KIRNAVI BHAVSAR

Ahmedabad, IN,380058 | kirnavibhavsar7@gmail.com | +91 9978272234

CAREER SUMMARY

Cybersecurity Analyst-in-training with hands-on experience in network defense, intrusion monitoring, and attack simulation. Skilled in creating secure lab environments and analyzing attacker behavior through practical experiments. Experienced in honeypot deployment, reverse shell simulations, and defensive automation.
Also enthusiastic about Artificial Intelligence and Machine Learning, exploring their applications in cybersecurity and data-driven analysis for predictive defense systems.

EDUCATION

Bachelor of Technology (B.Tech) **2022-2026**
Information Technology,Indus University
CGPA(till sem 6)- 9.46/10.0

WORK EXPERIENCE

Masterly Solutions Pvt. Ltd. — *Cybersecurity Intern* **July 2025 – October 2025**

SSH Honeypot Intrusion Detection and Prevention System (Windows–Kali VM Lab)
Designed and deployed an SSH-based honeypot integrated with an HTA reverse shell simulation to monitor, analyze, and block malicious activity in real time.
Key Responsibilities & Achievements:

- Configured a hybrid **attacker–victim–defender VM lab** using Kali Linux (attacker) and Windows (defender/victim).
- Captured attacker commands, payloads, and session behavior through real-time logging.
- Implemented **automatic IP blocking** for repeated intrusion attempts.
- Added a **second layer of Windows security defense** that isolated infected sessions and prevented privilege escalation.
- Performed forensic log analysis to understand attacker techniques and recommend mitigations.
- Tools used: *Python (Flask), PowerShell, Wireshark, VMware, Metasploit, Nmap.*

PROJECTS

HTA Reverse Shelling Simulation — Windows Security Testing
Created a controlled Windows VM-based lab to analyze reverse shell behavior and enhance system defenses.

- Used HTA-based payloads in a closed lab to observe connection attempts and generate detailed defensive logs.
- Configured Windows Defender and PowerShell scripts to detect, quarantine, and block malicious executions.
- Captured and analyzed network traffic using Wireshark to identify Indicators of Compromise (IoCs) and response timelines.

- Documented preventive measures and implemented user-awareness recommendations against similar phishing-based attacks.
- Tools & Tech: *HTA, PowerShell, VMware, Wireshark.*

DoS Attack Simulation — Flask-Based Defense Analysis
Developed a Flask-based web server to simulate Denial-of-Service (DoS) attacks and evaluate defense mechanisms.

- Implemented request logging, CPU and latency tracking, and automatic rate-limiting with account lockout.
- Monitored resource thresholds to trigger auto-restart and maintain uptime.
- Tools & Tech: *Python (Flask), Wireshark, VMware.*

Soccer Player Price Prediction — Data Science & ML Project
Built a Machine Learning model to predict soccer player market value using multiple performance metrics.

- Applied Linear Regression and Random Forest models for accurate prediction and comparison.
- Performed data cleaning, preprocessing, visualization, and feature correlation analysis.
- Tools & Tech: *Python, pandas, NumPy, scikit-learn, Matplotlib, Seaborn.*

Brute Force Attack Simulation — Authentication Hardening
Simulated brute-force attacks against a Flask login system to test security controls and lockout mechanisms.

- Added rate-limiting, account lockout, and logging for failed attempts to analyze attack behavior.
- Evaluated system resilience under various attack frequencies and optimized threshold settings.
- Tools & Tech: *Python, Flask, Bash scripts, Logging module.*

CERTIFICATIONS & ACHIEVEMENTS

- **Cybersecurity Analyst Job Simulation** — *Forage*
- **Deloitte Cyber Job Simulation** — *Forage*
- **Ethical Hacking Training** — *Internshala Trainings*
- **Introduction to Futuristic Technologies** — *Indus University*
- **Content Head, CESA (Computer Engineering Student Association)** — *Indus University*

SKILLS

Cybersecurity Tools: Kali Linux, Burp Suite, Wireshark, Metasploit, VMware, Nmap
Programming & Scripting: Python, Bash, PowerShell
Web & Frameworks: Flask, HTML, CSS, JavaScript (basic)
AI/ML & Data Analysis: pandas, NumPy, scikit-learn, Matplotlib, Seaborn
Other Tools: Git, Excel, SQL
Soft Skills: Leadership, Communication, Critical Thinking, Problem Solving, Collaboration

LANGUAGES

English · Hindi · Gujarati