Item: 12 (Ref:Auerbach-CISSP.10.1.3)

Telecommunications and Network Security

In which of the following situations is the network itself not a target of attack?

mlj A denial-of-service attack on servers on a network

mlj Hacking into a router

mlj A virus outbreak saturating network capacity

mlj A man-in-the-middle attack

Answer:

A man-in-the-middle attack

Explanation:

Although the modification of messages will often happen at the higher network layers, networks can be set up to provide robustness or resilience against interception and change of a message (man-in-the-middle attack) or replay attack. Ways to accomplish this can be based on encryption or checksums on messages, as well as on access control measures for clients that would prevent an attacker from gaining the necessary access to send a modified message into the network.

Item: 19 (Ref:Auerbach-CISSP.10.1.18)

A botnet can be characterized as:

mlj A network used solely for internal communications

mlj An automatic security alerting tool for corporate networks

mlj A group of dispersed, compromised machines controlled remotely for illicit reasons.

mlj A type of virus

Answer:

A group of dispersed, compromised machines controlled remotely for illicit reasons.

Explanation:

"Bots" and "botnets" are most insidious implementations of unauthorized, remote control of compromised systems. Such machines are essentially zombies controlled by ethereal entities from the dark places on the internet.

Item: 49 (Ref:Auerbach-CISSP.10.1.21)

In a very large organization where the user population is dynamic and static passwords are undesirable, which method of authentication would be desirable?

mlj Challenge Handshake Authentication Protocol (CHAP)

mlj Password Authentication Protocol (PAP)

mlj Extensible Authentication Protocol (EAP0

mlj Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Answer:

Extensible Authentication Protocol (EAP0

Explanation:

The Extensible Authentication Protocol (EAP) framework allows the authenticating partners to negotiate the authentication method during the authentication phase. EAP authentication methods include EAP-TLS (EAP, tunneled layered security), EAP-TTLS (EAP, tunneled TLS) and EAP-PEAP (EAP, protected EAP).

Item: 54 (Ref:Auerbach-CISSP.10.1.22)

All of the following activities are examples of active attacks EXCEPT which one?

mlj Sending a packet into the network with a spoofed source address

mlj Using a network analyzer to intercept and read FTP data

mlj ARP cache poisoning

mlj RIP route poisoning

Answer:

Using a network analyzer to intercept and read FTP data

Explanation:

Because ARP does not require authentication, an attacker could place bogus entries in the ARP cache to carry out other attacks, such as a man in the middle. Adding bogus entries in ARP cache is called ARP poisoning.

Item: 75 (Ref:Auerbach-CISSP.10.1.14)

Which of the following are true statements about IPSec?

a) IPSec provides mechanisms for authentication and encryption b) IPSec provides mechanisms for non-repudiation

c) IPSec will only be deployed with IPv6

d) IPSec authenticates hosts against each other

e) IPSec only authenticates clients against a server, f) IPSec is implemented in SSH and TLS

f) IPSec is implemented in SSH and TLS.

mlj a and d

mlj a, b and e

mlj a, b, c, d and f

mlj a, b, c, e and f

Answer:

a and d

Explanation:

IPSec is a suite of protocols for communicating securely with IP by providing mechanisms for authentication and encryption. Standard IPSec authenticates only host with each other.

Item: 78 (Ref:Auerbach-CISSP.10.1.9)

Which of the following is a principal security risk of wireless LANs?

mlj Lack of physical access control

mlj Demonstrably insecure standards

mlj Implementation weaknesses

mlj War driving

Answer:

Lack of physical access control

Explanation:

Wireless networks allow users to be mobile while remaining connected to a LAN. Unfortunately, this allows unauthorized users greater access to the LAN as well. In fact, many wireless LANs can be accessed off of the organization's property by anyone with a wireless card in a laptop, which effectively extends the LAN where there are no physical controls.

