IT Fundamentals for Cyber Security

Chapter 04: Common Cybersecurity Threats and Vulnerabilities

Co-funded by
the European Union

Table of Contents

List of figures

4. Common Cybersecurity Threats and Vulnerabilities

4.1. Types of Malwares

Malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users. Malware can take many forms. It's important for individuals and organizations to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

4.1.1. Importance of Understanding different types of Malware

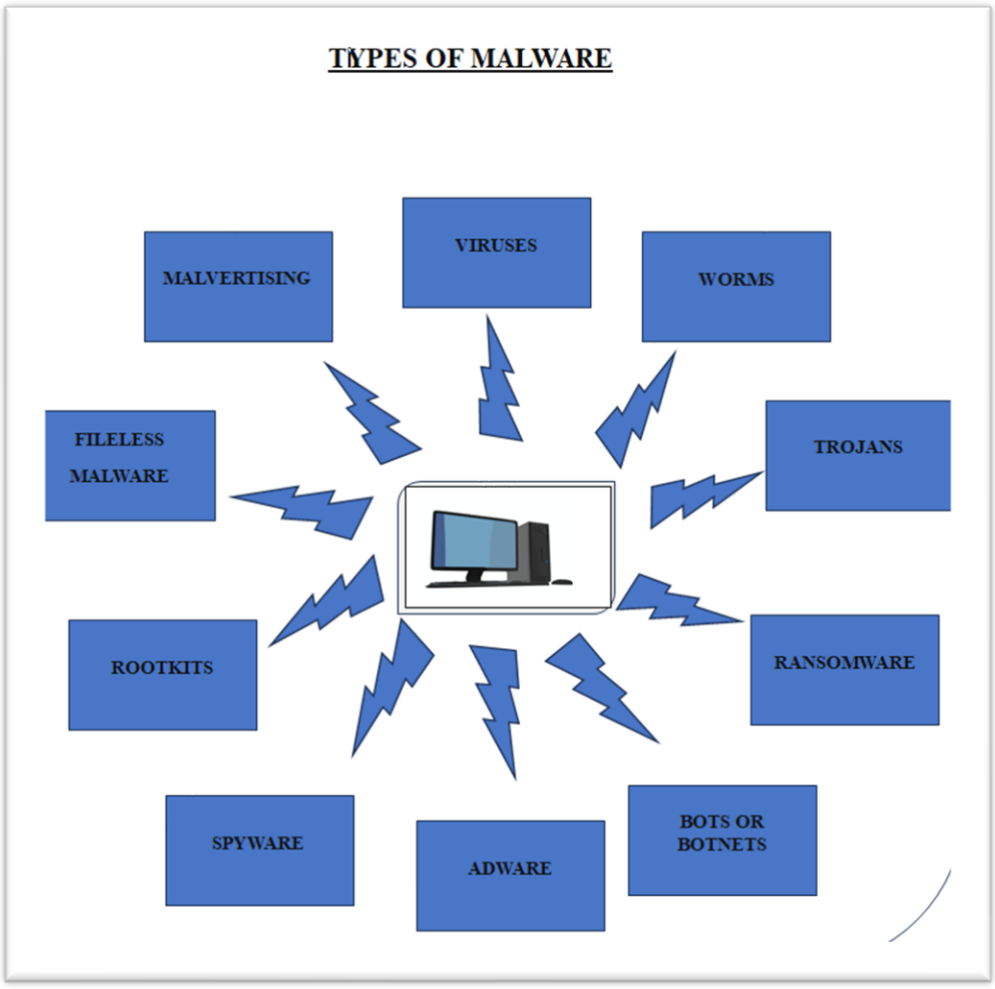

Figure 1. Types of Malware

1. **Viruses –** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

2. **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

3. **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.

4. **Ransomware –** Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system

5. **Adware –** It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.

6. **Spyware –** Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

7. **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

8. **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

9. **Backdoors –** A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

10. **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

4.2. Overview of Malwares Impact On Sytem and Data

A computer virus is malicious software code that can enter a computer system without the user's knowledge or permission. Viruses spread through mail attachments and network sharing, including USB drives, or by downloading files from websites. Once a computer is

infected with a virus, the virus will replicate itself. This is where it will try to spread to other computers on the same network.

