CSF3404 Cyber Security

Chapter 2
Identifying Security Threats and Vulnerabilities

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

Lesson Objectives

In this lesson, you will identify security threats and vulnerabilities:

- ✓ Identify social engineering attacks.
- ✓ Identify various malware threats.
- ✓ Identify software-based threats.
- ✓ Identify network-based threats.
- ✓ Identify wireless threats and vulnerabilities.
- ✓ Identify physical threats and vulnerabilities.

Introduction

UMT
We lead

Security is an ongoing process that includes;

- ✓ Setting up organizational security systems,
- ✓ Hardening them,
- ✓ Monitoring them,
- ✓ Responding to attacks in progress, **and**
- ✓ Deterring attackers.

As **a security professional**, you will be involved in all phases of that process.

So, you need to understand the **threats** and **vulnerabilities** you will be protecting your systems against.

Social Engineering

- Thinking of attacks on information systems may be limited only to the protection of the technological components of those systems, and this is not true.

- **People** or the **system users**; are as much a part of an information system as the technological components; they have their own **vulnerabilities**, and they can be the first part of the system to surrender to certain types of **attacks**.

- Here, you will learn to identify **social engineering attacks - threats** against the **human factors** in your technology environment.

- The **attackers** know that people in the system may be the **best target** for attack.

- If you want to protect your **infrastructure**, **systems**, and **data**;
  - ✓ You need to be able to recognize this kind of attack when it happens.

Social Engineering Attacks

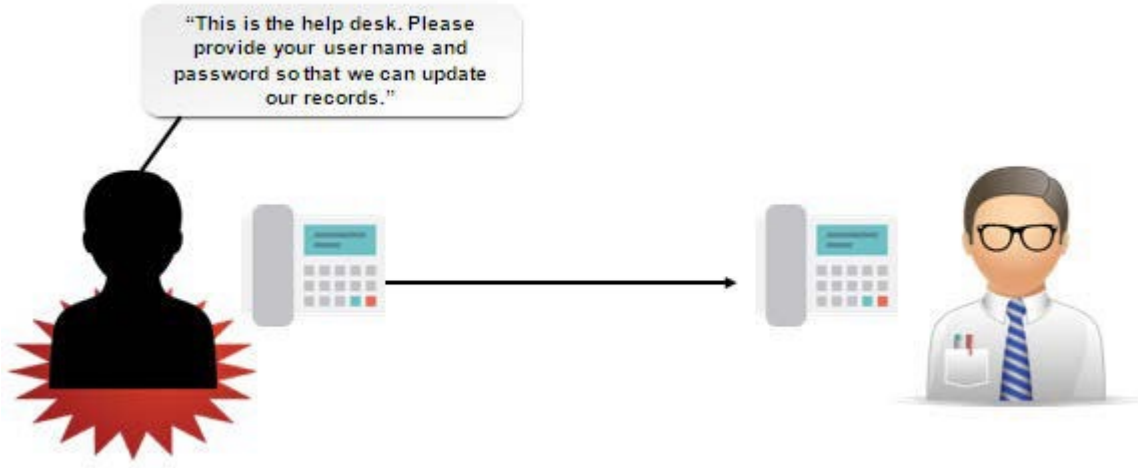
A **social engineering attack** is a type of attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines.

Social engineering is often a precursor to another type of attack.

✓ Because these attacks depend on **human factors** rather than on **technology**, their symptoms can be **vague** and **hard** to identify.

Social engineering attacks can come in a variety of methods:

- In person
- Through email
- Over the phone.



Social Engineering Effectiveness

UMT
We lead

- Very common and successful attack.
- Exploits human trust and inexperienced users.
- May pose as an authority figure or friend.
- Users may drop their guard when a request seems urgent or temporary.
- Users may rely too much on groupthink.
- More digital information means more danger.
- Organizations struggle to strengthen the human element.
- The weakest human link can compromise an entire system.
- All systems are vulnerable to deception and manipulation.

Types of Social Engineering

- Spoofing
- Impersonation
- Hoax
- Phishing
- Vishing
- Whaling
- URL Hijacking/Typo Squatting
- Spam and Spim
- Shoulder surfing
- Dumpster diving
- Tailgating

Types of Social Engineering

- **Spoofing:**
  - This is a **human-based** or **software-based attack** where the goal is to pretend to be someone else for the purpose of identity concealment.
  - Spoofing can occur in;
    - ✓ Internet Protocol (**IP**) addresses.
    - ✓ Network adapter hardware (Media Access Control (**MAC**)) addresses.
    - ✓ Email.
  - If employed in email, various email message headers are changed to conceal the originator's identity.

Types of Social Engineering

- **Impersonation:**
  - This is a **human-based attack** where an attacker pretends to be someone they are not.

  - **A common scenario is**;
    - When the attacker calls an employee and pretends to be calling from the help desk.
    - The attacker tells the employee he is reprogramming the order-entry database.
    - He needs the employee's user name and password to make sure it gets entered into the new system.
  - Impersonation is often successful in situations where identity cannot be easily established.

Types of Social Engineering

- **Hoax:**
  - This is an **email-based** or **web-based attack** that is intended to trick the user into performing undesired actions.

  - **Such as;**
    - ✓ Deleting important system files in an attempt to remove a virus.
    - ✓ A scam to convince users to give up important information or money for an interesting offer.

Types of Social Engineering

- **Phishing:**
  - This is a common type of **email-based social engineering attack**.
    - ✓ The attacker sends an email that seems to come from a respected bank or other financial institution.
    - ✓ The email claims that the recipient needs to provide an account number, Social Security number, or other private information to the sender in order to "verify an account".
    - ✓ The phishing attack often claims that the account verification" is necessary for security reasons.

  - When attackers target a specific individual or institution, this social engineering technique is known as spear phishing.
  - An attack similar to phishing, called **pharming**.
    - ✓ This can be done by redirecting a request for a website, typically an e-commerce site, to a similar-looking, but fake, website.

Types of Social Engineering

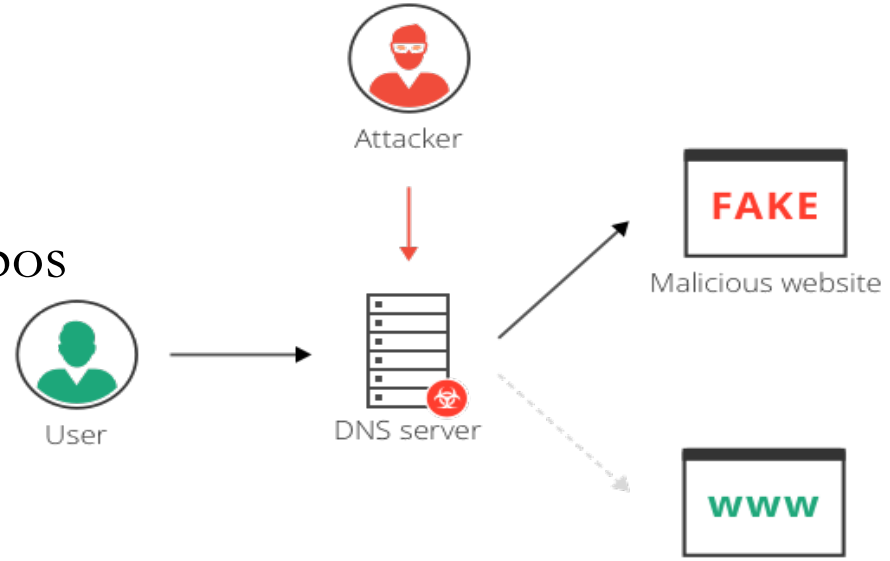
- **Vishing:**
  - This is a **human-based attack** where the goal is to extract
    - ✓ Personal
    - ✓ Financial
    - ✓ Confidential information from the victim by using services;
      - Such as:
        - ✓ Telephone system.
        - ✓ IP-based voice messaging services (Voice over Internet Pro VoIP) as the communication medium.
  - This is also called **voice phishing**.

Types of Social Engineering

- **Whaling:**
  - This is a form of spear phishing that targets individuals or organizations that are known to possess a good deal of wealth.
  - Whaling targets individuals who work in financial institutions whose salaries are expected to be high.
  - Exploiting the weakest link can result in a huge payoff for the attacker(s).

Types of Social Engineering

- **URL Hijacking:**
  - It is called typo squatting.
  - This is the tactic of exploiting typos that users sometimes make when entering a URL into a browser.



  - For example;
    - Aa malicious user might register a domain with the URL **www.compia.org**, which has a minor typo compared to the correct **www.comptia.org**.

  - A user who makes this mistake when entering the URL into their browser will be directed to the attacker's site.

  - Which may mimic the real website or contain malicious software that will infect the victim's computer.

Types of Social Engineering

- **Spam and Spim:**
  - Spam is an **email-based threat** where the user's inbox is flooded with emails which act as vehicles that carry advertising material for products or promotions for get-rich-quick schemes and can sometimes deliver viruses or wavure.

  - Spam can also be utilized within social networking sites such as Facebook and Twitter.

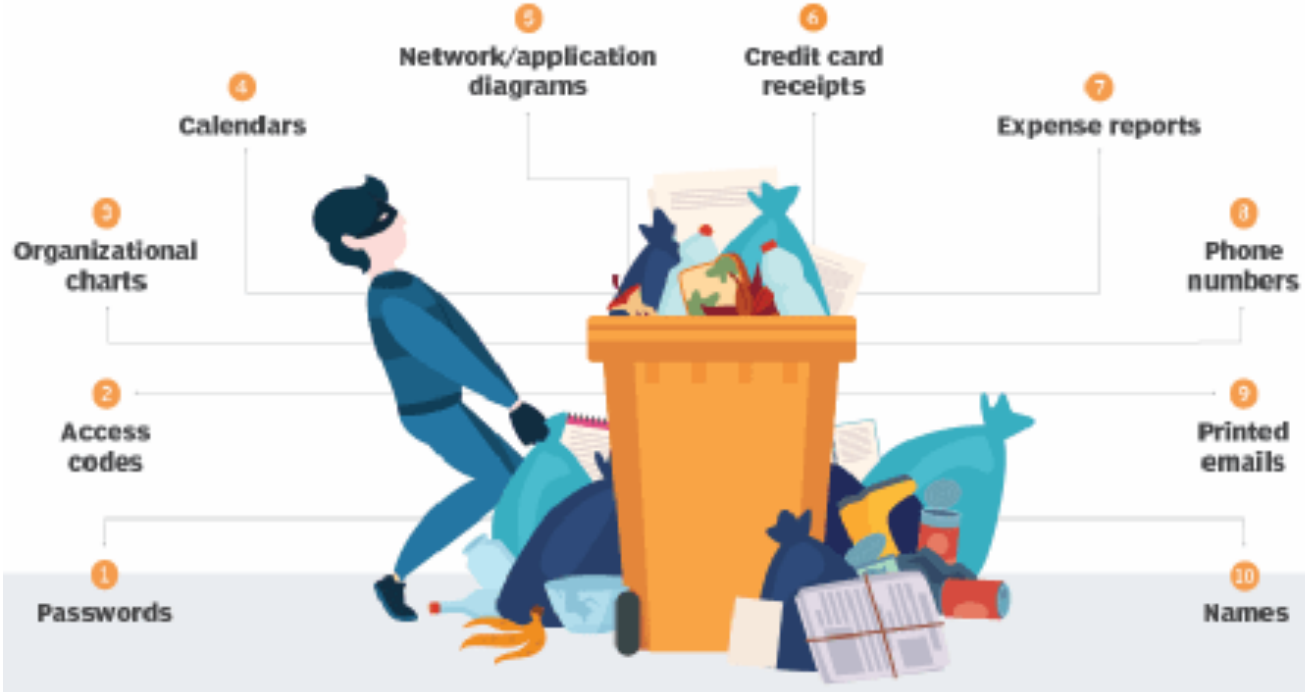
  - Spim is an attack similar to spam that is propagated through instant wwwssaging (IM) instead of through email.

