**CYBERYOUTH**

**Nonformal education for cyber-security training & resilience of youth organisations and young people**

***Cybersecurity online youth academy***

****

**Vulnerabilities, Attack, Techniques, and Threats**

Table of contents

[Introduction](#_heading=h.fpb3yt6tcffi)

[It could have happened to you…](#_heading=h.c7zxm1r80lor)

[What you will learn](#_heading=h.bd1t10x6k115)

[Why it is important](#_heading=h.1fqj6c1n3ygs)

[How it can help you in everyday life](#_heading=h.bddh90wxykhs)

[What career you can pursue](#_heading=h.l25siuf1d90q)

[Pre-requisites](#_heading=h.obikvf4haym5)

[Material](#_heading=h.snpqznqbwxs)

[2.1 Social Engineering Techniques](#_heading=h.2yz7x8bu8zb5)

[Phishing](#_heading=h.lzulet6qo51l)

[Impersonation](#_heading=h.pa4cto6ggiyl)

[Dumpster Diving](#_heading=h.2nku6pu7cn0y)

[Shoulder Surfing](#_heading=h.wr9hwff7j19z)

[Hoaxes](#_heading=h.bokmhdgx2zad)

[Watering Hole Attacks](#_heading=h.f78dhc7ivwau)

[Other Social Engineering Attacks](#_heading=h.r2tc4qk70oa5)

[Tailgating](#_heading=h.xn1pz9g87m8d)

[Invoice Scams](#_heading=h.mux1i75sot55)

[Conclusions](#_heading=h.q7y4utybp22l)

[2.2 Malware, Password Attacks, Physical Attacks, and Cryptographic Attacks](#_heading=h.wv8lmqsplpdd)

[Malware](#_heading=h.se3v82rotiu3)

[Password Attacks](#_heading=h.xa9iyn2x8esy)

[Physical Attacks](#_heading=h.3uw9tlbm0qe0)

[Malicious Universal Serial Bus (USB) cable](#_heading=h.g61b98n78hyq)

[Malicious Flash Drive](#_heading=h.7a85vxlxk24f)

[Skimming and Card Cloning](#_heading=h.i7smjsd67e63)

[Cryptographic Attacks](#_heading=h.k0foyer7huma)

[Birthday Attacks](#_heading=h.vvtxho23j43n)

[Collisions](#_heading=h.f3aujvhntcxv)

[Downgrade Attacks](#_heading=h.uxcuqzlpnlt)

[Conclusions](#_heading=h.jn7khpgf6mc9)

[2.3 Application Attacks](#_heading=h.g98km9urykdd)

[Cross-site Scripting](#_heading=h.d7j3sia9a2ue)

[Injection Attacks](#_heading=h.4rgr0sqkydi2)

[Buffer Overflows](#_heading=h.uu16mwe9cyzf)

[Replay Attacks](#_heading=h.aymlrjsxfl61)

[Request Forgeries](#_heading=h.ftn9wk72fv0s)

[Client-Server Architecture](#_heading=h.ardbnoqe7dks)

[Cross-Site Request Forgery (CSRF)](#_heading=h.qtcgn5j17qh1)

[Server-Side Request Forgery (SSRF)](#_heading=h.ix0f7ux1htyo)

[SSL Stripping](#_heading=h.pvms5389485n)

[What is SSL Stripping?](#_heading=h.trpmwlsq4ou5)

[How does SSL Stripping work?](#_heading=h.iszmb4va4v0j)

[Other Application Attacks](#_heading=h.rysu0c5swhxe)

[Conclusions](#_heading=h.ostdn54761l3)

[2.4 Network Attacks](#_heading=h.7pii0khen2cd)

[Rogue Access Points and Evil Twin](#_heading=h.byj2zirdlb0u)

[Rogue Access Points](#_heading=h.wsm452frqt02)

[Evil Twin Attacks](#_heading=h.ye32j6jz4n4j)

[Bluejacking and Bluesnarfing](#_heading=h.k4ckzix3tm3t)

[Bluejacking](#_heading=h.yl7gimyfb6g7)

[Bluesnarfing](#_heading=h.y0albsmjvgmv)

[Wireless Disassociation Attacks](#_heading=h.orqrn6qc565u)

[Wireless Jamming](#_heading=h.vjcqsj4bsmwp)

[RFID and NFC Attacks](#_heading=h.37am6mh0cj8h)

[RFID and NFC Technology](#_heading=h.574pgyebzznl)

[MAC Flooding and Cloning](#_heading=h.fx20s9j7icyq)

[MAC Flooding](#_heading=h.91g0i6aqx3k3)

[MAC Cloning](#_heading=h.f48rt3lrrrdo)

[DNS Attacks](#_heading=h.v0ty472ottau)

[DNS Poisoning](#_heading=h.4s8k7ye9jxrs)

[Domain Hijacking](#_heading=h.4mnfmlhrp9s)

[URL Hijacking](#_heading=h.ip53996lztgj)

[Domain Reputation](#_heading=h.o7fs8ps3yne2)

[Conclusions](#_heading=h.8fgh3pvuc4s3)

[2.5 Threat Actors, Vectors and Threat Intelligence Sources](#_heading=h.azw51npc11fy)

[Threat Actors](#_heading=h.ucvhdpx4godb)

[Attack Vectors](#_heading=h.eixtosnyduw0)

[Threat Intelligence](#_heading=h.rpetdaosatfp)

[Conclusions](#_heading=h.scbfee5behhv)

[2.6 Vulnerabilities](#_heading=h.hxk9abfklxgp)

[Vulnerability Types](#_heading=h.tqdszam6087u)

[Zero-day attacks](#_heading=h.mn6upcikdctv)

[Open permissions](#_heading=h.37zjomisizf7)

[Unsecured root accounts](#_heading=h.1eajqg1gcow7)

[Errors](#_heading=h.ea8dr3tugfev)

[Weak encryption](#_heading=h.oae4f6lp68fb)

[Insecure protocols](#_heading=h.4y35qh4gmawu)

[Default settings](#_heading=h.kkejfnvph1mf)

[Open ports and services](#_heading=h.69o5ohzgwrmh)

[Improper patch management](#_heading=h.nbar7adiozb3)

[Legacy platforms](#_heading=h.719ycey7elbb)

[Third-party Risks](#_heading=h.bae6rc5pzej9)

[System Integration Risk](#_heading=h.e1qabc6qxy3d)

[Lack of Vendor Support](#_heading=h.rqy35uirgi0a)

[Supply Chain Risk](#_heading=h.2ve41tmmhi9w)

[Outsourced Code Development](#_heading=h.5k3kdu724leo)

[Data Storage](#_heading=h.hqv8i6djgmk7)

[Vulnerability Impacts](#_heading=h.7yjr9328n6ss)

[Data loss](#_heading=h.3c1xoxduggg)

[Identity theft](#_heading=h.im4zxt363xzw)

[Financial loss](#_heading=h.h41dad1ufnlz)

[Reputation impacts](#_heading=h.21md2bvv754k)

[Availability loss](#_heading=h.ktacfwnb72lz)

[Conclusions](#_heading=h.nmzwup8r2vh3)

[2.7 Security Assessments](#_heading=h.syt91kbcyrsy)

[Threat Hunting](#_heading=h.9ay7suek8orz)

[Intelligence fusion](#_heading=h.esrggyix5ocq)

[Fusing the data](#_heading=h.5wxuj5e6vl21)

[Cybersecurity manoeuvres](#_heading=h.s8rk77cc7bd4)

[Vulnerability Scans](#_heading=h.7ti5mb3kg5p9)

[Scan Types](#_heading=h.9i1sl77g5tth)

[Identifying Vulnerabilities](#_heading=h.s9xjmp55gqsi)

[Vulnerability Research](#_heading=h.su021fpbykzq)

[Vulnerability Scan Log Review](#_heading=h.4zr0tg2x8pob)

[Dealing with False Positives](#_heading=h.65kmvvtf1ktb)

[Dealing with False Negatives](#_heading=h.f0crn6apbc5e)

[Tools](#_heading=h.15jc441vgumc)

[Security Information and Event Management](#_heading=h.2v49sw6y4fxe)

[SIEM & SOAR](#_heading=h.ywn33dsp5c7z)

[Tools](#_heading=h.oeuigkb8fl30)

[Conclusions](#_heading=h.euyxx85k8wz3)

[2.8 Penetration Testing](#_heading=h.wnlmwz5bi4mj)

[Pentest](#_heading=h.knibrfcg9hw8)

[Rules of Engagement](#_heading=h.tkhhilgafzk3)

[Working Knowledge](#_heading=h.t4yundfyilfg)

[Exploiting Vulnerabilities](#_heading=h.cqnwli2seelr)

[The Process](#_heading=h.6txpn3qo6jaq)

[Pentest Aftermath](#_heading=h.gymjpgy8ios2)

[Security Teams](#_heading=h.f1328ppf2bwy)

[Blue Team](#_heading=h.wkytpbwdhequ)

[Red Team](#_heading=h.t0wgmla3udmv)

[Purple Team](#_heading=h.o7ljvat6mh2i)

[White Team](#_heading=h.t5587gvr04b9)

[Conclusions](#_heading=h.wpral88a70jn)

[The Geek’s Corner](#_heading=h.floxyjcfjlz3)

[Conclusions](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[References](#_heading=h.ioedg3ublhq7)

# 

# **Introduction**

## **It could have happened to you…**

In 2017, Equifax, one of the largest consumer credit reporting agencies in the United States, suffered a massive data breach that exposed the personal information of over 143 million people (United States Securities and Exchange Commission, 2018). This incident not only cost the company millions of dollars but also severely damaged its reputation. The breach was caused by a vulnerability in Equifax's web application, which was exploited by cybercriminals using a technique called *SQL injection*.

Imagine if you have a breach in your own youth organisation site and have your website down, without the opportunity to network… that would be quite of a damage!

This attack highlights the importance of understanding and mitigating vulnerabilities, attacks, techniques, and threats in today's digital world. In this module, we will explore these concepts and learn how to defend against them.

## **What you will learn**

This module covers a range of topics related to cybersecurity, including common types of attacks and vulnerabilities, tools and techniques used by attackers, and methods for preventing and mitigating security incidents. Specific topics within this domain include: types of malware, social engineering attacks, network attacks, wireless attacks, physical security threats, vulnerability assessment tools and techniques, and penetration testing. This module is designed to ensure that you and your organisation have a solid foundation in understanding the nature of cyber threats and how they can be identified and defended against.

## **Why it is important**

This module is essential for you and your youth organisation as it provides a foundation for understanding the nature of cyber threats and how to mitigate them. Cybersecurity threats are constantly evolving and can cause significant damage to businesses and individuals alike. By acquiring expertise in the content of *Vulnerabilities, Attacks, Techniques, and Threats*, you can identify the various types of attacks and vulnerabilities, and develop strategies to prevent cyber incidents. The domain covers a broad range of topics, including malware, social engineering, network attacks, physical security, and vulnerability assessment, making it a critical component of any comprehensive cybersecurity training program.

## **How it can help you in everyday life**

Learning the material covered in this module is not only important for cybersecurity professionals, but also for individuals in their everyday lives. The prevalence of technology and the internet in today's society has made almost everyone susceptible to cyber threats. By understanding the nature of cyber threats and the techniques used by attackers, individuals can take steps to better protect their personal information and digital assets. For example, knowledge of common types of social engineering attacks, such as phishing and pretexting, can help individuals recognize and avoid suspicious emails or phone calls that may be attempting to steal their personal information. Similarly, understanding how to assess the security of a wireless network can help individuals ensure that their home networks are properly secured and not vulnerable to attacks. In addition, understanding the importance of physical security measures, such as locking devices or not leaving sensitive information in plain sight, can help individuals protect against physical theft of devices or data. Overall, the knowledge and skills gained from studying the following material can be applied to everyday life to help individuals protect themselves and their personal information in an increasingly connected world.

