**CYBERSENTINEL**

**SUMMER INTERNSHIP TRAINING REPORT**

***Submitted by***

**ISHA  
*in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

**AT**

****

**SCHOOL OF ENGINEERING, DESIGN AND AUTOMATION**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**JUNE – JULY, 2023**

**CANDIDATE’S DECLARATION**

I hereby certify that the work which is being presented in the 45- days summer internship project report entitled “CYBERSENTINEL” by “ISHA” in partial fulfillment of requirements for the award of degree of B.Tech (CSE) submitted in the Department of CSE at GNA University, Phagwara is an authentic record of my own work carried out during a period from 9th June, 2023 to 28th July, 2023 under the supervision of **DR. ANURAG SHARMA.**

**Signature of the Student**

**Isha**

**GU-2021-4164**

**BTech CSE (5th)**

This is to certify that the above statement made by the candidate is correct to the best of my/our knowledge.

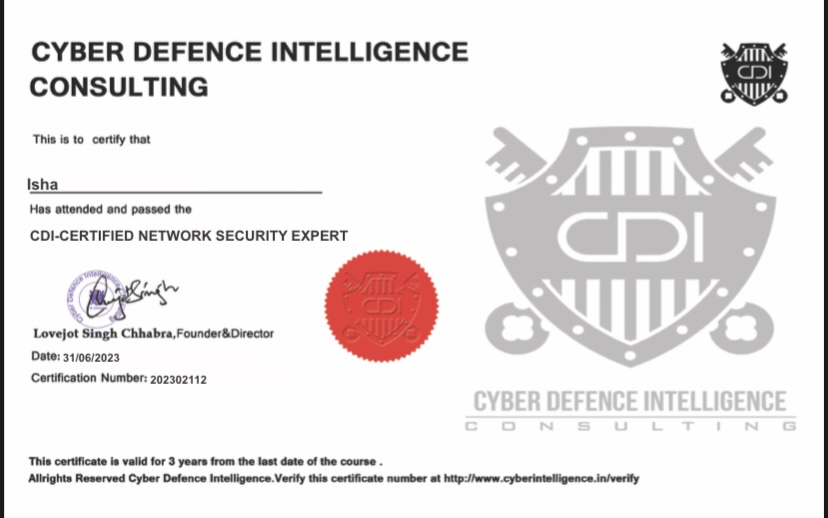
**Signature of the SUPERVISOR (S)**

The B.Tech Viva –Voce Examination of (NAME OF CANDIDATE) has been held on \_\_\_\_\_\_\_\_\_\_\_ and accepted.

**Signature of External Examiner**

**Signature of H.O.D**

**TRAINING COMPLETION CERTIFICATE**



**ACKNOWLEDGEMENT**

I would like to place on record my deep sense of gratitude to (Name of supervisor), Department of Computer Science and Engineering, GNA University, Phagwara, for his generous guidance, help and useful suggestions.

I express my sincere gratitude to Mr. Shubham**,** for his continuous guidance and support in carrying out industrial project work at Cyber Defence Intelligence, Sahibzada Ajit Singh Nagar.

I express my sincere gratitude to Dr. Anurag Sharma, HOD, Department of Computer Science and Engineering, GNA University, Phagwara, for his stimulating guidance, continuous encouragement and supervision throughout the course of present work.

I am extremely thankful to Dr. Vikrant Sharma, Dean (SEDA-E) for providing me infrastructural facilities to work in, without which this work would not have been possible.

**Isha**

**GU-2021-4164**

**BTech CSE (5th)**

**ABSTRACT**

CyberSentinel is designed to address various critical aspects of network security. In an increasingly interconnected world, protecting network assets against cyber threats is paramount. In straightforward language, we aim to explain and empower individuals and organizations to protect their digital assets against a multitude of threats.

The first aspect of the project deals with brute force attacks on FTP, SSH, and Telnet ports. Brute force attacks involve relentless attempts to guess usernames and passwords, exploiting vulnerabilities in these services. Through this project, we explore preventive measures and detection techniques to thwart these malicious endeavors.

Privilege escalation is another pivotal concern, both horizontally and vertically. Horizontal privilege escalation involves an attacker gaining access to another user's account with the same level of privilege, while vertical privilege escalation entails an attacker elevating their privileges to gain access to more sensitive data or systems. CyberSentinel explains these concepts and demonstrates methods to mitigate such vulnerabilities.

The project also explores how Shodan can be used to identify FTP servers, further emphasizing the importance of securing these servers against unauthorized access.

Lastly, the project emphasizes the role of pfSense, an open-source firewall, as a fundamental security measure. It demonstrates how pfSense can be configured to enhance network security, how to block single port as well as multiple ports and furthermore.

