Cybersecurity Portfolio

Created by Jathushan Karthigesar

What interests you most about a career in cybersecurity? Ensuring data protection

What do you want to learn more about in the field of cybersecurity? Ethical hacking and penetration testing

What do you hope to achieve as a cybersecurity analyst? Protection of an organization and its people

Strengths (3-5): collaboration, problem-solving, communication, time management, programming

Values (2-3): protecting organizations (commitment to helping organizations ensure confidential data is safe), protecting people (upholding an individual's right to privacy), ensuring equitable access

Core statement:

I am efficient in problem-solving and communication. I am also driven by cybersecurity.

I value protecting organizations. I am committed to helping organizations ensure confidential data is safe and protecting the people it serves.

Questions:
1. What am I most passionate about in the field of cybersecurity? Protection of organizational data

2. What would I like to be known for after I enter the field? Security Enhancement

3. Who is the audience for my professional statement (e.g., cybersecurity recruiters, specific organizations, government employers, etc.)? cybersecurity recruiters, specific organizations, government employers

4. **What differentiates me from my peers?** Dedication

5. **What do I have to offer potential employers that is unique?** Dedication

Professional Statement: (explains your strengths, values, and interest in the cybersecurity profession)

My name is Jathushan Karthigesar. I am driven by cybersecurity and enjoy contributing to solutions that can positively impact an organization and the people it serves. I like working with technology and analyzing and solving complex problems.

Controls assessment

To review control categories, types, and the purposes of each, read the control categories document.

Current assets

Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- Legacy system maintenance: end-of-life systems that require human monitoring

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	X	high
Disaster recovery	Corrective; business continuity	X	high

Administrative Controls			
plans	to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration		
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	high
Access control policies	Preventative; increase confidentiality and integrity of data	X	high
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	X	high
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	X	high

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	N/A	N/A
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	high
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	high
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	high
Password management system	Corrective; password recovery, reset, lock out notifications	X	high
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	high
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	high

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	X	Medium
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	Medium
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	High
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	Medium
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	Low
Locks	Preventative; physical and digital assets are more secure	X	High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	X	Medium

Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance document.

- ☐ **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

  The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

  Explanation:

- ☑ **General Data Protection Regulation (GDPR)**

  GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

  Explanation: The manager is also interested in conducting business in the European Union (E.U.).

- ☑ **Payment Card Industry Data Security Standard (PCI DSS)**

  PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: The manager is also interested in ensuring that they comply with regulations related to accepting online payments.

☐ **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation:

☐ **System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation:

Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

- Scope
- Goals
- Critical findings (must be addressed immediately)
- Findings (should be addressed, but no immediate need)
- Summary/Recommendations

Use information from the following documents:

- Botium Toys: Audit scope and goals
- Controls assessment (completed in “Conduct a security audit, part 1”)
- Compliance checklist (completed in “Conduct a security audit, part 1”)

[***Use the following template to create your memorandum]***

TO: IT Manager, Stakeholders
FROM: (Jathushan Karthigesar)
DATE: (Today’s Date)
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:
Botium Toys internal IT audit will assess the following:
● Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event

Management (SIEM) tool.
● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Ensure current user permissions, controls, procedures, and protocols in place align with align with PCI DSS and GDPR compliance requirements.
● Ensure current technology is accounted for. Both hardware and system access.

Goals:
The goals for Botium Toys' internal IT audit are:
● To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
● Establish a better process for their systems to ensure they are compliant
● Fortify system controls
● Implement the concept of least permissions when it comes to user credential management
● Establish their policies and procedures, which includes their playbooks
● Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):
The following must be implemented right away to ensure business continuity and compliance.

General Data Protection Regulation (GDPR)
Explanation: Botium Toys needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.

Payment Card Industry Data Security Standard (PCI DSS)
Explanation: Botium Toys needs to adhere to PCI DSS because they store, accept, process, and transmit credit card information in person and online.

System and Organizations Controls (SOC type 1, SOC type 2)
Explanation: Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	X	High
Disaster recovery plans	Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration	X	High
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	High
Access control policies	Preventative; increase confidentiality and integrity of data	X	High
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	X	High
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	X	High

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	High
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	High
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	High
Password management system	Corrective; password recovery, reset, lock out notifications	X	High
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	High
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	X	High

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	High
Locks	Preventative; physical and digital	X	High

	assets are more secure		

Findings (should be addressed, but no immediate need):

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	X	Medium/ Low
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	Medium/ Low
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	Medium
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	Low
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	X	Medium/ Low

The above must be addressed - but no immediate need - to ensure business continuity and compliance.

Summary/Recommendations:

The scope is to assess the current user permissions set, the current implemented controls, and the current procedures and protocols set. It is also ensure current user permissions, controls, procedures, and protocols are in place align with necessary compliance requirements; and to ensure current technology is accounted for both hardware and system access.

The audit's goal is to provide an overview of the risks the company might experience due to the current state of their security posture.

Thus, I recommend immediately implementing compliance with the mentioned policies (General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and System and Organizations Controls (SOC type 1, SOC type 2)) and the controls mentioned in “Critical findings”. The controls in the “Findings” should be addressed, but no immediate need.

This audit helps better secure the company’s infrastructure and helps identify and mitigate potential risks, threats, or vulnerabilities to critical assets.

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that udp port 53 is unreachable when attempting to access the secure company website www.yummyrecipesforme.com. This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53 is normally used for for DNS service. This may indicate that the message did not go through to the DNS server. Thus, my browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”

Part 2: Explain your analysis of the data and provide one solution to implement
Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. Then, I visited the company website and also received the error “destination port unreachable.” I loaded tcpdump and loaded the webpage again. This time, I receive a lot of packets in my network analyzer. The analyzer shows that when I send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.” We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the DNS server to have them check the system for signs of an attack. It is possible that a certain new hire may want to keep customers

fromaccessing the website. This person might have launched an attack to crash the company website.

Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Malicious actor is taking advantage of the TCP protocol by flooding the server with SYN packet requests for the first part of the handshake. Since the number of SYN requests is greater than the server resources available to handle the requests, the server is overwhelmed and unable to respond to the requests. This is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. This SYN flood attack simulates a TCP connection and floods the server with SYN packets. This DoS direct attack originates from a single source.

Section 2: Explain how the attack is causing the website to malfunction
Initially, the attacker's SYN request is answered normally by the web server (log items 52-54). However, the attacker keeps sending more SYN requests, which is abnormal. At this point, the web server is still able to respond to normal visitor traffic, which is highlighted and labeled as green. An employee visitor with the IP address of 198.51.100.14 successfully completes a SYN/ACK connection handshake with the webserver (log item nos. 55, 56, 58). Then, the employee's browser requests the sales.html webpage with the GET command and the web server responds (log item no. 60 and 62). In the next 20 rows, the log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace. The attacker is sending several SYN requests every second. The rows highlighted and labeled yellow are failed communications between legitimate employee website visitors and the web server. The two types of errors in the logs include: ● An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser. ● An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will receive a timeout error message in their browser

and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request.

The web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood attack.

Security incident report

Section 1: Identify the network protocol involved in the incident
Application layer: HTTP protocol (The log entry with the code HTTP: GET / HTTP/1.1 shows the browser is requesting data from yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. This could be the download request for the malicious file.)

Section 2: Document the incident
The first section of the DNS & HTTP traffic log file shows the source computer (your.machine.52444) using port 52444 to send a DNS resolution request to the DNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL (203.0.113.22). The next section shows the source computer sending a connection request (Flags [S]) from the source computer (your.machine.36086) using port 36086 directly to the destination (yummyrecipesforme.com.http). The .http suffix is the port number; http is commonly associated with port 80. The reply shows the destination acknowledging it received the connection request (Flags [S.]). The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (14:18) and the next DNS resolution request (see below for the 14:20 timestamp). The log entry with the code HTTP: GET / HTTP/1.1 shows the browser is requesting data from yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. This could be the download request for the malicious file. Then, a sudden change happens in the logs. The traffic is routed from the source computer to the DNS server again using port .52444

(your.machine.52444 > dns.google.domain) to make another DNS resolution request. This time, the DNS server routes the traffic to a new IP address (192.0.2.172) and its associated URL (greatrecipesforme.com.http). The traffic changes to a route between the source computer and the spoofed website (outgoing traffic: IP your.machine.56378 > greatrecipesforme.com.http and incoming traffic: greatrecipesforme.com.http > IP your.machine.56378). Note that the port number (.56378) on the source computer has changed again when redirected to a new website.

Section 3: Recommend one remediation for brute force attacks
Enforcing two-factor authentication (2FA): extra protection layer to bring brute force attacks to failure.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. The organization’s employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used. Password policies, Firewall, MFA

Part 2: Explain your recommendations
Use MFA Effectif because: MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. Offer extra layers of security How often: Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained. Everytime a person tries to log in, he has provide another authentication which causes brute force attacks to fail. Use Firewall Maintenance Effectif because: Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. How Often: This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.

Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	I am a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. My organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, my organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. Upon initial review, this vulnerability allowed the malicious attacker to overwhelm the company's network through a

	distributed denial of service (DDoS) attack. The organization experienced a DDoS attack, which compromised the internal network.
Protect	The network security team has implemented the following to prevent similar events in the future: - A new firewall rule to limit the rate of incoming ICMP packets - Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets - Network monitoring software to detect abnormal traffic patterns - An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	To filter out some ICMP traffic based on suspicious characteristics, the team will use a firewall rule and an intrusion detection system (IDS) to monitor all incoming ICMP traffic from non-trusted IP addresses.
Respond	The incident management team responded to the incident by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. We provided training to employees on how to protect the company's network against ICMP flood and DDOS attacks in the future. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the internal network by restoring critical and non-critical network services.

Reflections/Notes:

Apply filters to SQL queries

Project description

First, you'll retrieve all failed login attempts after business hours. Second, you'll retrieve all login attempts that occurred on specific dates. Third, you'll retrieve logins that didn't originate in Mexico. Then you'll retrieve information about certain employees in the Marketing department, you'll retrieve information about employees in the Finance or the Sales department, and you'll obtain information about employees who are not in the Information Technology department.

Retrieve after hours failed login attempts

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the log_in_attempts table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to return the rows where the value is 0 in the success column and the values are greater than 6h00 pm in the login_time column, simultaneously.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |       0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200  |       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232  |       0 |
+----------+----------+------------+------------+---------+-----------------+---------+
19 rows in set (0.176 sec)
```

Retrieve login attempts on specific dates

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the log_in_attempts table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to return the rows where the value in the login_date column is either 2022-05-09 or 2022-05-08.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-08' OR login_date = '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151  |       1 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.42   |       1 |
|       39 | yappiah  | 2022-05-09 | 07:56:40   | MEXICO  | 192.168.57.115  |       1 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208  |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.144 |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.24  |       1 |
|       49 | asundara | 2022-05-08 | 14:00:01   | US      | 192.168.173.213 |       0 |
|       53 | nmason   | 2022-05-08 | 11:51:38   | CAN     | 192.168.133.188 |       1 |
|       56 | acook    | 2022-05-08 | 04:56:30   | CAN     | 192.168.209.130 |       1 |
|       58 | ivelasco | 2022-05-09 | 17:20:54   | CAN     | 192.168.57.162  |       0 |
|       61 | dtanaka  | 2022-05-09 | 09:45:18   | USA     | 192.168.98.221  |       1 |
|       65 | aalonso  | 2022-05-09 | 23:42:12   | MEX     | 192.168.52.37   |       1 |
|       66 | aestrada | 2022-05-08 | 21:58:32   | MEX     | 192.168.67.223  |       1 |
|       67 | abernard | 2022-05-09 | 11:53:41   | MEX     | 192.168.118.29  |       1 |
|       68 | mrah     | 2022-05-08 | 17:16:13   | US      | 192.168.42.248  |       1 |
|       70 | tmitchel | 2022-05-09 | 10:55:17   | MEXICO  | 192.168.87.199  |       1 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169  |       0 |
|       72 | alevitsk | 2022-05-08 | 12:09:10   | CANADA  | 192.168.139.176 |       1 |
|       79 | abernard | 2022-05-09 | 11:41:15   | MEX     | 192.168.158.170 |       0 |
|       80 | cjackson | 2022-05-08 | 02:18:10   | CANADA  | 192.168.33.140  |       1 |
```

