QBank Quiz Domain 2

Test ID: 178834677

Question #1 of 51

Question ID: 1322923

Which operation has as its goal the identification of all available services on a device?

A) banner grabbing

B) port scan

C) ping scan

D) OS fingerprinting

Explanation

A port scan identifies the open ports on a device, and thus the services available.

A ping scan has as its goal the identification of all live devices in the network. A smurf attack is an attack where a ping request is sent to a broadcast network address with the aim of overwhelming the system.

Operating system (OS) fingerprinting has as its goal the identification of the operating system and version. Banner grabbing is a fingerprinting technique that relies on morphed or empty TCP packets that are sent over to a target machine. Telnet, Netcat, Nmap and other tools can be used to carry out banner grabbing.

Banner grabbing also has as its goal the identification of the operating system and its version. Banner grabbing intercepts a text file sent by a server or a host. The text file includes OS information and in the case of a web server, perhaps the basic configuration info. The attacker can then exploit that information.

Objective:
Security Monitoring

Sub-Objective:
Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

References:

Lifewire > Introduction to Port Scanning

Question #2 of 51

Question ID: 1322911

How does a rogue switch become the root bridge?

A) by sending an inferior BPDU

B) by sending a superior BPDU

C) by sending an ARP broadcast

D) by sending a jam signal

Explanation

Switches in a Spanning Tree Protocol (STP) topology use bridge protocol data unit (BPDU) values to elect the root bridge. If the rogue switch sends a BPDU with a better value than the current root bridge, it will assume the role of root bridge.

Switching loops occur when multiple Layer 2 paths to a network cause a switch to flood broadcasts endlessly. This endless broadcast flood is called a "broadcast storm," and it causes severe network congestion. Because the Layer 2 header does not support a time to live (TTL) value, if a frame is sent into a looped topology, it can loop forever. The Spanning Tree Protocol (STP) can be used to prevent these problems on a switched or bridged network.

The bridge ID, also known as the switch ID, is used to elect the root bridge in a redundant network topology. The switch with the lowest bridge ID is selected as the root bridge. If the same priority number is configured on two or more switches in the network, the switch with the lowest MAC address will become the root. Bridge Protocol Data Units (BPDUs) communicate the details of the switch with the lowest bridge ID in the network. The root bridge originates BPDUs every two seconds, which are propagated by other switches throughout the network. BPDUs are used as keepalives between switches, and if a switch stops receiving BPDUs from a neighboring switch for ten intervals (20 seconds), it will assume a designated role for the network segment. The root bridge should be centrally located with respect to the clients and the servers that generate the most traffic on the VLAN.

An inferior BPDU would not enable the switch to become the root bridge.

Neither an ARP broadcast nor a jam signal is used in this process.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Troubleshooting TechNotes > Spanning Tree PortFast BPDU Guard Enhancement > Document ID: 10586

Question #3 of 51

Question ID: 1322904

Which statement is true of a full packet capture?

- **A)** requires less space than session data
- **B)** requires less storage space than transaction, statistical, or session data
- **C)** requires more storage space than transaction data, but not statistical data
- **D)** requires more storage space than transaction, statistical, or session data

Explanation

Full packet captures can be quite large, even when run for a short period of time. Networks generate packets very quickly.

Transaction data will not be as large as a full packet capture because it will be a subset, concentrating on a specific transaction.

Session data as well will not be as large as a full packet capture because it will be a subset, concentrating on a specific session.

Statistical data takes the least amount of space because it is simply includes totals and times.

Objective:
Security Monitoring

Sub-Objective:
Describe the uses of these data types in security monitoring (Full packet capture; Session data; Transaction data; Statistical data; Metadata; Alert data)

References:

SecurityIntelligence > Is Full Packet Capture Worth the Investment?

Question #4 of 51

Question ID: 1322920

Which type of attack is targeted at multiple users?

A) DDoS
B) whaling
C) phishing
D) spear phishing

Explanation

Plain phishing attacks are targeted at many users with the expectation that some number of them will fall for it. A phishing attack is an e-mail attack where a hacker attempts to gain user credentials by requesting them via e-mail. The phishing e-mail closely resembles an official e-mail.

Spear phishing attacks are those targeted at a single user. Spear phishing is a special type of phishing that appears to come from a trusted individual. Digital signatures can help protect against spear phishing attacks, and improve the overall security posture, by assuring employees that an email originated from the CEO.

Whaling is a special type of phishing that targets a single power user, such as a Chief Executive Officer (CEO). Whaling is used to gain confidential information about the company, and usually occurs via e-mail.

While a distributed denial of service (DDoS) attack is sourced from multiple attacks points, it is targeted at a single device, not a group of users. A distributed denial of service (DDoS) attack is one in which the attacker recruits hundreds or thousands of devices to assist in the attack. The helpers are called zombies and as a group they are called a botnet. A DDoS attack usually involves the hijacking of several computers and routers to use as agents of the attack. Multiple servers and routers involved in the attack often overwhelm the bandwidth of the attack victim. For example, if a server has intermittent connection issues, the logs show repeated connection attempts from the same IP addresses, and the attempts are overloading the server to the point it cannot respond to traffic, then the server is experiencing a DDoS attack.

Objective:
Security Monitoring

Sub-Objective:
Describe social engineering attacks

References:

CSO > What is phishing? How this cyber attack works and how to prevent it

---

Question #5 of 51

Question ID: 1322898

Which statement is FALSE with respect to access lists?

A) the rule in the list are examined from top to bottom

B) the order of the rules is important

C) the first rule match is applied

D) every rule is examined before a decision is made

Explanation

Every rule is NOT necessarily examined. An access list is a list of rules defined in a specific order. The rules are examined from the top of the list to the bottom. When one of the rules is encountered which matches the traffic type of the packet being examined, the action specified in that rule is taken and no more rules are examined.

The order of the rules is important. For example, examine this set of conceptual rules:

Allow traffic from subnet 192.168.5.0/24
Deny traffic from 192.168.5.5/24

The second rule would never be invoked because the first rule would always match the traffic of 192.168.5.5.

If all of the rules in a set are examined and none match the traffic type, the packet will be disallowed by an implied deny all at the end of each set. To counteract that, most of the time we configure an allow all at the end of the set to counteract this implied rule.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Basic Access List Configuration for Cisco Devices

Question #6 of 51

Question ID: 1322907

You are reading the output of a Syslog message. What type of information is contained in the *facility* section?

A) relationship to other messages

B) message type (UDP or TCP)

C) security level

D) process that submitted the message

Explanation

The facility section identifies the process or application that submitted the message.

The relationship to other messages is contained in the *priority* section.

The security level of the message is contained in the *severity* section.

The message type is contained in the *transport* section.

Syslog messages and SNMP traps trigger notification messages that can be sent via email and SMS. A syslog server receives and stores log messages sent from syslog clients. A syslog client sends logging information to a syslog server. A syslog server ensures that a network administrator can review device error information from a central location.

Objective:
Security Monitoring

Sub-Objective:
Describe the uses of these data types in security monitoring (Full packet capture; Session data; Transaction data; Statistical data; Metadata; Alert data)

References:

Kiwi Syslog Server > Syslog Facilities

Question #7 of 51

Question ID: 1322930

Management has asked you to ensure that the certificates that have been validated in the corporate PKI are protected. What must be secured in the PKI?

