TOOLS AND METHODS USED IN CYBERCRIME

**Phishing**

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

**Types of Phishing**

**Advanced-fee scam** This common email phishing attack is popularized by the “Nigerian prince” email, where an alleged Nigerian prince in a desperate situation offers to give the victim a large sum of money for a small fee upfront. Unsurprisingly, when the fee is paid, no large sum of money ever arrives.

The interesting history is that this type of scam has been occurring for over a hundred years in different forms; it was originally known in the late 1800s as the Spanish Prisoner scam, in which a con artist contacted a victim to prey on their greed and sympathy. The con artist is allegedly trying to smuggle out a wealthy Spanish prisoner, who will reward the victim handsomely in exchange for the money to bribe some prison guards.

This attack (in all its forms) is mitigated by not responding to requests from unknown parties in which money has to be given to receive something in return. If it sounds too good to be true, it probably is. A simple Google search on the theme of the request or some of the text itself will often bring up the details of the scam.

**Account deactivation scam** By playing off the urgency created in a victim who believes an important account is going to be deactivated, attackers are able to trick some people into handing over important information such as login credentials.

Here’s an example: The attacker sends an email that appears to come from an important institution like a bank, and they claim the victim’s bank account will be deactivated if they do not take action quickly. The attacker will then request the login and password to the victim’s bank account in order to prevent the deactivation. In a clever version of the attack, once the information is entered, the victim will be directed to the legitimate bank website so that nothing looks out of place.

This type of attack can be countered by going directly to the website of the service in question and seeing if the legitimate provider notifies the user of the same urgent account status. It’s also good to check the URL bar and make sure that the website is secure. Any website requesting a login and password that is not secure should be seriously questioned, and nearly without exception should not be used.

**Website forgery scam** This type of scam is commonly paired with other scams such as the account deactivation scam. In this attack, the attacker creates a website that is virtually identical to the legitimate website of a business the victim uses, such as a bank. When the user visits the page through whatever means, be it an email phishing attempt, a hyperlink inside a forum, or via a search engine, the victim reaches a website which they believe to be the legitimate site instead of a fraudulent copy. All information entered by the victim is collected for sale or other malicious use.

In the early days of the Internet, these types of duplicate pages were fairly easy to spot due to their shoddy craftsmanship. Today the fraudulent sites may look like a picture-perfect representation of the original.

By checking the URL in the web browser, it is usually pretty easy to spot a fraud. If the URL looks different than the typical one, this should be considered highly suspect. If the pages listed as insecure and HTTPS is not on, this is a red flag and virtually guarantees the site is either broken or a phishing attack.

**Spear phishing** This type of phishing is directed at specific individuals or companies, hence the term spear phishing. By gathering details or buying information about a particular target, an attacker is able to mount a personalized scam. This is currently the most effective type of phishing, and accounts for over 90% of the attacks.

Here is an example: Joe is an executive assistant to a CEO named Mary. One day when Mary is on vacation abroad, Joe gets an urgent email from her. The email states that her luggage and phone have been stolen. She says she has no money or passport and needs him to send over her PayPal credentials ASAP so that she can book a hotel and buy a flight home. Joe might see this harrowing message from his employer and immediately send over the requested information.

This sort of "I'm in trouble and need money" request from a superior is a common spear phishing script. The attacker could be spoofing Mary's email, as well as sending the email to dozens of different combinations of Joe's name and initials in hopes of finding the correct one. The attacker may also have learned about Mary's vacation plans by following her on Twitter. Combining all of these tools, the attacker can devise a very convincing con.

A notable real-life example of this happened in 2016, when an attacker posed as the CEO of Snapchat and was able to convince an employee to hand over confidential payroll information.

Spear phishing The message was a phishing scam that impersonated Snapchat's CEO Evan Spiegel. In the email, a hacker posing as Spiegel requested payroll information for existing and ex-employees. The hacker then exposed that information to the outside world. Snapchat issued a public apology to its workers in a blog post on Sunday.

The startup has contacted all of the employees who were impacted by the scam, and offered them offered two years of identity-theft monitoring and insurance. Snapchat says it has strengthened its training programs too.

