CYBERSECURITY – CA3 – JAI SHREE RAM 🚩 🕉️

1. Differentiate between threat, vulnerability, and risk. Define the types of Cyber Security.

- A **threat** exploits a vulnerability and can damage or destroy an asset.
- **Vulnerability** refers to a weakness in your hardware, software, or procedures.
- **Risk** refers to the potential for lost, damaged, or destroyed assets.

  " Threats + Vulnerability = Risk "

- Cybersecurity can be categorized into **five** distinct types:
  - Critical infrastructure security
  - Application security
  - Network security
  - Cloud security
  - Internet of Things (IoT) security

2. Explain the steps of SQL Injection.

- Following are some steps for SQL injection attack:

I. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.

II. To check the source code of any website, right click on the webpage and click on "view source", source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the <FORM> and </FORM>have potential parameters that might be useful to find the vulnerabilities.

III. The attacker inputs a single quote under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as use "a"="a" (or something similar) then the website is found to be susceptible to an SQL injection attack.

IV. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

3. Explain Active & Passive attacks in Network security.

- There are two types of attacks that are related to security namely passive and active attacks.
- **Passive attacks** - In a passive attack, an attacker observes the messages and copies them.
  - A passive attack can monitor, observe or build use of the system's data for sure functions. However, it doesn't have any impact on the system resources, and also, the data can stay unchanged. The victim is difficult to note passive attacks as this sort of attack is conducted in secret.
  - Passive attack aims to achieve data or scan open ports and vulnerabilities of the network.
    - eavesdropping attack

        - release of messages

- **Active attacks -** In an active attack, an attacker tries to modify the content of the messages.
    - An active attack could be a network exploit during which the attackers will modify or alter the content and impact the system resource. It'll cause damages to the victims.
    - The attackers can perform passive attacks to gather info before they begin playacting a vigorous attack. The attackers attempt to disrupt and forced the lock of the system.
    - The victims can get informed concerning the active attack. This sort of attack can threaten their integrity and accessibility.
    - A vigorous attack is tougher to perform compared to a passive attack.
        - Denial-of-Service attacks (DoS)
        - Trojan horse attacks

4. Explain Phishing with examples.

- Phishing happens when a victim replies to a fraudulent email that demands urgent action.
- Examples of requested actions in a phishing email include:
    - Clicking an attachment
    - Enabling macros in Word document
    - Updating a password
    - Responding to a social media connection request
    - Using a new Wi-Fi hot spot.
- The following illustrates a common phishing scam attempt:
    - A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
    - The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.
    - Several things can occur by clicking the link. For example:
        - The user is redirected to myuniversity.edurenewal.com, a bogus page appearing exactly like the real renewal page, where both new and existing passwords are requested. The attacker, monitoring the page, hijacks the original password to gain access to secured areas on the university network.
        - The user is sent to the actual password renewal page. However, while being redirected, a malicious script activates in the background to hijack the user's session cookie. This results in a reflected XSS attack, giving the perpetrator privileged access to the university network.

4. Explain various active attacks in detail.

I. **Masquerade Attack -** In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.
    - Masquerade attacks are conducted in several different ways, including the following:
        - using stolen login identifications (IDs) and passwords;
        - finding security gaps in programs; and

- bypassing the authentication

II. **Session Hijacking Attack -** A session hijacking attack is also called a session replay attack.
    - In this attack, the attacker takes advantage of a vulnerability in a network or computer system and replays the session information of a previously authorized system or user.
    - The attacker steals an authorized user's session ID to get that user's login information.
    - The attacker can then use that information to impersonate the authorized user. A session hijacking attack commonly occurs over web applications and software that use cookies for authentication.
    - With the use of the session ID, the attacker can access any site and any data that is available to the system or the user being impersonated.

III. **Message Modification Attack -** In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or to modify the data on a target machine.
    - Message modification attacks are commonly email-based attacks. The attacker takes advantage of security weaknesses in email protocols to inject malicious content into the email message.
    - The attacker may insert malicious content into the message body or header fields.

IV. **DoS attack**: In a denial-of-service (DoS) attack, the attackers overwhelm the victim's system, network or website with network traffic, making it difficult for legitimate users to access those resources. Two ways a DoS attack can occur include:
    - **Flooding**: The attacker floods the target computer with internet traffic to the point that the traffic overwhelms the target system.
        - The target system is unable to respond to any requests or process any data, making it unavailable to legitimate users.
    - **Malformed data**: Rather than overloading a system with requests, an attacker may strategically send data that a victim's system cannot handle.
        - For example: A DoS attack could corrupt system memory, manipulate fields in the network protocol packets or exploit servers.

