310-301

Sun Certified Security Administrator

Version 5.1

www.testking.com

Leading The Way
in IT Testing And Certification Tools

www.testking.com

Important Note, Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Explanations
Currently this product does not include explanations. If you are interested in providing TestKing with explanations contact feedback@testking.com. Include the following information: exam, your background regarding this exam in particular, and what you consider a reasonable compensation for the work.

Copyright
Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

Note: Answers to the unanswered questions will be provided shortly. First customer, if any, faster than the TestKing team in proving the answers will receive credit:

- for each answer provided
- special credit for all unanswered questions

Send answers to feedback@testking.com.

QUESTION NO: 1
Part of a fire protection plan for a computer room should include:

A. Procedures for an emergency shutdown of equipment.
B. A sprinkler system that exceeds local code requirements.
C. The exclusive use of non-flammable materials within the room.
D. Fireproof doors that can be easily opened if an alarm is sounded.

Answer: A

QUESTION NO: 2
What network mapping tool uses ICMP (Internet Control Message Protocol)?

A. Port scanner
B. Map scanner
C. Ping scanner
D. Share scanner

Answer: C

QUESTION NO: 3
Which of the following would be most effective in preventing network traffic sniffing?

A. Deploy an IDS (Intrusion Detection System).
B. Disable promiscuous mode.
C. Use hubs instead of routers.
D. Use switches instead of hubs.

Answer: D

QUESTION NO: 4
A user wants to send an e-mail and ensure that the message is not tampered with while in transit. Which feature of modern cryptographic systems will facilitate this?

A. Confidentiality
B. Authentication
C. Integrity
D. Non-repudiation

Answer: C

QUESTION NO: 5
Which of the following type of attack CANNOT be deterred solely through technical means?

A. Dictionary
B. Man in the middle
C. DoS (Denial of Service)
D. Social engineering

Answer: D

QUESTION NO: 6
An organization is implementing Kerberos as its primary authentication protocol. Which of the following must be deployed for Kerberos to function?

A. Dynamic IP (Internet Protocol) routing protocols for routers and servers.
B. Separate network segments for the realms.
C. Token authentication devices.
D. Time synchronization services for clients and servers.

Answer: D

QUESTION NO: 7
Which of the following is likely to be found after enabling anonymous FTP (File Transfer Protocol) read/write access?

A. An upload and download directory for each user.
B. Detailed logging information for each user.
C. Storage and distribution of unlicensed software.
D. Fewer server connections and less network bandwidth utilization.

Answer: C

QUESTION NO: 8
NetBus and Back Orifice are each considered an example of a(n):

A. Virus
B. Illicit server
C. Spoofing tool
D. Allowable server

Answer: B

QUESTION NO: 9
Which of the following access control models introduces user security clearance and data classification?

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

Answer: C

QUESTION NO: 10
Why are unique user IDs critical in the review of audit trails?

A. They CANNOT be easily altered.

B. They establish individual accountability.
C. They show which files were changed.
D. They trigger corrective controls.

Answer: B

QUESTION NO: 11
Which of the following would NOT be considered a method for managing the administration of accessibility?

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

Answer: B

QUESTION NO: 12
In which risk assessment stage does the security auditor map the system and resources on a network?

A. Penetration
B. Cancellation
C. Activation
D. Discovery

Answer: D

QUESTION NO: 13
In a typical corporate environment, which of the following resources demands the highest level of security on the network?

A. Purchasing
B. Engineering
C. Sales
D. Accounting

Answer: D

QUESTION NO: 14
What is another term for a network security manager who acts as a potential hacker (a person looking for security loopholes)?

A. An agent
B. An auditor
C. An assessor
D. An analyzer

Answer: B

QUESTION NO: 15
What is the essential element in the implementation of any security plan?

A. Testing to make sure any server-side scripts are secure.
B. Testing patch levels.
C. Proper firewall configuration.
D. Auditing

Answer: D

QUESTION NO: 16
A malicious user has connected to your system and learned that specifics of your operating system, including its current patch levels and the operating system name.
What is the term for this type of scanning attack?

A. SYN detection
B. TCP priming
C. Cache poisoning
D. Stack fingerprinting

Answer: D

QUESTION NO: 17
What is the most important step in securing a Web server?

A. Logging all HTTP activity.
B. Enabling system-wide encryption.
C. Placing the operating system, Web server program, and server files on the same partition.
D. Placing the operating system, Web server program, and server files on separate partitions.

Answer: D

QUESTION NO: 18
What is the primary security risk in SNMP?

A. Login names and passwords are not encrypted.
B. Damaging programs can be executed on the client.
C. Damaging programs can be executed on the server.
D. Passwords and data are transferred in cleartext.

Answer: D

QUESTION NO: 19
Lucy is a systems administrator who wants to block all NNTP traffic between her network and the Internet.
How should she configure her firewall?

A. Configure the firewall to block all incoming and outgoing packets except for those with the source and destination port of 119.
Then, allow all traffic with destination ports above 1024 to traverse the firewall.
B. Configure the firewall to block all incoming packets with the source port of 119, and outgoing packets with a source port lower than 1024.
Then, block all packets with the destination port of 119 and with a source port lower than 1024.
C. Configure the firewall to block all incoming packets with the destination port of 119, and to block outgoing packets with the destination port of 119.
D. Configure the firewall to block all incoming packets with the source port of 119.

Answer: C

QUESTION NO: 20
Which port or ports are used for SMTP?

A. 20 and 21
B. 25
C. 53
D. 161 and 162

Answer: B

QUESTION NO: 21
Which type of attack causes a remote host to crash because it cannot respond to any new TCP connection requests?

A. Crack attack
B. Smurf attack
C. SYN flood
D. ICMP flood

Answer: C

QUESTION NO: 22
How are servers able to conduct a simple authentication check using DNS?

A. Forward DNS lookup
B. Reverse DNS lookup
C. RARP
D. Nslookup

Answer: B

QUESTION NO: 23
Which layer of the OSI/RM do proxy servers usually address?

A. Physical layer
B. Network layer
C. Transport layer
D. Application layer

Answer: D

QUESTION NO: 24
In a Linux system running inetd, how do you stop the POP3, IMAPD and FTP services?

A. By changing the permissions on the configuration file that controls the service (/sbin/inetd), then recompiling /etc/inetd.conf.
B. By commenting out the service using the # symbol in the text file /etc/inetd.conf, then restarting the inetd daemon.
C. By recompiling the system kernel, ensuring you have disabled that service.
D. By commenting out the service using the $ symbol in the text file /etc/inetd.conf, then restarting the inetd daemon.

Answer: B

QUESTION NO: 25
What is the major security issue with standard NIS (Network Information System)?

A. It is possible to enforce a centralized login scheme.
B. NIS provides no authentication requirement in its native state.
C. There is no way to encrypt data being transferred.
D. NIS is a legacy service used only in older, less secure operating systems and networks.

Answer: C

QUESTION NO: 26
What is a spoofing attack?

A. A hacker obtains access to the root account and poses as the system administrator.
B. A hacker calls a user and obtains the user's password.
C. A computer (or network) poses as a trusted host (or network).
D. A hacker gains entrance to the building where the network resides and accesses the system by pretending to be an employee.