A) the private key of a user's certificate
B) the private key of the root CA
C) the public key of a user's certificate
D) the public key of the root CA

Explanation

The private key of the root certification authority (CA) must be secured to ensure that the certificates that have been validated in a public key infrastructure (PKI) are protected. If the private key of the root CA has been compromised, then a new root certificate must be created and the PKI must be rebuilt. The public key is found in the trusted root CA. If the private key of a user's certificate has been compromised, then a new certificate should be created for that user and the user's compromised certificate should be revoked. The compromise of a user's certificate will not jeopardize other certificates in a PKI. A public key, as its name implies, is public, and does not need to be kept secret.

If the private key of a server has been compromised by an intruder, you should submit the public key to the CRL.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

References:

CompTIA Security+ Deluxe Study Guide: SY0-501. Chapter 4: Identity and Access Management

Question #8 of 51

Question ID: 1322889

Which one of the following mitigation techniques reduces the attack profile of a device or network?

A) Honeypot
B) Penetration testing
C) File integrity monitoring
D) Role separation

Explanation

Role separation involves dividing server duties amongst two or more servers to reduce an attack profile. For example, if a server running the Active Directory, DNS, and DHCP roles went down, all those services would be unavailable. If, on the other hand, Server A hosted Active Directory, Server B hosted DNS, and Server C hosted DHCP, an attack that brought Server B down would not affect the other services. Because fewer services are hosted on a single device or network, there are fewer services to attack. Attack profiles are also referred to as attack surfaces. Other ways to reduce the attack surface include disabling scripting types, closing unneeded ports, and turning off unneeded virtual servers.

Penetration testing is using hacking methodologies and tools to test the security of a client’s network on behalf of the client. Penetration testing can also be provided by in-house experts. Penetration testing does not affect an attack profile.

File integrity monitoring helps to identify unauthorized changes to files. The monitoring process looks at such events as if or when a file was changed, who made the change, the nature of the change and what can be done to restore the file to the pre-change state. File integrity monitoring does not affect an attack profile.

Honeypots and honeynets are closely related concepts. A honeypot is a file or object on a network designed to lure in a hacker, often to divert attention from other resources. An example would be a directory called “Passwords” containing useless passwords. The hacker would spend a lot of time on unsuccessful login attempts. A honeynet is a network of honeypots. Honeypots and honeynets increase the attack surface by providing false targets for an attacker.

Objective:
Security Monitoring

Sub-Objective:
Compare attack surface and vulnerability

References:

Microsoft Docs > Security Best Practices for Configuration Manager > Best Practices for Securing Site Systems

Question #9 of 51

Question ID: 1322894

Which of the following is NOT an element found in a NetFlow v5 record?

A) destination port
B) source IP address
C) referrer
D) source port

Explanation

The referrer is an HTTP header field that indicates the previous web page from which a request was routed. It is not part of a NetFlow v5 record.

NetFlow records flows, which are a unique combination of the following elements:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol

All communications sharing this same combination are part of the same flow or conversation between two systems.

Objective:
Security Monitoring

Sub-Objective:
Identify the types of data provided by these technologies (TCP dump; NetFlow Next-gen firewall; Traditional stateful firewall; Application visibility and control; Web content filtering; Email content filtering)

References:

HYPERLINK "https://www.solarwinds.com/what-is-netflow" SolarWinds > How NetFlow Works

---

Question #10 of 51

Question ID: 1325269

What is the standard for digital certificates?

A) X.500

B) IEEE 802.11

C) IEEE 802.3af

D) X.509

Explanation

The standard for digital certificates is X.509. These text documents include identifying information of the holder, the most important being the public key of the holder.

X.500 is the standard for directory services.

Power over Ethernet (PoE) is defined by the IEEE 802.3af and 802.3at standards. PoE allows an Ethernet switch to provide power to an attached device by applying power to the same wires in a UTP cable that are used to transmit and receive data. PoE+ is an enhanced version of PoE that provides more power and better reliability. PoE+ is most commonly deployed in enterprise networks, while PoE is usually sufficient for small business or home networks.

The IEEE 802.11 standard, which is the main standard for wireless LANs (WLANs), specifies using Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) for its media access method. Like an Ethernet network, which uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD), wireless adapter cards "sense," or listen, for network traffic before transmitting. If the network is free of traffic, the station will send its data. The 802.11 standard also refers to CSMA/CA as Distributed Coordination Function (DCF).

However, unlike an Ethernet network, wireless network cards cannot send and receive transmissions at the same time, which means that they cannot detect a collision. Instead, the sending station will wait for an acknowledgement packet (ACK) to be sent by the destination computer, verifying that the data was received. If, after a random amount of time, an acknowledgement has not been received, the sending station will retransmit the data.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

SSL > What Is an X.509 Certificate?

Question #11 of 51

Question ID: 1322897

The 802.1x standard is closely related to what process?

A) NAC

B) DNS

C) NAT

D) NTP

Explanation

Network access control (NAC) is a concept that denies access to a network unless certain health checks on the device are performed. It is closely related to the 802.1x standard for port-based access control. NAC events include the examination of the requesting device, the possible remediation of the offending device, and the subsequent opening of the devices port to the network.

Network address translation (NAT) is a service that allows the use of private IP addresses inside a network with access to the Internet using the IP address of the NAT device.

Domain Name System (DNS) resolves host names and domain names to IP addresses.

Network Time Protocol (NTP) keeps the clock synchronized on the network.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

Genians > What is Network Access Control?

Question #12 of 51

Question ID: 1322900

Which type of algorithm encrypts data bit by bit?

A) block

B) asymmetric

C) stream

D) symmetric

Explanation

Stream ciphers operate bit by bit rather than on a block of data at a time. Stream and block ciphers are the two main types of symmetric algorithms.

Block ciphers process one block of bits, and stream ciphers process one bit at a time. RC5 and RC6 are block ciphers.

Symmetric ciphers are those that use the same key to encrypt as to decrypt. Symmetric ciphers have modes of operation: ECB, CBC, CTM or CTR, and GCM.

- Electronic Code Book (ECB) mode implements the cipher in its original form.

- Cipher-block Chaining (CBC) mode uses the output of each block and XORs it with the following block to increase diffusion.
- Counter Mode (CTM or CTR) converts a block cipher into a stream cipher.
- Galois Counter Mode (GTM) uses a hash function to further complicate the encryption.

Asymmetric cryptography involves the use of different keys to encrypt and decrypt the data. These keys are referred to as private and public keys, respectively. The public encryption key is used to ensure only the intended recipient can decrypt the ciphertext. The public key is shared and used to encrypt information, and the private key is secret and used to decrypt data that was encrypted with the matching public key. ElGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement.

Block ciphers operate on a block of data at a time rather than bit by bit.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

IT Pro Today > Symmetric vs. Asymmetric Ciphers

Question #13 of 51

Question ID: 1325271

Which of the following is a key exchange algorithm?

A) AES
B) Diffie-Hellman
C) DES
D) SSH

Explanation

Diffie-Hellman is an algorithm that makes possible the generation and exchange of a symmetric key used to encrypt data. Diffie-Hellman is one of the first implementations of a public/private key system.

Asymmetric algorithms include Diffie-Hellman, RSA, ElGamal, Elliptic Curve Cryptosystem (ECC), CAST, and Knapsack. Asymmetric algorithms exchange public/private key pairs.

