Lecture 1

What is the difference between a closed policy and an open policy?

A closed policy assumes that everything is denied by default, while an open policy assumes that everything is allowed by default.

What is a file handle used for?

Answer

A file handle is an opaque identifier for a file or folder that is used to perform file operations such as opening, reading, writing, executing, and closing files.

What is the main advantage of decentralised access control administration?

It allows people closer to the resources to control access, which means changes can happen faster.

Question

What are some countermeasures for SQL injection attacks?

Some countermeasures for SQL injection attacks include defensive coding practices, parameterized query insertion, detection using signature-based, anomaly-based, or code analysis techniques, and run-time prevention.

What are the four fundamental goals of cryptography?

The four fundamental goals of cryptography are confidentiality, integrity, authentication, and non-repudiation.

What is the purpose of integrity in cryptosystems?

Answer

The purpose of integrity is to ensure that data is not altered without authorization, protect against all forms of alteration, and check if the received message is identical to the sent message.

What is a Distributed Denial of Service (DDoS) attack?

A DDoS attack is similar to a DoS attack but is carried out by multiple compromised systems that are coordinated to flood a target with traffic or requests.

What is the difference between a passive and an active attack?

Answer

A passive attack attempts to learn or make use of information from the system but does not affect system resources, while an active attack attempts to alter system resources or affect their operation.

What is a peer-to-peer network?

A peer-to-peer network is an example of a decentralized architecture where devices are connected directly to each other.

What is a protocol?

A protocol is a set of rules or conventions that dictate communication.

What is a security attack?

A security attack is any action that compromises the security of information owned by an organization.

What is a security breach?

A security breach is any event that results in a violation of any of the CIA security tenets.

How does a virus spread through a network environment?

A virus spreads through a network environment by infecting programs and replicating itself to other content.

What is a vulnerability?

Answer

A vulnerability is a flaw or weakness in an asset’s design, implementation, or operation and management that could be exploited by some threat.

Question

Give an example of a client/server architecture.

A website is an example of a client/server architecture.

What is an access control entry (ACE)?

An ACE is an entry that allows or denies a certain type of access to a file or folder by a user or group.

What is a security intrusion?

An unauthorized act of bypassing the security mechanisms of a system.

Who are APT attacks typically attributed to?

APT attacks are typically attributed to state-sponsored organizations and criminal enterprises.

What are the characteristics of an APT?

APTs are advanced, persistent, and pose a threat to the selected targets.

What is intrusion detection?

Answer

It is a hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions.

Why is it important to ensure that machine language corresponds to the algorithm?

It is important to ensure that machine language corresponds to the algorithm to prevent bugs that could be exploited.

What is the purpose of providing Internet security?

It is to protect against various threats and ensure the confidentiality, integrity, and availability of data.

What is IT security management?

Answer

IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability,

What is the aim of activist attacks?

The aim of their attacks is often to promote and publicize their cause, typically through website defacement, denial of service attacks, and theft and distribution of data that result

in negative publicity or compromise of their targets.

What are the components of a virus?

Answer

The components of a virus include the infection mechanism, trigger, and payload.

What is the concern associated with the dynamic memory allocation?

The concern associated with dynamic memory allocation is memory leak, which is the steady reduction in memory available on the heap to the point where it **it is completely exhausted.**

Question

How did the development of virus-creation toolkits in the early 1990s change the development and deployment of malware?

The development of virus-creation toolkits in the early 1990s greatly assisted in the development and deployment of malware, allowing even novices to deploy malware through a variety of propagation mechanisms and payload modules.

Question

What are the four possible flags in a TCP packet header?

The four possible flags in a TCP packet header are SYN (Synchronize), ACK (Acknowledge), FIN (Finished), and RST (Reset).

What are the goals of cryptography?

The goals of cryptography are to hide information from unauthorized individuals, make obtaining the information too work-intensive or time-consuming to be worthwhile to the attacker, and to ensure the integrity and authenticity of the information.

What is the intent of APT attacks?

The intent of APT attacks is to infect the target with sophisticated malware with multiple propagation mechanisms and payloads.

What are the IT security management functions?

The IT security management functions include: (1) determining organizational IT security objectives, strategies, and policies; (2) determining organizational IT security requirements; (3) identifying and analyzing security threats to IT assets within the organization; (4) identifying and analyzing risks; (5) specifying appropriate safeguards; (6) monitoring the implementation and operation of safeguards that are necessary to cost-effectively protect the information and services within the organization; (7) developing and implementing a security awareness program; and (8) detecting and reacting to incidents.

What is the OSI model?

The OSI model is a seven-layer model that describes a particular set of functions and behaviors for communication.

What is the Ping of Death attack?

The Ping of Death attack is a DoS attack that involves sending a ping packet that exceeds the maximum size using IP fragmentation. This can cause buffer overflows and crashes in some operating systems.

What is the principle of Complete Mediation?

The principle of Complete Mediation dictates that every access must be checked against the access control mechanism

What is the principle of Compromise Recording?

The principle of Compromise Recording states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent

What is the principle of Economy of Mechanism?

The principle of Economy of Mechanism states that security measures embodied in both hardware and software should be as simple and small as possible.

What is the principle of Fail-safe defaults?

The principle of Fail-safe defaults states that access decisions should be based on permission rather than exclusion—the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.

What is the principle of Least Common Mechanism?

The principle of Least Common Mechanism states that in systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized.

What is the principle of Least Privilege?

The principle of Least Privilege states that every process and every user of the system should operate using the least set of privileges necessary to perform the task.

What is the principle of Open Design?

The principle of Open Design states that the design of a security mechanism should be open rather than secret.

What is the principle of Psychological Acceptability?

The principle of Psychological Acceptability states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.

What is the principle of Separation of Privilege?

The principle of Separation of Privilege dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.

What is the principle of Work Factor?

The principle of Work Factor states that the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.

What is the purpose of a penetration test?

The purpose of a penetration test is to test the security of systems and architectures from the point of view of an attacker (hacker, cracker).

What is the purpose of an initial engagement in a penetration test?

The purpose of an initial engagement is to engage the external team to perform the penetration test.

What is the purpose of authentication in cryptosystems?

The purpose of authentication is to verify the claimed identity of system users.

What is the purpose of follow-up in a penetration test?

The purpose of follow-up is to verify that any vulnerabilities found during the penetration test have been remediated and to retest the systems and applications to ensure that they are secure.

What is the purpose of IT Security Management?

The purpose of IT Security Management is to ensure that critical assets are sufficiently protected in a cost-effective manner.

What is the purpose of non-repudiation in cryptosystems?

The purpose of non-repudiation is to provide assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender and prevent the sender from claiming that they never sent the message in the first place.

What is the purpose of reporting in a penetration test?

The purpose of reporting is to document the results of the penetration test and provide recommendations for remediation of any vulnerabilities found.

What is the purpose of scoping in a penetration test?

The purpose of scoping is to define the scope of the penetration test, including the systems and applications that will be tested and the types of tests that will be performed.

What is the purpose of testing in a penetration test?

The purpose of testing is to perform the penetration test and attempt to identify vulnerabilities in the systems and applications being tested.

What needs to be examined when addressing an organisation's IT security?

The role and importance of IT systems in the organization need to be examined.

How can a sender make it difficult to trace a packet back to an attacker in IP?

The sender can spoof the source address, making it difficult to trace the packet back to the attacker

What is the Smurf IP attack?