Types of Social Engineering

- **Shoulder Surfing:**
  - This is an attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN.
  - This is very easy to do today with camera-equipped mobile phones.

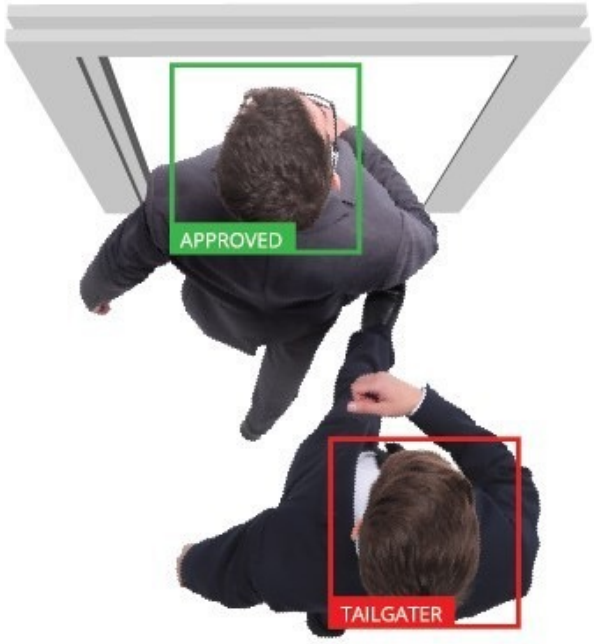
Types of Social Engineering

- **Dumpster Diving:**
  - This is an attack where the goal is to reclaim important information by inspecting the contents of trash containers.
  - This is especially effective in the first few weeks of the year as users discard old calendars with passwords written in them.



Types of Social Engineering

- **Tailgating:**
  - It is known as piggy backing.
  - This is a **human-based attack** where the attacker will slip in through a secure area following a legitimate employee.
  - The only way to prevent this type of attack is by installing a **good access control mechanism** and **to educate users** not to admit unauthorized personnel.



Malware

- One of the most prevalent threats to computers today is malicious code.

- Malware is insidious and difficult to remove, so it can cause a significant amount of damage in many different ways.

- Malware is not a monolithic threat, but rather a collection of different methods that can exploit the vulnerabilities in your information security.

- By identifying the various types of malware and how they operate;
  - ✓ You will be better prepared to fight their infection, or better yet, prevent them from infecting your systems in the first place.

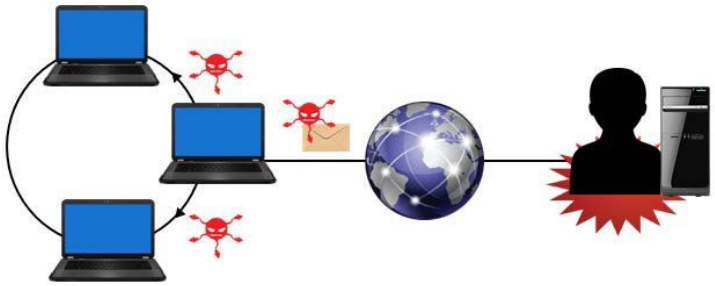
  - ✓ As a security professional, or even as a regular computer user, you will likely have experience in dealing with unwanted software infecting your systems.

Malicious Code Attacks

- A malicious code attack is a type of software attack where an attacker inserts some type of undesired or unauthorized software, or malware, into a target system.

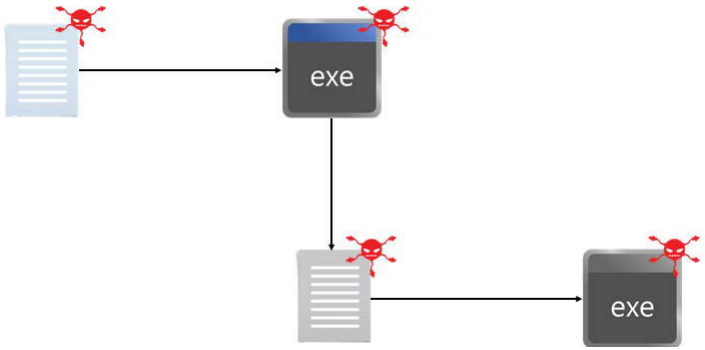
- In the past, many malicious code attacks were intended to disrupt or disable an operating system or an application, or force the target system to disrupt or disable other systems.

- More recent malicious code attacks attempt to remain hidden on the target system, utilizing available resources to the attacker's advantage.
-
- Potential uses of malicious code include;
  - Launching Denial of Service attacks on other systems;
  - Hosting illicit or illegal data;
  - Skimming personal or business information for the purposes of
    - Identity theft
    - Profit
    - Extortion
    - Displaying unsolicited advertisements.



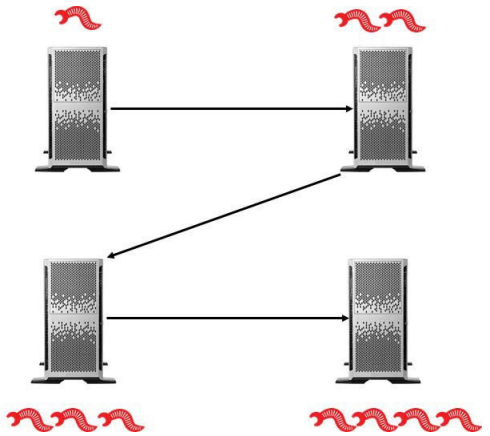
Viruses

- A **virus** is a piece of code that spreads from one computer to another by attaching itself to other files through a process of self-replication.
- The code in a virus executes when the file it is attached to is opened.
- Viruses are intended to enable further attacks, send data back to the attacker, or even corrupt or destroy data.
- Because of their **self-replicating nature**;
  - ✓ Viruses are difficult to completely remove from a system.
  - ✓ It causes billions of dollars in damages every year.



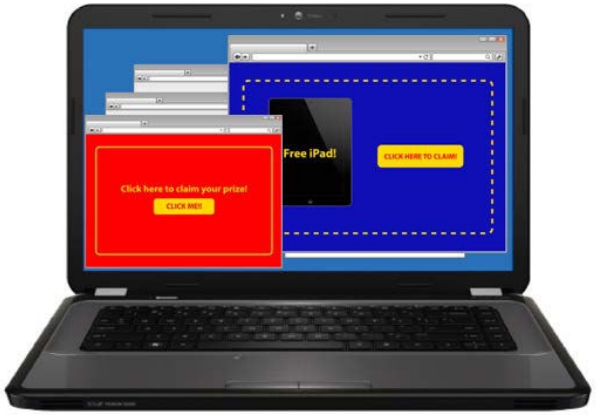
Worms

- A worm is malware that, like a virus, replicates itself across the infected system.
- Unlike a virus, it does not attach itself to other programs or files.
- Viruses tend to interfere with the functions of a specific machine. While, Worms are often intended to interrupt network capabilities.



Adware

- Adware is software that automatically displays or downloads unsolicited advertisements when it is used.
- Adware often appears on a user's computer as a browser pop-up.
- While not all adware is overtly malicious, many adware programs have been associated with spyware and other types of malicious software.
- It can reduce user productivity by slowing down systems and simply by being an annoyance.

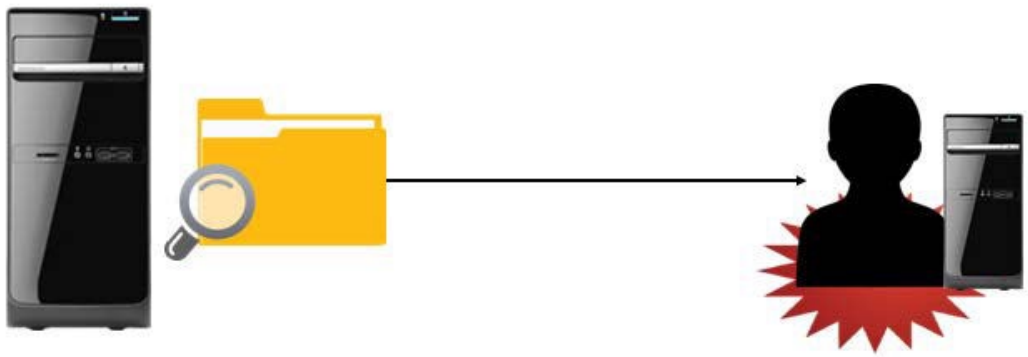


Spyware

- Spyware is surreptitiously installed malicious software that is intended to track and report the usage of a target system or collect other data the author wishes to obtain.