Symmetric algorithms include Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Blowfish, RC4, RC5, and RC6. Symmetric algorithms are sometimes called block ciphers.

Secure Shell (SSH) is an encrypted alternative to using Telnet, which is clear text. SSH is a method for securing sessions between network computers.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

CompariTech > What is the Diffie–Hellman key exchange and how does it work?

Question #14 of 51

Question ID: 1322924

Which of the following describes a resource exhaustion attack?

A) receiving an abnormally low volume of scanning from numerous source

B) receiving an abnormally high volume of scanning from numerous source

C) waiting for an opportune moment

D) performing actions slower than normal

Explanation

In a resource exhaustion attack, the goal is to overwhelm the IPS or IDS such that it cannot keep up. Therefore, this attack uses an abnormally high volume of scanning from numerous sources. Resource exhaustion occurs when a system runs out of limited resources, such as bandwidth, RAM, or hard drive space. Without the required storage space (as an example), the system can no longer perform as expected, and crashes.

A Distributed Denial of Service (DDoS) is one in which the attacker recruits hundreds or thousands of devices to assist in the attack. The helpers are called zombies and as a group they are called a botnet. A DDoS attack usually involves the hijacking of several computers and routers to use as agents of the attack. Multiple servers and routers involved in the attack often overwhelm the bandwidth of the attack victim. For example, if a server has intermittent connection issues, the logs show repeated connection attempts from the same IP addresses, and the attempts are overloading the server to the point it cannot respond to traffic, then the server is experiencing a DDoS attack.

Timing attacks are those in which the operations carried out are done much slower than normal to keep the IPS or IDS from assembling the operation into a recognizable attack.

Attackers really have no way of recognizing or acting upon an “opportune“ moment.

Objective:
Security Monitoring

Sub-Objective:
Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Security IPS 642-627 Official Cert Guide: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

Question #15 of 51

Question ID: 1322939

Which of the following represents standards for public key cryptography created by RSA?

A) PKCS

B) transform set

C) RFCs

D) cipher suite

Explanation

PKCS stands for Public Key Cryptography Standards. There are currently 11 in effect:

- PKCS # 1 - The RSA encryption standard. This standard defines mechanisms for encrypting and signing data using the RSA public key system.
- PKCS # 3 - The Diffie-Hellman key-agreement standard. This defines the Diffie-Hellman key agreement protocol.
- PKCS # 5 - The password-based encryption standard (PBE). This describes a method to generate a secret key based on a password.
- PKCS # 6 - The extended-certificate syntax standard. This is currently being phased out in favor of X509 v3.
- PKCS # 7 - The cryptographic message syntax standard. This defines a generic syntax for messages which have cryptography applied to it.
- PKCS # 8 - The private-key information syntax standard. This defines a method to store Private Key Information.
- PKCS # 9 - This defines selected attribute types for use in other PKCS standards.
- PKCS # 10 - The certification request syntax standard. This describes a syntax for certification requests.
- PKCS # 11 - The cryptographic token interface standard. This defines a technology independent programming interface for cryptographic devices such as smartcards.
- PKCS # 12 - The personal information exchange syntax standard. This describes a portable format for storage and transportation of user private keys, certificates etc.
- PKCS # 13 - The elliptic curve cryptography standard. This describes mechanisms to encrypt and sign data using elliptic curve cryptography.

A Request for Comment (RFC) is a document soliciting feedback on a potential standard.

In cryptography, the cipher suite describes the type, size, and methods that are used when data (plaintext) is encrypted.

A transform set is a collection of settings used in an IPsec configuration.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

Techopedia > Public Key Cryptography Standards (PKCS)

Question #16 of 51

Question ID: 1322905

Which tool is used to obtain session data?

A) Wireshark
B) SIEM
C) syslog
D) NetFlow

Explanation

NetFlow is a Cisco tool used to capture information about sessions. A session is a set of exchanges that use the same 5- tuple of source and destination IP address, source and destination MAC address, and transport protocol.

Wireshark is packet capture utility used for full or partial packet capture. When used maliciously it can capture data, and it is if unencrypted, Wireshark can read the data.

Security incident and event management (SIEM) software aggregates log files and analyzes them in real time for malicious activity. Aggregation is a SIEM feature that allows the collection of various events that are flagged by network hardware and software applications. Correlation is a SIEM feature that looks for similarities in events that are collected from different devices. Correlation allows the analyst to examine seemingly unique events and determine the patterns between them.

Syslog servers collect and centralize the log files from the network devices. Syslog messages and SNMP traps trigger notification messages that can be sent via email and SMS. A syslog server receives and stores log messages sent from syslog clients. A syslog client sends logging information to a syslog server. A syslog server ensures that a network administrator can review device error information from a central location.

Objective:
Security Monitoring

Sub-Objective:
Describe the uses of these data types in security monitoring (Full packet capture; Session data; Transaction data; Statistical data; Metadata; Alert data)

References:

Cisco > Products & Services > Cisco IOS and NX-OS Software > Cisco IOS Technologies > Management Instrumentation > Cisco IOS NetFlow

---

Question #17 of 51

Question ID: 1325267

Which of the following is used to validate and in some cases revoke certificates?

A) PGP
B) DHCP
C) PKI
D) POP

Explanation

A public key infrastructure (PKI) contains software hardware and policies that allow digital certificates to be created, validated, or revoked. A digital signature provides integrity, authentication, and non-repudiation in electronic mail. A PKI typically consists of the following components: certificates, a key repository, a method for revoking certificates, and a method to evaluate a certificate chain, which security professionals can use to follow the possession of keys.

Pretty Good Privacy (PGP) is an email encryption system. PGP uses a web of trust to validate public key pairs. In a web of trust model, users sign their own key pairs. If a user wants to receive a file encrypted with PGP, the user must first supply the public key.

Post Office Protocol (POP) is a client email program. It is used to retrieve email from the email server.

Dynamic Host Configuration Protocol (DHCP) is a protocol that allows network administrators to centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP can automatically assign a new IP address when a computer is plugged into a different location on the network.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of certificates on security (includes PKI, public/private crossing the network,

asymmetric/symmetric)

References:

SSH > PKI - Public Key Infrastructure

Question #18 of 51

Question ID: 1325268

Which algorithm is a symmetric cipher?

A) El Gamal

B) ECC

C) RSA

D) 3DES

Explanation

Triple DES or 3DES is a symmetric algorithm, which means the key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of DES that performs three rounds of encryption. A 3DES algorithm uses 48 rounds of computation. It offers high resistance to differential cryptanalysis because it uses so many rounds. The encryption and decryption process performed by 3DES takes longer due to the higher processing power required. Data Encryption Standard (DES) is also symmetric.

The other algorithms are all asymmetric. Asymmetric cryptography involves the use of different keys to encrypt and decrypt the data. These keys are referred to as private and public keys, respectively. The public encryption key is used to ensure only the intended recipient can decrypt the ciphertext. These algorithms use two keys that do not match, but are mathematically related such that if encryption is performed using one, the other is used for decryption. Asymmetric algorithms include Diffie-Hellman, RSA, ElGamal, Elliptic Curve Cryptosystem (ECC), CAST, and Knapsack.

ElGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement. It is used for digital signatures, encryption of data, and key exchange.

Rivest, Shamir, and Adleman (RSA) is used as the worldwide de facto standard for digital signatures. RSA is a public key algorithm that provides both encryption and authentication.