Retrieve login attempts outside of Mexico

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the log_in_attempts table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to return the rows where the value is NOT like MEX% in COUNTRY column where % can represent zero, one, or multiple characters. In the log_in_attempts table, Mexico is written as

MEXICO or MEX.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT  country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.245 |       1 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.147 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |       1 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.186  |       0 |
|       31 | acook    | 2022-05-12 | 17:36:45   | CANADA  | 192.168.58.232  |       0 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |       0 |
|       33 | zbernal  | 2022-05-11 | 02:52:10   | US      | 192.168.72.59   |       1 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151  |       1 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.42   |       1 |
|       41 | apatel   | 2022-05-10 | 17:39:42   | CANADA  | 192.168.46.207  |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.208  |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.144 |       0 |
|       45 | dtanaka  | 2022-05-11 | 10:28:54   | US      | 192.168.223.157 |       1 |
```

Retrieve employees in Marketing

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the employee table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to return the rows where the value is Marketing in the DEPARTMENT column and the value is like

EAST% in OFFICE column , simultaneously. % can represent zero, one, or multiple characters.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
7 rows in set (0.001 sec)
```

Retrieve employees in Finance or Sales

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the employee table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to

return the rows where the value is either Finance or Sales in the DEPARTMENT column.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215   |
|        1025 | z381a365b233 | jhill    | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
|        1035 | j236k3031245 | bisles   | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin | Sales      | North-208   |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
|        1045 | t567u844v434 | pwashing | Finance    | East-115    |
|        1046 | u429v921w138 | daquino  | Finance    | West-280    |
|        1047 | v109w587x644 | cward    | Finance    | West-373    |
|        1048 | w167x592y375 | tmitchel | Finance    | South-288   |
|        1049 | NULL         | jreckley | Finance    | Central-295 |
|        1050 | y132z930a114 | csimmons | Finance    | North-468   |
|        1057 | f370g535h632 | mscott   | Sales      | South-270   |
|        1062 | k3671639m697 | redwards | Finance    | North-180   |
|        1063 | l686m140n569 | lpope    | Sales      | East-226    |
|        1066 | o678p794q957 | ttyrell  | Sales      | Central-444 |
|        1069 | NULL         | jpark    | Finance    | East-110    |
|        1071 | t244u829v723 | zdutchma | Sales      | West-348    |
|        1072 | u905v920w694 | esmith   | Sales      | East-421    |
|        1076 | y347z204a710 | fgarcia  | Finance    | Central-270 |
|        1078 | a667b270c984 | sharley  | Sales      | North-418   |
|        1081 | d647e310f618 | qcorbit  | Finance    | South-290   |
```

Retrieve all employees not in IT

The first 3 lines are my query. Line 1 = Select all columns. Line 2 = Select the columns from the employee table. Line 3 is where we apply the filter after the WHERE keyword. Line 3 tells to

return the rows where the value is NOT Information Tecnology in the DEPARTMENT column.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
+-------------+-------------+----------+-----------------+-------------+
| employee_id | device_id   | username | department      | office      |
+-------------+-------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
|        1003 | d394e816f943 | sgilmore | Finance         | South-153   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127   |
|        1005 | f551g340h864 | gesparza | Human Resources | South-366   |
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406   |
|        1008 | i858j583k571 | abernard | Finance         | South-170   |
|        1009 | NULL         | lrodriqu | Sales           | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance         | South-109   |
|        1011 | l748m120n401 | drosas   | Sales           | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance         | North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources | North-229   |
|        1017 | r550s824t230 | jclark   | Finance         | North-188   |
|        1018 | s310t540u653 | abellmas | Finance         | North-403   |
|        1020 | u899v381w363 | arutley  | Marketing       | South-351   |
|        1022 | w237x430y567 | arusso   | Finance         | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales           | South-215   |
|        1025 | z381a365b233 | jhill    | Sales           | North-115   |
|        1026 | a998b568c863 | apatel   | Human Resources | West-320    |
|        1027 | b806c503d354 | mrah     | Marketing       | West-246    |
|        1028 | c603d749e374 | aestrada | Human Resources | West-121    |
|        1029 | d336e475f676 | ivelasco | Finance         | East-156    |
|        1030 | e391f189g913 | mabadi   | Marketing       | West-375    |
|        1031 | f419g188h578 | dkot     | Marketing       | West-408    |
|        1034 | i679j565k940 | bsand    | Human Resources | East-484    |
|        1035 | j236k3031245 | bisles   | Sales           | South-171   |
|        1036 | k550l533m205 | rjensen  | Marketing       | Central-239 |
|        1038 | m873n636o225 | btang    | Human Resources | Central-260 |
|        1039 | n253o917p623 | cjackson | Sales           | East-378    |
|        1040 | o783p832q294 | dtarly   | Human Resources | East-237    |
|        1041 | p929q222r778 | cgriffin | Sales           | North-208   |
|        1042 | q175r338s833 | acook    | Human Resources | West-381    |
```

Summary

I had to obtain specific information about employees, their machines, and the departments they belong to from the database. My team needed data to investigate potential security issues and to update computers. I was responsible for filtering the required information from the database.

File permissions in Linux

Project description

In this project, I must examine and manage the permissions on the files in the /home/researcher2/projects directory for the researcher2 user.