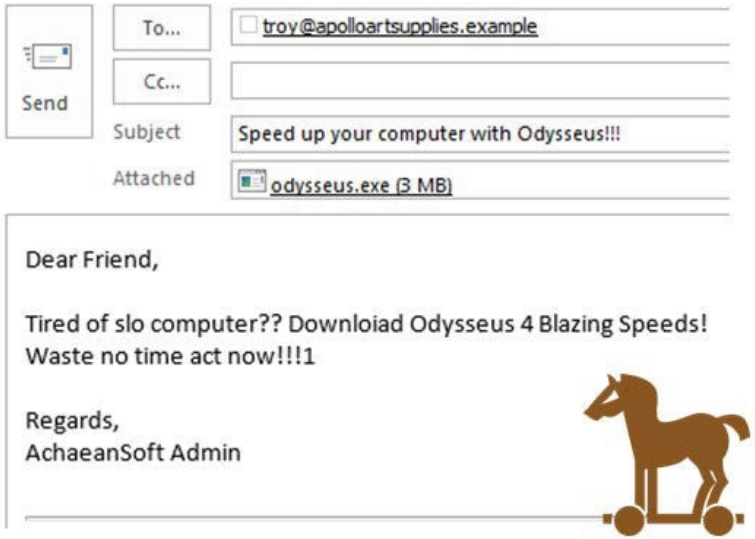
- Data collected can include web browsing history, personal information, banking and other financial information, and user names and passwords.

- Although it can infect a computer through social engineering tactics, some spyware is included with otherwise legitimate software.



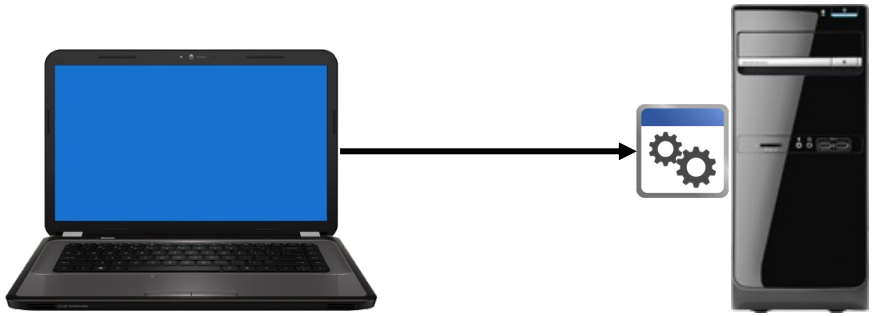
Trojan Horses

- A Trojan Horse, often simply called a Trojan.
- It is hidden malware that causes damage to a system or gives an attacker a platform for monitoring and/or controlling a system.
- Unlike viruses, Trojans do not replicate themselves, nor do they attach to other files.



Rootkits

- A rootkit is a code that is intended to take full or partial control of a system at the lowest levels.
- Rootkits often attempt to hide themselves from monitoring or detection and modify low-level system files when integrating themselves into a system.
- Rootkits can be used for non-malicious purposes such as virtualization.
- Most rootkit infections install backdoors, spyware, or other malicious code once they have control of the target system.



Logic Bombs

- A **logic bomb** is a piece of code that sits dormant on a target computer until it is triggered by a specific event, such as a specific date.

- Once the code is triggered, the logic bomb detonates, and performs whatever actions it was programmed to do.

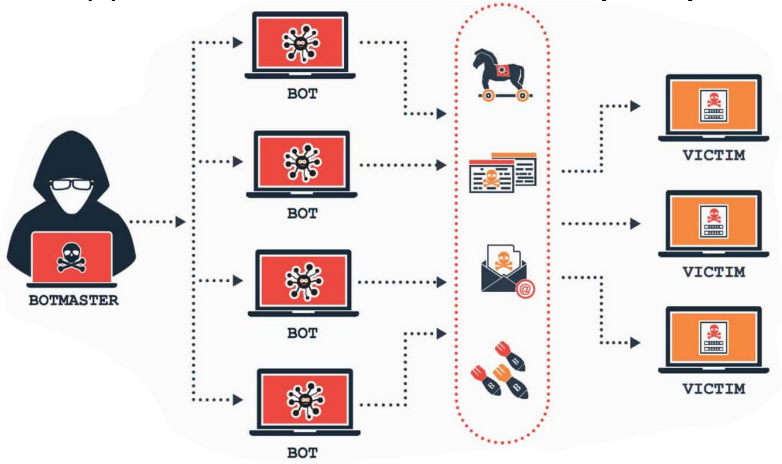
- This includes erasing and corrupting data on the target system

Botnet

- A botnet is a set of computers that have been infected by a control program called a bot that enables attackers to collectively exploit those computers to mount attacks.

- Typically, black hats use botnets to coordinate denial of service attacks, send spam emails, and mine for personal information or passwords.

- Users of these infected machines called zombies or drones are often unaware that their computers are being used for nefarious purposes.

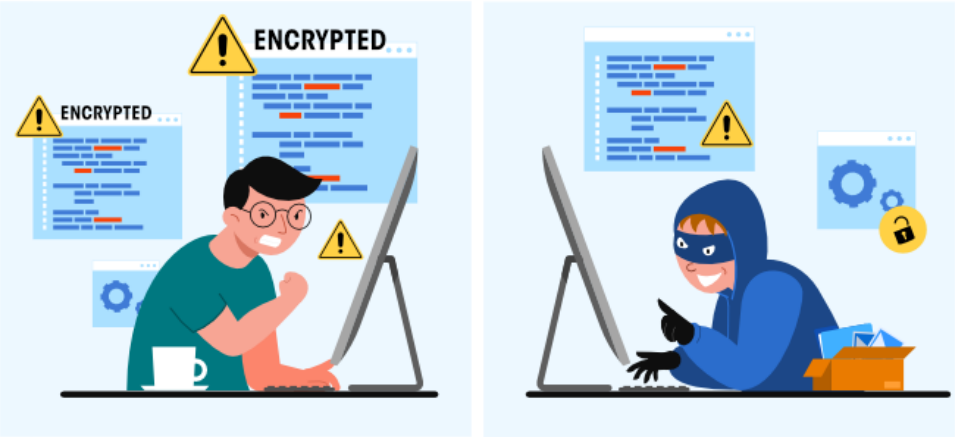


Ransomware

- It is an increasingly popular variety of malware in which an attacker infects a victim's computer with code that restricts the victim's access to their computer or the data on it.

- Then, the attacker demands a ransom be paid, under threat of keeping the restriction or destroying the information they have locked down.

- Ransomware is most damaging when it exploits the power of encryption to essentially render data that isn't backed up worthless, which makes victims more likely to pay the ransom to get their files unencrypted.

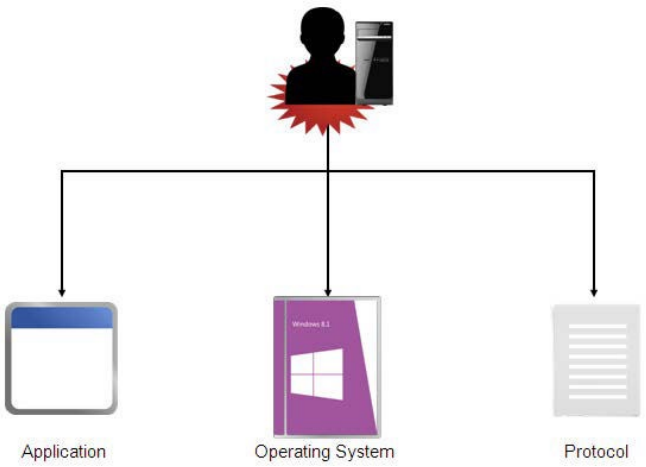


Software Attacks

- It is any attack against software resources, including operating systems, applications, protocols, and files.

- The goal of a software attack is to disrupt or disable the software running on the target system, or to somehow exploit the target system to gain access to the target system, to other systems, or to a network.

- Many software attacks are designed to surreptitiously gain control of a computer so that the attacker can use that computer in the future, often for profit or further malicious activity.



Password Attacks

- It is any type of attack in which the attacker attempts to obtain and make use of passwords illegitimately.
- The attacker can guess or steal passwords, or crack encrypted password files.
- A password attack can show up in audit logs as repeatedly failed logons and then a successful logon, or as several successful logon attempts at unusual times or locations.
  - Protecting Password Databases
  - Attackers know the storage locations of encrypted passwords on common systems, such as the Security Accounts Manager (SAM) database on standalone Windows systems.
  - Password-cracking tools take advantage of known weaknesses in the security of these password databases, so security might need to be increased.

Types of Password Attacks

- Guessing
- Stealing
- Dictionary attack
- Brute force attack
- Rainbow tables
- Hybrid password attack
- Birthday attack

Types of Password Attacks

- Guessing:
  - The simplest type of password attack is making individual, repeated attempts to guess a password by entering different common password values, such as the user's name, spouse's name, or a significant date.
  - Most systems have a feature that will lock out an account after a specified number of incorrect password attempts.
- Stealing:
  - Passwords can be stolen by various means, including sniffing network communications, reading handwritten password notes, or observing a user in the act of entering a password.
- Dictionary attack:
  - This attack type automates password guessing by comparing passwords against a predetermined list of possible password values, like words in a dictionary.
  - Dictionary attacks are only successful against fairly simple and obvious passwords.
    - Because they rely on a dictionary of common words and predictable variations, such as adding a single digit to the end of a word.

Types of Password Attacks

- Brute force attack:
  - The attacker uses **password-cracking software** to attempt every possible alphanumeric password combination.
  - Brute force attacks are heavily constrained by time and computing resources, and are therefore most effective at cracking **short passwords**.
  - Brute force attacks that are distributed across multiple hardware components, like a cluster of high-end graphics cards, can be very successful at cracking longer passwords.
- Rainbow tables:
  - These are sets of related plaintext passwords and their hashes.
  - The underlying principle of rainbow tables is to do the central processing unit (CPU)-intensive work of generating hashes in advance, trading time saved during the attack for the disk space to store the tables.
    - Beginning with a base word such as "password" the table then progresses through a large number of possible variations on that root word, such as "password" or "p@ssword."
  - Rainbow table attacks are executed by comparing the target password hash to the password hashes stored in the tables, then working backward in an attempt to determine the actual password from the known hash.

Types of Password Attacks

- Hybrid password attack:
  - This attack type utilizes **multiple attack methods**;
  - Including dictionary, rainbow table, and brute force attacks when trying to crack a password.
- Birthday attack:
  - This attack type exploits weaknesses in the mathematical algorithms used to generate hashes.
  - This type of attack takes advantage of the probability of different inputs producing the same encrypted outputs, given a large enough set of inputs.
  - It is named after the surprising statistical fact that there is a 50 percent chance that two people in a group of 23 will share a birthday.

