



Exam : 310-301

Title : Sun Certified Security Administrator

Ver : 10.27.08

QUESTION 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 20:

Which port or ports are used for SMTP?

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

Answer: B

QUESTION 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 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 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 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 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 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 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 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 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 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 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 32:

A virus that hides itself by intercepting disk access requests is:

- A. Multipartite
- B. Stealth
- C. Interceptor
- D. Polymorphic

Answer: B

QUESTION 33:

File encryption using symmetric cryptography satisfies what security requirement?

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

Answer: A

QUESTION 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 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 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 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 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 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 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 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 42:

Which device is similar to a packet filter, 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 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 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 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 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 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 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 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 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 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 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 53:

What are three platform security mechanisms? (Choose three)

- A. EAL
- B. PAM
- C. ESP
- D. BSM
- E. OCSP

Answer: B, D, E

QUESTION 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

QUESTION 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 56:

An 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 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 58:

Searching through trash is used by an attacker to acquire data such as network diagrams, IP (Internet Protocol) address lists and:

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

Answer: C

QUESTION 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 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 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 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 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 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 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 66:

Which port does FTP use for a control connection?

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

Answer: A

QUESTION 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 98:

Tavowants 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 99:

Which type of attack specifically utilizes packet spoofing?

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

Answer: B

QUESTION 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 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 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 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 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 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 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 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 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 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 110:

Which action is most commonly associated with physical security?

- A. Setting the OBsecurity-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 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 112:

LDAP (Lightweight Directory Access Protocol) directories are arranged as:

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

Answer: B

QUESTION 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 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 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 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 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 118:

Which two terms are associated with security threats? (Choose two)

- A. Integrity
- B. Scalability
- C. Performance
- D. Confidentiality

Answer: A, D

QUESTION 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 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 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 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 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 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 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, C, E
SC-300, 1-41

QUESTION 126:

The security administrator at Certkiller .com needs to create an account Jackfor 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/Jack Jack
- B. useradd-m -s /usr/bin/ksh -d /export/home/guests/Jack Jack
- C. useradd-m -s /usr/bin/rksh -d /export/home/guests/Jack Jack
- D. useradd-m -s /usr/bin/pfksh -d /export/home/guests/Jack

Jack

Answer: C

QUESTION 127:

Exhibit:

```
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
loginauth requisite pam_authtok_get.so.1
loginauth required pam_dhkeys.so.1
loginauth required pam_unix_auth.so.1
loginauth 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: Other

QUESTION 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 129:

Which type of attacker strikes the most often?

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

Answer: A

QUESTION 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: D

QUESTION 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: A, C, E

QUESTION 132:

Which network 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 133:

You are considering changing the information that nmap-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: C

QUESTION 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: D

QUESTION 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: A

QUESTION 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 boot 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 137:

CORRECT TEXT

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 minfreethreshold?

Answer: tuneefs

QUESTION 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: A

QUESTION 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: C

QUESTION 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: D

QUESTION 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: B, D

QUESTION 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: A

QUESTION 143:

Exhibit:

```
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login auth requisite pam_authok_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
Certkiller .com has acquired a PAM module (pam_otp.so.1)that implements one-time
passwords. As an administrator at Certkiller you must enable this module for
telnetaccess in such a way that all users are required to use
one-time passwords for telnetaccess.
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: B

QUESTION 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: B

QUESTION 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: B

QUESTION 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: D

QUESTION 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: D

QUESTION 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 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 frclass 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: C

QUESTION 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 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: B

QUESTION 152:

A security administrator at Certkiller 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: A

QUESTION 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: D

QUESTION 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: D

QUESTION 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: C

QUESTION 156:

A security administrator has modified the /etc/security/audit_controlfile 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 -scommand to update the runtime audit configuration.
- D. Use the audit -ucommand 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 157:

How does setting up network services like DNS and FTP in a chrootenvironment 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 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: A, C, E

QUESTION 159:

Exhibit:

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

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. A
- B. B
- C. C
- D. D
- E. E

Answer: A

QUESTION 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: A

QUESTION 161:

Which Sun product provides enterprise authentication?

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

Answer: D

QUESTION 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 `kill -TERM inetd` command.
- C. Use the `enable-inetd <servicename>` command and run the `kill -HUP inetd` command.
- D. Modify `JASS_SVCS_ENABLE` and execute the Solaris Security Toolkit and `kill -HUP inetd` commands.

Answer: D

QUESTION 163:

After running a network scanner, a security administrator at Certkiller 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: D

QUESTION 164:

What is the functional purpose of the Solaris Security Toolkit?

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

Answer: B

QUESTION 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: A

QUESTION 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, D

QUESTION 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=sumcommand 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 168:

Exhibit:

Connection 1

\$ telnet Certkiller .com

Trying 10.100.0.24...

Connected to Certkiller .com.

Escape character is '^['

Connection to Certkiller .com closed by foreign host.

Connection 2

\$ telnet Certkiller .com

Trying 10.100.0.24...

telnet: Unable to connect to remote host: Connection refused

Connection 3

\$ telnet Certkiller .com

Certkiller .com: Unknown host

Connection 4

\$ telnet Certkiller .com

Trying 10.100.0.24...

Connected to Certkiller .com

Escape character is '^['.

SunOS 5.9

login: Certkiller

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 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: B

QUESTION 170:

What is the safest setting for the Protocol variable in the etc/ssh/sshd_configfile?

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

Answer: B

QUESTION 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 AllowTcpForwarding to yes in /etc/ssh/ssh_config
- D. set AllowTcpForwarding to yes in /etc/ssh/sshd_config

Answer: D

QUESTION 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 173:

Which identifies a message digest algorithm?

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

Answer: A

QUESTION 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 175:

When should sshhost 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 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: B

QUESTION 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 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 list 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: B

QUESTION 179:

Which statement is true about the `crypt(1)` command?

- A. It uses a weaker encryption algorithm than DES.
- B. It uses DES encryption algorithm which uses 64-bit key.
- C. It uses AES encryption algorithm which uses 128-bit key.
- D. It uses 3DES encryption algorithm which uses 168-bit key.

Answer: A

QUESTION 180:

Exhibit

```
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login auth required          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
```

Certkiller .com has acquired a PAM module to implement dictionary checks at password-change time.

Where should this module be declared in the PAM stack to install it as an additional strength checking measure? (Choose Two.)

