Legery Parkman

Phone: (404) 587-1019 | Email: legery39@bellsouth.net | McDonough, Ga 30253
Linkedin: /legery-parkman

Summary

Cybersecurity Specialist with a background in IT. Excellent communication and effectively collaborates with cross-functional teams to ensure goals are achieved. Currently pursuing a Certification in CompTia Security+. Graduate of Cybersecurity Bootcamp through Georgia Tech and with an AWS SAA certification. Proficient in vulnerability analysis, server hardening, and addressing security best practices. Diligent in implementing strategies to prevent exploitations and improve the company security posture.

Certifications

AWS Certified Solutions Architect – Associate
CompTia A+
Security+ (training in progress)

Technical Skills

Operating Systems: Windows, Linux, Ubuntu Linux, Kali Linux
Languages: T-Sql, Bash Scripting, Powershell
Databases: SQL Server, MySQL
Tools: Wireshark, Snort, Cryptography
Cloud: AWS, Azure
SIEMs: Kibana, Splunk

Projects

Final Engagement |
https://drive.google.com/drive/folders/1RgPDzG1XEpwoFNrDpGd61QPrJYb1Ny-d?usp=sharing
Summary: As a Red Team member: enumerated, penetrated, established persistence, and exfiltrated data from a vulnerable network. As a Blue team member: deployed an Elk Stack to create alerts in Kibana to monitor and analyze the Red Team attack and provide recommendations to harden the company's website and network.
Role: Red Team/Blue Team member
Tools: Nmap, John, MySql, Python, Wireshark, Kibana

Red vs Blue | https://drive.google.com/drive/folders/13HXJGHWCGMWWs9UK-HSU8a58v0JT6nMl?usp=sharing
Summary: Performed a security assessment on Capstone's security network using exploitation tools to identify vulnerabilities, analysis, and recommended improvements to their network security.
Role: Pen Tester and group contributor
Tools: Nmap, Hydra, John the Ripper, Metasploit, Kibana

Elk Stack | https://github.com/legery39/Unit13HW
Summary: Created an Elk Stack deployment on Azure with an automated process using Docker containers.
Role: Group contributor.
Tools: Azure, Docker

Experience

nVision Global **05/2020 - Present**
Sr. SQL Database Administrator **McDonough, Ga**

- Introduced and collaborated with senior management to draft a business continuity and disaster recovery policy for the company as well as new client evaluation.
- Created a backup and recovery plan for all SQL servers reducing the chances of data loss.
- Implemented a Change Management process that will ensure accountability for production requests.
- Performed security audits of SQL Servers ensuring they are compliant with the latest patches.

WestRock **06/2012 to 09/2019**
SQL Database Administrator **Norcross, GA**

- Participated in migration projects, server upgrades from hardware to virtualization, saving the company millions in hardware and licensing expenses.
- Administered vulnerability scans on all SQL servers, providing stakeholders and external auditors the assessments.
- Planned and collaborated with cross functional teams to ensure servers were patched and SOX compliant.
- Disabled and removed all user accounts of employees who were terminated and contractors with expired accounts reducing any vulnerability or retaliation attempts.

Ceridian **05/2001 – 5/2012**
SQL Database Administrator **Sandy Springs, GA**

- Processed all user requests requiring access to SQL Server.
- Ensured client's data was protected, available, and encrypted for distribution upon request.
- Implemented database backup plans for any point and time recovery model.
- Collaborated with developers to ensure proper Q&A and change management policies were followed.

Education

Boot Camp Certificate: Georgia Institute of Technology – Atlanta, GA
An intensive 24-week long boot camp. Skills learned: Wireshark, Linux, Cloud Security, Cryptography, Pen Testing, and training towards Security+

A+ Certification, Network+ Certificate: Mercer University ICTS - Atlanta, GA
B.S. Business Administration: Morris Brown College - Atlanta, GA