

Anmol Chaudhary

✉ anmolchaudhary8317@gmail.com | 📞 +91 7453878899 | 🌐 anmolchaudhary01 | 🏠 bustayaga

Objective

Computer Applications graduate seeking an entry-level role in Network Engineering, Infrastructure, or Cybersecurity (SOC Analysis, Red Teaming, or Digital Forensics). Practical capability demonstrated through 20+ HackTheBox machines covering web exploitation, Active Directory, network forensics, CVE research, and privilege escalation. Committed to translating hands-on lab skills into real-world security value.

Education

Bachelor of Computer Application — Rabindranath Tagore University	2022 – 2025
Raja Rammohan Roy Academy, Dehradun	2020 – 2022

Projects

Web Application Exploitation & Privilege Escalation *HackTheBox Labs — Cap, Reactor, Conversor, DevHub, Expressway, CodePartTwo, HackNet*

- Exploited a range of web vulnerabilities across 7 HTB machines: IDOR (Cap — enumerated PCAP captures via Burp Suite to retrieve leaked FTP credentials); SSTI (HackNet — Django template injection to dump plaintext passwords); insecure file upload (DevHub, Conversor); and unauthenticated Next.js RCE (Reactor, CVE-2025-55182).
- Escalated privileges using diverse techniques: cracked MD5 hashes from an exposed SQLite database and hijacked a root-owned Node.js V8 debug port via SSH tunnel (Reactor); abused cron job write access (Conversor); exploited js2py sandbox escape (CodePartTwo); and weaponised pickle deserialization on a world-writable cache (HackNet).
- Lab writeups and methodology notes documented at github.com/bustayaga

Network Forensics, Active Directory Attacks & CVE Exploitation *HackTheBox Labs — Voleur, Silentium, Cap*

- Enumerated an Active Directory environment on Voleur using BloodHound and NetExec (Kerberos-only, NTLM disabled); identified and exploited misconfigured AD permissions to escalate to Domain Admin.
- Recovered plaintext FTP credentials from a PCAP file on Cap via IDOR and Wireshark TCP stream analysis; escalated to root by identifying cap_setuid on the Python binary using getcap.
- Chained CVE-2025-58434 and CVE-2025-59528 on Silentium (Flowise unauthenticated password reset + authenticated RCE) to land inside a Docker container; escaped by leaking SSH credentials from environment variables and exploiting internal Gogs (CVE-2025-8110) for root.
- Detailed attack chain documentation and findings available at github.com/bustayaga

SIEM Deployment & Threat Detection — Microsoft Sentinel *Personal Lab — Microsoft Azure*

- Provisioned Microsoft Sentinel on Azure; connected firewalls, VMs, and web apps as data sources to build a centralised log ingestion and alerting pipeline.
- Wrote custom KQL detection rules for brute-force, lateral movement, and IOC alerts; simulated attacks to validate coverage and reduce false positives.
- Lab setup documentation and KQL rule templates published at github.com/bustayaga

Learning

- Completed 20+ machines on HackTheBox spanning web exploitation, Active Directory, network forensics, CVE research, privilege escalation, and reverse engineering
- Self-study: TCP/IP, subnetting, VLANs, OSI model, routing protocols (OSPF/BGP), firewall configuration, IDS/IPS

Skills

- Networking:** TCP/IP, DNS, DHCP, VLANs, Subnetting, OSI Model, OSPF/BGP basics, Wireshark, Nmap, Packet Analysis
- Offensive Security:** Burp Suite, Metasploit, Gobuster, Netcat, Hydra, Hashcat, LinPEAS/WinPEAS, BloodHound, NetExec, Python exploit scripting
- Defensive / SOC:** Microsoft Sentinel, KQL, SIEM Log Analysis, IOC Identification, MITRE ATT&CK, Incident Triage, Alert Tuning
- Infrastructure & Cloud:** Microsoft Azure, Linux (Kali/Ubuntu), Windows Server, Active Directory, Docker, VMware/VirtualBox, SSH
- Programming & Tools:** Python, Bash, SQL, Git, Salesforce Service Cloud, Genesys Cloud CX