## **What career you can pursue**

After completing this module, you will have gained a foundational understanding of the fundamentals of cybersecurity. This knowledge will provide you with a starting point to explore various careers in the cybersecurity industry. Some potential entry-level career paths include:

* Cyber Security Specialists
* IT Auditor
* Penetration and Vulnerability Tester

## **Pre-requisites**

It is important to note that although the material of the module is designed to introduce beginners to the fundamental concepts of cybersecurity, it assumes that you have already completed *Module 1: Core Cybersecurity Principles*. This foundational module covers the basic principles of cybersecurity, providing a necessary theoretical background to build upon in subsequent modules.

# 

# **Material**

## **2.1 Social Engineering Techniques**

In today's technology-driven world, cyber threats are becoming increasingly sophisticated, and social engineering is one of the most commonly used tactics. Social engineering is a type of cyber attack that leverages human interaction and psychological manipulation to deceive individuals or organisations into divulging sensitive information or taking actions that benefit the attacker. By understanding these tactics, you can better protect yourself and your organisations against social engineering attacks.

### **Phishing**

Phishing is a type of social engineering attack that typically comes in the form of an email, text message, or phone call that appears to be from a legitimate organisation. The goal of phishing is to trick the victim into divulging personal or sensitive information, such as passwords or credit card numbers.

Phishing attacks often begin with **reconnaissance**, where an attacker gathers information about their target (such as their email address, social media profiles, or other online activity) in order to craft a more believable **pretext**.

The key to a successful phishing attack is to create a believable pretext that will convince the target to reveal their sensitive information. This might involve using information that the attacker has gathered during reconnaissance or creating a sense of **urgency** or **fear** in the target.

Types of Phishing:

* **Email Phishing**: The most common type of phishing attack that involves sending an email with a malicious link or attachment that can compromise the victim's device.
* **Spear Phishing**: A more targeted form of phishing attack that is tailored to a specific individual or group, often using information from social media profiles or other sources.
* **Smishing:** A type of phishing that involves sending fraudulent text messages to the victim's mobile device.
* **Vishing** - A type of phishing that involves a voice call that appears to be from a legitimate organisation, often using spoofed phone numbers.

Phishing Tactics and Techniques:

* **Link Spoofing**: This tactic involves using a disguised link that appears to lead to a legitimate website but actually redirects the victim to a malicious site.
* **Pretexting**: This tactic involves creating a believable pretext, such as a fake emergency or account issue, to convince the victim to divulge sensitive information.
* **Typosquatting**: This tactic involves using a domain name that is similar to a legitimate website to trick the victim into entering their login credentials or other sensitive information (e.g. “www.gogel.com” instead of “www.google.com”).
* **Pharming**: This technique involves redirecting the victim to a fake website even if they enter the correct URL for a legitimate site.

*Note:* ***Spoofing*** *is a technique used by attackers to falsify data or identities, in order to deceive or trick a user or a system.*

How to Prevent Falling Victim to a Phishing Attack:

* Be cautious when opening emails or text messages from unknown senders or suspicious-looking messages from known senders.
* Check the sender's email address, domain name, or phone number to ensure it is legitimate.
* Never click on links or download attachments from unknown or untrusted sources.
* Be wary of urgent or threatening messages and verify the information before taking any action.
* Use anti-phishing software and regularly update security software on all devices.
* Keep yourself informed about current phishing trends and tactics.

### **Impersonation**

Impersonation is a technique used in cyberattacks to deceive and manipulate victims. Attackers use various methods to impersonate legitimate entities or individuals in order to gain access to sensitive information or systems. Understanding the different types of impersonation techniques can help you to recognize and prevent these attacks.

Types of Impersonation Techniques:

* **Email Spoofing**: Attackers send emails that appear to be from a trusted source but are actually fake. This can be done by using a similar email address or by altering the display name.
* **Caller ID Spoofing**: Attackers use a fake phone number to make it appear as if they are calling from a legitimate organisation or individual.
* **Website Spoofing**: Attackers create a fake website that appears to be legitimate to trick users into entering their credentials or other sensitive information.
* **Social Media Impersonation**: Attackers create fake social media profiles that look like a legitimate entity or individual to gather information or conduct further attacks.
* **Domain Spoofing**: Attackers use a similar domain name to trick users into thinking they are on a legitimate website.

Motives behind Impersonation Attacks:

* **Stealing Personal Information**: Attackers can use impersonation techniques to steal personal information such as passwords, credit card numbers, or social security numbers.
* **Financial Gain**: Attackers can use stolen information to commit financial fraud or identity theft.
* **Access to Sensitive Information**: Attackers can use impersonation techniques to gain access to sensitive information such as trade secrets or company data.

Protecting Against Impersonation Attacks:

* **Be Suspicious of Unsolicited Email**s: If an email seems suspicious, double-check the sender's email address and avoid clicking on links or downloading attachments.
* **Verify the Identity of Callers**: If you receive a call from a number that seems suspicious, verify the identity of the caller before providing any sensitive information.
* **Use Two-Factor Authentication**: Use two-factor authentication whenever possible to prevent unauthorised access to sensitive information.
* **Use Strong Passwords**: Use strong, unique passwords for all accounts and consider using a password manager to help keep track of them.
* **Educate Yourself**: Stay informed about the latest phishing and impersonation techniques and regularly review your security protocols.

### **Dumpster Diving**

Dumpster Diving is a social engineering technique that involves searching through trash or discarded materials for information that can be used for malicious purposes. This technique is used to gain access to sensitive information, such as personal or financial information, confidential business information, or even passwords. Dumpster Diving is a low-tech and low-cost method, but can be very effective in obtaining information that can be used to compromise an organisation or individual.

Preventing Dumpster Diving Attacks:

* Implementing a **shred-all** policy for sensitive documents before disposing of them
* Ensuring that employees are trained on the proper handling and disposal of sensitive information
* Limiting the amount of personal or sensitive information that is printed or written down
* Locking dumpsters and trash cans to prevent unauthorised access
* Monitoring and auditing trash disposal practices

Best Practices for Disposal of Sensitive Materials:

* Shredding all documents containing sensitive information before disposing of them
* Using secure shredding services for particularly sensitive materials
* Storing sensitive materials in a locked area until they can be disposed of properly
* Maintaining a record of all disposed materials, including when and how they were disposed of

### **Shoulder Surfing**

Shoulder surfing is a social engineering technique that involves observing or spying on someone while they enter sensitive information such as passwords, credit card numbers, or other confidential information. This technique is often used in public places such as airports, coffee shops, or train stations, where people tend to be less aware of their surroundings.

Potential Risks of Shoulder Surfing:

* **Identity theft**: Attackers can use the stolen information to create fake identities, access bank accounts, or make fraudulent purchases.
* **Financial loss**: Stolen credit card numbers can be used to make unauthorised purchases, leading to financial losses.
* **Unauthorised access**: Attackers can use stolen passwords to access email accounts, social media profiles, and other sensitive information.

Signs of a Shoulder Surfing Attack:

* Someone standing too close while you enter sensitive information.
* People who seem to be more interested in you than their own business.
* Individuals who appear to be taking pictures or recording videos of you while you enter information.
* People who keep glancing in your direction.

Preventing Shoulder Surfing Attacks:

* Be aware of your surroundings and the people around you.
* Use privacy filters on your mobile devices and laptops to reduce the viewing angle of your screen.
* Use your body to shield the keypad or screen as you enter passwords or sensitive information.
* Cover the keypad with your hand while entering a PIN.
* Change your passwords frequently and avoid using the same password for multiple accounts.

### **Hoaxes**

Hoaxes are a type of social engineering attack in which an attacker uses deception to trick people into believing false information. This can be accomplished through a variety of mediums, including email, social media, and other forms of online communication. Hoaxes can be used for a variety of purposes, including spreading malware, stealing personal information, and spreading false rumours.

How do hoaxes work?

* Hoaxes work by taking advantage of people's emotions and beliefs.
* They often use sensational or alarming headlines to get people's attention.
* Hoaxes may ask people to click on a link or download an attachment, which can lead to malware infections or phishing attacks.
* They may also ask people to share the information with others, which can help the hoax to spread further.

Types of hoaxes:

* **Virus hoaxes**:False warnings about non-existent computer viruses.
* **Email chain letters**: Emails that ask you to forward the message to others.
* **Disaster hoaxes**: False warnings about natural disasters or terrorist attacks.
* **Health hoaxes**: False claims about medical treatments or diseases.
* **Financial hoaxes**: False investment opportunities or lottery scams.

How to avoid falling for hoaxes:

* **Check the source**: Be wary of information that comes from unknown or unreliable sources.
* **Verify the information**: Use search engines or fact-checking websites to confirm the validity of the information.
* **Think before you click**: Don't click on links or download attachments if you're not sure where they came from.
* **Don't share information blindly**: Verify the information before you share it with others.
* **Keep your software up to date**: Use antivirus software and keep your operating system and applications up to date.

### **Watering Hole Attacks**

A watering hole attack is a type of cyber attack in which cybercriminals compromise a website that their intended victims frequently visit. They infect the site with malware, which allows them to gain access to the victim's system once they visit the infected site. The attack is called a "watering hole" attack because it is similar to a predator waiting at a watering hole for its prey.

A watering hole attack usually involves a few steps:

* Reconnaissance: The attackers identify the target audience and their habits.
* Identify the "Watering Hole": The attackers identify the website that their intended victims frequently visit.
* Compromise the Site: The attackers infect the site with malware that can exploit vulnerabilities on the victim's system.
* Wait: The attackers wait for the victims to visit the infected website.
* Infect: The attackers deliver the malware to the victim's system through the infected website.

There are two main types of watering hole attacks:

* **Strategic**: The attackers target specific groups, such as a company, a government agency, or an industry.
* **Opportunistic**: The attackers target anyone who visits a popular website.

How to Protect Against Watering Hole Attacks:

* **Keep your software up-to-date**: Ensure that your system and software are always updated with the latest patches.
* **Use a reputable antivirus software**: A good antivirus software can protect your system from known and unknown malware.
* **Use a web filtering software**: Web filtering software can prevent access to known malicious websites.
* **Train your employees**: Educate your employees on the risks of watering hole attacks and how to recognize and avoid them.
* **Monitor your network traffic**: Network traffic monitoring can help detect watering hole attacks.

### **Other Social Engineering Attacks**

In addition to the type of attacks mentioned above, there are several other types of social engineering attacks that individuals and organisations need to be aware of. **Tailgating** and **invoice scams** are examples of other types of social engineering attacks.

#### **Tailgating**

Tailgating, also known as piggybacking, is a social engineering attack that involves following an authorised person into a restricted area. This type of attack is common in workplaces where employees are required to use access cards or ID badges to enter restricted areas. A social engineer may approach an employee and ask them to hold the door open for them, allowing them to gain access to the restricted area. To mitigate this type of attack, employees should be trained to question individuals who are not authorised to enter restricted areas and report any suspicious activity to security personnel.

#### **Invoice Scams**

Invoice scams involve the creation of a fake invoice or bill that appears to be from a legitimate vendor or supplier. Social engineers may use various tactics to convince individuals to pay the invoice, such as offering a discount or threatening legal action. To mitigate this type of attack, organisations should implement a verification process for all invoices and bills received, including confirming the authenticity of the vendor or supplier.

### **Conclusions**

As we come to the end of this learning journey on social engineering techniques, it's clear that attackers use a wide range of tactics to manipulate people into revealing sensitive information, bypassing security controls, or carrying out unauthorised actions. Social engineering attacks can take many forms, including phishing, dumpster diving, shoulder surfing, hoaxes, watering hole attacks, and more. By understanding these tactics and the warning signs, you can better protect yourself and your organisation against these types of threats.