The impact of malware and viruses on computer performance can include anything from:

1. Decreased speed
2. Crashing of programs,
3. Data corruption
4. Unauthorized access
5. Even total system failure.

Viruses can also steal confidential information stored on your computer. This can result in identity theft or financial loss. To avoid getting a virus or malware, it's important to be aware of these potential risks when browsing online. Fortunately, there are steps you can take today, such as:

1. Installing an antivirus program
2. Avoiding opening suspicious links or email attachments
3. Using a firewall, backing up all of your important files and data regularly
4. Educating yourself about cybersecurity risks
5. Using secure passwords for all accounts

Social Engineering Techniques

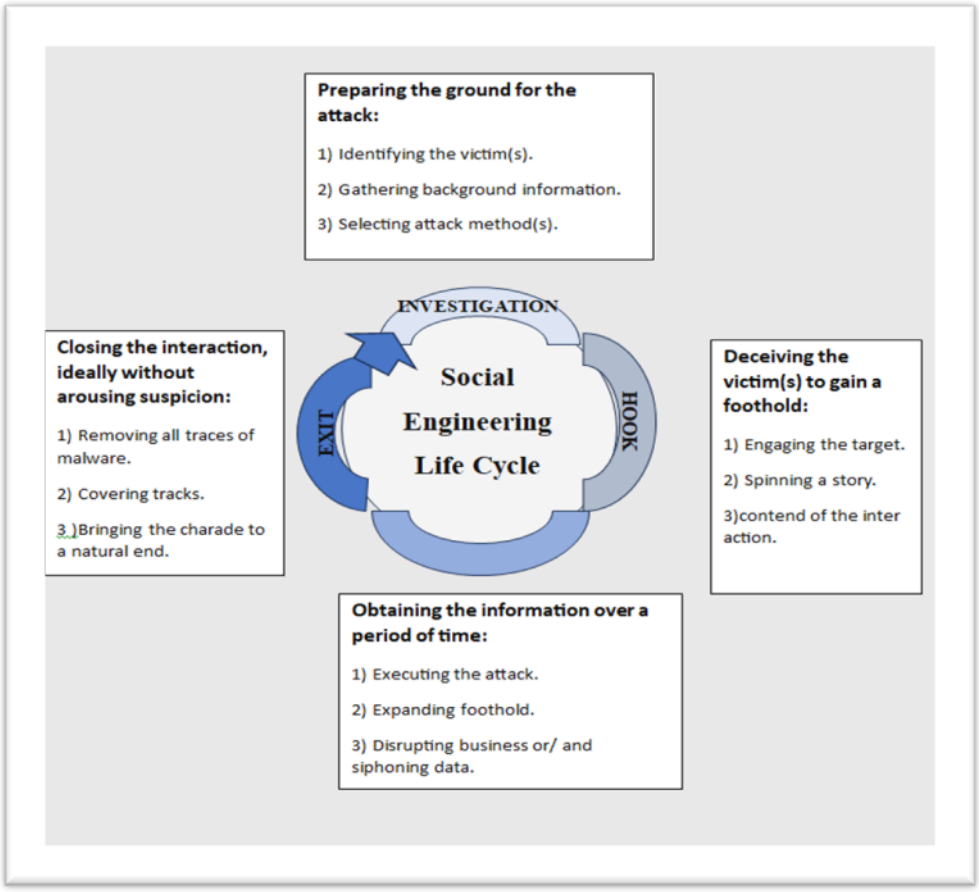

Figure 2. Social Engineering Life Cycle

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

4.2.1. Definition and Importance of Understanding Social Engineering

Definition: Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Importance of Social Engineering

As evident from the various types of social engineering attacks and various other methods which are not covered above such as DNS spoofing, peer to peer network attacks etc., plays an important role for securing devices. Wherever there is a threat there is a need for security, thus, social engineering attacks indirectly promote a sense for security of devices. Precautions are also as important as security as precautions help you to spot these attacks and in order to spot these attacks at institutional and individual levels, one may follow the tips suggested below:

- There should be effective training of all employees.
- Creation of security awareness.
- Cyber security software must be in use and updated regularly.
- Must be able to identify social engineering attacks.
- Use only trusted websites for software download.
- Must not act hastily to share credentials.
- Must check the background of websites before making any kind of transaction.

