PUSHPENDER SINGH RATHORE

Offensive Security Researcher | Security Software Engineer | Open-Source Contributor

+91 7300301634 pushpendersingh046@gmail.com pushpenderrathore.github.io
github.com/Pushpenderrathore Bahal, Haryana, India

SUMMARY

3rd-year B.Tech Computer Science student at BRCM CET focused on offensive security research, malware and botnet analysis, and low-level / systems programming in C, C++, Assembly, and Python. Google Summer of Code 2026 contributor at the Metasploit Framework (Rapid7), building inline tracing presenters for Kerberos tickets and X.509 certificates. Hands-on experience across Active Directory Certificate Services (AD CS), ESC attack-path research, PKINIT, LDAP Schannel, and reverse-engineering tooling, with a defensive emphasis on detecting stealthy, low-and-slow command-and-control (C2) traffic. Authored 5 upstream pull requests (2 merged, 1 in review, ~1,200 lines of Ruby merged) validated end to end against live infrastructure.

EXPERIENCE

Google Summer of Code 2026 Contributor

Rapid7 / Metasploit Framework

05/2026 - Present | Remote

summerofcode.withgoogle.com/programs/2026/organizations/metasploit

Mentors: @jheysel-r7, @zeroSteiner

- Designed and merged CertificateTracePresenter, a new X.509 certificate and CSR tracing subsystem following Metasploit's Presenter architecture, with full RSpec coverage.
- Extended certificate tracing to LDAP Schannel authentication, surfacing certificate material during certificate-based binds.
- Restored and wired CSR tracing into the AD CS / MS-ICPR enrollment flow, decoding requested certificate templates, SANs, and EKU OIDs from live CSRs.
- Prototyped centralized Kerberos ticket tracing with metadata/full verbosity modes and module integration, informing the current presenter design.
- Validated every feature end to end against a live Windows Server 2022 AD CS lab, including ESC1-style enrollment and on-behalf-of CMS paths.
- Followed strict upstream conventions: small reviewable PRs, nil-safe output, backward compatibility, and honest, non-overclaiming documentation.

Upstream Pull Requests (github.com/rapid7/metasploit-framework):

- #21198 - CertificateTracePresenter + certificate/CSR tracing | +1,032 | merged | /pull/21198
- #21469 - CertificateTrace support for LDAP Schannel authentication | +137 | merged | /pull/21469
- #21580 - CSR tracing for AD CS / MS-ICPR enrollment | +277 | in review | /pull/21580
- #21190 - Kerberos-trace: centralized Kerberos tracing | +920 | prototype | /pull/21190
- #21152 - KerberosTicketTrace: metadata/full modes + module integration | +645 | prototype | /pull/21152

Open-Source Contributor

BlackArch Linux

Active

- Package work, tool packaging, and offensive-security tooling research within the BlackArch penetration-testing distribution, in a controlled environment.
- #4645 - Polished README structure and style as per feedback | +137 | merged | github.com/BlackArch/blackarch/pull/4645

Mirai Source Code - IoT Botnet Research Mirror

C / C++ / Go / Shell

TECHNICAL SKILLS

Languages

Ruby | Python | C / C++ | Bash | x86 / x86-64 Asm | JavaScript

Reverse Engineering

Ghidra | gdb | Binary Ninja | objdump | xxd | YARA

Pentesting

Metasploit | Nmap | Wireshark | Burp Suite | Impacket | Rubeus

AD & Auth

Kerberos | ADCS ESC1-ESC16 | Kerberoasting | Pass-the-Hash | Golden / Silver Ticket | PKINIT | LDAP Schannel

Cryptography

OpenSSL | ASN.1 | DER / PEM | X.509 | AES-GCM | PBKDF2

Malware & Network Research

botnet / RAT | C2 architecture analysis | malware lifecycle mapping | beaconing / jitter | low-and-slow C2 detection | socket & protocol analysis | IoT / Linux malware | evasion vs. detection

ML / Data

PyTorch | TensorFlow | Keras | scikit-learn | NumPy | Pandas | Transformers | Ollama

