CERTKILL

CompTIA SY0-101

SY0-101 Security+

Practice Test

Version 3.1

QUESTION NO: 1

A real estate company recently deployed Kerberos authentication on the network. Which of the following does Kerberos require for correct operation? (Select TWO).

A. POP-3
B. Accurate network time
C. Key Distribution Center
D. Extranets
E. SSL/TLS

Answer: B,C

QUESTION NO: 2

401.Which of the following are MOST likely to be analyzed by Internet filter appliances/servers? (Select THREE).401.Which of the following are MOST likely to be analyzed by Internet filter appliances/servers? (Select THREE).

A. Content
B. TLSs
C. Keys
D. URLs
E. CRLs
F. Certificates

Answer: A,D,F

QUESTION NO: 3

An administrator is selecting a device to secure an internal network segment from traffic external to the segment. Which of the following devices could be selected to provide security to the network segment?

A. NIPS
B. HIDS
C. Internet content filter
D. DMZ

Answer: A

QUESTION NO: 4

Which of the following VPN implementations consists of taking IPv6 security features and porting them to IPv4?

A. SSL
B. IPSec
C. L2TP
D. PPTP

Answer: B

QUESTION NO: 5

A user is assigned access rights based on the function within the organization. This is a feature of which of the following types of access control models?

A. Role Based Access Control (RBAC)
B. Rule Based Access Control (RBAC)
C. Mandatory Access Control (MAC)
D. Discretionary Access Control (DAC)

Answer: A

Explanation:
Role based access control contains components of MAC (mandatory access control) and DAC (discretionary access control), and is characterized by its use of profiles. A profile is a specific role that a group of employees perform in a function and the resources they need access to. When an employee is hired he is put into a profile, and when the entire profile of workers needs more or less resources they can all be facilitated together.

QUESTION NO: 6

Which of the following types of malicious software travels across computer networks without requiring a user to distribute the software?

A. Trojan horse
B. Worm
C. Virus
D. Logic bomb

Answer: B

QUESTION NO: 7

Which of the following would be MOST important to have to ensure that a company will be able to recover in case of severe environmental trouble or destruction?

A. Alternate sites
B. Disaster recovery plan
C. Fault tolerant systems
D. Offsite storage

Answer: B

QUESTION NO: 8

A task-based control model is an example of which of the following?

A. Rule Based Access Control (RBAC)
B. Role Based Access Control (RBAC)
C. Discretionary Access Control (DAC)
D. Mandatory Access Control (MAC)

Answer: B

QUESTION NO: 9

Which of the following is often misused by spyware to collect and report a user's activities?

A. Session cookie
B. Tracking cookie
C. Persistent cookie
D. Web bug

Answer: B

QUESTION NO: 10

Which definition best defines what a challenge-response session is?

A. A challenge-response session is a workstation or system that produces a random login ID that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification

Number).
B. A challenge-response session is a workstation or system that produces a random challenge string that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
C. A challenge-response session is a special hardware device used to produce random text in a cryptography system.
D. A challenge-response session is the authentication mechanism in the workstation or system that does not determine whether the owner should be authenticated.

Answer: B

Explanation:
A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

Reference:
http://www.webopedia.com/TERM/C/challenge_response.html

QUESTION NO: 11

Which of the following describes a type of algorithm that cannot be reversed in order to decode the data?

A. One Way Function
B. Symmetric
C. Asymmetric
D. Pseudorandom Number Generator (PRNG)

Answer: A

QUESTION NO: 12

An administrator wants to implement a procedure to control inbound and outbound traffic on a network segment. Which of the following would achieve this goal?

A. HIDS
B. ACL
C. Proxy

D. NIDS

Answer: B

QUESTION NO: 13

Which of the following freeware forensic tools is used to capture packet traffic from a network?

A. nmap
B. NESSUS
C. tcpdump
D. dd

Answer: C

QUESTION NO: 14

When reviewing traces from an IDS, the following entries are observed:

Date Time Source IP Destination IP Port Type
10/21 0900 192.168.5.2 10.10.2.1 20 SYN
10/21 0915 192.168.5.2 10.10.2.1 21 SYN
10/21 0920 192.168.5.2 10.10.2.1 23 SYN
10/21 0930 192.168.5.2 10.10.2.1 25 SYN
Which of the following is MOST likely occurring?

A. Port scanning
B. SYN Flood
C. Denial of service (DoS)
D. Expected TCP/IP traffic

Answer: A

QUESTION NO: 15

Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. SNMP (Simple Network Management Protocol).
B. Network News Transfer Protocol (NNTP)
C. Domain Name Service (DNS)

D. Internet Control Message Protocol (ICMP)

Answer: A

QUESTION NO: 16

Which of the following must be installed for HTTPS to work properly on a web site?