Spear phishing attacks can also leverage information from data breaches. Another example:

Steve buys a computer at a major [online retailer](https://www.cloudflare.com/ecommerce/), but a few weeks later the retailer has a data breach. Although sensitive data like credit card numbers and passwords were hash-protected, customer email addresses and order histories were leaked.

A few days later, Steve gets an email from the manufacturer of his new computer announcing that his model is being recalled, and providing a link to receive a refund. The link takes Steve to a fake version of the manufacturer's website and provides a form for Steve to enter his credit card number for the refund. The attacker used some fairly harmless data to gain Steve's confidence and trick him into handing over his financial information

**Whaling**  Whaling is a spear phishing attack that targets a very high-profile victim, usually a top executive at a company or a celebrity. Whaling attacks tend to be more sophisticated, and in many cases attackers will first carry out spear phishing attacks on smaller targets, such as employees of the "whale," in order to gain access to their ultimate victim.

For example: While on vacation, Mary the CEO gets an email or call from someone she knows on her IT team letting her know that they are enduring a cyber attack and requesting access to her work computer and her accounts to ensure that company data can be secured. It is possible that an attacker compromised her IT team in order to gain Mary's trust, in hopes of convincing her to hand over her credentials.

Protection against Spear phishing and whaling 1. Never share financial information, passwords, or any other sensitive data over phone, chat, or email. 2. Do not click on links in emails, even if they appear to be from a trusted source. Copying and pasting or hand-typing the URL can help protect from cross-site scripting attacks. 3. Enable 2-factor authentication on all important accounts, so that stolen login credentials are not enough. 4. Enable Zero Trust security policies to ensure that an intruder does not have open access to a network.

**What is whaling?** For attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used. These type of attacks are typically targeted with content likely to require the attention of the victim such as legal subpoenas or other executive issues.

**Clone phishing** Clone phishing involves mimicking a previously delivered legitimite email and modifying its links or attached files in order to trick the victim into opening a malicious website or file. For example, by taking an email and attaching a malicious file with the same filename as the original attached file, and then resending the email with a spoofed email address that appears to come from the original sender, attackers are able to exploit the trust of the initial communication in order to get the victim to take action.

**Whaling** Another common vector of this style of attack is whaling scam emails that appear to come from an executive. A common example would be an email request coming from a CEO to someone in the finance department requesting their immediate help in transferring money. Lower-level employees are sometimes fooled into thinking the importance of the request and the person it’s coming from supersede any need to double check the request’s authenticity, resulting in the employee transferring large sums of money to an attacker.

**Password Cracking**

Password cracking means recovering passwords from a computer or from data that a computer transmits. This doesn’t have to be a sophisticated method. A brute-force attack where all possible combinations are checked is also password cracking

If the password is stored as plaintext, hacking the database gives the attacker all account information. However, now most passwords are stored using a key derivation function (KDF). This takes a password and runs it through a one-way encryption cipher, creating what’s known as a “hash.” The server stores the hash-version of the password.

While passwords are a very popular account security tool, they aren’t necessarily the safest option. That’s especially the case if a user creates a weak password, reuses it, and stores its plaintext copy somewhere online. That’s why using a password manager, biometric data (which has its cons too) or adding a second factor will make most of the cracking methods below useless.

A typical password cracking attack looks like this: 1. Get the password hashes 2. Prepare the hashes for a selected cracking tool 3. Choose a cracking methodology 4. Run the cracking tool 5. Evaluate the results 6. If needed, tweak the attack 7. Go to Step 2

**Popular Password Cracking Techniques**

1. Phishing: Phishing is the most popular technique that involves luring the user into clicking on an email attachment or a link that contains malware. The methods for doing so usually involve sending some important and official-looking email that warns to take action before it’s too late. In the end, password-extracting software is installed automatically or the user enters his account details into a look-alike website.

1. Malware: Two of the most common malware types for stealing passwords are keyloggers and screen scrapers. keyloggers sends all your keystrokes to the hacker, Screen Scrapers uploads the screenshots.

A backdoor trojan can grant full access to the user’s computer, and this can happen even when installing so-called grayware. Also known as potentially unwanted applications, these programs usually install themselves after clicking the wrong “Download” button on some website. While most will display ads or sell your web usage data, some might install much more dangerous software.