Answer: C

QUESTION NO: 27
Which two threats should be defined in a Solaris threat model? (Choose two)

A. Insiders
B. Polymorphism
C. Malicious code
D. Polyinstantiation
E. Cosmic radiation

Answer: A, C

QUESTION NO: 28
Which weakness diminishes a security administrator's ability to detect an intrusion?

A. Inadequate logging and reporting.
B. Information leakage by network services.
C. Web CGI programs with weak privilege checks.
D. Firewalls that allow access to unnecessary services.

Answer: A

QUESTION NO: 29
Which three are examples of network security mechanisms? (Choose three)

A. IPSec
B. Syslog
C. Kerberos
D. TCP Wrappers
E. Basic Security Module
F. Role-based Access Control

Answer: A, C, D

QUESTION NO: 30
Which two steps are performed as part of system hardening? (Choose two)

A. Disable any system services that are not being used.
B. Correct files on the system that are not assigned to a valid user.
C. Install enough memory to protect against DoS attacks by memory depletion.
D. Use a private, non-routable IP address instead of a public, routable IP address.
E. Remove the root user account to prevent privilege escalation by normal users.

Answer: A, B

QUESTION NO: 31
Which are threats to electronic assets?

A. Disclosure, software, loss, and trust.
B. Loss, security policy, trust, and modification.
C. Disclosure, modification, loss, and interruption.
D. Modification, trust, destruction, and availability.

Answer: C

QUESTION NO: 32
A virus that hides itself by intercepting disk access requests is:

A. Multipartite
B. Stealth

C. Interceptor
D. Polymorphic

Answer: B

QUESTION NO: 33
File encryption using symmetric cryptography satisfies what security requirement?

A. Confidentiality
B. Access control
C. Data integrity
D. Authentication

Answer: A

QUESTION NO: 34
What ports does FTP (File Transfer Protocol) use?

A. 20 and 21
B. 25 and 110
C. 80 and 443
D. 161 and 162

Answer: A

QUESTION NO: 35
An organization's primary purpose in conducting risk analysis in dealing with computer security is:

A. To identify vulnerabilities to the computer systems within the organization.
B. To quantify the impact of potential threats in relation to the host of lost business functionality.
C. To delete responsibility.

Answer: B

QUESTION NO: 36
Discouraging employees from misusing company e-mail is best handled by:

A. Enforcing ACLs (Access Control List).
B. Creating a network security policy.
C. Implementing strong authentication.
D. Encrypting company e-mail messages.

Answer: B

QUESTION NO: 37
Security controls may become vulnerabilities in a system unless they are:

A. Designed and implemented by the system vendor.
B. Adequately tested.
C. Implemented at the application layer in the system.
D. Designed to use multiple factors of authentication.

Answer: B

QUESTION NO: 38
A wireless network with three access points, two of which are used as repeaters, exist at a company. What step should be taken to secure the wireless network?

A. Ensure that employees use complex passwords.
B. Ensure that employees are only using issued wireless cards in their systems.
C. Ensure that WEP (Wired Equivalent Privacy) is being used.
D. Ensure that everyone is using adhoc mode.

Answer: C

QUESTION NO: 39
Which of the following hash functions generates a 160-bit output?

A. MD4 (Message Digest 4)
B. MD5 (Message Digest 5)
C. DES (Data Encryption Standard)
D. SHA-1 (Secure Hashing Algorithm 1)

Answer: D

QUESTION NO: 40
What is the most common security problem on a client/server network?

A. Outdated software
B. Old login accounts
C. Non-secured ports
D. Browser flaws

Answer: B

QUESTION NO: 41
While assessing the risk to a network, which step are you conducting when you determine whether the network can differentiate itself from other networks?

A. Considering the business concerns.
B. Analyzing, categorizing and prioritizing resources.
C. Evaluating the existing perimeter and internal security.
D. Using the existing management and control architecture.

Answer: C

QUESTION NO: 42
Which device is similar to a packet filer, but also provides network address translation?

A. A circuit-level gateway.
B. An application-level gateway.
C. A proxy server.

D. A choke router.

Answer: A

QUESTION NO: 43
Which of the following will help control unauthorized access to an e-mail server?

A. Disable CGI scripts.
B. Prohibit relaying.
C. Limit the number of e-mail messages a given account can receive in a day.
D. Scan all e-mail messages at the firewall or SMTP server.

Answer: B

QUESTION NO: 44
Which of the following is a potential security risk when using CGI scripts?

A. CGI scripts can contain viruses that can be used against your system.
B. Compromised CGI scripts are often used in packet spoofing because they do not check packets they generate.
C. CGI scripts can create broadcast storms on the local network.
D. Remote user input can be used to execute local commands.

Answer: D

QUESTION NO: 45
Which choice lists the two greatest security problems associated with HTTP?

A. Community names and unencrypted passwords.
B. IP spoofing and ICMP spoofing.
C. Viewer applications and external programs used by the HTTP server.
D. Anonymous access and no bound checking on arrays.

Answer: C

QUESTION NO: 46
What is the primary security problem with traditional user-based FTP accounts?

A. Anonymous logins do not require a password.
B. Damaging programs can be executed on the client.
C. Damaging programs can be executed on the server.
D. The login name and password are sent to the server in cleartext.

Answer: D

QUESTION NO: 47
You have installed a proxy server that authenticates users. However, you find that one user has bypassed the proxy server by entering the default gateway IP address.
How can you solve this problem?

A. Configure the default gateway to deny access to all systems.
B. Confront the user.
C. Reconfigure the user's machine.
D. Configure the default gateway to reject all requests to all systems except for the proxy server.

Answer: D

QUESTION NO: 48
Which protocol is normally used to communicate errors or other conditions at the IP layer, but has also been used to conduct denial-of-service attacks?

A. TCP
B. ICMP
C. SNMP
D. UDP

Answer: B

QUESTION NO: 49
At which layer of the OSI/RM do packet filters function?

A. Data link layer
B. Physical layer
C. Network layer
D. Transport layer

Answer: C

QUESTION NO: 50
What are the security issues that arise in the use of the NFS (Network File System)?

A. Synchronization of user and group IDs is poor, so it is easy to spoof trusted hosts and user names.
B. The lack of logging in one place or on one machine, and the multiple logs this requires, can create bottlenecks.
C. The possibility arises for cleartext passwords to be sniffed on the network if it does not use Secure RPC.
D. NFS uses a weak authentication scheme and transfers information in unencrypted form.

Answer: D

QUESTION NO: 51
You must apply permissions to a file named /projects/group1/myfile.txt, and you need to fulfil the following requirements:

- **You want full access to the file.**
- **People in your group should be able to read the file.**
- **People in your group should not be able to write to the file.**
- **People outside of your group should be denied access to the file.**

What are the most secure permissions you would apply to this file?

A. chage 700 /home/myname/myfile.txt
B. chage 744 /home/myname/myfile.txt
C. chmod 640 /home/myname.myfile.txt
D. chmod 064 /home/myname/myfile.txt

Answer: C

QUESTION NO: 52
Which end-user actions gives a false sense of security?

A. Turning off systems when not in use.
B. Locking screens when leaving the office.
C. Refraining from opening email attachments.
D. Refraining from downloading and installing software.