Password-Cracking Utilities

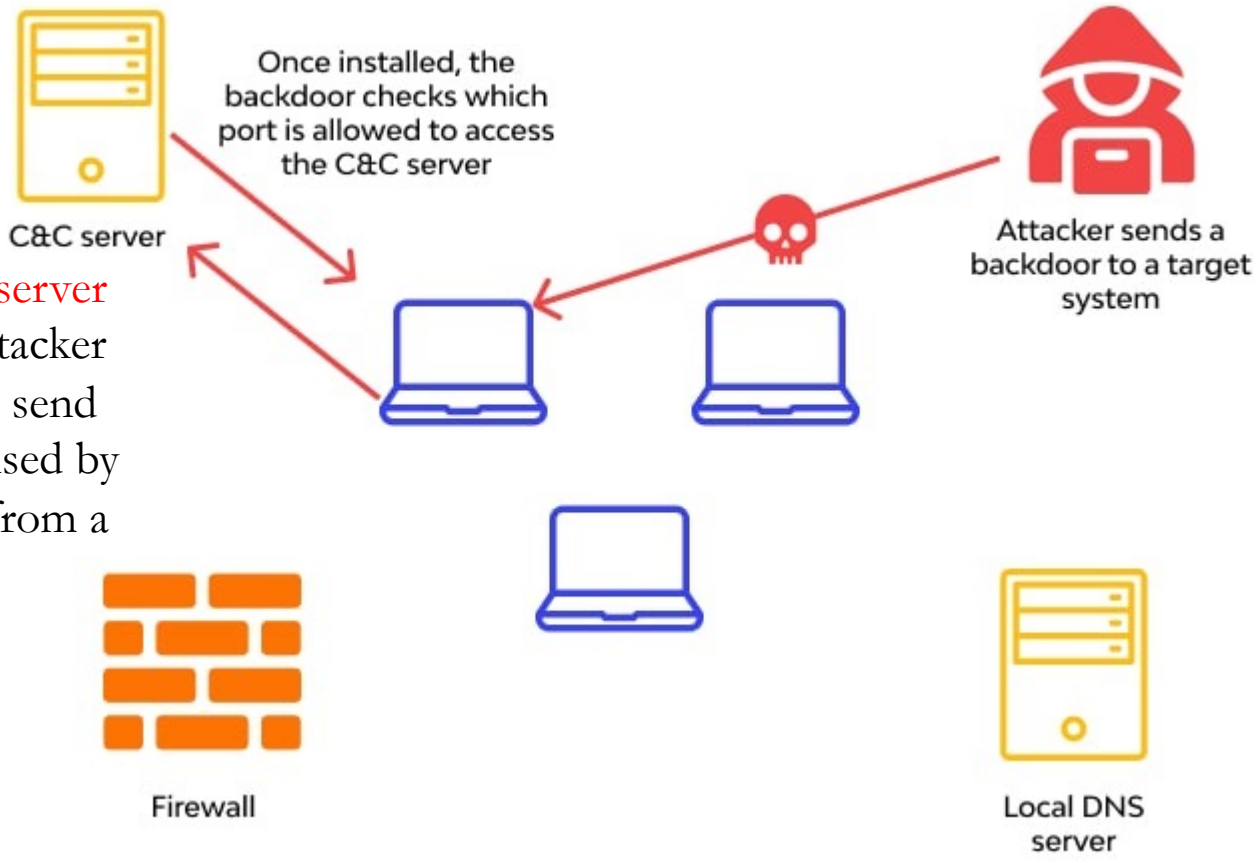
- Commonly available password-cracking utilities include:
  - Ophcrack.
  - LOphtCrack.
  - John the Ripper.
  - Cain & Abel.
  - THC Hydra.
  - RainbowCrack.
  - Aircrack.
  - Airsnort.
  - Pwdump.
  - KerbCrack.
  - Brutus.

Backdoor Attacks

- A backdoor attack is a type of **software attack** where an attacker creates a software mechanism called a back door to gain access to a computer.
- The backdoor can be a software utility or an illegitimate user account.
- A backdoor is delivered through use of a Trojan horse or other malware.
- Backdoor software typically listens for commands from the attacker on an open port.
- The backdoor mechanism often survives even after the initial intrusion has been discovered and resolved.
- Backdoor attacks can be difficult to spot because they may not leave any obvious evidence behind.

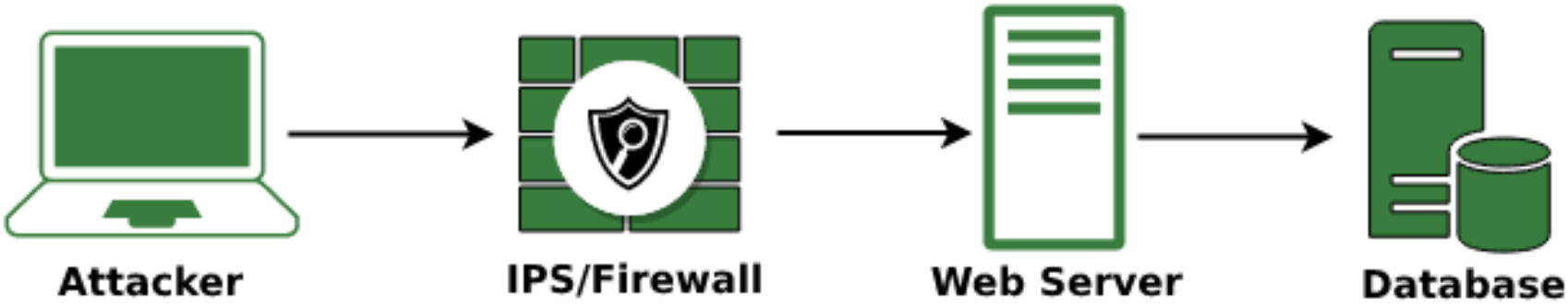
Backdoor Attacks

A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.



Application Attacks

- Application attacks are software attacks that are targeted at web-based and other client-server applications.
- They can threaten application and web servers, users, other back-end systems, and the application code itself.
- These attacks can lead to an authentication breach, customer impersonation, information disclosure, source code disclosure or tampering, and further network breaches.
- Application attacks that specifically exploit the trust between a user and a server are called client-side attacks.



Types of Application Attacks

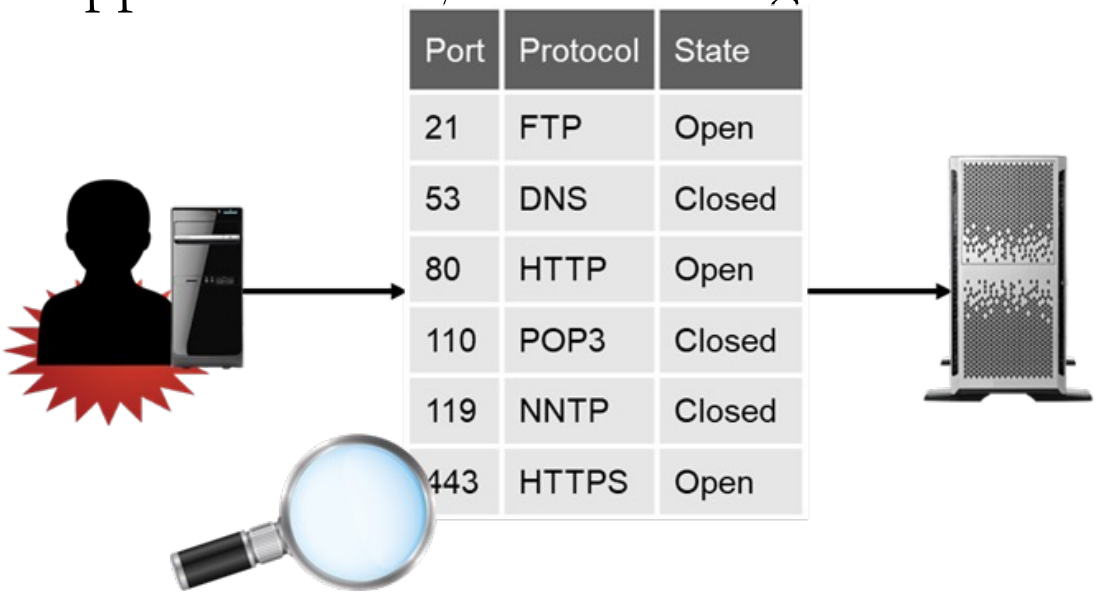
Application Attack	Description
Cross-site scripting (XSS)	An attack that injects malicious scripts into trusted websites to be run when a user visits the site.
Command injection attacks	Command injection attacks include several types: ✓ SQL injection ✓ LDAP injection ✓ XML injection ✓ Directory traversal
Zero day exploit	An attack that occurs when the security level of a system is at its lowest, immediately after the discovery of a vulnerability.
Cookies manipulation	An attack where an attacker injects a meta tag in an HTTP header, making it possible to modify a cookie stored in a browser.
LSO attack	An attack where a website running Flash stores data objects (Flash cookies) on a user's computer that are difficult to detect and remove, and may threaten the user's privacy.
Attachment attack	An attack where the attacker can merge malicious software or code into a downloadable file or attachment on a web server so that users download and execute it on client systems.

Types of Application Attacks

Application Attack	Description
Malicious add-ons	An add-on that is meant to look like a normal add-on, except that when a user installs it, malicious content will be injected to target the security loopholes that are present in a web browser.
Header manipulation	An attack where the attacker manipulates the header information passed between the web servers and clients in HTTP requests.
Buffer overflow	An attack in which data goes past the boundary of the destination buffer and begins to corrupt adjacent memory, which may cause an app to crash or rogue code to execute on a system.
Integer overflow	An attack in which a computed result is too large to fit in its assigned storage space, which may lead to crashing or data corruption, and may trigger a buffer overflow.
Arbitrary code execution	An attack that exploits application vulnerabilities by allowing an attacker to execute any command on a victim's machine, potentially taking complete control over a system.

Port Scanning Attacks

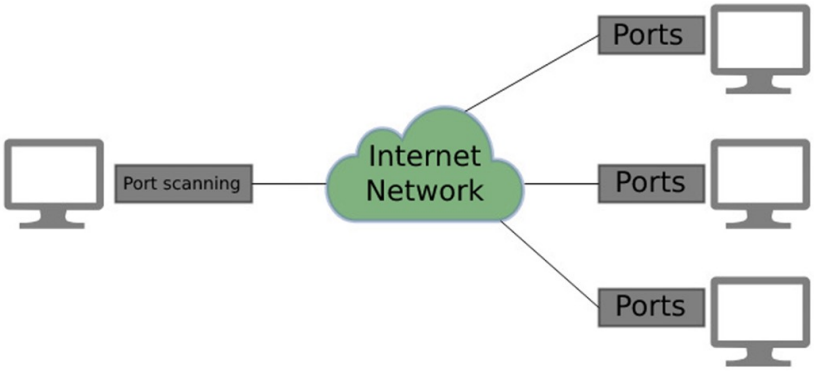
- A port scanning attack is a type of network attack where a potential attacker scans the **computers** and **devices** that are connected to the **Internet** or other **networks** to see which TCP and UDP ports are listening and which services on the system are active.
- Port scans can be easily automated.
  - Any system on the Internet will be scanned almost constantly.
- Some monitoring software can detect port scans.
  - Might happen without your knowledge.