Elliptic Curve Cryptosystem (ECC) serves as an alternative to the RSA algorithm and provides similar functionalities, but ECC has a higher strength per bit than RSA.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

References:

Vocal > Triple Data Encryption Standard (Triple-DES)

Question #19 of 51

Question ID: 1325270

Which of the following describes the type, size, and methods that are used when data (plaintext) is encrypted?

A) method list

B) algorithm collection

C) transform set

D) cipher suite

Explanation

In cryptography, the cipher suite describes the type, size, and methods that are used when data (plaintext) is encrypted. Weak cipher suites and implementations can cause system vulnerabilities. As an example, a SOHO router using inherently weak Wireless Encryption Protocol (WEP) encryption can lead to an easy network attack.

A transform set is a collection of settings used in an IPsec configuration. Internet Protocol Security (IPsec) is a protocol that secures IP communication over a private or public network. IPSec allows a security administrator to implement a site-to-site VPN tunnel between a main office and a remote branch office.

Neither algorithm collection nor method list are terms used when discussing cryptography.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

The SSL Store > SSL/TLS Cipher Suites

Question #20 of 51

Question ID: 1322913

Which attack requires a botnet?

A) DDoS

B) password theft

C) man in the middle

D) DoS

Explanation

A Distributed Denial of Service (DDoS) attack is one in which the attacker recruits hundreds or thousands of devices to assist in the attack. The helpers are called zombies, and as a group they are called a botnet.

A DDoS attack usually involves the hijacking of several computers and routers to use as agents of the attack. Multiple servers and routers overwhelm the bandwidth of the attack victim. For example, if a server has intermittent connection issues, the logs will show repeated connection attempts from the same IP addresses, and the attempts are overloading the server to the point it cannot respond to traffic, then the server is experiencing a DDoS attack.

A man in the middle attack makes use a single attack machine. The intent is to position the attacker between two communicating devices such that they are sending to the attacker rather than sending to one another. Using a packet analyzer to gather packets from a network connection between two computers is a method that can be used to initiate a man in the middle (MITM) attack.

A DoS attack is one that is sourced from a single machine. A denial of service (DoS) attack occurs when attackers overrun a server with requests so that legitimate users cannot access the server.

Password theft uses a single attack machine as well.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Digital Attack Map > What is a DDoS Attack?

Question #21 of 51

Question ID: 1322914

Which of the following describes a TCP injection attack?

A) many TCP SYN packets are captured with the same sequence number, but different source and destination IP addresses and different payloads

B) many TCP SYN packets are captured with the same sequence number, source, and destination IP address, but different payloads

C) an attacker performs actions slower than normal

D) there is an abnormally high volume of scanning from numerous sources

Explanation

A TCP injection attack occurs when the attacker injects data into a TCP packet. Evidence of this attack would be many TCP SYN packets captured with the same sequence number, source and destination IP address but different payloads.

In a resource exhaustion attack, the goal is to overwhelm the IPS or IDS such that it cannot keep up. Therefore, it uses an abnormally high volume of scanning from numerous sources. Resource exhaustion occurs when a system runs out of limited resources, such as bandwidth, RAM, or hard drive space. Without the required storage space (as an example), the system can no longer perform as expected, and crashes.

Timing attacks are those in which the operations are carried out at a much slower than normal pace to keep the IPS or IDS from assembling the operation in to a recognizable attack.

Capturing many TCP SYN packets captured with the same sequence number, but different source and destination IP address and different payloads, is possible but unlikely. It would not represent a TCP injection attack.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Security IPS 642-627 Official Cert Guide: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

Question #22 of 51

Question ID: 1322892

Which of the following increases when additional functionality is added to an application? Choose the BEST answer.

A) risk

B) threats

C) attack surface

D) vulnerabilities

Explanation

The attack surface consists of functionalities that a malicious individual might compromise. As you add functionality, you also increase the attack surface. Determining the attack surface will help you identify the different components that can be attacked, and reviewing the architecture will help you identify network architecture security issues. For example, most VPN solutions require one or more new ports to be opened on the firewall, which increases the attack surface of the organization.

A vulnerability is a susceptibility to a threat that exists in a system.

A threat is an external danger. A system may or may not be vulnerable to a specific threat. A threat is a potential danger that could take advantage of a system if it is vulnerable. For example, there might be threat to SQL servers but if you use Oracle, it is not a vulnerability, only a threat. Because threats are external, they are not affected by increasing functionality.

Risk may be increased IF a vulnerability is created but not unless, therefore it is not the best answer. Risk is the likelihood that an external threat leverages an internal vulnerability. We reduce the risk of a breach when we apply controls that mitigate the likelihood or the impact of the threat.

Objective:
Security Monitoring

Sub-Objective:
Compare attack surface and vulnerability

References:

RedSeal > Understanding and Managing Your Attack Surface

Question #23 of 51

Question ID: 1322919

Which of the following is NOT a social engineering attack?

A) someone enters the building by following someone with a key card

B) receiving an invite to the your department WebEx meeting

C) a call from someone falsely claiming to be from IT asking for your password

D) an unexpected email from an unknown person with a strange attachment from a different person in the same company

Explanation

Simply receiving an invitation to your department WebEx meeting is not a social engineering attack. These are attacks that use social skills and take advantage of user’s desire to comply with instructions.

All the following are examples of social engineering attacks:

- Receiving a call from someone falsely claiming to be from IT asking for your password
- Receiving an unexpected email from an unknown person with a strange attachment from a different person in the same company as the recipient

- Someone entering a locked building by following someone with a key card
- Someone standing behind your back and observing you entering a password

Social engineering refers to tricking someone into sharing classified information by pretending to be an authorized person. Social engineering is used to discover confidential information, such as system passwords, which are later used by the intruder to gain unauthorized access either to the system or to the network.

Objective:
Security Monitoring

Sub-Objective:
Describe social engineering attacks

References:

WebRoot > What is Social Engineering?

Question #24 of 51

Question ID: 1322890

Which action would you perform to look for candidates for exploitation across an information system?

A) Patch management

B) Vulnerability scanning

C) Port scanning

D) Log reviewing

Explanation

Vulnerability scanning looks for areas that are candidates for exploitation (weak spots) in networks, operating systems, applications, and equipment. Vulnerability scans can also identify the effectiveness of in-place systems designed to prevent those exploits.

Log reviewing is the process of studying the event logs and looking for patterns or key triggers (such as a failed logon) that would indicate a potential problem. As an example, in the Windows OS you could look for event codes 525-537 or 539, which are indicative of a failed login attempt.

Patches are updates to operating systems and applications. Patch management is the process of applying those updates, auditing for installation, and verifying that the most current patch has been applied. While some patches address performance features, they are more often associated with correcting security issues.

Port scanning examines ports (0-65535) to determine if they are available for traffic (open) or blocked (closed). A company may want to enable port 80 for HTTP traffic, but disable ports 20/21 to block FTP traffic. While open ports may be candidates for exploitation, port scanning does not provide the level of information that vulnerability scanning does.

Objective:
Security Monitoring

Sub-Objective:
Compare attack surface and vulnerability

References:

SecureWorks > Vulnerability Scanning vs. Penetration Testing

CompTIA Network+ N10-007 Cert Guide, Chapter 12: Network Security, Defending Against Attacks

Question #25 of 51

Question ID: 1322929

You suspect that several users are using expired digital certificates and that other digital certificates are very close to expiration. You need to examine the list of serial numbers of digital certificates that have not expired, but should be considered invalid. Which PKI component should you examine?