- A. Before the line containing pam_dhkeys.so.1
- B. After the line containing pam_authtok_check.so.1
- C. After the line containing pam_authtok_store.so.1
- D. Before the line containing pam_authtok_check.so.1

Answer: B, D

QUESTION 181:

What are three results of a fork-bomb denial of service (DoS) attack on a CPU? (Choose

three)

- A. The system will become completely unresponsive
- B. The system runs out of memory while allocating new processes
- C. Users already logged on will not be affected because they already have allocated CPU resources
- D. The process table reaches its limit and there are no process table slots left to execute a new process
- E. The process table grows dynamically to accommodate the fork bomb until the system runs out of memory

Answer: A, D, E

QUESTION 182:

Which two statements are true about the key management mechanism for Solaris IPSec?
(Choose two)

- A. It supports SKIP
- B. It supports IDEA encryption
- C. It supports pre-shared key-based authentication
- D. It does not support manual keying for authentication
- E. It supports public key certificate-based authentication

Answer: A, C

QUESTION 183:

How is it possible to control processes dispatched by init?

- A. Configure TCP wrappers
- B. Configure /etc/inittab
- C. Configure /etc/inet/init. Conf
- D. Configure /etc/inet/inetd.conf

Answer: B

QUESTION 184:

Exhibit, Part #1

```
# Authentication management
#
# login service (explicit because of
pam_dial_auth)
#
login auth required
    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
```

Exhibit, Part #2

```
    pam_authtok_get.so.1
ppp    auth required
    pam_dhkeys.so.1
ppp    auth required
    pam_unix_auth.so.1
ppp    auth required
    pam_dial_auth.so.1
#
# Default definition for Authentication
management
# Used when service name is not explicitly
mentioned
#
other auth requisite
    pam_authtok_get.so.1
other auth required
    pam_dhkeys.so.1
other auth required
    pam_unix_auth.so.1
#
# passwd command (explicit because of a
different
# authentication module)
#
passwd    auth required
    pam_passwd_auth.so.1
#
# cron service (explicit because of
non-usage
# of pam_roles.so.1)
#
cron    account required    pam_projects.so.1
cron    account required
    pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly
mentioned
# for account management
#
```

Exhibit, Part #3


```
# of pam_roles.so.1)
#
cron account required pam_projects.so.1
cron account required
    pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly
mentioned
# for account management
#
other account requisite pam_roles.so.1
other account required pam_projects.so.1
other account required
    pam_unix_account.so.1
#
# Default definition for Session management
# Used when service name is not explicitly
mentioned
# for session management
#
other session required
    pam_unix_account.so.1
#
# Default definition for Password
management
# Used when service name is not explicitly
mentioned
# for password management
#
other password required pam_dhkeys.so.1
other password requisite
    pam_authtok_get.so.1
other password requisite
    pam_authtok_check.so.1
other password required
    pam_authtok_store.so.1
```

The pam_rhost_auth.so.1 module is sufficient.

If this module succeeds, what other PAM modules are executed to authenticate the user?

- A. No other modules are executed
- B. The additional modules defined in the other authentication stack are executed
- C. The rest of the PAM stack defined for rlogin is executed, but any errors encountered are ignored
- D. The rest of the PAM stack defined for rlogin is executed and errors encountered will result in a failed login attempt

Answer: A

QUESTION 185:

How do you enable the logging of PAM messages for the login service?

- A. Update /etc/syslog.conf to enable logging for auth
- B. Update /etc/policy.conf to enable logging for auth
- C. Update /etc/default/login to enable logging for auth
- D. Update /etc/pam.conf to add the logging for each auth statement

Answer: A

QUESTION 186:

Network segmentation is a highly recommended mechanism to protect your JumpStart environment. What is the most secure configuration for protecting JumpStart in a data center?

- A. Physically isolate the JumpStart servers
- B. Use VLANs to achieve network segmentation
- C. Use firewall rules to permit JumpStart network traffic only
- D. Segment the network using static hardware address assignment

Answer: A

QUESTION 187:

The date is Monday, March 1, 2003. Certkiller .com hired a consultant to work on your system. The consultant needs temporary shell access for the week and will finish on Friday. The account will be called temp.

Which policy absolutely disables the shell account after Friday?

- A. usermod -f 5 temp
- B. passwd -l -e 5 temp
- C. passwd -f 3/5/2003 temp
- D. usermod -e 3/5/2003 temp

Answer: D

QUESTION 188:

Which command is used to print all world-writable files?

- A. find / -perm -a=w -print
- B. find / -perm -o=w -print
- C. find / -perm -u=w -print
- D. find / -perm -a=777 -print

Answer: B

QUESTION 189:

Your work as an administrator at Certkiller .com. You are setting up an application server on a Solaris 9 system. This application will be configured using the user app. This user does not require shell access to the system.

What is the most secure way to add a user?

- A. `useradd -d /export/home/app -m app`
- B. `useradd -d /export/home/app -m -s /bin/csh app`
- C. `useradd -d /export/home/app -m -s /bin/false app`
- D. `useradd -d /export/home/app -m -k /etc/skel -s /bin/csh app`

Answer: C

QUESTION 190:

A number of users is allowed to su (1M) to a role named groupadm. You want to track file system alterations made by this role and correlate the alterations to the actual user.

What form of logging do you need?

- A. BSM auditing
- B. `/var/adm/sulog`
- C. process accounting
- D. TCP Wrapper logging

Answer: A

QUESTION 191:

A file system stores static application data only.

How should this file system be mounted most defensively in `/etc/vfstab`?

- A. `/dev/dsk/c0t3d0s6 /dev/rdsk/c0t3d0s6 /opt ufs 2 yes`
- B. `/dev/dsk/c0t3d0s6 /dev/rdsk/c0t3d0s6 /opt ufs 2 yes ro`
- C. `/dev/dsk/c0t3d0s6 /dev/rdsk/c0t3d0s6 /opt ufs 2 yes nosuid`
- D. `/dev/dsk/c0t3d0s6 /dev/rdsk/c0t3d0s6 /opt ufs 2 yes nosuid,ro`

Answer: D

QUESTION 192:

A system user exploits a buffer overflow to become root.

What type of attack is it?

- A. Port scan attack
- B. Superuser attack
- C. Resource exhaustion attack
- D. Escalated privileged access attack

Answer: D

QUESTION 193:

Which statement is true about Discretionary Access Control?

- A. All access to objects must be audited
- B. Users must take explicit action to share files
- C. Users must have sufficient clearance to view an object
- D. The owner of the data is authorized to grant access to any user

Answer: D

QUESTION 194:

What kind of compromise renders the system untrusted?

- A. A fork-bomb attack
- B. Exhaustion of free disk space
- C. Buffer overflow in a daemon process
- D. Network saturation due to excessive scanning

Answer: C

QUESTION 195:

What problem can occur when sending intrusion detection information over a network?

