**BILLY GIBENDI**

**Security Engineer Portfolio**

**Summary**

Dedicated and results-oriented IT Security Professional with 3+ years of experience in safeguarding IT infrastructure and data. Proven track record in identifying and mitigating security threats, conducting incident response investigations, and implementing robust security measures. Committed to protecting sensitive information and delivering exceptional security solutions.

**Featured Projects**

**1. Network Attack Analysis**

Project Description: Analyzed network logs to identify a SYN flood attack targeting a web server. The analysis identified the specific attack type and its impact on the server's functionality.

*Key Achievements:*

* Successfully identified a SYN flood attack as the root cause of network interruptions.
* Explained the mechanisms of SYN flood attacks and their impact on network performance.
* Provided recommendations for mitigating future SYN flood attacks.

**2. Phishing Incident Analysis**

Project Description: Investigated a phishing attempt involving a malicious email attachment claiming to be a resume and cover letter. Analyzed the attachment's hash and confirmed its malicious nature using VirusTotal; a threat intelligence tool.

*Key Achievements:*

* Identified a phishing email targeting the organization.
* Analyzed the malicious attachment and confirmed its threat level.
* Escalated the incident to a level-two SOC analyst for further investigation and containment.

**3. Cybersecurity Incident Response**

Project Description: Took lead in responding to a data breach incident involving the unauthorized access and exfiltration of customer personal identifiable information (PII) and financial information. Conducted a thorough investigation to determine the root cause, scope of the breach, and affected individuals. Implemented effective containment and remediation measures to mitigate further damage and protect sensitive data.

*Key Achievements:*

* Identified the vulnerability in the e-commerce web application that allowed unauthorized access to customer data.
* Collaborated with the public relations department to effectively communicate the incident to affected customers and provide necessary support.
* Implemented robust security controls to prevent similar incidents in the future, including:
* Regular vulnerability scans and penetration testing
* Allowlisting and access control mechanisms
* Enhanced user authentication and authorization

**4. Incident Response and Recovery**

Project Description: Actioned the response to a mock security incident involving unauthorized access to customer data through a phishing attack. Conducted a thorough investigation to identify the root cause, assess the damage, and implement recovery measures.

*Key Achievements:*

* Identified the phishing attack as the method used to gain unauthorized access.
* Assessed the extent of data exposure and the potential impact on customers.
* Implemented new authentication policies to prevent future attacks, including multi-factor authentication and login attempt limits.
* Conducted training for employees on how to protect login credentials.
* Implemented a new protective firewall configuration and invested in an intrusion prevention system (IPS).
* Restored deleted data from a recent backup and notified affected customers of the incident.

**5. File Permissions Management**

Project Description: Conducted a comprehensive review of file and directory permissions to ensure they aligned with organizational security policies. Identified and addressed discrepancies to prevent unauthorized access.

*Key Achievements:*

* Accurately identified existing file and directory permissions using the ls -la command.
* Modified permissions to restrict access to authorized users only.
* Implemented appropriate permissions for hidden files.
* Restricted access to the drafts directory to the researcher2 user.

**Technical Skills**

* Network Security Analysis (TCP/UDP protocols, ICMP)
* Network Traffic Analysis (tcpdump)
* Incident Response Investigation
* Vulnerability Assessment
* Penetration Testing
* Risk Management
* Compliance Management
* File Permissions Management
* Linux Command-Line Interface (CLI), Powershell
* Security Tools (e.g., Nessus, Metasploit, Wireshark, Nmap, VirusTotal)

***Certifications***

AWS Cloud Practitioner: Amazon Web Services Aug 2024

Google Google Cybersecurity Professional: Grow With Google: Identity India May 2024

Cybersecurity Security Operation Analyst (SOA): Cyber Shujaa + Microsoft ADC May 2024

Security, Compliance, and Identity Fundamentals: Microsoft Jan 2023

Cyber Security Analyst: Cyber Shujaa Jan 2023

Certified in Cybersecurity (CC): (ISC)² Jan 2023

***Professional Affiliations***

Kenya Cyber Security & Forensics Association (KCSFA) : Member  
Kenya ICT Action Network (KICTANet): Member