1. Social Engineering: This password cracking technique relies on gullibility and may or may not employ sophisticated software or hardware – phishing is a type of social engineering scheme. Technology has revolutionized social engineering. In 2019 hackers used AI and voice technology to impersonate a business owner and fooled the CEO to transfer $243,000. This attack demonstrated that faking voice is no longer the future, and video imitation will become commonplace sooner than you think.

This password cracking technique relies on gullibility and may or may not employ sophisticated software or hardware – phishing is a type of social engineering scheme. Technology has revolutionized social engineering. In 2019 hackers used AI and voice technology to impersonate a business owner and fooled the CEO to transfer $243,000. This attack demonstrated that faking voice is no longer the future, and video imitation will become commonplace sooner than you think.

1. Brute Force Attack: If all else fails, password crackers have the brute force attack as a last resort. It basically involves trying all possible combinations until you hit the jackpot. However, password cracking tools allow to modify the attack and significantly reduce the time needed to check all variations. The user and his habits are the weak links again here.If the attacker was able to brute force a password, he will assume the password has been re-used and try the same combination of login credentials on other online services. This is known as credential stuffing and is very popular in the age of data breaches.

1. Dictionary Attack: A dictionary attack is a type of brute force attack and it’s often used together with other brute force attack types. It automatically checks if the password is not some often-used phrase like “iloveyou” by looking at the dictionary. The attacker might also add passwords from other leaked accounts. In such a scenario, the chance of a successful dictionary attack increases substantially.

1. Spidering: Spidering is a supplementary password cracking technique that helps with the above-mentioned brute force and dictionary attacks. It involves gathering information about the victim, usually a company, presuming that it uses some of that info for password creation. The goal is to create a word list that would help guess the password faster.

After checking the company’s website, social media, and other sources, one can come up with something like this: Founder name – Mark Zuckerberg Founder DOB – 1984 05 14 Founder’s sister – Randi Founder’s other sister – Donna Company name – Facebook Headquarters – Menlo Park Company mission – Give people the power to build community and bring the world closer together

Now all you have to do is upload it to a proper password cracking tool and reap the benefits.

While guessing is far from the most popular password cracking technique, it relates to business-oriented spidering above. Sometimes the attacker doesn’t even have to gather information about the victim because trying some of the most popular passphrases is enough.

If you recall using one or more of the pathetic passwords in the list below, we strongly recommend changing them now.

Some of the most common passwords worldwide: • 123456 • 123456789 • qwerty • password • 12345 • qwerty123 • 1q2w3e • 12345678 • 111111 • 1234567890

1. Rainbow table attack: Experienced hackers usually have a rainbow table that also involves leaked and previously cracked passwords, making it more effective. Most often, rainbow tables have all possible passwords that make them extremely huge, taking up hundreds of GBs. On the other hand, they make the actual attack faster because most of the data is already there and you only need to compare it with the targeted hash-password. Luckily, most users can protect themselves from such attacks with large salts and key stretching, especially when using both.

If the salt is large enough, say 128-bit, two users with the same password will have unique hashes. This means that generating tables for all salts will take an astronomical amount of time. As for the key stretching, it increases the hashing time and limits the number of attempts that the attacker can make in given time.

**Password Cracking Tools**

1. John the Ripper: John the Ripper is a free, open-source, command-based application. It’s available for Linux and macOS while Windows and Android users get Hash Suite, developed by a contributor.

1. Cain and Abel: Cain & Abel is another popular tool for password cracking. But contrary to John the Ripper, it uses GUI, making it instantly more user-friendly. That and the fact that it’s available on Windows only makes Cain & Abel a go-to tool for amateurs, also known as script kiddies.

1. Cain and Abel: Cain & Abel can act as a packet analyzer, record VoIP, analyze route protocols, or scan for wireless networks and retrieve their MAC addresses. If you already have the hash, this tool will offer a dictionary or brute force attack option. Cain & Abel can also display passwords that are hiding beneath the asterisks.