Item: 79 (Ref:Auerbach-CISSP.10.1.6)

Which of the following end-point devices might be considered part of a converged IP network?

mlj file server

mlj IP phone

mlj security camera

mlj all of the above

Answer:

all of the above

Explanation:

See Figure 10.3

Item: 102 (Ref:Auerbach-CISSP.10.1.24)

An intrusion detection system (IDS) that develops baselines of normal traffic activity and throughput and alerts the

IDS administrator if there is a deviation from the norm is using what method of detection?

mlj Attack signature detection

mlj Statistical anomaly detection

mlj Protocol anomaly detection

mlj Traffic anomaly detection

Answer:

Statistical anomaly detection

Explanation:

The statistical anomaly-based IDS analyzes event data by comparing it to typical, known, or predicted traffic profiles in an effort to find potential security breaches. It attempts to identify suspicious behavior by analyzing event data and identifying patterns of entries that deviate from a predicted norm.

Item: 126 (Ref:Auerbach-CISSP.10.1.5)

What is the optimal placement for network-based intrusion detection systems (NIDS)?

mlj On the network perimeter, to alert the network administrator of all attack attempts

mlj On network segments with business-critical systems; e.g., demilitarized zones (DMZs) and on certain intranet segments

mlj At the network operations center (NOC)

mlj At an external service provider

Answer:

On the network perimeter, to alert the network administrator of all attack attempts

Explanation:

Intrusion detection systems monitor activity and send alerts when they detect suspicious traffic. There are two broad classifications of IDS: host-based IDS, which monitor activity on servers and workstations, and network- based IDS, which monitor network activity.

Item: 137 (Ref:Auerbach-CISSP.10.1.13)

Which of the following is the principal benefit of personal firewalls?

mlj They provide a PC on a public network with a reasonable degree of protection; if the PC connects to a trusted network later on (for instance, an Intranet), it will prevent the PC from becoming an agent of attack;

e.g., by spreading viruses.

mlj They offer an additional degree of protection on intranets to the PC because, due to the trend of incremental weakening of the network boundary, these networks can no longer be considered trusted.

mlj They protect networks the PC connects to from threats, such as virus infections, that the PC could become an agent to.

mlj They prevent attacks on individual PCs. If everybody would use them, the Internet would be safe from virus attacks.

Answer:

They provide a PC on a public network with a reasonable degree of protection; if the PC connects to a trusted network later on (for instance, an Intranet), it will prevent the PC from becoming an agent of attack; e.g., by spreading viruses.

Explanation:

Following the principle of security in depth, personal firewalls are installed on workstations, which protect the user from all hosts on the network. It is critical for home users with DSL or cable modem access to the Internet to have a personal firewall installed on every PC, especially if they do not have a firewall protecting their network.

Item: 138 (Ref:Auerbach-CISSP.10.1.20)

An attacker is sending ICMP echo request messages into the network. The destination address is a directed broadcast and the source address is actually the address of the victim. What type of attack is the hacker doing?

mlj Fraggle

mlj Smurf

mlj Teardrop

mlj Land

Answer:

Smurf

Explanation:

See Smurf and Fraggle Attacks.

Item: 149 (Ref:Auerbach-CISSP.10.1.11)

Which of the following is the principal security risk of broadband Internet access proliferation for home users?

mlj Users using peer-to-peer file-sharing networks for breaches of intellectual property.

mlj PCs connected permanently to the Internet are prone to receive more spam mails, thereby increasing the risk for the user to become infected with viruses and Trojans.

mlj PCs will become infected with dialers on DSL lines (run over telephony lines), thereby exposing the user to almost limitless financial risk.

mlj Home computers that are not securely configured or maintained and are permanently connected to the

Internet become easy prey for attackers.

Answer:

Home computers that are not securely configured or maintained and are permanently connected to the Internet become easy prey for attackers.

Explanation:

DSL allows the users to be connected to the Internet for much longer time intervals. Certainly, this is very convenient for the user, but extended time exposed to the hostile Internet greatly increases the risk of being attacked. To mitigate this serious risk, it is imperative that the host has a firewall, vendor security patches are installed, and dangerous and unused protocols are disabled. As with DSL, cable modems allow home users to enjoy high-speed Internet connectivity. Cable modem users must take the same precautions as DSL users: ensure that PCs on the home network have a personal firewall, install vendor security patches, and disable dangerous and unused protocols.