Attackers often rely on misdirection, trust, and a believable pretext to gain access to sensitive information. They may use a variety of channels, from email and phone to physical access to a building or facility. In addition, attackers may rely on social media and other publicly available information to conduct reconnaissance and craft more convincing attacks.

It's important to note that social engineering attacks are not limited to the workplace. They can occur in our personal lives as well, with attackers using similar tactics to gain access to personal information, financial accounts, and other sensitive data. By being aware of the risks and taking steps to protect ourselves and our information, we can all be better prepared to defend against social engineering attacks.

## **2.2 Malware, Password Attacks, Physical Attacks, and Cryptographic Attacks**

This unit refers to a set of techniques and methods that attackers use to breach the security of a system or network. This includes different types of attacks such as malware attacks, password attacks, physical attacks, and cryptographic attacks. These attacks can target various components of a system, such as software, hardware, or human vulnerabilities, and can result in different types of damage, including data loss, financial loss, or system disruption. It is essential to understand these types of attacks to develop effective security strategies and protect against potential threats.

### **Malware**

**Malware**, short for **mal**icious soft**ware**, refers to any program or code designed to harm or exploit computer systems, networks, or devices. It can come in many forms, such as viruses, worms, trojan horses, ransomware, adware, spyware, and more. Malware can cause significant harm to organisations and individuals, including data breaches, financial losses, and reputational damage.

Types of Malware:

* **Viruses**: Viruses are a type of malware that infects a computer by attaching itself to a legitimate program or file. Once the file is opened, the virus can execute its malicious code, replicate itself, and spread to other files on the computer.
* **Crypto-malware**: Crypto-malware is a type of malware that encrypts files on the victim's computer and demands payment in exchange for the decryption key. Crypto-malware is often spread through email attachments or malicious downloads.
* **Ransomware**: Ransomware is a type of malware that prevents users from accessing their files or system until a ransom is paid. Ransomware can be spread through email attachments, malicious downloads, or vulnerabilities in software.
* **Worms**: Worms are self-replicating malware that can spread through a network without any user interaction. Worms often exploit vulnerabilities in software or weak passwords to gain access to the system.
* **Trojan Horse**: A Trojan Horse is a type of malware that disguises itself as legitimate software or files, tricking users into downloading or installing it. Once installed, the Trojan Horse can perform a variety of malicious activities, such as stealing data, deleting files, or creating backdoors for hackers to gain access to the system.
* **Rootkit**: A rootkit is a type of malware that hides its presence on a computer by modifying the operating system or kernel. Rootkits can be used to create backdoors, steal data, or control the system remotely.
* **Keylogger**: A keylogger is a type of malware that records keystrokes on a computer, allowing hackers to steal passwords, credit card numbers, or other sensitive information.
* **Adware/Spyware**: Adware and spyware are types of malware that display unwanted ads or collect data on the user's browsing habits. Adware and spyware can be spread through malicious downloads, social engineering tactics, or vulnerabilities in software.
* **Botnet**: A botnet is a network of infected computers that can be controlled remotely by a malicious actor. Botnets are often used to launch **DDoS** attacks, steal data, or send spam emails.

*Note:* ***DDoS*** *stands for Distributed Denial of Service, which is a type of cyber attack that aims to overwhelm a targeted website or online service with a flood of traffic from multiple sources, making it unavailable to users. In a DDoS attack, the attacker uses a network of infected computers, also known as a botnet, to send a huge amount of traffic to the targeted site, causing it to crash or become unresponsive.*

How Malware Can Infect Your System:

* **Phishing**: Malware can be delivered through phishing emails that appear to be legitimate and trick the user into clicking on a malicious link or downloading an infected attachment.
* **Drive-by Download**: This is a type of malware attack where the malware is downloaded and installed without the user's knowledge or consent when they visit a malicious website.
* **Software vulnerabilities**: Malware can exploit software vulnerabilities to gain access to the system.
* **Infected software**: Malware can be bundled with legitimate software and unknowingly installed on the system.
* **Social engineering**: Malware can be delivered through social engineering techniques, such as enticing users to click on links or download attachments.

Prevention and Protection Against Malware:

* **Keep software up-to-date**: Regularly update your software to patch any vulnerabilities and ensure that your system is secure.
* **Use antivirus software**: Antivirus software can detect and remove malware from your system.
* **Use strong passwords**: Strong passwords make it more difficult for attackers to gain access to your system.
* **Be cautious with email**: Do not open attachments or click on links from unknown or suspicious sources.
* **Be careful when downloading software**: Download software from trusted sources and verify that the software is legitimate.
* **Backup your data**: Back up your data regularly to protect it in case of a malware attack.

### **Password Attacks**

Passwords are a common method of authentication and access control for digital systems. Password attacks are attempts to gain unauthorised access to these systems by exploiting weaknesses in the password itself, or in the methods used to manage and protect passwords. Password attacks can take many forms, from simple guessing to sophisticated cracking techniques, and can have serious consequences for individuals and organisations alike.

Types of Password Attacks:

* **Brute Force Attack**: An attacker attempts to guess a password by trying different combinations of characters until the correct password is found.
* **Dictionary Attack**: An attacker uses a pre-built list of common passwords or words to try and gain access to a system.
* **Rainbow Table Attack**: An attacker uses pre-computed **hash** values to crack passwords quickly.
* **Credential Stuffing Attack**: An attacker uses stolen credentials (e.g., username and password) from one website to try and gain access to another website where the same credentials are used.

*Note: A* ***hash*** *is a fixed-length string of characters generated from a plaintext input using a mathematical algorithm. In the context of a rainbow table attack, a hash function is used to generate a hashed representation of the passwords stored in a database. The attacker can then use a precomputed table of possible plaintext values and their corresponding hashes, known as a rainbow table, to quickly crack the hashed passwords without having to perform the computationally expensive task of brute-forcing each password individually.*

Methods of Password Attacks:

* **Phishing**: Attackers can trick users into giving away their passwords through phishing emails or websites that appear legitimate.
* **Social Engineering**: Attackers can use social engineering tactics to obtain passwords, such as tricking users into revealing their password or using passwords written on sticky notes or stored in unsecured locations.
* **Keystroke Logging**: Attackers can use software or hardware to capture keystrokes and record passwords as users enter them.
* **Man-in-the-Middle (MITM) Attack**: An attacker intercepts communication between a user and a system and captures passwords as they are transmitted.

Prevention of Password Attacks:

* **Use strong passwords**: Strong passwords are harder to guess and make it more difficult for attackers to crack.
* **Use Multi-Factor Authentication**: Multi-factor authentication provides an extra layer of security beyond a password.
* **Stay vigilant**: Be cautious of phishing attempts and always verify the authenticity of websites before entering passwords.
* **Use password managers**: Password managers can generate and store strong passwords for different accounts.
* **Regularly change passwords**: Regularly changing passwords can help prevent attackers from gaining access.

*Note:* ***Multi-factor authentication*** *(****MFA****) is a security mechanism that requires users to provide two or more forms of authentication before granting access to an application, system, or device.*

### **Physical Attacks**

Physical attacks are a type of attack that rely on gaining physical access to a device or network in order to compromise its security. Attackers use a variety of techniques to gain access, ranging from social engineering to brute force. We will cover several common types of physical attacks, including malicious Universal Serial Bus (USB) cables, Malicious Flash Drives, Skimming and Card Cloning.

#### **Malicious Universal Serial Bus (USB) cable**

Attackers can create malicious USB cables that look like normal cables but have additional components that allow them to access the computer when the cable is plugged in. These cables can be used to install malware or gain remote access to a system.

Prevention:

* Use only trusted USB cables and avoid using untrusted cables from unknown sources.

#### **Malicious Flash Drive**

Malicious flash drives are similar to USB cables in that they can be used to install malware or gain remote access to a system. Attackers may leave these flash drives in public places, such as a parking lot, to trick someone into plugging them into their computer.

Prevention:

* Use only trusted flash drives and avoid using untrusted flash drives from unknown sources.

#### **Skimming and Card Cloning**

Skimming is a type of physical attack that involves the theft of credit card or debit card information through the use of an unauthorised device. The device is placed on top of or in place of the legitimate card reader, often at points of sale such as ATMs or gas pumps. When a victim inserts their card, the device reads and stores the card's magnetic stripe data. This data can then be used to create counterfeit cards or conduct fraudulent transactions.

Prevention:

* Be aware of your surroundings when using an ATM or other card reader and regularly monitor your account for suspicious activity.

### **Cryptographic Attacks**

Cryptography is the practice of protecting information by converting it into a form that can only be read by those who have the key to decipher it. Cryptographic attacks refer to attempts made by unauthorised parties to break encryption algorithms and gain access to sensitive information. We will cover the different types of cryptographic attacks, including Birthday Attacks, Collisions, and Downgrade Attacks.

#### **Birthday Attacks**

A birthday attack is a type of cryptographic attack that exploits the probability of two messages producing the same hash value. A hash function is a mathematical function that takes a variable-length input and converts it into a fixed-length output. The hash function ensures that the output value is unique for every input value, but as the number of inputs increases, the probability of two or more inputs producing the same output value increases. Attackers can use this vulnerability to create two or more messages with the same hash value, allowing them to manipulate the data or bypass security measures.

*Fun fact: In a room of just 23 people there’s a 50-50 chance of at least two people having the same birthday. In a room of 75 there’s a 99.9% chance of at least two people matching.*

#### **Collisions**

A collision is a cryptographic attack that occurs when two different inputs produce the same hash value. Cryptographic hash functions are designed to minimise the likelihood of collisions, but it is impossible to completely eliminate the possibility. Attackers can exploit collisions to create a fake certificate, access an unauthorised system, or execute a code remotely.

#### **Downgrade Attacks**

A downgrade attack is a type of cryptographic attack that exploits the weaknesses in a secure communication protocol. The attacker forces the system to use an older version of the protocol that has known vulnerabilities, allowing them to access sensitive information. Attackers can use downgrade attacks to intercept encrypted data, modify the data, or launch further attacks.

Prevention Measures:

* **Use Strong Cryptographic Algorithms**: One of the most important ways to prevent cryptographic attacks is to use strong encryption algorithms, such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC). These algorithms use longer key sizes and are more resistant to attacks.
* **Regularly Update Cryptographic Protocols**: Regularly updating cryptographic protocols can prevent downgrade attacks by ensuring that only the most secure versions of protocols are used.
* **Use Hash Salting**: Hash salting involves adding random data to the input of a hash function. This makes it difficult for attackers to create messages with the same hash value, thereby preventing birthday attacks and collisions.
* **Implement Digital Certificates**: Digital certificates provide a way to verify the identity of a user or system. They are issued by a trusted third party and contain information about the user or system, including public keys. Implementing digital certificates can prevent attackers from impersonating a legitimate user or system.

### **Conclusions**

As we conclude this learning journey on different types of attacks, it's evident that attackers use various methods to gain unauthorised access to information or systems. From malware and password attacks to physical attacks and cryptographic attacks, attackers exploit weaknesses in the security infrastructure of an organisation or individual.

Prevention measures such as regular software updates, strong passwords, multi-factor authentication, and security awareness training can mitigate the risks of these attacks. It's crucial to understand that these attacks are not limited to the workplace and can occur in our personal lives too.

By being aware of these types of attacks and taking steps to protect ourselves and our information, we can be better prepared to defend against them. It's essential to remain vigilant and adopt a proactive approach to security to keep our systems, data, and ourselves safe from the dangers of these types of attacks.

## **2.3 Application Attacks**

Welcome to the world of Application Attacks. As we rely more on technology in our daily lives, applications have become an essential part of our personal and professional activities. However, with the increased usage of applications, there has been a rise in the number of attacks aimed at exploiting vulnerabilities in these applications. Application attacks can take many forms, including injection attacks, buffer overflow attacks, and cross-site scripting attacks. These attacks can result in data theft, financial losses, and even complete system compromise. By understanding the types and methods of application attacks, you can better protect yourself and your organisation against these types of threats.