The above are some of the precautionary measures which must be adopted by persons to secure themselves from social engineering attacks. These attacks are a threat to the society by affecting the economic structure of its members. The only important part social engineering plays is that it creates a sense of security in the cyber world, otherwise it has only a negative part to play, as these attacks cannot be eliminated because of unpredicted innovations in the cyber world but they can surely be mitigated by being aware.

4.2.2. Overview and its impact on Individual and Organization

Impact on Organization

1. Impact on Reputation
2. Getting Hit by Ransomware
3. Falling Prey to Watering Hole Attacks
4. Cost on Business Productivity
5. Financial Losses
6. Disruption in Operations

Impact on Individual

1. Identity theft
2. Malware attacks
3. Ransomware attacks,
4. Reputational damage
5. Data theft
6. Service disruption and unauthorized access

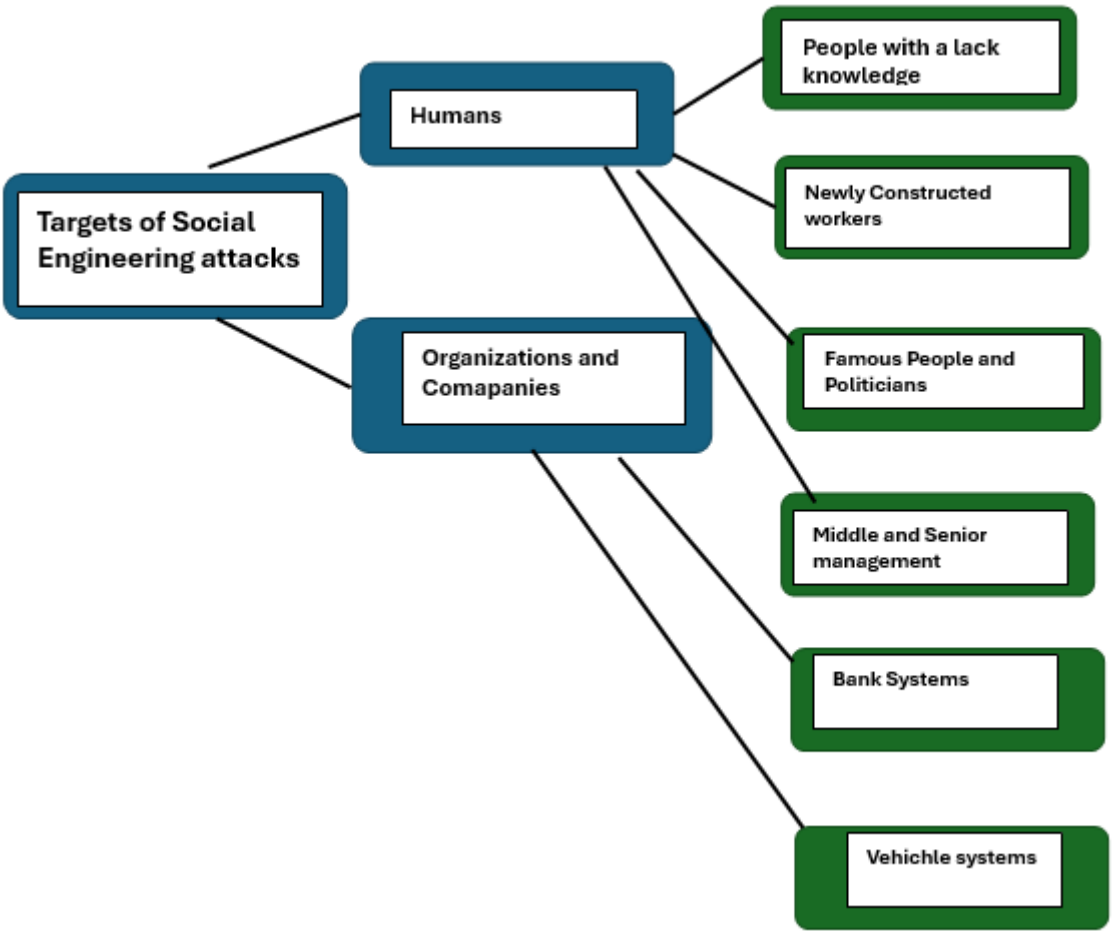

Figure 3. Impact on Individual and Organization

4.3. Threats and Vulnerabilities

Risk = Threats x Vulnerabilities

Figure 4. Information Risks, Threats and Vulnerabilities

Components of a Threat

1. **Threat agents –** criminals, terrorists, subversive or secret groups, state sponsored, disgruntled employees, hackers, pressure groups, commercial groups.
