Ashutosh Joshi

- Chicago, IL • +1 312-714-8039 • ashutoshjoshi003@gmail.com
- https://www.linkedin.com/in/ajoshi37/ • https://github.com/ajoshi37/Profile
- Clearance: **None** • Relocation: Highly Relocatable

EDUCATION

ILLINOIS INSTITUTE OF TECHNOLOGY, CHICAGO, IL 2019 – 2021

Master of Science

- Master of Science in Information Technology and management. (Computer & Information Security)

RAJASTHAN TECHNICAL UNIVERSITY, KOTA, INDIA 2012 - 2016

Bachelor of Technology

- Computer Science and Engineering

CERTIFICATIONS

Splunk 7.x Fundamentals

Qualys - Endpoint Detection and Response (EDR) - Foundation

Academic Projects

Penetration testing & Vulnerability Assessment Fall - 2021

- Performed 25+ Pentesting and Vulnerability Assessment on college private IP'S and virtual labs

Malware Analysis Spring - 2020

- Investigated the malware (such as Emotet, Qbot, Sirefef and Zbot) from malicious payloads by investigating Architecture, Subsystem, MD5, SHA1, SHA3, SHA256 and Hashes with Hybrid Analysis and Virustotal

Incident Response with GRALYLOG Spring - 2020

- Effective at finding, managing and documenting logs using **GrayLog**. Created an Incident Response report using Graylog to find malicious attacker from 10,000 logs given logs

AWS Cloud Computing Fall - 2019

- Created a whole cloud Infrastructure using Bash Scripting includes backend and frontend server such as Lambda, EC2, Load Balancer, DynamoDB, SNS, SQS S3 and Lambda.

Experience

Network Engineer 2016 - 2018

RAJASTHAN PATRIKA Rajasthan, India

- Researched and eliminated network security incident, actor techniques, advanced threats and suspicious activity from potential and active risks to network and data
- Collaborated for configuring, managing, administering, and troubleshooting operating systems, including on Windows XP, Windows 2000/2003/2008/2012 Server, UNIX, Linux, Windows and iOS. Upgrade and troubleshoot network.
- Detected 50 plus network vulnerabilities by testing infrastructure security and tracking potential threats to the network.

- Reviewed and assessed services, ports, Firewalls, VPN, Web Proxy and admin activities on Ubuntu, Linux, CentOS, and CISCO
- Achieved improved network performance by 20% through monitoring and app prioritization.
- Summarized and prepared network topologies for 100+ users including routers, access switches, rack layout and firewall.
- Deployed 20+ servers in a Windows 2012 environment. Maintained all DNS, DHCP and TCI/IP, Microsoft windows server settings and upgrades.
- Examined and conducted various network and host security logs to detect and resolve issues from the network

SKILLS

- Evaluated network and host-based security logs (Firewalls, NIDS, HIDS, Sys Logs.) to determine correct remediation actions and escalation paths for each incident.
- Knowledge of Secure SDLC (Software development life cycle) such as Agile and Waterfall. Also familiarized web application security architecture.
- Scan and monitor system **vulnerabilities** on servers and infrastructure devices deploying a Threat and Vulnerability security solutions
- Experience in creating reports and how to prevent known vulnerabilities, exploits, **penetration tests** and network attacks Expertise in OWASP Top 10, CWE, SANS vulnerabilities and CIS top 18 critical controls.
- Knowledge of common threat analysis model such as **MITRE's ATT&CK framework**, Diamond Model and Cybersecurity Kill-chains.
- Hands on experience for ongoing review of **SIEM dashboards**, system, application logs, and custom monitoring tools such as Splunk and snort
- Expertise in SPLUNK user accounts (create, delete, update and modify). Conducted overall management of the SPLUNK platform. Examined Splunk to oversee log files, databases, web services, and other types of monitoring end points
- Experienced with Malware Analysis, Threat Analysis and **Cyber Forensics**.
- Experience with Email security protocols to prevent Phishing such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). Identified and remediate Phishing emails with SANS Top 10 SMTP Test Tools to Detect Server Issues and to Test Email Security.
- Proficient with exploits such as Cross-Site Scripting, SQL Injection, Privilege Escalation, Sensitive Data, Exposure, Cross-Site Request Forgery, DOS and Broken Authentication.
- Implemented the Single Sign On, Identity and Access Management solution for OKTA to: Salesforce, Facebook, Zendesk, Office 365, Zoom, Box, Workday, Concur, Tableau, JIRA

Kali Linux Tools

- Depth knowledge of Kali tools such as Metasploit, Burpsuite, Maltego, Hashcat, Dirbuster, harvester and Bettercap

Cybersecurity Frameworks

- Cybersecurity frameworks such as HIPPA, PCI-DSS, NIST CSF, COBIT/CISA, SOC 2, and 3

Network Security and Monitoring

- Analyzed network monitoring and security tools such as NMAP, Wireshark, TShark and Nessus

Windows

- Sysinternals, PowerShell, Windows subsystem for Linux, WMIC, Firewall and Registry

Languages

- Python, Bash, R Programming, HTML, SQL, JavaScript and PHP