The researcher2 user is part of the research_team group.

I must check the permissions for all files in the directory, including any hidden files, to make sure that permissions align with the authorization that should be given. When it doesn't, I must change the permissions.

Check file and directory details

command I can use to check permissions:
Ls -l : permission for files and subdirectories without the hidden files/directories
Ls -la : permission for files and subdirectories including the hidden files/directories

```
researcher2@936387a35758:~$ pwd
/home/researcher2
researcher2@936387a35758:~$ cd projects
researcher2@936387a35758:~/projects$ ls -l
total 20
drwx--x--- 2 researcher2 research_team 4096 Jun 29 22:22 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jun 29 22:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_t.txt
researcher2@936387a35758:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 22:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 23:19 ..
-rw--w---- 1 researcher2 research_team   46 Jun 29 22:22 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jun 29 22:22 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jun 29 22:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_t.txt
researcher2@936387a35758:~/projects$
```

Describe the permissions string

Example:

```
drwx--x--- 2 researcher2 research_team 4096 Jun 29 22:22 drafts
```

Short description that explains the 10-character string:
This string is to indicate the permission for a directory or file, for the following owner types: user, group and other.

1st Character = file type
- `d` for directory
- `-` for a regular file

2nd Character = read permissions for the user
- `r` if the user has read permissions
- `-` if the user lacks read permissions

3rd Character = write permissions for the user
- `w` if the user has write permissions
- `-` if the user lacks write permissions

4th Character = execute permissions for the user
- `x` if the user has execute permissions
- `-` if the user lacks execute permissions

5th Character = read permissions for the group
- `r` if the group has read permissions
- `-` if the group lacks read permissions

6th Character = write permissions for the group
- `w` if the group has write permissions
- `-` if the group lacks write permissions

7th Character = execute permissions for the group
- `x` if the group has execute permissions
- `-` if the group lacks execute permissions

8th Character = read permissions for the other
- `r` if the other has read permissions
- `-` if the other lacks read permissions

9th Character = write permissions for the other
- `w` if the other has write permissions
- `-` if the other lacks write permissions

10th Character = execute permissions for the other

- `x` if the other has execute permissions
- `-` if the other lacks execute permissions

Change file permissions

```
-rw-rw-rw- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
```

To remove the write permission for other, I will use this command:

```
chmod o-w project_k.txt
```

Here is the result:

```
researcher2@936387a35758:~/projects$ chmod o-w project_k.txt
researcher2@936387a35758:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 22:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 23:19 ..
-rw--w---- 1 researcher2 research_team   46 Jun 29 22:22 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jun 29 22:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jun 29 22:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_t.txt
researcher2@936387a35758:~/projects$
```

Change file permissions on a hidden file

The command I will use only allow the read permission for the user and group:

```
chmod u=r--,g=r--,o=--- .project_x.txt
```

The output:

```
researcher2@936387a35758:~/projects$ chmod u=r--,g=r--,o=--- .project_x.txt
researcher2@936387a35758:~/projects$ ls la
ls: cannot access 'la': No such file or directory
researcher2@936387a35758:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 22:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 23:19 ..
-r--r----- 1 researcher2 research_team   46 Jun 29 22:22 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jun 29 22:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jun 29 22:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_t.txt
researcher2@936387a35758:~/projects$
```

Change directory permissions

The command I will use to only allow the execute permission for the user:

```
researcher2@936387a35758:~/projects$ chmod g-x drafts
```

The output:

```
researcher2@936387a35758:~/projects$ chmod g-x drafts
researcher2@936387a35758:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 22:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Jun 29 23:19 ..
-r--r----- 1 researcher2 research_team   46 Jun 29 22:22 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Jun 29 22:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Jun 29 22:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Jun 29 22:22 project_t.txt
researcher2@936387a35758:~/projects$
```

Summary

First, I checked the user and group permissions for all files in the projects directory. Next, I checked whether any files have incorrect permissions and change the permissions as needed. Finally, I checked the permissions of the /home/researcher2/projects/drafts directory and modified these permissions to remove any unauthorized access.

Risk register

Operational environment:

The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure their data and funds, like having enough cash available each day to meet Federal Reserve requirements.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	3	6
	Compromised user database	*Customer data is poorly encrypted.*	1	3	3
	Financial records leak	*A database server of backed up data is publicly accessible.*	1	3	3
	Theft	*The bank's safe is left unlocked.*	2	2	4
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* Due to malicious attacker and human error, these risks can occur: Business email compromise and theft. Due to natural hazards, these risks can occur: Compromised user database, and Financial records leak. Due to environmental hazards, Supply chain disruption can occur.				

Asset: The asset at risk of being harmed, damaged, or stolen.
Risk(s): A potential risk to the organization's information systems and data.
Description: A vulnerability that might lead to a security incident.

Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.
Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.
Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

Sample risk matrix

Likelihood	Severity: Low 1	Severity: Moderate 2	Severity: Catastrophic 3
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3

Data leak worksheet

Incident summary: A sales manager shared access to a folder of internal-only documents with their team during a meeting. The folder contained files associated with a new product that has not been publicly announced. It also included customer analytics and promotional materials. After the meeting, the manager did not revoke access to the internal folder, but warned the team to wait for approval before sharing the promotional materials with others.

During a video call with a business partner, a member of the sales team forgot the warning from their manager. The sales representative intended to share a link to the promotional materials so that the business partner could circulate the materials to their customers. However, the sales representative accidentally shared a link to the internal folder instead. Later, the business partner posted the link on their company's social media page assuming that it was the promotional materials.

Control	**Least privilege**
Issue(s)	*What factors contributed to the information leak?* The manager forgot to unshare a folder with the rep. This contained files associated with a new product offering, including customer analytics and marketing material. The representative unintentionally shared a link to the entire folder instead of only sending the link to the marketing materials with a customer during a sales call.
Review	*What does NIST SP 800-53: AC-6 address?* It defines the security control known as Least Privilege (PoLP). It provides a description of how the control should be implemented. Also provides a list of suggestions to improve the effectiveness of the control.