Answer: A

QUESTION NO: 53
What are three platform security mechanisms? (Choose three)

A. EAL
B. PALM
C. ESP
D. BSM
E. OCSP

Answer: B, D, E

QUESTION NO: 54
What is the primary source of security breached on UNIX systems?

A. Worms
B. Viruses
C. Programming errors
D. Guesses user names

Answer: C

www.testking.com

QUESTION NO: 55
ActiveX controls _____ to prove where they originated.

A. Are encrypted.
B. Are stored on the web server.
C. Use SSL (Secure Sockets Layer).
D. Are digitally signed.

Answer: D

QUESTION NO: 56
En e-mail relay server is mainly used to:

A. Block all spam, which allows the e-mail system to function more efficiently without the additional load of spam.
B. Prevent viruses from entering the network.
C. Defend the primary e-mail server and limit the effects of any attack.
D. Eliminate e-mail vulnerabilities since all e-mail is passed through the relay first.

Answer: C

QUESTION NO: 57
WTLS (Wireless Transport Layer Security) provides security services between a mobile device and a:

A. WAP (Wireless Application Protocol) gateway.
B. Web server.
C. Wireless client.
D. Wireless network interface card.

Answer: A

QUESTION NO: 58
Searching through trash is sued by an attacker to acquire data suck as network diagrams, IP (Internet Protocol) address lists and:

A. Boot sectors
B. Process lists
C. Old passwords
D. Virtual memory

Answer: C

QUESTION NO: 59
An alternate site configured with necessary system hardware, supporting infrastructure and an on site staff able to respond to an activation of a contingency plan 24 hours a day, 7 days a week is a:

A. Cold site
B. Warm site
C. Mirrored site
D. Hot site

Answer: D

QUESTION NO: 60
A police department has three types of employees: booking officers, investigators, and judges. Each group of employees is allowed different rights to files based on their need. The judges do not need access to the fingerprint database, the investigators need read access and the booking officers need read/write access. The booking officers would need no access to warrants, while an investigator would need read access and a judge would need read/write access.
This is an example of:

A. DAC (Discretionary Access Control) level access control
B. RBAC (Role Based Access Control) level access control
C. MAC (Mandatory Access Control) level access control
D. ACL (Access Control List) level access control

Answer: B

QUESTION NO: 61
Which of the following is required to use S/MIME (Secure Multipurpose Internet Mail Extensions)?

A. Digital certificate
B. Server side certificate
C. SLL (Secure Sockets Layer) certificate
D. Public certificate

Answer: A

QUESTION NO: 62
Helga is a system administrator. She sees that an attacker from a remote location is sending invalid packets, trying to monopolize Helga's network connection so that a denial of service occurs.
What characteristic of the activity makes Helga think this is a denial-of-service attack?

A. Bandwidth consumption
B. Hijacking of internal user resources
C. Use of an illicit server
D. System slowdown

Answer: A

QUESTION NO: 63
Helga deleted extraneous services from a system to ensure that it is relatively secure from attack.
Which term describes this activity?

A. Securing the system
B. Operating system hardening
C. Auditing
D. System maintenance

Answer: B

QUESTION NO: 64
When using Microsoft Internet Information Server (IIS) on Windows NT/2000, what has primary control over security?

A. The operating system
B. IIS
C. The Gina
D. The SSL service

Answer: A

QUESTION NO: 65
Which port is used by DNS when conducting zone transfers?

A. UDP port 53
B. UDP port 23
C. TCP port 53
D. TCP port 23

Answer: C

QUESTION NO: 66
Which port does FTP use for a control connection?

A. 21
B. 25
C. 53
D. 162

Answer: A

QUESTION NO: 67
Which choice lists the correct order of events in the establishment of a TCP/IP connection?

A. Passive Open, Active Open, ACK
B. Passive Open, ACK, Active Open
C. Active Open, Active Open, ACK
D. Active Open, Passive Open, ACK

Answer: D

QUESTION NO: 68
Which layer of the OSI/RM stack controls the flow of information between hosts?

A. Data link layer
B. Physical layer
C. Network layer
D. Transport layer

Answer: D

QUESTION NO: 69
Why is the rlogin command dangerous to network security?

A. Remote logins are a security threat regardless of the protocol and should be avoided.
B. There is no way to prevent the user from becoming root if he successfully uses rlogin.
C. The rlogin command has a history of buffer overflows that has not been corrected.
D. The rlogin command relies on IP-based authentication, which is easily defeated.

Answer: D

QUESTION NO: 70
How frequently should risk analysis for a Solaris installation be conducted?

A. Never
B. Continuously
C. Prior to making changes.
D. When risk managers ask for it.

Answer: B

QUESTION NO: 71
Which three prevention tasks should be performed on a system before it is released into production? (Choose three)

A. Install the most recent release the Solaris 9 OE.
B. Force all users to set their own password at first login.
C. Apply the latest recommended patch cluster from sunsolve.sun.com.
D. Enable all network service to ensure that users have uninterrupted access to a system.
E. Collect md5 signatures of system binaries and store them on removable, read-only media.

Answer: A, C, E

QUESTION NO: 72
What has the highest priority when choosing safeguards?

A. Costs of the safeguard.
B. System administrator roles.
C. Replacement value of the asset.
D. Assessment that control provides maximum effectiveness.
E. Control cost compared with the asset that needs protection.

Answer: E

QUESTION NO: 73
Which of the following is an HTTP (Hypertext Transfer Protocol) extension or mechanism used to retain connection data, user information, history of sites visited, and can be used by attackers for spoofing an on-line identity?

A. HTTPS (Hypertext Transfer Protocol over SLL)
B. Cookies
C. HTTP (Hypertext Transfer Protocol)/1.0 Caching
D. vCard v3.0

Answer: B

QUESTION NO: 74
A decoy system that is designed to divert an attacker from accessing critical systems while collection information about the attacker's activity, and encouraging the attacker to stay on the system long enough for administrators to respond is known as a(n):

A. DMZ (Demilitarized Zone)
B. Honey pot
C. Intrusion detector
D. Screened host

Answer: B

QUESTION NO: 75
How must a firewall be configured to make sure that a company can communicate with other companies using SMTP (Simple Mail Transfer Protocol) e-mail?

A. Open TCP (Transmission Control Protocol) port 110 to all inbound and outbound connections.
B. Open UDP (User Datagram Protocol) port 110 to all inbound connections.
C. Open UDP (User Datagram Protocol) port 25 to all inbound connections.
D. Open TCP (Transmission Control Protocol) port 25 to all inbound and outbound connections.

Answer: D

QUESTION NO: 76
Which of the following is the greatest problem associated with Instant Messaging?

A. Widely deployed and difficult to control.
B. Created without security in mind.
C. Easily spoofed.
D. Created with file sharing enabled.

Answer: B

QUESTION NO: 77
The theft of network passwords without the use of software tools is an example of:

A. Trojan programs
B. Social engineering
C. Sniffing
D. Hacking

Answer: B

QUESTION NO: 78
An attacker can determine what network services are enabled on a target system by:

A. Installing a rootkit on the target system.
B. Checking the services file.
C. Enabling logging on the target system.
D. Running a port scan against the target system.

