# Secure Router Configuration

C|EH

- Routers are the main gateway to the network and not designed to be security devices

- Routers are vulnerable to different attacks from inside and outside of the network

- An administrator needs to configure a router securely; a misconfigured router is a target for mounting attacks

**Hardening a Router will enable the Admins to prevent attackers from:**

- Gaining information about the network

- Disabling routers and the disrupting the network

- Reconfiguring routers

- Using routers to perform internal attacks

- Using routers to perform external attacks

- Rerouting network traffic

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

# Router Security Measures

C|EH

| | | | | |
|---|---|---|---|---|
| **1** | Implement written, approved, and distributed router policy | **8** | Shutdown unnecessary interfaces |
| **2** | Returned IOS version should be checked and up-to-date | **9** | Identify and check the ports and protocols |
| **3** | Configure users and passwords | **10** | Implement ACL to limit traffic to the required ports and protocols |
| **4** | Enable password encryption | **11** | Implement ACL to block reserved and inappropriate addresses |
| **5** | Implement access restriction on console | **12** | Enable logging |
| **6** | Disable unnecessary services | **13** | Use NTP, to set the router's time of day accurately |
| **7** | Properly configure necessary services such as DNS | **14** | Logs checked, reviewed, and archived as per defined policy |

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

**Notes:** _____

_____

_____

_____

_____

_____

## Design, Implement, and Enforce Router Security Policy

**CEH**

### Router Security Policy Should consist of:

- Password Policy
- Authentication Policy
- Remote Access Policy
- Filtering Policy
- Backup Policy

- Redundancy Policy
- Documentation Policy
- Physical Access Policy
- Monitoring Policy
- Update Policy

## LO#04: Explain Data Leakage Concepts

Notes: _____

_____

_____

_____

_____

_____