2. **Capability –** software, technology, facilities, education and training, methods, books and manuals.
3. **Threat inhibitors –** fear of capture, fear of failure, level of technical difficulty, cost of participation, sensitivity to public perception, law enforcement activity, target vulnerability, target profile, public perception, peer perception.
4. **Threat amplifiers –** peer pressure, fame, access to information, changing high technology, deskilling through scripting, skills and education levels, law enforcement activity, target vulnerability, target profile, public perception, peer perception.
5. **Threat catalysts –** events, technology changes, personal circumstances.
6. **Threat agent motivators –** political, secular, personal gain, religion, power, terrorism, curiosity.

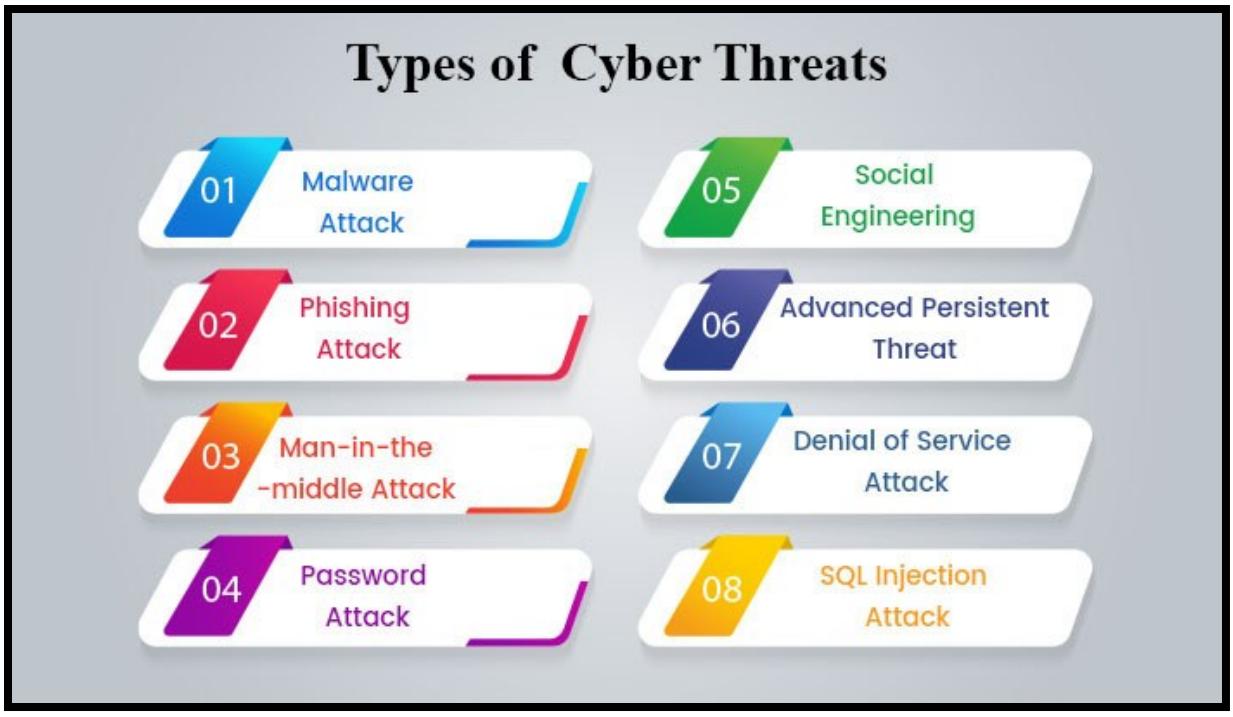

Figure 5. Types of Cyber Threats

Threat Agents

1. **Natural** – fire, floods, power failure, earth quakes, etc.
2. **Unintentional –** insider, outsider – primarily nonhostile
3. **Intentional –** insider, outsider – hostile or nonhostile (curious)

Foreign agents, industrial espionage, terrorists, organized crime, hackers and crackers, insiders, political dissidents, vendors and suppliers