Recommendation(s)	*How might the principle of least privilege be improved at the company?* ● Restrict access to sensitive resources based on user role. ● Automatically revoke access to information after a period of time.
Justification	*How might these improvements address the issues?* Restrict access to sensitive resources based on user role: The rep will only hav access to the info he requires to perform his task, thus maintaining PoLP and reducing the likelihood of another data leak. Automatically revoke access to information after a period of time: This could have removed access to the entire folder or the other sections of the folder that the rep did not need to complete his tasks, thus maintaining PoLP and reducing the likelihood of another data leak.

Security plan snapshot

The NIST Cybersecurity Framework (CSF) uses a hierarchical, tree-like structure to organize information. From left to right, it describes a broad security function, then becomes more specific as it branches out to a category, subcategory, and individual security controls.

Function	Category	Subcategory	Reference(s)
Protect	PR.DS: *Data security*	PR.DS-5: *Protections against data leaks*.	NIST SP 800-53: AC-6

In this example, the implemented controls that are used by the manufacturer to protect against data leaks are defined in NIST SP 800-53—a set of guidelines for securing the privacy of information systems.

Note: References are commonly hyperlinked to the guidelines or regulations they relate to. This makes it easy to learn more about how a particular control should be implemented. It's common to find multiple links to different sources in the references columns.

NIST SP 800-53: AC-6

NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories. Each control provides a few key pieces of information:

- **Control:** A definition of the security control.
- **Discussion:** A description of how the control should be implemented.
- **Control enhancements:** A list of suggestions to improve the effectiveness of the control.

AC-6	**Least Privilege**
	Control: Only the minimal access and authorization required to complete a task or function should be provided to users.
	Discussion: Processes, user accounts, and roles should be enforced as necessary to achieve least privilege. The intention is to prevent a user from operating at privilege levels higher than what is necessary to accomplish business objectives.
	Control enhancements: • Restrict access to sensitive resources based on user role. • Automatically revoke access to information after a period of time. • Keep activity logs of provisioned user accounts. • Regularly audit user privileges.

Note: In the category of access controls, SP 800-53 lists least privilege sixth, i.e. AC-6.

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* ● *When did it occur?* ● *What device was used?* *A Legal\Administrator user caused this incident at 8:29:57 AM on 10/03/2023. The user used a Up2-NoGud computer (IP: 152.207.255.255).*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* *The user has an admin level of access and shouldn't have that level of access since he is a legal attorney. Their account should be deactivated since the end date as an employee is 12/27/2019.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* *Have procedures in place to revoke access to files when an employee is no longer with the company.* *Use MFA for authentication.*

Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The reason for this vulnerability assessment;

- *The company stores information on a remote database server, since many of the employees work remotely from locations all around the world.*
- *Employees of the company regularly query, or request, data from the server to find potential customers.*
- *If the server was disabled, then the employees wouldn't be able to request data from it and the company's business operations would come to an end unless they find a solution.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*
Business	*Alter/Delete critical information*	*1*	*3*	*3*

partner				

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

The threat sources that I chose are Competitor, Hacker, and *Business partner because the server is publicly available. Competitiors and Hackers are obvious threat sources. A Business partner is a non-obvious threat source worth mentioning because they can become competitors/traitors if they benefit from it.*

The threat events that I chose are Obtain sensitive information via exfiltration, Conduct Denial of Service (DoS) attacks and Alter/Delete critical information; I chose these since these events have a high probability of damaging business operations.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

We should use Principle of least privilege and Multi-factor authentication (MFA) to only permit the employees access the database server.

We should implement Defense in depth, by adding different layers of protection in order to protect the business operation and the CIA triad of the data in the database.

We should Authentication, Authorization, Accounting (AAA) framework to authenticate employees and authorize them to access the server and to monitor the activities in the server to ensure that only authorized employees are conducting them without misconduct.

Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* *There are files that contain PII such as a new hire letter and a resume. There is a sensitive work file such as the employee shift schedule. It is not safe to store personal files with work files since attackers can easily use this sensitive information to target the data owner or others around them.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* *The information can be used against employees by mimicking them to gain access to their accounts (commit fraud) or in other ways since the device contains information on shift schedules, employee budgets and a new hire letter. The information can be used against relatives by mimicking them to gain access to their accounts (commit fraud) or in other ways since the device contains wedding lists, vacation ideas, and family & pet pictures. This information can provide access to the business if the attacker impersonates an employee through the information he collected.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* *Malicious software that can be hidden on these devices (USB similar) is worms or malwares. If another employee found an infected USB and didn't use the virtualization tool to verify the USB, that employee could have damaged a computer (installing malicious software, etc.) by plugging the USB into that computer.*

	Sensitive information could a threat actor find on a device like this are PII and SPII. Attackers can easily use this sensitive information to target the data owner or others around them, by impersonating them to gain access and commit fraud or threatening the target to give money if the target doesn't want the information to be leaked. Technical controls: We can install antivirus software on workstations since it provides protection against malware infection. Operational controls: We can spread awareness and training to employees to reduce the risks of USB baiting. Managerial controls: We can perform pen tests to test how resilient the systems are to USB-baiting attacks and find where improvements are required.

