# **1. INTRODUCTION**

This Incident Response Plan encompasses all information systems, networks, and digital assets managed by KNUST, including those hosted on-campus and in the cloud. It applies to all university personnel, contractors, and third-party entities with access to the University's information systems. The primary objective of this Incident Response Plan is to provide a structured and coordinated approach for addressing and mitigating cybersecurity incidents within the University's information technology infrastructure. Whether faced with a malware infection, a data breach, or any other security incident, this document serves as a guide for ISTAD personnel, university staff, and relevant stakeholders to respond effectively, minimize and restore normal operations swiftly.

## 1.1 SOC TIERS

The Security Operations Centre (SOC) is responsible for coordinating and carrying out the activities outlined in this plan. The SOC is divided into 3 tiers with each tier handling specific stages of the Incident Response Plan (IRP).

# 2. SOC TIER 1

This is a critical component of the Incident Response Plan (IRP), as it is the first line of defense, this tier plays a pivotal role in event logging, incident detection, initial assessment, and timely escalation, contributing to the overall resilience of the university's information technology infrastructure.

## 2.1 EVENT LOGGING AND INFORMATION GATHERING

At this stage, events from various University Systems, networks, and resources are collected and documented in the form of logs either through the SIEM solutions or manual/external reports(Call-ins and forms)

### 2.1.1 LOGS FROM SIEM SOLUTIONS

Grafana provides a view of the logs collated from Wazuh. These logs should be investigated and monitored every 30 minutes to pick up on security events and possible incidents.

### 2.1.2 REPORTED EVENTS

In the case where the events or activities are reported by end users, they should be reported through ISTAD-UITS Support Ticket center. End Users can access this platform through the ISTAD Whatsapp Support Line, ISTAD, UITS websites and the KNUST Help Desk.

## 2.2 INCIDENCE CLASSIFICATION AND MANAGEMENT

* Through Investigation, logs and events/activity should first be classified as mere events or incidents.
* If the event is indeed classified as an incident, further investigation should be done to determine the specific classification of the incident (malware, DDOS Attack, etc.)
* Events are deemed to be incidents (and further grouped into incident classes) if they follow specific patterns described in Section 5 (incidents)

## 2.3 INCIDENT ESCALATION AND REPORT

* After Incidents are properly classified, they should be documented through the Event Investigation Template and made available on the cloud for easy access by other personnel in and outside the tier.
* The document should clearly state the entire logging and event investigation process while clearly stating the exact patterns the events exhibited that led to the classification.
* A ticket should then be created in the GLPI and assigned to members in tier 2 for further action. The ticket should be assigned an urgency score, a name, and a code.

### 2.3.1 Urgency Score

The urgency score ensures that the very urgent and most compromising incidents are resolved first. The score is determined by the risk rating of the affected assets and the rating of the specific events.

### 2.3.2 Name

The Ticket name should be the name of the classified incident (eg Malware)

### 2.3.3 Code

The Ticket code should clearly show the date, incident code, and number of the said incident in the format: yy/mm/dd-incident code-no (for example, the 3rd malware incident (malware has a code of 1) of today will be 240112-01-03)

# **3. SOC TIER 2**

The SOC Tier 2 team plays a crucial role in the investigation, analysis, and mitigation of security incidents. Tier 2 personnel possess specialized expertise to handle complex incidents, ensuring a swift and effective response to protect the university's information technology infrastructure.

## 3.1 INCIDENT VERIFICATION

* After receiving a ticket from tier one, the incidents must be verified to ensure that they are indeed what they are said to be.
* Verification is done by reviewing the reports for tier 1 on the said incident.
* If the incident is found to be a false positive, a report must be sent to tier 1 on the reasons for the determination as a false positive for further investigation.
* If the incident is verified, then Incident Response should be initiated

NB: A Ticket should only be addressed if it has the highest urgency score in the batch.

## 3.2 INCIDENT RESPONSE

This is the stage where the incident is handled. In this stage, the incident is contained and eradicated and recovery is initiated when necessary.

### 3.2.1 CONTAINMENT

* Containment is done to prevent the incident from affecting other assets and prevent lateral movement of threats.
* Each incident has a specific containment procedure that is specified in Section 5 (Incidents)
* For Incidents that cannot be contained, the eradication phase should be initiated immediately.

### 3.2.2 ERADICATION

* This stage involves the complete resolution of the incident. The root cause of the incident is determined and removed.
* Eradication is done with a set of tools provided in the SOC Security Toolkit.
* Specific tools and software vary for each incident and is specified in Section 5 (Incidents)

### 

### 3.2.3 RECOVERY

If an incident or containment of an incident renders a system or service inactive, the recovery phase’s purpose is to restore all system activities to the original state before the incident.

## 3.3 POST INCIDENT ACTIVITY

This is where discussion and documentation on the Incident response is done. SOC personnel are to have meetings in 3 folds.

