Network security – session 9-2

Router Security

Network II

Router security

- First line of defense of the network
- Compromise of a router can lead to many issues:
  - Denial of network services
  - Degrading of network performance
  - Exposure of network configuration details
  - Exposure of the network topology
  - Exposure of the sensitive data

Security issue

- Pysical security – lock and key
- Easiest access is via console port
- Password recovery possible
- Up to date Operating system – most stable release of IOS

- Configuration hardening

Configuration hardening

- Local access restriction
  - console line
- Remote access restriction
  - Vty line
- Use line & Exec password – to gain access to the router
- Service password encryption command encrypts the line passwords
- EXEC level password – enable secret command

Configuration hardening (cont…)

- Two password protection schemes used in Cisco IOS:
- **Type 7** uses a Cisco encryption algorithm, which is not as strong as
- **Type 5** protection, which uses MD5 hash.

Configuration hardening (cont…)

- Create a user account for authorized personnel – for keeping track and log each time a system is accessed
- Create a local user account on the router

Username [*name*] **privilege** [*level*] **password** [*password_string*]

```
RouterA(config)# username admin privilege 10 password
@dm1np@$$wd
```

Configuration hardening (cont…)

- Cisco provides 16 levels (0-15) of privileges – level 15 the highest – equivalent to privileged EXEC mode
- Local user admin is created with level 10

- Disadvantage of creating local user:
  - The same user to be created on all routers in the network!
  - Mmmmh where is scalability?

Configuration hardening (cont…)

- Cisco offers Authentication, Authorization and Accountability (AAA) service to centrally manage and control user access
- RADIUS (Remote Authentication Dial In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus), are supported with AAA
- Implies that cisco routers can communicate with RADIUS or TACACS+ servers for central authentication

Configuration hardening (cont…)

- AAA enables authentication based on the router's local user database, enable, line passwords, as well as other access protocols
- Configuration example –define authentication method

```
RouterA(config)# aaa new-model
RouterA(config)# aaa authentication login default local
group tacacs+
RouterA(config)# aaa authorization exec default local
group tacacs+
if-authenticated
```

Configuration hardening (cont...)

- Apply authentication to any access entry point.
  - Line console
  - Auxiliary port
  - Virtual terminal – vty lines
- Enforces authentication using the local user database and the timeout of 5 minutes if the user input is not detected
- Prevents the remote access to the console port via reverse-telnet -transport input none:

Configuration hardening (cont…)

- Demo configuration

```
RouterA(config)#line con 0
RouterA(config-line)#login local
RouterA(config-line)#exec-time 5 0
RouterA(config-line)#transport input none
```

**Login authentication required

To enable SSH

- Need to generate an RSA key
- You require to pre-configure a hostname and a domain name on the router to generate an RSA key – will be used as part of the key

  ip domain-name test ?

  crypto key generate rsa – Command
- After the RSA key is generated, the remote VTY access can be configured with SSH as the transport

To enable SSH

```
RouterB(config)# access-list 15 permit 10.10.20.0
0.0.0.255
RouterB(config)# access-list 15 deny any
RouterA(config)# line vty 0 4
RouterA(config-line)# access-class 15 in
RouterA(config-line)# login authentication default
RouterA(config-line)# transport input ssh
RouterA(config-line)#exec-time 5 0
```

- The command *transport input ssh* enforces SSH as the only access method

Router Services

- Routers have many services enabled by default
- Disable unnecessary service &
- Tighten the necessary services
- Enabled TCP/IP services by default
  - echo,
  - discard,
  - daytime,
  - chargen,
  - finger,
  - identd, and
  - Snmp
  - bootps,

Router Services

- To disable them globally use the following commands:

```
RouterA(config)#no service tcp-small-servers
RouterA(config)#no service udp-small-servers
RouterA(config)#no ip bootp server
RouterA(config)#no service finger
RouterA(config)#no ip identd
```

- The following services: echo, discard, daytime, and chargen are considered TCP and UDP small services
- Disabled using *no service tcp-small-servers* and *no service udp-small-servers*

Router Services

- Tighten security for needed services like:
  - Simple Network Management Protocol (SNMP)
  - HTTP
- SNMP default community string **must not** be used
- Use a new community string which should be difficult to guess
- Avoid read-write access - use read only access