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. ● *Will the app process transactions?* ● *Does it do a lot of back-end processing?* ● *Are there industry regulations that need to be considered?* *The app will process transactions; Proper payment handling is really important because the company wants to avoid legal issues.* *The app does a lot of back-end processing; sales should be clear and quick to process.* *Data privacy is a big concern for the company; they want users to feel confident that the company is being responsible for their information.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. *SQL is the first one I will prioritize since the database contains all important information about the sneakers that are for sale, as well as the sellers who are selling them. Thus, we have to make sure the app is not vulnerable to SQL injection attacks.* *SHA-256 is the 2nd one I will prioritize since it is used to protect sensitive user data, like passwords and credit card numbers. Thus, we have to make sure that it is not vulnerable to Brute-force attacks.*

	Public key infrastructure (PKI) is the 3rd one I will prioritize since the app uses a combination of asymmetric and symmetric encryption algorithms, and we have to make sure the encryption/decryption keys cannot be stolen by malicious actors. *Application programming interface (API) is the last I will prioritize since it is a set of rules that define how software components interact with each other, I have to ensure that they match the app's security requirements and that they contain no vulnerabilities.*
III. Decompose application	Sample data flow diagram
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *What are the internal threats?* ● *What are the external threats?* *SQL injection and Session hijacking*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Could there be things wrong with the codebase?* ● *Could there be weaknesses in the database?* ● *Could there be flaws in the network?* *Not having prepared statements if hackers tried to access/modify the database through SQL injection* *Weak login credentials; a hacker can succeed at brute forcing login credentials and then hijack the session.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. Use of prepared statements Use of MFA Use of Salting while hashing with SHA256 Promoting awareness to users about security risk

Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 02/08/2023 Record the date of the journal entry.	**Entry: 1** Record the journal entry number.
Description	**This entry is about a ransomware phishing attack at U.S. Healthcare Clinic.** **The phase of the NIST Incident Response Lifecycle the incident investigation occurred in is the Detection and Analysis since we are documenting an incident with an incident handler's journal.**
Tool(s) used	List any cybersecurity tools that were used. **N/A**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers caused the incident. • **What** happened? A small U.S. healthcare clinic experienced a security incident that severely disrupted its business operations. An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

	• **When** did the incident occur? On Tuesday at 9:00 a.m., the incident occurred. • **Where** did the incident happen? At a small U.S. healthcare clinic, the incident happened. • **Why** did the incident happen? The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.
Additional notes	Include any additional thoughts, questions, or findings. **Is there a way to decrypt the files without exchanging money for the decryption key?** **How can I get the IP address of the hackers?**

Date: 11/08/2023 Record the date of the journal entry.	**Entry: 2** Record the journal entry number.
Description	This entry is about a phishing attempt and download of malware. The phase of the NIST Incident Response Lifecycle the incident investigation occurred in “Containment, Eradication, and Recovery” because we are using a playbook to respond to a phishing incident.
Tool(s) used	List any cybersecurity tools that were used. **N/A**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious actor

	• **What** happened? The attacker attempted Phishing and the user downloaded malware • **When** did the incident occur? The email was sent on Wednesday, July 20, 2022, at 09:30:14 AM • **Where** did the incident happen? On the user's device. • **Why** did the incident happen? The user may have opened a malicious email and opened attachments.
Additional notes	Include any additional thoughts, questions, or findings. Alert severity = Medium → good indication that a ticket might require escalation. Sender details = There is a mismatch between the sender's email address and the sender's name → this is a good indication that the email might be a phishing email. Receiver's IP address and e-mail address: <hr@inergy.com> <176.157.125.93> Sender's IP address and e-mail address: <76tguyhh6tgftrt7tg.su> <114.114.114.114> Message body: message body and subject line contain grammatical errors → can be an indication of a phishing attempt. Attachments or links: 2 files have been attached to this email → Phishing emails contain malicious links or attachments that are used to steal sensitive information or download malicious software or code on the recipient's device

Date: 19/08/2023 Record the date of the journal entry.	**Entry: 3** Record the journal entry number.
Description	This entry is about exploring signatures and logs with Suricata. The phase of the NIST Incident Response Lifecycle the incident investigation occurred in is the Detection and Analysis since we; - Explored custom rules in Suricata. - Ran Suricata with a custom rule in order to trigger it, and examined the output logs in the fast.log file. - Examined the additional output that Suricata generates in the standard eve.json log file.
Tool(s) used	- Suricata - It is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS) - It can be used to detect and prevent a wide range of network threats.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen? This is a lab activity. Not an incident response.
Additional notes	Include any additional thoughts, questions, or findings.

	Explored custom rules in Suricata. Ran Suricata with a custom rule in order to trigger it, and examined the output logs in the fast.log file. Examined the additional output that Suricata generates in the standard eve.json log file.

Date: 19/08/2023 Record the date of the journal entry.	**Entry: 4** Record the journal entry number.
Description	This entry is about investigating a suspicious file hash using the VirusTotal website. The phase of the NIST Incident Response Lifecycle where the incident investigation occurred is the Detection and Analysis since we are analyzing/investigating the detected file.
Tool(s) used	- VirusTotal website - It is used to analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, and automatically share them with the security community. - It can be used to identify false positives.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Malicious actor

	• **What** happened? I have received an alert about a suspicious file being downloaded on an employee's computer. • **When** did the incident occur? Here is a timeline of the events leading up to this alert: 1:11 p.m.: An employee receives an email containing a file attachment. 1:13 p.m.: The employee successfully downloads and opens the file. 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC. • **Where** did the incident happen? On an Employee's Computer at a financial services company • **Why** did the incident happen? The employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, and then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Additional notes	This file has been identified as malicious, since it has a high vendors' ratio, a negative community score, and there are malware detections in the security vendors' analysis section.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident?

	• **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.

1. Were there any specific activities that were challenging for you? Why or why not?
   The labs were challenging since you had to finish them within a specific time. However, they were fun and gave me the chance to practice what I learned.

2. Has your understanding of incident detection and response changed since taking this course?

   I learned effectif and efficient ways to detect and respond to incidents. Thus, my understanding of incident detection and response has improved.

3. Was there a specific tool or concept that you enjoyed the most? Why?
   I enjoyed learning about SIEM tools and how logs are ingested into SIEM tools. These tools are very important since they provide analysts with a view of what is happening on a network, and we must use them effectively to get the data necessary for our investigations.