Ten web threats

1. B**igger, Subtler DDoS Attacks** – Distributed Denial of Service Attacks
2. **Old Browsers, Vulnerable Plug-Ins –** e.g., browser vulnerabilities and, more frequently, the browser plug-ins that handle Oracle's Java and Adobe's Flash and Reader.
3. **Good Sites Hosting Bad Content –** in VOHO watering hole attack, attackers infected legitimate financial and tech industry websites in Massachusetts and Washington, D.C., commonly accessed by their intended victims
4. **Mobile Apps and The Unsecured Web –** bring-your-own-device movement has led to a surge in consumer-owned devices inside corporate firewalls
5. **Failing To Clean Up Bad Input** – e.g., Since 2010, SQL injection has held the top spot on the Open Web Application Security Project's list of top 10 security vulnerabilities
6. **The Hazards of Digital Certificates –** a series of hacks against certificate authorities gave attackers the tools they needed to issue fraudulent SSL certificates that could disguise a malicious website as a legitimate.

7. **The Cross-Site Scripting Problem** – An attacker going after a banking site with a cross-site scripting vulnerability could run a script for a login box on the bank's page and steal users' credentials.
8. **The Insecure 'Internet of Things** – Routers and printers, video conferencing systems, door locks and other devices are now networked via Internet protocols and even have embedded Web servers. In many cases, the software on these devices is an older version of an open source library that's difficult.
9. **Getting In the Front Door** – Automated Web bots scrape from Web pages information that can give a competitor better intelligence on your business.
10. **New Technology, Same Problems** – People click links all day long - people are pretty trained to think that clicking a link on the Web is safe.

Vulnerabilities

Some weakness of a system that could allow security to be allowed."

Vulnerabilities in network security can be summed up as the "soft spots" that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

Technological Weaknesses

Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Configuration Weaknesses

Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

Security Policy Weaknesses

Security policy weaknesses can create unforeseen security threats. The network can pose security risks to the network if users do not follow the security policy

Types of vulnerabilities

A. Physical vulnerabilities
B. Natural vulnerabilities
C. Hardware/software vulnerabilities
D. Media vulnerabilities (e.g., stolen/damaged disk/tapes)
E. Emanation vulnerabilities---due to radiation
F. Communication vulnerabilities
G. Human vulnerabilities

How do the vulnerabilities manifest?

The different types of vulnerabilities manifest themselves via several misuses:

1. **External misuse –** visual spying, misrepresenting, physical scavenging
2. **Hardware misuse** – logical scavenging, eavesdropping, interference, physical attack, physical removal
3. **Masquerading –** impersonation, piggybacking attack, spoofing attacks, network weaving
4. **Pest programs –** Trojan horse attacks, logic bombs, malevolent worms, virus attacks
5. **Bypasses –** Trapdoor attacks, authorization attacks (e.g., password cracking)
6. **Active misuse –** basic active attack, incremental attack, denial of service
7. **Passive misuse –** browsing, interference, aggregation, covert channels

Web Based Threats and Vulnerabilities

Web security threats are a form of internet-borne cybersecurity risk that could expose users to online harm and cause undesired actions or events. Web security issues can severely damage businesses and individuals.

Common types of web security threats include <computer viruses, data theft, and phishing attacks. While they are not limited to online activity, web security issues involve cyber criminals using the internet to cause harm to victims. They typically cause problems like denial of access to computers and networks, unauthorized access to and usage of corporate networks, theft and exposure of private data, and unauthorized changes to computers and networks.

Web security threats and approaches have evolved in sophistication with the rise of faster mobile networks and smart devices. Increased web adoption through popular communication and productivity tools, as well as the Internet of Things (IoT), has outpaced the security awareness and readiness of most businesses and end-users.

4.3.1. Common Web Based Threats

1. Phishing

Phishing attacks involve attackers targeting users through email, text messages, or social media messaging sites. They pose as a sender the user trusts to trick them into giving up sensitive information like account numbers, credit card data, and login credentials. A successful phishing attack can also result in cyber criminals gaining unauthorized access to corporate networks, enabling them to steal business data. Phishing is most commonly committed through email, which remains the most significant attack vector.