- A. Attackers may cover their steps
- B. Attackers may observe your capabilities by watching the network
- C. Attackers may hijack a UDP network stream to the intrusion detection information collection system
- D. Attackers may lead you to believe that they are after a network target that they are not really interested in.

Answer: B

QUESTION 196:

Your work as a security administrator at Certkiller .com. A site security policy dictates that

the root account is never permitted to remotely log in to a system. A root shell should only be obtained through the use of the su (1) command. You set the CONSOLE parameter in the /etc/default/login file. You then attempt to remotely access the system using the Solaris Secure Shell as the root account and surprisingly is able to log in.

Why is this problem?

- A. DenyRootLogin is set to No in /etc/ssh/sshd_config
- B. AdminRootLogin is set to Yes in /etc/ssh/sshd_config
- C. AllowRootLogin is set to Yes in /etc/ssh/sshd_config
- D. EnableRootLogin is set to Yes in /etc/ssh/sshd_config
- E. PermitRootLogin is set to Yes in /etc/ssh/sshd_config

Answer: E

QUESTION 197:

You need to configure TCP Wrappers to allow access to all wrapped services to the private local area network (LAN). The LAN is on a Class C network with a network address of 192.168.1.0.

Which is the correct configuration in the /etc/hosts.allow file?

- A. All:192.168.1.0
- B. All:192.168.1.255
- C. All:192.168.1.0/24
- D. All:192.168.1.255/24
- E. All:192.168.1.0/255.255.255.0

Answer: E

QUESTION 198:

By default, sshd is not configured to tunnel X11 connections. How can this functionality be enabled?

- A. run the ssh command with the -x option
- B. run the sshd command with the -x option
- C. set x11Forwarding to yes in /etc/ssh/ssh_config
- D. set x11Forwarding to yes in /etc/ssh/sshd_config

Answer: D

QUESTION 199:

When you receive signed email and the digital signature is validated by your email application, you can be assured _____.

- A. The return address of the email is valid
- B. Your mail has not been read by anyone else
- C. The message has not been modified in transit
- D. The sender knows that you have received the mail

Answer: C

QUESTION 200:

/var/adm/messages contains this output:
Jan 28 21:23:18 mailhost in.telnetd[20911]:
[ID 808958 daemon.warning] refused connect from
ns.foo.com {access denied}
why was this line generated?

- A. A user connecting from ns.foo.com failed to authenticate
- B. The user daemon is not allowed to log in from ns.foo.com
- C. A portscan was run against mailhost from ns.foo.com
- D. The TCP Wrapper configuration does not allow telnet connections from ns.foo.com

Answer: D

QUESTION 201:

What should you do to enable the Solaris Secure Shell in the Solaris 9 OE?

- A. Run the command /etc/default/sshd
- B. Run the command touch/etc/sshd/startup
- C. Run the command /usr/local/sshd/startup
- D. You do nothing. The service is enabled by default.

Answer: D

QUESTION 202:

Which threat can be mitigated by setting the Open Boot PROM security mode to full?

- A. System panics
- B. Booting into single user mode
- C. Remotely accessing the console
- D. Logging in as root at the console

Answer: B

QUESTION 203:

An attacker has compromised a system by guessing a user account. The attacker then escalates privileges through a Trojan horse. The attacker will then put back doors on the system.

What enables a remote root shell, bypassing the PAM mechanism?

- A. echo + > /.rhosts
- B. cp /bin/ksh /bin/lpd
Chmod 4555 /bin/lpd
- C. echo 'ingeslock stream tcp nowait root /bin/sh sh -i' >> /tmp/ .x; inetd -s /tmp/ .x
- D. echo "bob:x:0:1:::/bin/bash" >> /etc/passwd;
echo "bob::6445::::::" >> /etc/shadow

Answer: C

QUESTION 204:

Which is NOT a result of a host-based denial of service attack?

- A. Unresponsiveness due to memory depletion
- B. Inability to store data due to disk space exhaustion
- C. Inability to spawn new tasks due to CPU congestion
- D. Unreachability due to excessive ICMP broadcast packets

Answer: D

QUESTION 205:

You decide that it may be a good idea to prevent Trojan horse and backdoor attacks. Which three commands are often replaced by root kits? (Choose three)

- A. ps(1)
- B. bc(1)
- C. ls(1)
- D. login(1)

Answer: A, C, D

QUESTION 206:

You are asked to manually verify a Solaris Security Toolkit configuration. What should you do?

- A. Run the command ps -elf
- B. Run the command netstat -an
- C. Run the command netstat -an and ps -elf
- D. Integrate your verification process into the application QA test plans

Answer: D

QUESTION 207:

How do you distinguish between denial of service attacks and programming errors?

- A. You cannot make this distinction
- B. You examine the audit events for the process
- C. You verify that the process user ID is that of a valid user
- D. You check the binary against the Solaris Fingerprint Database

Answer: A

QUESTION 208:

/var filled up, and even though you delete some large files, /var immediately fills up again. Apparently, some process is writing to a file in /var at high speed. You use /bin/find to search for a large and recently changed file in /var, but nothing shows up. What is the reason?

- A. The file name starts with a '.', so it is hidden
- B. The file is a soft link to a file on another file system
- C. The file is a hard link to a file on another file system
- D. The file has been deleted, but is still opened by a process

Answer: D

QUESTION 209:

You suspect that the ls (1) command may have been Trojaned on a Solaris 9 OE system. What can you use to list the contents of a directory prior to starting your forensic analysis?

- A. Nothing
- B. The vi editor
- C. The echo shell built-in
- D. The nawk(1) command

Answer: C

QUESTION 210:

Your work as an administrator at Certkiller .com. You suspect that one of your systems has been compromised. You want to inspect the system's binaries and kernel modules by checksumming them and comparing them to the Solaris Fingerprint Database.

What prerequisite step should you take before generating the checksums?

- A. Make sure all users are logged out
- B. Bring the system down to single user level
- C. Shut down the system, and analyze the system's disk on a trusted system
- D. Reboot the system into single user mode to make sure any running Trojan horses are terminated

Answer: C

QUESTION 211:

A security administrator is reviewing the BSM configuration on a system. While looking at the `/etc/security/audit_control` file, the administrator finds that the system is configured to audit the `fa` audit class.

Which two statements are true? (Choose two)

- A. The security of the system will be significantly enhanced
- B. The performance of the system will be significantly degraded
- C. The performance of the system will be significantly enhanced
- D. The system will audit all failures and alert events on the system
- E. The system will audit all file accesses for all users and processes
- F. The system will audit all failed administrative actions on the system

Answer: A, B

QUESTION 212:

Which command is used to configure BSM to track all arguments to an executed command?