The Smurf IP attack is a DoS attack that involves sending ping requests to a broadcast address using a spoofed source address. This causes all hosts on the network to reply to the spoofed address, overwhelming it with traffic.

What are the three categories of vulnerabilities?

The three categories of vulnerabilities are corrupted (loss of integrity), leaky (loss of confidentiality), and unavailable or very slow (loss of availability).

What are the three concepts that form the CIA triad?

The three concepts are confidentiality, integrity, and availability.

What are the three questions that IT Security Management seeks to answer?

The three questions are: (1) What assets need to be protected? (2) How are those assets threatened? (3) What can be done to counter those threats?

What is the three-way handshake in TCP packet exchange?

The three-way handshake is a process used to initiate a TCP connection, where the initiating system sends a SYN packet to the destination, the destination sends an ACK to acknowledge receipt of the first packet (a combined SYN/ACK packet), and the initiating system sends an ACK packet to acknowledge receipt of the SYN/ACK packet. Data transfer can then begin.

What is the trigger of a virus?

The trigger is the event or condition that determines when the payload is activated or delivered, sometimes known as a logic bomb.

What are the two broad defence approaches to buffer overflow attacks?

The two broad defence approaches to buffer overflow attacks are compile-time, which harden programs to resist attacks in new programs, and run-time, which detect and abort attacks in existing programs.

What are the two types of data that need to be considered when developing a cryptographic system for confidentiality?

The two types of data are data at rest and data in motion.

What is the typical pattern of a penetration test engagement?

The typical pattern of a penetration test engagement is initial engagement, scoping, testing, reporting, and follow-up. There should be a severity rating for any issues found.

What is the underground economy in relation to malware?

The underground economy involves the sale of attack kits, access to compromised hosts, and stolen information.

What is an example of threats on a typical network?

These can include malware, viruses, phishing, denial of service attacks, and unauthorized access.

What is a script-kiddie?

They are hackers with minimal technical skill who primarily use existing attack toolkits.

Who are cyber criminals?

They are individuals or members of an organized crime group with a goal of financial reward.

What is the relative location of security facilities in the TCP/IP protocol stack?

They are located between the application layer and the network layer.

What are some approaches to providing Internet security?

They include using firewalls, encryption, intrusion detection/prevention systems, virtual private networks, and secure sockets layer/transport layer security.

What are the services that various security approaches provide in relation to the TCP/IP protocol stack?

They provide services such as confidentiality, integrity, authenticity, and non-repudiation.

What are some typical privileges included in an ACL in DAC?

Typical privileges include Read, Write, Update, Execute, Delete, or Rename.

What is the User Datagram Protocol (UDP)?

UDP is a lightweight and connectionless transport layer protocol that provides more control over when data is sent but does not compensate for loss of packets or deliver packets in order.

How can XSS attacks be prevented?

XSS attacks can be prevented by examining any user-supplied input and removing or escaping any dangerous code to block its execution.

What is an example of an attack kit?

Zeus and Angler are examples of attack kits.

How does NIST 800-83 define malware?

"A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim."

How does NCSC define malware?

"A term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals."

What is an application-level gateway?

Must have proxy code for each application. Tends to be more secure than packet filters

What is a blind hijack attack?

A blind hijack attack is an attack where an attacker injects data such as malicious commands into communications, but cannot see the response to that data.

What is a blind SQL injection attack?

A blind SQL injection attack is a type of inferential attack that allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker.

What is a botnet and what can it be used for?

A botnet is a collection of bots capable of acting in a coordinated manner. It can be used for distributed denial-of-service (DDoS) attacks, spamming, sniffing traffic, keylogging, spreading new malware, installing advertisement add-ons and browser helper objects (BHOs), attacking IRC chat networks, and manipulating online polls/games.

What is a buffer overflow attack?

A buffer overflow attack occurs when a program tries to store more data in a buffer than it can hold, causing the excess data to overflow into adjacent memory spaces and potentially allowing an attacker to execute malicious code.

What is a Caesar cipher?

A Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

What is the difference between a centralized and decentralized network architecture?

A centralized network architecture has a single, centralized entity that controls communication, while a decentralized network architecture has no centralized entity and allows devices to communicate directly with each other.

What is a distributed denial-of-service (DDoS) attack and how does it differ from a traditional DoS attack?

A DDoS attack is a type of DoS attack that uses multiple hosts to amplify the attack. Instead of overwhelming the target system with traffic or data from a single source, a DDoS attack uses a network of intermediary hosts to generate enough traffic to disrupt entire networks or server farms. This makes DDoS attacks much more difficult to detect and mitigate than traditional DoS attacks.

disrupt entire networks or server farms. This makes DDoS attacks much more difficult to detect and mitigate than traditional DoS attacks.

What is a denial of service attack?

A denial of service attack is a type of attack that aims to disrupt the availability of a service or resource by overwhelming it with traffic or other requests.

What is the difference between a DoS attack and a DDoS attack?

A DoS attack attempts to overwhelm a network connection for a targeted host through a more powerful host, while a DDoS attack uses multiple intermediary hosts to generate enough traffic to disrupt server farms or a whole network segment, and possibly beyond.

What is a denial-of-service (DoS) attack and how does it work?

A DoS attack is a type of cyber attack that aims to prevent legitimate users from accessing a system. This is typically done by flooding the target system with traffic or data, overwhelming its resources and causing it to crash or become unresponsive. This can be accomplished through a variety of techniques, including sending large numbers of packets to the target system, using IP source spoofing to hide the attacker's identity, or exploiting vulnerabilities in the system's software or hardware.

What is the purpose of a firewall in network security?

A firewall is used to monitor and control incoming and outgoing network traffic based on predetermined security rules.

What is a man-in-the-middle attack?

A man-in-the-middle (MiTM) attack is an attack where an attacker intercepts all communications between two hosts by positioning themselves so that communications between a client and server must flow through them.

What is a network?

A network is a set of technologies that connects computers, allowing communication and collaboration between users. It is a collection of computers and devices connected together.

What is a one-time pad?

A one-time pad is an extremely powerful type of substitution cipher that is made up of truly random values and used only one time.

What does a low interaction honeypot emulate?

A particular IT service or system well enough to provide a realistic initial interaction.

What is a passive attack?

A passive attack is an attempt to learn or make use of information from a system without affecting its resources.

How is a penetration test similar to a financial audit?

A penetration test is similar to a financial audit in that it verifies and tests the effectiveness of internal processes and systems in place. Just as a financial audit ensures that internal finance processes are sufficient, a penetration test ensures that internal security measures are effective.

What is a virus?

A piece of software that infects programs, modifies them to include a copy of the virus, replicates, and goes on to infect other content.

What is a buffer overflow?

A programming error when a process attempts to store data beyond the limits of a fixed-sized buffer. </h4>

What is a protocol?

protocol is a set of rules or conventions that dictate communication between two or more parties.

What is a risk register?

A risk register is a document that records the results of the risk analysis process.

What is a rootkit and why is it difficult to detect and remove?

A rootkit is a type of malware that modifies or replaces one or more existing programs to hide the fact that a computer has been compromised. It is difficult to detect and remove because it modifies parts of the operating system to conceal traces of its presence.

What is a rootkit?

A rootkit is a type of malware that provides continued privileged access to a computer while hiding its presence and actions from the operating system and antivirus software.

What is the purpose of a security mechanism?

A security mechanism is designed to detect, prevent, or recover from a security attack, in order to enhance the security of a system or organization.

What is a session theft attack?

A session theft attack is an attack where the attacker creates new sessions or utilizes old sessions to gain access to a system or application.