Answer: D

QUESTION NO: 79
A security consideration that is introduced by a VPN (Virtual Private Network) is:

A. An intruder can intercept VPN (Virtual Private Network) traffic and create a man in the middle attack.
B. Captured data is easily decrypted because there are a finite number of encryption keys.
C. Tunnelled data CANNOT be authenticated, authorized or accounted for.
D. A firewall CANNOT inspect encrypted traffic.

Answer: D

QUESTION NO: 80
Andreas is conducting a risk assessment of a network. He asks the following questions:

- **What is the target?**
- **How serious is the threat of intrusion?**
- **What is the probability of the threat occurring?**

Considering these questions, which step of risk assessment is Andreas conducting?

A. Analyzing, categorizing and prioritizing resources.
B. Using the existing management and control architecture.
C. Evaluating the existing perimeter and internal security.
D. Considering the business concerns.

Answer: A

QUESTION NO: 81
How do firewalls limit attacks waged from outside the network?

A. By requiring encrypted passwords.
B. By making internal IP addresses accessible only to authenticated users.
C. By making incoming traffic pass through source checks.
D. By not allowing external hosts to resolve MAC addresses.

Answer: C

QUESTION NO: 82
What is the best way to secure CGI scripts?

A. Configure the firewall to filter CGI at ports 80 and 443.
B. Disable anonymous HTTP logins when using CGI.
C. Ensure that the code checks all user input.
D. Activate Java on the primary Web server.

Answer: C

QUESTION NO: 83
Which port is used by HTTP to listen for secure connections?

A. UDP 80
B. TCP 443
C. TCP 8080
D. UDP 8080

Answer: B

QUESTION NO: 84
What is the Windows NT/2000 equivalent to a UNIX daemon?

A. A thread
B. A process
C. A protocol
D. A service

Answer: D

QUESTION NO: 85
Andreas must advise his users about which client to employ when accessing remote systems. Which of the following is a connection-oriented protocol that can contain unencrypted password information from Telnet sessions?

A. TCP
B. TTP
C. HTTP
D. UDP

Answer: A

QUESTION NO: 86
Which choice lists the ports used by Microsoft internal networking that should be blocked from outside access?

A. UDP 137 and 138, and TCP 139.
B. Ports 11, 112 and 79.
C. UDP 1028, 31337 and 6000.
D. Port 80, 134 and 31337.

Answer: A

QUESTION NO: 87
A computer on your network is responding very slowly to network request, and then it stops responding at all. You use a packet sniffer and create a filter that views packets being sent to that host. You see that the host is receiving thousands of ICMP packets a minute.
What type of attack is causing the system to slow down?

A. A spoofing attack.
B. A root kit installed on the system.
C. A denial-of-service attack.
D. A man-in-the-middle attack.

Answer: C

QUESTION NO: 88
A security administrator has a requirement to build a secure Solaris system.
What must be taken into account when obtaining software?

A. Signed patches are available.
B. md5 checksums will verify integrity.
C. CD-ROMs will always contain valid software.
D. Security patches will always be in the "Recommended and Security" patch cluster.

Answer: A

QUESTION NO: 89
Which three must a security administrator first identify and clearly understand before securing a new server? (Choose three)

A. Intended use of the system.
B. Disaster recover procedures.
C. Security policies and standards.
D. User account issuance processes.
E. Business and support requirements.

Answer: A, C, E

QUESTION NO: 90
Which two activities are components of a risk management process? (Choose two)

A. Falsifying OS type.
B. Selecting safeguards.
C. Implementing controls.
D. Masquerading as Nobody.
E. Writing flames to /dev/null(7D)

Answer: B, C

QUESTION NO: 91
An e-mail is received alerting the network administrator to the presence of a virus on the system if a specific executable file exists.
What should be the first course of action?

A. Investigate the e-mail as a possible hoax with a reputable anti-virus vendor.
B. Immediately search for and delete the file if discovered.
C. Broadcast a message to the entire organization to alert users to the presence of a virus.
D. Locate and download a patch to repair the file.

Answer: A

QUESTION NO: 92
What are three measures which aid in the prevention of a social engineering attack?

A. Education, limit available information and security policy.
B. Education, firewalls and security policy.
C. Security policy, firewalls and incident response.
D. Security policy, system logging and incident response.

Answer: A

QUESTION NO: 93
An inherent flaw of DAC (Discretionary Access Control) relating to security is:

A. DAC relies only on the identity of the user or process, leaving room for a Trojan horse.
B. DAC relies on certificates, allowing attackers to use those certificates.
C. DAC does not rely on the identity of a user, allowing anyone to use an account.
D. DAC has no known security flaws.

Answer: A

QUESTION NO: 94
Digital certificates can contain which of the following items:

A. The CA's (Certificate Authority) private key.
B. The certificate holder's private key.
C. The certificate's revocation information.
D. The certificate's validity period.

Answer: D

QUESTION NO: 95
What is the name of the risk assessment stage in which you bypass login accounts and passwords?

A. Penetration
B. Control
C. Activation
D. Discovery

Answer: A

QUESTION NO: 96

Helga's Web server is placed behind her corporate firewall. Currently, her firewall allows only VPN connections from other remote clients and networks. She wants to open the Internet-facing interface on her firewall so that it allows all users on the Internet to access her Web server.
Which of the following must Helga's rule contain?

A. Instructions allowing all UDP connections with a destination port of 80 and a source port of 1024.
B. Instructions allowing all UDP connections with a source port of 80 on the external interface and a destination port of 1024.
C. Instructions allowing all TCP connections with a source port of 80 on the internal interface and a destination port of 80,
D. Instructions allowing all TCP connections with a source port higher than 1024 and a destination port of 80.

Answer: D

QUESTION NO: 97
You are using a packet sniffer to capture transmissions between two remote systems. However, you find that you can only capture packets between your own system and another.
What is the problem?

A. You have configured your filter incorrectly.
B. You are sniffing packets in a switched network.
C. Tcpdump captures packets only between your host and another host.
D. Your system does not have its default gateway configured.

Answer: B

QUESTION NO: 98
Tavo wants to improve the security on his FTP server. He is especially worried about password-sniffing attacks.
Which of the following is the best action for Tavo to take?

A. Disable anonymous logins.
B. Allow only anonymous logins.
C. Configure the firewall to block port 21.
D. Place the FTP server outside of the firewall.

Answer: B

QUESTION NO: 99
Which type of attack specifically utilizes packet spoofing?

A. Crack attack
B. Smurf attack
C. Flood attack
D. Worm attack

Answer: B

QUESTION NO: 100
What is the purpose of blocking services on any given server?

A. To limit the number of targets a cracker can choose from.
B. To limit the number of processes that run at any given time, enhancing response time in case of a security breach.
C. To keep the operating system and its processes as simple as possible so administration is easier.
D. None, most services are needed and pose only minor security threats.

Answer: A

QUESTION NO: 101
Which three questions must be answered before a security policy can be determined? (Choose three)

A. What am I protecting?
B. What security tools are needed?
C. What applications do I need to patch?
D. Why am I protecting a specific system?
E. Who am I protecting my enterprise from?

Answer: A, D, E

QUESTION NO: 102
Which activity is considered a network security control?