Port	Protocol	State
21	FTP	Open
53	DNS	Closed
80	HTTP	Open
110	POP3	Closed
119	NNTP	Closed
443	HTTPS	Open

Port Scanning Utilities

- There are many utilities available that potential attackers can use to scan ports on networks, including:
  - ✓ Nmap.
  - ✓ SuperScan.
  - ✓ Strobe.
  - ✓ Any Telnet client.



Ping Scan	The simplest scan, a ping scan looks for any ICMP replies indicating if a target is alive.
TCP Half Open	A fast and common scan that requests an ACK packet from a computer. Also called a SYN scan.
TCP Connect	Similar to the TCP Half Open scan, but the TCP Connect scan completes the TCP connection.
UDP	Slower than a TCP scan, a UDP scan works best when you send a specific payload to a target, such as a DNS request.
Stealth Scanning	Quiet and unobvious, stealth scanning is commonly used by hackers for this reason.

- Many utilities can be downloaded for free.

Eavesdropping Attacks

- An eavesdropping attack or sniffing attack uses special monitoring software to gain access to private network communications, either to steal the content of the communication itself or to obtain user names and passwords for future software attacks.

- Attackers can eavesdrop on both wired and wireless network communications.

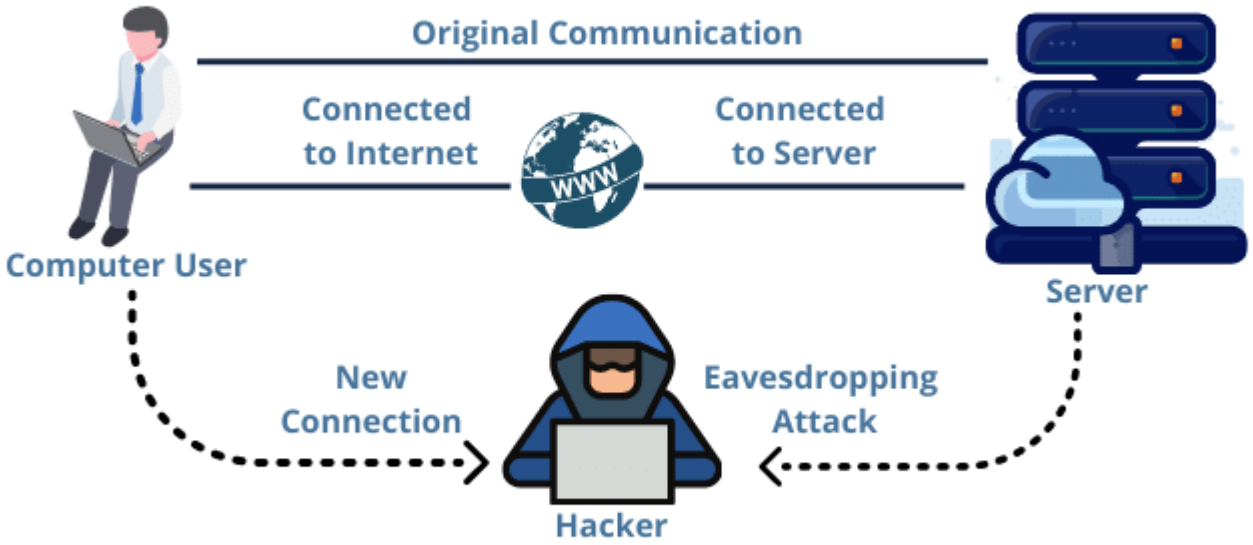
  - ✓ On a wired network, the attacker must have physical access to the network or tap into the network cable.

  - ✓ On a wireless network, an attacker needs a device capable of receiving signals from the wireless network.

- Eavesdropping is very hard to detect, unless you spot an unknown computer leasing an IP address from a DHCP server.

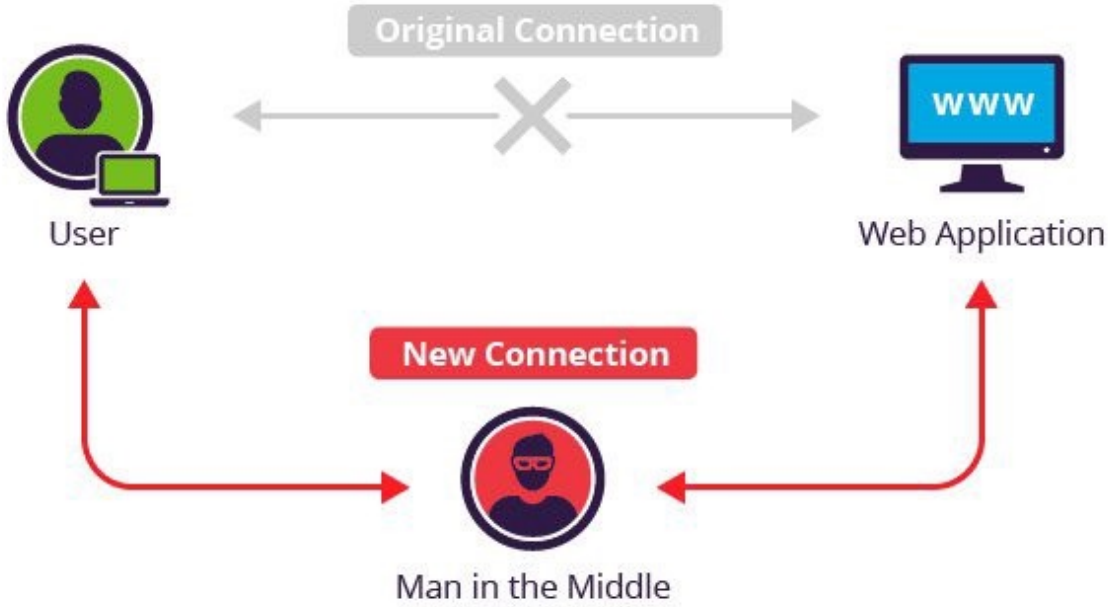
Eavesdropping Utilities

- Many utilities are available that will monitor and capture network traffic.
- Some of these tools can only sniff the traffic that is sent to or received by the computer on which they are installed.
- Other tools are capable of scaling up to scan very large corporate networks.
  - Examples of these tools include:
  - Wireshark.
  - Microsoft Network Monitor Capture.
  - Tcpdump.
  - Dsniff.



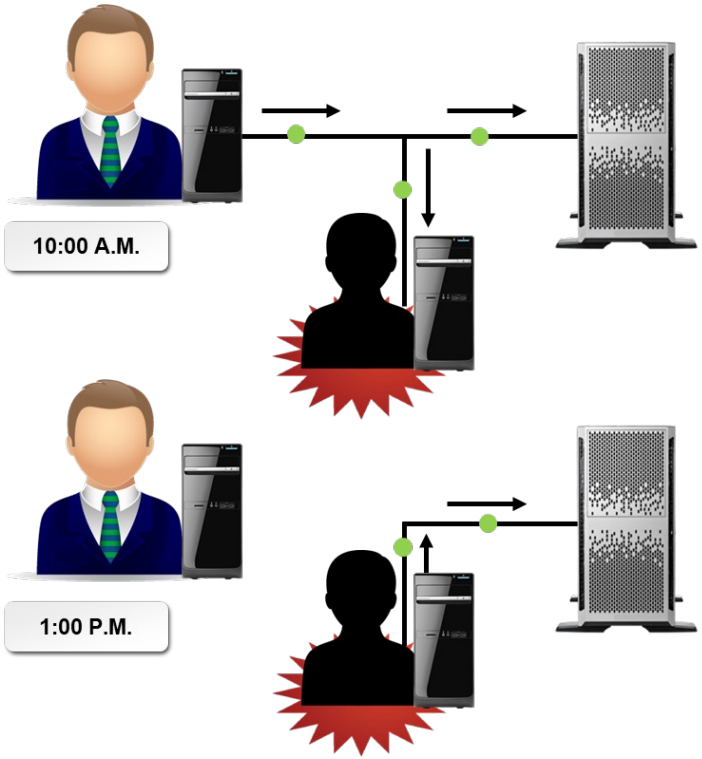
Man-in-the-Middle Attacks

- A man-in-the-middle attacks is a form of eavesdropping where the attacker makes an independent connection between two victims (two clients or a client and a server).
- The man-in-the-middle attacker relays information between the two victims as if they are directly talking to each other over a closed connection.
  - ✓ The attacker is controlling the information that travels between the two victims.
- During the process, the attacker can view or steal information to use it fraudulently.



Replay Attacks

- A replay attack is a network attack where an attacker captures network traffic and stores it for retransmitting at a later time to gain unauthorized access to a specific host or a network.
- This attack is particularly successful when an attacker captures packets that contain user names, passwords, or other authentication data. In most cases, replay attacks are never discovered.



Social Network Attacks

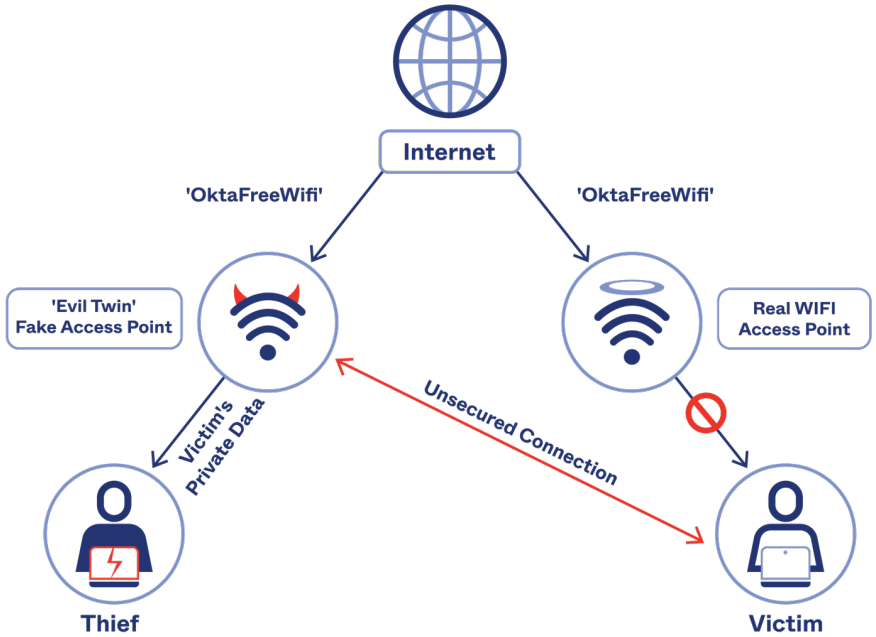
- Social network attacks are attacks that are aimed at social networking sites such as Facebook, Twitter, and LinkedIn.
  - Because these types of websites have become incredibly popular both for personal and professional use.