What is a remote exploit?

A software vulnerability in a network server that could be triggered by a remote attacker.

What is a local exploit?

A software vulnerability that can be exploited by an attacker to gain elevated privileges

What is a substitution cipher?

A substitution cipher is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

What is a TCP SYN Flood attack?

A TCP SYN Flood attack is a type of DoS attack where the attacker sends out a SYN packet to overflow the receiver's buffer.

What is a threat in the context of security risk assessment?

A threat is a potential for a threat source to exploit a vulnerability in some asset, which, if it occurs, may compromise the security of the asset and cause harm to the asset's owner.

What is a threat?

A threat is anything that could exploit a vulnerability to breach security and cause harm to an asset.

What is a UDP Flood attack?

A UDP Flood attack is a type of DoS attack where the attacker sends UDP packets to a random port, generating illegitimate packets that tie up system resources sending back packets.

What is a VPN and how does it work?

A VPN (virtual private network) is a secure connection between a user's device and a remote network over the internet. It works by encrypting traffic between the user's device and the VPN server, effectively creating a private tunnel through which data can be transmitted securely.

What is a vulnerability in the context of security risk assessment?

A vulnerability is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

What is the difference between a vulnerability scan and a penetration test?

A vulnerability scan is an automated process of identifying vulnerabilities in a system, whereas a penetration test is a manual process of attempting to exploit the identified vulnerabilities to assess the level of security of the system.

What is a worm and how does it spread?

A worm is a program that actively seeks out more machines to infect, and it spreads through network connections, shared media, email attachments, and instant messenger file transfers.

What are the five stages of a typical cyber attack?

A1: The five stages of a typical cyber attack are reconnaissance and footprinting, scanning and enumeration, gaining access, maintaining access, and covering tracks.

What is the goal of a penetration test?

The goal of a penetration test is to identify vulnerabilities in a system that may allow unauthorized access or other malicious activity and determine which flaws pose a threat to the application.

What are the phases of a model penetration test engagement?

The phases of a model penetration test engagement are initial engagement, scoping, testing, reporting, and follow up.

What is the purpose of initial engagement in a penetration test?

The purpose of initial engagement in a penetration test is to establish the goals, scope, and logistics of the test.

What is the purpose of scoping in a penetration test?

The purpose of scoping in a penetration test is to define the systems and components to be tested and the methods and tools to be used.

What is the purpose of testing in a penetration test?

The purpose of testing in a penetration test is to perform the actual testing of the systems and components according to the defined scope.

What is the purpose of reporting in a penetration test?

The purpose of reporting in a penetration test is to document the findings and vulnerabilities discovered during the testing and provide recommendations for remediation.

What is the purpose of follow up in a penetration test?

The purpose of follow up in a penetration test is to ensure that the identified vulnerabilities are remediated and to perform retesting to confirm that the remediation was effective.

Is penetration testing a guarantee of security?

No, penetration testing is not a guarantee of security.

Is penetration testing an alternative to other IT security measures?

No, penetration testing is not an alternative to other IT security measures but rather complements them.

What is the purpose of reconnaissance and footprinting?

The purpose of reconnaissance and footprinting is to gather information about a target network, including identifying network layouts, domains, servers, and infrastructure details.

What is the purpose of scanning and enumeration?

The purpose of scanning and enumeration is to find vulnerabilities and entry points in a target network.

What is the purpose of gaining access?

The purpose of gaining access is to break into a network and map the organization's defenses from the inside, creating a battle plan for information to target.

What is the purpose of maintaining access?

The purpose of maintaining access is to continue to access and control the target network, including conducting data exfiltration.

What is the purpose of covering tracks?

The purpose of covering tracks is to hide or delete any evidence of an attacker's access and actions in the target network.

What is whitebox testing?

Whitebox testing is a type of testing where full information about the target is shared with the testers, allowing them to confirm the efficacy of internal vulnerability assessment and management controls.

What is blackbox testing?

Blackbox testing is a type of testing where no information is shared with the testers about the internals of the target, forcing them to perform the testing from an external perspective.

What is access control and what does it prevent?

Access control is the process of protecting a resource so that it is used only by those allowed to use it. It prevents unauthorized use and puts mitigations in place to protect a resource from a threat.

What are some operating systems-based DAC policy considerations?

Access control method, new user registration, and periodic review are some operating systems-based DAC policy considerations.

What is accountability in access control?

Accountability in access control involves audit logs and monitoring to track subject activities with objects to ensure that the person who makes data or system changes can be identified.

What is the difference between act-alone malware and coordinated malware?

Act-alone malware runs on their own and have a specific target, while coordinated malware contributes to a larger-scale attack and can cause damage when multiple infected devices are used together.

What is active content and what are its potential weaknesses?

Active content refers to dynamic objects that do something when the user opens a webpage, and its potential weaknesses can be exploited by malware.

What is an Access Control List (ACL) in DAC?

An ACL is a list or a file of users who are given the privilege of access to a system or resource, such as a database. It contains a user ID and an associated privilege or set of privileges for that user and that resource.

What is an Access Control List (ACL)?

An ACL is a list or a file of users who are given the privilege of access to a system or resource. Within the file is a user ID and an associated privilege or set of privileges for that user and that resource.

What is an asset in the context of security risk assessment?

An asset is anything that needs to be protected because it has value to the organization and contributes to the successful attainment of the organization's objectives.

How does an attacker hijack a TCP session?

An attacker can hijack a TCP session by spoofing the client's IP address, determining the correct sequence number that the server is expecting from the client, and injecting data into the session before the client sends its next packet.

What is an XSS reflection vulnerability?

An attacker includes the malicious script content in data supplied to a site.

What is an intrusion prevention system (IPS)?

An extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. Can be host-based, network-based, or distributed/hybrid. Can use anomaly detection or signature/heuristic detection to identify known malicious behavior

Is Dhinuk a nonce?

Yes,all the time.

What is an inband attack?

An inband attack is an injection attack where code and results are transferred through the same channel.

What is an out-of-band attack?

An out-of-band attack is an injection attack where data is retrieved using a different channel than the one used for injection.

What are the two main approaches to IDS analysis? Anomaly detection and Signature/Heuristic detection

Anomaly detection and Signature/Heuristic detection.

What are some additional security controls that can be installed?

Anti-virus software, Host-based firewalls, IDS or IPS software and Application white-listing

What are some of the attacks suitable for Anomaly Detection?

Application layer reconnaissance and attacks, Transport layer reconnaissance and attacks, Network layer reconnaissance and attacks, Unexpected application services, and Policy violations.

What should be done during the system planning process?

Assess risks and plan the system deployment. Secure the underlying operating system and then the key applications. Ensure any critical content is secured. Ensure appropriate network protection mechanisms are used. Ensure appropriate processes are used to maintain security.

What are the key steps in the process of securing an operating system?

Assessing risks and planning system deployment. Securing the operating system and key applications. Ensuring critical content is secured. Using appropriate network protection mechanisms. Maintaining security through appropriate processes

What does non-repudiation provide in cryptosystems?

Assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender, and prevents the sender from claiming that they never sent the message in the first place.

What is a Cross Site Scripting (XSS) attack?

Attacks where input provided by one user is subsequently output to another user.

What is the difference between authentication and authorization?

Authentication is the process of verifying a user's identity, while authorization is the process of determining whether a user has permission to access a particular resource or perform a specific action.

What are the functions that are involved in access control?

Authentication, Authorization, and Accountability/Audit.

