### **Tafara Mutero**

**Skills**

* Strong analytical and problem-solving skills
* Clear written and verbal communication
* Commitment to continuous learning and growth

### **My Values**

* Protecting people and organizations through ethical responsibility
* Ensuring fairness and trust in technology

**Audience**

1. **Interest in cybersecurity**
   * I am fascinated by how cybersecurity safeguards critical systems and data while constantly evolving to outpace threats.
2. **Audience**
   * Cybersecurity recruiters and organizations seeking motivated, entry-level professionals.
3. **Support to organizations**
   * By combining problem-solving skills, communication abilities, and ethical values, I can analyze risks, provide clear solutions, and help maintain trust in secure systems.

**Professional Statement**

I am a motivated and detail-oriented professional with strong analytical and problem-solving skills, excellent communication abilities, and a commitment to continuous learning. I am passionate about cybersecurity because it plays a critical role in protecting people, organizations, and data from evolving threats. Guided by my values of ethical responsibility and fairness, I aim to contribute to building secure and trustworthy systems. My strengths and dedication make me eager to support organizations in achieving their security goals while adapting to the challenges of an increasingly digital world.

PROJECT 2

# **Home Asset Inventory**

### **New Devices Added**

1. **External Hard Drive**
2. **Webcam**
3. **Printer**

### **Asset Inventory Table**

| **Asset** | **Network Access** | **Owner** | **Location** | **Notes** | **Sensitivity** |
| --- | --- | --- | --- | --- | --- |
| External Hard Drive | Occasional (when backing up files) | Business owner | Next to desktop computer | Stores sensitive business data and client files; connects via USB, not always on network. | **Confidential** |
| Webcam | Frequent (whenever video conferencing is active) | Business owner | Attached to desktop computer | Used for video meetings; potential risk if hacked (privacy breach). | **Internal** |
| Printer | Occasional (when printing/scanning) | Business owner | Near router in home office | Connected via Wi-Fi; stores temporary copies of documents, invoices, or IDs. | **Confidential** |

### **Explanation of Classifications**

* **External Hard Drive → Confidential** Because it stores sensitive business and client files. If compromised, data could be stolen or lost.
* **Webcam → Internal** It doesn’t hold files but could compromise privacy if hacked. Needs strong security but is less critical than stored data.
* **Printer → Confidential** Printers often cache or store document data temporarily. If breached, sensitive invoices or personal IDs could leak.

This meets all requirements:

* Three devices added
* Network access, owner, and location listed
* Notes on information type & risks
* Sensitivity classification included

PROJECT 3: Scoring Risk based on their likelihoods

## **Step 1: Notes (2–3 sentences)**

The bank’s funds are at risk due to both human and environmental factors. With 120 employees and a large customer base, insider threats, human error, and cyberattacks like database breaches or phishing are realistic risks. Additionally, supply chain disruptions and theft could severely impact operations, compliance, and customer trust.

## **Step 2: Risk Register with Scores**

| **Risk** | **Description** | **Notes** | **Likelihood (1–3)** | **Severity (1–3)** | **Priority (L x S)** |
| --- | --- | --- | --- | --- | --- |
| Business email compromise | Attackers impersonate employees to steal funds or data via phishing. | Bank employees are frequent targets; phishing is common in financial institutions. | **3** | **3** | **9** |
| Compromised user database | Unauthorized access to customer accounts and data. | High-value target with 2,200 accounts; breach would trigger fines and reputational loss. | **2** | **3** | **6** |
| Financial records leak | Exposure of sensitive financial transactions or account details. | Regulatory violations and trust loss make this a critical risk. | **2** | **3** | **6** |
| Theft | Physical theft of cash or equipment. | Low-crime coastal area, but banks remain a natural theft target. | **1** | **2** | **2** |
| Supply chain attack | Disruption in services or cash delivery. | Coastal location makes weather a factor; third-party vendors add risk. | **2** | **2** | **4** |

## **Step 3: Final Breakdown**

* **Likelihood scores:** 3, 2, 2, 1, 2
* **Severity scores:** 3, 3, 3, 2, 2
* **Overall risk scores (Priority):** 9, 6, 6, 2, 4

This gives the bank a clear **risk prioritization**:

* **Top priority:** Business email compromise (score 9)
* **Medium priority:** Database compromise & financial records leak (scores 6 each)
* **Lower priority:** Supply chain attack (score 4)
* **Lowest priority:** Theft (score 2)

PROJECT 4: DATA RISK ASSESSMENT REVIEW

### **Issue(s)**

The data leak occurred because a manager failed to remove sharing permissions on a confidential folder, giving unnecessary access to an employee. The employee then accidentally shared a link to the entire folder instead of a single file, exposing internal documents to an external partner.

