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

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

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)

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

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

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

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

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

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

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.

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

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.

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

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

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

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.

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.

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

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)

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

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

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

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

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