### **Cross-site Scripting**

In the world of cybersecurity, cross-site scripting (XSS) is a type of attack that targets web applications. In this attack, the attacker injects malicious code into a web page viewed by other users, thereby compromising the integrity and security of the page.

There are three types of XSS:

* **Stored XSS** occurs when the attacker injects the malicious code into a server, which then serves it to all users who access that page.
* **Reflected XSS**, on the other hand, occurs when the attacker injects the malicious code into a link, email, or input field, which then gets reflected back to the user.
* **DOM-based XSS** occurs when the attacker injects the malicious code into the Document Object Model (DOM) of the page.

*Note: The* ***D****ocument* ***O****bject* ***M****odel (****DOM****) is a programming interface for web documents.*

*It represents the page so that programs can change the document structure, style, and content. The DOM represents the document as nodes and objects.*

Prevention Techniques:

* To prevent XSS attacks, it is essential to use secure coding practices, such as input validation, output encoding, and proper handling of user input. Additionally, implementing a [Content Security Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) (CSP) can help mitigate the risk of XSS attacks. CSP is a security feature that specifies the sources of content that a browser should consider as legitimate for a specific web page.

Impact of XSS:

* XSS attacks can have a significant impact on web applications and their users. An attacker can use XSS to steal sensitive user information, such as login credentials, credit card details, and other personal data. In some cases, the attacker can also use XSS to take control of the user's session, allowing them to carry out unauthorised actions on the web application.

### **Injection Attacks**

Injection attacks are one of the most common types of application attacks, where an attacker inserts malicious code into an application to exploit its vulnerabilities. These attacks can result in data loss, theft of sensitive information, and system damage.

Types of Injection Attacks:

* **SQL Injection**: This type of attack involves injecting SQL commands into an application's input field. Attackers can use these commands to manipulate the database and access sensitive information.
* **Command Injection**: In this attack, an attacker injects malicious commands into an application's input field. These commands can be executed on the targeted system, allowing attackers to gain access to sensitive data or even take control of the system.
* **LDAP Injection**: Attackers use [LDAP](https://ldap.com/) (Lightweight Directory Access Protocol) injection to inject malicious code into an application's input fields. They can then access sensitive information from the LDAP directory.
* **XPath Injection**: Attackers use this type of injection to exploit an application's XPath query language. By injecting malicious code, attackers can retrieve sensitive information from the application's XML data.

*Note:*

* ***SQL*** *(****S****tructured* ***Q****uery* ***L****anguage) is a programming language used for managing relational databases. It is used to manipulate and retrieve data stored in a database management system. SQL is widely used in web development and other areas that require database management.*
* ***XML*** *(****Ex****tensible* ***M****arkup* ***L****anguage) is a markup language used for encoding documents in a format that is both human-readable and machine-readable. It uses tags to define data elements and attributes to provide additional information about those elements. XML is commonly used for data exchange between different applications and systems.*
* ***XPath*** *is a query language used to navigate and select elements in an XML document. It uses path expressions to select nodes or sets of nodes in the XML tree structure.*

Prevention Measures:

* **Input Validation**: Ensure that all user input is validated and sanitised to prevent malicious code from being executed.
* **Use Prepared Statements**: Prepared statements use parameterized queries that separate the SQL logic from the input data. This helps to prevent SQL injection attacks.
* **Use Least Privilege**: Limit application and database access to only what is necessary for the system to function. This helps to limit the damage in case of a successful injection attack.
* **Use Content Security Policy** (CSP): CSP is a security standard that helps prevent injection attacks by specifying which sources of content are trusted on a website.

### **Buffer Overflows**

Buffer overflows are a common type of software vulnerability that can be exploited by attackers to execute malicious code or crash a system. In a buffer overflow attack, the attacker sends more data than the buffer can handle, causing the excess data to overwrite adjacent memory locations. By carefully crafting the data, the attacker can cause the program to execute code of their choice.

Types of Buffer Overflows:

* **Stack-based Buffer Overflow**: This is the most common type of buffer overflow. In a stack-based buffer overflow, the attacker overflows a buffer on the stack, which allows them to overwrite the return address of a function. By doing so, they can redirect the flow of execution to their own malicious code, which is usually stored in another part of memory.
* **Heap-based Buffer Overflow**: This type of buffer overflow targets dynamically allocated memory on the heap. Unlike stack-based buffer overflows, heap-based buffer overflows are more complex and harder to exploit. In a heap-based buffer overflow, the attacker overflows a buffer in the heap, which can allow them to modify memory that they shouldn't have access to.

*Note: In computer memory, the* ***stack*** *and* ***heap*** *are two different regions used for storing data. The stack is a contiguous block of memory used for storing temporary variables, function parameters, and return addresses. It is a last-in, first-out (LIFO) data structure. The heap, on the other hand, is a region of memory used for dynamically allocating memory during program execution.*

Methods of Attack:

* Attackers can use various methods to exploit buffer overflows, including sending oversized input to a program, modifying function pointers, and injecting code into the program's memory. By taking advantage of these vulnerabilities, attackers can gain control of a system or execute arbitrary code.

Prevention Measures:

* To prevent buffer overflow attacks, developers can use techniques such as input validation, bounds checking, and implementing secure coding practices. Additionally, using memory-safe languages such as Java or Python can help mitigate the risk of buffer overflows.

### **Replay Attacks**

Replay attacks are a type of network attack that occurs when an attacker intercepts and maliciously retransmits data that has already been transmitted. These types of attacks are also known as playback attacks or echo attacks. Replay attacks can occur in a variety of contexts, including authentication protocols, network communication, and even financial transactions.

Types of Replay Attacks:

* **Simple Replay Attacks**: In this type of attack, the attacker captures a packet of data and retransmits it to the target system, attempting to impersonate the original sender.
* **Man-in-the-Middle (MitM) Replay Attacks**: In this type of attack, the attacker intercepts data as it is transmitted between two systems and retransmits it to one or both parties, allowing them to manipulate or intercept the data in real-time.
* **Self Replay Attack**: In a self replay attack, an attacker sends a legitimate request to a server and captures the response. The attacker then replays the same request to the server multiple times, causing the server to perform the same action multiple times.

Prevention Measures:

* **Encryption**: One way to prevent replay attacks is to use encryption to protect the data being transmitted. Encryption can help to ensure that the data cannot be intercepted or manipulated by an attacker.
* **Timestamps**: Timestamps can be used to prevent replay attacks by including a timestamp with the original data packet. The receiving system can then verify that the timestamp is valid and reject any data packets that are outside of the expected timeframe.
* **Nonces**: Nonces are random values that are used to prevent replay attacks by ensuring that each data packet is unique. The receiving system can check the nonce value to ensure that the data packet is not a replay.

### **Request Forgeries**

In this learning unit, we will discuss request forgery attacks. We will start by looking at the client-server architecture and then move on to discussing Cross-Site Request Forgery (CSRF) and Server-Side Request Forgery (SSRF) attacks.

#### **Client-Server Architecture**

The client-server architecture is a widely used model for network communication. In this model, the client sends requests to the server, and the server sends responses back to the client. The client can be a web browser or any other application that sends requests to the server, and the server can be any machine that responds to those requests.

#### **Cross-Site Request Forgery (CSRF)**

Cross-Site Request Forgery (CSRF) is a type of attack that allows an attacker to force a user to perform actions on a website without the user's knowledge or consent. The attacker sends a malicious request to the website, which is then executed by the user's browser when the user visits the attacker's website. This can result in the user unknowingly changing their account details, making a payment, or performing any other action that the attacker desires.

Prevention measures include:

* Including a secret token in each request that is validated by the server to ensure that the request is legitimate.
* Using the [HTTP Only flag](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies#restrict_access_to_cookies) for cookies to prevent the cookie from being accessed by JavaScript, reducing the risk of malicious requests.
* Implementing CAPTCHAs or other mechanisms to verify that the user is human and not a bot.

*Note:* ***CAPTCHA*** *stands for* ***C****ompletely* ***A****utomated* ***P****ublic* ***T****uring test to tell* ***C****omputers and* ***H****umans* ***A****part. It is a security measure to prevent automated bots from accessing a system or service. CAPTCHAs often require users to solve a challenge, such as identifying distorted characters or clicking on certain images, to prove they are human.*

#### **Server-Side Request Forgery (SSRF)**

Server-Side Request Forgery (SSRF) is a type of attack that occurs when an attacker tricks a server into making a request to a URL specified by the attacker. The attacker can use this attack to bypass security controls and gain access to sensitive information or services. For example, an attacker could use SSRF to access an internal network or to make requests to a third-party service on behalf of the server.

Prevention measures include:

* Validating user input and sanitising any data before using it to make requests.
* Whitelisting allowed domains and blocking requests to any unauthorised domains.
* Implementing rate-limiting or other mechanisms to prevent excessive requests.

*Note: A* ***domain*** *is a unique name that identifies a website on the internet. It's a part of a website's URL, such as google.com.*

### **SSL Stripping**

Secure Sockets Layer (SSL) is a protocol used to establish an encrypted link between a web server and a web browser. It helps ensure that sensitive information such as login credentials, financial information, and personal details are transmitted securely over the internet. However, SSL stripping is a type of attack that can undermine the security of SSL by allowing an attacker to intercept traffic between a user and a website and decrypt sensitive information. This learning unit will cover the basics of SSL stripping, how it works, and how to protect against it.

#### **What is SSL Stripping?**

SSL stripping is a type of man-in-the-middle attack that involves intercepting traffic between a user and a website and downgrading the secure HTTPS connection to an unsecured HTTP connection. The attacker can then read and manipulate the traffic, potentially stealing sensitive information such as login credentials and credit card details.

#### **How does SSL Stripping work?**

SSL stripping works by exploiting the fact that many users are not familiar with the differences between HTTP and HTTPS connections. The attacker intercepts the initial request from the user to the website and responds with a fake HTTPS page that appears identical to the legitimate site. However, the attacker's page is not secured with SSL, and any data entered by the user is sent in plaintext. The attacker can then intercept and manipulate this data before forwarding it on to the legitimate website.

To protect against SSL stripping attacks, you can:

* Use a web browser extension like [HTTPS Everywhere](https://www.eff.org/https-everywhere) that can force SSL/TLS connections for specific websites or all websites to prevent attackers from downgrading the connection to HTTP. Additionally, always check for "https" in the URL and the padlock icon in the browser's address bar to ensure a secure connection.

### **Other Application Attacks**

In addition to the type of attacks mentioned above, there are several other types of application attacks that individuals and organisations need to be aware of. Here is a concise list of other attacks that can exploit applications flaws:

* **Race Conditions**: A race condition occurs when two or more processes access a shared resource at the same time, potentially causing unexpected behaviour. Attackers can exploit race conditions to bypass security checks or gain access to sensitive data.
* **Directory Traversal**: Directory traversal attacks involve exploiting vulnerabilities in an application's input validation to access files outside of the intended directory. This can allow attackers to view, modify, or delete sensitive files.
* **Improper Error Handling**: Improper error handling can occur when an application provides too much information about an error, allowing attackers to exploit vulnerabilities in the code.
* **API Attacks**: APIs are often used to allow different applications to communicate with each other. However, vulnerabilities in APIs can be exploited by attackers to gain unauthorised access to data or perform other malicious actions.
* **Resource Exhaustion**: Resource exhaustion attacks involve overwhelming an application's resources, such as memory or CPU, causing it to crash or become unresponsive.

*Note:* ***API*** *stands for* ***A****pplication* ***P****rogramming* ***I****nterface. It is a set of protocols, routines, and tools for building software applications. An API specifies how software components should interact and makes it easier for developers to use certain functionalities in their own programs. APIs are commonly used in web development to enable communication between different software systems or services.*

Prevention:

* To protect against these types of application attacks, it is important to implement proper input validation and error handling, restrict access to sensitive files and resources, and ensure that APIs are secure and properly authenticated. Regular security testing and code reviews can also help to identify and address vulnerabilities before they can be exploited.

