# 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 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** |
| 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 | Medium |
| 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 vulnerabilitiesMedium | 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 | Low |
| 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 |

# Portfolio: Automating IP Address Updates with Python Algorithm

## Project Description

In the context of managing access to restricted content at my organization through an IP allow list, I developed a Python algorithm to streamline the process of updating the "allow_list.txt" file. This algorithm automatically removes IP addresses from the list based on a predefined remove list, ensuring accurate and efficient content access control.

## Algorithm Workflow

### Step 1: Opening the Allow List File

```
import_file = "allow_list.txt"

with open(import_file, 'r') as file:
    ip_addresses = file.read().split()
```

I began by opening the "allow_list.txt" file in read mode and converting its content into a list of IP addresses using the `.read()` method and `.split()` function.

### Step 2: Iterating Through the Remove List

```
for element in remove_list:
    if element in ip_addresses:
        ip_addresses.remove(element)
```

I used a `for` loop to iterate through the `remove_list` of IP addresses to be removed. Within the loop, I checked if each IP address was present in the `ip_addresses` list and removed it using the `.remove()` method.

## Step 3: Converting List Back to String

```
updated_ip_addresses = "\n".join(ip_addresses)
```

After updating the `ip_addresses` list, I used the `.join()` method to convert it back into a string format, with each IP address separated by a newline character.

## Step 4: Updating the Allow List File

```
with open(import_file, 'w') as file:
    file.write(updated_ip_addresses)
```

Finally, I opened the "allow_list.txt" file in write mode and updated its contents with the revised list of IP addresses using the `.write()` method.

## Summary

I designed an algorithm that automates the process of updating the "allow_list.txt" file, which controls access to restricted content through IP addresses. This algorithm efficiently removes specified IP addresses from the list while maintaining accuracy. By leveraging file handling, list manipulation, and conditional statements, I created an effective solution that enhances access control management in real-world scenarios.

## Outcomes

- Efficiency: The algorithm significantly reduces the manual effort required for updating the IP allow list.
- Accuracy: By automating the removal of IP addresses, the algorithm ensures precise and error-free updates.
- Scalability: The solution can effortlessly handle an increasing number of IP addresses in the allow list.

## Reflection

This project allowed me to showcase my proficiency in Python programming, file handling, list operations, and conditional statements. The algorithm's successful implementation demonstrates my ability to solve practical challenges using code, contributing to improved efficiency and accuracy in access control procedures.

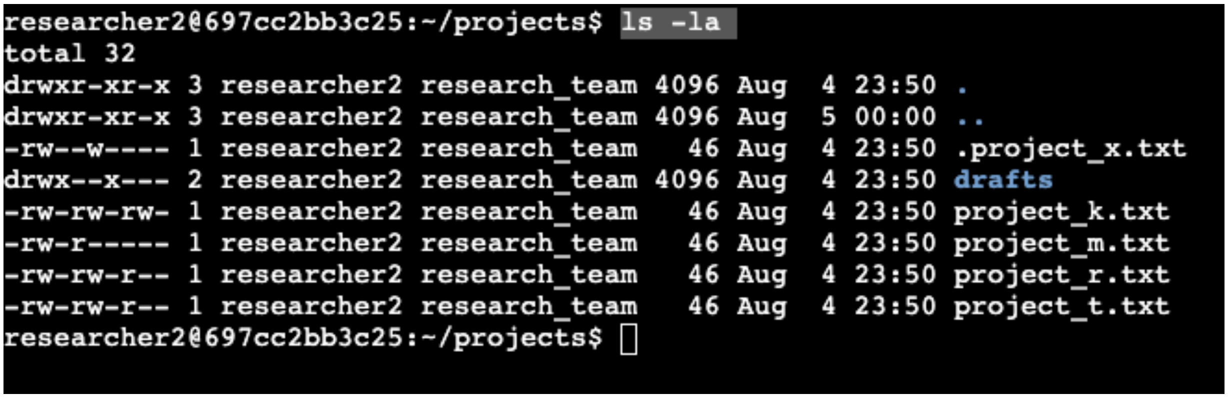
# File permissions in Linux

## Project description

You are a security professional at a large organization. You mainly work with their research team. Part of your job is to ensure users on this team are authorized with the appropriate permissions. This helps keep the system secure. Your task is to examine existing permissions on the file system. You'll need to determine if the permissions match the authorization that should be given. If they do not match, you'll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.