Wireshark

- Uses GUI
- Wireshark offers an extensive range of analysis features with its powerful toolset. With color coding, filters, and protocol dissectors, Wireshark has the ability to reassemble and follow streams, providing in-depth analysis of packets.

Similarities

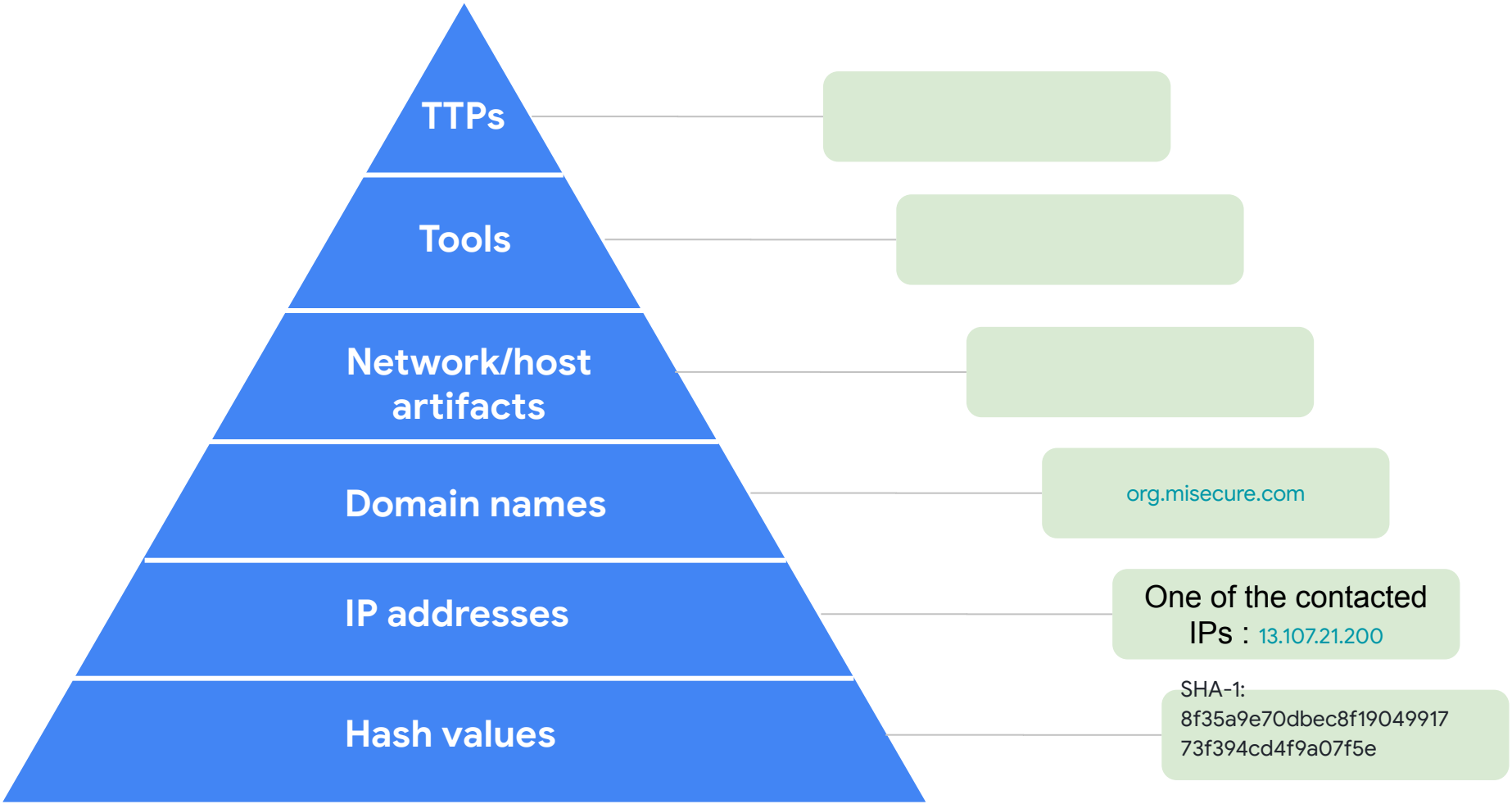
- Display both source and destination MAC addresses
- They allow allow capturing packets and can both read pcap files.
- Both Wireshark and tcpdump use dotted code to translate the source and destination IP addresses.

tcpdump

- Uses CLI
- Tcpdump is limited in its analysis capabilities, displaying packet data directly in the terminal.

Has this file been identified as malicious? Explain why or why not.

This file has been identified as malicious, since it has a a high vendors' ratio, a negative community score, and there are malware detections in the security vendors' analysis section.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
org.misecure.com
One of the contacted IPs : 13.107.21.200
SHA-1:
8f35a9e70dbec8f19049917
73f394cd4f9a07f5e

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

Ticket comments
My key findings indicated that this was a phishing email, thus I verified the reputation of the file attachment through its hash value using VirusTotal. Since the file hash was malicious, since the alert severity is medium and since the message body and subject line contain grammatical errors, I escalated the ticket. Here are My findings; - Alert severity = Medium → indication that a ticket might require escalation. (1st Reason for escalation) - Sender details = There is a mismatch between the sender's email address and the sender's name → indication that the email might be a phishing email. Receiver's IP address and e-mail address: <hr@inergy.com> <176.157.125.93> Sender's IP address and e-mail address: <76tguyhh6tgftrt7tg.su> <114.114.114.114> - Message body: message body and subject line contain grammatical errors → indication of a phishing attempt (2nd Reason for escalation). - Attachments or links: A file has been attached to this email → Phishing emails contain malicious links or attachments that are used to steal sensitive information or download malicious software or code on the recipient's device

- 3rd Reason for escalation: I checked the reputation of the file attachment through its hash value using VirusTotal, and the file hash is malicious.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"

Algorithm for file updates in Python

Project description

I am required to update a file that identifies the employees who can access restricted content. I created an algorithm that uses Python code to check whether the allow list contains any IP addresses identified on the remove list. If so, I removed those IP addresses from the file containing the allow list.

