1. What is SELinux used for in Linux?

A) Kernel Debugging
B) System Boot Process Optimization
C) Mandatory Access Control (MAC)
D) Encrypting File Systems

Answer: C) Mandatory Access Control (MAC)
Explanation: SELinux (Security-Enhanced Linux) enforces Mandatory Access Control policies to restrict actions users and applications can perform, enhancing system security.

---

2. What command is used to view the SELinux mode on a Linux system?

A) `getenforce`
B) `sestatus`
C) `checkpolicy`
D) `enforce`

Answer: B) `sestatus`
Explanation: The `sestatus` command shows the SELinux status and mode (enforcing, permissive, or disabled). Alternatively, `getenforce` displays the current mode but with less detail.

---

3. Which Linux file contains the default rules for the firewall managed by `iptables` or `nftables`?

A) `/etc/iptables.conf`
B) `/etc/firewall.rules`
C) `/etc/sysconfig/iptables`
D) `/etc/default/firewall.conf`

Answer: C) `/etc/sysconfig/iptables`
Explanation: For systems using `iptables`, the rules are often stored in `/etc/sysconfig/iptables`. Newer systems using `nftables` may store them in a different file.

---

4. What does the `chattr +i` command do to a file in Linux?

A) Makes the file immutable
B) Changes file permissions
C) Encrypts the file
D) Hides the file

Answer: A) Makes the file immutable
Explanation: The `+i` attribute using `chattr` makes the file immutable, meaning it cannot be modified, deleted, or renamed until the attribute is removed.

---

5. What is the primary role of AppArmor in Linux security?

A) User authentication
B) File system encryption
C) Application-level access control
D) Backup and recovery

Answer: C) Application-level access control
Explanation: AppArmor is a Linux security module that provides application-level access control using profiles that define what resources applications can access.

---

6. How can you securely wipe a file in Linux to prevent data recovery?

A) `rm file`
B) `shred file`
C) `delete file`
D) `erase file`

Answer: B) `shred file`
Explanation: The `shred` command overwrites the file's content multiple times to make recovery nearly impossible.

---

7. What does the command `sudo visudo` do?

A) Opens the sudo log file
B) Allows direct editing of `/etc/sudoers`
C) Safely edits the `/etc/sudoers` file
D) Changes the default shell for sudo users

Answer: C) Safely edits the `/etc/sudoers` file
Explanation: The `visudo` command locks the sudoers file while editing, ensuring no syntax errors that could compromise administrative access.

---

8. What is the purpose of the `/var/log/auth.log` file?

A) Stores application logs
B) Records user authentication and sudo activities
C) Logs kernel events
D) Contains web server logs

Answer: B) Records user authentication and sudo activities
Explanation: The `/var/log/auth.log` file tracks login attempts, sudo usage, and other authentication-related events, crucial for security monitoring.

---

9. What command can you use to scan open ports on a Linux system?

A) `tcpdump`
B) `nmap`
C) `iptables`
D) `top`

Answer: B) `nmap`
Explanation: The `nmap` tool scans networks and systems to identify open ports and running services, helping detect vulnerabilities.

---

10. What is the `fail2ban` tool used for?

A) File system encryption
B) Preventing brute force attacks
C) Database management
D) Disabling unused services

Answer: B) Preventing brute force attacks
Explanation: `fail2ban` monitors logs for failed login attempts and blocks IPs temporarily, protecting systems from brute force attacks.

---

11. What Linux command lists user accounts and their last login time?

A) `who`
B) `last`
C) `finger`
D) `login`

Answer: B) `last`
Explanation: The `last` command shows the login history for all users, including their last login time and source IP.

---

12. Which of the following ensures file integrity by monitoring changes to key files?

A) SELinux
B) AppArmor
C) AIDE
D) Tripwire

Answer: C) AIDE
Explanation: AIDE (Advanced Intrusion Detection Environment) and Tripwire are file integrity monitoring tools that detect unauthorized changes to files.