A. Disabling the telnet service.
B. Installing a firewall at the perimeter of the network.
C. Implementing separate systems for LAN and WAN access.
D. Using a private (non-routable) Internet address range for your systems.

Answer: B

QUESTION NO: 103
Which two protocols are VPN (Virtual Private Network) tunneling protocols?

A. PPP (Point-to-Point Protocol) and SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol) and PPTP (Point-to-Point Tunneling Protocol)
C. L2TP (Layer Two Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol)
D. SMTP (Simple Mail Transfer Protocol) and L2TP (Layer Two Tunneling Protocol)

Answer: C

QUESTION NO: 104
The Diffie-Hellman algorithm allows:

A. Access to digital certificate stores from a certificate authority.
B. A secret key exchange over an insecure medium without any prior secrets.
C. Authentication without the use of hashing algorithms.
D. Multiple protocols to be used in key exchange negotiations.

Answer: B

QUESTION NO: 105
A DRP (Disaster Recovery Plan) typically includes which of the following:

A. Penetration testing

B. Risk assessment
C. DoS (Denial of Service) attack
D. ACLs (Access Control Lists)

Answer: B

QUESTION NO: 106
When assessing the risk to a machine or network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources.
B. Evaluating the existing perimeter and internal security.
C. Checking for a written security policy.
D. Analyzing the use of existing management and control architecture.

Answer: C

QUESTION NO: 107
Raul wants to ensure that a hacker cannot access his DNS zone files.
What action should he take at the firewall?

A. Filter TCP port 53, but allow UDP port 53 so that only certain DNS hosts can authenticate at the firewall.
B. Configure the firewall to accept zone transfer requests only from specific hosts.
C. Configure all routers to block zone transfers and encrypts zone transfer messages.
D. Disable nslookup on all hosts in the network, then disable named on the DNS server at certain times to thwart illicit zone transfers.

Answer: B

QUESTION NO: 108
Which choice lists the correct sequence of events in the termination of a TCP/IP connection?

A. Active Close, Passive Close, FIN, ACK
B. Passive Close, Active Close, FIN, ACK
C. Active Close, Passive Close, ACK, FIN

D. Passive Close, Active Close, ACK, FIN

Answer: A

QUESTION NO: 109
What is the primary function of IPSec?

A. It thwarts denial-of-service attacks.
B. It provides encryption.
C. It authenticates users.
D. It provides access control.

Answer: B

QUESTION NO: 110
Which action is most commonly associated with physical security?

A. Setting the OB security-mode to full.
B. Using a theft-protection cable to secure your laptop.
C. Installing a retinal scanner as part of the user authentication process.
D. Disabling the Stop-A sequence by setting KEYBOARD_ABORT in /etc/default/kbd.

Answer: B

QUESTION NO: 111
A server placed into service for the purpose of attracting potential intruder's attention is known as as:

A. Honey pot
B. Lame duck
C. Teaser
D. Pigeon

Answer: A

QUESTION NO: 112
LDAP (Lightweight Directory Access Protocol) directories are arranged as:

A. Linked lists
B. Trees
C. Stacks
D. Queues

Answer: B

QUESTION NO: 113
Non-repudiation is generally used to:

A. Protect the system from transmitting various viruses, worms and Trojan horses to other computers on the same network.
B. Protect the system from DoS (Denial of Service) attacks.
C. Prevent the sender or the receiver from denying that the communication between them has occurred.
D. Ensure the confidentiality and integrity of the communication.

Answer: C

QUESTION NO: 114
Which tool utilizes a database of known security problems to test a network?

A. Operating system add-on
B. Network scanner
C. Logging and log analysis tool
D. SNMP

Answer: B

QUESTION NO: 115
You want to secure your SMTP transmissions from sniffing attacks.

How can you accomplish this?

A. Forbid relaying.
B. Enforce masquerading.
C. Use an SSL certificate.
D. Use strict bounds checking on arrays.

Answer: C

QUESTION NO: 116
Which term describes the process of replacing valid source IP addresses with false IP addresses?

A. Hijacking
B. Spoofing
C. Spamming
D. Brute force

Answer: B

QUESTION NO: 117
What is the primary reason that systems are unsecure?

A. People
B. Passwords
C. Round of errors
D. Automaticity errors
E. Boundary condition errors
F. Time of check to time of use errors.

Answer: A

QUESTION NO: 118
Which two terms are associated with security threats? (Choose two)

A. Integrity

B. Scalability
C. Performance
D. Confidentiality

Answer: A, D

QUESTION NO: 119
Which of the following is the best description of "separation of duties"?

A. Assigning different parts of tasks to different employees.
B. Employees are granted only the privileges necessary to perform their tasks.
C. Each employee is granted specific information that is required to carry out a job function.
D. Screening employees before assigning them to a position.

Answer: A

QUESTION NO: 120
Which encryption key is used to verify a digital signature?

A. The signer's public key.
B. The signer's private key.
C. The recipient's public key.
D. The recipient's private key

Answer: B

QUESTION NO: 121
What is the final step in assessing the risk of network intrusion from an internal or external source?

A. Using the existing management and control architecture.
B. Evaluating the existing perimeter and internal security.
C. Analyzing, categorizing and prioritizing resources.
D. Considering the business concerns.

Answer: A

QUESTION NO: 122
What is the standard method for securing individual e-mail messages sent between a company and other users that do not use your e-mail server?

A. Invoke encryption at the e-mail server.
B. Invoke encryption on each client.
C. Filter firewall port 42 on the company firewall.
D. Store all e-mail messages on a separate partition.

Answer: B

QUESTION NO: 123
Which type of port is used by a network client when it establishes a TCP connection?

A. Ephemeral
B. Well-known
C. Restricted
D. Static

Answer: A

QUESTION NO: 124
Which single service can you disable to stop approximately two-thirds of the exploitation tools used against Windows NT/2000?

A. The Schedule service.
B. The POSIX subsystem with the C2Config tool.
C. The Ansi.sys from the boot loader.
D. The NetBIOS service.

Answer: D

QUESTION NO: 125
Which three topics must be described in an IT security policy? (Choose three)

A. Employees' work schedules.
B. Ownerships of systems and responsibilities
C. Password selection criteria and password aging schedules.
D. Documentation of user skills to identify potential user threats.
E. Backup schedules and expectations of restorations of lost data.

Answer: B, D, E

QUESTION NO: 126
The security administrator at TestKing.com needs to create an account `tess` for a temporary employee. The employee will only perform simple document editing, so must not be allowed to modify the login environment.
What is the correct way to add this user account?

