PRAJWAL T M

Cyber Security Consultant

+91 9972360344

prajwaltm42@gmail.com

Linkedin-Profile

Davanagere, Karnataka, India

SUMMARY

Experienced Security Consultant with 1.4 years of expertise in providing strong cybersecurity solutions. Proficient in conducting purple teaming exercises and improving security measures through collaborative efforts between red and blue teams. Skilled in utilizing SIEM tools such as Splunk to effectively monitor, detect, and respond to real-time security threats. Adept in AWS cloud architecture and Windows Active Directory (ADDS) environments, demonstrating a solid understanding of securing cloud infrastructure and managing access control. Committed to leveraging technical acumen to protect digital assets and ensure smooth security operations.

EDUCATION

GM Institute of Technology

Bachelor's Engineering in Information Science
Davanagere, Karnataka, India
Oct 2019 – Jul 2022

Imarticus Learning

Post Graduate Programme in Cyber Security
Bengaluru, Karnataka, india
Sep 2022 – July 2023

SKILLS

- Vulnerability Assessment
- Penetration Testing
- Network Scanning
- Log Analysis
- Breach and attack simulation
- Threat Modeling
- Firewall Configuration
- Active Directory Domain Service
- CTF Challanges

TOOLS

- **Redteam** : Caldera
- **SIEM** : Splunk
- **EDR**: OpenEDR
- **Web Security** : Burpsuite
- **Network** : Metasploit-Framework
- **Bruteforce** : Hydra
- **Network Scanner** : Nmap
- **Firewall** : Comodo & malwarebyte Firewall
- **Hidden Directory** : dirbuster
- **Network Analyzer**: Wireshark

PROFESSIONAL EXPERIENCE

Security Consultant

Occult Cyber Company | Aug 2023 - Nov 2024

Roles and Responsibilities

- Spearheaded purple teaming initiatives, simulating real-world adversary tactics using the Caldera tool, resulting in enhanced collaboration between red and blue teams, improving threat detection capabilities by 30%.
- Conducted 20+ threat emulation simulations using Caldera, replicating real-world adversary behavior from threat groups like APT29 and Oilrig, directly improving incident response readiness and reducing potential attack surfaces.
- Implemented real-time threat detection rules in Splunk, resulting in a 95% reduction in false positive alerts and a 30% faster response time to genuine security threats.
- Enhanced network security by monitoring systems for potential threats and vulnerabilities.
- Configured and maintained robust replication strategies within Windows ADDS to ensure high availability and disaster recovery capabilities; minimized potential downtime to under 1 hour.
- Analyzed log files for anomalies, identifying potential intrusions or malicious activity before significant damage occurred.
- Enhanced client security by conducting comprehensive risk assessments and recommending appropriate countermeasures.
- Developed comprehensive Reporting & Remediation Plans, detailing findings from security assessments and providing actionable remediation strategies to stakeholders.

CERTIFICATIONS

- CEH:CERTIFIED ETHICAL HACKER (ceh v12 Practical) - **EC-council**
- Microsoft Certified: Windows Server Hybrid Administrator Associate - **Microsoft**
- MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training - **cybrary**
- MITRE ATT&CK Defender™ (MAD) ATT&CK® SOC Assessments Certification Training - **cybrary**
- Python Essentials -1 - **Cisco**