks these days are becoming progressively destructive. Cybercriminals are  using more sophisticated ways to initiate cyber-attacks.

**Cyber security Fundamentals – Confidentiality:**

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding  data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle  (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

∙ Data encryption

∙ Two-factor authentication

∙ Biometric verification

∙ Security tokens

**Integrity**

Integrity refers to protecting information from being modified by unauthorized parties. Standard measures to guarantee integrity include:

∙ Cryptographic checksums

∙ Using file permissions

∙ Uninterrupted power supplies

∙ Data backups

**Availability**

Availability is making sure that authorized parties are able to access the information when needed. Standard measures to guarantee availability include:

∙ backing up data to external drives

∙ implementing firewalls

∙ having backup power supplies

∙ Data redundancy

.

.

.

**Types of Cyber Attacks**

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

1. **Web-based attacks**

**2) System-based attacks**

**Web-based attacks**

These are the attacks which occur on a website or web applications. Some of the important  web-based attacks are as follows

**1. Injection attacks**

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

**Example-** SQL Injection, code Injection, log Injection, XML Injection etc. **2. DNS Spoofing**

DNS spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

**3. Session Hijacking**

It is a security attack on a user session over a protected network. Web applications create  cookies to store the state and user sessions. By stealing the cookies, an attacker can have  access to all of the user data.

**4. Phishing**

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

**5. Brute force**

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

**System-based attacks**

These are the attacks which are intended to compromise a computer or a computer network.  Some of the important system-based attacks are as follows

**1. Virus**

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of it into other computer programs when executed. It can also execute instructions that cause harm to the system.

**2. Worm**

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

**3. Trojan horse**

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

**4. Backdoors**

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

**5. Bots**

A bot (short for "robot") is an automated process that interacts with other network services.  Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

**PROJECT UNDERTAKEN:**

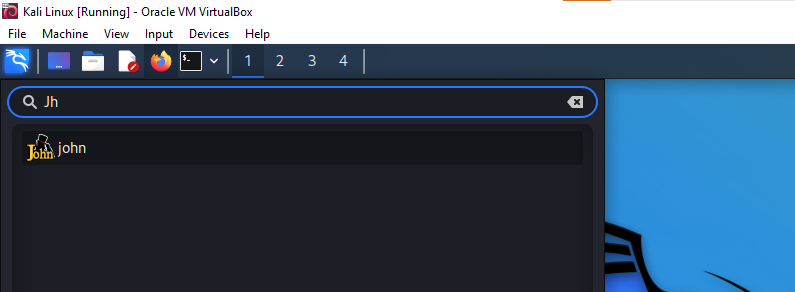
**The aim of this project is Password Cracking tool (John the ripper),** Basically **John the ripper** is software in Kali Linux that cracks the password of types of flies for example rar ,zip ,txt etc .Depending upon the type of password the tool works accordingly and it can even crack tough password but it requires time to crack it.

# About John The Ripper:

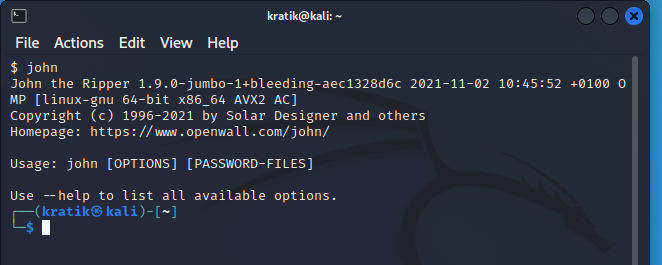
John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. **John the Ripper jumbo** supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, \*BSD, Solaris, AIX, QNX, etc.), One of the modes John can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