---

13. How can you check all running processes with their security contexts on an SELinux-enabled system?

A) `ps -eZ`
B) `ps -aux`
C) `sestatus`
D) `getenforce`

Answer: A) `ps -eZ`
Explanation: The `-Z` option with `ps` displays the security context of each process in an SELinux-enabled environment.

---

14. What is the main purpose of the `/etc/security/limits.conf` file?

A) Define firewall rules
B) Set system-wide resource limits
C) Configure SELinux policies
D) Control password complexity

Answer: B) Set system-wide resource limits
Explanation: The `/etc/security/limits.conf` file allows administrators to set limits on processes, memory usage, and open files for users or groups.

---

15. What is the default location of user password hashes in a Linux system?

A) `/etc/passwd`
B) `/etc/shadow`
C) `/var/passwd`
D) `/var/shadow`

Answer: B) `/etc/shadow`
Explanation: The `/etc/shadow` file contains hashed passwords, with restricted permissions to improve security.

16. You suspect a compromised system. Which tool would you use to scan for rootkits and their signatures on a Linux system?

A) `chkrootkit`
B) `nmap`
C) `tcpdump`
D) `netstat`

Answer: A) `chkrootkit`
Explanation: `chkrootkit` is specifically designed to detect rootkits on a system by scanning for known rootkit signatures. If you suspect that your system has been compromised by a rootkit, this is the tool you would use to check for it.

---

17. During an audit, you are asked to block access to a specific service for a certain IP address. Which file should you modify on a Linux system to deny the IP's access to all services?

A) `/etc/hosts.deny`
B) `/etc/firewall.rules`
C) `/etc/services.deny`
D) `/etc/sysconfig/iptables`

Answer: A) `/etc/hosts.deny`
Explanation: The `/etc/hosts.deny` file is used to deny access to network services managed by TCP Wrappers for specific IP addresses. By modifying this file, you can block an IP from accessing the system.

---

18. You want to securely encrypt a file before sending it over email. Which of the following GPG commands would you use?

A) `gpg -e file`
B) `gpg --encrypt file`
C) `gpg --file-encrypt`
D) `gpg -secure file`

Answer: B) `gpg --encrypt file`
Explanation: The `gpg --encrypt file` command is used to encrypt files using GPG, ensuring that only the recipient with the corresponding decryption key can access its contents.

---

19. You are setting up a Linux server and want to ensure that all files created on the system have secure default permissions. Which command can be used to control this?

A) `umask`
B) `chmod`
C) `chown`
D) `setfacl`

Answer: A) `umask`
Explanation: The `umask` command defines the default file permissions for newly created files and directories. By setting an appropriate umask value, you can enforce a secure permission scheme across the system.

---

20. After a security incident, you need to lock a user's account to prevent further unauthorized access. Which command will you use?

A) `passwd -l username`
B) `usermod -L username`
C) `chage -E 0 username`
D) `lockuser username`

Answer: A) `passwd -l username`
Explanation: The `passwd -l` command locks the user account by disabling its password, effectively preventing login access to the system.

---

21. You are tasked with enabling auditing to track all changes to critical files on your Linux system. Which tool do you use to configure auditing rules?

A) `auditctl`
B) `auditd`
C) `ausearch`
D) `auditd-config`

Answer: A) `auditctl`
Explanation: The `auditctl` command allows you to configure audit rules, which are crucial for monitoring changes to critical files, system calls, and user actions. It is part of the Linux auditing system.

---

22. You are configuring a firewall on a Linux system and need to append a rule to the INPUT chain to allow incoming SSH traffic. Which command will you use?

A) `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
B) `iptables -I INPUT -p tcp --dport 22 -j ACCEPT`
C) `iptables -A INPUT -p udp --dport 22 -j ACCEPT`
D) `iptables -A SSH -p tcp --dport 22 -j ACCEPT`

Answer: A) `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
Explanation: The `iptables -A INPUT` command appends a rule to the INPUT chain, allowing incoming SSH traffic on port 22. This rule is crucial for remote server administration via SSH.