What is the difference between auto-spreading malware and user-activated malware?

Auto-spreading malware runs and looks for other vulnerable machines on the Internet, while user-activated malware is run on a computer only because a user accidentally downloads and executes it.

What is the initial critical step in writing more secure program code?

Awareness of the known areas of concern, such as the critical web application security flaws.

What are backdoors and rootkits, and what privileges do they give to attackers?

Backdoors are secret entry points into a program that allow the attacker to gain access and bypass security access procedures. Rootkits are sets of hidden programs installed on a system to maintain covert access to that system. They give administrator (or root) privileges to the attacker, allowing them to add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.

What are some examples of logical access control solutions?

Biometrics, Tokens, Passwords and Single Sign on solutions

What do browsers do to restrict data access in XSS attacks?

Browsers impose security checks and restrict data access to pages originating from the same site.

What are three errors related to risky resource management in the CWE/SANS list?

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), and Download of Code Without Integrity Check.

What is a host-based IPS (HIPS)?

Can make use of either signature/heuristic or anomaly detection techniques to identify attacks. Examples of the types of malicious behavior addressed by a HIPS include modification of system resources, privilege-escalation exploits, buffer-overflow exploits, etc.

What is the disadvantage of a packet filtering firewall?

Cannot prevent attacks that employ application specific vulnerabilities or functions, Limited logging functionality, Do not support advanced user authentication, Vulnerable to attacks on TCP/IP protocol bugs and Improper configuration can lead to breaches

What should be considered during the system planning process regarding users and groups?

Categories of users on the system, Privileges they have, Types of information they can access and How and where they are defined and authenticated

What is the definition of computer security as given in RFC 4949?

Computer security is defined as measures that implement and assure security services in a computer system, particularly those that assure access control service.

What are the three information security properties that malware can attack?

Confidentiality, Integrity, and Availability.

What are the two services provided by the TLS Record Protocol for TLS connections?

Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of TLS payloads. The message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported. Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC), which is similar to HMAC.

What is a personal firewall?

Controls traffic between a personal computer or workstation and the Internet or enterprise network. Typically much less complex than server-based or stand-alone firewalls. Primary role is to deny unauthorized remote access.

What can be the consequences of a buffer overflow?

Corruption of program data, unexpected transfer of control, memory access violations, execution of code chosen by the attacker.

What should be done during application configuration?

Creating and specifying appropriate data storage areas for application. Making appropriate changes to the application or service default configuration details.

Why is cryptography important?

Cryptography is important because it is an effective way of protecting sensitive information as it is stored on media or transmitted through untrusted network communication paths.

What is Discretionary access control (DAC)?

DAC controls access based on the identity of the requestor and access rules (authorizations) stating what requestors are (or are not) allowed to do.

What is data exfiltration in the cyber attack process?

Data exfiltration is the process of extracting data from the network using tools and techniques to simulate the actions of hackers.

What are honeypots?

Decoy systems designed to lure a potential attacker away from critical systems, collect information about the attacker's activity, and encourage the attacker to stay on the system long enough for administrators to respond.

What algorithms are used for encrypting S/MIME messages?

Default algorithms used for encrypting S/MIME messages are AES and RSA.

What are some default items that some applications or services may include?

Default data, scripts, and user accounts

What are some common forms of symmetric key block cipher cryptosystems?

DES and Triple-DES.

What are the three technical mechanisms that can be used for threat mitigation if prevention fails?

Detection, Identification and Removal

What is the most difficult design issue with sandbox analysis?

Determining how long to run each interpretation.

What are the two default policies of a packet filtering firewall?

Discard (Deny) and Forward (Permit)

What are the four types of Access Control Policies

Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC), and Attribute-based access control (ABAC).

What is DKIM?

DKIM stands for DomainKeys Identified Mail and is a specification of cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream.

What is DNS cache poisoning?

DNS cache poisoning is when an attacker gives DNS servers false records and gets them cached.

What is DNS hijacking?

DNS hijacking is when an attacker attempts to change the IP associated with a server maliciously.

What is the domain name system (DNS)?

DNS is an application-layer protocol for mapping domain names to IP addresses.

How can DNS cache poisoning be prevented?

DNS Security (DNSSEC) can be deployed to ensure the authenticity and integrity of DNS replies by signing DNS replies at each step of the way using public-key cryptography.

What is used to enforce message integrity in cryptosystems?

Encrypted message digests, known as digital signatures created upon transmission of a message.

What is the goal of security testing?

Ensure the previous security configuration steps are correctly implemented. Identify any possible vulnerabilities.

What is of particular concern with remotely accessed services such as Web and file transfer services?

Ensuring that most of the files can only be read, but not written, by the server.

How does ESP in tunnel mode encrypt and authenticate the IP packet?

ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.

What is ethical hacking?

Ethical hacking is the practice of testing the security of computer systems and networks using the same tools and techniques as malicious hackers, but with the permission and knowledge of the system owners to identify vulnerabilities and improve security.

What are the two approaches to classifying malware?

Focusing on how they spread or propagate through an information system environment to reach the desired target/s or considering all dimensions of malware in order to classify them.

What are the four ways in which an attacker can use malicious code to inflict harm?

Gaining administrative control of a system and using commands, sending commands directly to a system, using software programs that harm a system or make data unusable, or using legitimate remote administration tools and security probes to identify and exploit security vulnerabilities on a network.

How can an attacker exploit a buffer overflow?

Getting a shell that allows the attacker to execute arbitrary commands with high privileges.

What is the difference between Host-Based IDS (HIDS) and Network-Based IDS (NIDS)?

HIDS monitors a single host while NIDS monitors traffic at selected points on a network.

What are the dimensions of malware taxonomy used by NCSC?

Host dependent or independent, persistent or transient, where it installs itself (persistent malware only), how it is triggered, static or dynamically updated, and act alone or coordinated attack.

Why is HTTP basic authentication insecure?

HTTP basic authentication is insecure because full credentials pass over the wire and data is sent in the clear.

What is HTTP basic authentication?

HTTP basic authentication is the most basic authentication method where the authentication is based on the existence of an IP address. It is insecure as full credentials pass over the wire and data is sent in the clear.

What is IKE and what is its purpose?

IKE (Internet Key Exchange) is the key management portion of IPsec and involves the determination and distribution of secret keys.

What are some best practices for authentication by knowledge, such as using passwords or passphrases?

Implement account lockout policies to prevent brute-force attacks. Audit logon events to track authentication attempts and identify potential security breaches. Use strong passwords or passphrases that are difficult to guess.

Name three errors related to insecure interaction between components in the CWE/SANS list?

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), and Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

What is the difference between inband and out-of-band attacks?

In inband attacks, data are retrieved and presented directly in application web pages, whereas in out-of-band attacks, data are retrieved using a different channel.

What is the difference between independent malware and host-dependent malware?

Independent malware is a complete program that can run on its own once installed on a compromised machine and executed, whereas host-dependent malware requires a host program to run.

What are the two types of monitoring software used in perimeter scanning approaches?

Ingress monitors and egress monitors.

What are the steps involved in the system security planning process?

Initiation, Development, Implementation, Maintenance

What is a network-based IPS (NIPS)?

Inline NIDS with the authority to modify or discard packets and tear down TCP connections. Makes use of signature and anomaly detection. Methods used to identify malicious packets include protocol anomaly, signature-based detection, heuristic-based detection, and stateful protocol analysis.

What are the three categories in which the errors in the CWE/SANS list are grouped?