- They have become bigger targets for a variety of threats to security.

- The more common attacks launched against social networks and their users are:
  - ✓ Evil twin attack/account phishing
  - ✓ Drive-by download
  - ✓ Clickjacking
  - ✓ Password stealer
  - ✓ Spamming

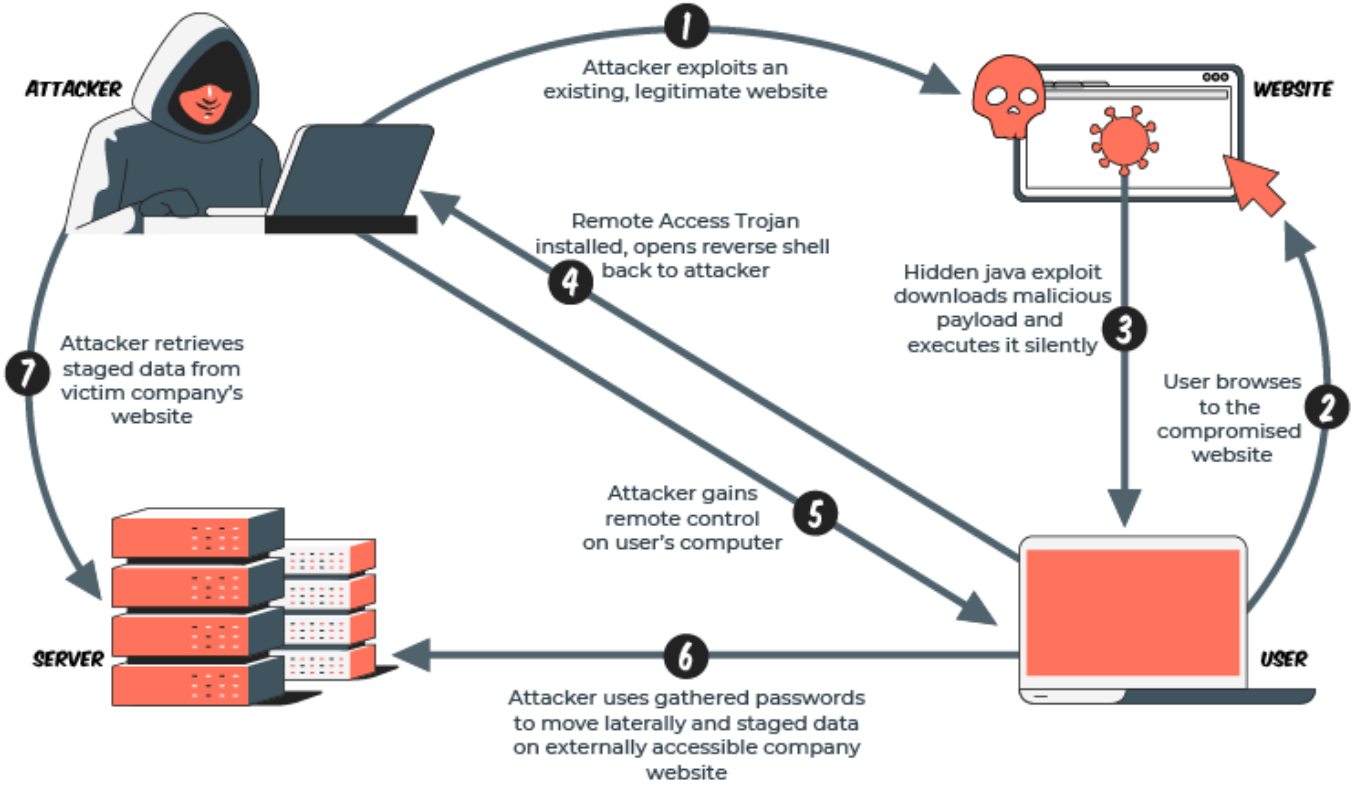
Evil Twin Attack & Account Phishing

- It is an attack where an attacker creates a social network account to impersonate a genuine user.
  - ✓ When the friends of that user allow the attacker to become friends with them or join a group, the attacker can gain access to various personal details and even company information if a company has a page on the site.
- This is often preceded by account phishing, in which an attacker creates an account and joins the friends list of an individual just to try to obtain information about the individual and their circle of friends or colleagues.



Drive-by Download

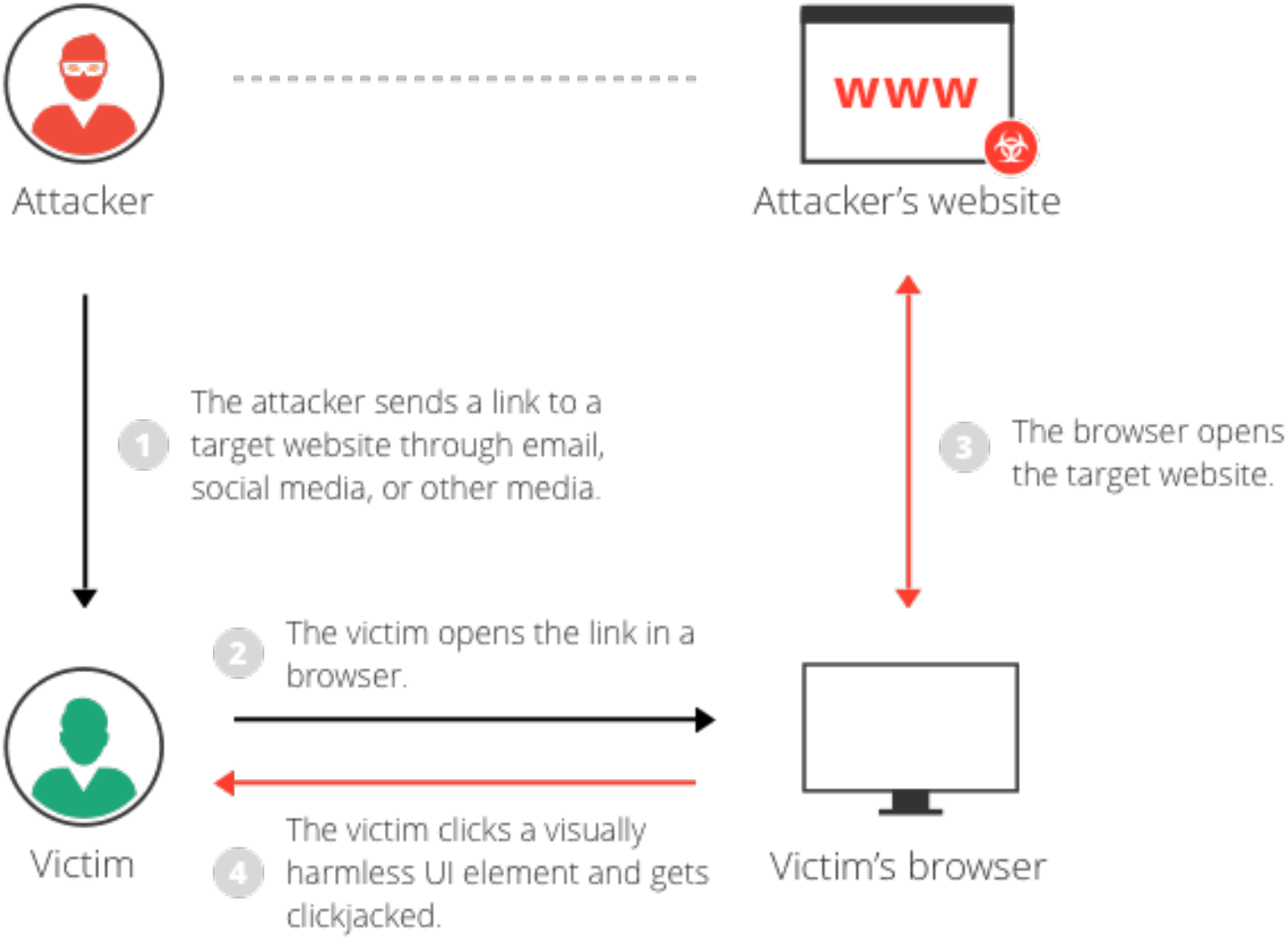
- This is a program that is automatically installed on a computer when a user accesses a malicious site.
  - Even without clicking a link or giving consent.
- This often happens when a user searches for a social networking site and selects a site using a fraudulent link.
- Sometimes a drive-by download may be packaged invisibly together with a program that a user requests to download.



Clickjacking

- An attack that tricks a user into clicking an unintended link.
- The attacker uses a combination of visible and invisible HTML frames to fool the user into thinking what they are clicking is what's visible, when in fact the invisible link is layered on top of or beneath the visible frame.
- This happens when a user is going through a fraudulent networking site or a site that has been hijacked by an attacker.
  - For example, someone posts a video on Facebook, and the embedded link redirects to an external site.
- When you select the Play button, you also select the embedded Facebook Like option, which posts to your page and possibly to all your friends' pages. Or, perhaps the Play button is linked to a malicious download.