1. Ophcrack: Ophcrack is a free and open-source password cracking tool that specializes in rainbow table attacks. To be more precise, it cracks LM and NTLM hashes where the former addresses Windows XP and earlier OSs and the latter associates with Windows Vista and 7. NTLM is also available, to a certain degree, on Linux and freeBSD. Both of these hash types are insecure – it’s possible to crack a NTLM hash in less than 3 hours with a fast computer.

1. Wireshark: Wireshark. Wireshark enables you to do packet sniffing. It is an award-winning packet analyzer used not only by hackers but also by business and governmental institutions.

1. Metasploit: This is a popular penetration testing framework. Designed for security professionals, Metasploit can also be used by hackers to retrieve password hashes.

**Creating Strong passwords**

1. Length. As it often is, length is the most important factor. 2. Combine letters, numbers, and special characters. This greatly increases the number of possible combinations. 3. Do not re-use. Even if your password is strong in theory, re-using it will leave you vulnerable. 4. Avoid easy-to-guess phrases. A word that’s in the dictionary, on your pet’s collar or on your license plate is a big NO.

Password Cracking: Bottom Lines Password cracking is easier than most users think. There are plenty of free tools and some of them are easy enough even for novice crackers. There’s also more than one password cracking technique to try. Starting with a simple brute force attack and moving on to sophisticated methods that combine different techniques, password cracking is evolving every day. The best defense against password cracking is using a strong password. Using enough symbols and different characters ensures that even the fastest computer won’t crack your account in this lifetime. And since remembering multiple strong passwords is unlikely, the best bet is to use a reliable password manager. Two-factor authentication is still a pain in the rear for any hacker, so adding a finger or face ID will keep your data safe, at least for the foreseeable future.fcom

Types of Password Cracking Brute Force Attack: In a brute force attack, the attacker tries every possible combination of characters until the correct password is found. It's a straightforward but time-consuming method. Brute force attacks can be mitigated by using strong, complex passwords and rate limiting login attempts.

Dictionary Attack: In a dictionary attack, attackers use a list of common words, phrases, or passwords to guess the target's password. This approach is more efficient than brute force because it relies on known words and patterns. To defend against dictionary attacks, users should avoid using common words or phrases in their passwords.

Rainbow Table Attack: A rainbow table is a precomputed table of hashed values for common passwords or character combinations. Attackers use these tables to look up the original password from its hash quickly. To protect against rainbow table attacks, it's essential to use a unique salt for each password before hashing it.

Hybrid Attack: A hybrid attack combines elements of both dictionary and brute force attacks. It starts with a dictionary attack and then appends or prepends characters to the words in the dictionary, creating variations.

Credential Stuffing: In a credential stuffing attack, attackers use previously stolen username and password combinations to gain unauthorized access to multiple accounts. This type of attack relies on the fact that many users reuse passwords across multiple sites. Using unique passwords for different services is a defense against credential stuffing.

Phishing: Phishing attacks involve tricking users into revealing their passwords. Attackers create fake login pages or emails that appear to be from legitimate sources and ask users to enter their passwords. Users should always be cautious and verify the authenticity of login pages and emails.

Social Engineering: Social engineering attacks involve manipulating individuals into revealing their passwords or other sensitive information. Attackers may impersonate trusted individuals, ask for passwords over the phone, or trick users into revealing their credentials. Security awareness and education can help protect against social engineering attacks.

Keylogging: Keyloggers are malicious software or hardware that record keystrokes on a user's device. They can capture passwords and other sensitive information as users type. Protecting against keyloggers involves using up-to-date antivirus software and being cautious about downloading files from untrusted sources.

Online Attacks: In online attacks, attackers make repeated login attempts directly on the target system, such as a web application or server. Countermeasures against online attacks include account lockouts, CAPTCHA challenges, and rate limiting.

Offline Attacks: In offline attacks, attackers obtain a hashed password (e.g., from a compromised database) and attempt to crack it on their own system. They use methods like dictionary attacks, brute force attacks, or rainbow tables to guess the original password.

Man-in-the-Middle (MITM) Attack: In a MITM attack, an attacker intercepts communication between the user and a legitimate service, capturing passwords in the process. Using encrypted connections (HTTPS) and verifying digital certificates can protect against MITM attacks.