Insecure interaction between components, risky resource management, and porous defenses.

What are the three categories of errors in the CWE/SANS Top 25 Most Dangerous Software Errors list?

Insecure interaction between components, risky resource management, and porous defenses.

What are some ways to secure the base operating system?

Installing and patching the operating system, Removing unnecessary services, applications, and protocols. Configuring users, groups, and permissions, Configuring resource controls. Configuring resource controls. Testing the controls

How can IPsec be used to enhance electronic commerce security?

IPsec can be used to secure remote access over the Internet, establish extranet and intranet connectivity with partners, and enhance electronic commerce security.

What is the scope of IPsec?

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

What is the purpose of IPsec?

IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet.

Why is sandbox analysis useful for malware detection?

It allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system.

What can a virus do when attached to an executable program?

It can do anything that the program is permitted to do, and executes secretly when the host program is run.

What is the consequence of insufficient checking and validation of data and error codes in programs?

It can lead to critical web application security flaws.

What is the purpose of Distributed or Hybrid IDS?

It combines information from multiple sensors, both host and network-based, to better identify and respond to intrusion activity.

What is a drive-by download attack?

It exploits browser and plugin vulnerabilities to download and install malware on the system without the user's knowledge or consent.

What is a boot sector infector virus?

It infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

What is host-based behaviour-blocking software?

It integrates with the operating system of a host computer and monitors program behavior in real time for malicious action.

What is Signature Detection?

It involves matching a large collection of known patterns of malicious data against data stored on a system or in transit over a network.

What is Rule-based Heuristic Identification?

It involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.

What is the Advanced Encryption Standard (AES)?

It is a block cipher that works on 128-bit blocks and can have one of three key sizes of 128, 192, or 256 bits. It is now the most widely used symmetric key algorithm.

What is the CWE/SANS Top 25 Most Dangerous Software Errors list?

It is a list of poor programming practices that are the cause of the majority of cyber attacks.

What is defensive programming?

It is a programming practice that requires programmers to validate program assumptions and handle potential failures safely and gracefully.

What does a high interaction honeypot entail?

It is a real system with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers, and may occupy an attacker for an extended period.

What is a Denial-of-Service attack?

It is a type of attack that attempts to prevent legitimate users from accessing a system.

What is a polymorphic virus?

It is a virus that mutates with every infection.

What is buffer overflow?

It is a vulnerability that occurs when a program allocates insufficient space for input, causing data to overwrite adjacent memory locations.

What is clickjacking?

It is a vulnerability used by an attacker to collect an infected user's clicks and trick them into performing unintended actions.

What is security by design?

It is an approach to software development that emphasizes designing software with security in mind.

What is the infection mechanism of a virus?

It is the means by which a virus spreads or propagates, also referred to as the infection vector.

What is Single Sign-On (SSO)?

It is the process of signing on to a computer or network once, and using identification and authorization credentials to access all computers and systems where authorized.

What is the payload of a virus?

It is what the virus does besides spreading, which may involve damage or benign but noticeable activity.

What is the danger in failure to validate input interpretation?

It may result in an exploitable vulnerability.

What is malvertising?

It places malware on websites without actually compromising them, by paying for advertisements that incorporate malware.

What is the importance of the CWE/SANS Top 25 Most Dangerous Software Errors list?

It provides a consensus view on the poor programming practices that cause the majority of cyber attacks and serves as a reference for developers to write more secure program code.

What is the disadvantage of SPA?

It requires high resource usage.

What is a chroot jail?

It restricts the server's view of the file system to just a specified portion, confining a process by mapping the root of the file system to some other directory.

What is IT security management, and what questions does it answer?

IT security management is a formal process of protecting critical assets in a cost-effective manner. It answers the questions of what assets need to be protected, how are those assets threatened, and what can be done to counter those threats.

What was the 2014 Heartbleed OpenSSL bug, and what caused it?

It was a vulnerability that allowed attackers to access sensitive information, and it was caused by a failure to check the validity of a binary input value.

What is logical access control?

Logical access control involves deciding which users can get into a system, monitoring what each user does on that system, and restraining or influencing a user's behavior on that system.

What is Mandatory access control (MAC)?

MAC controls access based on comparing security labels with security clearances.

What are the limitations of host-based behaviour-blocking software?

Malicious code can cause harm before it has been detected and blocked.

What is malware and how can it be prevented?

Malware is any software designed to harm or exploit a computer system or network. It can be prevented by using antivirus and anti-malware software, keeping software and operating systems up to date, avoiding suspicious downloads and links, and using strong passwords.

What are the different types of payloads that malware can carry out?

Malware payloads can include system corruption, attack agents (bots), remote control facility, information theft (keyloggers and spyware), phishing, stealthing (backdoor and rootkit).

What is the purpose of MIME?

MIME is an extension to the old RFC 822 specification for mail format and provides a number of new header fields that define information about the body of the message.

What are two errors related to porous defenses in the CWE/SANS list?

Missing Authentication for Critical Function and Missing Authorization.

What are some key components of security maintenance?

Monitoring and analyzing logging information. Performing regular backups. Recovering from security compromises. Regularly testing system security. Patching and updating critical software. Monitoring and revising configuration as needed

Which access control principle do most of the common operating systems on the market today rely on?

Most of the common operating systems on the market today (Windows, Macintosh, UNIX, and others) rely on DAC principles for access and operation.

What should be considered when evaluating human threat sources in security risk assessment?

Motivation, capability, resources, probability of attack, and deterrence should be considered when evaluating human threat sources.

What is NIST's definition of cloud computing?

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

What is Non-Discretionary Access Control?

Non-Discretionary Access Control is an access control model in which access rules are closely managed by security administrators, not system owners or ordinary users.

What is packet sniffing?

Packet sniffing is a technique used to capture and monitor network traffic, even those not meant for the listener, by setting the network interface card into promiscuous mode.

What are some key components of Linux/Unix security?

Patch management. Application and service configuration. Users, groups, and permissions. Chroot jail

How does penetration testing help in ensuring system security?

Penetration testing helps in identifying vulnerabilities in the system that can be exploited by attackers, and helps in determining the effectiveness of security measures in place.

What is penetration testing?

Penetration testing is a method of testing the security of IT systems by attempting to breach the security of the system, using the same tools and techniques as an adversary might.

What is the difference between persistent malware and transient malware?

Persistent malware is installed in persistent storage, while transient malware is installed in volatile memory such as RAM.

What is phishing and how does it exploit social engineering?

Phishing is a type of information theft that exploits social engineering by masquerading as communication from a trusted source to trick the user into revealing sensitive information such as login credentials. It can be done through spam emails, fake websites, or spear-phishing.

What is phishing and how can it be prevented?

Phishing is a type of social engineering attack where attackers attempt to trick users into divulging sensitive information such as login credentials or financial data. It can be prevented by educating users on how to identify and avoid phishing emails, using spam filters and anti-phishing software, and implementing multi-factor authentication.

What is the difference between physical and logical access control?

Physical access control restricts access to physical resources such as doors, elevators, and parking lots using smart cards or similar technologies. Logical access control, on the other hand, focuses on managing access to computer systems and applications, monitoring user activity, and restraining user behavior.

What are the four main elements of prevention for malware?

Policy, Awareness, Vulnerability mitigation, and Threat mitigation

What is the ideal solution to the threat of malware?

Prevention

Why is privileged access necessary for maintaining access in the cyber attack process?

Privileged access is necessary for maintaining access because it allows the attackers to move freely within the environment and gain control over the network.