### **Conclusions**

Throughout the units created, we have covered a range of important topics related to application security. We started with Cross-Site Scripting (XSS) attacks, which can manipulate web applications to steal sensitive information or take control of user accounts. We then discussed Injection attacks, such as SQL and buffer overflow, which can exploit vulnerable code to execute malicious commands. Next, we covered various types of application attacks, including race conditions, directory traversal, and resource exhaustion. Finally, we explored SSL stripping, and other measures to protect against attacks.

Overall, these learning units provide a comprehensive overview of the key threats and vulnerabilities in application security. By understanding these concepts, individuals and organisations can better protect themselves from cyber attacks and safeguard their sensitive data. It is important to stay vigilant and up-to-date with the latest security practices to ensure the safety of our digital infrastructure.

## **2.4 Network Attacks**

In the world of cybersecurity, network attacks are a common threat that individuals and organisations face on a daily basis. These attacks are designed to exploit vulnerabilities in computer networks to gain unauthorised access to sensitive data, steal personal information, and cause damage to computer systems. It is crucial for individuals and organisations to understand the various types of network attacks and take appropriate measures to protect their systems. We will explore different types of network attacks, and discuss strategies for preventing and mitigating their impact.

### **Rogue Access Points and Evil Twin**

Wireless networks have become ubiquitous in both personal and professional settings, providing convenience and flexibility in accessing the internet and network resources. However, the very nature of wireless networks also makes them vulnerable to security threats. One of these threats is the use of rogue access points and evil twin attacks, which can compromise the security of the network and the devices connected to it.

#### **Rogue Access Points**

A rogue access point is an unauthorised wireless access point that is installed on a network without the knowledge or approval of the network administrator. Attackers may set up rogue access points to gain unauthorised access to the network, monitor network traffic, and steal sensitive information. Rogue access points can be installed by physically connecting to the network or by using wireless devices to create an ad-hoc network.

To prevent rogue access point attacks, it's important to implement security measures such as wireless intrusion prevention systems ([WIPS](https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system)), which can detect and alert administrators to the presence of rogue access points. Additionally, network administrators should implement strict policies and procedures for connecting devices to the network and regularly monitor network activity for signs of unauthorised access.

#### **Evil Twin Attacks**

An evil twin attack is a type of wireless attack where attackers create a fake wireless access point with the same name as a legitimate access point, in an attempt to trick users into connecting to it instead of the legitimate access point. Once a user connects to the evil twin access point, the attacker can intercept and monitor network traffic, steal login credentials, and inject malware onto the user's device.

To prevent evil twin attacks, it's important to educate users about the risks of connecting to unknown wireless networks and to always verify the SSID and MAC address of the legitimate access point. Additionally, implementing strong encryption and authentication protocols such as Wi-Fi Protected Access (WPA) and 802.1X can help prevent unauthorised access to the network.

*Note:*

* *SSID stands for Service Set Identifier, it's a unique name given to a wireless network to identify it, and it's used by devices to connect to a specific network. An SSID can be up to 32 characters long and can consist of letters, numbers, and symbols.*
* *A Media Access Control (MAC) address is a unique identifier assigned to a network interface controller (NIC) for use as a network address. It is used to uniquely identify devices on a network. MAC addresses are 48-bit addresses represented in hexadecimal format.*

Prevention:

* To effectively combat rogue access points and evil twin attacks, a multi-layered approach is needed. This includes implementing security measures at both the network and device levels. Network administrators should regularly monitor the network for unauthorised devices and implement strict policies for connecting to the network. Additionally, users should be educated on the risks of connecting to unknown wireless networks and how to verify the legitimacy of access points.

### **Bluejacking and Bluesnarfing**

Bluejacking and bluesnarfing are two types of Bluetooth-based attacks that can compromise the security of devices and data. In this learning unit, we will discuss these attacks, how they work, and ways to prevent them.

#### **Bluejacking**

Bluejacking is a form of spamming or unsolicited messaging that involves sending unwanted messages or advertisements to Bluetooth-enabled devices. Attackers can use this technique to exploit a vulnerability in the Bluetooth protocol, which allows devices to communicate with each other without establishing a pairing relationship. Bluejacking attacks are usually harmless, but they can be annoying and distracting.

#### **Bluesnarfing**

Bluesnarfing, on the other hand, is a more serious type of Bluetooth attack that allows an attacker to gain unauthorised access to a Bluetooth-enabled device and extract personal or sensitive information, such as contacts, text messages, and emails. This attack works by exploiting a vulnerability in the Bluetooth protocol that allows devices to connect to each other without authentication or encryption. Attackers can use specialised tools to scan for vulnerable devices and extract data remotely.

Prevention:

* To protect against bluejacking and bluesnarfing attacks, it is recommended to keep Bluetooth turned off when not in use or to set the device to "non-discoverable" mode. Users should also avoid accepting unsolicited Bluetooth connections and be cautious when opening messages from unknown senders. Additionally, users should keep their Bluetooth devices up-to-date with the latest security patches and updates to ensure they are protected against known vulnerabilities.

### **Wireless Disassociation Attacks**

Wireless Disassociation Attacks are a type of Denial-of-Service (DoS) attack that targets wireless networks. The objective of these attacks is to disrupt the communication between wireless clients and Access Points (APs) by sending spoofed disassociation or deauthentication packets.

Types of Wireless Disassociation Attacks:

* **Disassociation Attacks**: In this type of attack, an attacker sends a spoofed disassociation frame to a wireless client or AP, causing them to disconnect from the network.
* **Deauthentication Attacks**: In this type of attack, an attacker sends a spoofed deauthentication frame to a wireless client or AP, causing them to log out of the network.

*Note: A* ***spoofed disassociation frame*** *is a type of wireless attack where an attacker sends a fake message to a wireless access point, causing it to disconnect a legitimate user. This can result in a denial of service attack or allow the attacker to capture sensitive information.*

Methods of Conducting Wireless Disassociation Attacks:

* **Manual Attack**: In this method, the attacker manually sends spoofed disassociation or deauthentication packets using a wireless packet injection tool.
* **Automated Attack**: In this method, the attacker uses a software tool that automates the process of sending spoofed packets, making it easier to launch an attack on multiple targets.

*Note: One example of a wireless packet injection tool is* [*Aircrack-ng*](https://www.aircrack-ng.org/)*, which is a popular open-source tool used for network auditing and penetration testing. It can be used to perform a variety of wireless attacks, including packet injection, WEP and WPA/WPA2-PSK cracking, and deauthentication attacks.*

Preventing Wireless Disassociation Attacks:

* **Implementing WIPS**: Wireless Intrusion Prevention Systems (WIPS) can help detect and prevent wireless disassociation attacks by monitoring network traffic and detecting anomalous behaviour.
* **MAC Address Filtering**: This technique involves creating a list of trusted MAC addresses and only allowing devices with those addresses to connect to the network.
* **Signal Jamming**: This method involves using specialised equipment to jam the wireless signals, rendering the attack ineffective.

### **Wireless Jamming**

Wireless jamming is a form of denial-of-service (DoS) attack that disrupts wireless communications by transmitting a high volume of interfering signals. This type of attack can affect a wide range of wireless technologies, including Wi-Fi, Bluetooth, and cellular networks. We will explore the different types of wireless jamming attacks, how they work, and some techniques to defend against them.

There are two main types of wireless jamming attacks, constant jamming and random jamming:

* Constant jamming involves transmitting a continuous radio signal on a specific frequency to create interference and disrupt communication.
* Random jamming, on the other hand, involves transmitting random signals on multiple frequencies, making it harder to isolate and block the source of interference.

How Wireless Jamming Attacks Work

Wireless jamming attacks work by flooding the target device or network with interference signals, effectively blocking legitimate signals from being received. This disruption can cause devices to lose connectivity or reduce their performance. Jamming attacks can be carried out using various methods, including software-defined radios (SDRs), directional antennas, and power amplifiers.

*Note: Software-defined radio is a radio communication system that can be programmed and reconfigured using software instead of hardware modifications. It uses a general-purpose processor and digital signal processing to transmit and receive radio signals. This flexibility allows for greater adaptability and interoperability in wireless communication.*

Prevention:

* Defending against wireless jamming attacks requires a multi-layered approach that includes physical security measures, network segmentation, and intrusion detection systems (IDS). Physical security measures, such as locking up access points and antennas, can prevent attackers from physically tampering with the wireless infrastructure. Network segmentation involves separating the wireless network into smaller, more manageable segments to limit the impact of an attack. IDS can detect and alert administrators to the presence of unusual wireless activity, such as a sudden increase in interference or the appearance of unknown devices.

*Note: An Intrusion Detection System (IDS) is a security technology that monitors and analyses network traffic for signs of suspicious or malicious activity. IDS can alert administrators to potential security threats, such as hacking attempts, malware infections, and other unauthorised access. IDS can also provide detailed information on the nature and scope of an attack, helping security teams to respond more effectively.*

### **RFID and NFC Attacks**

Radio Frequency Identification (RFID) and Near Field Communication (NFC) are technologies that allow for wireless communication between devices. While they have many useful applications, they can also be vulnerable to attacks by malicious actors. In this learning unit, we will explore some common types of attacks on RFID and NFC systems, as well as some prevention measures that can be taken.

#### **RFID and NFC Technology**

RFID is a wireless technology that uses radio waves to read and transmit data stored on tags attached to objects. NFC is a subset of RFID technology that allows for communication between two devices in close proximity. These technologies have become increasingly popular in various industries due to their convenience and efficiency.

Types of RFID and NFC Attacks:

* **Eavesdropping**: An attacker intercepts and listens to the communication between devices in order to obtain sensitive information.
* **Replay attacks**: An attacker captures and replays a legitimate signal in order to gain unauthorised access.
* **Denial of Service (DoS) attacks**: An attacker sends a high volume of requests to overwhelm the system and prevent legitimate communication.
* **Man-in-the-Middle (MitM) attacks**: An attacker intercepts and alters the communication between devices to steal data or inject malicious code.

Prevention:

* **Encryption**: Data transmitted between devices should be encrypted to prevent eavesdropping and data theft.
* **Authentication**: Devices should be authenticated to prevent unauthorised access and replay attacks.
* **Access Control**: Systems should be designed with access control mechanisms to prevent DoS attacks and MitM attacks.
* **Physical Security**: RFID and NFC tags and devices should be physically secured to prevent tampering or theft.

### **MAC Flooding and Cloning**

MAC (Media Access Control) flooding and cloning are two types of network attacks that target the MAC address of a device. MAC flooding is a type of denial-of-service (DoS) attack that floods the switch with a large number of fake MAC addresses, which causes the switch to fail and disrupts the network. MAC cloning, on the other hand, involves duplicating a legitimate MAC address to gain unauthorised access to the network.

#### **MAC Flooding**

MAC flooding is a type of attack that targets the switch's MAC address table. The switch uses this table to store the MAC addresses of connected devices and their corresponding switch ports. When a device sends data to the switch, the switch uses the MAC address table to determine the device's location and sends the data to the correct port. In a MAC flooding attack, the attacker sends a large number of fake MAC addresses to the switch, causing the table to become full. Once the table is full, the switch starts broadcasting data to all ports, resulting in a DoS attack.

Prevention:

* To prevent MAC flooding, network administrators can implement port security measures, such as limiting the number of MAC addresses per port and configuring the switch to disable the port if it detects MAC flooding.

#### **MAC Cloning**

MAC cloning is a type of attack where the attacker copies the MAC address of a legitimate device to gain unauthorised access to the network. Once the attacker gains access to the network, they can launch other attacks, such as stealing sensitive data or launching further attacks on the network.

