CONTACT ME AT

20, Meenatchi nagar, Near
Teacher's Colony, Ganapathy,
Coimbatore-641006

maheshashwin99@gmail.com

https://mahesh-ashwin.github.io

+91-9940955076

SKILLS SUMMARY

WAF - F5 Big-IP(LTM+ASM), F5 Silverline, Radware Appwall, Barracuda WAF

DDoS - Arbor, Radware Defense Pro, Cloudflare

IPS - Checkpoint, Cisco, PaloAlto

Programming - Python

Cloud - Azure, AWS

Ticketing Tools - Service Now, IOP, Jira

OS - Windows, Linux (Debian, Ubuntu)

Pentest Tools - Metasploit, Nmap, SQL map

Protocols - HTTP, TCP, TLS, IPSec

Firewall - Fortinet, PaloAlto

Proxy - iboss - CASB

Cyber Basics - Malware Analysis, Intrusion Detection, Threat Detection, Log Analysis

PROJECTS

- Security Automation - Automated Big-IP for APM, AFM using REST API and Python
- Home automation using Google assistant
- Implementation of artificial intelligence in Raspberry Pi
- Automated petrol pump system using UPI payment
- Published 1 Android App in Google Play Store.

MAHESH ASHWIN

CYBER SECURITY ENGINEER

PROFILE AT A GLANCE

Cyber Security Engineer with 5+ years protecting global web applications and networks across on-premise and cloud (AWS/Azure). Specialized in DDoS mitigation (Arbor, Radware), WAF (Web Application Firewall), Bot Defense—F5 BIG-IP (ASM/APM/AFM), CASB, Proxy, SAST/DAST (Checkmarx), Secure Code Review Assessments, Cloudflare—and next-gen firewalls/IPS (Fortinet, Palo Alto, Cisco Firepower,). Partnered with SOC to tune SIEM detections and WAF/IPS policies, reducing false positives by 15–30% while strengthening Layer 7 defenses against OWASP Top 10 and API abuse. Built Python/REST/Jenkins automations for policy changes, SSL renewals, and pre/post validations, cutting deployment time and manual errors while improving reliability.

WORK EXPERIENCE

Cyber Security Engineer

Wipro Ltd | Nov 2020 - Oct 2023 | 2 Years 11 Months

Summary: With Around 3 years of hands-on experience in network security, I have a proven track record in configuring, managing, and troubleshooting Web Application Firewalls (WAFs), Intrusion Prevention Systems (IPS), and Distributed Denial of Service (DDoS), Bot Defense and Firewall security devices. My expertise lies in safeguarding web applications from layer 7 attacks and network-based threats by fine-tuning WAF policies and IPS signatures and firewall policies.

Key Responsibilities:

WAF Configuration and Management (Cloud and On prem):

- Deployed, configured, and managed WAF solutions for various web applications.
- Implemented WAF policies to protect against common web application vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

Live Troubleshooting:

- Provided timely and effective troubleshooting for client-reported WAF-related issues. Analyzed error logs and network traces to pinpoint the root cause of problems.
- Implemented corrective measures to restore WAF functionality and minimize service disruptions.

EDUCATIONAL HISTORY

Bachelor of Engineering in Electronics and Communication Engineering (ECE) at SNS College of Technology, Coimbatore | January 2016 - December 2020

- Graduated first class with distinction.
- Worked and created various embedded projects on IOT and AI integration.
- Contributed for two 3D design projects and proposals

Completed Schooling at Amrita Vidyalayam, Coimbatore
HSC and SSLC | Till 2016

- SSLC(CBSE): 8.8 CGPA, HSC: 85.6%
- Studied in Computer Science stream

CERTIFICATIONS

- Automation Anywhere University - RPA Certified
- Fortinet NSE-3 Certified
- Barracuda WAF Advanced Certified
- Azure AZ-900 Certified
- Radware AppWall Certified
- Certified Ethical Hacker (CEH)

ACHIEVMENTS

- Contributed to propose one design patent
- 1st Price in Out of the box Event conducted by Sri Krishna college of technology, Coimbatore
- Winner in Kho-Kho Inter District Competition
- Automated F5 Big-IP APM and AFM policy modification using Python and REST API

Policy and Signature Fine-tuning:

- Continuously evaluated and refined WAF policies and IPS signatures to enhance protection against emerging threats.
- Balanced security and performance requirements to ensure optimal WAF and IPS operation.
- Stayed updated on the latest security trends and best practices.