### **Review**

NIST SP 800-53: AC-6 emphasizes the *principle of least privilege*, ensuring users only have access necessary for their duties. It provides guidelines for restricting access rights, preventing privilege escalation, and enforcing separation of duties to minimize data exposure risks.

### **Recommendation(s)**

1. **AC-6 (1) – Authorize Access to Security Functions:** Limit user permissions so only specific roles can access or share sensitive files.
2. **AC-6 (5) – Privileged Accounts:** Implement role-based access control (RBAC) and regular audits to verify that sharing permissions match job requirements.

### **Justification**

These controls ensure employees only have the minimum access necessary and prevent accidental oversharing. By enforcing RBAC and conducting regular access reviews, the company can detect and remove unnecessary permissions, reducing the likelihood of future data leaks.

PROJECT 5: IMPROVE AUTHENTICATION

### **Access Control Worksheet**

#### **Notes about the user**

1. The event log shows that the suspicious login occurred from an **unfamiliar IP address** outside normal business hours.
2. The login credentials used belonged to **a former employee** who no longer works at the company, suggesting their account was never deactivated.

#### **Access control issues**

1. **Former employees still have active accounts** — access was not revoked when they left the organization.
2. **No multi-factor authentication (MFA)** — access to sensitive financial systems relies only on usernames and passwords, making it easier for attackers to gain entry.

#### **Recommendations for mitigations**

1. **Implement strict account management procedures:** Disable or delete user accounts immediately after an employee leaves the company. Conduct regular audits to ensure only current employees have active credentials.
2. **Enable multi-factor authentication (MFA):** Require MFA for all employees accessing financial or sensitive systems to prevent unauthorized access even if passwords are compromised.
3. *(Optional additional recommendation)* — **Use role-based access control (RBAC):** Limit access to sensitive financial data only to staff who need it (e.g., finance team and management).

**Summary:** The incident occurred because a former employee’s credentials were still active and unprotected by MFA. By implementing proper account lifecycle management and stronger authentication methods, the company can prevent similar security breaches in the future.

PROJECT 6: ANALYZING A VULNERABLE SYSTEM

### **Purpose**

The purpose of this vulnerability analysis is to assess the security risks associated with the company’s publicly accessible database server. This server stores valuable customer and business data that employees frequently query to support operations and sales. Because it is open to the public, it poses a major security risk and could easily be exploited by attackers. Conducting this assessment helps the company identify weaknesses, understand the potential business impacts, and develop strategies to secure its data and maintain customer trust.

### **Risk Assessment Table**

| **Threat Source** | **Threat Event** | **Likelihood (1–3)** | **Severity (1–3)** | **Risk (L×S)** |
| --- | --- | --- | --- | --- |
| External hacker | Unauthorized access leading to data breach | 3 | 3 | 9 |
| Insider threat (employee) | Misuse of credentials to alter or leak data | 2 | 3 | 6 |
| System failure or misconfiguration | Accidental data exposure or service outage | 2 | 2 | 4 |

### **Approach**

The selected threats were chosen because they represent the most significant and realistic risks to the company’s operations. External hackers are a major concern due to the public exposure of the database server, making unauthorized access highly likely. Insider threats are included because employees with broad access could intentionally or accidentally compromise data. System failure or misconfiguration is another credible risk since remote work increases the chance of improper settings or accidental exposure. These three threats could all directly harm business continuity, customer trust, and data confidentiality.

### **Remediation**

To mitigate these risks, the company should immediately restrict public access to the database by implementing proper authentication and authorization controls. Access should follow the **principle of least privilege**, ensuring employees only have the permissions they need. The company should deploy **multi-factor authentication (MFA)** for all accounts accessing sensitive systems. Additionally, **network firewalls and intrusion detection systems (IDS)** should be used as part of a **defense-in-depth** strategy. Finally, regular vulnerability scans, audits, and security training should be conducted to maintain a strong security posture and prevent reoccurrence.

PROJECT 7: IDENTIFY ATTACK VECTORS

**Contents:** The USB drive contains both personal and work-related information, including family and pet photos, a new hire letter, and an employee shift schedule. These files may include personally identifiable information (PII) such as names, contact details, and employee data. This combination of personal and professional content makes the drive a potential target for attackers seeking sensitive information.

**Attacker Mindset:** An attacker could use the files to gather intelligence about Jorge or the hospital. They could use employee data to craft phishing emails or social engineering attacks targeting staff. The attacker might have intentionally planted the USB to gain unauthorized access to the hospital’s systems once someone plugged it in.

**Risk Analysis:** USB baiting attacks can deliver malware such as ransomware, spyware, or keyloggers that compromise sensitive data or control systems. If another employee had plugged in the device, it could have infected the hospital’s network. To mitigate these risks, the hospital should implement **technical controls** like USB port restrictions and antivirus scanning, **operational controls** such as staff cybersecurity awareness training, and **managerial controls** like clear data handling policies and incident response procedures.