1. At the end of the week discuss all incidents resolved/yet to be resolved throughout the week. This meeting should touch on the procedure followed in each stage of the plan
2. At the end of the month discuss All incidents resolved/yet to be resolved throughout the month. This meeting should look at the frequency of certain events and the similarities in patterns.
3. At the end of the year audit all monthly reports and determine the viability of the plan going into the next year.

### 3.3.1 INTELLIGENCE ESCALATION AND REPORT

* After the response process, a report should be prepared through the Incidence Response Template and made available on the cloud for easy access by other personnel in and outside the tier.
* This report should clearly state the specific measures taken to resolve the incident and also any new patterns identified throughout the process.
* In the case where an incident cannot be solved by personnel in this tier, the assigned ticket in GLPI should be re-assigned to members of tier 3.

# //4. SOC TIER 3//

# 

# **5. INCIDENTS**

In this section, common incidents are tackled with specific instructions to SOC personnel as specified in Section 2 (SOC Tier 1) and Section 3 (SOC Tier 2)

## 5.1 MALWARE

This refers to any software specifically designed to harm or exploit computer systems, networks, or user devices. There are various types of malware; Trojans, Worms, rootkits, Ransomware, etc.

### **5.1.1 MALWARE IDENTIFICATION**

In looking at a set of events, both externally reported and internally captured, if the following patterns are found, there is a high likelihood of it being an Incident and specifically Malware. These Identification patterns are segmented into popular classes of malware for more concise identification.

* Ransomware Identification

1. Unusual file extension
2. Ransom notes
3. Sudden file modifications
4. Persistent Antivirus alerts

* Rootkit Identification

1. Frequent Blue Screens
2. Unusual web browser behavior
3. Slow system performance
4. Unintended changes to Windows settings

* Worms Identification

1. Slow system performance
2. Frequent freezing/crashing of the system
3. Programs opening and running automatically \*\*
4. Irregular web browser performance
5. Unusual computer behavior
6. Firewall warnings
7. Missing/modified files or folders
8. Appearance of strange/unintended desktop files or icons
9. Operating system errors and system error messages
10. Emails sent to contacts without the user’s knowledge
11. Multiple Failed Login Attempts prompt
12. Unusual Hard disk usage
13. Unusual hidden files or folders
14. Unwarranted file duplication
15. Unwanted shortcuts

* Trojan Identification

1. Suspicious third-party applications that were not installed by the user
2. Disabled Security Software
3. Unwanted software installation
4. Changes in system settings
5. Unexpected files or programs on the system

### 5.1.2 MALWARE CONTAINMENT

In the event where a malware is confirmed, the following must be done to contain the malware and prevent it from spreading.

1. Disconnect the affected system from the internet.
2. Disable other wireless connectivity to other devices (e.g. Bluetooth, file-sharing services)
3. Backup critical files
4. Restart in safe mode- Safe mode only allows the running of essential programs
5. Reset all credentials.
6. Monitor and close all suspicious applications.
7. Scan the system to detect the Malware.

NB: In the event of a ransomware incident, skip step 3 and move straight to eradication after step

### 5.1.3 MALWARE ERADICATION

* Ransomware Eradication

1. Contact Law Enforcement and report the situation
2. Analyze ransom texts for clues and hints to determine the ransomware variant.
3. Use the XYZ Decryption tools to attempt decryption
4. If decryption is successful, jump to step 9
5. If decryption is unsuccessful, prepare to restore a backup
6. Safely wipe the infected devices and reinstall the OS.
7. Before restoring from a backup, verify that it is free from any malware. Only restore from backups that have been verified to be clean.
8. Connect devices to a clean network to download, install, and update the OS and all other software.
9. Install, update, and run certified antivirus software.
10. Reconnect to the network.
11. Monitor network traffic and run antivirus scans to identify if any infection remains.

* Rootkit Eradication

1. Perform a complete system scan with the university's verified antivirus software or Windows Defender in the case of Windows systems
2. Antivirus/ Windows Defender would automatically eliminate the rootkit if it is not a deep infection.
3. If the rootkit is not automatically removed, the scan will still reveal the location, and the rootkit should be removed manually.
4. If the manual removal is successful, jump to step 8
5. If the manual removal is unsuccessful, prepare to restore a backup
6. Safely wipe the infected devices and reinstall the OS.
7. Before restoring from a backup, verify that it is free from any malware. Only restore from backups that have been verified to be clean.
8. Connect devices to a clean network to download, install, and update the OS and all other software.
9. Install, update, and run certified antivirus software.
10. Reconnect to the network.
11. Monitor network traffic and run antivirus scans to identify if any infection remains.