Router Services

- SNMP access should be restricted to certain known SNMP agents
- Use SNMP version 3
- Example with a read-only configuration
  - *RouterA(config)#snmp-server community M@ke1tD1ff1cuLT ro 10*
- Web-based administration via HTTP can reveal passwords – option, HTTPS

Router Services

- HTTPS that provides end-to-end SSL encryption, as shown:

```
RouterA(config)# no ip http server
RouterA(config)# ip http secure-server
RouterA(config)# ip http access-class 15
RouterA(config)# ip http authentication aaa
```

- Normal HTTP service disabled
- HTTPS service enabled
- HTTP access is restricted with the access-list 15
- HTTP will use AAA authentication

Router Services

- Other services to disable includes
  - CDP
  - Remote configuration downloading &
  - Source-routing

```
RouterA(config)#no cdp run
RouterA(config)#no service config
RouterA(config)#no ip source-route
```

- Source-routing can be used in many kinds of attacks.
- disabling the feature - the router will disregard the IP packet with source routes information

Securing router

- Interface level
  - Shutdown unused ports
  - Disable Directed broadcasts – can usedas a DoS attack fx smurf attact (new IOS – disabled)
  - Disable interface acting as intermediary for ARP or ARP-proxy

```
RouterA(config)# interface fastethernet0/1
RouterA(config-if)#shutdown
RouterA(config)# interface fastethernet0/2
RouterA(config-if)# no ip directed-broadcast
RouterA(config-if)# no ip proxy-arp
RouterA(config-if)# no ip unreachables
RouterA(config-if)# no ip redirects
RouterA(config-if)# no ip mask-reply
```

Securing router

- Router Logging and Access-List
- Administrator to analyze the events that occur and use the given information to correlate and find the issues
- To keep accurate logs, the correct time on a router has to be set up
- Cisco routers support the Network Time Protocol (NTP), which can be set up to synchronize the router's clock with the time server

- There are 8 levels (0–7) of log severity:
  - Emergencies (0)
  - Alerts (1)
  - Critical (2)
  - Errors (3)
  - Warnings (4)
  - Notifications (5)
  - Informational (6)
  - Debugging (7)

Securing router

- To correlate the time with the log events, a timestamp service will need to be initiated
- To keep accurate logs, the correct time on a router has to be set up
- Cisco routers support the Network Time Protocol (NTP), which can be set up to synchronize the router's clock with the time server

Log example

```
RouterA(config)# service timestamps log datetime msec
RouterA(config)# logging on
RouterA(config)# logging buffered 16000 debugging
RouterA(config)# logging trap debugging
RouterA(config)# logging 172.20.20.20
```

OR by using access list

```
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 101 permit tcp any any eq 80
access-list 101 deny ip any any log
```

The following example shows an access-list 102 that contains an IP address spoofing protection for the internal network of 12.12.12.0/24.

Applied to the outbound interface

```
access-list 102 deny ip 12.12.12.0 0.0.0.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 permit ip any any
```

Switch Security

- Switch Port Security

```
SwitchA(config)# interface range Gigabitethernet1/1-24
SwitchA(config-if)#shutdown
```

- To configure the maximum number of MAC addresses on a switch port, use the command *switchport port-security maximum [number]*
- To configure a port to allow certain MAC addresses to pass traffic, use the command switchport port-security mac-address [mac_address] or switchport port-security mac-address sticky [mac_address]

Switch Security

- Switch Port Security
- To configure a port to allow certain MAC addresses to pass traffic, use the command *switchport port-security mac-address [mac_address]* or *switchport port-security mac-address sticky [mac_address].*
- Define a violation action as:
  - protected, restrict, and shutdown

Switch Security

- Switch Port Security
- Define a violation action as:
  - protected, restrict, and shutdown
  - The violation action protected will drop packets from the violated MAC address(es)
  - violation action restrict is the same as the protected mode, but it will also send SNMP trap messages to the SNMP server

Switch Security

- Switch Port Security
- Violation action shutdown is to shutdown the port and put the port in ERRDISABLE state.

example of a port security configuration

```
SwitchA(config)# interface Gigabitethernet1/10
SwitchA(config-if)#switchport port-security maximum 2
SwitchA(config-if)#switchport port-security mac-address
sticky
0011.2233.440a
SwitchA(config-if)#switchport port-security mac-address
sticky
0011.2233.440b
SwitchA(config-if)#switchport port-security violation
shutdown
```