## Check file and directory details

Use this command: ls -la , this displays permission to the files and directories including hidden files.



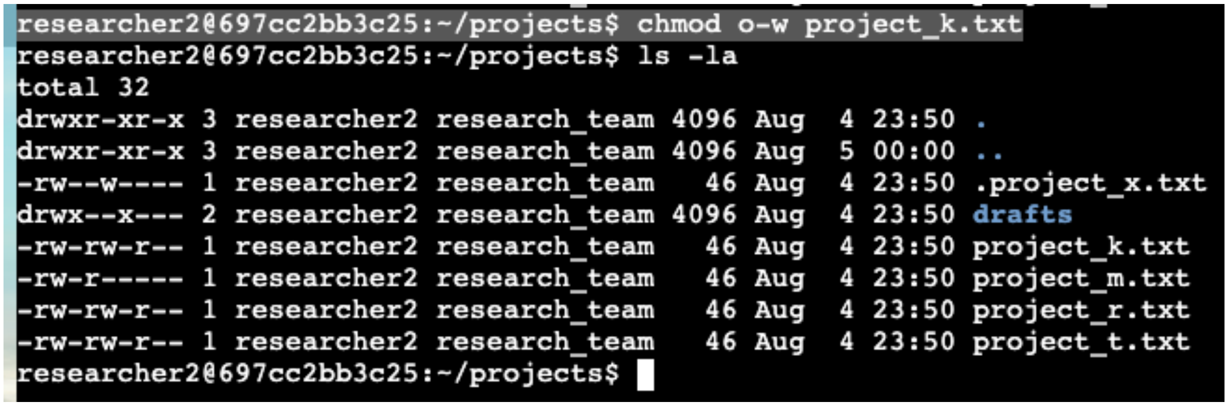
```
researcher2@697cc2bb3c25:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug  4 23:50 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug  5 00:00 ..
-rw--w---- 1 researcher2 research_team   46 Aug  4 23:50 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug  4 23:50 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Aug  4 23:50 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Aug  4 23:50 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug  4 23:50 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug  4 23:50 project_t.txt
researcher2@697cc2bb3c25:~/projects$ 
```

## Describe the permissions string

The file permissions are represented by a 10 character string. In this example, drafts , 10 character string means; d, it is a directory, user has read, write and execute permissions; group has execute permissions and other has not been granted any permissions.

## Change file permissions

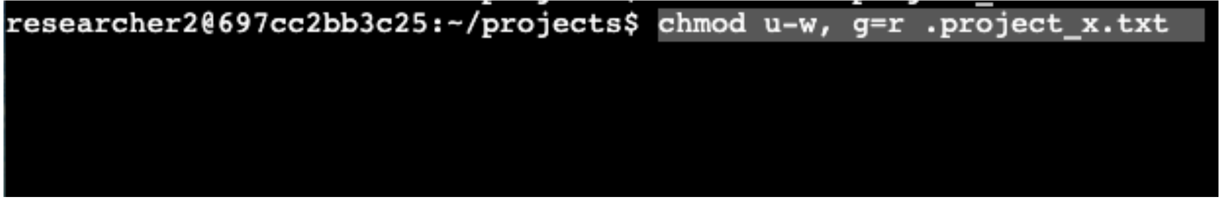
I used the chmod command to remove the execute permission from the other owner type in the project_k.txt file. Then I used ls -la to make sure the permissions were changed.



```
researcher2@697cc2bb3c25:~/projects$ chmod o-w project_k.txt
researcher2@697cc2bb3c25:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Aug  4 23:50 .
drwxr-xr-x 3 researcher2 research_team 4096 Aug  5 00:00 ..
-rw--w---- 1 researcher2 research_team   46 Aug  4 23:50 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Aug  4 23:50 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Aug  4 23:50 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Aug  4 23:50 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug  4 23:50 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Aug  4 23:50 project_t.txt
researcher2@697cc2bb3c25:~/projects$ 
```