Keyloggers and Spywares Spyware is largely invisible software that gathers information about your computer use, including browsing. Keyloggers are a form of spyware that capture every keystroke you type; they can send this information to remote servers, where login information--including your passwords--can be extracted and used.

Keyloggers RemoteSpy is one of those spyware examples that's equipped with keylogging capabilities. CyberSpy Software LLC sold this malicious software to organizations and advertisers to enable them to monitor consumers' computers secretly.

Types: Adware: Collects data for targeted advertising. Trojans: Appears as legitimate software but has malicious functions. Tracking Cookies: Records user browsing habits. System Monitors: Capture various system activities and data.

Preventative Measures: • Use reputable anti-spyware software to detect and remove spyware. • Be cautious when clicking on ads or downloading free software. • Regularly update your operating system and software to patch vulnerabilities.

Spywares Types: Adware: Collects data for targeted advertising. Trojans: Appears as legitimate software but has malicious functions. Tracking Cookies: Records user browsing habits. System Monitors: Capture various system activities and data.

Purpose: Spyware can track and collect personal information, browsing habits, and more for various purposes, including marketing, identity theft, and espionage.

Preventative Measures: Use reputable anti-spyware software to detect and remove spyware. Be cautious when clicking on ads or downloading free software. Regularly update your operating system and software to patch vulnerabilities.

Keyloggers vs Spywares Key Differences: Keyloggers focus on capturing keystrokes, while spyware collects a broader range of information, including online activities. Keyloggers can be either hardware or software, while spyware is typically software-based. Keyloggers are often used for identity theft and credential theft, while spyware can be used for a range of purposes, including targeted advertising and espionage.

Overall Security Measures: • Keep your operating system, software, and antivirus programs up to date. • Use strong, unique passwords and enable multi-factor authentication. • Regularly review and monitor your financial and online accounts for any unauthorized activity. • Be cautious when downloading and installing software from untrusted sources. • Educate yourself and practice good online hygiene to protect against malicious software.

1. Malware Attacks •Viruses: Malicious code that attaches itself to legitimate programs and spreads when the infected program is executed. •Worms: Self-replicating programs that spread across networks, often exploiting vulnerabilities to infect other systems. • Trojans: Programs that appear harmless but have malicious functions, such as stealing data or providing unauthorized access.

Virus •A virus is a type of malware that attaches itself to a legitimate program or file and spreads when that program or file is executed. • Viruses often have the ability to replicate and attach to other files, making them self-propagating.

Virus Example •Imagine you download a game from the internet. The game executable file contains a hidden virus. When you run the game, the virus attaches itself to other executable files on your computer, spreading each time you run an infected program.

Worm •A worm is a self-replicating malware that spreads independently, typically through network connections, without needing to attach to other files or programs. •Worms can exploit vulnerabilities in operating systems or applications to infect other computers.

Worm Example: •Let's say you receive an email with an attachment containing a worm. When you open the email, the worm is activated and starts sending copies of itself to all the email addresses in your contact list. Those recipients may also open the infected email and unwittingly spread the worm further

Trojan (Trojan Horse): •A Trojan, short for "Trojan Horse," is malware disguised as legitimate software or files. Unlike viruses and worms, Trojans do not self-replicate but are designed to trick users into executing them. •Trojans often perform harmful actions, such as stealing sensitive information, providing unauthorized access to a system, or damaging data.

Trojan Horse Example •You download what appears to be a legitimate software update from a website. However, it's actually a Trojan disguised as the update. When you run the file, it silently installs malicious software on your computer, allowing remote hackers to gain control over your system or steal your personal information.

In summary … •Virus: Attaches to legitimate files and spreads when those files are executed. •Worm: Self-replicates and spreads independently through network connections without attaching to other files. • Trojan: Disguises itself as legitimate software or files, tricking users into executing it, and then performs harmful actions.

Steganography Steganography is the practice of concealing a message, file, image, or video within another medium in order to hide its existence. Unlike cryptography, which focuses on making the content of a message secret, steganography aims to keep the existence of the message itself a secret. The goal is to embed the information in such a way that it is difficult to detect.

