IT认证电子书

质量更高　服务更好

半年免费升级服务

http://www.itrenzheng.com

Exam : 3X0-104

Title : level 1 security.ethics and privacy

Version : DEMO

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.
Answer: 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
Answer: 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.
Answer: 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
Answer: 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
Answer: BD

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
Answer: 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. AVPN

C. Tripwire D. Packet filters
Answer: 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.
Answer: BC

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
Answer: 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

Answer: D