A. Digital certificate
B. Symmetric key
C. 3DES encryption
D. Security token

Answer: A

QUESTION NO: 17

You work as the security administrator. You want to implement a solution which will provide a WLAN (Wireless Local Area Network) with the security typically associated with a wired LAN (Local Area Network):
Which solution should you implement?

A. WEP (Wired Equivalent Privacy)
B. VPN (Virtual Private Network)
C. ISDN (Integrated Services Digital Network)
D. ISSE (Information Systems Security Engineering)

Answer: A

Explanation:
Wired Equivalent Privacy is a wireless protocol designed to provide privacy equivalent to that of a wired network.

Reference:
Mike Pastore and Emmett Dulaney , Security+ Study Guide , 2nd Edition, Alameda , Sybex , 2004, p 372

QUESTION NO: 18

From the options, which is a tunneling protocol that can only work on IP networks because it requires IP connectivity?

A. PPTP protocol
B. SSH
C. IPX protocol
D. L2TP protocol

Answer: A

Explanation:
Point-to-Point Tunneling Protocol
You can access a private network through the Internet or other public network by using a virtual private network (VPN) connection with the Point-to-Point Tunneling Protocol (PPTP).
Developed as an extension of the Point-to-Point Protocol (PPP), PPTP tunnels and/or encapsulates, IP, IPX, or NetBEUI protocols inside of PPP datagrams
PPTP does not require a dial-up connection. It does, however, require IP connectivity between your computer and the server.
Not B: L2TP is an industry-standard Internet tunneling protocol with roughly the same functionality as the Point-to-Point Tunneling Protocol (PPTP). Like PPTP, L2TP encapsulates Point-to-Point Protocol (PPP) frames, which in turn encapsulate IP, IPX, or NetBEUI protocols

QUESTION NO: 19

A user downloads and installs a new screen saver and the program starts to rename and delete random files. Which of the following would be the BEST description of this program?

A. Trojan horse
B. Logic bomb
C. Virus
D. Worm

Answer: A

QUESTION NO: 20

Which of the following BEST describes an attack that takes advantage of a computer not fully updated with the most recent operating system patches?

A. Software exploitation
B. Vulnerability
C. Brute force
D. Spoofing

Answer: A

QUESTION NO: 21

Secret Key encryption is also known as:

A. symmetrical
B. asymmetrical
C. replay
D. one way function.

Answer: A

QUESTION NO: 22

A companys security' specialist is securing a web server that is reachable from the Internet. The web server is located in the core internal corporate network. The network cannot be redesigned and the server cannot be moved. Which of the following should the security specialist implement to secure the web server? (Select TWO).

A. Network-basedfirewal
B. Host-based IDS
C. Host-based firewall
D. Network-based IDS
E. Router with an IDS module
F. Router with firewall rule set

Answer: B,C

QUESTION NO: 23

A program allows a user to execute code with a higher level of security than the user should have access to. Which of the following is this an example of?

A. DoS
B. Privilege escalation
C. Default accounts
D. Weak passwords

Answer: B

QUESTION NO: 24

A security specialist has completed a vulnerability assessment for a network and applied the most current software patches. The next step before placing the network back into operation would be to:

A. conduct a follow-up vulnerability analysis
B. update the baseline
C. perform penetration testing
D. test the essential functionality

Answer: D

QUESTION NO: 25

In a certificate hierarchy, the ultimate authority is called the:

A. Private Branch Exchange (PBX).
B. Terminal Access Controller Access Control System (TACACS).
C. Certificate Revocation List (CRL).
D. Root Certifying Authority (Root CA).

Answer: D

QUESTION NO: 26

For which reason are clocks used in Kerberos authentication?

A. Clocks are used to ensure that tickets expire correctly.
B. Clocks are used to both benchmark and specify the optimal encryption algorithm.
C. Clocks are used to ensure proper connections.
D. Clocks are used to generate the seed value for the encryptions keys.

Answer: A

Explanation:
The actual verification of a client's identity is done by validating an authenticator. The authenticator contains the client's identity and a timestamp.

To insure that the authenticator is up-to-date and is not an old one that has been captured by an attacker, the timestamp in the authenticator is checked against the current time. If the timestamp is not close enough to the current time (typically within five minutes) then the authenticator is rejected as invalid. Thus, Kerberos requires your system clocks to be loosely synchronized (the