CTF Platforms

HackTheBox | TryHackMe | OverTheWire | WeChall

Tooling

Git | RSpec | pytest | systemd | Kali Linux | BlackArch | Parrot OS

github.com/Pushpenderrathore/Mirai-Source-Code

- Maintained mirror of the Mirai botnet source preserved strictly for educational, research, and cybersecurity-analysis purposes. Used to study how large-scale IoT malware operates at a technical level: infection vectors, C2 protocols, scanning routines, and load distribution.
- #46 - Improved README.md with research and usage guidelines | +154 | merged | github.com/jgamblin/Mirai-Source-Code/pull/46

EDUCATION

B.Tech, Computer Science & Engineering
BRCM College of Engineering & Technology (Maharshi Dayanand University)
CGPA **7.0** / 10.0

- Bahal, Haryana | 3rd Year (Current) | Expected 2028
- Coursework and self-directed study in systems programming, networks, operating systems, and applied cryptography.

RSCIT Computer Diploma
Rajasthan State Certificate in IT, Government of Rajasthan

- Completed

RESEARCH FOCUS

Botnet / RAT & C2 design
Beaconing patterns, persistence, propagation, and abuse of legitimate infrastructure for stealthy communication.

Malware behavior analysis
Infection lifecycle mapping and architectural trade-offs of Linux and IoT malware families, studied strictly for defensive/educational research.

Network detection
Identifying low-frequency, jittered, and protocol-misusing C2 traffic that evades signature-based defenses; closing defensive blind spots.

AI-assisted defense
Lightweight LLMs and behavioral analytics applied to malware detection, threat hunting, and SOC workflows.

KEY ACHIEVEMENTS

- **Google Summer of Code 2026 - selected contributor (175-hour project), Metasploit / Rapid7.**
- **AlgoUniversity Tech Fellowship 2025 - selected via national coding challenge (mentors from Google, Apple, Microsoft, ICPC World Finalists).**
- **5 pull requests to Metasploit upstream - 2 merged, 1 in review, 2 Kerberos-tracing prototypes.**
- **~1,200 lines of Ruby merged into the Rapid7 codebase across the certificate-trace subsystem.**
- **5+ Hack The Box machines solved; OverTheWire (Bandit / Natas); WeChall (rootanonymous) ~1000 rank, 50,000 pts.**

FIND ME ONLINE

LinkedIn
linkedin.com/in/pushpender-singh-rathore-72466a260

GitHub
github.com/Pushpenderrathore

FEATURED PROJECTS

PyScanner - Network Security Scanner
Python / C++ - v10 with ~47 features, including a full C++ port with zero-copy kernel TX and a stateless HMAC ISN architecture. Roughly 37% Nmap feature parity, with genuine advantages in batch transmission, offline CVE lookup, and the stateless ISN design.

Contactsd - Encrypted Contacts Daemon
C / Python - Secure CLI-based contacts manager. AES-256-GCM for confidentiality / integrity / authentication; keys derived from a master password via PBKDF2-HMAC-SHA256 (150k iterations, per-record salt). All cryptography via OpenSSL.

Venice Firewall - AI-Assisted Network Filter
Python / C / Shell - Integrates offline AI models and online AI services to analyse traffic patterns, detect anomalies, and resolve filtering decisions automatically. Real-time adaptive filtering with an admin mail/messaging alert system.

MAC Address Randomizer Daemon
Python / Shell - Periodically randomises MAC addresses for all active interfaces via macchanger. Arch / Debian / Fedora support, dynamic interface detection, and a kill-switch that blocks the network if spoofing fails.

Inline Certificate & Kerberos Tracing for Metasploit
Ruby, RSpec, AD CS, Kerberos - Operator-facing trace output with configurable verbosity (off / metadata / full); reuses extension formatters to decode X.509 extensions, SANs, and policy OIDs. Currently scoping PKINIT certificate tracing.

CERTIFICATIONS

OSCP - Offensive Security Certified Professional
Offensive Security · in progress

CompTIA Security+
CompTIA · in progress

CEH - Certified Ethical Hacker
EC-Council · in progress

RSCIT - Rajasthan State Certificate in IT
Government of Rajasthan · completed

LANGUAGES

English
Professional

Hindi
Native