

# Aslam Mahimkar

Doha, Qatar | [amahimkar@moi.gov.qa](mailto:amahimkar@moi.gov.qa) | <https://aslammahi.github.io> | [Blogs](#) | (+974) 55945675

## Summary

---

OSCP-certified penetration tester with strong experience in finding and fixing security issues across networks, systems, and applications. Skilled in red teaming, vulnerability testing, and creating clear reports to improve security. Always learning new techniques, sharing knowledge, and helping teams build stronger defenses.

## Professional Experience

---

### Red Team & Cloud Security

September 2022–Present

SELF, Doha, Qatar

- Built personal labs for penetration testing and red team exercises.
- Focused on Active Directory attacks: privilege escalation, Kerberos abuse, lateral movement.
- Explored Azure and AWS environments to identify misconfigurations and privilege escalation paths.
- Conducted web application testing using OWASP Top 10 methodologies (authentication, injection, access control).
- Automated tasks with scripting to streamline workflows.
- Published technical blogs and clear reports documenting findings.

### Senior System Engineer

May 2018–present

TELECOMMUNICATION DEPARTMENT, Doha, Qatar

- Led deployment of NOC systems (NMS, BMC, NetAct) and ITSM tools, optimizing IT processes.
- Designed ITSM processes (incident, change, problem, SLA) and integrated monitoring to detect anomalies.
- Managed NOC infrastructure, including servers, network equipment, and monitoring systems, ensuring robust security and compliance.
- Defined project scope, monitored execution, and collaborated with stakeholders to mitigate risks.

### Assistant System Engineer

April 2014–April 2018

TELECOMMUNICATION DEPARTMENT, Doha, Qatar

- Enhanced network monitoring, achieving 99.9% uptime and reducing false alerts by 40%.
  - Provided initial incident response for network/system issues, reducing resolution time by 30%.
  - Assisted in network/server setup, diagnostics, and security monitoring.
  - Documented processes to support future incident investigation and troubleshooting.
  - Worked with team members during outages to restore services quickly.
- Supported upgrades and patching of systems to improve performance and security.

### Network Support Engineer

May 2012–March 2014

SPANCO BPO SERVICES LIMITED, Vashi, Navi Mumbai

- Delivered first-level network support and resolved LAN/WAN connectivity issues.
- Assisted in network expansions, hardware setup, and monitoring with a focus on minimizing downtime.
- Followed security protocols and documented incidents for continuous improvement.
- Provided user support for basic network and system issues, improving response time.

## Certifications

---

Certified Azure Red Team Professional (CARTP)	August 8 2028
Certified Information Systems Security Professional (CISSP), ISC2	April 2027
Offensive Certified Professional (OSCP), Offsec	Present
Certified Red Team Professional (CRTP)	December 2027
Certified in Cybersecurity (CC), ISC2	November 2026
CCIE Service Provider, CISCO	September 2020
CCIE Enterprise Infrastructure, CISCO	September 2020
CCNP Routing and Switching, CISCO	September 2020
CCNA Routing and Switching, CISCO	September 2020
Microsoft Certified Professional (MCP), Microsoft	January 2015
Information Technology Infrastructure Library (ITIL V3)	December 2015

## Education

---

IMPERIAL COLLEGE OF ENGINEERING AND RESEARCH, PUNE UNIVERSITY, India	April 2012
<b>Bachelor of Electronics and Telecommunication Engineering</b>	
<ul style="list-style-type: none"><li>Completed a four-year degree with distinction grades</li></ul>	

## Awards & Projects

---

CVE-2024-36598 <a href="#">Unauthenticated Remote Code Execution (RCE)</a>	May 2024
CVE-2024-36597 <a href="#">SQL injection vulnerability</a>	May 2024
CVE-2024-36599 <a href="#">Cross-Site Scripting (XSS)</a>	May 2024
CVE-2024-44727 <a href="#">SQL injection vulnerability</a>	August 2024
CVE-2024-44728 <a href="#">Stored Cross-Site Scripting (XSS)</a>	August 2024
CVE-2024-45932 <a href="#">Stored Cross-Site Scripting (XSS)</a>	October 2024
CVE-2024-45933 <a href="#">Stored Cross-Site Scripting (XSS)</a>	October 2024

### Threat Detection Lab ([GitHub](#))

This lab provides Docker-based deployments of several key security tools such as Splunk, Elastic SIEM, Cribl, n8n SOAR, and Shuffle.	September 2024
--	----------------

### HoneyLogix ([GitHub](#))

A flexible honeypot designed to monitor and log IPs, usernames, passwords, and commands across SSH and HTTP protocols. Built with Python for visual insights.	September 2024
---	----------------

## Additional Skills

---

### Offensive Security Skills

Experienced with penetration testing tools and methodologies, including Burp Suite Pro, Nmap, SQLmap, Nessus, Metasploit, winPEAS/linPEAS, feroxbuster/gobuster, BloodHound, and Active Directory enumeration. Skilled in Kerberos abuse, lateral movement, OWASP Top 10 testing, and cloud basics in Azure and AWS, including IAM, Key Vault, and Service Principals.

### Teamwork

Communicates effectively within teams, takes initiative, and can delegate tasks when needed.

### Computing

Skilled at using most mainstream operating systems, such as Windows, Linux as well as Linux server variations.

### Programming & Scripting

Python (Intermediate), PowerShell (Basic), Bash (Basic), SQL (Basic), PHP (Basic).