SECURING A CISCO ROUTER

OVERVIEW

A. Configure fundamental router security

B. Examine principles of routing

C. Examine the use of Access Control Lists (ACLs) on a Cisco router

D. Configure logging on a Cisco router

Image by rawpixel.com

A. CONFIGURE FUNDAMENTAL ROUTER SECURITY

1. Key Topics

1.1 Cisco AutoSecure

```
Router# auto secure

                    --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
```

When configuring a newly setup router, Cisco's AutoSecure feature can assist with enhancing system security. After entering the **auto secure** command in privileged EXEC mode, a script will run a series of prompts for the administrator to customize the system's security configuration.

After selecting this to be an internal router:

```
Is this router connected to internet? [no]: no

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
```

- Services with common vulnerabilities are disabled
- Services to enhance system security are enabled
- Device passwords are encrypted within the configuration file

After completing the AutoSecure script, your router can have additionally been configured with:

- *Login Blocking Period (deter brute-force attack)*
- *Maximum Login Failures*
- *TCP Intercept Feature (prevent tcp syn attack)*
- *..and more*

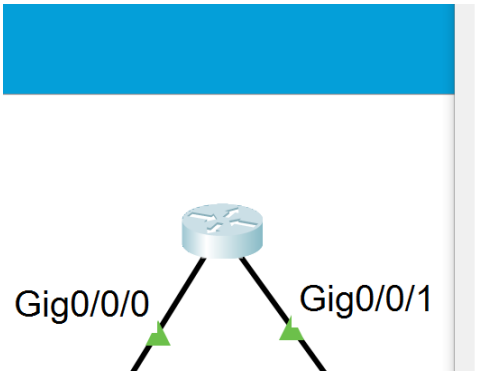
Note: Cisco AutoSecure will not FULLY secure your system by any means

The script implements configurations with some fallbacks that will require additional configuration. For example, if you do not setup an SSH server configuration during the prompts, ***vty lines*** *will be set to allow* ***telnet*** *connections. Telnet is a network service (port 80) used to remotely interface into a system, but does not utilize encryption or credentials and remains unsecure for use.*

```
line vty 0 4
 login authentication local_auth
 transport input telnet
```

1.2 Manually Shutdown & Label Unused Ports

This is an administrative best practice to secure ports left unused by the current network implementation. If users have access to the physical location of the router, it would be possible for them to **connect an unauthorized device** to an available physical interface on the router.




```
Router#show ip int brief
Interface                  IP-Address
Status                     Protocol
GigabitEthernet0/0/0       192.168.0.1
up                         up
GigabitEthernet0/0/1       192.168.1.1
up                         up
GigabitEthernet0/0/2       unassigned
up                         down
```

- The **router** on the left currently has two active connections, **G0/0/0** and **G0/0/1**
- However, there exists a third connection that is up, **G0/0/2**
- Manually shut down **G0/0/2** and set a description for documentation

```
Router(config)# int g0/0/2
Router(config-if)# shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/2, changed state to administratively down

Router(config-if)# description Administratively Shutdown
Router(config-if)#
```

1.3 Passwords

Purpose	*Router Command*
Encrypt all plaintext passwords	***service password-encryption***
Set minimum password length	***security passwords min-length** 10*
Deter brute-force attack	***Login block-for** 180 **attempts** 3 **within** 60*

1.4 Secure Setup Remote Access using SSH

Step 1) Configure a unique device hostname

Step 2) Configure the IP domain name

Step 3) Generate RSA keys to encrypt SSH traffic

Step 4) Verify/Create a local database entry

Step 5) Authenticate against the local database

Step 6) Enable vty inbound SSH sessions

```
Router(config)#hostname R1-demo
R1-demo(config)#ip domain name cisco.com
R1-demo(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1-demo.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:19:40.611: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1-demo(config)#username admin secret dg489^x#12v
R1-demo(config)#line vty 0 15
R1-demo(config-line)# login local
R1-demo(config-line)#transport input ssh
R1-demo(config-line)#exit
```

Note: Telnet becomes disabled and only SSH is allowed on virtual terminal lines 0 through 15. This means we can have up to 16 terminal sessions (max) connected securely at one time.