5. Describe the categories of computer security.

- Here are a few types of computer security tactics that are used widely for the protection of software, hardware, electronic data, and network in computer systems.
    - **Application Security**: Application security is the introduction of security features in applications during their development process.
        - This actively helps prevent potential cyber threats such as data breaches, denial-of-service attacks (DoS), SQL injection, and many others.
        - Some examples of application security tools are antivirus software, firewalls, web application firewalls, encryption, etc

    - **Information Security:** Information security is a set of practices that aim to protect the confidentiality, integrity, and availability (known as the CIA triad) of data from unauthorized access and misuse.

- **Network Security**: Network security is any activity that aims to protect the integrity and usability of a network and data.
    - It consists of both hardware and software technologies that are specifically designed to prevent unauthorized intrusion into computer systems and networks.
- **Endpoint Security**: End-users are increasingly becoming the biggest security risk unintentionally.
    - With no-fault from their end, exempting the lack of awareness, the virtual gates of an organization are open to hackers and attacks.
    - Most of the end-users are unaware of the ICT policy, and therefore, it is imperative that the users who handle sensitive information on a regular basis understand and be knowledgeable about all comprehensive security policies, protocols, and procedures.
- **Internet Security**: Internet security is one of the most important types of computer security that come with a set of rules and protocols that focus on specific threats and activities that happen online.
    - It provides protection against hacking, DoS attacks, computer viruses, and malware.

6. Explain the digital signature algorithm.

- Digital Signatures Algorithm is a FIPS (Federal Information Processing Standard) for digital signatures. It was proposed in 1991 and globally standardized in 1994 by the National Institute of Standards and Technology (NIST). It functions on the framework of modular exponentiation and discrete logarithmic problems, which are difficult to compute as a force-brute system.
- DSA Algorithm provides three benefits, which are as follows:
    - Message Authentication: You can verify the origin of the sender using the right key combination.
    - Integrity Verification: You cannot tamper with the message since it will prevent the bundle from being decrypted altogether.
    - Non-repudiation: The sender cannot claim they never sent the message if verifies the signature.

7. Explain the Feistel cipher in detail.

- The Feistel cipher is a design model or structure used to build various symmetric block ciphers, such as DES. This design model can have invertible, non-invertible, and self-invertible components. Additionally, the Feistel block cipher uses the same encryption and decryption algorithms.
- The Feistel structure is based on the Shannon structure proposed in 1945, demonstrating the confusion and diffusion implementation processes. Confusion produces a complex relationship between the ciphertext and encryption key, which is done by using a substitution algorithm. On the other hand, diffusion creates a complex relationship between plain text and cipher text by using a permutation algorithm.

- The Feistel cipher proposed the structure that implements substitution and permutation alternately. Substitution replaces plain text elements with ciphertext.
- Permutation changes the order of the plain text elements rather than being replaced by another element as done with substitution.

8. Compare symmetric and asymmetric encryption algorithms.

- **Symmetric Key Encryption**: Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.
- **Asymmetric Key Encryption**: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

9. Describe Intrusion Detection System.

- **An Intrusion Detection System (IDS)** is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations centre (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat an IDS can either be host-based or network-based.
- **Host-Based IDS (HIDS):** A host-based IDS is deployed on a particular endpoint and designed to protect it against internal and external threats. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the host computer's internals.
- **Network-Based IDS (NIDS):** A network-based IDS solution is designed to monitor an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents. This wider viewpoint provides more context and the ability to detect widespread threats; however, these systems lack visibility into the internals of the endpoints that they protect.

10. Describe Intrusion Prevention System.

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System.
- It is a network security application that monitors network or system activities for malicious activity.
- Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.
- Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.
- IPS typically record information related to observed events, notify security administrators of important observed events and produce reports.
- Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

- Classification of Intrusion Prevention System (IPS): Intrusion Prevention System (IPS) is classified into 4 types:
    - **Network-based intrusion prevention system (NIPS):** It monitors the entire network for suspicious traffic by analysing protocol activity.
    - **Wireless intrusion prevention system (WIPS):** It monitors a wireless network for suspicious traffic by analysing wireless networking protocols.
    - **Network behaviour analysis (NBA):** It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
    - **Host-based intrusion prevention system (HIPS):** It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

11. Describe Security risk and analysis.

- Risk analysis refers to the review of risks associated with the particular action or event.
- The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis.
- Risks are part of every IT project and business organizations.
- The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats.
- The strategic risk analysis helps to minimize the future risk probability and damage.
- Enterprise and organization used risk analysis:
    - To anticipates and reduce the effect of harmful results occurred from adverse events.
    - To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.
    - To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
    - To identify the impact of and prepare for changes in the enterprise environment.

12. Explain Cyber security & Information security.

I. "Information security" (commonly known as InfoSec) refers to the procedures and practices that corporations use to protect their data. This contains policy settings that prevent unauthorized people from accessing company or personal data. Information security is a fast-evolving and dynamic discipline that includes everything, from network and security design to testing and auditing.