Cloud CDN/WAF and DDoS Solution:

- Managed global edge infrastructure using Cloudflare, focusing on CDN caching strategies (Page Rules, Cache Levels) and advanced security configurations.
- Expertly tuned the Web Application Firewall (WAF) to mitigate OWASP Top 10 vulnerabilities and implemented Advanced Rate Limiting to prevent API abuse.

SOC Monitoring and Incident Response:

- Developed and tuned complex correlation rules within [SIEM Tool - Splunk] to detect multi-stage attacks, reducing false positives by 15% and improving SOC analyst efficiency.

Achievements:

- Reduced false positive alerts by 30% through optimized WAF and IPS configurations.
- Implemented cost-effective security solutions that aligned with business objectives.
- I am a dedicated and results-oriented security professional with a passion for safeguarding digital assets. My technical expertise and problem-solving skills enable me to effectively protect organizations from a wide range of cyber threats.

Cyber Security Engineer - 2

Comcast | Oct 2023 - Till Date | 2+ Years

Summary: Hands on experience in delivering DDoS mitigation services, WAF Layer 7 Security, Bot defense Technologies, managing FortiGate firewalls and F5 VPN solutions, and working with various network infrastructure technologies. Also I have successfully automated F5 Big-IP APM and AFM policy modification using Python and REST API, enhancing efficiency and reducing manual errors.

Key Responsibilities:
DDoS and WAF Mitigation:

- Provided DDoS mitigation services to a large customer base, protecting them from over 23 types of DDoS attacks.
- Configured and managed NETSCOUT Arbor Sightline appliances for effective DDoS mitigation.
- Implemented WAF policies in F5 BIG-IP ASM to protect against common web application vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
- Analyzed Application traffic to refine detection logic and reduce false positives for legitimate customers.

CLIENTS WORKED WITH

- Cynergy Bank (UK)
- Diageo
- Innovapost (Canada)
- RSA (IRE & UK)
- Easyjet(Switzerland)
- ADM (Canada)
- Chemours (US)

FortiGate Firewalls and F5 VPN:

- Configured and managed Fortinet firewalls for various customers, ensuring secure network connectivity.
- Troubleshot connectivity issues related to FortiGate firewalls, MPLS circuits and IPsec VPN tunnels.
- Managed F5 AFM and APM policies for VPN connectivity, providing support to multiple vendors.

Vulnerability Assessment and Patching:

- Worked on Nessus scanner for Vulnerability Assessment
- Worked with Multiple teams for OS patches, firmware updates, and application patches.

Bot Defense:

- Managed automated bot mitigation rules across global Data centers and WAF architectures (Big-IP ASM and Bot defense) to filter malicious traffic at the edge.
- Optimized rate-limiting policies and challenge-action workflows (CAPTCHA, JavaScript challenges) to balance security with a seamless user experience.

Collaborated with SOC Monitoring and Response Team:

- Worked with SOC team to triage high-priority alerts across a diverse security stack (SIEM, IDS/IPS, VPN and WAF) and providing Root Cause Analysis for the team.
- Provided finetuning suggestions on the existing rules to SOC team to enhance threat detection and mitigation.

Security Tool Automation:

- Worked on Automating the security devices to push security policies across multiple data center using Python and Jenkins
- Automated SSL certificate renewal for the security devices using Python and Jenkins.
- Automated Pre and Post validation steps of change implementation using shell scripts.

Achievements:

- Successfully automated F5 Big-IP APM and AFM policy modification using Python and REST API, improving efficiency and reducing errors.
- Mitigated numerous DDoS attacks, protecting critical infrastructure and services.
- Provided exceptional customer support for network connectivity and security issues.
- Contributed to a secure and reliable network infrastructure.