Clickjacking



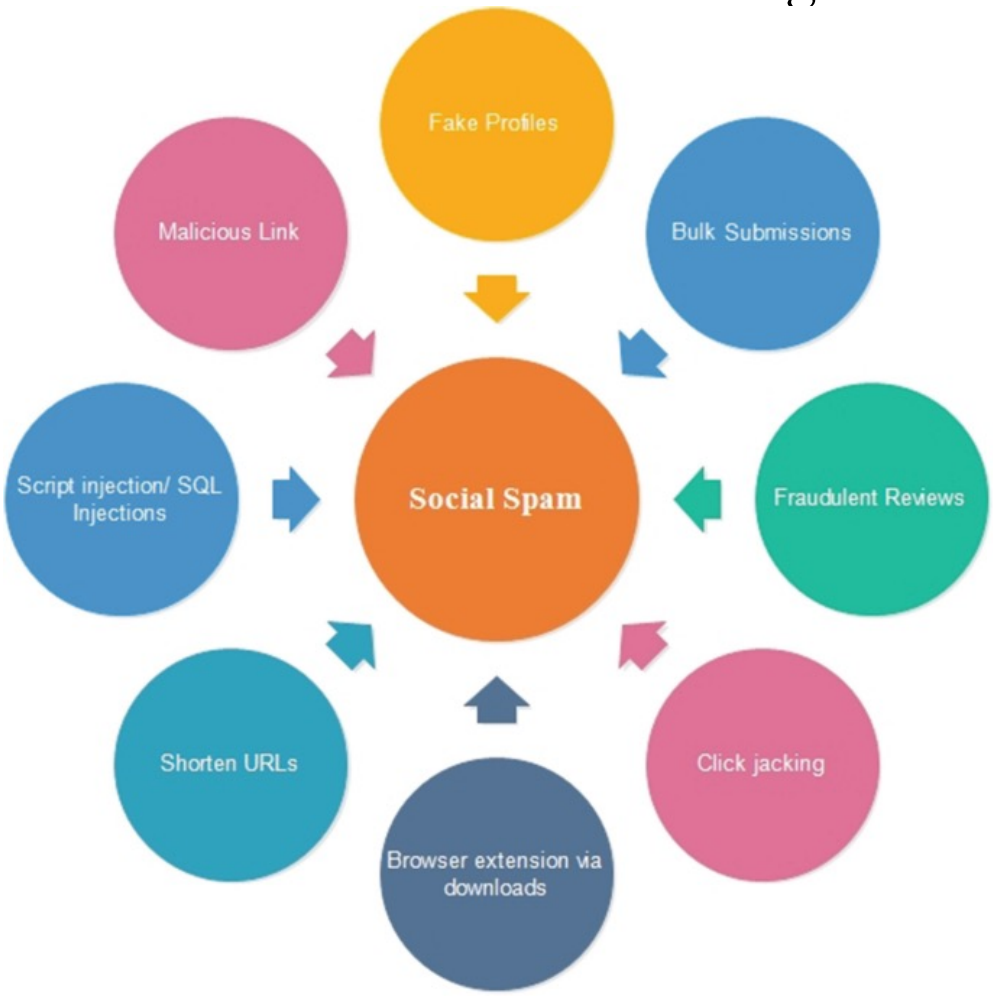
Password Stealer

- A type of software that, when installed on a system, will be able to capture all the passwords and user names entered into the instant messaging application or social network site that it was designed for.

- This information is sent back to the attacker who can use it for fraudulent purposes.

Spamming

- Within social networking,
  - Spamming refers to sending unsolicited bulk messages by misusing the electronic messaging services inside the social networking site.

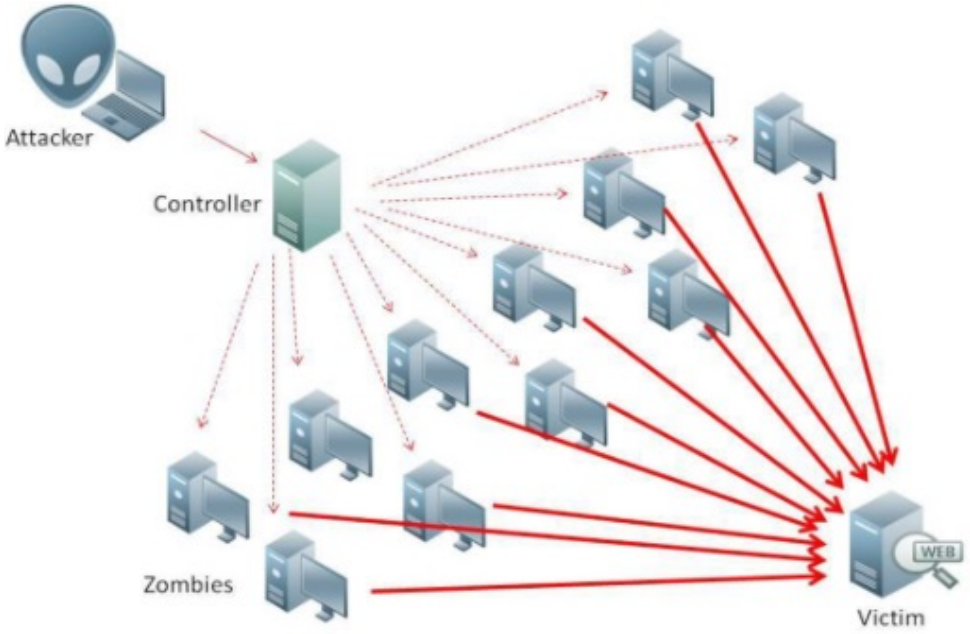


DoS Attacks

- It is a type of network attack in which an attacker attempts to disrupt or disable systems that provide network services by various means, including:
  - Flooding a network link with data to consume all available bandwidth.
  - Sending data designed to exploit known flaws in an application.
  - Sending multiple service requests to consume a system's resources.
  - Flooding a user's email inbox with spam messages, causing the genuine messages to get bounced back to the sender.

Types of DoS Attacks:

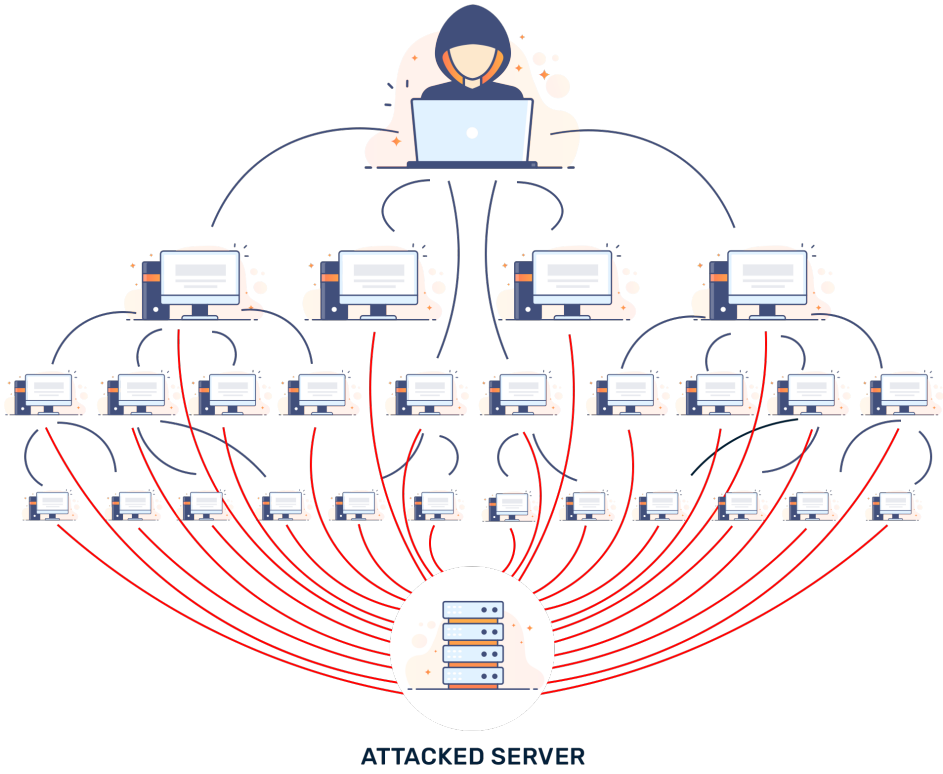
- ✓ ICMP flood
- ✓ UDP flood
- ✓ SYN flood
- ✓ Buffer overflow
- ✓ Reflected DoS attack
- ✓ Permanent DoS attack



Distributed Denial of Service (DDoS) Attack

- It is a type of DoS attack that uses multiple computers on disparate networks to launch the attack from many simultaneous sources.

- The attacker introduces unauthorized software that turns the computer into a zombie/drone that directs the computers to launch the attack.



Session Hijacking Attacks

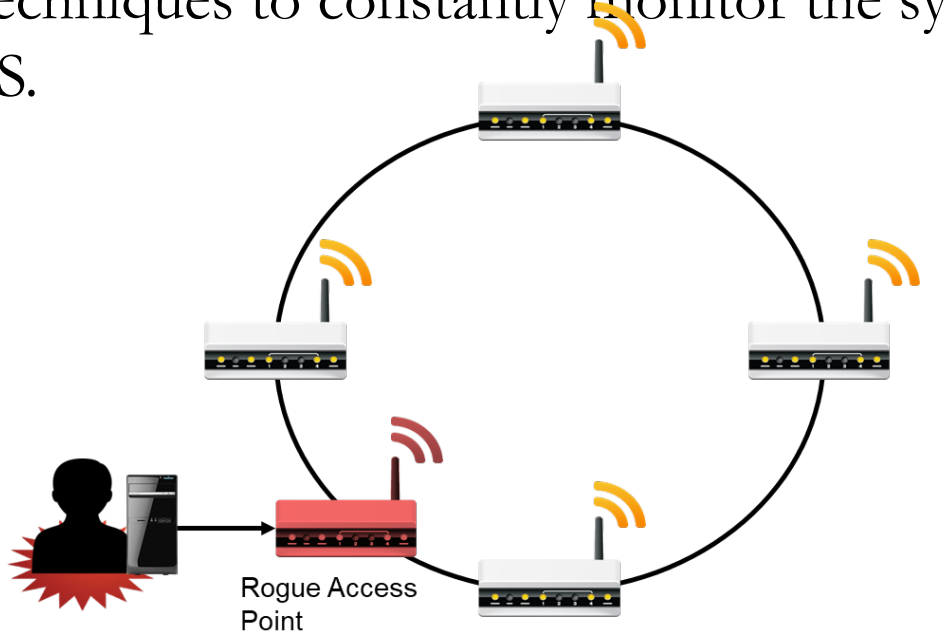
- A session hijacking attack involves exploiting a computer in session to obtain unauthorized access to an organization's network or services.
- It involves stealing an active session cookie that is used to authenticate a user to a remote server and using that to control the session thereafter.
- Session hijacking attacks may be used to execute denial of service to either the client's system or the server system, or in some cases, both systems.
- Attackers may also hijack sessions in order to access sensitive information, like bank accounts or private communications.

P2P Attacks

- Peer-to-peer (P2P) attacks are launched by malware propagating through P2P networks.
- P2P networks typically have a shared command and control architecture, making it harder to detect an attacker.
- A P2P attack can be used to launch huge DoS attacks.
- Within a P2P network, personal computers with high-speed connections can be compromised by malware such as viruses and Trojans.
- An attacker can then control all these compromised computers to launch a DDoS attack.