A. `useradd -m -s /usr/bin/sh -d /export/home/guests/tess tess`
B. `useradd -m -s /usr/bin/ksh -d /export/home/guests/tess tess`
C. `useradd -m -s /usr/bin/rksh -d /export/home/guests/tess tess`
D. `useradd -m -s /usr/bin/pfksh -d /export/home/guests/tess tess`

Answer: D

QUESTION NO: 127
Exhibit:

```
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login auth requisite          pam_authtok_get.so.1
login auth required           pam_dhkeys.so.1
login auth required           pam_unix_auth.so.1
login auth required           pam_dial_auth.so.1
#
# rlogin service (explicit because of
pam_rhost_auth)
```

```
#
rlogin      auth sufficient
      pam_rhosts_auth.so.1
rlogin      auth requisite
      pam_authtok_get.so.1
rlogin      auth required            pam_dhkeys.so.1
rlogin      auth required
      pam_unix_auth.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh   auth sufficient         pam_rhosts_auth.so.1
rsh   auth required           pam_unix_auth.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
PPP   auth requisite          pam_authtok_get.so.1
PPP   auth required           pam_dhkeys.so.1
```

Based on the `/etc/pam.conf` file as shown in the exhibit, which service is responsible for the authentication for the `su(1)` command?

Answer:

QUESTION NO: 128
Which type of attack does the Solaris Fingerprint Database help prevent?

A. Trojan horse
B. Escalated privileged access
C. Host-based denial of service
D. Network-based denial of service

Answer: A

QUESTION NO: 129
Which type of attacker strikes the most often?

A. Insider
B. Terrorist
C. Ethical hacker
D. Black-hat hackers

Answer: A

QUESTION NO: 130
Why are Common Criteria evaluated systems desirable?

A. The products are better supported.
B. Their vendors are more reliable than others.
C. They have more security features than other systems.
D. A licensed third party has made an independent evaluation.

Answer:

QUESTION NO: 131
Which three files are used for trusted remote host and user equivalence? (Choose three)

A. `$HOME/.netrc`
B. `$HOME/.rhosts`
C. `$HOME/.shosts`
D. `/etc/hosts.deny`
E. `/etc/hosts.equiv`
F. `/etc/hosts.allow`

Answer:

QUESTION NO: 132
Which networks service can provide confidentiality of password data in transit over the network?

A. AH
B. IKE
C. scp

D. `/etc/shadow`

Answer: C
Explanation: scp transmits password in encrypted format.

QUESTION NO: 133
You are considering changing the information that `nmap -o` uses when fingerprinting a host.
What problem can occur if you change the output of "revealing information" in a Solaris configuration?

A. People will be confused.
B. Printing will be confusing.
C. A protocol specification will be violated.
D. Users will not know how to access their application.

Answer:

QUESTION NO: 134
You are in the process of configuring RBAC for a specific command that requires a single user name (or a numeric user ID) to run. After creating the appropriate entry in `/etc/security/exec_attr`, you should verify that the program will work using the `euid` of the user.
Why is this preferred?

A. If you specify the `uid`, then the program will gain all privileges.
B. If you specify the `uid`, then the program will always run as `uid=0`.
C. If you specify the `uid`, then the program will always run as seruid `root`.
D. If you specify the `uid`, then the program will gain the profiles of the `uid`.

Answer:

QUESTION NO: 135
Who performs Common Criteria evaluations?

A. Licensed private companies.
B. Agencies of the government.

C. The product vendor's original developers.
D. The product vendor's quality assurance staff.

Answer:

QUESTION NO: 136
Exhibit:

```
# eeprom security-mode=full
Changing PROM password:
New password:
Retype new password:
#
```

As the result of a weak security configuration, an attacker is able to gain local access to a system. Next, the attacker gains administrative access by exploiting a local buffer overflow in the `ufsrestore(1M)` program because it had not been properly patched. Continuing, the attacker executes the commands found in the exhibit.
What is the impact on the system?

A. There is no impact on the system because this command is no longer used in the Solaris 9 OE.
This setting is ignored and a message to that effect is sent to the `syslog` facility.
B. The system's configuration is automatically tuned for enhanced security.
This is done to protect the attacker's prize by preventing the system from being exploited by other attackers.
C. The system does not boo until a boot-time password is entered.
This is a form of denial of service because the security administrator does not know the password and will therefore not be able to boot the system.
D. The system panics because this parameter must only be set at run level 1.
Because this command makes a change to the system's programmable read-only (PROM) chip, changes must only be made to a system running in single user mode.

Answer: C

QUESTION NO: 137
To prevent regular users from filling up a file partition, you can specify a `minfree` option to `newfs`. If you forget to specify this option when the file system is created, the file system characteristics can be changed at a later time.
What is the name of the tool used to change the `minfree` threshold?

Answer:

QUESTION NO: 138
The system administrator finds a Trojaned login command using `md5` and the Solaris Fingerprint Database.
What is true about the system administrator's incident response tasks?

A. The server must be rebuilt.
B. BSM will identify the attacker.
C. All other replaced system files can be identified using `md5` and the Solaris Fingerprint Database.
D. All other replaced system files can be identified using `md5` and the Solaris Fingerprint Database and replaced with trusted versions.

Answer:

QUESTION NO: 139
During a security assessment of a Solaris OE system, the examiner finds the run-control script, `/etc/rc3.d/s20wyapp`. After verifying the need for this script with the system's custodian, the examiner notices that the script starts a program in `/opt/myapp/bin`.
Which is a possible security concern with this configuration?

A. There is no security concern with this configuration.
This is a common necessary practice for starting unbundled applications at boot time.
B. The program may have unmet dependencies on other software packages that cause the application to either fail or hang during the boot process.
C. The attacker may be owned by an application user.
If access to this user account can be obtained, and attacker can easily gain `root` access to the system.
D. The application started by the `/etc/rc3.d/s20myapp` run-control script may contain a locally exploitable buffer overflow causing the security of the system to be violated.

Answer:

QUESTION NO: 140
Which is part of a time of check, time of use (TOCTOU) attack?

A. Guessing a user password through automated tools or brute force methods.
B. Supplying a specially crafted argument list to the `ffbconfig(1M)` command.
C. Modifying a user's shell initialization files to add `/var/tmp/.../bin` directory to their `PATH` parameter.
D. Creating a symbolic link in the `/tmp` file system to exploit a race condition causing the `/.rhosts` file to be overwritten.

Answer:

QUESTION NO: 141
Which two describe attack methods that can cause a user to unexpectedly execute a Trojan horse instead of an intended `setuid` program? (Assume only that the user's shell initialization file is writable to the attacker)

A. Changing the user's `PATH` environment variable.
B. Changing the user's `LD_ORIGIN` environment variable.
C. Changing the user's `LD_LIBRARY_PATH` environment variable.
D. Executing the `pathconf(2)` command to reset the user's PATH.
E. Creating a shell alias of the same name pointing to the Trojan horse.

Answer:

QUESTION NO: 142
When should a security administrator consult the Solaris Fingerprint Database?

A. When any suspicious Solaris file is found.
B. When any suspicious application file is found.
C. When any suspicious Sun-supplied file is found.
D. When a suspicious Solaris kernel module is found.

Answer:

QUESTION NO: 143

Exhibit:

```
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login auth requisite          pam_authtok_get.so.1
login auth required           pam_dhkeys.so.1
login auth required           pam_unix_auth.so.1
login auth required           pam_dial_auth.so.1
#
# rlogin service (explicit because of
pam_rhost_auth)
#
rlogin     auth sufficient
      pam_rhosts_auth.so.1
rlogin     auth requisite
      pam_authtok_get.so.1
rlogin     auth required            pam_dhkeys.so.1
rlogin     auth required
      pam_unix_auth.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh   auth sufficient         pam_rhosts_auth.so.1
rsh   auth required          pam_unix_auth.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
PPP   auth requisite          pam_authtok_get.so.1
PPP   auth required          pam_dhkeys.so.1
```

TestKing.com has acquired a PAM module (`pam_otp.so.1`) that implements one-time passwords. As an administrator at TestKing you must enable this module for `telnet` access in such a way that all users are required to use one-time passwords for `telnet` access.
What change should you make to the default `/etc/pam.conf`?

