1. What aspect of security involves measures such as locks, fences, and surveillance cameras?

a) Network Security
b) Physical Security
c) Cybersecurity
d) Application Security

Answer: b) Physical Security
Explanation: Physical security refers to the protection of physical assets, locations, and resources from unauthorized access, damage, or harm.

2. Which system component regulates user access to resources and functionalities based on predefined rules?

a) Firewall
b) Router
c) Access Control List (ACL)
d) Intrusion Detection System (IDS)

Answer: c) Access Control List (ACL)
Explanation: ACLs are lists of permissions attached to a resource that specify which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

3. What command is commonly used to display and modify ACL entries on a file in Unix-based systems?

a) ls
b) chmod
c) aclchk
d) getfacl

Answer: d) getfacl
Explanation: The getfacl command is used to display the Access Control Lists (ACLs) for files and directories in Unix-based systems.

4. How can you restrict FTP access to certain users or groups?

a) By using a VPN
b) By configuring TCP Wrappers
c) By modifying the system kernel
d) By disabling FTP altogether

Answer: b) By configuring TCP Wrappers
Explanation: TCP Wrappers provide a host-based access control mechanism that allows or denies access to network services based on the IP address of the client machine.

5. Which user account typically has unrestricted access to all system resources and settings?

a) Administrator
b) Super User
c) Guest
d) Standard User

Answer: b) Super User

Explanation: The super user, often named ‘root’ in Unix-based systems, has the highest level of access and privileges, allowing them to perform any operation on the system.

6. What tool is commonly used to monitor super user access and system activities?

a) Wireshark
b) Snort
c) Tripwire
d) sudo

Answer: c) Tripwire
Explanation: Tripwire is an integrity monitoring tool used to detect changes to files and directories, including unauthorized changes made by super users.

7. Which mechanism allows for controlling access to network services based on the IP address of the client machine?

a) MAC Filtering
b) VPN
c) TCP Wrappers
d) SSH Tunneling

Answer: c) TCP Wrappers
Explanation: TCP Wrappers provide access control based on the IP address of the client machine, allowing administrators to permit or deny access to network services.

8. What command is used to modify permissions on a file or directory in Unix-based systems?

a) chmod
b) chown
c) ls
d) grep

Answer: a) chmod
Explanation: The chmod command is used to change the permissions of a file or directory in Unix-based systems.

9. What is the primary purpose of using a restricted shell for user accounts?

a) To enhance file compression
b) To restrict access to specific system commands
c) To increase network bandwidth
d) To improve system performance

Answer: b) To restrict access to specific system commands
Explanation: A restricted shell limits the commands and functionalities available to a user, providing increased security by restricting their actions within the system.

10. How can you delete specific entries from an Access Control List (ACL) attached to a file in Unix-based systems?

a) Using the ‘rm’ command
b) Using the ‘delete’ command
c) Using the ‘delacl’ command
d) Using the ‘setfacl’ command

Answer: c) Using the ‘delacl’ command
Explanation: The ‘delacl’ command is used to delete specific entries from an Access Control List (ACL) attached to a file in Unix-based systems.