Here are some common techniques used in steganography:

Image Steganography: LSB Substitution: One of the simplest methods involves replacing the least significant bits of the pixels in an image with the hidden data. This alteration is often imperceptible to the human eye.

JPEG Concealing

Notice that every single JPEG file starts and ends with the SOI and EOI markers, respectively. What this means is that any image interpreting application (e.g. Photoshop or GIMP, any internet browser, the standard photo viewing software that comes with your operating system, etc.) looks for these markers inside the file and knows that it should interpret and display whatever comes between them. Everything else is automatically ignored. Hence, you can insert absolutely anything after the EOI marker like this:

Of course, if you put a lot of data after EOI, your file size will increase significantly and might, therefore, arouse suspicion – so you have to be wary of that. In this case, it might be an idea to use a high resolution JPEG file (that naturally has a large file size) to turn attention away from your hidden message.

If you would like to try this steganography technique out yourself, download a hex editor for your machine (if you use Windows, WinHex is a good program), search for FF D9 (which is the hex version of EOI), paste anything you want after this section marker, and save your changes. You will notice that the file is opened like any other JPEG file. The hidden message simply piggybacks on top of the image file. Quite neat!

The Least Significant Bit Technique: This is based on the fact that small changes in pixel colour are invisible to the naked eye.

What about if we were to change the 255 into 254 – i.e. change 11111111 into 11111110? Would we notice the difference in the colour red? Absolutely not. How about changing 11111111 to 11111100 (255 to 252)? We still would not notice the difference – especially if this change is happening to single pixels!

Let’s look at an example. Suppose we want to hide a message like “SOS“. We choose to use the ASCII format to encode our letters. In this format each character has its own binary representation. The binary for our message would be:

What we do now is split each character into two-bit pairs (e.g. S has the following four pairs: 01, 01, 00, 11) and spread these pairs successively along multiple pixels. So, if our image had four pixels, our message would be encoded like this:

Grayscale Modification: Another approach is to subtly modify the intensity of pixels in grayscale images.

Audio Steganography: Similar to image steganography, audio files can be manipulated by modifying the least significant bits or by using other frequency domain techniques to hide information.

Text Steganography: Concealing information within a text document without altering the apparent text. This can be achieved by, for example, using invisible ink or by hiding information in the formatting of the text.

Video Steganography: Concealing data within video files, often by subtly altering the frames or other components.

Network Steganography: Embedding information in network protocols, such as within the headers of packets, to avoid detection.

File Steganography: Hiding data within other types of files, like compressing files or embedding one file within another.

The primary challenge in steganography is to ensure that the alterations made to the carrier medium are subtle enough to avoid detection, yet robust enough to withstand various attacks and transformations that the carrier medium might undergo. Detection of steganography often involves statistical analysis and pattern recognition techniques to identify irregularities or anomalies in the carrier medium.

It's important to note that while steganography can be used for legitimate purposes (such as digital watermarking or embedding metadata), it can also be misused for malicious activities, such as hiding malware or covert communication in a network. As a result, there are ongoing efforts to develop techniques for detecting and preventing the use of steganography for malicious purposes.

Denial of Service (DoS) Attacks •Distributed Denial of Service (DDoS): Attackers use multiple compromised systems to flood a target system or network, making it unavailable to users. •Ping Flood: Overwhelming a target with a high volume of Internet Control Message Protocol (ICMP) ping requests.

DDoS Attack History. •One of the earliest known instances of a DDoS attack occurred in 1996 when a computer science student named Michael Calce, who went by the online pseudonym "Mafiaboy," launched a series of DDoS attacks against high-profile websites.

The Mafiaboy Attack (February 2000): • The most notable DDoS attack associated with Michael Calce occurred on February 7, 2000, when he orchestrated a series of attacks against several major websites, including Yahoo!, CNN, Amazon, and eBay. • Calce used a network of compromised computers, known as a "botnet," to flood these websites with a massive volume of traffic, overwhelming their servers and causing extended downtime.

• The attack received significant media attention and exposed the vulnerabilities of major internet companies to such attacks. • Michael Calce was eventually apprehended and convicted of multiple cybercrimes. He received a relatively lenient sentence given his age (he was a teenager at the time of the attacks) but became a cautionary tale about the potential consequences of cyber attacks.