### Change file permissions on a hidden file

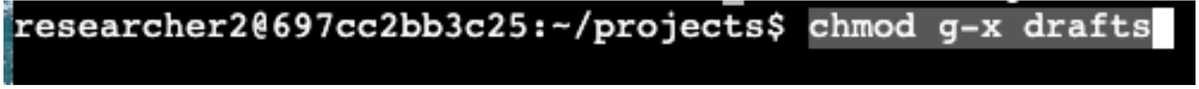
I used the chmod command again to change the user permission by taking away the write permission and the changing group to read only. This makes it so both groups only have read permissions.



```
researcher2@697cc2bb3c25:~/projects$ chmod u-w, g=r .project_x.txt
```

### Change directory permissions

I used chmod command again to take away the group execute permissions making it so only researcher 2 user has the ability to access the draft directory and its content.



```
researcher2@697cc2bb3c25:~/projects$ chmod g-x drafts
```

### Summary

This task has given me practical experience in using Basic LINUX Bash Shell commands to examine file and directory permissions, change permissions on files and change permissions on directories.

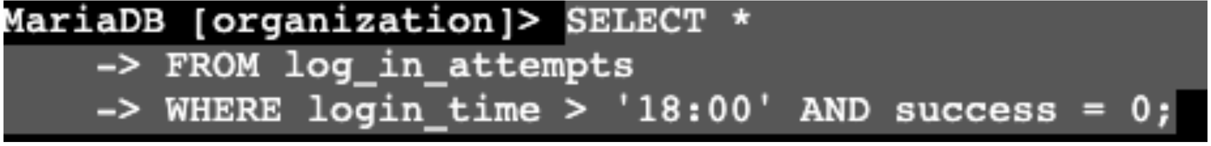
# Apply filters to SQL queries

## Project description

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines. Your task is to examine the organization’s data in their employees and log_in_attempts tables. You’ll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

## Retrieve after hours failed login attempts

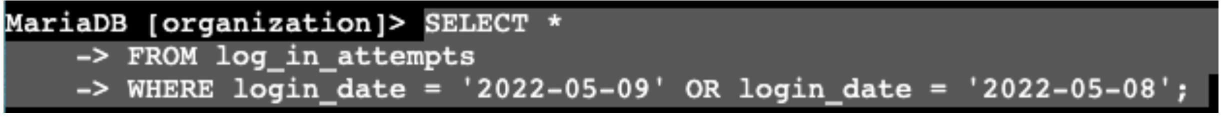
To get the login time from the login attempts I select *(select all) from the login attempts and then since we only want login time for after 18:00 that were failed, I use > and the AND operator success = 0 (0 represents failed) to get the desired query.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
```

## Retrieve login attempts on specific dates

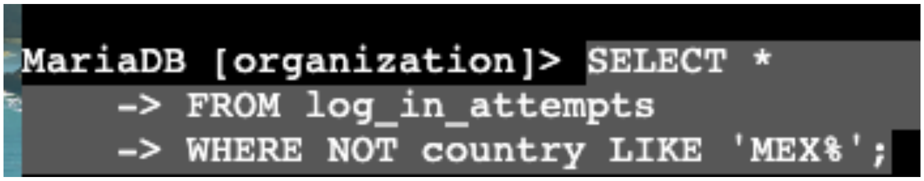
For this query, I wanted to retrieve login attempts that occurred on 2022-05-08 or 2022-05-09 so I used select all again and from the login attempts, they I filtered the two dates using OR operator to get queries from either one or both.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

## Retrieve login attempts outside of Mexico

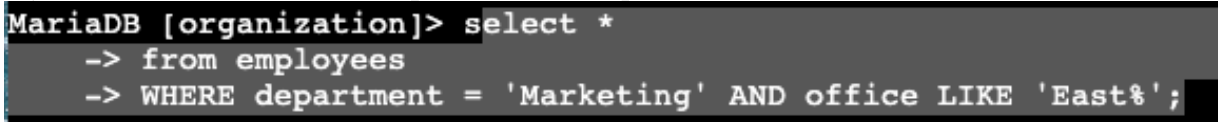
In this example, the team was investigating logins that did not originate from Mexico and the country filed entries included MEX and Mexico, so in order to do this I selected all again from the login attempts but this time used NOT to exclude Mexico and used the LIKE operator to include MEX as well.