* Worm Eradication

1. Identify the entry point or initial infection vector of the worm to prevent reinfection.
2. Run antivirus and anti-malware scans on infected systems to detect and remove the worm. Ensure that antivirus signatures are up to date and perform thorough scans of both files and system memory.
3. monitor the progress of the removal operation. This includes regularly checking the status of antivirus scans and ensuring that infected systems are being properly cleaned and restored to a secure state.
4. Perform additional scans with different antivirus or anti-malware programs to ensure that no remnants of the malware remain.
5. Update the affected systems with the latest security patches and software updates to remediate vulnerabilities exploited by the Trojan. Prioritize critical systems and ensure that all security patches are deployed promptly.

* Trojan Eradication

1. Manually identify and remove any malicious files, registry entries, scheduled tasks, or startup entries associated with the Trojan. Exercise caution when deleting files to avoid removing critical system files.
2. Run antivirus and anti-malware scans on infected systems to detect and remove the Trojan. Ensure that antivirus signatures are up to date and perform thorough scans of both files and system memory.
3. Monitor the progress of the removal operation. This includes regularly checking the status of antivirus scans and ensuring that infected systems are being properly cleaned and restored to a secure state.
4. Perform additional scans with different antivirus or anti-malware programs to ensure that no remnants of the malware remain.
5. Update the affected systems with the latest security patches and software updates to remediate vulnerabilities exploited by the Trojan. Prioritize critical systems and ensure that all security patches are deployed promptly.

5.1.4 MALWARE RECOVERY

1. Change all passwords associated with affected systems including user accounts and emails.
2. If you have backups of your data from before the malware infection occurred, consider restoring your system from those backups. Make sure the backups are clean and free from malware before restoring.
3. Conduct a thorough root cause analysis to identify the underlying vulnerabilities, misconfigurations, or security gaps that allowed the malware infection to occur. Take steps to address these issues to prevent future malware infections.

NB: Document the findings during the incident response process for use in post-incident activities

## 5.2 PHISHING

Phishing is a type of scam where people receive fake emails or messages that appear to be from legitimate companies. The goal is to trick individuals into sharing their confidential and sensitive information such as passwords, credit card numbers, and other personal data. There are various types of phishing attacks; Spear phishing, Vishing, Email phishing, and Pharming.

5.2.1 PHISHING IDENTIFICATION

1. Check the sender's email address for any inconsistencies or suspicious domain names. Phishers often use email addresses that mimic legitimate organizations but contain slight variations or misspellings.
2. Phishing emails often contain spelling or grammatical errors. Look for unusual sentence structures, awkward phrasing, or poor language quality.
3. Phishers often use urgency or fear tactics to manipulate victims. Be cautious of emails that create a sense of urgency, demand immediate action, or threaten consequences for non-compliance.
4. Always be doubtful when you receive emails that ask you for money, whether that’s for expenses, fees, or other costs.
5. Emails may use tricks, such as free prizes or other rewards, to convince people to hand over money or personal information.
6. By carefully examining the URL of the website you're visiting. Phishing websites may mimic legitimate sites by using similar domain names or URLs that include additional subdomains or random characters.
7. Be cautious of websites that generate multiple pop-up windows or redirect you to other sites without your consent. These websites may try to deceive you into providing sensitive information or downloading malicious software.
8. Unexpected requests, such as someone claiming to be a colleague or authority figure asking for sensitive information or money.
9. Phishing emails often use generic salutations like "Dear Customer" instead of addressing you by name. Legitimate organizations usually personalize their communications.

5.2.2 PHISHING CONTAINMENT

1. Quarantine affected systems and remove them from the network, or apply access controls to isolate them from production networks.
2. Block access to any identified Remote Access Tools (RATs) to prevent communication with command and control servers, websites, and exploited applications.
3. Identify compromised or at risk user credentials and reset them immediately.
4. Scan the system to detect any malicious code.

5.2.3 PHISHING ERADICATION

1. The primary defense against phishing attacks is a Secure Email Gateway. Email gateways filter malicious messages and automatically quarantine them before they reach users. Proofpoint email gateways can detect compromised accounts and prevent them from sending spam or phishing emails to your partners, ensuring your company's reputation remains intact.
2. You can use technologies such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) to authenticate email senders and prevent domain spoofing.
3. Require multi-factor authentication (MFA) for accessing sensitive systems and applications.

