[SYSTEM BOOT] IDENTITY MODULE LOADED — CLEARANCE: TOP SECRET

NISARG CHASMAWALA

root@nisarg:~# Penetration Tester | Offensive Security Engineer | Cybersecurity Researcher

CPENT	CEH Master	CHFI	ISO 27001	MSc Cyber Sec
Pentest Pro	EC-Council Elite	Forensic Investigator	Lead Auditor	BCU · 1st Place Hackathon

ONLINE PRESENCE

Portfolio
Blog
GitHub
Kaggle

CONTACT

nisargkc@gmail.com
+44 7554 469437
Birmingham, England, UK
LinkedIn

CLEARANCE

CPENT
Certified Penetration Tester Pro
EC-Council · Nov 2024

CEH Master
Certified Ethical Hacker — Master
EC-Council · Apr 2024 · 180/200

CHFI
Computer Hacking Forensic Investigator
EC-Council · Dec 2023 · 90.7%

CEH v13
Certified Ethical Hacker v13
EC-Council · Dec 2025

ISO 27001 LA
Lead Auditor — ISO/IEC 27001:2022
Mastermind · Jan 2026

EHE
Ethical Hacker Essentials
EC-Council · Jan 2026 · 96%

CRTOM
Certified Red Team Ops Management
Red Team Leaders · Jan 2026

CTIGA
Threat Intel & Governance Analyst
Red Team Leaders · Jan 2026

CCPP
Certified C++ Practitioner
Red Team Leaders · Jan 2026

CCEP
Cybersecurity Educator Professional
Red Team Leaders · Jan 2026

TOEFL iBT
English Proficiency
ETS · 2024 · 91/120

ARSENAL

> OFFENSIVE
Penetration Testing · Red Team Ops · Exploit Dev · Privilege Escalation · Social Engineering · OSINT · CVSS v3.1 · OWASP Top 10 · MITRE ATT&CK · Cyber Kill Chain

> TOOLING
Metasploit · Burp Suite · Nmap · Nessus · OpenVAS · Wireshark · SQLmap · Aircrack-ng · Hydra · John the Ripper · Ghidra · Snort · OSINT Framework · Maltego · Autopsy · FTK Imager · Magnet AXIOM · Acunetix · Nikto

> CLOUD & DEV
AWS IAM · FastAPI · Flask · React · Next.js 14 · TypeScript · C++ · PostgreSQL · NetworkX · Bash · Zero-Trust · SAST/DAST

> ML / AUTOMATION
Python · TensorFlow · XGBoost · Scikit-Learn · ExtraTreesRegressor

> FORENSICS
Chain of Custody · Disk Imaging · Mobile Forensics · IoT Forensics · ISO 27037/42/43 · UK GDPR · FSR · NIST · HIPAA · PCI-DSS

> PLATFORMS
Kali Linux · Parrot OS · Ubuntu · Debian · macOS · iOS · Android · Windows 11

EDUCATION

MSc Cyber Security

root@nisarg:~$ cat PROFILE.log

Award-winning Offensive Security Engineer and elite Penetration Tester holding CPENT, CEH Master (Practical: 180/200), CHFI (90.7%), CEH v13, and ISO/IEC 27001:2022 Lead Auditor. 1st-Place winner of the BCU Cyber Security Society Hackathon (Aegis-IAM privilege escalation platform, STEAMhouse, UK). Currently pursuing an MSc in Cyber Security at Birmingham City University, uniquely integrating AI and Machine Learning into offensive security pipelines. Seeking a UK-based Penetration Testing or Offensive Security role to drive measurable security outcomes.

root@nisarg:~$ cat EXPERIENCE.log

IT Hardware Support Engineer
[Mar 2025 – Sep 2025]
NIVA TECHNO TRANSITION · *Surat, India*

- Installed and maintained enterprise computing systems and LAN/Wi-Fi infrastructure; diagnosed hardware/software/network faults; performed security checks, OS updates, and provided on-site and remote technical support.

