Router Device Security Lab

Configuring Secure Passwords

1. Configure the enable secret and password

```
  enable password TRUSTME
  enable secret letmein
```

Look at the configuration: `show config terminal`
Note the difference between the number '5' and number '7' which indicates the encryption technique used to encrypt the key. Also note that the command 'password service encryption' is in the configuration file. This command is enabled by default and ensures that passwords and secrets in the configuration files are stored in an encrypted form.

Which takes precedence, the enable password or the enable secret ?

- disconnect and log in using the enable password
- disconnect and log in using the enable secret

What happens when you configure the following:

```
enable secret 5 letmein
```

You should see that the configuration expects the key to be in encrypted form if you use the syntax:

```
 enable secret 5 <secret>
```

or

```
enable password 7 <password>
```

2. Configure local database of users

```
   username <name1> secret <secret1>
   username <name2> secret <secret2>
```

Note that you can also use the 'password' command but the 'secret' command gives you a better encryption algorithm.

Configuring Console and Vty Access

1. Configure the console interface with a timeout of 15 minutes

```
line con 0
 exec-timeout 15 0
 transport input none
```

2. Configure a filter to allow only the trusted hosts to have Telnet access. Note that all tries are logged to have an audit trail of all access to the router.

```
access-list 103 remark VTY Telnet Access ACL
access-list 103 permit tcp host <IP address> host 0.0.0.0
eq 23 log-input
access-list 103 permit tcp host <IP address> host 0.0.0.0
eq 23 log-input
access-list 103 deny ip any any log-input
```

3. Configure the Vty ports

```
line vty 0 4
 access-class 103 in
 exec-timeout 15 0
 transport input telnet
```

Test to make sure that only telnet from the configured host can have access to the router.

4. Enable SSH connectivity which is much more secure than telnet.

Generate the router key with the command: `crypto key generate rsa`
Note that the command is NOT performed in configuration mode.

Create the filter to allow SSH access. Create a new filter which can be tested and then later the old one can be removed:

```
access-list 104 remark VTY Telnet and SSH Access ACL
access-list 104 permit tcp host <IP address> host 0.0.0.0
range 22 23 log-input
access-list 104 permit tcp host <IP address> host 0.0.0.0
range 22 23 log-input
access-list 104 deny ip any any log-input
```

Modify vty access command to allow ssh:

```
line vty 0 4
 access-class 104 in
 exec-timeout 15 0
 transport input telnet ssh
```

Test to make sure that ssh from the permitted host can get access to the router.

Configuring Logging

1. Configure good timestamps in the logs

```
service timestamps debug datetime msec show-timezone
localtime
```

```
service timestamps log datetime msec show-timezone
localtime
```

2. Configure fallback local logging as backup to syslog server and do not log anything to console to save CPU cycles

```
logging buffered 16384 debugging
no logging console
```

3. Set the proper timezone. Note that it is good to standardize on one timezone for all routers to simplify problem tracking.

```
clock timezone GMT 0
```

4. Configure the loopback0 interface as the source of our log messages. This is often used for routing protocols as well. Select an IP address that uniquely identifies this router. One trick is to allocate a netblock for use as the router loopback netblock.

```
int loopback0
 ip address 10.192.168.X 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
```

5. Configure the syslog logging host and capture all of the logging output with FACILITY LOCAL5.

```
logging trap debugging
logging facility local5
logging source-interface loopback0
logging <IP Address of syslog server>
```

Test logging by trying to connect to the router. Check the local buffer logging information by using the command: `sh buffer`

Note: It is important to Synchronize the clocks with a local (trusted and authenticated) NTP server. When authenticating between an NTP client (the router) and server, the configured key must be the same on both the router and the NTP server. The following commands would be used:

```
ntp authentication-key 6767 md5 <KEY>
ntp authenticate
ntp update-calendar
ntp server <IP Address of NTP server>
```

Disable All Unused Access Capabilities and Services

1. Disable the http server(s) since they are never used

```
no ip http server
no ip http server-secure
```

2. Disable CDP which contains important router information. This command is disabled CDP globally: `no cdp run`

[Note that if you ever require CDP on an interface, use the global command `cdp run` and disable cdp by using the command `no cdp enable` on the Internet-facing interface.]

3. Disable services which can be used for reconnaissance attempts or other attacks:

```
no service pad
no ip source-route
no ip finger
no ip bootp server
no ip domain-lookup
```

Secure SNMP Access

1. Configure the filter which only allows SNMP access to specific hosts

```
access-list 20 remark SNMP ACL
access-list 20 permit <IP Address of SNMP server>
access-list 20 deny any log
```

2. Configure SNMP to have READ-ONLY access and treat the COMMUNITY string as a password - keep it difficult to guess.

```
snmp-server community <COMMUNITY> RO 20
```

Miscellaneous

Configure an appropriate banner. As an example:

```
banner motd %
Access to this device is prohibited without express written
permission. All access is logged.  Violators will be
prosecuted to the fullest extent of both civil and criminal
law.
%
```