Prevention:

* To prevent MAC cloning, network administrators can implement authentication measures, such as the use of IEEE 802.1X, which requires devices to authenticate with a network before they can access it. Network administrators can also monitor the network for unusual MAC addresses and take action if they detect any suspicious activity.

### **DNS Attacks**

Domain Name System (DNS) is a critical component of the internet that translates domain names into IP addresses. DNS attacks target the DNS infrastructure to redirect users to malicious websites or steal sensitive information. This learning unit covers several types of DNS attacks, including DNS Poisoning, Domain Hijacking, URL Hijacking, and Domain Reputation.

#### **DNS Poisoning**

DNS Poisoning, also known as DNS Spoofing or DNS Cache Poisoning, is an attack in which an attacker exploits vulnerabilities in the DNS infrastructure to redirect DNS requests to a malicious website. The attacker can then steal sensitive information, such as login credentials or financial data, from the unsuspecting user. DNS Poisoning is often accomplished by injecting false DNS records into a DNS resolver's cache or by compromising a DNS server.

Prevention:

* Use DNSSEC (DNS Security Extensions) to digitally sign DNS records and protect against DNS spoofing attacks.
* Configure firewalls to block DNS traffic from untrusted sources.
* Regularly update and patch DNS servers to protect against known vulnerabilities.

*Note:* ***DNSSEC*** *(DNS Security Extensions) is a set of protocols that provides authentication and data integrity to the Domain Name System (DNS). It adds a layer of security to prevent DNS attacks such as DNS cache poisoning and DNS spoofing. DNSSEC works by digitally signing DNS records to ensure their authenticity and preventing unauthorised changes to them.*

#### **Domain Hijacking**

Domain Hijacking is an attack in which an attacker gains control of a domain name by compromising the account credentials of the domain owner or by exploiting vulnerabilities in the domain registrar's system. The attacker can then redirect traffic to a malicious website or use the domain name to send spam or phishing emails.

*Note: A* ***domain registrar*** *is a company or organisation that manages the reservation of internet domain names and their registration with the Internet Corporation for Assigned Names and Numbers (ICANN) or a country code top-level domain (ccTLD) authority.*

Prevention:

* Use strong and unique passwords for domain registrar accounts.
* Enable two-factor authentication (2FA) to prevent unauthorised access to domain registrar accounts.
* Regularly monitor domain registration records for unauthorised changes.

#### **URL Hijacking**

URL Hijacking is an attack in which an attacker modifies the URL of a legitimate website to redirect users to a malicious website. The attacker can use social engineering tactics, such as phishing emails or fake advertisements, to trick users into clicking on the modified URL.

Prevention:

* Use browser extensions that verify the authenticity of URLs and alert users to suspicious or modified URLs.
* Educate users about the risks of clicking on links in unsolicited emails or advertisements.
* Regularly scan websites for signs of URL hijacking or other malicious activities.

#### **Domain Reputation**

Domain Reputation is a measure of the trustworthiness of a domain name based on its past behaviour. Attackers can exploit domain reputation by registering new domain names or hijacking legitimate domains with a good reputation to carry out malicious activities, such as phishing or distributing malware.

Prevention:

* Use reputation-based security services to block access to known malicious domains.
* Monitor domain reputation using threat intelligence tools to identify and block suspicious domains.
* Educate users about the risks of visiting unfamiliar or suspicious websites.

### **Conclusions**

As we conclude this learning journey on wireless and network attacks, we have covered a range of threats that can compromise the security of our devices, data, and network infrastructure. From rogue access points and evil twins to DNS attacks, we have explored different types of attacks that can take advantage of vulnerabilities in wireless and networking protocols.

In this unit we have seen that attackers are constantly evolving their techniques, and staying vigilant is essential to protecting ourselves and our networks. Employing best practices such as using strong passwords, keeping software up to date, implementing network segmentation, and monitoring for unusual activity can go a long way in preventing attacks. By staying informed and taking proactive measures, we can mitigate the risks of wireless and network attacks and safeguard our digital assets.

## **2.5 Threat Actors, Vectors and Threat Intelligence Sources**

In the world of cybersecurity, understanding the various types of threats is essential to ensuring the safety and security of networks, systems, and sensitive information. Threat actors, or the individuals and groups behind cyber attacks, use a range of techniques and attack vectors to gain access to networks and data. By analysing these attack vectors and understanding the motivations of threat actors, security professionals can better defend against cyber attacks. In addition, threat intelligence sources such as open-source intelligence, vulnerability databases, and dark web intelligence provide valuable information for detecting and preventing cyber attacks. In this learning unit, we will explore the concept of threat actors, attack vectors, and the various sources of threat intelligence.

### **Threat Actors**

Threat actors refer to individuals, groups, or organisations that have the intention and capability to launch a cyber attack. These actors can range from script kiddies to advanced persistent threats (APTs) sponsored by nation-states. Understanding the different types of threat actors is crucial in developing an effective cybersecurity strategy.

Types of Threat Actors:

* **Hacktivists**: Individuals or groups who use hacking as a means of political or social activism, often motivated by a specific cause or ideology.
* **Cybercriminals**: Individuals or groups who commit crimes for financial gain, such as stealing sensitive information or money, ransomware attacks, or selling stolen data on the dark web.
* **Advanced Persistent Threats (APTs)**:These are highly skilled and well-resourced attackers who have the capability to launch sophisticated and long-term attacks. They are often sponsored by nation-states and target government agencies, critical infrastructure, and large corporations.
* **Insiders**: Employees, contractors, or partners who have access to an organisation's systems and data and can misuse their privileges intentionally or unintentionally.
* **Competitors**: Individuals or organisations who engage in cyber espionage or sabotage to gain an advantage in a competitive market or industry.
* **Script kiddies**: Individuals with little to no technical expertise who use pre-packaged tools and exploits to carry out attacks for fun or notoriety.

### **Attack Vectors**

Attack vectors are the methods or pathways that threat actors use to carry out their malicious activities. In previous units, we have covered various attacks that are commonly used by attackers. Following are some of the common attack vectors used by threat actors.

Types of attack vectors:

* **Direct access attack** vectors are those that rely on gaining physical access to a device, network, or system. This can be achieved through stealing or manipulating physical assets such as keys or badges, or by exploiting vulnerabilities in the physical security controls of a facility. Threat actors may use these attack vectors to install malware or to steal sensitive information.
* **Wireless attack** vectors target wireless networks, which can be vulnerable to attacks such as rogue access points and man-in-the-middle attacks. Threat actors may also use wireless attacks to steal login credentials, launch denial-of-service attacks, or intercept and manipulate data.
* **Email attack** vectors are one of the most common methods used by threat actors. Phishing attacks, and spear-phishing attacks all rely on tricking users into clicking on malicious links or attachments. Once the user interacts with the malicious content, threat actors can install malware, steal login credentials, or carry out other malicious activities.
* **Social media attack** vectors are similar to email attack vectors, in that they rely on tricking users into interacting with malicious content. Threat actors may use social media platforms to spread malware, steal login credentials, or gain access to sensitive information.
* **Removable media attack** vectors refer to attacks carried out through USB drives, CDs, and other removable storage devices. These attacks can be particularly dangerous if the removable media is infected with malware, as it can quickly spread throughout a network or system.
* As more businesses move their operations to the cloud, **cloud attack** vectors are becoming increasingly common. Threat actors may target cloud-based systems to steal data, launch denial-of-service attacks, or gain access to sensitive information.

### **Threat Intelligence**

Threat intelligence is a crucial component in cybersecurity defence strategy. It involves gathering and analysing data from various sources to identify potential security threats and vulnerabilities. This information is used to develop proactive measures and responses to mitigate the impact of attacks.

There are several types of threat intelligence sources available to security professionals:

* One of the most commonly used is open-source intelligence (**OSINT**), which involves collecting information from publicly available sources such as news articles, social media, and online forums. This can provide valuable insights into the tactics, techniques, and procedures (TTPs) of threat actors.

*Note:* ***TTPs*** *is an abbreviation for Tactics, Techniques, and Procedures. It refers to the methods used by threat actors to carry out attacks, compromise networks, and exfiltrate data. By analysing TTPs, security analysts can better understand the behaviour of threat actors and develop effective strategies for defence.*

* Another important source of threat intelligence is **vulnerability databases**, which provide information about known security weaknesses and software vulnerabilities. This can help organisations identify and patch vulnerabilities before they can be exploited by attackers.

*Note: Examples of vulnerability databases include the National Vulnerability Database (*[*NVD*](https://nvd.nist.gov/)*), Common Vulnerabilities and Exposures (*[*CVE*](https://cve.mitre.org/)*), Exploit Database, and the Open Web Application Security Project (*[*OWASP Top 10*](https://owasp.org/www-project-top-ten/)*).*

* **Indicators of compromise** (IOCs) are another valuable source of threat intelligence. These are pieces of information that indicate that a system has been compromised or is at risk of being compromised. IOCs can include IP addresses, domain names, file hashes, and other types of data that can be used to identify and track malicious activity.

The most common indicators of compromise (IOCs) include:

* **Malicious IP addresses**: IP addresses used by threat actors to launch attacks or exfiltrate data.
* **Suspicious network traffic**: Anomalous network traffic that may indicate the presence of an attacker or malware.
* **Unusual login activity**: Unusual or unauthorised login activity on systems or applications.
* **System logs**: System logs that may contain evidence of an attack or security incident.
* **User behaviour anomalies**: Anomalous user behaviour that may indicate the presence of an attacker or insider threat.
* The **dark web is another source of threat intelligence**, providing insights into the underground marketplace for cybercriminal activities, including the sale of malware, exploits, and stolen data. Dark web intelligence can help organisations better understand the motivations and tactics of threat actors and identify potential threats to their networks and data.

### **Conclusions**

As we come to the end of this learning journey on threat actors, attack vectors, and threat intelligence, it's clear that cybersecurity is an ever-evolving landscape. Understanding who the potential attackers are, their motives, and the methods they use is crucial to building effective defences. Likewise, understanding the various attack vectors that they use to exploit vulnerabilities can help us better prepare and protect our networks, systems, and data.

Finally, having access to relevant and up-to-date threat intelligence, such as open-source intelligence, vulnerability databases, and dark web intelligence, is a critical component of a proactive cybersecurity strategy. The ability to predict and prevent attacks before they occur is becoming increasingly important in today's threat landscape.

By incorporating these concepts and strategies into our overall cybersecurity posture, we can better safeguard our organisations and ourselves from the risks posed by cyber threats and malicious actors.

## **2.6 Vulnerabilities**

Vulnerabilities are a major concern in the world of cybersecurity, as they provide attackers with opportunities to exploit weaknesses in software, systems, or networks. Vulnerabilities can be caused by a range of factors, including coding errors, unsecured accounts, weak encryption, and more. Attackers can leverage these vulnerabilities to carry out a range of attacks, from stealing data and credentials to taking control of systems or networks. Understanding common vulnerabilities and how to address them is a critical aspect of maintaining a secure environment.

### **Vulnerability Types**

There are several types of vulnerabilities that can exist in a system, network, or software, including but not limited to: zero-day attacks, open permissions, unsecured root accounts, errors, weak encryption, insecure protocols, default settings, open ports and services, improper patch management, and legacy platforms. Following, we will explore each type of vulnerability in more detail and understand how they can be exploited by attackers.

#### **Zero-day attacks**

A zero-day vulnerability refers to a flaw or weakness in a software or system that is unknown to the vendor or security community.

Attackers can exploit these vulnerabilities to gain unauthorised access, steal data, or deploy malware.

To mitigate the risk of zero-day attacks, organisations should keep their software and systems up to date with the latest patches and security updates.

#### Open permissions

Open permissions refer to the situation where users have more access privileges than necessary.

Attackers can exploit this vulnerability to gain access to sensitive data or systems.

To address this vulnerability, organisations should implement the principle of **least privilege**, where users are granted only the necessary level of access to perform their job functions.

#### **Unsecured root accounts**

Root accounts have the highest level of privilege on a system or network.

If these accounts are not secured properly, they can be exploited by attackers to gain unrestricted access to an organisation's infrastructure.

To mitigate this risk, organisations should use strong passwords, implement multi-factor authentication, and regularly monitor and audit root account activity.

#### **Errors**

Errors in software code or configurations can create vulnerabilities that attackers can exploit.

Common errors include buffer overflows, injection flaws, and cross-site scripting.

To address this vulnerability, organisations should implement secure coding practices, conduct regular security testing and vulnerability scanning, and ensure that software is kept up to date with security patches.

#### **Weak encryption**

Weak encryption algorithms or keys can make it easier for attackers to intercept and decrypt sensitive data.

To address this vulnerability, organisations should use strong encryption algorithms and keys, and regularly review and update their encryption practices to keep up with evolving security threats.

#### **Insecure protocols**

Insecure network protocols, such as FTP and Telnet, can expose sensitive data to interception and manipulation by attackers.

To address this vulnerability, organisations should use secure protocols, such as SSH and HTTPS, and disable insecure protocols wherever possible.

#### **Default settings**

Many software and systems come with default settings that may not be secure or appropriate for an organisation's needs.

Attackers can exploit these settings to gain unauthorised access or compromise sensitive information.

To address this vulnerability, organisations should review and update default settings as necessary to ensure that they align with their security requirements.

#### **Open ports and services**

Open ports and services on a network can provide attackers with entry points into an organisation's infrastructure.

To address this vulnerability, organisations should regularly scan their networks to identify open ports and services, and close or restrict access to those that are not necessary.

#### **Improper patch management**

Failure to keep software and systems up to date with security patches can create vulnerabilities that attackers can exploit.

To address this vulnerability, organisations should implement a patch management process that includes regular patching and testing, and prioritises critical security updates.

#### **Legacy platforms**

Older operating systems or software that are no longer supported by vendors may contain known vulnerabilities that are not being patched.

To address this vulnerability, organisations should upgrade to newer, supported platforms wherever possible, and implement compensating controls, such as firewalls and intrusion detection systems, to mitigate the risk of attacks.

### **Third-party Risks**

Organisations rely heavily on third-party vendors, suppliers, and contractors to provide products, services, and support. However, these third-party relationships can also introduce significant security risks. Following, we will explore different types of third-party risks that organisations face and strategies to mitigate them.

*Note:* ***Third-party risks*** *refer to security threats that arise from an organisation's dependence on third-party vendors or contractors. These risks can include data breaches, cyber attacks, or other security incidents that impact an organisation's network or data.*

#### **System Integration Risk**

System integration risk occurs when third-party products or services are integrated into an organisation's infrastructure, potentially exposing vulnerabilities in the system.

This risk can be mitigated by conducting thorough security assessments of third-party products before integrating them into the system.

#### **Lack of Vendor Support**

When third-party vendors stop supporting their products, it can lead to vulnerabilities going unpatched. This can put an organisation at risk of a cyber attack.

To mitigate this risk, it is important to establish clear contractual obligations and timelines for vendor support.

#### **Supply Chain Risk**

The supply chain risk arises from an organisation's reliance on third-party suppliers, which can introduce security threats. Attackers may target these suppliers to access an organisation's sensitive data or network.

Organisations can mitigate this risk by conducting security assessments of suppliers and monitoring their security practices.

#### **Outsourced Code Development**

Outsourcing code development to third-party vendors can introduce vulnerabilities, particularly if security is not a primary consideration during the development process.

To mitigate this risk, organisations should conduct regular security assessments of third-party code and ensure that security requirements are included in contracts with code developers.

#### **Data Storage**

When an organisation stores data with a third-party vendor, it can introduce security risks, particularly if the vendor's security practices are inadequate.

Organisations can mitigate this risk by carefully selecting vendors with strong security practices and ensuring that they comply with applicable security regulations and standards.

### **Vulnerability Impacts**

Vulnerabilities in the cybersecurity field refer to weaknesses or gaps in systems or networks that could be exploited by threat actors to carry out attacks. The impacts of these vulnerabilities can be severe and long-lasting, affecting various aspects of organisations and individuals. This learning unit will cover the different impacts of vulnerabilities, including data loss, identity theft, financial loss, reputation impacts, and availability loss.

#### **Data loss**

Vulnerabilities that lead to data loss can have significant consequences, particularly for organisations that rely on data for their operations. Attackers can exploit vulnerabilities to steal sensitive data such as personal information, intellectual property, or financial information. The loss of data can cause financial losses, legal liabilities, and reputational damage.

#### **Identity theft**

Vulnerabilities that expose personal information can result in identity theft. Attackers can use stolen information to impersonate individuals, open fraudulent accounts, or carry out other malicious activities. Victims of identity theft can suffer financial loss, damage to credit scores, and reputational damage.

#### **Financial loss**

Vulnerabilities can lead to financial losses for both individuals and organisations. Attackers can exploit vulnerabilities to carry out fraudulent activities such as unauthorised money transfers, fraudulent transactions, and stolen financial information. These activities can lead to significant financial loss and legal liabilities.

#### **Reputation impacts**

Vulnerabilities can also have severe impacts on an organisation's or individual's reputation. If a vulnerability results in data breaches or other malicious activities, it can lead to a loss of trust from customers, partners, or stakeholders. The reputational damage can result in loss of revenue, legal liabilities, and difficulties in attracting new partnerships.

#### **Availability loss**

Vulnerabilities that result in system downtime or unavailability can significantly impact an organisation's operations. Attackers can exploit vulnerabilities to carry out denial-of-service attacks or other malicious activities that can lead to system downtime, which can result in a loss of productivity, revenue, and partner/customer trust.

### **Conclusions**

In conclusion, understanding vulnerabilities and their potential impacts is essential to developing a strong cybersecurity posture. Vulnerabilities can come in many forms, including system integration risks, supply chain risks, and third-party risks. These types of risks can lead to data loss, identity theft, financial loss, reputation impacts, and availability loss. Organisations must take proactive steps to identify and address vulnerabilities in their systems and third-party relationships to reduce the risk of security incidents. By doing so, they can protect their valuable assets and maintain the trust of their stakeholders.

## **2.7 Security Assessments**

Security Assessments are an essential part of an organisation's security posture, as they enable proactive identification and mitigation of potential security threats. By conducting assessments such as threat hunting, vulnerability scanning, and Security Information and Event Management systems, organisations can identify and address security gaps and reduce the likelihood of successful attacks. These assessments help organisations to improve their overall security posture and minimise the risk of data breaches and other security incidents.

### **Threat Hunting**

Threat hunting is a proactive approach to detecting and responding to threats that have evaded traditional security measures. It involves using intelligence fusion and cybersecurity manoeuvres to identify potential threats and prevent them from causing harm.

Following are some key concepts related to threat hunting.

#### **Intelligence fusion**

Threat hunting involves gathering and analysing data from multiple sources to create a comprehensive picture of the security landscape. This includes data from threat intelligence feeds, security logs, network traffic, and other sources.

#### **Fusing the data**

Once the data is gathered, it must be analysed to identify patterns and anomalies that may indicate a potential threat. This process involves using advanced analytics tools and techniques, such as machine learning and artificial intelligence, to identify and correlate data points.

#### **Cybersecurity manoeuvres**

Threat hunting often involves using a variety of cybersecurity manoeuvres to identify and respond to potential threats. These may include isolating suspicious network traffic, disabling compromised systems, and conducting forensic investigations to determine the extent of a breach.

By incorporating threat hunting into their security strategy, organisations can proactively identify and respond to threats, reducing the risk of data breaches and other security incidents.

### **Vulnerability Scans**

Vulnerability scanning is a critical component of any cybersecurity program. It involves the use of automated tools to identify security vulnerabilities in systems, applications, and networks. We will cover the various aspects of vulnerability scans, including scan types, identifying vulnerabilities, vulnerability research, log review, and managing false positives.

#### **Scan Types**

There are various types of vulnerability scans, including **host-based**, **network-based**, and **application-based** scans:

* **Host-based scans** check the systems and devices on the network for vulnerabilities.
* **Network-based scans** look for vulnerabilities in the network devices and communication channels.
* **Application-based scans** check for vulnerabilities in the applications and software installed on the network.

#### **Identifying Vulnerabilities**

The primary purpose of a vulnerability scan is to identify vulnerabilities in the network and applications. The scan results include a list of vulnerabilities identified, their severity, and recommendations for remediation. Vulnerability scans can be conducted manually or using automated tools.

#### **Vulnerability Research**

Vulnerability research involves studying and analysing security vulnerabilities to understand how they work and how to protect against them. This is an ongoing process that involves monitoring emerging threats and keeping up to date with new vulnerabilities and exploits.

By understanding how vulnerabilities work, cybersecurity professionals can develop effective mitigation strategies.

When conducting vulnerability research, one valuable resource to consult is the National Vulnerability Database ([NVD](https://nvd.nist.gov/)), which is a comprehensive database of known vulnerabilities in software and systems. The NVD is maintained by the National Institute of Standards and Technology (NIST) and provides detailed information on vulnerabilities, including Common Vulnerability Scoring System (CVSS) scores and Common Vulnerabilities and Exposures (CVE) identifiers. [CVSS](https://www.first.org/cvss/) is a standardised system for scoring the severity of vulnerabilities, while [CVE](https://cve.mitre.org/) provides unique identifiers for each known vulnerability.

#### **Vulnerability Scan Log Review**

Vulnerability scan logs contain a wealth of information about the scan results, including the vulnerabilities identified and the systems and devices affected. Reviewing the vulnerability scan logs is essential for identifying security gaps and developing an effective security strategy. Analysing vulnerability scan logs can also help identify trends and patterns that may indicate a larger security issue.

#### **Dealing with False Positives**

False positives are vulnerabilities that are reported as present in a system but are not actually present. False positives can occur due to errors in the scanning tool, misconfiguration of the system, or other factors. It is important to manage false positives effectively to avoid wasting time and resources on remediation efforts that are not necessary.

#### **Dealing with False Negatives**

False negatives are vulnerabilities that are not reported by the scanning tool but are actually present in the system. False negatives can occur due to the scanning tool's limitations, lack of visibility, or other factors. Cybersecurity professionals must be aware of the potential for false negatives and use other tools and techniques to identify vulnerabilities that may have been missed by the scan.

#### **Tools**

Here is a list of popular free and open source vulnerability scanning tools:

* [OpenVAS](https://www.openvas.org/): A powerful vulnerability scanner that can perform comprehensive vulnerability scans on a wide range of systems and networks. It is compatible with various operating systems, including Linux, Windows, and macOS.
* [Nmap](https://nmap.org/): A popular network exploration tool that can also be used for vulnerability scanning. It can identify open ports, running services, and operating systems, and can detect potential vulnerabilities.
* [Metasploit](https://www.metasploit.com/): A widely-used penetration testing framework that includes a vulnerability scanner. It can scan for known vulnerabilities in a target system and exploit them to gain access.
* [Nikto](https://github.com/sullo/nikto): A web server scanner that can identify potential vulnerabilities in web servers and applications. It can scan for outdated software versions, misconfigurations, and other security issues.
* [OWASP ZAP](https://www.zaproxy.org/): A popular web application security scanner that can identify vulnerabilities in web applications. It can detect vulnerabilities such as SQL injection, cross-site scripting (XSS), and more.
* [Wapiti](https://wapiti-scanner.github.io/): A web application vulnerability scanner that can detect vulnerabilities in web applications. It supports various web technologies and can identify issues such as SQL injection, XSS, and more.

These tools can be used by cybersecurity professionals, system administrators, and developers to identify vulnerabilities and address them before they can be exploited by threat actors.