A) UDP
B) CRL
C) KDC
D) CA

Explanation

A certificate revocation list (CRL) contains a list of serial numbers for digital certificates that have not expired, but that a certification authority (CA) has specified to be invalid. Typically, the serial number of a digital certificate is placed in a CRL because the digital certificate has been compromised in some way. A CA generates and validates digital certificates. The CA verifies the authenticity of the certificate elements.

A Key Distribution Center (KDC) is used in Kerberos network authentication to distribute resource access keys. User Datagram Protocol (UDP) provides connectionless communications on TCP/IP networks.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

References:

CompTIA Security+ Deluxe Study Guide: SY0-501. Chapter 4: Identity and Access Management

Question #26 of 51

Question ID: 1322928

Which of the following describes a timing attack?

A) waits for an opportune moment
B) delays attack for an amount of time
C) performs actions slower than normal
D) performs actions faster than normal

Explanation

Timing attacks are those in which the operations carried out are done much slower than normal to keep the IPS or IDS from assembling the operation into a recognizable attack.

Performing actions faster than normal might even make it easier for the IPS or IDS to assemble the parts of the operation into a recognizable attack.

Delaying the attack will have no bearing how easily the IPS may or may not recognize the attack.

Attackers really have no way of recognizing or acting upon an “opportune” moment.

Objective:
Security Monitoring

Sub-Objective:
Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Security IPS 642-627 Official Cert Guide: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

---

Question #27 of 51

Question ID: 1322934

Which of the following is a block cipher that also be used as a stream cipher?

A) AES

B) DES

C) 3DES

D) AES_256 CTR

Explanation

While AES is usually classified as a block cipher, in counter mode (CTR) it can be used as a stream cipher. The other ciphers are also block ciphers, but lack the ability to be a stream cipher. Counter (CTR) Mode converts a block cipher (blocks of data) into a stream cipher (one bit at a time). It utilizes synchronous counters at the sender and the receiver.

Stream and block ciphers are the two main types of symmetric algorithms. Block ciphers process one block of bits, and stream ciphers process one bit at a time.

Digital Encryption Standard (DES), Triple DES or 3DES, and Advanced Encryption Standard (AES) are all symmetric algorithms. Symmetric algorithms are sometimes called block ciphers.

Rivest Cipher 4 (RC4) is the most widely used of all stream ciphers.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

StackOverflow > AES 256 in CTR mode

Question #28 of 51

Question ID: 1322909

What is the term for any evasion attempt where the attacker splits malicious traffic to avoid detection or filtering?

A) fragmentation

B) LAND attack

C) network mapping

D) SYN flood

Explanation

One of the earliest attempts at evading IDS and IPS system was to fragment the malicious traffic in such a way the IDS/IPS does not recognize the attack. If the IPS does not perform reassembly before analysis, detection can be evaded in this way.

SYN flood attacks are a denial-of-service (DoS) attack that uses synchronization request packets. SYN flood attacks are not used to evade IDS/IPS systems.

Network mapping is using a tool, such as nmap, to identity the devices and their relationships to one another.

A LAND attack occurs when a SYN packet is sent that appears to come from the target itself. This causes the target device to lock up.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Security IPS 642-627 Official Cert Guide: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

---

Question #29 of 51

Question ID: 1325264

What is used to remotely manage a device at the command line?

A) SSH

B) DES

C) 3DES

D) AES

Explanation

Secure Shell (SSH) is an encrypted alternative to using Telnet, which is clear text. SSH is a method for securing sessions between network computers. SSH is most often used in UNIX environments, but is also available for Windows and OS/2 computers. Port number 22 is reserved for Secure Shell (SSH) remote login.

Telnet uses port 23. Telnet is a terminal emulation protocol. You can use Telnet to establish a remote session with a server and to issue commands on a server.

AES is currently the best encryption algorithm available commercially. The Advanced Encryption Standard (AES) is the strongest of the listed encryption algorithms, and uses 128-bit, 192-bit, and 256-bit encryption keys. It is not used to remotely manage a device at the command line.

Data Encryption Standard (DES) is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted. The DES algorithm uses 16 rounds of computation. DES has many security issues.

3DES is a version of DES that performs three rounds of DES encryption. It is not used to remotely manage a device at the command line.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

Hostinger > How does SSH Work

Question #30 of 51

Question ID: 1322893

Which of the following is a standard for port-based access control?

A) 802.1x

B) 802.3

C) 802.11n

D) X.509

Explanation

The 802.1x standard is for port-based access control using a central server, such as a RADIUS server.

802.11n is a standard for 802.11 wireless local area network (WLAN).

802.3 is the standard for Ethernet.

X.509 is the standard for digital certificates.

Objective:
Security Monitoring

Sub-Objective:
Identify the types of data provided by these technologies (TCP dump; NetFlow Next-gen firewall; Traditional stateful firewall; Application visibility and control; Web content filtering; Email content filtering)

References:

PC Mag > 802.1X

Question #31 of 51

Question ID: 1322921

What is DNS poisoning?

A) the practice of continually sending a DNS server synchronization messages with spoofed packets

B) the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash

C) the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash

D) the practice of dispensing IP addresses and host names with the goal of traffic diversion

Explanation

DNS poisoning is the practice of dispensing IP addresses and host names with the goal of traffic diversion. Properly configured DNS security (DNSSEC) on the DNS server can provide message validation, which, in turn, would prevent DNS poisoning.

A SYN flood is the practice of continually sending a DNS server synchronization messages with spoofed packets. A SYN flood can transpire when a high number of half-open connections are established to a single computer.

A DNS denial-of-service (DoS) attack is the practice of one computer transmitting malformed packets to the DNS server to cause the server to crash. A DNS distributed DoS (DDoS) attack is the practice of many computers transmitting malformed packets to the DNS server to cause the server to crash.

Address Resolution Protocol (ARP) poisoning is similar to DNS poisoning. In this attack, a malicious actor sends falsified ARP messages over a local area network.

In a domain hijacking attack, the registration of a domain name is changed without the permission of the original registrant.

Objective:
Security Monitoring

Sub-Objective:
Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

References:

Adventure in Security > DNS Cache Poisoning: Definition and Prevention (PDF)

Question #32 of 51

Question ID: 1325266

Which of the following is a Layer 3 attack?

A) VLAN hopping

B) MAC spoofing

C) ARP attacks

D) IP spoofing

Explanation

As IP addresses reside on Layer 3 of the OSI model, IP spoofing is considered a Layer 3 attack.

Other types of spoofing attacks apart from IP spoofing are e-mail spoofing and Web spoofing. Do not confuse e-mail spoofing with pharming attacks. While both do involve being redirected to a fake Web site to obtain confidential information, pharming often involves poisoning the DNS cache to ensure the user is redirected to the fake site even if they correctly enter the real site's URL. E-mail spoofing just involves clicking links in a hoax e-mail. Pharming is considered a more browser-related attack because it is designed to affect browser usage over the long term.

As ARP resolves IP addresses to MAC addresses, and MAC addresses reside on Layer 2 of the OSI model, ARP attacks are considered a Layer 2 attack.