Item: 150 (Ref:Auerbach-CISSP.10.1.19)

What would be the best tool to deal with a distributed port scan?

mlj Penetration test

mlj Event log

mlj Intrusion Detection System (NDS)

mlj Firewall

Answer:

Firewall

Explanation:

Protection from port scanning includes restriction of network connections, e.g.,

by means of a host-based or network-based firewall or by defining a list of valid source addresses on an application level.

Item: 163 (Ref:Auerbach-CISSP.10.1.16)

Which of the following is the principal weakness of DNS (Domain Name System)?

mlj Lack of authentication of servers, and thereby authenticity of records

mlj Its latency, which enables insertion of records between the time when a record has expired and when it is refreshed

mlj The fact that it is a simple, distributed, hierarchical database instead of a singular, relational one, thereby giving rise to the possibility of inconsistencies going undetected for a certain amount of time

mlj The fact that addresses in e-mail can be spoofed without checking their validity in DNS, caused by the fact that DNS addresses are not digitally signed

Answer:

Lack of authentication of servers, and thereby authenticity of records

Explanation:

Authentication has been proposed but attempts to introduce stronger authentication into DNS have not found wider acceptance. Authentication services have been delegated upward to higher protocol layers. Applications in need of guaranteeing authenticity cannot rely on DNS to provide such but will have to implement a solution themselves.

Item: 164 (Ref:Auerbach-CISSP.10.1.15)

A Security Event Management (SEM) service performs the following function:

mlj gathers firewall logs for archiving

mlj aggregates logs from security devices and application servers looking for suspicious activity

mlj reviews access controls logs on servers and physical entry points to match user system authorization with physical access permissions

mlj coordination software for security conferences and seminars

Answer:

aggregates logs from security devices and application servers looking for suspicious activity

Explanation:

SEM/SEIM systems have to understand a wide variety of different applications and network element (routers/switches) logs and formats; consolidate these logs into a single database and then correlated events looking for clues to unauthorized behaviors that would be otherwise inconclusive if observed in a single log file.

Item: 174 (Ref:Auerbach-CISSP.10.1.17)

Which of the following statements about open e-mail relays is incorrect?

mlj An open e-mail relay is a server that forwards e-mail from domains other than the ones it serves.

mlj Open e-mail relays are a principal tool for distribution of spam.

mlj Using a blacklist of open e-mail relays provides a secure way for an e-mail administrator to identify open mail relays and filter spam.

mlj An open e-mail relay is widely considered a sign of bad system administration.

Answer:

Using a blacklist of open e-mail relays provides a secure way for an e-mail administrator to identify open mail relays and filter spam.

Explanation:

Although using blacklists as one indicator in spam filtering has its merits, it is risky to use them as an exclusive indicator. Generally, they are run by private organizations and individuals according to their own rules, they are able to change their policies on a whim, they can vanish overnight for any reason, and they can rarely be held accountable for the way they operate their lists.

Item: 175 (Ref:Auerbach-CISSP.10.1.7)

Which of the following is an advantage of fiber-optic over copper cables from a security perspective?

mlj Fiber optics provides higher bandwidth. mlj Fiber optics are more difficult to wiretap. mlj Fiber optics are immune to wiretap.

mlj None. The two are equivalent; network security is independent from the physical layer.

Answer:

Fiber optics are more difficult to wiretap.

Explanation:

From a security perspective, fiber optics' immunity to electromagnetic interference (EMI) and radio frequency interference (RFI) is important. Because fiber optics emit extremely small amounts of energy from the cable, data cannot be as easily intercepted as information is transported through electric current in wires.

Item: 186 (Ref:Auerbach-CISSP.10.1.4)

Which of the following are effective protective or countermeasures against a distributed denial-of-service attack?

a) Redundant network layout

b) Secret fully qualified domain names (FQDN)

c) Reserved bandwidth d) Traffic filtering

e) Network Address Translation (NAT)

mlj b and e

mlj b, d, and e

mlj a and c

mlj a, c, and d

Answer:

a, c, and d

Explanation:

Countermeasures to a denial-of-service attack include, but are not limited to, multiple layers of firewalls, careful filtering or firewalls, routers and switches, internal network access controls (NAC), redundant (diverse) network connections, load balancing, reserved bandwidth (quality of service, which would at least protect systems not directly targeted), and blocking traffic from an attacker on an upstream router.