Vulnerability Assessment & Penetration Tester
[Feb 2024 – Feb 2025]
SYSAP TECHNOLOGIES · *Pune, India — Remote · Part-Time*

- Executed full-scope penetration tests across web apps, REST APIs, networks, and cloud environments via Metasploit, Burp Suite, Nmap, Nessus, and OpenVAS; classified vulnerabilities per CVSS v3.1 and OWASP Top 10 with full exploitation PoC.
- Delivered executive-ready pentest reports with attack narratives, root-cause analysis, and prioritised remediation roadmaps; re-tested all critical findings post-patch; tracked adversary TTPs via MITRE ATT&CK.

Vulnerability Scanning & Penetration Testing Intern
[Jul 2023 – Jan 2024]
SYSAP TECHNOLOGIES · *Pune, India*

- Scanned 50+ systems with Nessus/OpenVAS against OWASP Top 10, CWE, NIST SP 800-115; contributed to live engagements — recon, exploitation, and privilege escalation using Nmap and Metasploit; authored formal pentest reports.

Network Specialist
[Jan 2023 – Apr 2023]
AIRLINK COMMUNICATION PVT. LTD. · *Surat, India — Internship*

- Network troubleshooting and monitoring; router/switch config, documentation, and customer technical support.

Network Engineer
[Jun 2022 – Jul 2022]
NIVA TECHNO TRANSITION · *Surat, India — Internship*

- Network infrastructure setup, structured cabling, access-issue resolution, and technical documentation.

root@nisarg:~$ cat PROJECTS.log

HEAVEN | Autonomous Penetration Testing Framework [GitHub ↗]
FastAPI · React · PostgreSQL · ExtraTreesRegressor · MITRE ATT&CK · OWASP

- Architected a production-grade autonomous pentest platform featuring 31 live testing modules and a deterministic two-stage false-positive suppression engine; integrated an ExtraTreesRegressor (R^2=0.9925, trained on NVD data) to dynamically predict CVSS v3.1 risk scores with automated MITRE ATT&CK and Cyber Kill Chain compliance mapping.

Aegis-IAM Dashboard | Cloud IAM Risk Intelligence 🏆 1st Place — BCU Hackathon [GitHub ↗]
Python · NetworkX · AWS IAM · MITRE ATT&CK · OWASP · FastAPI

- Engineered a graph-traversal IAM risk analysis engine scoring 57 dangerous IAM verbs across 10 MITRE ATT&CK tactics; hardened to pass 38 end-to-end security tests (XSS, CSRF, JSON depth-bomb); generated instant CLI patch commands. Won 1st Place at BCU Cyber Security Society Hackathon (STEAMhouse, UK).

HEAVEN-GeoIntel | Zero-API OSINT & Reconnaissance Platform [GitHub ↗]
Next.js 14 · TypeScript · Zero External APIs · 110+ OSINT Pivots

- Built a fully offline OSINT platform processing 400+ NPA area codes and 1,000+ disposable domains with absolute OPSEC and zero external data leakage; automated 110+ targeted OSINT pivots and 64 custom Google Dorks for red-team credential harvesting.

AI-Driven CVSS Vulnerability Severity Predictor | ML & NVD [GitHub ↗]
Python · Scikit-Learn · TensorFlow · NVD Dataset (337,705 CVE records)

- Processed 337,705 NVD CVE records through a multi-paradigm feature selection pipeline; trained Extra Trees and Gradient Boosting regressors achieving R^2=0.9988 and MAE=0.0400 — delivering a production-ready automated severity scoring model.

Predictive IoT Network Flow Analysis | ML & Telemetry [GitHub ↗]
Python · TensorFlow · Scikit-Learn · RT-IoT2022 (117,000+ records)

- 24 model configs on RT-IoT2022 (117K+ records); Gradient Boosting achieved R^2=0.9999 / MAE=0.0010; Extra Trees maintained R^2=0.9996 after 87% dimensionality reduction.

Android Malware Detection System | Mobile Security & ML [GitHub ↗]
Python · XGBoost · Scikit-Learn · Drebin (15,000+ samples)

Birmingham City University, UK
Expected Mar 2027 · Professional Placement

B.Eng. Computer Science & Eng.
SN Patel Institute — GTU, India
Jan 2024 · CGPA 7.86 / 10

LANGUAGES

English — Native / Bilingual (TOEFL 91)
Hindi · Gujarati — Native / Bilingual

- Static-analysis APK pipeline on Drebin (15K+ samples); L1 Regularisation + Chi-Square feature extraction; XGBoost F1-Score 98.47% and near-perfect ROC-AUC.