As MAC addresses reside on Layer 2 of the OSI model, MAC spoofing attacks are also considered Layer 2 attacks. MAC addresses are 48-bit addresses in hexadecimal that are permanently attached to the network interface by the manufacturer.

VLANs are Layer 2 concepts, therefore VLAN hopping attacks are considered Layer 2 attacks. Switches are typically deployed to create virtual local area networks (VLANs). The switch isolates the VLAN from the rest of the network to provide better security for the VLAN.

Objective:
Security Monitoring

Sub-Objective:
Describe social engineering attacks

References:

CloudFlare > What is IP Spoofing?

Question #33 of 51

Question ID: 1322910

Which attack is underway when a SYN packet is sent that appears to come from the target itself?

A) SYN flood

B) Teardrop

C) Fraggle

D) LAND attack

Explanation

A LAND attack occurs when a SYN packet is sent that appears to come from the target itself. This causes the target device to lock up.

A Fraggle attack is one that recruits other devices to take part in overwhelming the target with UDP packets.

SYN flood attacks are a denial-of-service (DoS) attack.

A teardrop attack is when a hacker sends a TCP packet with the SYN flag set to a target, with the packet fragmented in such a way that the fragment reassembly process cannot take place. This locks the target up.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Cisco Press > Articles > Cisco Certification > CCNP > CCNP Security IPS 642-627 Official Cert Guide: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

---

Question #34 of 51

Question ID: 1322926

Which type of link is used to pass the traffic of multiple VLANs?

A) VPN

B) EtherChannel

C) trunk

D) access

Explanation

Trunk links between switches, and between switches and routers, are used to carry the traffic of multiple VLANs. Each frame is tagged with the number of the VLAN to which it belongs as it traverses the trunk link. A trunk port, which serves as the connection between switches, tags the VLAN traffic.

EtherChannel provides a way to combine multiple ports on a switch to create a single link, but is not used to carry multiple VLAN traffic unless all ports in the EtherChannel are set as trunk links. When configuring EtherChannel as a trunk link, all ports that are bundled in the channel must be set for trunk for the link to operate correctly.

Access links can only carry the traffic of a single VLAN. An access port, which is the connection to an end device, does not tag. Port tagging and VLANs are not used in unsegmented networks.

VPN links can only carry multiple VLANs if the link is configured as a trunk link. A virtual private network (VPN) is a private network that users can connect to over a public network. Tunneling techniques are used to protect the internal resources.

Objective:
Security Monitoring

Sub-Objective:
Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

References:

Cisco > Configuring Access and Trunk Interfaces (PDF)

Question #35 of 51

Question ID: 1322927

Which of the following is used to encrypt HTTPS?

A) Triple DES

B) AES

C) SSL/TLS

D) DES

Explanation

HTTPS, the encrypted form of HTTP makes use of SSL/TLS. One of the issues this creates is when attempting to perform security monitoring the packets cannot be read.

Advanced encryption algorithm (AES) is the strongest of the listed encryption algorithms. The Advanced Encryption Standard (AES) uses 128-bit, 192-bit, and 256-bit encryption keys.

Digital encryption standard (DES) is the first version of DES and the weakest of the listed encryption algorithms. Digital encryption standard (DES) is an encryption algorithm not a hashing algorithm. Data Encryption Standard (DES) is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted. The actual key size of the Data Encryption Standard (DES) is 64 bits. A key size of 8 bits is used for a parity check. Therefore, the effective key size of DES is 56 bits.

Triple DES is a later version of DES that performs three rounds of encryption. A Triple DES (3DES) algorithm uses 48 rounds of computation. It offers high resistance to differential cryptanalysis because it uses so many rounds. The encryption and decryption process performed by 3DES takes longer due to the higher processing power required.

Objective:
Security Monitoring

Sub-Objective:
Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

References:

Cloudflare > What Is HTTPS?

Question #36 of 51

Question ID: 1322916

Which cross-site scripting attack is sometimes called persistent?

A) reflected
B) stored
C) directed
D) DOM based

Explanation

A stored XSS attack is one in which the injected script is stored in the server and received from the server by the user device. Cross-site scripting (XSS) poses the most danger when a user accesses a financial organization's site using his or her login credentials. The problem is not that the hacker will take over the server. It is more likely that the hacker will take over the client's session. This will allow the hacker to gain information about the legitimate user that is not publicly available. To prevent XSS, a programmer should validate input to remove hypertext. You can mitigate XSS by preventing the use of HTML tags or JavaScript image tags.

A reflected or non-persistent attack is one that is reflected off the web server and not stored on the server.

A DOM based attack is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim’s browser.

Directed is not a term used to describe cross site scripting attacks

Objective:
Security Monitoring

Sub-Objective:
Describe web application attacks, such as SQL injection, command injections, and crosssite scripting

References:

OWASP > Cross-site Scripting (XSS)

Question #37 of 51

Question ID: 1322935

Which of the following is the most widely used public key cipher?

A) 3DES

B) El Gamal

C) AES

D) RSA

Explanation

Rivest, Shamir, Adleman (RSA) is the most widely used public key or asymmetric cipher. RSA supports encryption and decryption and secures data with an algorithm that is based on the difficulty of factoring large numbers.

A public key encryption algorithm is sometimes referred to as an asymmetric encryption algorithm. With asymmetric encryption, the public key is shared and used to encrypt information, and the private key is secret and used to decrypt data that was encrypted with the matching public key. Using RSA, messages traveling between two points are encrypted and authenticated. RSA tokens are used to provide a rolling password for one-time use.

Triple DES or 3DES is a symmetric algorithm, which means the key used to encrypt is identical to the key used to decrypt. Triple DES is a later version of Data Encryption Standard (DES) that performs three rounds of encryption. The encryption and decryption process performed by 3DES takes longer due to the higher processing power required.

While El Gamal is a public key or asymmetric cipher, it is not the most widely used.

AES is a symmetric algorithm that is currently the best encryption algorithm available commercially. Advanced Encryption Algorithm (AES) is the strongest of the listed encryption algorithms. The Advanced Encryption Standard (AES) uses 128-bit, 192-bit, and 256-bit encryption keys.

Objective:
Security Monitoring

Sub-Objective:
Identify the certificate components in a given scenario (Cipher-suite; X.509 certificates; Key exchange; Protocol version; PKCS)

References:

Techopedia > RSA Encryption

Question #38 of 51

Question ID: 1325265

What is the source of alert data?

A) NetFlow

B) sniffers

C) IPS

D) application log files

Explanation

Intrusion prevention systems (IPS) collect alerts data, which are indications of potential malicious activity.

Application log files contain transaction data.

Sniffers generate packet captures. Wireshark is packet capture utility used for full or partial packet capture. When used maliciously it can capture data, and it is if unencrypted, Wireshark can read the data.

NetFlow is a Cisco tool used to capture information about sessions. A session is a set of exchanges that use the same 5- tuple of source and destination IP address, source and destination MAC address and transport protocol.

Objective:
Security Monitoring

Sub-Objective:
Describe the uses of these data types in security monitoring (Full packet capture; Session data; Transaction data; Statistical data; Metadata; Alert data)

References:

Cisco > Products > Security > Cisco IOS Intrusion Prevention System (IPS)

Question #39 of 51

Question ID: 1322895

You are examining NetFlow records. What is the state of the connection when you receive a packet with the RST flag set in response to a packet with the SYN flag set?