PROJECT 8: APPLYING THE PASTA MODEL

### **Stage I – Business Objectives**

1. Enable users to easily **buy and sell sneakers**, including secure account management, login, and messaging between buyers and sellers.
2. Ensure **data privacy and user trust** by handling personal and financial information responsibly.
3. Provide a **smooth checkout process** with multiple secure payment options to comply with financial regulations.

### **Stage 2 – Technological Scope**

I would first evaluate the **API**, since it’s the main communication channel between the app, the database, and third-party services. APIs are often targeted through poorly configured endpoints, insecure authentication, or data exposure. Evaluating API security helps ensure user data and payment information are protected from interception or manipulation.

### **Stage 3 – Information Analysis**

The app collects, transmits, and stores sensitive user data such as login credentials, messages, and payment details. Data flows between the user’s device, the API, and the backend SQL database. Encryption (AES/RSA) and hashing (SHA-256) must be applied at all points of transmission and storage to maintain confidentiality and integrity.

### **Stage 4 – Threat Analysis**

1. **SQL injection attacks** exploiting weaknesses in input validation to access or manipulate database information.
2. **Man-in-the-middle (MITM) attacks** during data transmission between the app and server if encryption keys are improperly implemented or expired.

### **Stage 5 – Vulnerability Analysis**

1. **Unsecured API endpoints** that allow unauthorized data requests or privilege escalation.
2. **Weak input validation** on login or payment forms that could enable injection attacks or cross-site scripting (XSS).

### **Stage 6 – Attack Tree Summary**

Threat actors might start by probing the API for open endpoints or weak authentication, then inject malicious SQL commands to extract user data, modify transactions, or deploy malware through compromised communication channels.

### **Stage 8 – Security Controls / Defenses**

1. Implement **multi-factor authentication (MFA)** for users and administrators.
2. Use **input validation and prepared statements** to prevent SQL injections.
3. Apply **TLS encryption** for all data in transit and **AES-256** for data at rest.
4. Conduct regular **security audits, vulnerability scans, and patch management** to identify and fix new threats.

PROJECT 9: DOCUMENTING AN INCIDENT

### **Incident Handler’s Journal**

**Date:** October 8, 2025  
 **Entry #:** 1

**Description:** This entry documents a ransomware attack that occurred at a small U.S. health care clinic, which led to the encryption of patient data and disruption of business operations. The incident originated from a phishing email campaign targeting clinic employees.

**Tool(s) Used:** No tools were directly used during this stage of documentation. (Future tools may include malware analysis tools, antivirus software, and email filtering systems for investigation and prevention.)

### **The 5 W’s**

**Who caused the incident?** An organized group of unethical hackers known for targeting healthcare and transportation industries.

**What happened?** The attackers sent phishing emails containing a malicious attachment that, once downloaded, deployed ransomware. The ransomware encrypted critical files across the clinic’s systems, locking employees out of their data and displaying a ransom note demanding payment.

**When did the incident occur?** The attack occurred on a Tuesday morning at approximately 9:00 a.m.

**Where did the incident happen?** At a small health care clinic in the United States.

**Why did the incident happen?** The incident happened because employees fell victim to phishing emails that bypassed security awareness and controls, allowing malware to be downloaded and executed on the system.

**Additional Notes:** This incident highlights the importance of employee cybersecurity awareness and email filtering systems. Implementing regular phishing simulations, data backups, and stronger endpoint protection could help prevent or reduce the impact of similar attacks in the future. I’d like to explore which ransomware variant was used and whether the clinic had an existing incident response plan before the event.

PROJECT 10- NETWORK PROTOCOL ANALYZERS

### **Wireshark vs tcpdump Comparison Chart**

| **Category** | **Wireshark** | **tcpdump** |
| --- | --- | --- |
| **User Interface** | Has a **graphical user interface (GUI)** that visually displays packets and network flows. | Operates through a **command-line interface (CLI)**; no graphical display. |
| **Primary Use Case** | Ideal for **in-depth packet analysis** with filtering, decoding, and visualization. | Best for **quick packet capture and basic inspection** directly from the terminal. |
| **Features** | - Can display **detailed protocol breakdowns** and follow TCP streams.  - Supports exporting data in multiple formats for reports.  - Real-time and offline packet analysis. | - Can **capture packets efficiently** with minimal system resources.  - Allows **saving captures** to .pcap files for later analysis.  - Supports **complex capture filters**. |
| **Installation & Accessibility** | Open-source software available on Windows, macOS, and Linux. Requires GUI support. | Also open-source, pre-installed or easily available on most Unix/Linux systems. |
| **Usage Scenario** | Used by analysts who need **visual insights** into packet data and network issues. | Used by analysts or admins for **lightweight, quick packet capture or automation** tasks. |
| **Limitations** | Can be **resource-intensive** during live captures; requires GUI environment. | Has a **steeper learning curve** for beginners due to CLI syntax; lacks visualization. |

### **Similarities Between Wireshark and tcpdump**

1. Both are **open-source** network protocol analyzers used for capturing and analyzing packets.
2. Both can **save and read .pcap files**, allowing captures to be shared between tools.
3. Both support **powerful filtering options** (using display filters or capture filters) to isolate specific network traffic.