---

23. A user reports that a kernel module is not loading correctly. You need to list all currently loaded modules to troubleshoot the issue. Which command would you use?

A) `lsmod`
B) `modinfo`
C) `modprobe`
D) `insmod`

Answer: A) `lsmod`
Explanation: The `lsmod` command lists all currently loaded kernel modules, helping you identify if the required module is loaded correctly or if there are any issues.

---

24. You need to implement a policy that requires users to change their password every 30 days and prevents reusing the last 5 passwords. Which PAM module would you configure?

A) `pam_tally2`
B) `pam_unix.so`
C) `pam_pwquality.so`
D) `pam_unix.passwd`

Answer: B) `pam_unix.so`
Explanation: The `pam_unix.so` module controls password aging and history, allowing you to configure password expiration and prevent the reuse of previous passwords for a specified number of changes.

---

25. After a security breach, you want to find out which processes are holding open files or network connections. Which command can you use to investigate this?

A) `lsof`
B) `netstat`
C) `ps -ef`
D) `strace`

Answer: A) `lsof`
Explanation: The `lsof` command shows all open files and network connections, which can help you identify suspicious activity such as unauthorized processes or files being accessed by malicious software.

---

26. You need to enforce a policy that requires users to create passwords that are at least 12 characters long, contain both uppercase and lowercase letters, and include special characters. Which PAM module should you configure?

A) `pam_tally2`
B) `pam_unix.so`
C) `pam_pwquality.so`
D) `pam_cracklib.so`

Answer: C) `pam_pwquality.so`
Explanation: The `pam_pwquality.so` module enforces password complexity rules, such as minimum length and required character types (uppercase, lowercase, digits, special characters).

---

27. As part of a vulnerability assessment, you need to scan a Linux system for open ports and running services. Which tool should you use?

A) `nmap`
B) `ncat`
C) `netstat`
D) `iptables`

Answer: A) `nmap`
Explanation: `nmap` is a powerful tool for scanning open ports and identifying running services on a network or system, which is essential for vulnerability management.

---

28. Your organization requires all SSH connections to be encrypted with the strongest possible encryption algorithms. Which file would you modify to change SSH settings?

A) `/etc/ssh/sshd_config`
B) `/etc/ssh/ssh_config`
C) `/etc/ssh/ssh_server.conf`
D) `/etc/ssh/secure.conf`

Answer: A) `/etc/ssh/sshd_config`
Explanation: The `/etc/ssh/sshd_config` file contains configuration settings for the SSH server, including encryption algorithms, ciphers, and other security-related settings.

---

29. During a security audit, you need to ensure that all users are logged out after 30 minutes of inactivity. Which configuration file should you modify to set this timeout?

A) `/etc/passwd`
B) `/etc/login.defs`
C) `/etc/ssh/sshd_config`
D) `/etc/profile`

Answer: B) `/etc/login.defs`
Explanation: The `/etc/login.defs` file contains system-wide settings such as login timeouts. You can configure the `TMOUT` variable to log users out after a period of inactivity.

---

30. You have just configured a system to use SSL/TLS for encrypted communication. Which tool can you use to verify that the encryption is working correctly on a server?

A) `openssl s_client`
B) `curl -v`
C) `nmap --script ssl-enum-ciphers`
D) `tcpdump`

Answer: A) `openssl s_client`
Explanation: `openssl s_client` is a command-line tool used to test SSL/TLS connections, verifying encryption settings, certificate validity, and cipher suites.

---

31. You are tasked with configuring a Linux server for multi-user access while ensuring that users cannot execute commands with higher privileges without authorization. What tool can be used to grant temporary administrative privileges to specific users without giving them full root access?