- A. `audit -c ex +argv`
- B. `audit -setpolicy -c ex`
- C. `auditconfig -setpolicy +cnt`
- D. `auditconfig -setpolicy +argv`

Answer: D

QUESTION 213:

Your work as an administrator at Certkiller .com. You administer a system which has BSM enabled. You just added an extra audit-class to the `flag:` entry in `/etc/security/audit_control`, and you executed `audit -s`. Now you want to validate that this extra class is audited correctly, so you execute a command that should generate an audit record. Unfortunately, nothing appears in the audit log because the audit pre-selection mask is not yet in effect.

What do you minimally need to do to get the pre-selection mask in effect for your test?

- A. Reboot
- B. Restart auditd
- C. Execute audit -n
- D. Start a new login session

Answer: D

QUESTION 214:

Exhibit.

```
header,81,2,login - telnet,,Wed 29 Jan 2003
08:12:33 PM EST, + 356 msec
subject,joe,joe,other,joe,other,497,497,8194
65559 localhost
text,successful login
return,success,0

[...]

header,142,2,execve(2),,Wed 29 Jan 2003
08:12:41 PM EST, + 865 msec
path,/usr/sbin/ufsrestore
attribute,104555,root,hin,8388608,7699,0
exec_args,1,
/usr/sbin/ufsrestore
subject,joe,root,other,joe,other,502,497,8194
65559 localhost
return,success,0

header,119,2,execve(2),,Wed 29 Jan 2003
08:12:41 PM EST, + 871 msec
path,/usr/bin/sh
attribute,100555,root,root,8388608,390,0
exec_args,2,
sh,-p
subject,joe,root,other,joe,other,502,497,8194
65559 localhost
return,success,0

header,118,2,execve(2),,Wed 29 Jan 2003
08:13:55 PM EST, + 426 msec
path,/usr/sbin/modload
attribute,100555,root,hin,8388608,1628,0
exec_args,2,
/usr/sbin/modload,0w3nd
subject,joe,root,other,joe,other,503,497,8194
65559 localhost
return,success,0
```

During a review of a BSM audit trail, a security administrator detected an interesting sequence of commands.

Which two did the administrator find? (Choose two)

- A. The user joe was able to load a new kernel module
- B. The ufsrestore command was exploited to gain a root shell
- C. The ufsrestore command was used to unload a kernel module
- D. The ufsrestore command was used to overwrite /etc/passwd
- E. The user joe logged in while a root user was restoring the system
- F. Two users, joe and root, were working on the system at the same time

Answer: A, F

QUESTION 215:

A site security policy dictates that all failed logins to critical systems must be logged and monitored.

Which parameter must be changed in /etc/default/login to enable this functionality?

- A. SYSLOG
- B. LOG_LOGIN_FAILURES
- C. SYSLOG_LOG_FAILURES
- D. LOG_SYSLOG_FAILURES
- E. SYSLOG_FAILED_LOGINS

Answer: E

QUESTION 216:

To detect if user sam has assumed the identity of user bob on a system, which log file should the security administrator check?

- A. /var/adm/sulog
- B. /var/log/aculog
- C. /var/adm/lastlog
- D. /var/log/authlog

Answer: A

QUESTION 217:

When BSM is enabled, which command results in the execution of a device clean script?

- A. mount
- B. share
- C. volcheck
- D. deallocate

Answer: D

QUESTION 218:

Which type of user interactions will Solaris process accounting report?

- A. User logon/logoff records
- B. The system calls used by the process
- C. The user ID of the user executing the su (1M) command
- D. The user ID being switched to with the su (1M) command

Answer: C

QUESTION 219:

Which IPSec mechanism provides confidentiality for network traffic?

- A. AH
- B. IKE
- C. ESP
- D. SKIP

Answer: C

QUESTION 220:

Given:

`rpcinfo -p Certkiller`

If an attacker has penetrated a local area network (LAN), the attacker can use the `rpcinfo` command to gather intelligence about a system running RPC. When run against the host Certkiller, which type of information will the command return to the attacker?

- A. Query all open ports on Certkiller and report which ports have bound RPC applications
- B. Query all open RPC ports on Certkiller and report the RPC applications bound to those ports
- C. Query the `rpcbind` daemon on Certkiller and report all of the registered RPC applications
- D. Query the `rpcbind` daemon on Certkiller and report all of the process IDs (PID) of running RPC applications

Answer: C

QUESTION 221:

DRAG DROP

You work as a network administrator at Certkiller .com. Your boss, Mrs. Certkiller,

310-301

orders you to place each RBAC term to its description. You need to comply.

Term	Description
Place here	account that performs privileged tasks
Place here	a grouping of one or more commands
Place here	grants privileged access to an application
Place here	user attributes checked by applications

PROFILE	EXECUTION ATTRIBUTES
ROLE	AUTHORIZATIONS

Answer:

Term	Description
ROLE	account that performs privileged tasks
PROFILE	a grouping of one or more commands
AUTHORIZATIONS	grants privileged access to an application
EXECUTION ATTRIBUTES	user attributes checked by applications

QUESTION 222:

DRAG DROP

You work as a network administrator at Certkiller .com. Your boss, Mrs. Certkiller, orders you to place the Solaris Security Toolkit directories on their matching description. You need to comply.

Solaris Security Toolkit Directory	Directory Description
Place here	stores system installation settings used by JumpStart
Place here	stores the Toolkit framework, configuration, and security profile files
Place here	stores individual security scripts used to harden a system
Place here	stores copies of a filesystem objects that are copied to a system
Place here	stores system configuration parameters used by JumpStart
Drivers	Files
Finish	Profiles
sysidcfg	

Answer:

QUESTION 223:

What command loads a DSA identity into a Solaris Secure Shell authentication agent?

- A. ssh-add
- B. ssh-agent
- C. ssh-keyadd
- D. ssh-keyload
- E. ssh-load-identity

Answer: A

QUESTION 224:

What cryptographic assurance is provided by public key cryptography that is NOT provided by secret key cryptography?

- A. integrity
- B. confidentiality
- C. authentication
- D. non-repudiation

Answer: D

QUESTION 225:

Which two types of host keys are supported by Solaris Secure Shell? (Choose two.)

- A. AES
- B. RSA

- C. DSA
- D. DES
- E. 3DES

Answer: B,C

QUESTION 226:

Which is a public key encryption algorithm?