```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
```

## Retrieve employees in Marketing

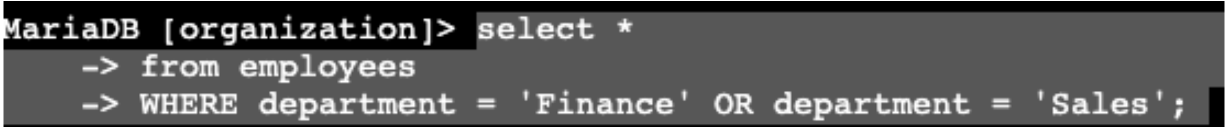
This example I needed to obtain information about employees from the Marketing department who are located in all offices in the East building. To do this I used select all again and from employees because we are searching for employees and then filtered for the Marketing department since that is the type of employees I am looking for and then used AND and LIKE because we want the marketing employees in the East buildings and since the buildings can be any number I used the % for the pattern to encompass them all.



```
MariaDB [organization]> select *
    -> from employees
    -> WHERE department = 'Marketing' AND office LIKE 'East%';
```

Retrieve employees in Finance or Sales

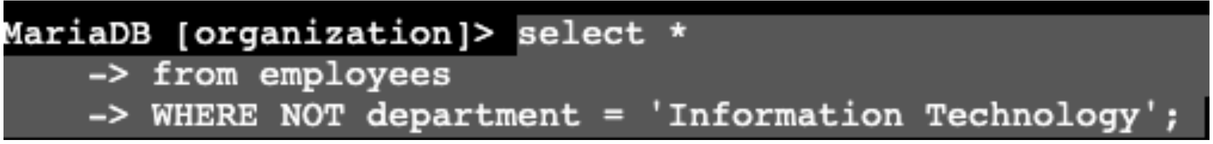
For this example, I was tasked with locating the information for employees in the Sales or finance department, so I again select all, from employees and since we are okay with having either one I used the OR operator. This gave me a query of employees from the sales and finance departments.



```
MariaDB [organization]> select *
    -> from employees
    -> WHERE department = 'Finance' OR department = 'Sales';
```

Retrieve all employees not in IT

This task needed me to get information on employees who are not in the IT department. So once again I use select all, from employees and then use the NOT operator to exclude the IT department but include everything else.