A) the port is closed
B) the port is blocked by the firewall
C) the connection is set up
D) the port is open

Explanation

Receiving a packet with the RST flag in response to a packet with the SYN flag means the port is closed. When a port is closed, the device answers back with a TCP packet with the RST flag set.

If the port were open, the response packet would have the SYN and ACK flags set.

Transmission Control Protocol (TCP) is a session-oriented or connection-based protocol. It uses a three-way handshake to ensure that every packet sent is successfully received and acknowledged by the destination. The handshake is performed at the start of each session by TCP, and contains a set of three segments (TCP "packets").

- The sender sends the first segment to the receiver with the Synchronization (SYN) flag enabled.
- Step two: The receiver sends the second segment back to the sender with both the Acknowledgement flag (ACK) and the Synchronization (SYN) flag enabled.
- Step three: The sender sends the third segment back to the receiver with just the Acknowledgement (ACK) flag enabled (in response to the server's Synchronization request).

Were the connection successfully set up, the response packet would have the ACK flag set.

If the port were blocked by the firewall, there would be no response. Firewalls do not send diagnostic or error messages when blocking a transmission.

Objective:
Security Monitoring

Sub-Objective:
Identify the types of data provided by these technologies (TCP dump; NetFlow Next-gen firewall; Traditional stateful firewall; Application visibility and control; Web content filtering; Email content filtering)

References:

Lifewire > Introduction to Port Scanning

Question #40 of 51

Question ID: 1322901

Which of the following provides non-repudiation?

A) hashing

B) encryption

C) digital signature

D) redundancy

Explanation

A digital signature provides non-repudiation, which means the signing cannot be denied at a later time. This is done by hashing the document and then encrypting the hash value with the private key of the sender. The public key of the signer is used to verify a digital signature.

A digital signature provides integrity, authentication, and non-repudiation in electronic mail. Integrity involves providing assurance that a message was not modified during transmission. Authentication is the process of verifying that the sender is who he says he is.

Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption. Digital signatures do not provide encryption and cannot ensure availability.

Redundancy, or the use of multiple components, increases availability, the A in CIA. Redundancy ensures that there are multiple ways to control the static environment Redundancy occurs when you have systems in place ready to come online when a system fails.

Hashing algorithms generate hash values which can be compared to identify if data has changed. Hashing ensures integrity, not non-repudiation. Protecting data from unauthorized change provides integrity. Hashing algorithms include MD2, MD4, MD5, HAVAL, and all of the Secure Hash Algorithm (SHA) variants.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

AssureSign > Electronic Signatures Vs Digital Signatures… What’s the Difference?

Question #41 of 51

Question ID: 1322903

Which of the following uses port 443?

A) SSH

B) DNS

C) Telnet

D) HTTP

E) SSL

Explanation

Secure Sockets Layer (SSL) is a security protocol that uses both encryption and authentication to protect data sent in network communications. SSL and HTTPS use port 443.

Port number 22 is reserved for Secure Shell (SSH) remote login.

Telnet uses port 23. Telnet is a terminal emulation protocol. You can use Telnet to establish a remote session with a server and to issue commands on a server. Telnet client software provides you with a text-based interface and a command line from which you can issue commands on a server that supports the Telnet protocol. Telnet works at the Application layer of the OSI model.

HTTP uses port 80. HTTP is used to traverse web pages.

DNS uses port 53. Domain Name System (DNS) is the protocol that will manage the FQDN to IP address mappings.

There are a total of 65,535 ports in the TCP/IP protocol that are vulnerable to attacks. The following are the most commonly used ports and protocols:

- FTP - ports 20 and 21
- SSH, SCP, and SFTP - port 22
- Telnet - port 23
- SMTP - port 25
- TACACS - port 49
- DNS server - port 53
- DHCP - ports 67 and 68
- TFTP - port 69
- HTTP - port 80
- Kerberos - port 88
- POP3 - port 110
- NetBIOS - ports 137-139
- IMAP4 - port 143
- SNMP - port 161
- LDAP - port 389
- SSL and HTTPS - port 443
- SMB - port 445
- LDAP with SSL - port 636
- FTPs - ports 989, 990
- Microsoft SQL Server - port 1433
- Point-to-Point Tunneling Protocol (PPTP) - port 1723
- RDP protocol and Terminal Services - port 3389

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

SSL > What is SSL?

Question #42 of 51

Question ID: 1322917

What is the initial aim of a man in the middle attack?

- **A)** data theft
- **B)** password theft
- **C)** denial of service
- **D)** eavesdropping

Explanation

While other goals may be in mind, the initial goal is to eavesdrop. An example is eavesdropping on an IP phone conversation. A man in the middle (MITM) attack makes use a single attack machine. The intent is to position the attacker between two communicating devices such that they are sending to the attacker rather than sending to one another. Using a packet analyzer to gather packets from a network connection between two computers is a method that can be used to initiate a man in the middle (MITM) attack.

Password theft is rarely is ever the goal of this attack. Passwords are rarely divulged in the process.

Denial of service is rarely the goal. A DoS attack is one that is sourced from a single machine. A denial of service (DoS) attack occurs when attackers overrun a server with requests so that legitimate users cannot access the server.

Data theft might occur, but that will not be the initial goal.

Objective:
Security Monitoring

Sub-Objective:
Describe social engineering attacks

References:

GlobalSign > What is a Man-in-the-Middle Attack and How Can You Prevent It?

Question #43 of 51

Question ID: 1322891

What is the difference between an exploit and a vulnerability?

- **A)** The two terms are interchangeable
- **B)** A vulnerability is a flaw, and an exploit takes advantage of that flaw
- **C)** An exploit is a threat, and a vulnerability is a flaw.
- **D)** An exploit is a flaw, and a vulnerability takes advantage of that flaw

Explanation

When comparing exploits vs. vulnerabilities, a vulnerability is a flaw or weakness, and an exploit takes advantage of that flaw. As examples, a vulnerability could be a section of code in an application that fails to validate user input against a range of acceptable values. The exploit would be the active use of that failure to validate to introduce malicious data, such as an SQL injection attack.

A threat is the likelihood that an event is going to occur.

The terms exploit and vulnerability are not interchangeable.

Objective:
Security Monitoring

Sub-Objective:
Compare attack surface and vulnerability

References:

Live Hacking > The difference between an expoit and vulnerability

Question #44 of 51

Question ID: 1322922

Which statement is false with respect to exploit kits?

A) they take advantage of software vulnerabilities
B) they require a deep understanding of exploits
C) they are deployed on webpages
D) they spread malware

Explanation

Exploit kits are sold and require little understanding of the attacks they make possible. They are used by less experienced hackers.

Exploit kits are tools commonly used by threat actors on webpages to take advantage of software vulnerabilities to spread malware and perform other types of attacks.

Sometimes exploit kits are also called root kits.

Objective:
Security Monitoring

Sub-Objective:
Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

References:

Trend Micro > exploit kit

Question #45 of 51

Question ID: 1322915

Which of the following makes a command injection possible?

A) web server that accepts input from the user and passes it to a bash shell
B) input is accepted without bounds checking
C) two passwords that hash to the same value
D) unneeded service ports left open

Explanation

When a web server accepts input and passes it to a bash shell (command line), an attacker might input a command as part of the input that might be accepted and processed by the web server.

