Title Page

➢ Title:

CyberCrack: A Red Team Simulation Toolkit for Beginner-Level CTF and Ethical Hacking Practice

Submitted as part of the Cybersecurity Internship Project

Organized by: Digisuraksha Parhari Foundation

Powered by: Infinisec Technologies Pvt. Ltd.

➢ Submitted by:

Sachi Ravindra Rane & Yash Dhumali

BSc IT (Final Year), Sathaye College

GitHub: github.com/sachiyash

Abstract

CyberCrack is a basic-level cybersecurity project that simulates a Red Team environment using Capture the Flag (CTF)-style challenges. It helps beginners practice ethical hacking by solving different problems across 15 levels. The toolkit is inspired by famous platforms like OverTheWire (Krypton, Leviathan, and Natas) and is designed to run on Linux. Each level is organized in a separate folder with a challenge and hints. This project encourages users to learn important tools like terminal commands, file permissions, and cryptography. CyberCrack is a great learning tool for anyone new to cybersecurity.

Problem Statement & Objective

Many beginners in cybersecurity struggle to find practical, beginner-friendly environments to practice ethical hacking. There is a need for an offline, easy-to-use toolkit that simulates real-life hacking tasks.

Objective:

To develop an offline, Linux-based Red Team simulation toolkit called CyberCrack with 15 CTF-style challenges for beginners to learn ethical hacking.

Literature Review

1. OverTheWire’s CTF platforms (like Krypton and Leviathan) provide inspiration for structured learning.

2. Platforms like HackTheBox and TryHackMe offer advanced features but may not be beginner-friendly.

3. Tools like Burp Suite, cURL, and Linux terminal are essential for ethical hacking.

4. Offline toolkits are rare, especially for red team practices at the beginner level.

This project builds on these existing systems but makes it simpler and local.

Research Methodology

1. Planning: Decided the project theme based on internship tasks.

2. Tool Selection: Used Linux, Bash, Python scripts, Burp Suite, and cURL.

3. Level Design: Created 15 levels with unique problems like hidden files, password cracking, encoded messages, etc.

4. Testing: Verified every level for bugs and accuracy.

5. Documentation: Each level has a manual file to explain the task.

Tool Implementation

The CyberCrack toolkit has:

A main folder named levels.

Each sub-folder (level1 to level15) contains a specific challenge.

Examples of challenges:

Level 3: Finding hidden files.

Level 6: Decoding an encrypted string.

Level 10: Analyzing and editing a C program.

Hints and solutions are stored in manual.txt files.

Users can interact via terminal or basic scripting.

Results & Observations

Successfully created and tested all 15 levels.

Peer testers were able to solve the challenges.

Learned key concepts like:

File and directory permissions.

Password cracking techniques.

Use of Linux tools (grep, strings, chmod, etc).

GitHub repository was set up to store the project and documentation.

Ethical Impact & Market Relevance

Ethical Impact:

CyberCrack promotes legal, safe, and responsible hacking skills. It helps users understand vulnerabilities without harming any real systems.

Market Relevance:

The demand for ethical hackers is growing. CyberCrack gives hands-on practice to students and interns looking to enter cybersecurity fields. It’s a beginner's step toward real-world certifications and careers.

Future Scope

Add Blue Team (defense) scenarios.

Add web-based interface for solving levels.

Include scoring system and timer.

Build advanced versions with networking and web exploits.

Turn it into a learning module for schools and colleges.

References

1. OverTheWire (https://overthewire.org)

2. Hack The Box (https://www.hackthebox.com/)

3. TryHackMe (https://tryhackme.com/)

4. Linux Command Library
(https://linuxcommandlibrary.com/)

5. OWASP Top 10 (https://owasp.org/www-project-top-ten/)

6. Burp Suite Documentation (https://portswigger.net/burp)

7. Kali Linux Tools (https://tools.kali.org/)

8. Git Documentation (https://git-scm.com/doc)

9. cURL Documentation (https://curl.se/docs/)

10. Digisuraksha Parhari Foundation Guidelines