2. Ransomware

Ransomware is a form of malware that results in an attacker holding their victim's data or computer hostage. The attacker threatens to block access to, corrupt, or publish the data unless their victim pays a ransom fee.

Ransomware attacks are typically initiated through phishing emails that contain malicious attachments or links that lead the user's computer to download malware. The device gets infected by the malware, which looks for files to encrypt and prevents users from accessing them. Ransomware is also spread via drive-by downloading, which occurs when users visit an infected website that downloads malware onto their device without them knowing.

3. SQL injection

Structured Query Language (SQL) is a computing language used to search and query databases. SQL injection is a web security threat in which attackers exploit vulnerabilities in the application code. Attackers achieve this by inserting an SQL query in standard online form fields, such as login boxes on a website, which are passed to the application's SQL database.

SQL injection attacks have succeeded in exploiting vulnerabilities on shared codebases like WordPress plugins. A vulnerability in the code can lead to hundreds of thousands of websites using the code being hacked. Attackers use this web security issue to steal corporate data, such as customer files and financial information.

4. Cross-site scripting

Cross-site scripting (XSS) is a form of web security issue that enables attackers to execute malicious scripts on trusted websites. In an XSS attack, web applications or pages are used to submit malicious code and compromise user interactions. The attacker can then seize a user's identity to carry out malicious activity, gain authorized access to corporate information, or steal their data.

The script used in XSS attacks prevents users' browsers from identifying malicious activity. The attacker is therefore free to browse the user's cookies, sensitive data, and session tokens stored in their browser.

5. Distributed denial-of-service (DDoS) attack

A DDoS attack is a web security threat that involves attackers flooding servers with large volumes of internet traffic to disrupt service and take websites offline. The sheer volume of fake traffic results in the target network or server being overwhelmed, which leaves them inaccessible.

DDoS attacks are often carried out by disgruntled employees or hacktivists who want to cause harm to an organization by taking their server offline. Others are done for the fun of exploiting cyber weakness, and many DDoS attacks are financially motivated, such as certain organizations stealing information from their competitors. They can also be used as part of a ransomware attack.

6. Viruses and worms

Viruses and worms are malicious programs that spread through computers and networks. Both exploit software vulnerabilities that allow an attacker to steal data from systems. Viruses and

worms also install backdoors into systems that an attacker can use to gain unauthorized access, corrupt files, and inflict broader damage to a company.

Worms, in particular, eat up vast amounts of computer memory and network bandwidth, which leads to servers, systems, and networks overloading and malfunctioning. Worms can operate independently, enabling them to spread between systems, but a virus requires a host computer to carry out malicious activity.

7. Spyware

Spyware is a form of malware that gathers data from users and their devices then sends it to third-party individuals without consent. Spyware typically collects sensitive information and shares it with advertisers, data collection firms, and cyber criminals, who can use that data to make a profit. It is also used to steal and sell user data like bank accounts, credit card numbers, login credentials, and internet usage information—or to commit broader identity fraud and identity spoofing.

Spyware can be difficult to identify and can cause severe damage to devices and networks. It can also leave a business vulnerable to data breaches, affect device and network performance, and inhibit user activity.

4.3.2. Web Application Security Best Practices

Don't open emails and attachments from suspicious sources – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.

Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.

Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.

Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

Maintain Security During Web App Development

Encrypt your data

Apply Authentication, Role Management & Access Control

Scanning for malware and malicious activity

Ensuring all devices, software, and business tools are up to date

Enabling multi-factor authentication (MFA) and never relying on usernames and passwords alone

Creating backups of valuable data and storing it in secure locations

Implementing firewalls to monitor, detect, filter, and restrict web traffic

Ensuring proper security configuration for session management and user access rights

Conducting regular security awareness training with employees to ensure they understand their cyber risk and responsibilities

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber SecurityEssentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security,Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

1. https://www.researchgate.net/publication/338419380_Cyber_Security_Threats_and_Vulnerabilities_A_Systematic_Mapping_Study
2. https://www.researchgate.net/publication/369186216_A_Comprehensive_Review_of_Cyber_Security_Vulnerabilities_Threats_Attacks_and_Solutions
3. https://www.mdpi.com/2079-9292/12/6/1333
4. https://www.sciencedirect.com/book/9780128162033/emerging-cyber-threats-and-cognitive-vulnerabilities

Marks

Questions Answers

Q. No. 01

Question: Describe Malware, and justify why is it important to understand its different types? **05**

Answer: Malware refers to malicious software designed to cause harm to computer systems, networks, or users. It encompasses various forms like viruses, worms, Trojans, ransomware, adware, spyware, and more, each with distinct behaviors and impacts.