### 5.2.1 PHISHING IDENTIFICATION

* Phishing through Text Identification

1. Carefully examine the sender's name displayed in the email. Attackers may use familiar or trusted names to deceive recipients. Pay attention to any slight variations or misspellings in the sender's name.
2. Look closely at the sender's email address. Attackers may use email addresses that mimic legitimate ones but have slight differences or unusual domain names. Watch out for misspellings, additional characters, or unfamiliar domains.
3. Be cautious of emails that create a sense of urgency, demand immediate action, or threaten negative consequences for not complying. Attackers often use urgency to pressure recipients into making hasty decisions without proper scrutiny.
4. Be cautious of emails that use generic greetings like "Dear Customer" instead of addressing you by name. Legitimate organizations often personalize their communications.
5. Hover your mouse cursor over any links in the email without clicking. Verify that the displayed URL matches the expected destination. Be cautious of mismatched or suspicious URLs that may lead to phishing websites.
6. Examine the email headers for any signs of manipulation or suspicious activity. Look for mismatched domains, unauthorized email relays, or unusual IP addresses.
7. If you receive an email from someone you don't know or an unexpected source, be cautious. Verify the legitimacy of the email through other trusted communication channels.
8. Establish a reporting mechanism within your organization to encourage employees to report suspicious emails promptly. Reporting can help raise awareness and enable the organization to take appropriate actions.

* Vishing Identification

1. Inconsistencies and contradictions in caller’s story.
2. If the caller claims to be from a legitimate organization but his caller ID says otherwise.
3. Pressure to provide sensitive information.
4. Threats of consequences for not complying.
5. Urgent and threatening tone.
6. Receiving unusual requests such as transferring funds, installing software, or providing remote access to your device.

### 5.2.2 SPEAR PHISHING CONTAINMENT

1. Assess the extent of the spear phishing attack by identifying the affected systems, accounts, or individuals. Determine if any sensitive data has been compromised.
2. If a specific system or account is compromised, isolate it from the network to prevent further spread of the attack. Disconnect compromised devices from the network or disable compromised accounts.
3. Inform the appropriate internal stakeholders, such as the IT department, incident response team, and management, about the spear phishing incident. Provide them with relevant details and any evidence collected.
4. Instruct affected individuals to immediately change their passwords for all relevant accounts, including email, network, and other systems. Encourage the use of strong, unique passwords or passphrases
5. Implement or enforce the use of MFA (Multi Factor Authentication) for all accounts where feasible. This adds an extra layer of security by requiring additional verification beyond just a password.
6. Preserve any available evidence related to the spear phishing incident, such as email headers, attachments, or network logs. This evidence can aid in the investigation and potential legal actions.
7. Analyze the attack vector and determine how the spear phishing attack was executed. Assess the potential impact on systems, data, or operations to understand the extent of the breach.
8. Evaluate the effectiveness of the incident response plan and make necessary updates based on lessons learned from the spear phishing incident
9. Implement enhanced monitoring and logging capabilities to detect any further spear phishing attempts or suspicious activity. Continuously monitor systems and network traffic for indicators of compromise.

Vishing Containment

If you have already executed requests such as giving out system and account credentials, installing software or providing remote access to your device;

1. Quarantine affected systems and remove them from the network, or apply access controls to isolate them from production networks.
2. Disable other wireless connectivity to other devices.
3. Reset the usernames and passwords of the systems and accounts associated with the compromised credentials.
4. Scan your system for malware.
5. In case you have already been tricked into completing a transaction, get in touch with your bank or service provider and disclose the attack along with crucial information.

### 5.2.6 SPEAR PHISHING ERADICATION

1. Deploy advanced spam filters and email security solutions that can detect and block spear phishing emails before they reach users' inboxes. These solutions use various techniques, such as machine learning and reputation analysis, to identify and filter out malicious emails.
2. Utilize secure email gateways that perform deep inspection of email content and attachments. These gateways can detect and prevent spear phishing attacks by analyzing email headers, links, and attachments for signs of malicious intent.
3. Implement web filtering solutions that can block access to known phishing websites and suspicious URLs (Uniform Resource Locators). These solutions can help prevent users from inadvertently visiting malicious websites or clicking on phishing links.
4. Conduct simulated phishing campaigns within your organization to test employees' awareness and responsiveness to spear phishing attempts. Use the results to identify areas that require further training and reinforcement.
5. Develop a comprehensive incident response plan specifically tailored to address spear phishing incidents.
6. Perform regular security audits and assessments to identify vulnerabilities and weaknesses in your organization's security controls. Use the findings to enhance your security posture and address any gaps.

Vishing Eradication

1. Contact Law Enforcement and the service provider of the call number and report the situation.
2. Block contact used by the attacker.
3. Implement caller ID authentication technologies, such as STIR/SHAKEN (Secure Telephony Identity Revisited/Signature-based Handling of Asserted information using toKENs).

## 5.3 DENIAL/DISTRIBUTED DENIAL OF SERVICE ATTACK

DoS/DDoS is a cyberattack in which the attacker floods a server with internet traffic with the goal of exhausting the target system’s resources, which, in turn, renders the target unreachable or inaccessible, denying legitimate users access to the service.

### 5.3.1 DoS/DDoS IDENTIFICATION

1. Abnormally high network traffic.
2. Unavailability or inaccessibility of websites.
3. Network latency (a delay in network communication) or unusually slow network performance in opening files or accessing websites.
4. Suspicious amounts of traffic originating from a single IP address or IP range
5. Firewalls and Intrusion Detection systems may detect and trigger alerts when they detect unusual traffic patterns or an influx of traffic from specific IP addresses. Pay attention to any unexpected alerts or notifications from your network security systems.

