|  |  |  |  |
| --- | --- | --- | --- |
| **Practical No** | **Details** | **Date** | **Sign** |
| **1** | **Configure Routers** |  |  |
| **a** | OSPF MD5 authentication. |  |  |
| **b** | NTP. |  |  |
| **c** | to log messages to the syslog server. |  |  |
| **d** | to support SSH connections. |  |  |
|  |  |  |  |
| **2** | **Configure AAA Authentication** |  |  |
| **a** | Configure a local user account on Router and configure authenticate on the console  and vty lines using local AAA |  |  |
| **b** | Verify local AAA authentication from the Router console and the PC-A client |  |  |
|  |  |  |  |
| **3** | **Configuring Extended ACLs** |  |  |
| **a** | Configure, Apply and Verify an Extended Numbered ACL |  |  |
|  |  |  |  |
| **4** | **Configure IP ACLs to Mitigate Attacks and IPV6 ACLs** |  |  |
| **a** | Verify connectivity among devices before firewall configuration. |  |  |
| **b** | Use ACLs to ensure remote access to the routers is available only from  management station PC-C. |  |  |
| **c** | Configure ACLs on to mitigate attacks. |  |  |
|  |  |  |  |
| **5** | **Configuring IPv6 ACLs** |  |  |
|  |  |  |  |
| **6** | **Configuring a Zone-Based Policy Firewall** |  |  |
|  |  |  |  |
| **7** | **Configure IOS Intrusion Prevention System (IPS) Using the CLI** |  |  |
| **a** | Enable IOS IPS. |  |  |
| **b** | Modify an IPS signature. |  |  |
|  |  |  |  |
| **8** | **Layer 2 Security** |  |  |
| **a** | Assign the Central switch as the root bridge. |  |  |
| **b** | Secure spanning-tree parameters to prevent STP manipulation attacks. |  |  |
| **c** | Enable port security to prevent CAM table overflow attacks. |  |  |