1.5 Disable Unused Services

*Verify what services are running with the **'show ip ports all'** command.*

Purpose	*Router Command*
Disable DNS lookup	***no ip domain-lookup***
Disable viewing users logged on	***no ip finger***
Disable HTTP (unsecure web browsing)	***no ip http server***
Disable IP messages used to map out the network topology	***no ip unreachables***
Disable ICMP mask replies containing network information	***no ip mask-reply***
Disable CDP (which is enabled default)	***no cdp enable***

B. PRINCIPLES OF ROUTING

Key Topics

1.1 Routing Concepts

1.2 Static Routing

1.3 Dynamic Routing

1.1 Routing Concepts

- **Routing** – router (or L3 switch) determines which physical interface should be used to forward IP packets to a destination
- **Path Determination** – routes that go into a router's IP table with the **most** network bits are the **best (longest) entries** for forwarding packets
- **Routing Table** is maintained and consulted by a router to determine where to send a packet
  - Directly connected networks are added when a local physical interface is active (UP) and configured with a valid IP address and subnet mask
  - Remotely connected networks are not directly connected to a router, but instead is learned from one of two ways: **statically** OR **dynamically**
- **Default route** specifies the next-hop router for when a routing table does not contain the destination IP within a packet

1.2 Static Routing

- **Static routes** are manually configured and include a remote network address and the IP address of the next hop router

```
R1-demo(config)# ip route 192.168.1.0 255.255.255.0 104.113.45.226
```

Where **192.168.1.0 255.255.255.0** = Remote Network

And **104.113.45.226** = Next Hop Router

- **Characteristics**:
  - Not automatically updated and requires manual reconfiguration
  - Best used in smaller networks with few redundant links
  - Commonly used with DRP (Dynamic Routing Protocol) to configure a default route

1.2 Dynamic Routing

- **Dynamic routes** are remote networks automatically learned by a router from other routers. This is done through dynamic routing protocols, such as OSPF or EIGRP.

```
R1-demo(config)# router ospf 1
R1-demo(config-router)# network 192.168.3.0 0.0.0.255 area 0
R1-demo(config-router)#exit
```

Where **ospf 1** is the process ID

And **network 192.168.3.0** is the remote network

And **0.0.0.255** is the wildcard mask (inverted subnet mask)

And **area 0** can be replaced with any valid OSPF area number

- **Characteristics**:
  - Discover remote networks from other routers
  - Automatically maintain routing information
  - Attempt to find a new best path if the current one is not available
  - Prioritize the best path to send packets to destination networks

C. EXAMINE ROUTER ACLS

- **Access Control Lists (ACLs)** are rule-based lists that filter network traffic based on (source/destination) IP addresses or port numbers
- Before accepting traffic, routers check ACL entries top-to-bottom for a matching rule

  Once a matching rule is found, any following rules below it will not be taken into consideration

  If no matching rule is found, the packet will be dropped
- There is a hidden **Deny Everything** (Implicit Deny) at the bottom of every ACL

- **Types:**
  - **Standard**
    - Numbers 1-99
    - Identifies traffic on Source Address only

```
R1-demo(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

ACL # | Action | Source IP | Wildcard Mask

  - **Extended**
    - Numbers 100-199
    - Identifies traffic on (Source/Destination) IP address and Protocol

Dest. IP & Wildcard

```
R1-demo(config)#access-list 150 deny tcp 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.0 eq ftp
```

Protocol | Operator “eq” Service “ftp”

  - **Named**
    - Replaces the number an ACL (standard or extended) is assigned with a desired name for better identification and management

```
R1-demo(config)# ip access-list extended demo_ACL
```

ACL Name

- Cisco ACL Documentation

D. CONFIGURE LOGGING

1. Key Topics

1.1 System Message Logging Basics

1.2 Configuring Logging

1.3 Displaying logging configuration

1.1 System Message Logging Basics

- By default, wireless devices send system message outputs to a **logging process**.

  The **logging process** can send the outputs to destinations such as:

  - Logging buffer
  - Terminal lines
  - UNIX syslog server
  - Console

- When **logging is disabled**, messages are sent only to console
- Logs can be accessed through the access point CLI or by saving them to a syslog server
- Message properties:
  - <= 80 characters
  - % sign follows sequence num or timestamp (if configured)
  - Displayed as:

    seq no:timestamp: %facility-severity-MNEMONIC:description
- Cisco Logging Documentation

1.2 Configuring Logging

Purpose	Router Command (Global Config)
Log messages to internal system buffer *(Default size 4096 -> set up to 2147483647 bytes)* *(Levels -> emergencies (0); alerts (1); crticial (2); errors (3); warnings (4); notifications (5); informational (6); debugging (7)*	***logging buffered [size] [level]***
Log messages to syslog server host	***logging [host ip or name]***
Log messages to non-console terminal (current session only)	***terminal monitor***
Disable Logging	***no logging on***

Enabling/Disabling Log Metadata & Filter Levels

Purpose	Router Command (Global Config)
Enable log timestamps ***Same as previous but with desired parameters***	***Service timestamps log uptime*** *Or* ***Service timestamps log datetime [msec] [localtime] [show-timezone]***
Enable log sequence numbers	***service sequence-numbers***
Limit messages logged to console	***logging console [level]***
Limit messages logged to syslog servers	***logging trap [level]***
Limit messages logged to terminal lines	***logging monitor [level]***