### 5.3.2 DoS/DDoS CONTAINMENT.

**Step 1: Block the Initial Attack**

1.1 Access network and server logs to identify patterns in traffic that indicate the source of the attack. Look for signs of unusual traffic, such as high volumes from specific IP addresses, unusual ports, or protocols.

1.2 Block by IP Address:

Identify both internal and external IP addresses contributing to the attack.

Update firewall rules to block the identified IP addresses.

Use Access Control Lists (ACLs) to restrict traffic from suspicious IP addresses.

1.3 Determine if the attack is originating from specific geographical regions and apply geofencing rules to block traffic from those regions, especially if the attack appears to be localized.

1.4 Power Down Compromised Local Devices

-Examine logs and network monitoring tools to identify local devices that are generating malicious traffic.

-Immediately isolate these devices from the network to prevent further contribution to the attack.

-Power down compromised devices to stop them from generating traffic. Ensure that this step is coordinated with IT support to avoid disrupting critical services.

**Step 2: Side-Step the Attack**

2.1 Change Server IP Address

- Assign a new IP address to the affected server.

- Update DNS records to reflect the new server IP address.

- Communicate the expected propagation time for DNS changes to stakeholders and customers.

2.2 Change Router IP Address

- Reassign the router's public-facing IP address.

- Ensure that the new router IP address is properly configured in network settings and firewall rules.

- Verify that the new configuration maintains connectivity and does not disrupt other services.

2.3 Change Website URL

- Set up a new domain or subdomain to point to the server.

- Implement HTTP 301/302 redirects from the old URL to the new one.

- Update DNS records to ensure that the new URL resolves correctly.

- Inform users and stakeholders of the temporary URL change and provide the new URL.

**Step 3: Stop the Service**

3.1 Determine which services are critical to business operations and which can be temporarily halted without causing significant harm.

3.2 Identify any dependencies between services to ensure stopping one does not unintentionally impact others.

3.3 Inform relevant internal teams and stakeholders about the decision to stop the affected service.

3.4 Safely stop the affected service to minimize disruption and prevent data loss.

3.5 Disable web services or specific endpoints under attack.

3.6 Temporarily take down applications or features such as file downloads, shopping carts, etc.

3.7 Isolate and power down internal routers or other network devices if they are the target.

**NB:** Stopping the service under attack is a last-resort measure to protect the overall integrity of the network and operations. This step should only be pursued if steps 1 and 2 cannot provide enough time to pursue other steps below.

## 5.3.3 DoS/DDoS ERADICATION

1. Set up continuous monitoring and automated alert systems to detect and respond to potential DDoS attacks early. Use anomaly detection tools to identify unusual traffic patterns that may indicate an impending attack.
2. Looking at the number of traffic coming in and out of the servers and systems and limiting how much we will accept over a specific time interval.
3. Ensure all network devices, including routers, firewalls, and servers, are configured securely and have the latest security patches.
4. Engage with a DDoS protection service provider that can offer real-time mitigation against large-scale attacks.
5. Employ anti-virus solutions to prevent malware infections.

# **5.4 SESSION HIJACKING**

Session hijacking refers to the malicious act of taking control of a user’s web session. It is when someone steals your digital "key" that allows you to access a website or online service. This key, called a session token, proves to the website that you are who you say you are.

By stealing this key, an attacker can pretend to be you and access your account, data, or perform actions on your behalf without your knowledge.

## 5.4.1 SESSION HIJACKING IDENTIFICATION

1. Unexpected changes in session durations or locations
2. Multiple concurrent sessions from different IP addresses
3. Unusual patterns of session activity that could indicate scripted attacks
4. Users are frequently logged out unexpectedly, indicating potential session disruption.
5. Significant changes in traffic patterns or unexpected high traffic volumes may indicate an attacker is manipulating sessions

## 5.4.2 SESSION HIJACKING CONTAINMENT

1. Terminate the affected sessions and reset the session tokens.
2. Users should be prompted to change their passwords immediately, and any security loopholes that were exploited should be closed.
3. Conduct a detailed forensic analysis to understand how the attack occurred, what vulnerabilities were exploited, and what data may have been compromised.
4. Examine server and application logs to trace the attacker’s actions and identify the scope of the breach.

## 5.4.3 SESSION HIJACKING ERADICATION

1.Ensure all communication between the client and server is encrypted using HTTPS. This prevents attackers from intercepting session cookies.

2. Implement a short session timeout period to reduce the window of opportunity for an attacker.

3. Regenerate the session ID after successful login and periodically during the session to prevent fixation.

4.Store the user's IP address and User-Agent in the session and validate them on each request.