What is ransomware and what tactics does it use to pressure victims to pay the ransom?

Ransomware is malware that encrypts a large number of files and demands a ransom payment in Bitcoin to recover them. It may threaten to publish sensitive personal information or permanently destroy the encryption key after a short period of time to increase the pressure on the victim to pay up.

What is Role-based access control (RBAC)?

RBAC controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

How does Rule-Based Access Control (RBAC) work?

RBAC uses specific rules that indicate what can and cannot happen between a subject and an object, and before a subject can access an object in a certain circumstance, it must meet a set of predefined rules.

What is risk?

Risk is the potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset’s owner.

What is RSA?

RSA (Rivest-Shamir-Adleman) is a public key cryptosystem.

What is sandbox analysis?

Running potentially malicious code in an emulated sandbox or on a virtual machine

What are the functions provided by S/MIME?

S/MIME provides the ability to sign and/or encrypt e-mail messages.

What is S/MIME?

S/MIME stands for Secure/Multipurpose Internet Mail Extension and is a security enhancement to the MIME Internet e-mail format.

What is the difference between scanning and enumeration in the cyber attack process?

Scanning involves identifying entry points by scanning the organization's network, while enumeration involves actively counting vulnerabilities and assessing potential attacks and threats to the target system.

In which type of web applications are XSS attacks commonly seen?

Scripted web applications.

What is second-order injection?

Second-order injection is a type of injection attack where a malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself.

What is the first critical step in securing a system?

Securing the base operating system

What is the first critical step in securing a system?

Securing the base operating system.

What is a major security concern when augmenting or replacing on-premises systems with cloud services?

Security is a major concern when augmenting or replacing on-premises systems with cloud services.

What is the final step in the process of initially securing the base operating system?

Security testing

What should be done following the initial hardening of the system?

Security testing.

What are the three logical components of an Intrusion Detection System (IDS)?

Sensors, Analysers, and User Interface.

What are the three components of NIDS?

Sensors, Management servers, and Management consoles.

What is the difference between session hijacking and session theft attacks?

Session hijacking involves an attacker taking control of or modifying any communications between two hosts, whereas session theft attacks involve an attacker creating new sessions or utilizing old sessions without intercepting or injecting data into existing communications.

What is session hijacking?

Session hijacking is an attack where an attacker takes control of or modifies any communications between two hosts.

What is a circuit-level gateway?

Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host. Relays TCP segments from one connection to the other without examining contents. Typically used when inside users are trusted

What is the advantage of a packet filtering firewall?

Simplicity, Typically transparent to users and are very fast

What is social engineering and how can it be prevented?

Social engineering is the use of deception or manipulation to gain access to sensitive information or systems. It can be prevented by educating users on how to identify and avoid social engineering tactics, implementing security protocols such as multi-factor authentication, and conducting regular security awareness training.

What is the difference between software security, quality, and reliability?

Software quality and reliability are concerned with the accidental failure of program, while software security is triggered by inputs different from what is usually expected.

What is the concern of software security?

Software security is concerned with inputs that are different from what is usually expected.

What are some advantages of Mandatory Access Control (MAC)?

Some advantages of MAC include stronger security than DAC, the ability to determine the level of restriction by how sensitive the resource is (classification label), and temporal isolation/time-of-day restrictions.

What distinguishes SPA from other anomaly detection techniques?

SPA is trained with universal vendor-supplied profiles of benign protocol traffic rather than organization-specific traffic protocols.

What does SPA track to ensure that they progress as expected?

SPA tracks network, transport, and application protocol states.

What is SQL injection?

SQL injection is a type of injection attack that sends malicious SQL commands to the database server to exploit the nature of web application pages.

What is Secure Shell (SSH)?

SSH is a protocol for secure network communications designed to be relatively simple and inexpensive to implement.

What is SSL/TLS, and what are its two implementation choices?

SSL/TLS is one of the most widely used security services. It is a general-purpose service implemented as a set of protocols that rely on TCP. The two implementation choices are: Provided as part of the underlying protocol suite and/or Embedded in specific packages.

What are the three classification approaches used in Anomaly Detection?

Statistical, Knowledge-based, and Machine-learning.

What is steganography?

Steganography is a method of hiding data in another media type so the very existence of the data is concealed.

Why is steganography considered a type of security through obscurity?

Steganography is considered a type of security through obscurity because the message is hidden in a graphic, wave file, document, or other type of media and only the sender and receiver are supposed to be able to see the message.

What approach can be used to improve software quality and reliability?

Structured design and testing can be used to identify and eliminate as many bugs as possible from a program to improve software quality and reliability.

What is Stateful Protocol Analysis (SPA)?

Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic.

What is the difference between supportive and preventative controls?

Supportive controls are pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls. Preventative controls, on the other hand, focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.

What is the difference between symmetric and asymmetric encryption?

Symmetric encryption uses a single key to encrypt and decrypt data, while asymmetric encryption uses a public key to encrypt data and a private key to decrypt data.

What are some examples of authentication by ownership?

Synchronous tokens, which calculate a number at both the authentication server and the device using time-based or event-based synchronization systems. Asynchronous tokens, such as USB tokens, smart cards, or memory cards, that require the user to physically possess the token to authenticate their identity.

What is a bastion host?

System identified as a critical strong point in the network's security. Serves as a platform for an application-level or circuit-level gateway. Has common characteristics: runs secure O/S, only essential services, requires user authentication, etc.

How does tautology injection work in inband attacks?

Tautology injection in inband attacks injects code in one or more conditional statements so that they always evaluate to true.

What protocols are commonly used for network-level session hijacking attacks?

TCP and UDP are commonly used for network-level session hijacking attacks.

Why may testing fail to identify buffer overflow vulnerabilities?

Test inputs are unlikely to include large enough inputs to trigger the overflow.

What does integrity ensure in cryptosystems?

That data is not altered without authorization.

What is the Alert Protocol used for in TLS?

The Alert Protocol is used to convey messages regarding the session or connection that require action from the peer entity. It can be used to signal that an error occurred or to close the connection.

What are the factors that contribute to the strength of an encryption method?

The algorithm, the secrecy of the key, the length of the key, the initialization vectors, and how they all work together within the cryptosystem are the factors that contribute to the strength of an encryption method.

What is the assumption exploited in XSS attacks?

The assumption that all content from one site is equally trusted and hence is permitted to interact with other content from the site.

What is the authentication-only function of IPsec and why is it included in IPsecv3?

The authentication-only function is implemented using an Authentication Header (AH) and is included in IPsecv3 for backward compatibility, but should not be used in new applications because message authentication is provided by ESP.

What is the basic idea behind a man-in-the-middle attack?

The basic idea behind a man-in-the-middle attack is that an attacker intercepts all communications between two hosts, positioning themselves so that communications between a client and server must flow through them, which allows them to modify the communications.

What is the combined approach to security risk assessment?

The combined approach combines elements of the baseline, informal, and detailed risk analysis approaches to provide reasonable levels of protection as quickly as possible.

What is the concern of software quality and reliability?

The concern of software quality and reliability is the accidental failure of the program due to some theoretically random, unanticipated input, system interaction, or use of incorrect code.

What is the purpose of the Data Link layer in the OSI model?

The Data Link layer is responsible for formatting the data to be sent out on the transmission medium. Media Access Control (MAC) address is a layer 2 addressing. It identifies the network interface on the network so communications can get from one system to another on the local network.

What are the different methods of target discovery during the propagation phase?