**Summary:**

* **Wireshark** = Visual, detailed, user-friendly for deep packet analysis.
* **tcpdump** = Lightweight, text-based, ideal for scripting and quick diagnostics.

PROJECT 11: INCIDENT HANDLERS JOURNAL

## **Incident Handler’s Journal (Final Submission Example)**

## **Name: Tafara Mutero**

## **Role: Level-One SOC Analyst (Trainee)**

### **Entry #1 – Investigating a Phishing Alert**

**Date:** 2025-10-08  
 **Description:** Investigated a phishing alert involving a suspicious email attachment downloaded by an employee. Used the phishing playbook to verify that the file’s hash was malicious. Documented alert details, analyzed sender information, and determined escalation was required.  
 **NIST Phase:** Detection and Analysis  
 **The 5 W’s:**

* **Who:** An employee in the finance department.
* **What:** Downloaded a malicious attachment from a phishing email.
* **When:** Detected on 2025-10-08 at 10:35 AM.
* **Where:** Employee workstation within internal network.
* **Why:** The attacker used social engineering to impersonate a trusted vendor.  
   **Outcome:** Escalated alert for containment and eradication due to confirmed malware.

### **Entry #2 – Investigating a Data Breach Report**

**Date:** 2025-10-06  
 **Description:** Reviewed the final report of a major data breach affecting over one million users. Identified root cause, attack method, and response actions taken by the company. Summarized recommendations to strengthen data protection.  
 **NIST Phase:** Post-Incident Activity  
 **The 5 W’s:**

* **Who:** External threat actor exploiting e-commerce vulnerability.
* **What:** Data breach resulting in theft of user information.
* **When:** Incident occurred on 2025-09-28.
* **Where:** Company’s e-commerce web server.
* **Why:** Vulnerable web application due to missing access control mechanisms.  
   **Outcome:** Recommended implementing access control, routine vulnerability scans, and staff training.

### **Entry #3 – Using Wireshark to Analyze Network Traffic**

**Date:** 2025-09-30  
 **Description:** Used **Wireshark** to capture and analyze network packets. Learned how to identify packet headers, protocols, and suspicious traffic patterns. Practiced filtering HTTP and TCP packets to spot anomalies in transmitted data.  
 **Tool(s) Used:**

* **Wireshark:** Used to monitor and capture live network packets.
* Applied filters to isolate suspicious traffic (e.g., http and tcp.port==80).
* Analyzed packet payloads for signs of malicious activity or data exfiltration.  
   **Outcome:** Improved ability to recognize abnormal traffic and understand how protocol analyzers detect threats.

### **Entry #4 – Performing Queries with Splunk and Chronicle**

**Date:** 2025-10-04  
 **Description:** Explored **Splunk** and **Google Chronicle** for log analysis and threat detection. Learned how to query logs using SPL and UDM to identify suspicious login attempts. Compared both tools’ approaches to normalization and visualization.  
 **Tool(s) Used:**

* **Splunk:** Used SPL queries to filter authentication logs for failed login attempts.
* **Chronicle:** Used UDM to correlate data from multiple log sources.
* Both tools provided strong visualization for incident detection.  
   **Outcome:** Gained practical experience in using SIEM platforms to monitor, analyze, and respond to security events.

### **Reflections / Notes**

**Were there any specific activities that were challenging for you? Why or why not?** The phishing alert investigation was challenging because it required careful attention to email details and file hash verification. It helped me develop a more analytical and investigative mindset.

**Has your understanding of incident detection and response changed since taking this course?** Yes. I now understand that incident response involves multiple phases, not just identifying threats but also documenting, containing, and learning from them. Each phase is critical to reducing risk and improving future defenses.

**Was there a specific tool or concept that you enjoyed the most? Why?** I enjoyed working with Splunk because of its real-time data analysis and visualization capabilities. It made identifying patterns and correlating events across multiple log sources easier and more engaging.

**Final Checklist (Meets Requirements):**

* 4 journal entries
* 2 entries include “5 W’s” (incident investigations)
* 2 entries include “Tool(s) used”
* Reflections section completed (6–9 sentences total)
* Proper spelling, grammar, and clear formatting