⬡ **AI-Powered DDoS Detection | ML & Network Defence** [GitHub ↗]
└ Python · TensorFlow · XGBoost · CIC-DDoS2019 (225,000+ records)

- NIDS on 225K+ CIC-DDoS2019 records via 1D-CNN, MLP, ensemble; XGBoost achieved 1.0000 precision and 99.99% accuracy — zero false-positive analyst alerts.

⬡ **Adaptive Vulnerability Risk Scoring | AI Threat Assessment** [GitHub ↗]
└ Python · XGBoost · Random Forest · KNN · One-Hot Encoding

- Dynamic context-aware 0–10 risk scoring over static CVSS; engineered TCP/UDP feature pipelines; validated XGBoost, RF, Decision Tree, KNN regressors via MSE, RMSE, MAE, R^2.

root@nisarg:~$ cat ACADEMIC_LABS.log

⬡ **End-to-End Penetration Testing & RCE Assessment**
└ Nmap · Metasploit · Redis · Openfire · Git Hooks · Reverse Shells · CVSS 10.0

- Identified CVSS 10.0 RCE vulnerabilities across Redis, Openfire, and Gitea; achieved system-level access via Redis replication abuse, Openfire admin exploit, and Git Hooks weaponisation; delivered professional pentest report.

⬡ **Digital Forensic Investigation — Missing Person Case**
└ FTK Imager · Autopsy · Magnet AXIOM · MOBILedit · ISO 27037/42/43 · UK GDPR

- ISO-aligned forensic plan covering endpoints, mobile, IoT, cloud, and CCTV; full chain-of-custody management and timeline reconstruction compliant with UK GDPR, NPCC, and FSR guidelines.

⬡ **Strategic Security Audit — Cyberzone AI Ltd. (AI Healthcare & Fintech)**
└ ISO/IEC 27001:2023 · UK GDPR · DPA 2018 · HIPAA · FIDO2 · Purple Team

- Full ISO 27001:2023 audit of AI-driven healthcare and fintech systems; phased roadmap with MFA (FIDO2), automated patching, immutable backups, and Purple Team exercise recommendations.

root@nisarg:~$ cat ACHIEVEMENTS.log

- 🏆 1st Place — BCU Cyber Security Society Hackathon (STEAMhouse, Birmingham, UK): Aegis-IAM privilege escalation detection platform, outperforming competitive university teams.
- MSc Dissertation: Systematic literature review on Deep Reinforcement Learning and LLM integration in autonomous offensive security; formulated a secure-by-design framework compliant with EU AI Act and GDPR.
- 7 industry virtual job simulations (2025): Deloitte · MasterCard · Telstra · Datacom · TATA · AIG · Commonwealth Bank — threat analysis, SOC operations, fraud investigation, and telecom vulnerability assessment.

root@nisarg:~$ cat RESEARCH.log

⬡ **AI & Autonomous Penetration Testing Frameworks**
└ MSc Dissertation · BCU · 2025–26

- Evaluated DRL and LLMs in autonomous offensive security; compared MAS vs single-agent success-rate metrics on zero-day targets; proposed Neuro-Symbolic AI + HITL governance framework compliant with EU AI Act and GDPR.
- IT Project Management: 7-week Hybrid Agile-PRINCE2 plan (Monday.com, 5-phase WBS) for autonomous AI-driven pentesting system with GDPR/EU AI Act compliance guardrails.

root@nisarg:~$ cat BLOG.log

⬡ **Technical Security Blog** · Blog
└ Personal knowledge-sharing platform covering offensive security research, networking, cybersecurity hardware and software tools and ethical hacking and penetration testing.

root@nisarg:~$ cat FIELD_SIMULATIONS.log

Virtual cybersecurity simulations (2025): **Deloitte** · **MasterCard** · **Telstra** · **Datacom** · **TATA** · **AIG** · **Commonwealth Bank**