**Implementation:**

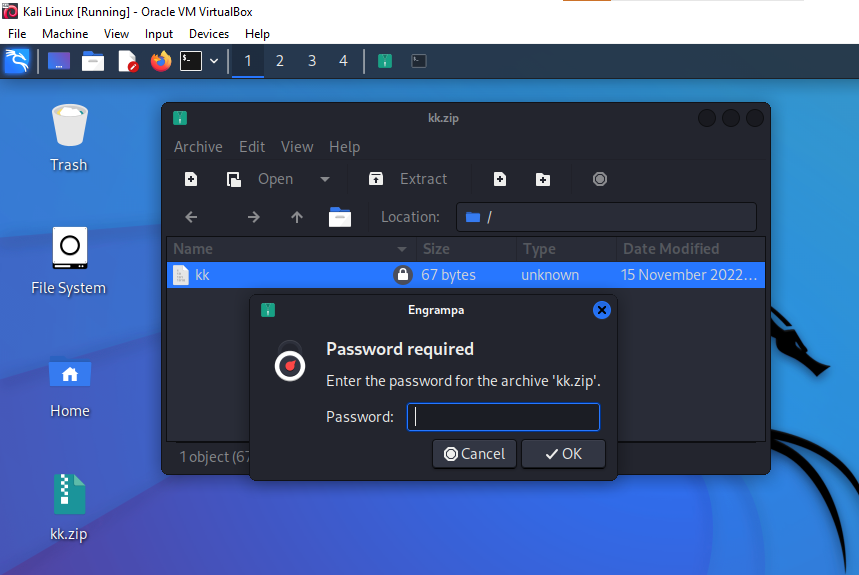
Here, we will use (Oracle Vm Virtual Box) Kali Linux and in kali linux the tool John the ripper is pre installed so we do not need to install it but it can easily be installed in the other devices too.

****

So this is the interface of the John the ripper password cracking tool and so through this we will be able to crack the password of the file. John the ripper uses password # to find out the password.



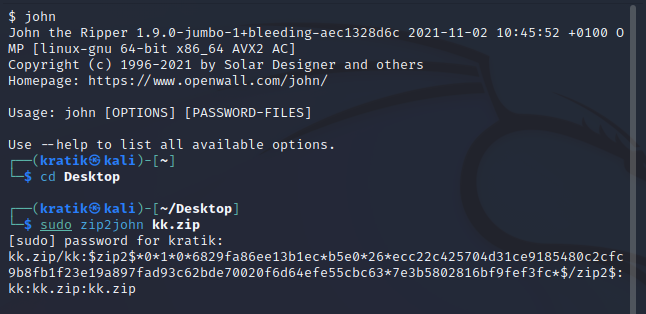
And then we will create a ZIP FILE and that will be a password protected file



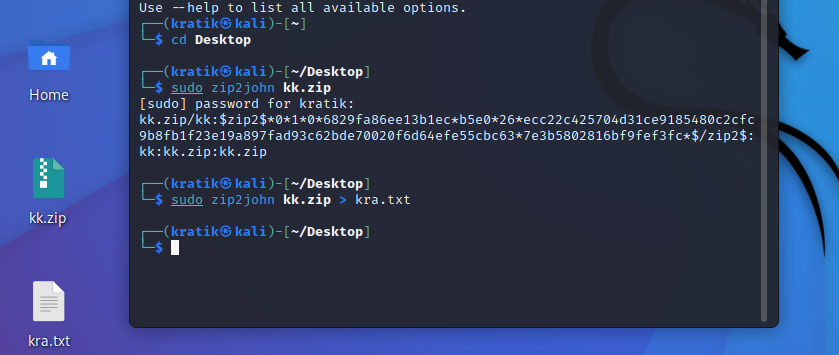
**PROJECT SCREENSHOTS**

**PROCESS**

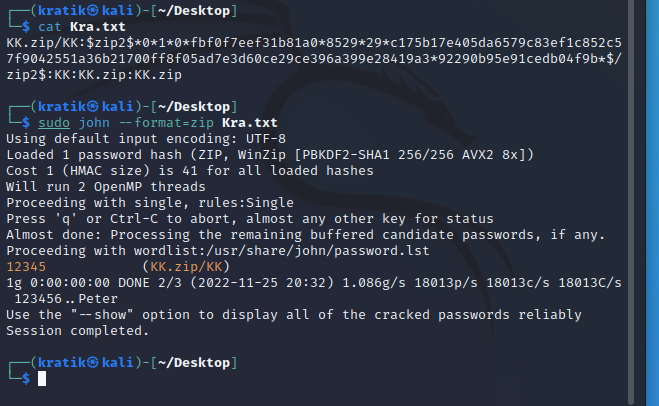
Alright Now , what we are going to do is that we will be using this tool the crack the password of our zip file . Now we have received the password in the encrypted format.



Now we will be exporting this encrypted password in the text format and we will be carrying out a dictionary attack.



So this is how we cracked the password of the zip file .



**CONCLUSION**

**Cyber security is one of the most important aspects of the fast-paced growing digital world**. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.

John is a popular and powerful password-cracking tool. It is often used by both penetration testers and black hat hackers for its versatility and ease of use. From automated hash discovery to dictionary-based attacks, John is a great tool to have in your penetration toolkit.

**REFERENCES**

1. www.Google.com
2. www.Youtube.com
3. "John the Ripper". sectools.org
4. https://www.cybersecurity.com