- A. AH
- B. AES
- C. RSA
- D. PGP
- E. IDEA

Answer: C

QUESTION 227:

Which cryptographic assurances are provided by SSL?

- A. confidentiality, integrity, availability
- B. authorization, confidentiality, message integrity
- C. confidentiality, client authentication, server authentication
- D. authentication, confidentiality, access control, non-repudiation

Answer: C

QUESTION 228:

Which command generates client key pairs and adds them to the \$HOME/.ssh directory?

- A. ssh-add
- B. ssh-agent
- C. ssh-keygen
- D. ssh-keyadd

Answer: C

QUESTION 229:

Which two services support TCP Wrappers by default in the Solaris 9 OE? (Choose two.)

- A. inetd
- B. rpcbind
- C. sendmail
- D. automountd
- E. Solaris Secure Shell

Answer: A,E

QUESTION 230:

Which is uncharacteristic of a Trojan horse program used to escalate privileges?

- A. It is installed in /usr/bin.
- B. It is owned by a normal user.
- C. It has the same name as a common program.
- D. It contains additional functionality which the user does not expect.

Answer: A

QUESTION 231:

Which setting in the /etc/system file limits the maximum number of user processes to 100 to prevent a user from executing a fork bomb on a system?

- A. set maxuprc = 100
- B. set maxusers = 100
- C. set user_procs = 100
- D. set max_nprocs = 100

Answer: A

QUESTION 232:

Which two regular user PATH assignments expose the user to a Trojan horse attack? (Choose two.)

- A. PATH=/usr/bin:/bin
- B. PATH=/usr/bin:/sbin:/usr/sbin
- C. PATH=/usr/bin:/sbin:/usr/sbin:
- D. PATH=./usr/bin:/sbin:/usr/sbin

Answer: C,D

QUESTION 233:

User fred runs a program that consumes all of the system's memory while

continuously spawning a new program. You decide to terminate all of fred's programs to put a stop to this. What command should you use?

- A. kill -u fred
- B. pkill -U fred
- C. passwd -l fred
- D. kill `ps -U fred -o pid`

Answer: B

QUESTION 234:

Which evasion technique can NOT be detected by system integrity checks?

- A. installing a rootkit
- B. adding user accounts
- C. abusing an existing user account
- D. installing a loadable kernel module

Answer: C

QUESTION 235:

Which statement about denial of service attack is FALSE?

- A. Denial of service is always preventable.
- B. Multiple machines may be used as the source of the attack.
- C. Service is denied on the victim host when a key resource is consumed.
- D. A denial of service attack is an explicit attempt by an attacker to prevent legitimate users of a service from using that service.

Answer: A

QUESTION 236:

Which command can customize the size for system log file rotation?

- A. dmesg
- B. logger
- C. logadm
- D. syslog
- E. syslogd

Answer: C

QUESTION 237:

Which syslog facility level specification can be used to record unsuccessful attempts to su(1M)?

- A. su.warning
- B. cron.debug
- C. kernel.alert
- D. auth.warning

Answer: D

QUESTION 238:

When will a removable diskette be deallocated?

- A. when the owner logs out
- B. when the system is rebooted
- C. when the owner removes the diskette
- D. when the root user allocates the device
- E. when the owner runs deallocate(1M)

Answer: E

QUESTION 239:

CORRECT TEXT

You add a new removable device to a workstation which has BSM enabled. Which files, apart from the device node itself, should you edit to make sure that this new device is maintained by the device allocation management? (Name one, specifying the full path name and using lower case characters.)

Answer: /ETC/SECURITY/DEVICE_MAPS

Answer: /ETC/SECURITY/DEVICE_ALLOCATE

QUESTION 240:

A system administrator sets up a global BSM policy that audits all user events except file access. Which is the correct entry in audit_user(4)?

- A. flags:all,^fa
- B. flags:^all:fc
- C. naflags:all:fr
- D. naflags:all:^fr

Answer: A

QUESTION 241:

You notice that the following line has been added to /etc/passwd:

admin:x:0:0:Administrator:/:bin/sh

You try to determine when this file was changed. You look at the file creation date, but based on that information, the file has not been touched since the system was installed. You look at the BSM logs for this system and find the three records that are shown in the exhibit.

What happened?

Exhibit:

```
header,61,2,AUE_STIME,,Wed Jun 05
10:30:00 2002, + 5 msec subject,foo,r
oot,other,root,other,752,713,0 32776
localhost return,success,0

header,107,2,AUE_OPEN_W,,Wed Jun 05
10:30:00 2002, + 140 msec
path,/etc/passwd attribute,100644,roo
t,sys,26738689,40851,0 subject,foo,ro
ot,other,root,other,746,713,0 32776
localhost return,success,3

header,61,2,AUE_STIME,,Wed Jan 29
07:52:00 2003, + 5 msec subject,foo,r
oot,other,root,other,755,713,0 32776
localhost return,success,0
```

- A. User root changed /etc/passwd and set the date of that file to 06/05/02.
- B. User root changed /etc/passwd after setting the system date to 06/05/02.
- C. User foo used su to become root, changed /etc/passwd, and set the date of that file to 06/05/02.
- D. User foo used su to become root and changed /etc/passwd after setting the system date to 06/05/02.

Answer: D

QUESTION 242:

Given:

\$ showmount -e

What information is provided?

- A. the NFS server statistics
- B. all file systems exported by the local system
- C. all file systems mounted on the local system
- D. all file systems mounted from the local file system by other systems

Answer: B

QUESTION 243:

Given that the entry below is listed in the /etc/dfs/dfstab file:

```
share -F nfs -o rw=foo,root=foo,ro /export
```

Who can write to this file system?

- A. all users on system foo
- B. the root user on system foo
- C. the root user on systems foo and ro
- D. all users on systems that have mounted this file system

Answer: A

QUESTION 244:

You are asked to harden a SunFire 15K server. Where do you look for the best information on securely configuring domains and system controllers?

- A. <http://www.cert.org/>
- B. <http://www.phrack.org/>
- C. <http://sunsolve.sun.com/>
- D. <http://www.sun.com/security/blueprints/>

Answer: D

QUESTION 245:

The Solaris 9 OE is configured, by default, to create core files for all non-set-ID processes. These files are created in the working directory of the process. These files can, however, be created in an administrator-defined location. This is often done to restrict access to these files to prevent unauthorized disclosure of information.

Which command can be used to create per-process core files in /var/core?

- A. gcore
- B. crash
- C. ulimit
- D. coreadm

Answer: D

QUESTION 246:

A system administrator hardens an application server with the Solaris Security Toolkit using their pre-existing JumpStart environment. When must a host security assessment be completed?