So, in a nutshell, It'll help us to understand and tackle brute force attacks, privilege escalation, Shodan, and using pfSense to lock down your ports.

**TABLE OF CONTENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Chapter** | **AIM** | **PAGE NO.** | **REMARKS** |
|  | Title Page | i |  |
|  | Candidate’s Declaration | ii |  |
|  | Training Completion Certificate | iii |  |
|  | Acknowledgement | iv |  |
|  | Abstract | v |  |
|  | List of Figures | viii-xi |  |
| 1. | **INTRODUCTION**   * 1. Introduction   2. Objectives   3. Methodology | 1-1 |  |
| 2. | **INSTALLATION AND SETUP**  2.1 VMware Workstation Pro  2.2 Kali Linux  2.3 Metasploitable2 | 2-4 |  |
| 3. | **COMPREHENSIVE ANALYSIS OF BRUTE FORCE**  3.1 Introduction  3.2 FTP  3.2.1 Description  3.2.2 Analysis  3.2.3 Practical  3.3 SSH  3.3.1 Description  3.3.2 Analysis  3.3.3 Practical  3.4 Telnet  3.4.1 Description  3.4.2 Analysis  3.4.3 Practical | 5-13 |  |
| 4. | **COMPREHENSIVE ANALYSIS OF PRIVILEGE ESCALATION**  4.1 Introduction  4.2 Horizontal Privilege Escalation  4.2.1 Practical  4.2.2 Techniques  4.2.3 Impacts  4.3 Vertical Privilege Escalation  4.3.1 Practical  4.3.2 Techniques  4.3.3 Impacts | 14-25 |  |
| 5. | **COMPREHENSIVE ANALYSIS OF SHODAN**  5.1 Introduction  5.2 Accessing any device using FTP | 26-28 |  |
| 6. | **COMPREHENSIVE ANALYSIS OF PFSENSE FIREWALL**  6.1 Introduction  6.2 Install and Set up  6.3 PFSense Login and DNS Configuration  6.4 Enable secure shell (SSH)  6.5 Add user in PFSense  6.6 Disable IPv6  6.7 Floating rules  6.8 Firewall Configuration  6.9 How to reject single port  6.10 How to add several ports  6.11 How to reject several ports  6.12 How to apply ICMP | 29-39 |  |
| 7. | Conclusion and Future Scope | 40 |  |
| 8. | References | 41 |  |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **FIGURE** | **PAGE** |
| 2.1.1 | VMWare download site | 2 |
| 2.1.2 | VMWare | 2 |
| 2.2.1 | Kali Linux download site | 3 |
| 2.2.2 | Kali Linux | 3 |
| 2.3.1 | Metasploitable2 download site | 4 |
| 2.3.2 | Metasploitable2 | 4 |
| 3.2.3.1 | **Quiet msfconsole** | 5 |
| 3.2.3.2 | FTP Seeker | 6 |
| 3.2.3.3 | FTP Scanner | 6 |
| 3.2.3.4 | Wordlist | 6 |
| 3.2.3.5 | Directory Changer | 6 |
| 3.2.3.6 | Userpass Configuration | 7 |
| 3.2.3.7 | Target IP Setter | 7 |
| 3.2.3.8 | Success Terminator | 7 |
| 3.2.3.9 | Option Explorer | 7 |
| 3.2.3.10 | Exploit Runner | 7 |
| 3.3.3.1 | SSH Finder | 8 |
| 3.3.3.2 | SSH Scanner | 8 |
| 3.3.3.3 | Wordlist | 9 |
| 3.3.3.4 | Directory Changer | 9 |
| 3.3.3.5 | Userpass Configuration | 9 |
| 3.3.3.6 | Target IP Setter | 10 |
| 3.3.3.7 | Verbose Setter | 10 |
| 3.3.3.8 | Success Terminator | 10 |
| 3.3.3.9 | Option Explorer | 10 |
| 3.3.3.10 | Exploit Runner | 10 |
| 3.4.3.1 | **Telnet Finder** | 11 |
| 3.4.3.2 | **Telnet Scanner** | 11 |
| 3.4.3.3 | Wordlist | 12 |
| 3.4.3.4 | Directory Changer | 12 |
| 3.4.3.5 | Userpass Configuration | 12 |
| 3.4.3.6 | Target IP Setter | 13 |
| 3.4.3.7 | Success Terminator | 13 |