The different methods of target discovery during the propagation phase include scanning, random, hit-list, topological, and local subnet.

What is the first step in the risk assessment process?

The first step is to establish the context, which includes determining the basic parameters of the risk assessment, identifying the assets to be examined, and exploring the political and social environment in which the organization operates.

What are the five classifications of rootkits based on their characteristics?

The five classifications of rootkits are persistent, memory-based, user mode, kernel mode, and external mode.

What are the five essential characteristics of the cloud computing model?

The five essential characteristics of the cloud computing model are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

What are the five layers of the secure IoT framework?

The five layers of the secure IoT framework are perception layer, transport layer, network layer, platform layer, and application layer.

What are the four components of access control?

The four components of access control are identification, authentication, authorization, and accountability.

What are the four deployment models of cloud computing?

The four deployment models of cloud computing are private, community, public, and hybrid.

What are the functions of IT security management?

The functions of IT security management include determining organizational IT security objectives, strategies, and policies; identifying and analyzing security threats to IT assets; specifying appropriate safeguards; monitoring the implementation and operation of safeguards; developing and implementing a security awareness program; and detecting and reacting to incidents.

What is the goal of a blind SQL injection?

The goal of a blind SQL injection is to allow attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker.

What is the goal of blackbox testing?

The goal of blackbox testing is to identify ways to access an organization's internal IT assets without sharing any information about the internals of the target with the testers.

What is the goal of penetration testing?

The goal of penetration testing is to identify and exploit vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.

What is the goal of the baseline approach to security risk assessment?

The goal of the baseline approach is to implement agreed controls to provide protection against the most common threats and forms a good base for further security measures.

What is the goal of the baseline approach to security risk assessment?

The goal of the baseline approach is to implement agreed controls to provide protection against the most common threats.

What is the goal of the gaining access phase in the cyber attack process?

The goal of the gaining access phase is to exploit vulnerabilities in a system and gain unauthorized access or conduct other malicious activities.

What is the vulnerability involved in XSS attacks?

The inclusion of script code in the HTML content.

What is the difference between the Internet layer and the Network layer in the TCP/IP model?

The Internet layer is responsible for addressing and routing packets across multiple networks, while the Network layer is responsible for managing communication within a single network.

What are the IoT gateway security functions?

The IoT gateway security functions include data acquisition and analysis, device and network management, protocol conversion, and security and privacy protection.

What is the ISO/IEC 27000 series of standards on IT security techniques?

The ISO/IEC 27000 series of standards is a set of guidelines for IT security management.

What is the main difference between Mandatory Access Control (MAC) and Discretionary Access Control (DAC)?

The main difference is that DAC allows the information owner to decide who gets to access the system(s), while MAC is determined by the sensitivity of the resource (classification label) and the system and owner make the decision to allow access.

What is the Mirai botnet attack?

The Mirai botnet attack is a DDoS attack that infected cameras, printers, routers, and thousands of other devices with the Mirai botnet malware. It generated an average of 1 Terabit per second, causing widespread disruption to websites and services.

What is the Mirai botnet and how did it enable DDoS attacks on a massive scale?

The Mirai botnet is a type of malware that targets Internet of Things (IoT) devices, such as IP CCTV cameras and routers. Once infected, these devices become part of a network of "zombie" hosts that can be controlled remotely by the attacker. This allows the attacker to launch DDoS attacks on a massive scale, using thousands or even millions of zombie hosts to flood the target system with traffic. The Mirai botnet was responsible for some of the largest DDoS attacks in history, including a 1 terabit per second attack in 2016.

What is the most common goal of an SQL injection attack?

The most common goal of an SQL injection attack is the bulk extraction of data.

What is the purpose of the Network layer in the OSI model?

The Network layer gets messages from one endpoint to another. It takes care of addressing and routing. The IP is one protocol that exists at this layer.

What is the objective of the NIST cloud computing reference architecture?

The objective of the NIST cloud computing reference architecture is to provide a technical reference for CSCs to understand, discuss, categorize, and compare cloud services, facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations, and illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model.

What should be the basis for developing a firewall access policy?

The organization's information security risk assessment and policy.

What is the OSI model and how many layers does it have?

The OSI (Open Systems Interconnection) model is a conceptual framework for understanding how communication systems operate. It has seven layers.

What is the OSI model?

The OSI model is a conceptual model that describes the layers of communication in a network, with each layer performing a specific set of functions.

What is the payload of a virus?

The payload is what the virus does besides spreading, which may involve damage or benign but noticeable activity.

What are the phases of a computer virus?

The phases of a computer virus include propagation, triggering, delivery, and execution.

What is the purpose of the Physical layer in the OSI model?

The Physical layer is responsible for managing the physical communications.

What is the policy definition phase of access control?

The policy definition phase of access control determines who has access and what systems or resources they can use. It is tied to the authorization phase.

What is the policy enforcement phase of access control?

The policy enforcement phase of access control grants or rejects requests for access based on the authorizations defined in the first phase. It is tied to the identification, authentication, and accountability phases.

What algorithms are used for signing S/MIME messages?

The preferred algorithms used for signing S/MIME messages use either an RSA or a DSA signature of a SHA-256 message hash.

What is the primary purpose of HIDS?

The primary purpose of HIDS is to detect intrusions, log suspicious events, and send alerts.

What is the principle behind Attribute-based Access Control (ABAC)?

The principle behind ABAC is that access is controlled based on attributes of the user, the resource to be accessed, and current environmental conditions.

What is the principle behind Role-based Access Control (RBAC)?

The principle behind RBAC is that access is controlled based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

What is the principle of Discretionary Access Control (DAC)?

The principle of DAC dictates that the information owner is the one who decides who gets to access the system(s).

What is the process for generating a digital signature in S/MIME?

The process involves taking the message, mapping it into a fixed-length code of 256 bits using SHA-256, encrypting the digest using RSA and the sender's private RSA key, and attaching the result to the message.

What is the purpose of a penetration test?

The purpose of a penetration test is to evaluate the security of a system by simulating an attack on the system to identify vulnerabilities and weaknesses that can be exploited by attackers.

What is the purpose of blackbox testing?

The purpose of blackbox testing is to identify ways to access an organization's internal IT assets from an external perspective.

What is the purpose of browser cache in HTTP basic authentication?

The purpose of browser cache in HTTP basic authentication is to store the user's credentials for a period of time, allowing them to authenticate without having to enter their credentials every time.

What is the purpose of covering tracks in the cyber attack process?

The purpose of covering tracks is to hide or delete any evidence of unauthorized access or malicious activity and ensure continued access without being detected.

What is the purpose of detection and recovery controls?

The purpose of detection and recovery controls is to focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

What is the purpose of DKIM in e-mail?

The purpose of DKIM is to permit a signing domain to claim responsibility for a message in the mail stream.

What is the purpose of management controls?

The purpose of management controls is to focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization’s mission.

What is the purpose of reconnaissance in the cyber attack process?

The purpose of reconnaissance is to gather information about the target, such as network layouts, domains, servers, and infrastructure details, to understand how the network works and identify potential entry points.

What is the purpose of whitebox testing?

The purpose of whitebox testing is to confirm the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organization's systems.

What is the security kernel?

The security kernel is a central point of access control that enforces access control for computer systems. It implements the reference monitor concept.

What is the security kernel, and what is its role in access control?

The security kernel is the central point of access control for computer systems. It enforces access control policies by intercepting access requests from users, checking them against a rules base or security kernel database, and allowing or denying access based on the defined access rules. It also logs all access requests for later tracking and analysis.

what are the three security operation principles all access control models are built on?