DDoS Attack •The term "DDoS" stands for Distributed Denial of Service attack. It's a type of cyberattack where multiple compromised computers, often referred to as a botnet, are used to flood a target system with a massive amount of traffic, overwhelming its capacity to respond to legitimate requests. This results in a disruption of service, making the targeted system or website unavailable to its users.

1. The Target: • In our story, the target is a popular e-commerce website that relies on its online presence for revenue.

2. Attack Preparation: • The attackers, often individuals or groups with malicious intent, identify the target website and decide to launch a DDoS attack against it. • They assemble a botnet, a network of compromised computers and devices, which may include infected servers, IoT devices, and even personal computers.

3. Launching the Attack: • The attackers initiate the attack by sending a massive volume of traffic to the target website simultaneously. • This traffic can be in the form of HTTP requests, UDP or TCP packets, or any other data that can flood the target's network and web servers.

4. Overwhelming the Target: • The sheer volume of traffic generated by the botnet overwhelms the target's network infrastructure and web servers. • Legitimate users trying to access the website experience slow loading times or complete unavailability.

5. Loss and Impact: • The impact of a successful DDoS attack can be severe. The target website experiences downtime, leading to financial losses due to lost sales and damage to its reputation. • The organization may also incur costs related to mitigating the attack and improving its defenses.

6. Mitigation and Recovery: • In response to the attack, the target organization may employ various mitigation techniques to filter out malicious traffic and allow legitimate traffic to pass. • Common mitigation strategies include deploying specialized DDoS protection services, using content delivery networks (CDNs), and adjusting firewall rules. • Recovery involves restoring normal operations once the attack subsides.

• CDNs are networks of distributed servers that work together to deliver web content to users based on their geographic location. They cache content and distribute it across multiple servers, reducing the load on any single server. • Purpose: CDNs can help mitigate DDoS attacks by distributing traffic across multiple servers, making it more challenging for attackers to overwhelm a single point of entry.

• Firewalls are network security systems that control and monitor incoming and outgoing network traffic based on predetermined security rules. Adjusting firewall rules involves configuring settings to better protect against DDoS attacks. • Purpose: By adjusting firewall rules, organizations can implement measures to filter out potentially malicious traffic and prevent it from reaching the target network or service.

7. Ongoing Protection: • After the attack, the organization takes steps to improve its security posture, which may include enhancing its network infrastructure, implementing better security practices, and monitoring for future attacks. • It might also engage with DDoS protection services to help defend against future threats.

8. Attribution and Reporting: • In some cases, organizations or law enforcement agencies attempt to trace the source of the attack and identify the attackers for legal action.

9. Lessons Learned: • Organizations affected by DDoS attacks often learn valuable lessons about their vulnerabilities and the importance of cybersecurity. They may revise their incident response plans and security policies accordingly.

10. Continuing Threat: • DDoS attacks remain an ongoing threat, with attackers continually evolving their tactics and techniques. Organizations must stay vigilant and invest in security measures to protect against future attacks.

DDoS Attack: Prevention Summary •To protect against DDoS attacks, organizations typically invest in dedicated DDoS mitigation services, deploy intrusion detection systems, implement web application firewalls, and maintain incident response plans. They may also use rate limiting, traffic shaping, and content delivery networks to help absorb and mitigate attack traffic. Regular monitoring and analysis of network traffic can help identify unusual patterns and potential attacks before they cause significant harm.

SQL Injection SQL Injection is a type of cyber attack that targets the vulnerabilities in an application's database layer. It occurs when an attacker inserts or manipulates malicious SQL code into input fields, with the aim of executing unauthorized SQL queries.

SELECT \* FROM users WHERE username = '' AND password = '';

A vulnerable implementation might directly insert user inputs into the SQL query without proper validation and sanitation. "SELECT \* FROM users WHERE username = '" + input\_username + "' AND password = '" + input\_password + "';"

If an attacker inputs something like ' OR '1'='1' – , the SQL query becomes: SELECT \* FROM users WHERE username = '' OR '1'='1' --' AND password = '';

This manipulated query always evaluates to true ('1'='1' is always true), allowing the attacker to bypass authentication.