Question-1

Password Recovery and Forensic Analysis

1. Password Recovery Procedure

Follow these steps if the enable secret password is forgotten:

Step 1: Enter ROMMON Mode

1. Connect via console cable and terminal emulator (e.g., PuTTY).
2. Power cycle the router.
3. Press **Ctrl + Break** during bootup to enter **ROMMON mode**.

Step 2: Bypass Startup Configuration

1. Change the configuration register to **0x2142**:

```
2. rommon> confreg 0x2142
3. rommon> reset
```

Step 3: Reset Password

1. The router boots with a default config.
2. Set a new password and restore settings:

```
3. Router> enable
4. Router# configure terminal
5. Router(config)# enable secret NEW_PASSWORD
6. Router(config)# config-register 0x2102
7. Router# write memory
8. Router# reload
```

---

2. Forensic Analysis of Router Logs

After regaining access, investigate for unauthorized activity:

Step 1: Check Login Attempts

```
Router# show login failures
```

Identify brute-force attacks.

Step 2: Review Command History

`Router# show history`Check for unauthorized changes.

Step 3: Review Logs

```
Router# show logging
```

Look for failed logins, unknown changes, and suspicious IPs.

Step 4: Verify User Accounts

```
Router# show running-config | include username
```

Remove unauthorized users:

```
Router(config)# no username HACKER_USER
```

Step 5: Check ACLs

```
Router# show access-lists
```

Delete unknown ACLs:

```
Router(config)# no access-list 101
```

These steps help recover the password and secure the router from unauthorized access.

Question-2

Password Policies in Cisco Devices

Cisco devices support various password policies to enhance security and prevent unauthorized access.

1. Types of Passwords in Cisco Devices:

- **Console Password** – Secures direct console access.
- **VTY Password** – Protects remote access via Telnet/SSH.
- **Enable Password** – Grants privileged EXEC mode (unencrypted).
- **Enable Secret Password** – Encrypted alternative using MD5.
- **AUX Password** – Used for modem/remote management.
- **Line Passwords** – Restrict access to different lines (TTY, VTY, AUX, Console).

2. Strong Password Enforcement Policies:

- **Minimum Length:** Set a minimum password length to prevent weak passwords.
- `Router(config)# security passwords min-length 8`
- **Password Complexity (AAA):** Enforce strong passwords with uppercase, lowercase, numbers, and special characters.

- `Router(config)# aaa new-model`
- `Router(config)# aaa authentication password-policies`
- **Encrypt Stored Passwords:** Prevent plaintext passwords in configuration files.
- `Router(config)# service password-encryption`
- **Use Enable Secret Instead of Enable Password:** Stores passwords securely using MD5 hashing.
- `Router(config)# enable secret STRONG_PASSWORD`

These policies enhance security by enforcing strong authentication and encryption.

Question-3

Role-Based Access Control (RBAC) and Its Importance in Network Security

RBAC is a security model that restricts access based on predefined roles rather than individual users. Users are assigned roles with specific permissions, ensuring they can only perform tasks relevant to their job.

Example Roles in RBAC:

- **Network Administrators** – Full control over routers and firewalls.
- **Support Staff** – View configurations but cannot modify them.
- **Guests** – Internet access only, no internal network privileges.

Importance of RBAC in Network Security:

1. **Enforces Least Privilege (PoLP):** Users get only necessary permissions, reducing security risks.
   - *Example:* Help desk technicians can reset passwords but not modify configurations.
2. **Minimizes Security Risks & Insider Threats:** Prevents unauthorized changes and data breaches.
   - *Example:* Junior IT staff cannot disable firewall rules.
3. **Simplifies User Management:** Assigns access by role instead of configuring users individually.
   - *Example:* New admins are added to the "Admin" role without manual permission settings.
4. **Ensures Compliance:** Helps meet security standards like ISO 27001, GDPR, HIPAA, and NIST.
   - *Example:* Only auditors can access financial records.

RBAC enhances security, simplifies management, and ensures regulatory compliance.