A) `sudo`
B) `su`
C) `setfacl`
D) `chown`

Answer: A) `sudo`
Explanation: `sudo` is used to grant temporary administrative privileges to specific users for executing certain commands. This minimizes the risk of unauthorized actions by limiting access to root privileges.

---

32. You notice that a user is repeatedly failing to log in, and after several attempts, the account is locked. Which PAM module would you configure to track login attempts and lock accounts after a certain number of failures?

A) `pam_tally2`
B) `pam_unix.so`
C) `pam_ldap.so`
D) `pam_access.so`

Answer: A) `pam_tally2`
Explanation: The `pam_tally2` module tracks login attempts and can lock accounts after a specified number of failed attempts, providing a basic security mechanism against brute-force attacks.

---

33. You are asked to implement a system that will automatically disable user accounts that have been inactive for over 90 days. Which of the following commands will help you identify such accounts?

A) `chage -l username`
B) `passwd -S username`
C) `usermod -L username`
D) `lastlog -t 90`

Answer: D) `lastlog -t 90`
Explanation: The `lastlog -t 90` command lists accounts that have not logged in within the last 90 days, helping to identify inactive accounts for further action.

---

34. You need to implement a security policy that prevents users from running any programs as root or with elevated privileges unless explicitly allowed. Which configuration file should you modify to configure the list of allowed commands for each user?

A) `/etc/sudoers`
B) `/etc/pam.d/sudo`
C) `/etc/login.defs`
D) `/etc/securetty`

Answer: A) `/etc/sudoers`
Explanation: The `/etc/sudoers` file defines what commands specific users or groups can run with `sudo` privileges. It helps restrict access to only necessary administrative tasks.

---

35. A critical application is running on your Linux server, and you want to monitor system calls made by this application to detect any abnormal behavior. Which Linux security tool would you use to trace system calls?

A) `strace`
B) `auditctl`
C) `psacct`
D) `lsof`

Answer: A) `strace`
Explanation: `strace` is a diagnostic tool that allows you to trace system calls and signals. It can be used to monitor application behavior and identify potential security issues, such as attempts to access unauthorized resources.

---

36. Your system was compromised, and you need to check which files have been modified recently. Which of the following commands would help you track file changes and modifications in a Linux environment?

A) `auditctl`
B) `find / -mtime`
C) `dstat`
D) `tail /var/log/syslog`

Answer: B) `find / -mtime`
Explanation: The `find / -mtime` command helps you locate files modified within a specific timeframe, which can be useful in identifying unauthorized changes made during a compromise.

---

37. A user is attempting to connect to the system via SSH, but the connection is being rejected. You need to review the server's SSH configuration for any restrictions on allowed authentication methods. Which configuration file should you check?

A) `/etc/ssh/sshd_config`
B) `/etc/ssh/ssh_config`
C) `/etc/login.defs`
D) `/etc/pam.d/sshd`

Answer: A) `/etc/ssh/sshd_config`
Explanation: The `/etc/ssh/sshd_config` file contains settings that control how the SSH server operates, including authentication methods (password, public key, etc.). It's the file you should check if SSH connections are being rejected.

---

38. Your system has a large number of failed login attempts. You want to block further login attempts from the IP address of the attacker for a period of time. Which Linux tool can help you achieve this?

A) `iptables`
B) `fail2ban`
C) `netstat`
D) `ufw`

Answer: B) `fail2ban`
Explanation: `fail2ban` is a tool that automatically bans IP addresses that exhibit malicious

behavior, such as multiple failed login attempts. It is a useful tool to mitigate brute-force attacks.

---

39. A user reports that they cannot access a directory, even though they have the correct permissions. After investigation, you discover that the directory is part of a shared network mount. Which of the following should you check to ensure proper access?

A) NFS export permissions
B) SELinux context
C) Directory ACLs
D) Mount options in `/etc/fstab`

Answer: A) NFS export permissions
Explanation: If the directory is part of an NFS share, you need to check the NFS export permissions to ensure that the client has been granted the correct access rights to the directory.

