|  |
| --- |
| ***MENTOR: MD. SHAIFU ZAMA*** |
| ***TEAM: AMIT KUMAR SAMANTA***  ***GOPU SATYA TARUN***  ***ANALA VASUKI SAI MANGA TAYARU*** |



**[Attack mitigation** is a detection and protection strategy used to safeguard **networks**, servers and applications by IT administrators in order to minimize the effect of malicious traffic and intrusion attempts while maintaining functionality for users.**]**

***NETWORK ATTACKS AND MITIGATION BY USING KALI LINUX***

***NETWORK ATTACKS AND MITGAION BY USING KALI LINUX***

**Introduction:**

The aim of the project is to acquire knowledge regarding the network attacks and to mitigate the attacks using various technologies. Here we come across the attack generation and detection where few Kali Linux tools are used to demonstrate it.

**Devices:**

Cisco networking devices are used.

**Services:**

Port security, static routing and SSH services are used.

**Tools:**

Metasploit Framework, Ettercap, Sqlmap ...etc are few tools used for attacking the network.

While wireshark, Nmap, Aircrack-ng, Nikto, metalsploit framework … etc are few Kali Linux tools.

Nslookup is an awesome tool to use when using Kali and is used to resolve a fully qualified domain name into an IP address.

**Network Attacks:**

Few major attacks that we come across are:

1. Password based attack

2. Malware Attack

3. DOS Attack

4. IP Spoofing

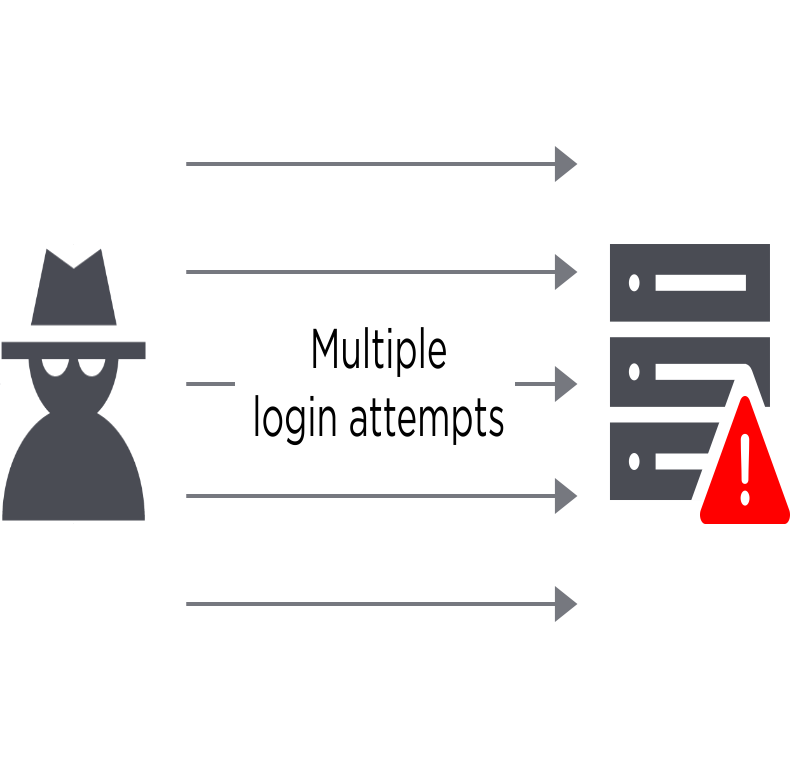
5. Man in the Middle Attack

6. SQL injection Attack

7. XSS Attack

1. **Password based attack:**

In this case the attackers try to duplicate a valid login or password sequence by multiple login attempts.