A. Add a line to the `other` section that reads
   `other auth required pam_otp.so.1`
B. Add a new section for `telnet` that reads
   `telnet auth required pam_otp.so.1`
C. Add a new section for `telnet` that reads
   `telnet auth sufficient pam_otp.so.1`
D. Replace the line

```
other auth required pam_unix.so.1
```
with
```
other auth required pam_otp.so.1
```

Answer:

QUESTION NO: 144
The security administrator maintains a number of servers in a facility shared by other organizations. Which OBP commands can the security administrator execute to prevent OpenBoot PROM parameters from unauthorized modification?

A. Use `passwd` command to set security-password and `setenv` the `security-mode` to `command`.
B. Use `password` command to set security-password and `setenv` the `security-mode` to `command`.
C. Use `passwd` command to set security-password and `setenv` the `security-level` to `command`.
D. Use `password` command to set security-password and `setenv` the `security-level` to `command`.

Answer:

QUESTION NO: 145
Which option used in `/etc/vfstab` to limit the size of a `tmpfs(7FS)` file system to 512MB to prevent a memory denial of service (DoS)?

A. `size=1024k`
B. `size=512m`
C. `set size=512`
D. `swapfs=512mb`

Answer:

QUESTION NO: 146
Which log files should be trusted to track an intrusion after a remote attacker with root privileges compromises a system on a local area network (LAN)?

A. The `/var/adm/sulog` file.
B. The `/var/adm/wtmpx` file with read-only permissions.
C. The syslog `/var/adm/messages` file with read-only permissions.
D. The forwarded syslog log files on a remote system with console access only.

Answer: C
Explanation: Once root access is there attacker can erase his logs on the machine. So remote logs will be trusted.

QUESTION NO: 147
How should you configure BSM to help you detect whether an attacker has removed audit records?

A. Audit records already indicate this by default.
B. You execute the command `bsmconv +cnt` and reboot.
C. `auditconfig -setpolicy +cnt` should be added to `/etc/security/audit_startup`.
D. `auditconfig -setpolicy +seq` should be added to `/etc/security/audit_startup`.

Answer:

QUESTION NO: 148
Which three keywords are used to configure the `/etc/security/audit_control` file? (Choose three)

A. `dir`
B. `warn`
C. `minfree`
D. `naflags`
E. `minblocks`

Answer: A, C, D
Explanation: dir, minfree and naflags comes in audit_control

QUESTION NO: 149

A user that you are investigating is logged in on a system with BSM enabled. The user is running vi, and you need to log which files the user is accessing. Unfortunately, the `fr` class is not audited, so you want to explicitly alter the audit pre-selection mask for this vi process.
Which command allows you to do that?

A. `audit`
B. `reboot`
C. `auditconfig`
D. `/etc/init.d/audit`

Answer:

QUESTION NO: 150
What information is collected by process accounting? (Choose two)

A. UID and GID.
B. Files modified by users.
C. IP address of the remote host.
D. A process's controlling terminal.

Answer: A, D

QUESTION NO: 151
Which file is unused in device allocation?

A. `/etc/security/auth_attr`
B. `/etc/security/policy.conf`
C. `/etc/security/device_maps`
D. `/etc/security/lib/fd_clean`

Answer:

QUESTION NO: 152

A security administrator at TestKing wants to use log facility to enter a log entry when system virus scan scripting completes.
What can be done to configure this task?

A. Use the `logger` command.
B. Use the `syslogd` command.
C. Customize the `/etc/syslogd.conf` file.
D. Customize the `/etc/dumpadm.conf` file.

Answer:

QUESTION NO: 153
Which is an inappropriate activity for a device clean script?

A. Ejecting a diskette.
B. Mounting a CD-ROM.
C. Restoring the audio settings.
D. Communicating with the Volume Management daemon.
E. Instructing the user about turning the microphone on or off.

Answer:

QUESTION NO: 154
Which RBAC database associates users and roles with authorizations and rights?

A. `auth_attr`
B. `exec_attr`
C. `prof_attr`
D. `user_attr`

Answer:

QUESTION NO: 155
To which file does the Solaris 9 OE accounting facility log commands?

A. `/var/adm/utmpx`
B. `/var/adm/pacct`
C. `/var/adm/exacct`
D. `/var/log/syslog`

Answer:

QUESTION NO: 156
A security administrator has modified the `/etc/security/audit_control` file to enable the auditing of file delete events.
What is the next step that must be performed to begin logging these new events?

A. No further changes are needed to begin logging these new events.
B. The system must first be rebooted to begin logging these new events.
C. Use the `audit -s` command to update the runtime audit configuration.
D. Use the `audit -u` command to update the runtime audit configuration.
E. Use the `auditd -u` command to update the runtime audit configuration.

Answer: C
Explanation: audit –s updates the audit control information

QUESTION NO: 157
How does setting up network services like DNS and FTP in a `chroot` environment help prevent an attacker from gaining privileged access?

A. A `chroot` environment prevents buffer overflow attacks.
B. A `chroot` environment prevents an attacker from initiating a reliable port scan.
C. Programs are limited to executing in the `chroot` directories and not the main system directories.
D. An attacker cannot initiate a denial of service (DoS) on the network service running in the `chroot` environment.

Answer: C
Explanation: Chroot puts the attackers in chroot jail. They can not comeout of that jail and access the files

QUESTION NO: 158
Which three methods are features of the Solaris Security Toolkit for management of the output generated during a run? (Choose three)

A. Generate SNMP traps.
B. Send the output to the BSM audit trail.
C. Display the output to the controlling terminal.
D. Save the output to a file specified by the user.
E. Email the output to a user-defined email address.

Answer:

QUESTION NO: 159
By default, the Solaris 9 OE permits the use of remote authentication using trusted host databases such as `.rhosts` and `/etc/hosts.equiv`. This is a weak form of authentication that should not be used. What file should be modified to permit the use of `rlogin` but restrict the use of trusted host databases?

A. `/etc/pam.conf`
B. `/etc/services`
C. `/etc/default/rshd`
D. `/etc/default/inetd`
E. `/etc/inet/inetd.conf`

Answer:

QUESTION NO: 160
The company security policy requires all application servers to be hardened and minimized. A hardened and minimized application server is built and tested in a test network. The application server is deployed in a production network.
What is an operational limitation of this server?

A. The server does not contain every possible support tool.
B. Formerly unused services must be enabled before they can be used.
C. The Solaris Security Toolkit must be integrated with a JumpStart to create an automated repeatable build process.
D. Hardening and minimization requires additional work to prepare a server for deployment into a production environment.

Answer:

QUESTION NO: 161
Which Sun product provides enterprise authentication?

