

AMANDEEP SINGH

Linux Administrator | System Administration | Cloud & Containers
Bhopal, India • +91-8602241181 • amansenu10@gmail.com • [GitHub](#) • [LinkedIn](#)

PROFESSIONAL SUMMARY

Entry-level Linux Administrator with hands-on lab experience managing RHEL/CentOS and Ubuntu systems. Wrote 20+ Bash automation scripts, deployed 10+ Docker/Podman containers, and hardened multi-VM environments using SELinux, SSH controls, iptables, and firewalld. Provisioned and managed AWS infrastructure across EC2, S3, IAM, and VPC. Completed Forage Cybersecurity Job Simulation with focus on security monitoring and incident response.

TECHNICAL SKILLS

- **Linux Systems:** RHEL/CentOS 7/8, Ubuntu 20.04/22.04, Kali Linux — system admin, package management (yum/dnf/apt), systemd
- **System Administration:** User/group management, file permissions, ACLs, SUID/SGID, disk management (fdisk, df, du, mount)
- **Service & Process:** systemctl, journalctl, ps/top/htop, cron/crontab — service admin, monitoring, scheduling
- **Security Hardening:** SELinux enforcing mode, SSH key-only auth, fail2ban, SUID/SGID auditing, /etc/sysctl.conf kernel tuning
- **Firewall:** iptables (INPUT/OUTPUT/FORWARD, NAT), firewalld (zones, rich rules), UFW — network segmentation
- **Log Analysis:** /var/log/auth.log, syslog, secure, messages — grep/awk/sed pipelines, anomaly detection
- **Containerization:** Docker (Dockerfile, volumes, networking, compose), Podman (rootless) — 10+ containers deployed
- **Cloud (AWS):** EC2, S3, IAM (least-privilege, MFA), VPC, Security Groups — provisioning and access control
- **Scripting & Automation:** Bash — 20+ automation scripts; Python (basic scripting); Go (CLI tool development)
- **Networking & Tools:** TCP/IP, DNS, SSH; Wireshark/tcpdump basics; ip/netstat/ss; Git & GitHub

EXPERIENCE

Linux System Administrator — Self-Built Home Lab | 2022 – Present

Note: This experience is self-directed and built entirely within a personal home lab environment on my own home network — not from a formal employer. However, all tasks were performed on real Linux systems (RHEL, CentOS, Ubuntu) configured and managed as production-equivalent server environments. Every skill listed below reflects genuine, hands-on technical work — not simulations or coursework.

- Designed and built a multi-VM home lab from scratch — configured static IPs, inter-VM routing, DNS resolution, and network segmentation across RHEL/CentOS and Ubuntu nodes to replicate a real server environment.
- Enforced least-privilege across all systems — sudoers configuration, ACLs, SUID/SGID auditing — significantly reducing simulated attack surface and unauthorized privilege escalation paths.
- Administered 15+ services via systemctl (Apache, Nginx, SSH, cron, rsyslog, fail2ban) — diagnosed failures through journalctl log analysis and restored uptime with zero data loss across all test cycles.
- Locked down SSH on every system — root login disabled, key-only authentication, AllowUsers directive configured, fail2ban deployed — zero brute force successes in all simulated attack tests.
- Deployed 10+ Docker containers and Podman pods — authored Dockerfiles, configured volumes and bridge networking, orchestrated multi-container environments with docker-compose.
- Wrote 20+ Bash scripts for log parsing, health reporting, automated backups, and user provisioning — eliminated repetitive manual admin tasks and improved consistency across the lab.
- Provisioned and managed AWS infrastructure — EC2 instances, S3 bucket policies, IAM least-privilege roles with MFA, VPC with Security Groups — following AWS security best practices.

PROJECTS

ReconForge — Bash Automation Pipeline • github.com/DaddyUchiha/reconforge

- End-to-end Bash pipeline: subdomain enum → alive filtering → directory fuzzing → JS extraction → API key scanning.

Gohunter — Go CLI Tool • github.com/DaddyUchiha/gohunter

- Concurrent Go CLI tool for subdomain enumeration and directory brute-forcing — goroutine worker pool, modular architecture.

403evasion — HTTP Research Tool • github.com/DaddyUchiha/403evasion

- Go tool for HTTP 403 bypass via header injection — demonstrates deep understanding of Linux web server behavior.

CERTIFICATIONS

Introduction to Cybersecurity Job Simulation — Forage | 2026

- Tasks completed: SOC monitoring, penetration testing, phishing analysis, incident response, and vulnerability assessment.

EDUCATION

B.Com — Sadhu Vaswani Autonomous College, Bhopal 2019–2022

Higher Secondary (Science) — Sanskar Public High School, Bhopal 2018

ADDITIONAL

Languages: English (Professional), Hindi (Native) • **Availability:** Open to on-site, remote, or hybrid roles •

Interests: Linux automation, system hardening, containerization, cloud infrastructure, open-source tooling