```
MariaDB [organization]> select *
    -> from employees
    -> WHERE NOT department = 'Information Technology';
```

Summary

This exercise gave me practical experience in using SQL to run SQL queries to retrieve information from a database and apply SQL AND, OR and NOT operators to filter SQL queries.

# Vulnerability Assessment Report

## 1$^{st}$ 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
Gain insight into potential likelihood and severity of risks and helps them make informed decisions about allocating resources, implementing controls and prioritizing remediation efforts. The server contains data that needs to be protected and it is important to secure this data because or regulations as well as preventing damage to rep and preventing monetary losses. Business may be halted, could lose lots of data and face fines and damage to company reputation.

Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
|---|---|---|---|---|
| *Standard user* | *Accidentally leaks private info* | *2* | *3* | *6* |
| Software | Software is not update to date leading to a vulnerability being exploited | 2 | 3 | 6 |
| Hardware | Improper storage leads to data being lost | 1 | 2 | 2 |

Approach
They have a likelihood of happening, and it is important to address these issues. The leaking of private info could have huge consequences for the company, software that is not up to date could also leave room for malicious attackers to attack. Improper storage could also lead to valuable day to day data that is needed becoming lost and hurting 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. Ensuring there is a access limit to sensitive files and limiting access to only those who need the files, implementing automatic updates to keep software up to date and ensuring hardware is properly stored and looked after to limit the

loss of data.

# 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)** | *The manager did not revoke access to the internal folder, the sales team member did not wait to get approval and shared the wrong link as well* |
| **Review** | *Protection against data leaks* |
| **Recommendation(s)** | *Only give access to the internal folder to people who need it and make sure they do not have access to it until it is ready to be shared, limit who can share it as well.* |
| **Justification** | *They stop it from being shared all together until it is ready and only have it in the hands of the person who needs it.* |

### 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:<br>Only the minimal access and authorization required to complete a task or function should be provided to users. |
| | Discussion:<br>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:<br>• Restrict access to sensitive resources based on user role.<br>• Automatically revoke access to information after a period of time.<br>• Keep activity logs of provisioned user accounts.<br>• Regularly audit user privileges. |

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

# 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 company website. Port 53 is a well known port for DNS service. This may a problem with the DNS server. |
| |

| Part 2: Explain your analysis of the data and provide one solution to implement |
|---|
| The incident occurred this afternoon when several customers reported that they were not able to access the company website. The network security responded and began running test with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53 which is used for DNS servers is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the company website. The word unreachable in the message indicates that the message did not go through to the DNS server. The browser was not able to obtain the IP address for the company site which it needs to access the website. No service was listening on the receiving DNS port as indicated by the error message “udp port 53 unavailable.” |

# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this network interruption** |
|---|
| This is a SYN flood attack that targets network bandwidth to slow traffic, it is simulating a TCP connection and flooding the server with SYN packets. This is a DoS attack by a malicious actor. It can’t keep up with all the request so it is overwhelmed and slow |
|  |

| **Section 2: Explain how the attack is causing the website to malfunction** |
|---|
| The website is being flooded by SYN packets that are simulating a TCP connection. This flooding is what causing the network to become slow and unresponsive because it can’t keep up with the amount of request this malicious attacker is sending. This can cause us to lose money and customers as well as leave us vulnerable to other threats or attacks. A few ways to prevent this is could be more advanced firewalls and encryption. |

Security incident report

**Section 1: Identify the network protocol involved in the incident**

Transmission Control Protocol

**Section 2: Document the incident**

The attacker initiated a brute force attack to gain access to the web host. They repeatedly entered known default passwords for an admin account until they correctly guessed the right one. In doing so they were able to obtain the source code to the website. Then they embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website that would then redirect the customers to the fake website. This affected multiple customers.

To investigate this a sandbox was used to observe the suspicious behavior of the website. Running the network protocol analyzer tcpdump I enter the url in to the website and am prompted to download and run the file, I then observe that the browser redirects me to a different url designed to look like the original site. The logs show that process.

**Section 3: Recommend one remediation for brute force attacks**

Require stronger more complex passwords; this will make it harder for brute force attacks to occur

# 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** | There was a DDos attack and our organization network services suddenly stopped due to a flooding of ICMP packets. Normal internal traffic could not access any network resources. The team responded by blocking the incoming ICMP packets and stopping all non critical network services offline and restoring critical services. After investigating they found that a malicious attacker had sent a flood of ICMP pings into the company's network through an unconfigured firewall, allowing for the DDoS attack. |
| Identify | This was a DDoS attack allowed by an unconfigured firewall |
| Protect | The firewall needs to be updated and configured |
| Detect | We can use IDS and SIEM tools to better monitor traffic |
| Respond | IPS can help block an attack like this in the future, we can use SIEM to monitor traffic as well |
| Recover | We need to have backups in place to restore data |

| |
|---|
| Reflections/Notes: |

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:**

**____**x**_ 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 wants to ensure we comply with the EU regulations and this is one of them.**

**___x__ 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: We are dealing with people's credit card info and selling toys globally, we should make sure we are up to standards with this and the customers info is secure.**

**_____ 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:**