A. PAM
B. IPSec
C. SunScreen
D. Sun Kerberos
E. Trusted Solaris

Answer:

QUESTION NO: 162
You are asked to help with root cause analysis of an application failure in a development Solaris server that you hardened with the Solaris Security Toolkit.
What must be done to enable an `inetd` service that is thought to be the problem?

A. Use the `init 1` command.
B. Use the `pkill -TERM inetd` command.
C. Use the `enable-inetd <servicename>` command and run the `pkill -HUP inetd` command.
D. Modify `JASS_SVCS_ENABLE` and execute the Solaris Security Toolkit and `pkill -HUP inetd` commands.

Answer:

QUESTION NO: 163
After running a network scanner, a security administrator at TestKing determines that a system is configured to use a weak initial sequence number (ISN) algorithm. Knowing that this is not the default value in the Solaris OE, the administrator changes the system to use the algorithm defined by RFC 1948.
What file and parameter was modified by the administrator?

A. `/etc/default/network` and `DEFAULT_ISN`

B. `/etc/default/init` and `TCP_STRONG_ISS`
C. `/etc/default/inet` and `ISN_DEFAULT_MODE`
D. `/etc/default/inetinit` and `TCP_STRONG_ISS`
E. `/etc/default/initinet` and `TCP_STRONG_ISN`

Answer:

QUESTION NO: 164
What is the functional purpose of the Solaris Security Toolkit?

A. Patching
B. Hardening
C. JumpStart
D. Authentication
E. Non-repudiation

Answer:

QUESTION NO: 165
Your company has implemented a policy that states that accounts should become unavailable if they have not been used in 21 days.
How is account inactivity calculated in the Solaris 9 OE if no naming service is used?

A. An entry in the `/var/adm/lastlog` file.
B. The last user entry in the `/var/adm/wtmpx` file.
C. The password timestamp in the `/etc/shadow` file.
D. The number of days since the user's last password change.

Answer: C
Explanation: Shadow file has a field for entering max. account inactivity

QUESTION NO: 166
What are three capabilities of Solaris SunScreen Firewall? (Choose three)

A. It provides stateful packet inspection.

B. It provides encryption and IPSec-based VPNs.
C. It provides virus scanning and spam protection.
D. It provides central administration using encryption.
E. It provides general-purpose network intrusion detection.

Answer: A, B

QUESTION NO: 167
Exhibit:

```
#./jass=check_sum
File Name                Saved CkSum      Current CkSum
-----------------------------------------------------
----
/etc/inet/inetd.conf     1207314467:5799
224920179:5801
/etc/.login              4057522760:574
1288382808:584
```

What is the significance of the output generated by the `jass=check=sum` command shown in the exhibit?

A. The two files were deleted since the last Solaris Security Toolkit run.
B. The two files were created since the last Solaris Security Toolkit run.
C. The two files were modified since the last Solaris Security Toolkit run.
D. The two files were archived since the last Solaris Security Toolkit run.

Answer: C

QUESTION NO: 168
Exhibit:
Connection 1

```
$ telnet testking.com
Trying 10.100.0.24...
Connected to testking.com.
Escape character is '^]'
Connection to testking.com closed by foreign host.
```

Connection 2

```
$ telnet testking.com
Trying 10.100.0.24...
telnet: Unable to connect to remote host: Connection refused
```

Connection 3

```
$ telnet testking.com
testking.com: Unknown host
```

Connection 4

```
$ telnet testking.com
Trying 10.100.0.24...
Connected to testking.com
Escape character is '^]'.

SunOS 5.9

login: testking
Password:
Login incorrect
```

Which connection demonstrates that `telnet` has been denied using TCP Wrappers?

A. Connection 1
B. Connection 2
C. Connection 3
D. Connection 4

Answer: A
Explanation: This one I tried on a server with wrappers installed.

QUESTION NO: 169
TCP Wrappers functionality is integrated into the inetd service in the Solaris 9 OE. Which syslog facility is used by inetd when TCP Wrappers messages are generated?

A. `LOG_AUTH`
B. `LOG_DAEMON`
C. Depends on the configuration in `/etc/syslogd.conf`

D. Depends on the configuration in `/etc/default/inetd`

Answer:

QUESTION NO: 170
What is the safest setting for the Protocol variable in the `etc/ssh/sshd_config` file?

A. Protocol 1
B. Protocol 2
C. Protocol any
D. Protocol 1, 2
E. Protocol 1, 2, 3

Answer: B

QUESTION NO: 171
You want to enable TCP port-forwarding for `ssh`.
Which settings should you check?

A. Make sure protocol version 1 is enabled.
B. Make sure protocol version 1 is disabled.
C. Set `AllowTopForwarding` to `yes` in `/etc/ssh/ssh_config`
D. Set `AllowTcpForwarding` to `yes` in `/etc/ssh/sshd_config`

Answer: D

QUESTION NO: 172
You want to enable your users to use `ssh` to log in to your system, and forward X11 connections from your server to their workstations. The server sits behind a firewall that refuses all incoming and outgoing connections.
Which port(s) should you open on the firewall?

A. 22 only
B. 22 and 600
C. 22 and 6010

D. 22 and 6010-6020

Answer: A

QUESTION NO: 173
Which identifies a message digest algorithm?

A. MD5
B. DSA
C. DES
D. SSL

Answer: A

QUESTION NO: 174
What does the `/usr/bin/ssh-agent` command provide?

A. Host private key store
B. User private key store
C. System-wide known hosts database
D. User-specific known hosts database

Answer: B

QUESTION NO: 175
When should `ssh` host keys be replaced? (Choose two)

A. Never
B. Once a year if 4096 bit keys are used.
C. When a server has been compromised.
D. As soon as a vulnerability is found in `sshd`.
E. As dictated by the organization's security policy.

Answer: C, E

QUESTION NO: 176
Which condition is impossible to configure using Access Control Lists (ACLs)?

A. Preventing specific users from executing a file.
B. Allowing multiple users to modify the ACL of a file.
C. Allowing multiple groups to have read-only access to a file.
D. Creating files in a directory that automatically inherit individual user access modes.

Answer:

QUESTION NO: 177
You want to display a legal banner to users connecting to your system from outside the local network using `telnet`. This banner should be displayed before the user enters any account information. Your legal text is in `/etc/default/banners/`.
What two configuration changes do you need to make? (Choose two)

A. Add the banner to `/etc/motd`.
B. Add the banner to `/etc/issue`.
C. Add a line for `in.telnetd` with a banners option in `/etc/hosts.deny`.
D. Add a line for `in.telnetd` with a banners option in `/etc/hosts.allow`.

Answer: A, B

QUESTION NO: 178
While looking for dormant accounts, you notice that `lastlog` has become very large. Because space is tight on your `/var` partition, you decide to add this file to the lost of files that is rotated by `logadm`.
Why is this a bad decision?

A. Password expiration does not work anymore.
B. Account inactivity can no longer be computed.
C. The `last(1M)` command does not work anymore.
D. `lastlog` contains binary data and will not compress well.

Answer: D
Explanation: lastlog cannot be compressed using logadm

Note: Answers to the unanswered questions will be provided shortly. First customer, if any, faster than the TestKing team in proving the answers will receive credit:

- for each answer provided
- special credit for all unanswered questions

Send answers to feedback@testking.com.

www.testking.com