5.Implement MFA to add an additional layer of security, making it harder for attackers to hijack sessions.

6.Use CSP to prevent cross-site scripting (XSS) attacks, which can be used to steal session cookies.

## 5.4.3 SESSION HIJACKING RECOVERY

1. Invalidate Compromised Sessions: Immediately invalidate the hijacked session to prevent further unauthorized access.

2. Force User Re-authentication: Require the affected user to log in again to ensure that the session is valid.

3. Notify the User: Inform the user about the potential hijacking attempt and advise them to change their password and review their account for any unauthorized activity.

4. Log and Analyze the Incident: Record details such as IP addresses, User-Agent strings, timestamps, and any actions taken during the compromised session. Look for patterns or anomalies that may indicate how the session was hijacked.

5. Educate Users: Educate your users about best practices for security, such as recognizing phishing attempts, using strong passwords, and enabling multi-factor authentication (MFA).

6. Implement Rate Limiting and CAPTCHA: Use rate limiting and CAPTCHA to prevent automated attacks that might exploit session vulnerabilities.

7. Consult Security Experts: If the incident is severe or if you are unable to identify the cause, consult with security experts to conduct a detailed investigation and provide recommendations.

# **5.5 SQL INJECTION ATTACKS**

SQL injection is a hacking method that tries to mess up the connection between a website and its database. Hackers do this, in order to trick the database into executing malicious code. This attack often works because of too much access given to users, user inputs that aren't properly checked, or actual flaws in the database software. Preventing SQL injection can be tricky because it can happen even if there are no obvious software issues, so it's not always just about installing a security update.

## 

## 5.5.1 SQL INJECTION IDENTIFICATION

1. **Unusual Database Error Messages:** If your application displays unexpected database error messages, it might be a sign of SQL injection attempts.
2. **Unexpected Data:** Look for any unexpected or modified data in your application, which could indicate unauthorized access.
3. **Changes in Application Behavior:** Notice any changes such as slow response times or increased server load.
4. **SQL Syntax Errors:** Check your application logs for SQL syntax errors or warnings.
5. **Unauthorized User Accounts:** Monitor your database for the presence of unauthorized user accounts or privileges.
6. **Login Bypass:** Ability to log in without correct credentials by using SQL injection payloads.

## 5.5.2 SQL INJECTION CONTAINMENT

1. **Isolate the Affected System:**

* Temporarily disconnect the affected system from the network to prevent further unauthorized access.
* Quarantine the Application: If possible, take the compromised application offline to stop the attack.

1. **Identify the Source and Scope:**

* Check server and database logs to identify the source of the attack and the extent of the compromise.
* Analyze the Payload: Determine the specific SQL injection payloads used to understand how the attack was executed.

1. **Change Credentials:**

* Update Database Credentials: Change database user passwords to prevent the attacker from using any compromised credentials.
* Review Access Controls: Ensure that only authorized personnel have access to sensitive systems.

1. **Fix Vulnerable Code:** Update the code to use prepared statements and parameterized queries to prevent SQL injection.

## 5.5.3 SQL INJECTION ERADICATION

**Network Level:**

1. Deny access to the internet except through proxies for Store and Enterprise servers and workstations.
2. Implement firewall rules to block or restrict internet and intranet access for database systems.
3. Implement firewall rules to block known malicious IP addresses.

**System / Application Level:**

1. Secure both the operating system and the application.

* Consider using NIST or other industry standard security checklists to harden both the operating systems and the applications Produced 2009 by US-CERT, a government organization.
* Run only the minimum required applications and services on servers necessary to

perform their intended function. In other words, disable all unnecessary applications and services.

* Follow application vendor security guidelines.

1. Update and patch production servers regularly.

* Include both operating system patches and application patches.

1. Disable potentially harmful SQL stored procedure calls.

* ‘xp\_cmdshell’ on MSSQL has been frequently used by attackers.

1. Deny extended URLs.

* Excessively long URLs can be sent to Microsoft IIS servers, causing the server to fail to log the complete request. Unless specific applications require long URLs, set a limit of 2048 characters. Microsoft IIS will process requests over 4096 bytes long, but will not place the contents of the request in the log files. This has become an effective way to evade detection while performing attacks.

1. Sanitize/validate input.

* Ensure data is properly typed.
* Ensure data does not contain escaped code.
* Consider using type-safe stored procedures/prepared statements.

1. Ensure error messages are generic and do not expose too much information.

* Keep error messages short and usable.
* Do not disclose internal database structure, table names, or account names.

1. Use principles of least privilege.

* Install and run authorized Microsoft SQL Server and IIS services under a non privileged account.
* Apply the principle of 'least privilege' on all SQL machine accounts.
* Remove guest accounts unless operationally necessary.
* Use an application account for database access.