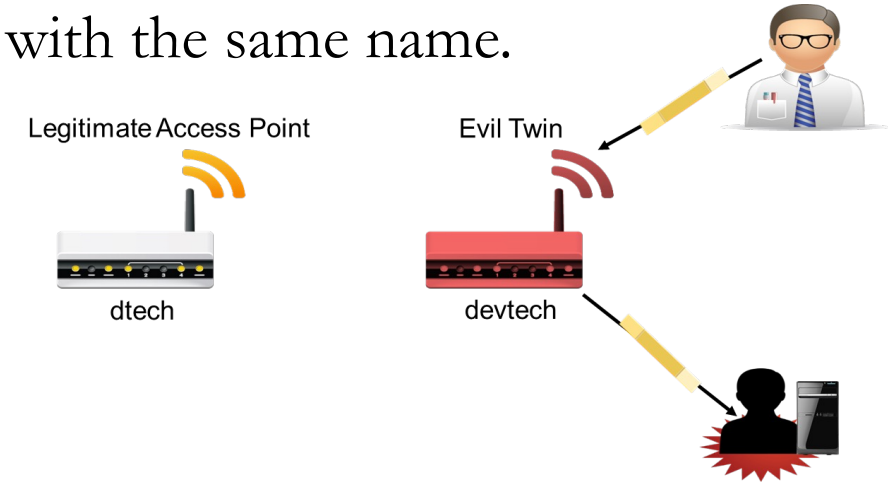
Rogue Access Points attacks

- It is an unauthorized wireless access point on a corporate or private network.
  - It can cause considerable damage to an organization's data.
  - It can allow man-in-the-middle attacks and access to private information.
- They are not detected easily and can allow private network access to many unauthorized users with the proper devices.
- Organizations should protect themselves from this type of attack by implementing techniques to constantly monitor the system, such as installing an IDS.



Evil Twins Attacks

- Evil twins in the context of wireless networking are access points on a network that fool users into believing they are legitimate.
  - They can be installed both in corporate and private networks, typically they are found in public Wi-Fi hotspots where users do not connect transparently and automatically as they do in a corporate network, but rather select available networks from a list.
- A malicious user can set up such an access point with something as basic as a smartphone with tethering capabilities.
- Evil twins can be more dangerous than rogue access points because the user thinks that the wireless signal is genuine, making it difficult to differentiate from a valid access point with the same name.



Jamming Attacks

- In wireless networking,
  - Jamming is also called interference.
    - It is an attack in which radio waves disrupt 802.11 wireless signals.
    - It usually occurs at home because of various electronic devices, such as microwaves, operating in a bandwidth close to that of the wireless network.
- When this occurs, it causes the 802.11 signals to wait before transmitting, and the wait can be indefinite at times.

- Attackers may use a radio transceiver to intercept transmissions and inject jamming packets, disrupting the normal flow of traffic across a network.

Bluejacking Attacks

- Bluejacking is a method used by attackers to send out unwanted Bluetooth signals from smartphones, mobile phones, tablets, and laptops to other Bluetooth-enabled devices.
    - Because Bluetooth has a 30foot transmission limit, this is a very close-range attack.
- With the advanced technology available today, attackers can send out unsolicited messages along with images and video.

http://www.tech-faq.com/bluejacking.html

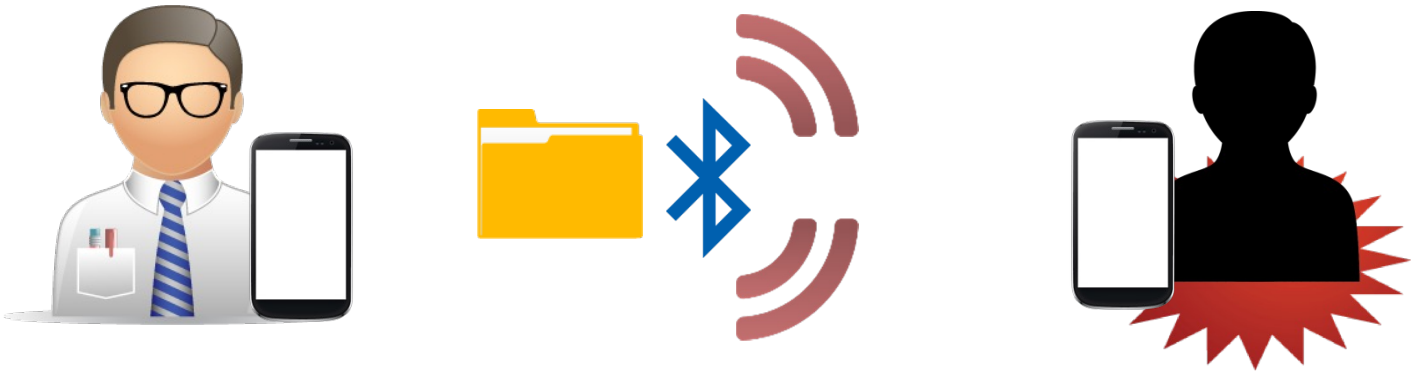
Bluesnarfing Attacks

- It is a method in which attackers gain access to unauthorized information on a wireless device using a Bluetooth connection within the 30-foot Bluetooth transmission limit.

- Unlike bluejacking, access to wireless devices such as smartphones, tablets, mobile phones, and laptops by bluesnarfing;

  - Can lead to the exploitation of private information, including email messages, contact information, calendar entries, images, videos, and any data stored on the device.

https://www.techadvisory.org/2017/06/bluesnarfing-what-you-need-to-know/



WEP and WPA Attacks

- The **Wired Equivalent Privacy** (**WEP**) algorithm was the earliest algorithm used to secure wireless networks.

- This method of data encryption was meant to match the security found in wired connections at the time.

- **WEP** came in 64-bit, 128-bit, and 256-bit key sizes.
  - ✓ However, because it used a stream cipher to encrypt data, WEP relied on an IV to randomize identical strings of text.
  - ✓ With a 24-bit IV size, WEP was extremely vulnerable to an IV attack that would be able to predict the IV value.

- In fact, some freely available software would be able to crack WEP encryption within minutes on standard consumer hardware.
  - ✓ Because of this vulnerability, WEP was deprecated in 2004 and should not be used.

WEP and WPA Attacks

IV: CF461E

Passphrase:

passw0rd

password
Password
PASSWORD
p4ssword
passw0rd

WEP and WPA Attacks

- The **Wired Equivalent Privacy** (**WEP**) algorithm was the earliest algorithm used to secure wireless networks.

- This method of data encryption was meant to match the security found in wired connections at the time.

- **WEP** came in 64-bit, 128-bit, and 256-bit key sizes.
  - ✓ However, because it used a stream cipher to encrypt data, WEP relied on an IV to randomize identical strings of text.
  - ✓ With a 24-bit IV size, WEP was extremely vulnerable to an IV attack that would be able to predict the IV value.

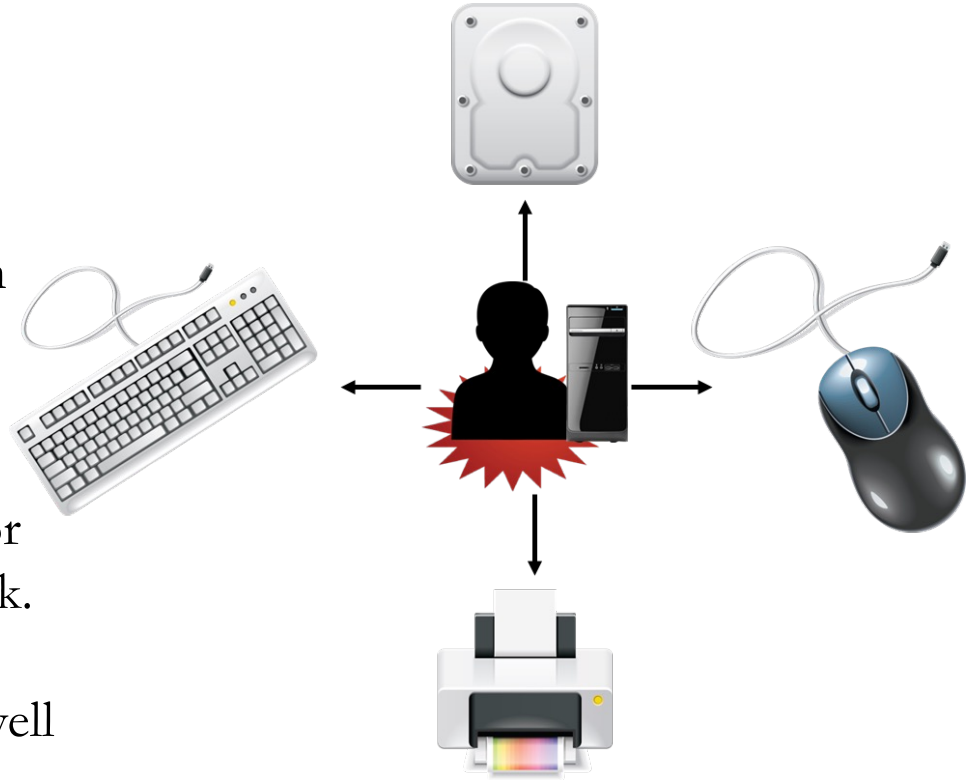
- In fact, some freely available software would be able to crack WEP encryption within minutes on standard consumer hardware.
  - ✓ Because of this vulnerability, WEP was deprecated in 2004 and should not be used.

WEP and WPA Attacks

- WEP was superseded by the much more secure **Wi-Fi Protected Access** (WPA) protocol and its successor, **WPA2**.
- Unlike WEP, WPA actually generates a **128-bit key** for each individual packet sent, which prevents easy cracking of encrypted information.
- Although **WPA** used the same **RC4** stream cipher, **WPA2** uses the more secure **AES** block cipher for encryption.
- Even with this enhanced security, both WPA protocols are vulnerable to attack.
- In particular, users who secure their WPA wireless networks with weak passwords are susceptible to brute force password cracking attacks.
- Another potential weakness in WPA allows attackers to inject malicious packets into the wireless data stream.
- Currently, WPA2 is considered the most secure wireless encryption protocol and should be used instead of WPA.

Hardware Attacks

- The goal of a hardware attack is to physically access a digital system to obtain secret information or modify the system behavior.
- These attacks can be classified as covert or overt based on the awareness of the attack.
- Each hardware attack has capabilities as well as objectives.



Thank you