II. Information security protects sensitive data from unauthorized acts such as scrutiny, modification, recording, disruption, or destruction. The goal is to secure and preserve the privacy of important data like client account information, financial information, or intellectual property.

III. "Cyber security" is the activity of securing computer systems, networks, devices, and applications from cyber-attacks of any kind. Cyber security threats have risen above critical levels because of the inevitable spread of digital transformation, putting your sensitive data in jeopardy.
IV. Because of its complexity in geopolitics and the more dispersed attack methods, corporations and national governments have begun to perceive cyber security as a key concern.
V. Many firms increasingly include information risk management into their overall risk management strategy.

13. Explain any 8 types of cyber-crimes. Discuss the attacks on wireless networks and mobile phones in detail.

I. **Malware**: Malware is a broad phrase that encompasses a wide range of cyberattacks such as Trojans, viruses, and worms. Malware can simply be described as code written to steal data or destroy things on a computer.

II. **Phishing**: Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.

III. **DDoS Attack**: As the name suggests, a denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working.

IV. **Man-in-the-middle Attack**: A man-in-the-middle attack can obtain information from the end-user and the entity with which they are communicating by impersonating the endpoints in the online information exchange.

V. **Drive-by Download Attack**: To become infected, we no longer need to click to accept a download or install a software update.
    - Simply opening a compromised webpage may now allow dangerous code to be installed on our device.
    - We only need to visit or drive by a website by clicking to accept for any software, and malicious code will be downloaded in the background on our device.

- Below are some of the most common types of **Wireless and Mobile Device Attacks**:

VI. **SMiShing**: Smishing become common now as smartphones are widely used.
    - SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling.
    - Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.

VII. **War driving**: War driving is a way used by attackers to find access points wherever they can be.
    - With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.

VIII. **WEP attack**: Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network with the same level of security as a wired LAN.
   - Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption.
   - WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow.
   - Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.

IX. **WPA attack**: Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP.
   - WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic.
   - WPA2 is susceptible to attack because cyber criminals can analyse the packets going between the access point and an authorized user.

X. **Bluejacking**: Bluejacking is used for sending unauthorized messages to another Bluetooth device.
   - Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

XI. **Replay attacks**: In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.

XII. **Bluesnarfing**: It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.

XIII. **RF Jamming**: Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.
   - Commonly known as wireless network attacks, penetration and intrusion acts that target wireless networks pose serious threats.
   - Wireless network attacks aim to capture the information sent across the network and/or intrude with the traffic of information.

XIV. **Packet Sniffing**: Networks are designed to facilitate and accelerate the traffic of information. In order to achieve this goal, the information is sent in packets across both wired and wireless networks.
   - Due to the nature of wireless networks, these packets are sent through the air. As a result, it is very easy to capture them.
   - A great deal of traffic is sent through wireless networks, such as RTP, SNMP or HTTP. The common feature of these is the fact that they are in plain text. Which means, one can easily read them with the help of free access tools like Wireshark. As a result, someone with malicious intentions can simply steal your passwords and similar sensitive information.
   - A wireless network can be encrypted to protect against packet sniffing

XV. **Rouge Access Point**: Rouge access point refers to any unauthorized access point (AP) on a network.

- It can be created by an attacker or even a misinformed employee. Moreover, rouge APs make the entire network vulnerable to DoS attacks, packet captures, ARP poisoning and more.
- You can use network access controls and network access protocols or introduce authentication processes to protect your organization.

XVI. **Jamming**: Jamming (also known as network interference) aims to disrupt the network. Due to the wireless features, interference is almost unavoidable.
- A pair of Bluetooth headphones or even a microwave oven can cause mild interference. Most of the time, ill intended intruders combine jamming techniques with other methods like evil twinning.
- To protect an organization, you should invest in a spectrum analyser, boosting the power of existing access points or using different frequencies.

XVII. **Evil Twinning**: One of the most popular methods employed by wireless network attackers is creating an evil twin.
- In other words, attackers get a wireless access point and configure it as the existing network. This way, the 'evil' access point cannot be distinguished from actual access points.
- One of the easiest ways to stop evil twins from stealing the information of your organization is opting for data encryption, so that even if an intruder successfully creates an evil twin they cannot read your data.
- If you would like to learn more about how you can protect your organization from cyber attackers, contact us! We offer state of the art SIEM and SOAR solutions that will keep an organization safe from malicious attacks of all kinds.

14. Explain the attacks on Discuss in detail identity theft (ID theft).

- Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation.

15. Explain the public key certificate and its implications for certifying authorities. Explain the legal challenges in computer forensics.

Public Key Certificate

- In cryptography**, a public key certificate**, also known as a digital certificate or identity certificate, is an electronic document used to prove the validity of a public key.
- The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer).
- If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization.