- A. only after testing the application
- B. after installing and testing the application
- C. before connecting the server to the production network
- D. after the server has been hardened with the Solaris Security Toolkit

Answer: C

QUESTION 247:

What is a security concern when using IPSec encrypted tunnels?

- A. Data may be encrypted twice.
- B. IPSec vendor applications might be incompatible.
- C. An attacker's actions may be concealed by the tunnel.
- D. Client side applications might have compatibility problems.

Answer: C

QUESTION 248:

Senior management has asked you to quantify the risks in your production Solaris Operating Environment. There are a number of ways you may attempt to measure the effectiveness of any of the safeguards you have implemented. When measuring residual risk, which statement is true?

- A. A false sense of security will always prevail.
- B. There is a law of diminishing return for security controls.
- C. The percentage of security breaches should be less than risk management calculations.
- D. The annualized loss expectancy should be less than the valuation of the assets multiplied by the residual risk factor.

Answer: B

QUESTION 249:

You notice that all mailboxes in /var/mail are world readable. Your company's policy states that a user's mailbox should be protected against access by other users. What security principle has been violated?

- A. integrity
- B. confidentiality
- C. accountability
- D. authentication

Answer: B

QUESTION 250:

How does BSM relate to the Solaris Common Criteria certification?

- A. BSM provides all of the required functionality.
- B. BSM must be enabled to meet the requirements.
- C. BSM meets the requirements for trusted recovery.
- D. BSM meets the requirements for Access Control Lists.
- E. BSM meets the requirements for password management.

Answer: B

QUESTION 251:

Which three topics must be described in an IT security policy? (Choose three.)

- A. employees' work schedules
- B. ownership 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,C,E

QUESTION 252:

What do Protection Profiles describe?

- A. the list of protected objects
- B. a set of security requirements
- C. the security rights associated with users
- D. how a product implements its security policy
- E. the procedures for evaluating a product's security features

Answer: B

QUESTION 253:

Which three naming services support password expiration? (Choose three.)

- A. files
- B. NIS
- C. NIS+
- D. LDAP

Answer: A,C,D

QUESTION 254:

How would you set up a user called dhoch who has access to the role snoopier that in turn has access to the profile Network Manager?

- A. roleadd -P "Network Manager" snoopier
useradd -d /export/home/dhoch -m -R snoopier dhoch
- B. roleadd -R snoopier dhoch
useradd -d /export/home/dhoch -m -P "Network Management" dhoch
- C. roleadd snoopier -R dhoch
useradd -d /export/home/dhoch -m -P "Network Management" dhoch
- D. roleadd -P "Network Manager" snoopier
useradd -d /export/home/dhoch -m -P "Network Management" dhoch

Answer: A

QUESTION 255:

What is the method used by Sun Kerberos to protect user passwords?

- A. User passwords are encrypted when sent to the authenticating Key Distribution Center (KDC) server.
- B. User passwords are sent only after the Key Distribution Center (KDC) server and client have established an IPSec connection.
- C. User passwords are used only to decrypt the secret key sent from the authenticating Key Distribution Center (KDC) server.
- D. User passwords are used to encrypt the user name, which is then sent to the authenticating Key Distribution Center (KDC) server.

Answer: C

QUESTION 256:

Under which directory should a new Solaris 9 PAM module be installed?

- A. /usr/local/pam
- B. /etc/pam/modules
- C. /usr/lib/security

D. /usr/local/pam/modules

Answer: C

QUESTION 257:

The security administrator wants to assign user bob to a netsec role so that the user can run the ifconfig(1M) and snoop(1M) commands with a rights profile named NSM. Which entries are contained in the /etc/security/exec_attr file after the required RBAC configuration has been implemented?

- A. NSM:bob:cmd:::/usr/sbin/ifconfig:uid=0
NSM:bob:cmd:::/usr/sbin/snoop:uid=0
- B. NSM:root:cmd:::/usr/sbin/ifconfig:uid=0
NSM:root:cmd:::/usr/sbin/snoop:uid=0
- C. NSM:suser:cmd:::/usr/sbin/ifconfig:uid=0
NSM:suser:cmd:::/usr/sbin/snoop:uid=0
- D. NSM:netsec:cmd:::/usr/sbin/ifconfig:uid=0
NSM:netsec:cmd:::/usr/sbin/snoop:uid=0

Answer: C

QUESTION 258:

Which is the best way to add new password triviality and composition checks into the Solaris OE?

- A. replace the /usr/bin/passwd command
- B. add the new checks to /etc/default/passwd
- C. install a PAM module and update /etc/pam.conf
- D. install a PAM module and update /etc/pam.d/passwd
- E. replace the /usr/lib/security/pam_authok_check.so.1 library

Answer: C

QUESTION 259:

You are setting up an application server on a Solaris 9 system. This application will be configured using the user app. This user does not require shell access to the system. What is the most secure way to add a user?

- A. useradd -d /export/home/app -m app
- B. useradd -d /export/home/app -m -s /bin/csh app
- C. useradd -d /export/home/app -m -s /bin/false app
- D. useradd -d /export/home/app -m -k /etc/skel -s /bin/csh app

Answer: C

QUESTION 260:

The date is Monday, March 1, 2003. Your company hired a consultant to work on your system. The consultant needs temporary shell access for the week and will finish on Friday. The account will be called temp. Which policy absolutely disables the shell account after Friday?

- A. usermod -f 5 temp
- B. passwd -l -e 5 temp
- C. passwd -f 3/5/2003 temp
- D. usermod -e 3/5/2003 temp

Answer: D

QUESTION 261:

To prevent man-in-the-middle attacks and provide strong user authentication, the security administrator configures the server using RSA authentication and the client using user RSA authentication. Assuming that the Solaris Secure Shell is configured to use version 2 of the Secure Shell protocol, what is the correct set of private keys?

- A. The client uses \$HOME/.ssh/id_rsa and the server uses /etc/ssh/ssh_host_rsa_key.
- B. The client uses /etc/ssh/ssh_host_rsa_key and the server uses /etc/ssh/ssh_host_rsa_key.
- C. The client uses \$HOME/.ssh/id_rsa.pub and the server uses /etc/ssh/ssh_host_rsa_key.pub.
- D. The client uses /etc/ssh/ssh_host_rsa_key.pub and the server uses /etc/ssh/ssh_host_rsa_key.pub.

Answer: A

QUESTION 262:

Solaris Secure Shell can be used to tunnel unencrypted network traffic between two systems. This process is known as port forwarding. Suppose that an administrator needs to securely forward a telnet connection from a client called "qcc" using local port 5003 to a server called "qcs". How should Solaris Secure Shell be configured and used to accomplish this task?

