3.0 Security

3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.

- **File and directory permissions**
  - Read, write, execute
  - User, group, other
  - SUID
  - Octal notation
  - umask
  - Sticky bit
  - SGID
  - Inheritance
  - Utilities
    - chmod
    - chown
    - chgrp
    - getfacl
    - setfacl
    - ls
    - ulimit
    - chage
- **Context-based permissions**
  - SELinux configurations
    - disabled
    - permissive
    - enforcing
  - SELinux policy
    - targeted
  - SELinux tools
    - setenforce
    - getenforce
    - sestatus
    - setsebool
    - getsebool
    - chcon
    - restorecon
    - ls -Z
    - ps -Z
  - AppArmor
    - aa-disable
    - aa-complain
    - aa-unconfined
    - /etc/apparmor.d/
    - /etc/apparmor.d/tunables
- **Privilege escalation**
  - su
  - sudo
  - wheel
  - visudo
  - sudoedit
- **User types**
  - Root
  - Standard
  - Service

3.2 Given a scenario, configure and implement appropriate access and authentication methods.

- **PAM**
  - Password policies
  - LDAP integration
  - User lockouts
  - Required, optional, or sufficient
  - /etc/pam.d/
  - pam_tally2
  - faillock
- **SSH**
  - ~/.ssh/
    - known_hosts
    - authorized_keys
    - config
    - id_rsa
    - id_rsa.pub
  - User-specific access
  - TCP wrappers
  - /etc/ssh/
    - ssh_config
    - sshd_config
  - ssh-copy-id
  - ssh-keygen
  - ssh-add
- **TTYs**
  - /etc/securetty
  - /dev/tty#
- **PTYs**
- **PKI**
  - Self-signed
  - Private keys
  - Public keys
  - Hashing
  - Digital signatures
  - Message digest
- **VPN as a client**
  - SSL/TLS
  - Transport mode
  - Tunnel mode
  - IPSec
  - DTLS

3.3 Summarize security best practices in a Linux environment.

- **Boot security**
  - Boot loader password
  - UEFI/BIOS password
- **Additional authentication methods**
  - Multifactor authentication
    - Tokens
      - Hardware
      - Software
    - OTP
    - Biometrics
  - RADIUS
  - TACACS+
  - LDAP
  - Kerberos
    - kinit
    - klist
- **Importance of disabling root login via SSH**
- **Password-less login**
  - Enforce use of PKI
- **Chroot jail services**
- **No shared IDs**
- **Importance of denying hosts**
- **Separation of OS data from application data**
  - Disk partition to maximize system availability
- **Change default ports**
- **Importance of disabling or uninstalling unused and unsecure services**
  - FTP
  - Telnet
  - Finger
  - Sendmail
  - Postfix
- **Importance of enabling SSL/TLS**
- **Importance of enabling auditd**
- **CVE monitoring**
- **Discouraging use of USB devices**
- **Disk encryption**
  - LUKS
- **Restrict cron access**
- **Disable Ctrl+Alt+Del**
- **Add banner**
- **MOTD**

3.4 Given a scenario, implement logging services.

- **Key file locations**
  - /var/log/secure
  - /var/log/messages
  - /var/log/[application]
  - /var/log/kern.log
- **Log management**
  - Third-party agents
  - logrotate
  - /etc/rsyslog.conf
  - journald
    - journalctl
- **lastb**

3.5 Given a scenario, implement and configure Linux firewalls.

- **Access control lists**
  - Source
  - Destination
  - Ports
  - Protocol
  - Logging
  - Stateful vs. stateless
  - Accept
  - Reject
  - Drop
  - Log
- **Technologies**
  - firewalld
    - Zones
    - Run time
  - iptables
    - Persistency
    - Chains
  - ufw
    - /etc/default/ufw
    - /etc/ufw/
  - Netfilter
- **IP forwarding**
  - /proc/sys/net/ipv4/ip_forward
  - /proc/sys/net/ipv6/conf/all/forwarding
- **Dynamic rule sets**
  - DenyHosts
  - Fail2ban
  - IPset
- **Common application firewall configurations**
  - /etc/services
  - Privileged ports

3.6 Given a scenario, backup, restore, and compress files.

- **Archive and restore utilities**
  - tar
  - cpio
  - dd
- **Compression**
  - gzip
  - xz
  - bzip2
  - zip
- **Backup types**
  - Incremental
  - Full
  - Snapshot clones
  - Differential
  - Image
- **Off-site/off-system storage**
  - SFTP
  - SCP
  - rsync
- **Integrity checks**
  - MD5
  - SHA