Understanding the different types of malware is essential because each type poses unique threats and requires specific defense strategies. For example, viruses spread through infected files, while worms self-replicate across networks without human intervention. Ransomware locks data, demanding payment, while spyware steals sensitive information discreetly. By recognizing these differences, individuals and organizations can implement appropriate security measures, such as antivirus software, firewalls, and regular updates, to mitigate specific risks

Q. No.02 **05**

Question: Is it possible to remove ransomware without paying the ransom? Justify your answer

Answer: Yes.

Justification: In some cases, ransomware victims can restore their data through backups or specialized decryption tools, avoiding the need to pay the ransom. It depends on the type of ransomware and whether the affected system had secure backups or available public decryptors. Paying the ransom doesn't guarantee that access will be restored, and experts generally advise against it. Organizations should focus on proactive protection and backups

Q. No.03 **05**

Does social engineering involve exploiting software vulnerabilities?

Answer: No.

Justification: Social engineering exploits human vulnerabilities, not software. It manipulates human emotions or behaviors to trick people into revealing sensitive information or bypassing security measures. Common techniques include phishing, baiting, and pretexting. The goal is to get users to unknowingly hand over access to systems, often without any technical hacking involved. This makes it difficult to detect

Q. No.04 **05**

Question: Can a virus spread through a network without infecting a file?

Answer: No.

Justification: A virus requires a file to attach itself to and spread. It cannot move between systems without a host file being transferred, such as through email attachments, USB drives, or network file sharing. The virus remains dormant until the infected file is executed. This dependence on files makes viruses different from worms, which can spread independently through networks

Q. No.05 **05**

Question: Does using antivirus software alone guarantee complete protection against malware?

Answer: No.

Justification: Antivirus software is an essential defense but not sufficient on its own. It can only detect known malware and requires regular updates. Additional measures like firewalls, regular system updates, secure browsing habits, and employee training are crucial for comprehensive protection. Advanced threats, like zero-day exploits, can bypass traditional antivirus defenses. A layered security approach is best

Q. No.06 **05**

Question: What is social engineering, and how does it exploit human behavior?

Answer: Social engineering is a form of cyberattack that relies on manipulating human behavior rather than exploiting technical vulnerabilities. Attackers use psychological tactics to deceive individuals into revealing confidential information or performing actions that compromise security, such as granting access to systems or divulging sensitive data.

Social engineers exploit emotions like trust, fear, urgency, or curiosity to manipulate their victims. For example, attackers might send a phishing email pretending to be from a trusted entity, urging the victim to click a link or provide personal details. By taking advantage of human tendencies like helpfulness or fear of consequences, social engineering bypasses technical defenses and breaches security at the human level

Q. No.07 **05**

Question: Describe the concept of a logic bomb in malware. 6 lines answer

Answer: A logic bomb is a type of malware that remains dormant within a system until triggered by a specific event, such as a certain date or action. Once the trigger occurs, the malicious code activates and executes harmful tasks like deleting files, corrupting data, or damaging hardware. Logic bombs are often hidden within legitimate programs, making them difficult to detect before activation. Unlike other types of malware, they rely on pre-defined conditions to cause damage. They can even attack physical components like cooling fans or hard drives, causing system failure

Q. No.08 **05**

Question: What are some precautions to prevent social engineering attacks

Answer:

1. Effective employee training
2. Security awareness programs
3. Regularly updated cybersecurity software
4. Avoiding hastily sharing credentials
5. Using trusted websites for downloads

Q. No.09 **05**

Question: What are some common impacts of social engineering on individuals?

Answer:

1. Identity theft
2. Data theft
3. Malware and ransomware attacks
4. Reputational damage
5. Service disruption

05

Q. No.10

Question: List some best practices for web application security.

Answer:

1. Use of multifactor authentication
2. Avoiding suspicious emails and attachments
3. Keeping antivirus software updated
4. Encrypting sensitive data
5. Implementing firewalls