Open the file that contains the allow list

I need with statement to handle the file. I need open() function to open the file. This function will take to parameter (1st parameter is the file name and second parameter will be the “r” command to specify tht we are opening the file for reading purpose.) Then we need the as keyword to tell python to use the variable file to store the file while you work with it inside the with statement. Finally, we must add a colon at the end the with statement header for syntax purpose.

```
# Assign `import_file` to the name of the file
import_file = "allow_list.txt"
# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.
remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]
# First line of `with` statement
with open(import_file, "r") as file:
```

Read the file contents

Now that the allow list file contents are saved in the file variable and we are working within the with statement, we will need the .read() method to be appended after the file variable; file.read(). This method will convert the contents of the allow list file into a string so that you can read them. Then we need store this string in a variable called ip_addresses; ip_addresses = file.read(). This line of code should be indented since it is being done within the with statement.

```
# Assign `import_file` to the name of the file
import_file = "allow_list.txt"
# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.
remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]
# Build `with` statement to read in the initial contents of the file
with open(import_file, "r") as file:
  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`
  ip_addresses = file.read()
# Display `ip_addresses`
print(ip_addresses)
```

Convert the string into a list

We need the .split() method to convert the ip_addresses string into a list. So since ip_addresses variable contains the string we want to convert, we append .split() method to it; ip_addresses.split(). Then we assign the resulting list to ip_addresses variable so we can reuse the list simply by calling ip_addresses. Since this done outside the with statement, this line of code does not need to be indented.

```
# Assign `import_file` to the name of the file
import_file = "allow_list.txt"
# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.
remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]
# Build `with` statement to read in the initial contents of the file
with open(import_file, "r") as file:
  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`
  ip_addresses = file.read()
# Use `.split()` to convert `ip_addresses` from a string to a list
ip_addresses = ip_addresses.split()
# Display `ip_addresses`
print(ip_addresses)
```

Iterate through the remove list

We need the for keyword to indicate the beginning of the for loop. We need element loop variable to temporarily store the elements in ip_addresses. We need in keyword to specify where we want to loop (in this case, ip_addresses list). Final we must add a colon at the end of the for loop header for syntax purpose.

```
# Assign `import_file` to the name of the file

import_file = "allow_list.txt"

# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.

remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]

# Build `with` statement to read in the initial contents of the file

with open(import_file, "r") as file:

  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`

  ip_addresses = file.read()

# Use `.split()` to convert `ip_addresses` from a string to a list

ip_addresses = ip_addresses.split()

# Build iterative statement
# Name loop variable `element`
# Loop through `ip_addresses`

for element in ip_addresses:

    # Display `element` in every iteration

    print(element)
```

Remove IP addresses that are on the remove list

Inside the for loop, we have to make an indented line that is a conditional statement header that checks if the loop variable element is part of the remove_list list: “ if element in remove_list:”. We have to add a colon at the end of the header of the conditional statement for syntax purposes. Then, within that conditional, we indent a new line where we apply the .remove() method to the ip_addresses list and remove the IP addresses identified in the loop variable element if that IP address is in the remove_list: ip_addresses.remove(element). Applying the .remove() method in this way is possible because there are no duplicates in the ip_addresses list.

```
# Assign `import_file` to the name of the file

import_file = "allow_list.txt"

# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.

remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]

# Build `with` statement to read in the initial contents of the file

with open(import_file, "r") as file:

  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`

  ip_addresses = file.read()

# Use `.split()` to convert `ip_addresses` from a string to a list

ip_addresses = ip_addresses.split()

# Build iterative statement
# Name loop variable `element`
# Loop through `ip_addresses`

for element in ip_addresses:

  # Build conditional statement
  # If current element is in `remove_list`,

    if element in remove_list:

        # then current element should be removed from `ip_addresses`

        ip_addresses.remove(element)

# Display `ip_addresses`

print(ip_addresses)
```

Update the file with the revised list of IP addresses

We must convert the ip_addresses list back into a string using the .join() method. The .join method takes the iterable it wants to convert as input. We have to apply .join() to the string "\n" in order to separate the elements in the string by placing them on a new line. Thus the code line will be written as "\n".join(ip_addresses). Then we need to store this string in a variable called ip_addresses so that we can call ip_addresses whenever we want to use the string; ip_addresses = "\n".join(ip_addresses).

```
# Assign `import_file` to the name of the file

import_file = "allow_list.txt"

# Assign `remove_list` to a list of IP addresses that are no longer allowed to access restricted information.

remove_list = ["192.168.97.225", "192.168.158.170", "192.168.201.40", "192.168.58.57"]

# Build `with` statement to read in the initial contents of the file

with open(import_file, "r") as file:

  # Use `.read()` to read the imported file and store it in a variable named `ip_addresses`

  ip_addresses = file.read()

# Use `.split()` to convert `ip_addresses` from a string to a list

ip_addresses = ip_addresses.split()

# Build iterative statement
# Name loop variable `element`
# Loop through `ip_addresses`

for element in ip_addresses:

  # Build conditional statement
  # If current element is in `remove_list`,

    if element in remove_list:

        # then current element should be removed from `ip_addresses`

        ip_addresses.remove(element)

# Convert `ip_addresses` back to a string so that it can be written into the text file

ip_addresses = "\n".join(ip_addresses)

# Build `with` statement to rewrite the original file

with open(import_file, "w") as file:

  # Rewrite the file, replacing its contents with `ip_addresses`

  file.write(ip_addresses)
```

Summary

There is an allow list for IP addresses permitted to sign into the restricted subnetwork. There's also a remove list that identifies which employees you must remove from this allow list. Thus the algorithm I wrote converts the allow list file contents into a string, and then to a list. Then the algorithm removes IP addresses indicated in the remove list from the “allow list file” list. Then the algorithm converts the updated list back to a string so that it can be used to replace the allow list file contents through the .write() method.