The security operation principles are Need to know, Least privilege, and Separation of duties and responsibilities.

What are the security requirements for the IoT according to ITU-T Recommendation Y.2066?

The security requirements for the IoT according to ITU-T Recommendation Y.2066 are communication security, data management security, service provision security, integration of security policies and techniques, mutual authentication and authorization, and security audit.

What are the services provided by IPsec?

The services provided by IPsec include access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality (encryption), and limited traffic flow (confidentiality).

How does the strength of an encryption method correlate to the amount of necessary processing power, resources, and time required to break the cryptosystem or to figure out the value of the key?

The strength of an encryption method correlates to the amount of necessary processing power, resources, and time required to break the cryptosystem or to figure out the value of the key.

What is the TCP/IP model?

The TCP/IP model is a simpler and more streamlined version of the OSI model, with four layers that describe the functions of a network.

What are the three categories of security controls?

The three categories of security controls are management controls, operational controls, and technical controls.

What are the three categories of session hijacking attacks?

The three categories of session hijacking attacks are man-in-the-middle attacks, blind hijack attacks, and session theft attacks.

The three main types of access control models are Discretionary, Mandatory, and Rule-Based.

What are the three risk likelihood categories used in risk analysis?

The three risk likelihood categories used in risk analysis are high, medium, and low.

What are the three service models of cloud computing?

The three service models of cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

What are the three types of resource records stored in DNS?

The three types of resource records stored in DNS are Address (A) record, Mail exchange (MX) record, and Name server (NS) record.

How does the TLS Handshake Protocol work?

The TLS Handshake Protocol comprises a series of messages exchanged by the client and server. The exchange has four phases: 1. Establish security capabilities 2. Server authentication and key exchange. 3. Client authentication and key exchange 4. Finish

What is the TLS Handshake Protocol, and what is its purpose?

The TLS Handshake Protocol is the most complex part of TLS. It is used before any application data is transmitted. Its purpose is to allow the server and client to authenticate each other, negotiate encryption and MAC algorithms, and negotiate cryptographic keys to be used. The handshake comprises a series of messages by the client and server, and the exchange has four phases.

What are the four protocols defined in TLS?

The TLS Record Protocol provides basic security services to various higher-layer protocols. Three higher-layer protocols are defined as part of TLS: The Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol. A fourth protocol, the Heartbeat Protocol, is defined in a separate RFC.

What are the TLS session and the TLS connection, and how are they related?

The TLS session is created by the Handshake Protocol and defines a set of cryptographic parameters. It is used to avoid the expensive negotiation of new security parameters for each connection. The TLS connection is a transport layer protocol that provides a suitable type of service. Every connection is associated with one session.

What are the top cloud-specific security threats listed by the Cloud Security Alliance?

The top cloud-specific security threats listed by the Cloud Security Alliance are abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, and account or service hijacking.

What is the purpose of the Transport layer in the OSI and TCP/IP models?

The Transport layer is responsible for segmenting messages for transmission and ensuring reliable communication between endpoints.

What is the purpose of the Transport layer in the OSI model?

The Transport layer takes care of segmenting messages for transmission. Both the TCP and the UDP are transport protocols. These protocols use ports for addressing, so receiving systems know which application to pass the traffic to.

What is the trigger of a virus?

The trigger is the event or condition that determines when the payload is activated or delivered, sometimes known as a logic bomb.

What are the two basic types of ciphers?

The two basic types of ciphers are stream ciphers and block ciphers.

What are the two components needed to create a risk to an asset?

The two components needed to create a risk to an asset are a threat and a vulnerability

What are the two main functions of IPsec?

The two main functions of IPsec are a combined authentication/encryption function called Encapsulating Security Payload (ESP) and a key exchange function.

What are the two risk consequence categories used in risk analysis?

The two risk consequence categories used in risk analysis are impact and likelihood.

What are the two types of penetration testing?

The two types of penetration testing are whitebox testing, where full information about the target is shared with the testers, and blackbox testing, where no information is shared with the testers about the internals of the target.

What are the three independent dimensions of a cryptographic system?

The type of operations used for transforming plaintext to ciphertext, the number of keys used, and the way in which the plaintext is processed are the three independent dimensions of a cryptographic system.

What are the types of penetration testing?

The types of penetration testing are whitebox testing and blackbox testing

What is the ultimate plan for any security practitioner in terms of securing all assets of their organization?

The ultimate plan is to secure all assets of the organization.

What is the World Wide Web, and how does it run over the Internet?

The World Wide Web is a client/server application running over the Internet and TCP/IP intranets.

How are smart cards used in physical access control?

They are programmed with an ID number and used to control access to physical resources such as parking lots, elevators, and office doors.

Why are macro and scripting viruses threatening?

They infect user documents rather than system programs, making traditional file system access controls of limited use in preventing their spread, and are much easier to write or modify than traditional executable viruses.

What is the role of software developers in addressing the known areas of concern related to insecure software code?

What information is typically logged by a NIDS sensor
What information is typically logged by a NIDS sensor?

Timestamp, connection/session ID, event/alert type, rating, network/transport/application layer protocols, source/destination IP addresses, source/destination TCP or UDP ports or ICMP types and codes, number of bytes transmitted over the connection, and decoded payload data such as application requests and responses.

What is the purpose of a firewall?

To establish a controlled link between a premises network and the Internet and to protect LANs.

What is the purpose of logging?

To provide a record of system activity for security monitoring and analysis.

What is the difference between transport mode and tunnel mode in IPsec?

Transport mode provides protection primarily for upper-layer protocols, while tunnel mode provides protection to the entire IP packet.

What is UDP and what are some of its characteristics?

UDP is a transport layer protocol that is lightweight and connectionless, with small packet sizes and no connection to create and maintain. It provides more control over when data is sent but does not compensate for loss of packet or deliver packets in order, and does not check if the network is busy.

What are the privacy issues in biometrics?

Unauthorized access to biometric data can lead to misuse as it is intrinsic to people and digitally recorded and stored.

Name three critical web application security flaws related to insecure software code?

Unvalidated input, Injection flaws, and Cross-site scripting

What is one of the most common failings in software security?

Unvalidated input.

What is User Provisioning?

User Provisioning is the process of granting access to new employees, which may include checking management approvals for granting access.

What is User Provisioning in DAC?

User Provisioning is the process of granting access to new employees. It may include checking management approvals for granting access.

What does authentication do in cryptosystems?

Verifies the claimed identity of system users.

How does the security kernel enforce access control?

When a subject requests access to an object, the security kernel intercepts the request and refers to its rules base or security kernel database to determine access rights. Access rights are set according to the policies an organization has defined. The kernel then allows or denies access based on the defined access rules, and all access requests handled by the system are logged for later tracking and analysis.

What are the benefits of implementing IPsec in a firewall or router?

When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

What is whitebox testing?

Whitebox testing is a type of testing in which full information about the target is shared with the testers.

What are some characteristics of worms?

Worms are multiplatform, multi-exploit, ultrafast spreading, polymorphic, metamorphic, and can exploit zero-day vulnerabilities.

What is port scanning and what are some common scanning techniques?

Port scanning is an essential step in the reconnaissance phase. Some common scanning techniques include ping scans, connect scans, SYN scans, and FIN scans.

YES WE ARE DONE. Aritha out, gnight.

With Love Signing off Ala Allanna Epa
Lesssgoooooooooo