1. Enforce best practice password and account policies.

* Require the use of a password on Microsoft SQL Server administrator, user, and machine accounts.
* Change default/built-in account passwords.
* Change application account passwords regularly.
* Use strong passwords.
* Lock out accounts after several unsuccessful logon attempts.

## 5.5.4 SESSION HIJACKING RECOVERY

## Identify the Vulnerability:

* Check your firewall logs, IIS logs, web pages, and SQL Server tables to locate the source of the injection.

1. Analyze the Damage:

* Determine what data or objects have been affected. Tools like ApexSQL Log can help audit and revert changes by reading transaction logs.

1. Remove Malicious Content:

* Clean up any malicious code or backdoors that may have been inserted into your database or web application.

1. Recover Data:

* Use tools like ApexSQL Recover to restore deleted or damaged data. This tool can mine the transaction log to recover lost data.

1. Patch the Vulnerability:

* Update your code to prevent SQL injection vulnerabilities. This includes using parameterized queries and stored procedures.

# **5.6 BRUTE FORCE ATTACK**

A brute force attack is a technique employed to acquire private user data like usernames, passwords, passphrases, or Personal Identification Numbers (PINs). These attacks are commonly executed through a script or bot to repeatedly attempt different combinations until the correct one is identified. Essentially, it is an unauthorized access method where attackers systematically try all possible password or key combinations to breach a system.

## 5.6.1 BRUTE FORCE ATTACK IDENTIFICATION

1. Login attempts at unusual hours can be a sign of automated brute force attacks.
2. Multiple failed login attempts from the same IP address. Although, this could be a result of a proxy server being used by a large organization.
3. Login attempts with multiple usernames from the same IP address. Again, this could simply be from a large organization.
4. Multiple login attempts for a single username coming from different IP addresses. This could also be a single person using a proxy.
5. An unusual pattern of failed login attempts, for example, following a sequential alphabetical or numerical pattern.
6. An abnormal amount of bandwidth being used after a successful login attempt. This could signal an attack designed to steal resources.

## 5.6.2 BRUTE FORCE ATTACK CONTAINMENT

1. Temporarily lock accounts after a certain number of failed login attempts to prevent further attempts from the same account.
2. Block the IP addresses that are identified as sources of brute force attacks. This can be done through firewall rules or security software.
3. Forcefully terminate active sessions that were initiated from suspicious IP addresses or accounts.
4. Limit the number of login attempts from a single IP address within a specific time frame. This can slow down or halt brute force attacks.
5. You should also disconnect any devices or services that are not essential for your operations or recovery.

## 5.6.3 BRUTE FORCE ATTACK ERADICATION

1. Utilizing or requiring strong passwords
2. Allowing a limited number of login attempts
3. Employing the use of CAPTCHAs
4. Setting time delays between attempts
5. Asking security questions
6. Enabling or requiring two-factor authentication
7. Using multiple login URLs
8. Tricking the attack software. For example, some bots are trained to recognize errors, but you could use redirects to different failure pages for simultaneous failed login attempts. This would mean that the attacker would at least need to step things up with more sophisticated software.
9. You should also scan your systems or accounts for any malware, backdoors, or vulnerabilities.
10. You should verify that your systems or accounts are functioning normally and securely.

## 5.6.4 BRUTE FORCE ATTACK RECOVERY

1. Assess the Impact

Identify Compromised Accounts: Determine which accounts, if any, were successfully compromised during the attack.

Review Logs: Analyze server and application logs to understand the scope and nature of the attack. Look for patterns in failed and successful login attempts.

Check for Unauthorized Access: Investigate any suspicious activities or changes made by potentially compromised accounts.

2. Secure the System

Change Compromised Passwords: Immediately reset passwords for all compromised accounts. Ensure that new passwords are strong and unique.

Update Security Measures: Apply any security patches and updates to your systems to address vulnerabilities that may have been exploited.

Enable Multi-Factor Authentication (MFA): If not already in place, implement MFA for all user accounts to add an extra layer of security.

3. Notify Affected Users

Communicate with Users: Inform affected users about the breach and the steps being taken to secure their accounts. Encourage them to change their passwords and enable MFA.

4. Monitor for Further Attacks

Continuous Monitoring: Set up real-time monitoring and alerts for suspicious activities, such as multiple failed login attempts or login attempts from unusual locations.

Review Security Logs: Regularly review security logs to detect any signs of ongoing or new attacks.

# **5.7** MAN IN THE MIDDLE ATTACK (MITM)

Man in the middle attack (MITM) is an attack where the perpetrator positions himself in a conversation between a user and an application either to eavesdrop or to impersonate one of the parties. The goal of the attack is to steal personal information such as login credentials, account details and credit card numbers. Information gained by the attacker can be used for many purposes, including identity theft, unapproved fund transfer or password change.