| 3.4.3.8 | Option Explorer | 13 |
| 3.4.3.9 | Exploit Runner | 13 |
| 4.2.1.1 | **Distcc Searcher** | 14 |
| 4.2.1.2 | **Distcc Exploiter** | 14 |
| 4.2.1.3 | Option Explorer | 15 |
| 4.2.1.4 | Target IP Setter | 15 |
| 4.2.1.5 | Display Payloads | 15 |
| 4.2.1.6 | Payload Setter | 15 |
| 4.2.1.7 | Session Creator | 16 |
| 4.2.1.8 | **Username Checker** | 16 |
| 4.2.1.9 | Root Privilege Detector | 16 |
| 4.2.1.10.1 | su Binary Check | 17 |
| 4.2.1.10.2 | nmap Binary | 17 |
| 4.2.1.10.3 | Interactive Nmap Shell User | 17 |
| 4.2.1.10..4 | Nmap version checker | 17 |
| 4.2.1.10.5 | Interactive nmapper | 17 |
| 4.2.1.10.6 | Shell Executor | 17 |
| 4.2.1.11.1 | Basic Info Gather | 18 |
| 4.2.1.11.2 | Shadow File Seeker | 18 |
| 4.3.1.1 | **Distcc Searcher** | 19 |
| 4.3.1.2 | **Distcc Exploiter** | 19 |
| 4.3.1.3 | Option Explorer | 19 |
| 4.3.1.4 | Target IP Setter | 20 |
| 4.3.1.5 | Display Payloads | 20 |
| 4.3.1.6 | Payload Setter | 20 |
| 4.3.1.7 | Session Creator | 20 |
| 4.3.1.8 | **Target Machine version** | 20 |
| 4.3.1.9 | Kernel Privilege Searcher | 21 |
| 4.3.1.10 | Release Identifier | 21 |
| 4.3.1.11 | Ubuntu Kernel Exploiter | 21 |
| 4.3.1.12 | Linux Vulnerability Locator | 22 |
| 4.3.1.13 | Copy Exploit Path | 22 |
| 4.3.1.14 | Change Directory | 22 |
| 4.3.1.15 | Run File | 22 |
| 4.3.1.16 | Content Viewer | 22 |
| 4.3.1.17 | Apache Status Checker | 22 |
| 4.3.1.18.1 | Apache Start | 23 |
| 4.3.1.18.2 | Apache Status Checker | 23 |
| 4.3.1.19.1 | 8572.c File Downloader | 23 |
| 4.3.1.19.2 | Run File Downloader | 23 |
| 4.3.1.20 | Check exploit id | 23 |
| 4.3.1.21 | Identification | 24 |
| 4.3.1.22.1 | Compile File | 24 |
| 4.3.1.22.2 | Colorful Lister | 24 |
| 4.3.1.23 | Listening | 24 |
| 4.3.1.24 | Exploit Launcher | 24 |
| 4.3.1.25 | Reverse Shell | 24 |
| 5.2.1 | Login Shodan | 26 |
| 5.2.2 | Anonymous FTP User | 27 |
| 5.2.3 | FTP Login | 28 |
| 5.2.4 | FTP Interface | 28 |
| 6.1.1 | PFSense Site | 29 |
| 6.2.1 | PFSense Download Guide | 29 |
| 6.2.2 | Shutdown and Reboot Guide | 30 |
| 6.2.3 | Network Setting | 30 |
| 6.3.1 | Network Checker (Kali) | 31 |
| 6.3.2 | Network Checker (PFSense) | 31 |
| 6.3.3 | PFSense Login and Setup | 31 |
| 6.3.4 | Time Server Setup | 31 |
| 6.3.5 | LAN Interface Configuration | 31 |
| 6.3.6.1 | Admin Password Change | 32 |
| 6.3.6.2 | Dashboard | 32 |
| 6.4.1 | Enabling SSH | 32 |
| 6.4.2 | Testing SSH | 32 |
| 6.5.1 | Adding New PFSense | 33 |
| 6.5.2 | Check new added user | 33 |
| 6.6.1 | Disabling Global IPv6 Traffic | 34 |
| 6.6.2 | Disabling IPv6 on WAN interface | 34 |
| 6.6.3 | Disabling dhcpv6 on LAN interface | 34 |
| 6.7 | Create the floating rules | 35 |
| 6.9.1 | Communication between virtual machines | 36 |
| 6.9.1 | Rejecting Traffic on LAN Port | 36 |
| 6.9.1 | Testing | 36 |
| 6.10.1 | Creating a New Alias for grouping ports | 37 |
| 6.10.2 | Creating firewall rule with alias | 37 |
| 6.11 | Blocking specific ports | 38 |
| 6.12 | Apply ICMP | 39 |