### **Security Information and Event Management**

Security Information and Event Management (**SIEM**) is an approach to security management that combines the data collection and analysis capabilities of Security Event Management (**SEM**) and Security Information Management (**SIM**). This allows for real-time monitoring and analysis of security-related events and alerts, as well as long-term storage and analysis of security-related data.

### **SIEM & SOAR**

SIEM technology is designed to provide a centralised view of an organisation's security posture by collecting and analysing security-related data from various sources. Some of the sources that SIEM technology may collect data from include:

* System logs
* Network traffic logs
* Intrusion detection and prevention systems
* Firewalls
* Antivirus and anti-malware software
* Application logs
* Identity and access management systems
* Endpoint detection and response systems

SIEM technology uses data analysis techniques to identify and prioritise security-related events and alerts. This can include correlation analysis, which compares events and alerts from multiple sources to identify potential security incidents, and anomaly detection, which uses statistical analysis to identify patterns and trends that may indicate a security breach.

SIEMs may also be used in conjunction with Security Orchestration, Automation and Response (**SOAR**) technology. SOAR technology uses automation to help security teams quickly respond to security incidents and alerts. This can include automating tasks such as network isolation, malware quarantine, and user account deactivation.

Analysing the data collected by SIEM technology is an important part of the security monitoring process. This can involve reviewing logs and alerts to identify potential security incidents, as well as conducting forensic analysis to determine the root cause of a security breach. It is important to ensure that the data collected by SIEM technology is accurate and up-to-date, as well as being properly analysed to identify potential security threats.

#### **Tools**

Here is a list of some free and open source SIEMs:

* [ELK Stack](https://www.elastic.co/what-is/elk-stack): A combination of Elasticsearch, Logstash, and Kibana that provides powerful log management and analysis capabilities. It allows users to ingest and parse logs from a wide range of sources and provides a powerful search and visualisation interface.
* [OSSIM](https://cybersecurity.att.com/products/ossim): An open source SIEM platform that includes a variety of security tools and features, such as event management, asset discovery, vulnerability assessment, and network monitoring. It provides a centralised view of an organisation's security posture and can help identify threats and attacks in real-time.
* [Wazuh](https://wazuh.com/): An open source security platform that integrates security information and event management, log management, and endpoint detection and response. It provides real-time analysis of security alerts and can help identify and respond to threats quickly.

Each of these SIEM platforms provides different functionalities, but they all offer powerful security analysis and monitoring capabilities.

### **Conclusions**

In conclusion, threat hunting, vulnerability scanning, and security information and event management (SIEM) are crucial components of any effective cybersecurity program. Threat hunting involves intelligence fusion and cybersecurity manoeuvres to proactively detect and respond to threats. Vulnerability scans identify potential vulnerabilities in an organisation's systems, allowing for timely patching and remediation. SIEM tools, such as the ELK stack, OSSIM, and Wazuh, collect and analyse security event data, enabling organisations to quickly detect and respond to security incidents. By utilising these techniques and tools, organisations can significantly enhance their cybersecurity posture and protect against potential threats.

## **2.8 Penetration Testing**

Penetration Testing is a practice used to test the security of a system, network or application by simulating an attack by a malicious actor. It is a proactive approach to identifying vulnerabilities and assessing the effectiveness of security controls. Before conducting a pentest, reconnaissance is performed to gather information about the target system. Pentesting is typically performed by specialised security teams with expertise in identifying and exploiting vulnerabilities in order to provide recommendations for remediation.

### **Pentest**

Penetration testing (or pentesting) is an essential component of any organisation's security strategy. It involves simulating real-world attacks to identify and exploit vulnerabilities in an organisation's systems, networks, and applications. This learning unit aims to provide a basic understanding of the pentest process, what penetration testers do, and how to interpret the results of a pentest report.

#### **Rules of Engagement**

Before a pentest, it's important to define the rules of engagement, which specify the scope of the test, the target systems, and the testing methods. The pentester and the organisation should agree on the terms and conditions of the test, including the duration of the test, the testing methods used, and the scope of the test.

#### **Working Knowledge**

Pentesters use a variety of tools and techniques to identify and exploit vulnerabilities in an organisation's systems. It's important to have a basic understanding of these tools and techniques to understand the results of the test.

#### **Exploiting Vulnerabilities**

Once vulnerabilities have been identified, pentesters attempt to exploit them to gain unauthorised access to the organisation's systems. This phase of the test helps identify weaknesses in the organisation's security defences and the potential impact of a successful attack.

#### **The Process**

The pentest process typically involves several phases, including reconnaissance, scanning, enumeration, exploitation, and post-exploitation. During each phase, the pentester uses a combination of manual and automated techniques to identify and exploit vulnerabilities.

The penetration testing process typically involves several key steps, including:

* **Planning and reconnaissance**: In this stage, the penetration tester will gather information about the target system or network, including IP addresses, network topology, and any available documentation or other information. This may involve tools such as port scanners, network mappers, and web application scanners.
* **Scanning**: Once the tester has gathered sufficient information, they will begin scanning the target system or network for vulnerabilities. This may include both automated scanning tools and manual testing techniques to identify weaknesses in the target.
* **Gaining access**: After identifying vulnerabilities, the tester will attempt to exploit them to gain access to the target system or network. This may involve exploiting weaknesses in web applications, software vulnerabilities, or social engineering techniques to trick users into providing sensitive information.
* **Maintaining access**: Once the tester has gained access to the target system or network, they will attempt to maintain that access in order to explore further and gather additional information about the target.
* **Analysis and reporting**: Finally, the penetration tester will analyse the results of the testing and generate a detailed report outlining the vulnerabilities that were identified, the methods used to exploit them, and recommendations for remediation.

It's important to note that the process may vary somewhat depending on the specific goals and scope of the penetration test, as well as the tools and techniques used by the tester. However, in general, these steps provide a good overview of the key stages involved in conducting a successful penetration test.

#### **Pentest Aftermath**

After the test is complete, the pentester provides a report outlining the vulnerabilities that were identified, the methods used to exploit them, and recommendations for remediation. It's important to understand the report and the severity of the vulnerabilities identified, as well as prioritise the remediation efforts based on the severity and impact of each vulnerability.

A successful pentest requires a well-defined scope, knowledgeable and experienced testers, and a thorough understanding of the process and results. By following the guidelines outlined in this learning unit, organisations can better prepare for a pentest, understand what penetration testers do, and effectively interpret the results of a pentest report to prioritise remediation efforts and improve their overall security posture.

### **Security Teams**

In the field of cybersecurity, security teams play an essential role in protecting organisations' systems and data from potential threats. There are different types of security teams, and each has a specific function to perform.

#### **Blue Team**

The blue team is responsible for the defence of an organisation's systems and data. Their primary role is to detect and respond to cyber threats in real-time. Blue team members are also responsible for implementing security measures such as firewalls, intrusion detection systems, and other security tools to prevent attacks from happening.

#### **Red Team**

The red team is a group of ethical hackers who simulate cyberattacks to identify vulnerabilities in an organisation's systems and applications. Their primary goal is to test the effectiveness of the organisation's security defences and identify weaknesses that need to be addressed.

#### **Purple Team**

The purple team is a combination of both the red and blue teams. The primary function of the purple team is to identify the gaps in the security defences by simulating attacks, and the blue team uses that information to enhance their security posture.

#### **White Team**

The white team is responsible for managing the rules of engagement during a security assessment. They ensure that the testing process adheres to a predefined scope and that the red team does not cause any damage to the organisation's systems.

Understanding the different roles of security teams is crucial for organisations to have a well-rounded security program. With the blue team responsible for defence, the red team responsible for offence, and the white team responsible for managing the testing process, organisations can ensure that their systems and data are secure. The purple team plays a vital role in bridging the gap between the red and blue teams, ensuring that the organisation is well-protected against potential threats.

### **Conclusions**

In conclusion, conducting a thorough and effective security assessment of an organisation's systems and processes is crucial to identifying and addressing potential vulnerabilities and threats. Penetration testing, when performed properly and with clear rules of engagement, can provide valuable insights into an organisation's security posture. Additionally, having a dedicated security team composed of both defensive and offensive security experts can help ensure ongoing security and risk management, through activities like threat hunting and incident response. With the right tools and processes in place, organisations can better protect their assets and prevent cyberattacks.

## **The Geek’s Corner**

Welcome to Geek's Corner, a section where you can explore various technical topics in more detail. In this section, we cover SQL injection.

**SQL injection** is a type of security vulnerability that allows attackers to inject malicious SQL statements into an application's database backend. This can lead to unauthorised access to sensitive information or even full control over the application and its data.

To understand SQL injection, it's important to have a basic understanding of SQL, which is the language used to interact with databases. SQL statements are used to retrieve, insert, update, and delete data from a database.

In SQL injection attacks, attackers can insert malicious SQL statements into the application's input fields, such as login forms or search bars. This is possible when the application fails to properly validate and sanitise user input, allowing attackers to execute their own SQL code.

To learn more about SQL injection and how to prevent it, check out this [link](https://portswigger.net/web-security/sql-injection) from the PortSwigger Academy (you can create an account for free).

The PortSwigger Academy offers a comprehensive guide on SQL injection, including interactive labs to help you practise identifying and exploiting SQL injection vulnerabilities. The labs are designed to simulate real-world scenarios, allowing you to learn how to detect and prevent SQL injection attacks in a safe and controlled environment.

By completing the labs, you'll gain a deeper understanding of SQL injection and its impact on web security. You'll also learn how to use tools like SQLMap and Burp Suite to automate and streamline the SQL injection testing process.

Overall, understanding SQL injection is critical for anyone involved in web development or web security. By taking the time to learn about this vulnerability and how to prevent it, you can help protect yourself and your organisation from potentially devastating attacks.

# **Conclusions**

In this module, we covered various topics related to vulnerabilities, attacks, techniques, and threats. We discussed social engineering techniques such as phishing and dumpster diving, malware, password attacks, physical attacks, and cryptographic attacks. We also explored application attacks such as cross-site scripting and injection attacks, network attacks including DNS poisoning and domain hijacking, and vulnerability types such as zero-day attacks and insecure root accounts. Additionally, we learned about security assessments, threat hunting, vulnerability scans, and penetration testing.

Overall, this module provided a comprehensive understanding of the different types of attacks and vulnerabilities that exist in the digital world, and how they can be exploited by threat actors. We also learned about various tools and techniques that can be used to prevent and detect such attacks. By the end of the module, you should have gained the necessary knowledge and skills to better protect yourself and your organisation from cyber threats.

## **Quiz**

**What is the primary goal of a penetration tester?**

a) To hack into an organisation's systems and steal data

b) To identify vulnerabilities in an organisation's systems and report them to management

c) To monitor an organisation's systems for security breaches

d) To provide guidance on compliance with industry regulations and standards

**What is a vulnerability in the context of cybersecurity?**

a) An unauthorised attempt to access a computer system

b) A flaw or weakness in a computer system's security that can be exploited

c) A type of cyber attack that involves stealing data from a system

d) A method used by hackers to gain access to a system

**What is a threat actor in the context of cybersecurity?**

a) A person or group who launches cyber attacks

b) A type of malware that infects computer systems

c) A technique used by hackers to steal data

d) A security measure used to protect computer systems

**What is the term for a cyber attack that involves tricking someone into revealing sensitive information?**

a) Social engineering

b) Denial of Service (DoS)

c) Brute force attack

d) Malware

**What is the term for a type of cyber attack where an attacker intercepts communication between two parties in order to steal sensitive information?**

a) Man-in-the-Middle (MitM) attack

b) Cross-Site Scripting (XSS) attack

c) Cross-Site Request Forgery (CSRF) attack

d) Ransomware attack

## **References**

United States Securities and Exchange Commission. (2018). Equifax Inc. Form 8-K: Current report filing (Amended). Retrieved from https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm