Exam Code: 3x0-104

Exam Name: level 1 security.ethics and privacy

Vendor: SAIR

Version: DEMO

Part: A

1: An administrator has implemented a chain of router packet filtering rules on a major system server. A user has sent a packet to the network protected by the packet filter. The packet originated from 190.15.65.0/24 and is destined for 212.220.0.0/16. Considering the chain of packet filtering rules below, what will happen to the packet and why?

rule	source	destination	action
A	190.15.60.0/24	212.220.0.0/16	deny
B	212.220.0.0/16	190.15.65.0/24	deny
C	190.15.0.0/16	212.220.0.0/16	permit
D	0.0.0.0/0	0.0.0.0/0	deny

A.The packet will be permitted because no rules apply.
B.The packet will be permitted because it matches rule C.
C.The packet will be denied because all sources and destinations are blocked by rule D.
D.The packet will be denied because the packet matches rule A.
Correct Answers: B

2: A large server has many services running, including FTP, NFS, and NIS. It is hard for the administrator to find security holes in the services' configuration files, and this leads to possible security risks. Which of the following tools could the administrator use to check these services for security holes?
A.NTOP
B.LogCheck
C.SAINT
D.Tripwire
Correct Answers: C

3: Which of the following describes the contents of the /var/log/btmp log file?
A.It stores only the users' real names and their login times.
B.It contains a list of failed login attempts in a format similar to the wtmp log file.
C.It contains all successful superuser login attempts.
D.It contains a list of all users currently logged in to the system, along with their IP addresses.
Correct Answers: B

4: Tom is a system administrator for Linux ServerA. Tom is running a Perl script that will initiate a connection request from ServerA to ServerB without completing the network connection. This is done multiple times until ServerB can no longer communicate on the network. What kind of attack has Tom initiated?
A.Spam blast
B.TCP bomb
C.Denial of Service
D.Internet Worm
Correct Answers: C

5: Tom, a system administrator for ServerA, is interested in security and has written a script that scans the password file for unauthorized promotion to root status. Which of the following should the script check? (Choose two.)
A.A UID number that has been set to one
B.A UID number that has been set to zero
C.An account with the GID set to
D.A user with a non-standard shell (i.e., "/bin/runasroot")
E.An account with the UID set to
Correct Answers: B D

6: The system administrator wants to log all of the kernel messages (e.g. kernel panics) to a file instead of having the messages go to the console (e.g. /dev/console). Which file should she edit, and what line in the file should she add, to perform this duty?
A./etc/klog.conf; kern /var/log/kernel.log
B./etc/logd; kernel. /var/log/kernel.log
C./etc/syslog.conf; notice /var/log/kernel.log
D./etc/syslog.conf; kern /var/log/kernel.log
E./etc/klog.conf; .notice /var/log/kernel.log
Correct Answers: D

7: Katheryn wants to maximize security on her system by replacing ftpd with a program that logs requests, denies unauthorized users, and runs the original ftpd daemon. What should Kathryn use?
A.TCP wrappers
B.A VPN
C.Tripwire
D.Packet filters
Correct Answers: A

8: Jim, who has recently been promoted to network administrator, wants to specify rules for routing. However, he is unsure about how router packet filters parse and apply rules. Which of the following are TRUE regarding router packet filtering? (Choose two.)
A.Rules are checked against packets by parsing the body of the packet for information in a way similar to the method the grep program uses to
parse text files.
B.The packet headers are parsed and tested against the routing rules.
C.Packet filtering rules can be applied to inbound and outbound network interfaces.
D.Router packet filters remove headers from packets and apply rules based on the content of the packet.
Correct Answers: B C

9: A malicious user has sent thousands of TCP connection requests to a server from various forged IPs. The server does not receive acknowledgments from any of the requesting clients because they do not exist. The massive strain on the server causes it to crash. This is an example of what

type of Denial of Service (DoS) attack?
A.SYN flood
B.ICMP flood
C.Smurf attack
D.Buffer overflow
Correct Answers: A

10: An administrator finds a program on a network server that modifies several system service records when a certain user logs in and out. The program masks the intruder's actions. This is most likely an example of what type of a _____.
A.Trojan horse
B.Worm
C.Back door
D.Logic bomb
Correct Answers: D

11: Molly wants to encrypt and send an e-mail containing sensitive material to Sandy. To ensure that no one besides Sandy can read the e-mail, Molly wants to use PGP encryption. Which of the following methods will allow Molly to encrypt the e-mail and provide a way for Sandy to decrypt it? (Choose two.)
A.Molly gives a password at encryption time that Sandy can use to decrypt the e-mail.
B.Molly encrypts the e-mail using a private key. Sandy must then decrypt it using the public key.
C.Molly encrypts the e-mail using a public key. Sandy must then decrypt it using the private key.
D.Molly encrypts the e-mail using a series of private keys. Sandy then decrypts it using one of the private keys sent along with the e-mail.
Correct Answers: A C

12: Which of the following protocols transmit encrypted ASCII text by default?
A.POP
B.IMAP
C.FTP
D.Telnet
E.https
Correct Answers: E

13: Which file contains configuration information for the logging daemon, specifies a pattern of facilities to be logged, a logging priority, and where the logs are stored?
A./etc/inittab
B./etc/inetd.conf
C./etc/syslog.conf
D./etc/sysconfig/log.conf
E./etc/modules.conf
Correct Answers: C

14: William, a network administrator for a small marketing firm, wants to provide maximum security for sensitive information on his network. To do this, he has decided to set up a closed path for data transmission between two points on the network. Which of the following network concepts is this an example of?
A.Ethernet bridge
B.TCP wrappers
C.Proxy server
D.Tunneling
E.Encrypted sticky packets
Correct Answers: D

15: Which file must be modified to set the default values for such items as password expiration and superuser PATH settings?
A./etc/permissions
B./etc/login.defs
C./etc/smb.conf
D./etc/defaults
Correct Answers: B

16: Given the code below from an /etc/syslog.conf file, which of the following lines is invalid?
1 kern. /dev/console
2 emerg;local3.none
3 mail |/var/log/maillog
4 authpriv. @log.somedomain.com
5 local7. /var/log/boot.log
A.1
B.2
C.3
D.4
E.5
Correct Answers: C

17: Before Linuxsite sets up its Network, it develops its Network Policy. Which of the following is NOT a reason why Linuxsite should have a Network Policy set up?
A.It will inform the users of the appropriate use of the system.
B.It will provide Linuxsite with liability protection if illegal activities are performed on their site without their knowledge.
C.It will block unauthorized users from accessing the network.
D.It will provide Linuxsite with a standard way to deal with problems concerning the Network.
Correct Answers: C

18: The system administrator needs to set the existing user jsmith's home directory to /mnt/home/jsmith. Which of the following commands can she use to do this?
A.useradd

B.setenv
C.vigr
D.usermod
Correct Answers: D

19: Jerry is setting up a firewall for a Local Area Network (LAN), and he wishes to use the firewall as the default gateway for the LAN. In order to do this, which of the following MUST Jerry do to the packets coming from the LAN to the firewall?
A.Forward
B.Sniff
C.Deny
D.Mangle
E.Encapsulate
Correct Answers: A

20: John has just set up shadowing on his Linux machine. As root, he looks in the /etc/shadow file and finds the line below. Which of the following is TRUE about the line he found?

jsmith:H7o12v$s:100:0:60:7:3::

A.The user jsmith's account has been disabled for 100 minutes.
B.The user jsmith's password can only be changed after the current password has been active for 3 days.
C.The user jsmith will be warned for 60 days until his password expires.
D.The user jsmith's account will be disabled 3 days after his password expires.
Correct Answers: D