---

40. You are tasked with ensuring that no unauthorized software can be executed on the system. What Linux feature allows you to restrict the execution of certain files based on their attributes?

A) SELinux
B) AppArmor
C) NoExec mount option
D) Binary whitelisting

Answer: D) Binary whitelisting
Explanation: Binary whitelisting is a security mechanism where only approved binaries can be executed. Tools like `AIDE` or `osquery` can be used to enforce this, ensuring that only authorized software is allowed to run on the system.

---

41. You have just implemented an Intrusion Detection System (IDS) on your Linux server, and you want to monitor system integrity by detecting any unauthorized file changes. Which tool would you use to implement file integrity monitoring?

A) `AIDE`
B) `tcpdump`

C) `netstat`
D) `lsof`

Answer: A) `AIDE`
Explanation: AIDE (Advanced Intrusion Detection Environment) is a file integrity monitoring tool that checks for unauthorized changes to critical system files, alerting administrators to potential security breaches.

---

42. After a security audit, you realize that there is an issue with the system's login process where an excessive number of unsuccessful login attempts are made. Which Linux log file would you examine to find detailed information about authentication failures?

A) `/var/log/auth.log`
B) `/var/log/syslog`
C) `/var/log/secure`
D) `/var/log/messages`

Answer: C) `/var/log/secure`
Explanation: `/var/log/secure` records security-related events, including login attempts (both successful and failed), making it the ideal log file to investigate authentication issues.

---

43. A critical system service has been stopped unexpectedly, and you need to investigate the root cause. Which of the following tools would you use to review system logs for errors or crashes related to this service?

A) `systemctl status`
B) `journalctl -xe`
C) `dmesg`
D) `tail /var/log/messages`

Answer: B) `journalctl -xe`
Explanation: `journalctl -xe` displays detailed logs of system events managed by `systemd`, including errors and failures related to specific services. It is an essential tool for investigating service crashes.

---

44. You need to ensure that your system's firewall is configured to only allow incoming traffic on ports essential for your web application. Which

tool would you use to configure the firewall on a Linux server running with `iptables`?

A) `firewalld`
B) `ufw`
C) `iptables`
D) `iptables-save`

Answer: C) `iptables`
Explanation: `iptables` is the default tool used to configure packet filtering rules on Linux systems. It allows administrators to define specific rules to control inbound and outbound traffic, including restricting access to certain ports.

---

45. Your company requires a secure login process where each user must authenticate using two factors: a password and a time-based one-time passcode (TOTP). Which of the following tools would you use to implement this type of authentication?

A) `PAM`
B) `Google Authenticator`
C) `OTP`
D) `PAM_google_authenticator`

Answer: D) `PAM_google_authenticator`
Explanation: The `PAM_google_authenticator` module allows the integration of Google Authenticator with PAM to enable TOTP-based two-factor authentication for Linux systems.

---

46. A user’s SSH login attempts are being denied, and you need to identify if there are any restrictions on the user's authentication methods. Which file would you check for possible restrictions related to password-based logins?

A) `/etc/ssh/sshd_config`
B) `/etc/passwd`
C) `/etc/pam.d/sshd`
D) `/etc/hosts.deny`

Answer: A) `/etc/ssh/sshd_config`
Explanation: The `/etc/ssh/sshd_config` file contains settings related to SSH

authentication methods, such as whether password authentication is allowed or if public key authentication is enforced. Restrictions can be found here.

---

47. You are tasked with securing your system and need to prevent users from accessing critical system files. Which Linux tool can you use to control access to files and directories based on user attributes?

A) `chown`
B) `setfacl`
C) `chmod`
D) `umask`

Answer: B) `setfacl`
Explanation: The `setfacl` (set file access control list) command allows you to define access control lists (ACLs) for files and directories, providing fine-grained control over permissions based on user attributes or groups, beyond standard ownership and permission settings.