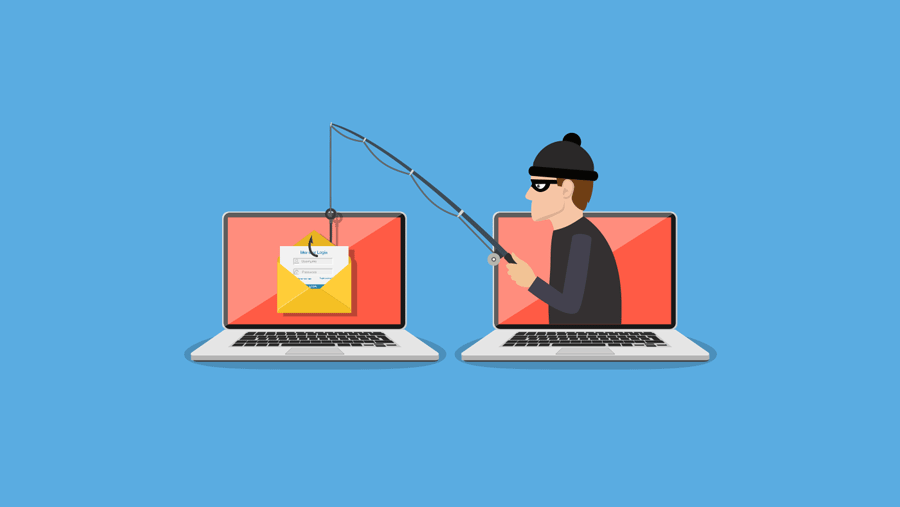


**Mitigation Technique**:

The solution typically entails a combination of strong password requirements, accounts lockouts, throttling authentication attempts, logging, and multi-factor authentication (MFA).

1. **MALWARE ATTACK:**

A malware attack is when cybercriminals create malicious software that’s installed on someone else’s device without their knowledge to gain access to personal information or to damage the device, usually for financial gain.

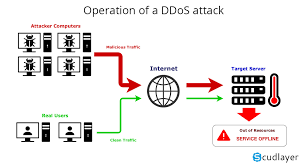
**

**Mitigation Technique**:

These include but are not limited to keeping the software updated, installing anti-**malware** and anti-virus software, running periodic checks on the computer, using security tokens and firewalls, avoid using open networks and adding protective layers to keep sensitive data secure.

1. **DOS Attack:**

**I**n computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

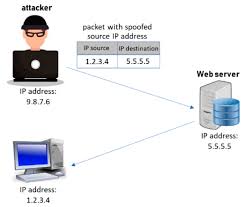


**Mitigation Techniques**:

* **Attack** Detection. The first step of any **mitigation** strategy is understanding when you are the target of a **DoS attack**. ...
* IP Whitelisting/Blacklisting. ...
* Rate Limiting. ...
* Upstream Filtering and DDS. ...
* Programming for Scale.

1. **IP SPOOFING:**

**IP spoofing** is the creation of Internet Protocol (**IP**) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. ... If the packet has been **spoofed**, the source address will be forged.



**Mitigation Techniques**:

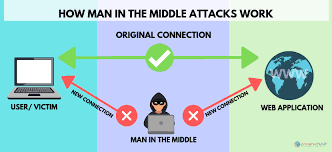
## **1.Block IP addresses**

## **2.Implement ACLs (access control lists)**

## **3.Use reverse path forwarding (ip verify)**

1. **Man in the Middle Attack:**

In cryptography and computer security, a **man-in-the-middle attack** (MITM), also known as a hijack **attack** is an **attack** where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.



**Mitigation Techniques**:

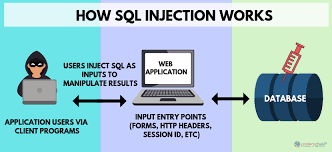
1. Employ Encryption.

2. Verify TLS/SSL Setups.

3. Manage Enterprise-Wide Certificates.

1. **SQL INJECTION ATTACK:**

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application.

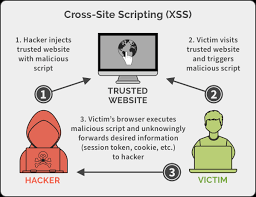


**Mitigation Techniques**:

* [Input validation](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "3)
* [Parametrized queries](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "4)
* [Stored procedures](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "5)
* [Escaping](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "6)
* [Avoiding administrative privileges](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "7)
* [Web application firewall](https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/" \l "8)

1. **XSS Attack:**

**Cross-Site Scripting** (**XSS**) **attacks** are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. **XSS attacks** occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.



**Mitigation Techniques**:

* **Filter input on arrival.** At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
* **Encode data on output.** At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
* **Use appropriate response headers.** To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
* **Content Security Policy.** As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.
* **Network Attack Prevention Tips:**

Some of the network attacks can be prevented by following ways:

* Install software updates
* Use unique password
* Use two-factor authentication
* Use strong password
* Use password manager
* Use firewall for your internet connection
* Browse safely online
* Clear browser after leaving computer

\_\_