Vijaysingh Puwar

Cybersecurity Engineer | Identity & Access Management | Network & Cloud Security

NYC | vpuwar77@gmail.com | +1-929-400-2052 | linkedin.com/in/vijaysinghpuwar | GitHub | TryHackMe: VoidHex

PROFILE

Mid-level Cybersecurity Engineer with hands-on experience across identity & access management (IAM), network security, and cloud security in Windows, Active Directory, and AWS environments. Hardened 150+ endpoints and servers, enforced MFA and least-privilege access, and used Python/PowerShell to automate account hygiene and log-based audits. Graduate-level training in automating information security, network security & defense, ethical hacking, and cyber intelligence, with a strong focus on practical, auditable security controls.

CERTIFICATIONS

CompTIA **CySA+**
CompTIA **Security+**
Cisco **CCNA**

RELEVANT EXPERIENCE

R.S. Infotech India
Cybersecurity & Systems Engineer Feb 2023 – Aug 2024

- Secured and maintained **150+** Windows and Linux endpoints and servers by enforcing baseline controls (patches, AV, BitLocker, host firewalls) to reduce exploitable attack surface.
- Performed **Active Directory identity hygiene** using ADUC, GPMC, Event Viewer, and PowerShell (`Get-ADUser`, `Search-ADAccount`, lastLogon attributes) to identify inactive, orphaned, and high-risk accounts; coordinated disablement and remediation with system owners.
- Supported **IAM operations** by assisting user onboarding/offboarding, adjusting group memberships and access rights based on role changes, and validating privileged groups against least-privilege and separation-of-duties expectations.
- Assisted with MFA and password policy enforcement through Group Policy and identity controls, reducing account takeover risk for remote-access and admin accounts.
- Used **Python/PowerShell** to automate log parsing, account and permission audits, and configuration checks, cutting triage time for recurring identity-related alerts.
- Deployed and secured AWS resources (IAM, VPC, EC2, S3, Security Groups, NACLs) and integrated CloudWatch + SNS alerts to surface suspicious activity and misconfigurations for remediation.

TECHNICAL SKILLS

Programming Languages: Python, PowerShell, Bash
Ethical Hacking & Penetration Testing: Nmap, Burp Suite, Metasploit basics, password/brute-force testing, simple web app assessments
Application Security: Authentication/authorization concepts, secure credential handling, basic web security (OWASP-style issues), logging & monitoring
Network Security: TCP/IP, VLANs, ACLs, VPN fundamentals, DNS/DHCP, firewalls, Wireshark, basic IDS/IPS concepts
Routing & Switching Protocols: Inter-VLAN routing (ROAS), Rapid-PVST, RIPv2, trunking, STP protections (PortFast, BPDU Guard, Root Guard)
Cloud & IAM: AWS IAM (users, roles, policies), VPC, EC2, S3, Security Groups, NACLs, CloudWatch, SNS, MFA, least-privilege design
Tools & Platforms: Windows 10/11, basic Linux CLI, AD DS, Group Policy, Docker, VirtualBox/VMware, Git/GitHub, ticketing tools (ServiceNow/Jira-style)

LEADERSHIP

Informal Mentor & Study Group Lead, Cybersecurity Peers 2024 – Present

- Guided classmates and junior peers through labs in networking, security automation, and cloud security; helped them interpret logs, design fixes, and structure incident-style reports.
- Shared scripts, lab notes, and troubleshooting guides, fostering a collaborative learning environment and improving lab completion rates.

ACADEMIC PROJECTS & LABS

Automating-InfoSec — Security Automation Labs (CYB 631) 2024

- Developed **Python/PowerShell** scripts to parse logs, summarize events, and automate common security checks (account & permission audits, simple anomaly detection).
- Turned manual SOC/IAM tasks into repeatable, auditable workflows, reinforcing the value of automation in incident triage and compliance evidence.

Configuring Cloud Security in AWS — IAM & Network Hardening 2024

- Designed a secure EC2 environment with IAM users/roles, least-privilege policies, and tightly scoped Security Groups/NACLs to protect services from unwanted access.
- Integrated CloudWatch metrics and SNS alerts to capture identity- and configuration-related events, modeling practical cloud security monitoring and notification.

Cisco Network Security Labs — Rapid-PVST & Inter-VLAN ROAS 2023

- Built campus-style topologies in Cisco Packet Tracer using **Rapid-PVST**, per-VLAN root load balancing, and protections like PortFast, BPDU Guard, and Root Guard.
- Implemented router-on-a-stick **inter-VLAN routing** and validated segmentation, trunking, and ACL-based network access control.

EDUCATION

Pace University, Seidenberg School of Computer Science and Information Systems New York, NY
M.S. in Cybersecurity | GPA: 4.0/4.0 Expected Dec 2026
Relevant Coursework: Automating InfoSec with Python & Shell (CYB 631); Network Security & Defense (CYB 623); Ethical Hacking & Penetration Testing (CYB 625); Information Security Management (CYB 621); Cyber Intelligence Analysis & Modeling (CYB 651).

G H Patel College of Engineering & Technology Gujarat, India
B.E. in Mechanical Engineering Jan 2024

ADDITIONAL TRAINING

CTFs & Labs — TryHackMe (*VoidHex*) Ongoing
Hands-on practice with Windows/AD, web app testing, and network security, emphasizing structured note-taking, timelines, and clear remediation steps.

Conferences & Meetups Ongoing
Participation in cybersecurity conferences and local meetups to stay current on emerging threats, IAM best practices, and defensive techniques.

ADDITIONAL EXPERIENCE

L&T—Sargent & Lundy Limited Vadodara, India
System Intern Jan 2023 – Apr 2023

- Authored **SOPs/runbooks** for common provisioning and troubleshooting flows, improving first-contact resolution and consistency across shifts.
- Practiced disciplined documentation and change tracking aligned with strict safety and regulatory standards.

Elecon Engineering Anand, India
Design Intern Jun 2022 – Jul 2022

- Collaborated with cross-functional engineering teams on precision manufacturing tasks, reinforcing habits in version control, quality checks, and structured handoffs.