---

48. You are conducting a vulnerability assessment and need to identify the installed packages and software versions on a Linux system. Which tool would you use to gather this information?

A) `dpkg -l`
B) `yum list installed`
C) `rpm -qa`
D) All of the above

Answer: D) All of the above
Explanation: Different Linux distributions use different package management systems. `dpkg -l` is used on Debian-based systems, `yum list installed` is for Red Hat-based systems, and `rpm -qa` lists packages on Red Hat and CentOS systems. These tools help identify the installed packages and versions.

---

49. To ensure that sensitive information like passwords and API keys are protected, you need to encrypt files before storing them. Which Linux command can you use to encrypt files with a symmetric encryption algorithm?

A) `gpg --symmetric`
B) `openssl aes-256-cbc`
C) `cryptsetup`
D) `tar -czf`

Answer: B) `openssl aes-256-cbc`
Explanation: The `openssl aes-256-cbc` command allows you to encrypt files with the AES-256 symmetric encryption algorithm. It is commonly used for securing sensitive data before storage or transmission.

---

50. Your team needs to monitor system performance to detect any unusual activity such as unexpected resource usage or malicious processes. Which tool would you use to get a real-time overview of system resource usage?

A) `htop`
B) `ps aux`
C) `top`
D) `uptime`

Answer: A) `htop`
Explanation: `htop` provides a dynamic, real-time view of the system's resource usage, including CPU, memory, and process management. It is more interactive and user-friendly compared to `top`, allowing you to sort and filter processes easily.

---

51. You are reviewing the system logs after a suspicious incident and need to find out which users accessed the system via SSH in the last 24 hours. Which log file would you inspect?

A) `/var/log/secure`
B) `/var/log/auth.log`
C) `/var/log/sshd.log`
D) `/var/log/messages`

Answer: A) `/var/log/secure`
Explanation: The `/var/log/secure` log file records security-related events, including SSH login attempts. This file would show you which users successfully logged in or attempted to log in via SSH.

---

52. You need to implement a policy that ensures only approved users can run specific commands as root. Which tool would you configure to define these rules?

A) `sudoers`
B) `chown`
C) `iptables`
D) `pam_listfile.so`

Answer: A) `sudoers`
Explanation: The `/etc/sudoers` file is used to define which users and groups are allowed to execute commands as root, specifying which commands can be run with elevated privileges. It is an essential file for controlling user privileges.

---

53. You are auditing a system and need to ensure that all passwords are stored securely in a hashed format. Which configuration file would you check to verify the password hashing algorithm being used?

A) `/etc/pam.d/common-password`
B) `/etc/ssh/sshd_config`
C) `/etc/passwd`
D) `/etc/shadow`

Answer: A) `/etc/pam.d/common-password`
Explanation: The `/etc/pam.d/common-password` file configures the password management for PAM. It is here you would specify the hashing algorithm, such as SHA-512, to ensure that passwords are securely hashed before being stored.

---

54. Your company requires a centralized logging system. Which tool would you use to configure your Linux system to send log messages to a remote server for centralized log management?

A) `syslog`
B) `rsyslog`
C) `logrotate`
D) `journalctl`

Answer: B) `rsyslog`
Explanation: `rsyslog` is a flexible and powerful logging daemon that allows you to send system logs to remote servers. It is commonly used for centralized logging in enterprise environments.

---

55. You need to implement a method to track the integrity of critical files on your system to detect unauthorized changes. Which of the following tools can help you achieve this?

A) `AIDE`
B) `chkrootkit`
C) `clamav`
D) `fail2ban`

Answer: A) `AIDE`
Explanation: AIDE (Advanced Intrusion Detection Environment) is used for file integrity monitoring. It checks for unauthorized changes to critical files and helps detect potential compromises or malicious activity on the system.