## 5.7.1 MAN IN THE MIDDLE IDENTIFICATION

1. Website names might be wrongly misspelled (e.g., [www.g00gle.com](http://www.g00gle.com) instead [www.google.com](http://www.google.com))
2. No "S" in the "HTTPS" connection in the web browser
3. If you are asked to log in again unexpectedly on a website where you were already authenticated, it could be an attempt to capture your credentials
4. If you receive unusual security warnings or certificate errors from websites you normally trust, it could be a sign of a MitM attack. For example, if a website's certificate cannot be verified or is reported as invalid, it might be intercepted.
5. An unexpected slowdown in your internet connection might be a result of a MITM attack, where the attacker is intercepting and possibly modifying data.

## 5.7.2 MAN IN THE MIDDLE CONTAINMENT

1. Isolate any systems or devices that are suspected to be compromised from the network to prevent the attacker from intercepting more data.
2. Restrict access to the network for all non-essential devices and users until the situation is under control.
3. Block malicious IP addresses that are identified, block them at the firewall level to cut off the attacker’s access to your network.
4. Immediately reset passwords for all user accounts, especially those that may have been intercepted during the attack.
5. Ensure all systems and applications are up to date with the latest security patches to close any vulnerabilities.

## 5.7.3 MAN IN THE MIDDLE ERADICATION

1. Do not allow workers to use public networks for any confidential work
2. Implement virtual private network to secure connections from your business to online application and enable employees to securely connect to your internal private network from remote locations
3. Ensure sensitive online transactions logins are secure with HTTPS using browser plugins like HTTPS everywhere
4. Use high security level of web browser
5. Utilize authentication credentials such as token or two factor authentication for sensitive accounts

## 5.7.4 MAN IN THE MIDDLE RECOVERY

1. Disconnect any systems you suspect have been affected from the network to prevent further data interception
2. Determine how the attacker gained access to your network. This could involve inspecting network logs, firewall logs, and using network analysis tools like Wireshark.
3. Check for compromised data that may have been intercepted or altered. This includes sensitive information such as login credentials, personal data, financial information, and other critical data.
4. Notify all affected users, employees, and stakeholders about the breach. Provide guidance on what steps they need to take to protect themselves, such as changing passwords and monitoring for suspicious activity.
5. Educate users about security best practices, phishing scams, and how to recognize potential security threats. Regular training can help prevent future attacks
6. Set up continuous monitoring and alert systems to detect unusual network activity and potential future attack

# **5.8.** DNS TUNNELING

DNS tunneling is a technique that routes DNS requests to the attacker's server, providing attackers a covert command and control channel, and data exfiltration path.

## 5.8.1 DNS TUNNELING CONTAINMENT

1. Tunneling activity may be indicated by an unusually high volume of DNS requests or by a regular pattern of queries to the same domain or subdomains.
2. Tunneling may be indicated by unusually large DNS request volumes coming from or going to a single server or domain.
3. Automated and periodic requests that do not correspond to user activity can signal malicious use.

## 5.8.2 DNS TUNNELING MITIGATION

1. Isolate critical systems and data from general network traffic to minimize the impact of any potential DNS tunneling attacks.
2. Configure firewalls and network devices to allow DNS traffic only to known and trusted DNS servers.This prevents unauthorized DNS queries from reaching potentially malicious external DNS servers, reducing the risk of tunneling.
3. Use advanced DNS security solutions that can filter and inspect DNS queries and responses for signs of tunneling.These solutions can detect and block suspicious DNS traffic in real-time, preventing malicious activities.
4. Set rate limits on the number of DNS queries that can be made by a single host or device within a specific time period.This helps to mitigate the impact of DNS tunneling by limiting the volume of data that can be transferred using DNS queries.

## 5.8.3 DNS ERADICATION

1. A Virtual Private Network (VPN) can encrypt all your internet traffic, including DNS queries. Select a VPN service that provides secure, encrypted DNS resolution as part of its service.
2. Invest in specialized DNS security appliances or subscribe to DNS security services that offer advanced threat detection and response capabilities from vendors like Cisco Umbrella, Infoblox, and Palo Alto Networks provide comprehensive DNS security features.
3. Develop training materials such as presentations, videos, and handouts. Include real-world examples and case studies of DNS tunneling attacks.
4. Regularly update DNS server software to the latest version to patch known vulnerabilities.

## 5.8.4 DNS TUNNELING RECOVERY

1. Apply the most recent security updates and patches to firewalls, DNS servers, and other network security appliances.
2. Eliminate any malware, backdoors, or unapproved software that the attacker may have installed. If required, reinstall operating systems.
3. Remove compromised systems from the network to stop additional attacks or data leaks.
4. Inform employees of the dangers of DNS tunneling and the need of following security best practices.
5. To identify and stop erroneous DNS traffic, use DNS security tools like response policy zones (RPZ), DNS filtering, and DNSSEC (DNS Security Extensions).