Two passwords that hash to the same value is called a hash collision, and can lead to either or both passwords being cracked. A Birthday attack captures hashed passwords from the network and uses brute force to try out different text strings using the same hashing algorithm, hoping to end up with a matching pair of hash values, referred to as a collision.

When input is accepted without bounds checking an integer overflow can occur, which is when a value is entered that is larger than expected leading to the integer overflow, a type of buffer overflow. IT occurs when a mathematic operation attempts to create a numeric value that is too large for the available storage space.

When unneeded service ports are left open, the attack surface of the device is increased. Increasing the attack surface makes more attacks possible, but does not make you more susceptible to command injection.

Other injection attacks include SQL injection, LDAP injection, XML injection, and file injection.

Objective:
Security Monitoring

Sub-Objective:
Describe web application attacks, such as SQL injection, command injections, and crosssite scripting

References:

OWASP > Command Injection

Question #46 of 51

Question ID: 1322906

What is the source of transaction data?

- **A)** NetFlow
- **B)** application log files
- **C)** SIEM
- **D)** sniffer

Explanation

Transaction data occurs between a user and an application, and thus is derived from application log files.

Sniffers generate packet captures. Wireshark is packet capture utility used for full or partial packet capture. When used maliciously it can capture data, and it is if unencrypted, Wireshark can read the data.

Security incident and event management (SIEM) software aggregates log files and analyzes them in real time for malicious activity. Aggregation is a SIEM feature that allows the collection of various events that are flagged by network hardware and software applications. Correlation is a SIEM feature that looks for similarities in events that are collected from different devices. Correlation allows the analyst to examine seemingly unique events and determine the patterns between them.

Automated alerting and triggers are a SIEM feature that allow the system to react based on predetermined criteria. Alerts include one or more systems that notify an administrator when a predetermined event occurs. Triggers take it a step further, and respond to the event with a series of programmed actions. As an example, an NIPS can shut down port 80 when an unusually high amount of web traffic floods the network.

NetFlow is a Cisco tool used to capture information about sessions. A session is a set of exchanges that use the same 5- tuple of source and destination IP address, source and destination MAC address and transport protocol.

Objective:
Security Monitoring

Sub-Objective:
Describe the uses of these data types in security monitoring (Full packet capture; Session data; Transaction data; Statistical data; Metadata; Alert data)

References:

Cisco Community > Networking > How to configure logging in Cisco IOS

Question #47 of 51

Question ID: 1322902

What is the purpose of the DSA algorithm?

A) encryption
B) hashing
C) transposition
D) digital signatures

Explanation

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was published by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Encryption is performed by another classification of algorithms, including DES, 3DES and AES. Digital encryption standard (DES) is the first version of DES and the weakest of the listed encryption algorithms. DES is a private key encryption standard that is used in IPSec to ensure that data packets are confidentially transmitted. The actual DES key size is 64 bits. 8 bits are used for a parity check. Therefore, the effective key size of DES is 56 bits.

Hashing is performed by another classification of algorithms, including MD5, SHA-1 and SHA-2. Hashing algorithms generate hash values which can be compared to identify if data has changed.

While transposition is one way in which algorithms may scramble data, it is not an algorithm classification.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of these technologies on data visibility (Access control list; NAT/PAT; Tunneling; TOR; Encryption; P2P; Encapsulation; Load balancing)

References:

Techopedia > Digital Signature Algorithm (DSA)

Question #48 of 51

Question ID: 1322931

Your company recently implemented an internal public key infrastructure (PKI). You need to ensure that all of the PKI components are secure and are currently researching the vulnerabilities on the entity that signs the certificates. Which entity are you examining?

A) a principal
B) a verifier
C) a subject
D) an issuer

Explanation

In a public key infrastructure (PKI), an issuer is the entity that signs a certificate. Signing a certificate verifies that the name and key in the certificate are valid. PKI is a system designed to securely distribute public keys. A PKI typically consists of the following components: certificates, a key repository, a method for revoking certificates, and a method to evaluate a certificate chain, which security professionals can use to follow the possession of keys. Chain of custody might be used in proving legal cases against hackers.

A principal is any entity that possesses a public key. A verifier is an entity that verifies a public key chain. A subject is an entity that seeks to have a certificate validated.

When using a PKI, keep the following points in mind:

- When encrypting a message with the public key, only the private key can decrypt it.
- When encrypting a message with the private key, only the public key can decrypt it.

Objective:
Security Monitoring

Sub-Objective:
Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

References:

CompTIA Security+ Deluxe Study Guide: SY0-501. Chapter 4: Identity and Access Management

TechGenix > Understanding the Role of the PKI

Cisco > Technology White Paper > Public Key Infrastructure: Deployment Benefits and Features

Question #49 of 51

Question ID: 1322912

Which of the following is most likely to be used in a reflected DoS attack?

A) NTP
B) STP
C) IGMP
D) ARP

Explanation

Network Time protocol (NTP) servers are often used in a reflected attack, which is an attack bounced off a third party to hit the target. This helps to hide the source of the attack. NTP is used to synchronize the clocks of computers on the network. Time synchronization is important in areas such as event logs, billing services, e-commerce, banking, and HIPAA security rules.

While spanning tree protocol can be used in network attacks on switches, it is not a DoS type attack. STP uses the Spanning Tree Algorithm (STA) to help a switch or bridge by allowing only one active path at a time. STP can prevent network congestion and broadcast storms.

There are two types of STP: spanning tree (802.1d) and rapid spanning tree (802.1w). 802.1d is an older standard that was designed when a minute or more of lost connectivity was considered acceptable downtime.

Address resolution protocol (ARP) is also used in attacks, especially man in the middle, but it is not a DoS attack. ARP tables show the relationship of IP address to MAC address. But they cannot be used for DNS and DHCP integration.

Internet Group messaging Protocol (IGMP) is not typically used in network attacks.

Objective:
Security Monitoring

Sub-Objective:
Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

References:

Imperva > NTP Amplification

Question #50 of 51

Question ID: 1322925

How is a local exploit different from a remote exploit?

A) local requires prior access to the target
B) remote is done by logging in to the target
C) local is over the network
D) remote requires prior access to the system

Explanation

A local exploit is one in which the attacker must have prior access to the system. It involves gaining access and using privileged escalation to increase the rights of the attacker to administrator. It requires physical access to the device

A remote exploit in which no prior physical access has occurred. It occurs over the network without logging in. For example leveraging a root kit would be a remote exploit because it does not involve physically logging in to the machine.

Local is done by logging into the system, while remote is done over the network.

Objective:
Security Monitoring

Sub-Objective:
Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

References:

SAINT > Exploit

Question #51 of 51

Question ID: 1325263

Which of the following is NOT a feature of a next generation firewall?

A) stateless firewall
B) URL filtering
C) application visibility and control
D) advanced malware protection

Explanation

Next generation firewalls (NGFW) are stateful firewalls, not stateless firewalls.

Some of the features of the Cisco NGFW are:

- Stateful firewall
- Application visibility and control
- NGIPS
- Advanced malware protection
- URL filtering
- VPN

With a stateful firewall, a packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Objective:
Security Monitoring

Sub-Objective:
Identify the types of data provided by these technologies (TCP dump; NetFlow Next-gen firewall; Traditional stateful firewall; Application visibility and control; Web content filtering; Email content filtering)

References:

Cisco > Products > Security > Next-Generation Firewalls