- A. on qcs, set Allow Tcp Forwarding to yes and restart the daemon sshd;
on qcc, run ssh -R5003:localhost:23 qcs
- B. on qcs, set Allow Tcp Forwarding to yes and restart the daemon sshd;
on qcc, run ssh -L5003:localhost:23 qcs

C.on qcc,set Allow Tcp Forwarding to yes and restart the daemon sshd;
on qcc, run ssh -R5003:localhost:23 qcs
D.on qcc,set Allow Tcp Forwarding to yes and restart the daemon sshd;
on qcc, run ssh -L5003:localhost:23 qcs

Answer: D

QUESTION 263:

Which two statements are true about the key management mechanism for Solaris IPSec? (Choose two.)

- A. It supports SKIP.
- B. It supports IDEA encryption.
- C. It supports pre-shared keys-based authentication.
- D. It does not support manual keying for authentication.
- E. It supports public key certificate-based authentication.

Answer: C,E

QUESTION 264:

You decide that it may be a good idea to prevent Trojan horse and backdoor attacks. Which three commands are often replaced by root kits? (Choose three.)

- A. ps(1)
- B. bc(1)
- C. ls(1)
- D. login(1)

Answer: A,C,D

QUESTION 265:

During a security assessment of a Solaris OE system, the examiner finds the run-control script, /etc/rc3.d/S20myapp. 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 and 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 program may be owned by an application user. If access to this user account can be obtained, an 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: C

QUESTION 266:

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?

Exhibit:

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

- 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 boot 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 memory (PROM) chip, changes must only be made to a system running in single user mode.

Answer: C

QUESTION 267:

The security administrator needs to create an account bob 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/bob bob
- B. useradd -m -s /usr/bin/ksh -d /export/home/guests/bob bob
- C. useradd -m -s /usr/bin/rksh -d /export/home/guests/bob bob

D. `useradd -m -s /usr/bin/pfksh -d /export/home/guests/bob bob`

Answer: C

QUESTION 268:

An attacker wants to gain information using technical engineering methods. The attacker can _____. (Choose two.)

- A. use port scanning for an active port
- B. obtain superuser privileges from the boss
- C. sniff a telnet connection for login and password
- D. take the system administrator's badge for server room access

Answer: A, C

QUESTION 269:

What is the primary objective of the Controlled Access Protection Profile?

- A. encryption
- B. trusted recovery
- C. system hardening
- D. mandatory access control
- E. discretionary access control

Answer: E

QUESTION 270:

What service can be configured to identify and authenticate users by public key cryptography?

- A. IKE
- B. IPSec
- C. TACACS+
- D. Secure Shell

Answer: D

QUESTION 271:

DRAG DROP

Place each action on the security life cycle term that describes its role within an organization.

Exhibit:

Action	Security Life Cycle Term
Place here	Disable unnecessary services in /etc/inet/inetd.conf
Place here	Review output of the praudit and auditreduce commands
Place here	Review security advisories to determine impact onsite
Place here	Communicate monitoring and abuse policies

Select from these

Deter	React
Prevent	Detect

Answer:

Action	Security Life Cycle Term
Deter	Disable unnecessary services in /etc/inet/inetd.conf
Detect	Review output of the praudit and auditreduce commands
React	Review security advisories to determine impact onsite
Prevent	Communicate monitoring and abuse policies

QUESTION 272:

As a result of a recent security audit, a security administrator is told to restrict access to the telnet and ftp services to a set of administrative workstations. All other services started from inetd should be disabled. Which three actions must be taken by the administrator to correctly respond to the audit finding? (Choose three.)

- A. pkill -HUP inetd
- B. pkill -HUP telnetd ftpd
- C. set the ENABLE_TCPWRAPPERS to YES in /etc/default/inetd
- D. set the ENABLE_TCP_WRAPPERS to YES in /etc/default/tcpd
- E. assign the telnet and ftp services to the administrative workstations in /etc/hosts.allow; add ALL to /etc/hosts.deny

F. assign the telnet and ftp services to the administrative workstations in /etc/tcpd/hosts.allow;add ALL to /etc/tcpd/hosts.deny

Answer: A,C,E

QUESTION 273:

What is the smallest Solaris OE meta-cluster that includes Solaris Secure Shell?

- A. SUNWCreq
- B. SUNWCall
- C. SUNWCuser
- D. SUNWCprog
- E. SUNWCXall

Answer: C

QUESTION 274:

Which command forwards the TCP port 3001 on the local host to the telnet port on the remote host xyzzy?

- A. telnet xyzzy 3001
- B. rsh xyzzy telnet 3001
- C. ssh localhost:3001 xyzzy:23
- D. ssh -L3001:localhost:23 xyzzy

Answer: D

QUESTION 275:

Which user configuration file contains the public keys of trusted remote servers?

- A. /etc/ssh/known_hosts
- B. /etc/ssh/identity.pub
- C. \$HOME/.ssh/known_hosts
- D. \$HOME/.ssh/identity.pub

Answer: C

QUESTION 276:

Which entry in /etc/inet/inetd.conf protects the in.fingerd service using TCP Wrappers?

- A. finger stream tcp6 nowait nobody /usr/sfw/sbin/tcpd in.fingerd

- B. finger stream tcp6 nowait nobody in.fingerd /usr/sfw/sbin/tcpd
- C. in.fingerd stream tcp6 nowait nobody /usr/sfw/sbin/tcpd finger
- D. in.fingerd stream tcp6 nowait nobody finger /usr/sfw/sbin/tcpd

Answer: A

QUESTION 277:

User alice begins to log in to a remote server named foo using Solaris Secure Shell.

This message is displayed:

The authenticity of host foo can't be established. RSA key fingerprint in md5 is:

04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26

Are you sure you want to continue connecting(yes/no)?

What is the meaning of the message?

- A. The user alice is being asked to accept, install, and save a public key for the user alice.
- B. The user alice is being asked to accept, install, and save a private key for the user alice.
- C. The user alice is being asked to accept, install, and save a public key for the server foo.
- D. The user alice is being asked to accept, install, and save a private key for the server foo.
- E. The user alice is being asked to accept, install, and save a public and private key pair for the user alice.

Answer: C

QUESTION 278:

Which two commands are used to detect a memory denial of service (DoS)? (Choose two.)

- A. sar
- B. mount
- C. vmstat
- D. cat /proc/meminfo

Answer: A, C

QUESTION 279:

A security administrator is asked to investigate a potential compromise of a Solaris 9 server. One of the signs of intrusion is that the listing of all files that should be owned by root are apparently owned by the nsa user. What is the cause of the problem?

- A. There is a backdoor present for the nsa user.
- B. The system has been hardened by the nsa user.
- C. There are multiple uid 0 entries in /etc/passwd file.
- D. The ls(1) command is owned by the nsa user in a chroot(2) directory.

Answer: C

QUESTION 280:

Which two commands can be used to effectively starve a system of its resources?
(Choose two.)

- A. /usr/sbin/crash
- B. cp /dev/zero /var/tmp/testfile
- C. cp /dev/null /var/tmp/testfile
- D. telnet localhost chargen | telnet localhost discard
- E. i=0; while ;; do touch /tmp/\$i; i=`expr \$i + 1`; done

Answer: B, E

QUESTION 281:

There are many files and directories that are world-writable in the default configuration of the Solaris OE. As a result, it is possible for a user to either maliciously or accidentally exhaust file system resources. If necessary, what command should be used to find these objects so that they can be cataloged and remediated?

- A. find / -perm 0002
- B. find / -mode +0002 -type -l -ls
- C. find / -prune -perm ugo=w -print
- D. find /\ (-type f -o -type d \) -perm -0002 -ls

Answer: D

QUESTION 282:

What are two capabilities of RBAC? (Choose two.)

- A. RBAC uses the security principle of least privilege.
- B. RBAC can separate superuser's capabilities into special roles.
- C. RBAC allows users to log in directly to a role assigned to them.
- D. RBAC System Administrator is a powerful role that is equivalent to root.
- E. RBAC checks for authorizations for all applications distributed by the Solaris OE.

Answer: A, B

QUESTION 283:

Which statement is true?

Exhibit:

```
#
# Account management
#
login    account requisite
pam_roles.so.1
login    account required
pam_projects.so.1
login    account required
pam_unix_account.so.1
#
rlogin   account required
pam_unix_account.so.1
rlogin   account required
pam_unix_account.so.1
#
other    account requisite
pam_roles.so.1
other    account required
pam_projects.so.1
other    account required
pam_unix_account.so.1
#
```

- A. Roles can directly log in to the system.
- B. Roles cannot be assumed using su(1M).
- C. Users can assume roles that they are not assigned using telnet.
- D. Roles can use rlogin regardless of whether they are assigned to users.

Answer: D

QUESTION 284:

Which historical least privilege facility does RBAC replace?

- A. sudo
- B. crack
- C. cron.deny
- D. hosts_deny

Answer: A

QUESTION 285:

A security audit of a system's security configuration resulted in a security administrator enabling password aging for all of the local system accounts. The security administrator set the MAXWEEKS parameter to 8 in /etc/default/passwd.

When does this change affect each user?

- A. after the next system reboot
B. immediately after MAXWEEKS is set
C. after the user's next password change
D. after the user's current password expires

Answer: C

QUESTION 286:

What are two problems with using lax or loose permissions? (Choose two.)

- A. It nullifies the setuid bits.
- B. It may cause a loss of confidentiality.
- C. It causes network performance issues.
- D. It makes file systems difficult to back up.
- E. It is easy to allow backdoors to be created.

Answer: B, E

QUESTION 287:

While examining the `/var/adm/messages` file, a security administrator discovers the error message included in the exhibit.

What should the administrator conclude based on the analysis of the message?

Exhibit:

```
May 18 16:56:56 saturn yppasswdd[191]:
yppasswdd: user
ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooL
oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
ooooooooooooooooooooooooooooP
`"?-?-?-"? ; /bin/sh-c echo 'rje stream tcp
nowait root /bin/sh sh -i'>z;/usr/sbin/inetd
-s z;rm z:: does not exist
```

- A. The system is operating normally.
- B. The message was created using an unsupported locale.
- C. Network Information Service (NIS) is not configured properly.
- D. The `rpc.yppasswdd(1M)` daemon was attacked using a buffer overflow.
- E. The `rpc.yppasswdd(1M)` daemon has been replaced by a Trojan horse.

Answer: D

QUESTION 288:

Which entry in the syslog.conf file causes all alert messages to be mailed to the user root?

- A.
A. *.alert,kern.err root,operator
B. B. user.alert root,operator
C. C. *.alert @root,operator
D. D. *.alert @localhost:root

Answer: A

QUESTION 289:

DRAG DROP

Place each file on the configuration entry with which it is associated.

Exhibit:

File	Configuration Entry
Place here	0x20000000:io:ioctl
Place here	root:lo:no
Place here	naflags:lo
Place here	6195:AUE_serialport_modify:modify serial port:ad

Select from these

/etc/security/audit_user	/etc/security/audit_class
/etc/security/audit_control	/etc/security/audit_event

Answer:

File	Configuration Entry
/etc/security/audit_class	0x20000000:io:ioctl
/etc/security/audit_control	root:lo:no
/etc/security/audit_user	naflags:lo
/etc/security/audit_event	6195:AUE_serialport_modify:modify serial port:ad

QUESTION 290:

Given:

fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean

To which file does this line belong?

- A. /etc/security/device_maps
- B. /etc/security/device_attr
- C. /etc/security/policy.conf
- D. /etc/security/device_allocate

Answer: D

QUESTION 291:

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: D

QUESTION 292:

While building a web server, a security administrator performs these steps:

1. installs the Solaris Operating Environment from CD-ROM
2. installs the Solaris Security Toolkit on the server
3. executes the Solaris Security Toolkit to perform hardening of the server
4. reboots the server

When should the network interfaces be connected?

- A. immediately before the system is rebooted
- B. immediately before the Solaris OE is installed
- C. immediately after the Solaris Security Toolkit is installed
- D. immediately before the Solaris Security Toolkit is executed

Answer: A

QUESTION 293:

You maintain an extremely protective policy when configuring your firewall rules. Your security policy denies all inbound connection requests to your corporate network. How is it possible that you still experience remote exploits your adversaries are using to obtain interactive sessions inside your firewall?

- A. TCP splicing is easy to do.
- B. Internal software may be vulnerable.
- C. UDP vulnerabilities are well-known and exploited.
- D. ICMP hijacking attacks can still succeed through any firewall.

Answer: B

QUESTION 294:

You want to prevent service foo from starting at boot time. What action do you take?

- A. remove /etc/init.d/foo
- B. remove /etc/rc2.d/K10foo
- C. remove /etc/rc3.d/S85foo
- D. remove foo from /etc/rc.local
- E. remove foo from /etc/services

Answer: C