Item: 197 (Ref:Auerbach-CISSP.10.1.23)

A road warrior wishes to access sensitive corporate information about future product releases while conducting a sales pitch to a potential customer who has signed a Non-Disclosure Agreement (NDA). Which of the following VPN technologies would be least suitable for this communication?

mlj IP Security (IPSec)

mlj Layer Two Tunneling Protocol (L2TP)

mlj Point to Point Tunneling Protocol (PPTP)

mlj Secure Socket Layer (SSL)

Answer:

Layer Two Tunneling Protocol (L2TP)

Explanation:

L2TP by itself does not address encryption; therefore, confidentiality of the data cannot be guaranteed.

Item: 200 (Ref:Auerbach-CISSP.10.1.12)

Who should be allowed to change rules on a firewall and for which reason?

mlj The network administrator for testing and troubleshooting purposes

mlj The firewall administrator on request of users after having assessed the validity of the business reason

mlj The firewall administrator in compliance with a change process that will, in particular, validate the request against the organization's security policy and provide proper authorization for the request

mlj The security manager, who will, in particular, validate the request against the organization's security policy and provide proper authorization for the request

Answer:

The firewall administrator in compliance with a change process that will, in particular, validate the request against the organization's security policy and provide proper authorization for the request

Explanation:

When changes to the environment are required to accommodate a need, they must be defined, approved, tested, applied, verified, deployed, audited, and documented. Changes can be minor, such as a static route being added to a network, or more significant, such as the redesign of a storage solution. Every organization must have a change control process to ensure that there is a formalized methodology for making and documenting changes to

the environment.

Item: 210 (Ref:Auerbach-CISSP.10.1.8)

Which of the following devices should not be part of a network's perimeter defense?

mlj A screening router

mlj A firewall

mlj A proxy server

mlj None of the above

Answer:

A proxy server

Explanation:

The security perimeter is the first line of protection between trusted and untrusted networks. In general, it includes a firewall and router that helps filter traffic. Security perimeters may also include proxies and devices, such as an instruction detection system, to warn of suspicious traffic. The defense perimeter extends out from these first protective devices, to include proactive defense such as boundary routers, which can provide early warning of upstream attacks and threat activities.

Item: 224 (Ref:Auerbach-CISSP.10.1.10)

Which of the following configurations of a WLAN's SSID offers adequate security protection?

mlj Using an obscure SSID to confuse and distract an attacker

mlj Not using any SSID at all to prevent an attacker from connecting to the network

mlj Not broadcasting an SSID to make it harder to detect the WLAN

mlj None of the above

Answer:

Not broadcasting an SSID to make it harder to detect the WLAN

Explanation:

Disabling beaconing is a useful if rudimentary safeguards for wireless LANs, but a patient attacker can still observe the SSID as soon as another client who knows the SSID comes into range and probes the wireless network.

Item: 237 (Ref:Auerbach-CISSP.10.1.1)

In the OSI reference model, on which layer can Ethernet (IEEE 802.3) be described?

mlj Layer 1 Physical layer mlj Layer 2 Data-link layer mlj Layer 3 Network Layer

mlj Layer 4 Transport Layer

Answer:

Layer 2 Data-link layer

Explanation:

Layer 2, the data-link layer, describes data transfer between machines, for instance, by an Ethernet.

Item: 248 (Ref:Auerbach-CISSP.10.1.2)

Which of the following tactics might be considered a part of a proactive network defense?

mlj Redundant firewalls

mlj Business continuity planning

mlj Disallowing P2P traffic

mlj Perimeter surveillance and intelligence gathering

Answer:

Perimeter surveillance and intelligence gathering

Explanation:

Ideally to counter an attack network security must also be proactive, anticipate and oppose the attack against their infrastructure by interdicting and disrupting an attack preemptively or in self-defense. This requires intelligence on the threat, active surveillance at the perimeter and beyond, and the ability to intercede upstream or disable a threat agent's tools.