- However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.

Legal challenges

- Digital evidence can be tampered easily, sometimes, even without any traces. It is common for modern computers to have multiple gigabyte sized disks. Seizing and freezing of digital evidence can no longer be accomplished just by burning a CD-ROM. Failure to freeze the evidence prior to opening files has invalidated critical evidence.
- There is also the problem of finding relevant evidence within massive amounts of data which is a daunting task. The real legal challenges involve the artificial limitations imposed by constitutional, statutory and procedural issues. There are many types of personnel involved in digital/computer forensics like technicians, policy makers, and professionals.
- Technicians have sound knowledge and skills to gather information from digital devices, understand software and hardware as well as networks. Policy makes establish forensics policies that reflect broad considerations. Professionals are the link between policy and execution who have extensive technical skills as well as good understanding of the legal procedures.

16. Discuss the phases in Computer forensics/Digital forensics in detail. Discuss in detail about the Botnets.

- **Phase I – First Response**
  - The action performed right after the occurrence of a security incident is known as the first response. It is highly dependent on the nature of the incident.

- **Phase II – Search and Seizure**
  - Under this phase, the professionals search for the devices involved in carrying out the crime. These devices then carefully seized to extract information out of them.

- **Phase III – Collect the Evidence**
  - After the search and seizure phase, professionals use the acquired devices to collect data. They have well-defined forensic methods for evidence handling.

- **Phase IV- Secure the Evidence**
  - The forensic staff should have access to a safe environment where they can secure the evidence. They determine if the collected data is accurate, authentic, and accessible.

- **Phase V – Data Acquisition**
  - Data acquisition is the process of retrieving Electronically Stored Information (ESI) from suspected digital assets. It helps to gain insights into the incident while an improper process can alter the data, thus, sacrificing the integrity of evidence.

- **Phase VI – Data Analysis**
  - Under data analysis, the accountable staff scan the acquired data to identify the evidential information that can be presented to the court. This phase is about examining, identifying, separating, converting, and modelling data to transform it into useful information.

- **Phase VII – Evidence Assessment**
  - The process of evidence assessment relates the evidential data to the security incident. There should be a thorough assessment based on the scope of the case.

- **Phase VIII – Documentation and Reporting**
  - This is a post-investigation phase that covers reporting and documenting of all the findings. Also, the report should have adequate and acceptable evidence in accordance to the court of law.

- **Phase IX – Testify as an Expert Witness**
  - The forensic investigators should approach the expert witness to affirm the accuracy of evidence. An expert witness is a professional who investigates the crime to retrieve evidence.

BOTNET

- A **botnet** (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot- herder."
- Each individual machine under the control of the bot-herder is known as a bot.
- Common botnet actions include:
  - Email spam– though email is seen today as an older vector for attack, spam botnets are some of the largest in size. They are primarily used for sending out spam messages, often including malware, in towering numbers from each bot.
  - The **Cutwail** botnet for example, can send up to 74 billion messages per day. They are also used to spread bots to recruit more computers to the botnet.

- **DDoS attack**: It leverages the massive scale of the botnet to overload a target network or server with requests, rendering it inaccessible to its intended users.
  - DDoS attacks target organizations for personal or political motives or to extort payment in exchange for ceasing the attack.

- **Financial breach**– includes botnets specifically designed for the direct theft of funds from enterprises and credit card information.

- Financial botnets, like the **ZeuS** botnet, have been responsible for attacks involving millions of dollars stolen directly from multiple enterprises over very short periods of time.

- **Targeted intrusions**: Smaller botnets designed to compromise specific high-value systems of organizations from which attackers can penetrate and intrude further into the network.
  - These intrusions are extremely dangerous to organizations as attackers specifically target their most valuable assets, including financial data, research and development, intellectual property, and customer information.

17. Discuss the SQL Injection in detail. What is buffer overflow? Discuss how to minimize Buffer Overflow.

- **SQL injection**, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.
  - This information may include any number of items, including sensitive company data, user lists or private customer details. The impact SQL injection can have on a business is far-reaching.
  - A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.
  - When calculating the potential cost of an SQLi, it's important to consider the loss of customer trust should personal information such as phone numbers, addresses, and credit card details be stolen.
  - While this vector can be used to attack any SQL database, websites are the most frequent targets.

- **Buffers** are memory storage regions that temporarily hold data while it is being transferred from one location to another.
  - A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
  - For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.
  - Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.
  - Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection.
  - In addition, modern operating systems have runtime protection. Three common protections are:
    - **Address space randomization (ASLR)—**randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
    - **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.

- **Structured exception handler overwrites protection (SEHOP)—**helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique.
- At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.
- Security measures in code and operating system protection are not enough. When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch.