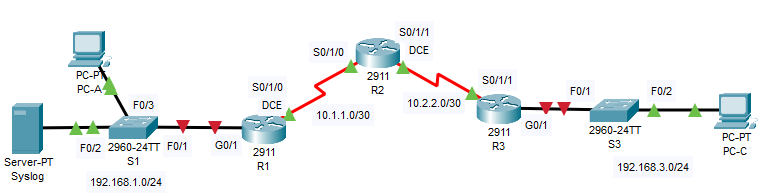
Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using the CLI

1. Topology



1. Addressing Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A | S1 F0/1 |
| S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | G0/1 | 192.168.3.1 | 255.255.255.0 | N/A | S3 F0/1 |
| S0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| Syslog | NIC | 192.168.1.50 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-A | NIC | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | S1 F0/3 |
| PC-C | NIC | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 | S3 F0/2 |

1. Objectives

Part 1: Configure Basic Router Settings

* Configure hostname, interface IP addresses, and access passwords.
* Configure the static routing.

Part 2: Use CLI to Configure an IOS IPS

* Configure IOS IPS using CLI.
* Modify IPS signatures.
* Examine the resulting IPS configuration.
* Verify IPS functionality.
* Log IPS messages to a syslog server.

1. Background / Scenario

In this lab, you will configure the Cisco IOS IPS, which is part of the Cisco IOS Firewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur. IPS alone is not enough to make a router into a secure Internet firewall, but when added to other security features, it can be a powerful defense.

You will configure IPS using the Cisco IOS CLI and then test IPS functionality. You will load the IPS Signature package from a TFTP server

Your task is to enable IPS on R1 to scan traffic entering the 192.168.1.0 network.

The server labeled Syslog is used to log IPS messages. You must configure the router to identify the syslog server to receive logging messages. Enable IOS IPS

**Note**: Within Packet Tracer, the routers already have the signature files imported and in place. They are the default xml files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.

1. Configure Basic Router Settings

In Part 1, you will set up the network topology and configure basic settings, such as hostnames, interface IP addresses, static routing, device access, and passwords.

**Note**: Perform the steps listed in Part 1 on all three routers. Only R1 is shown below.

* + 1. Cable the network as shown in the topology.

Attach the devices, as shown in the topology diagram, and cable as necessary.

* + 1. Configure the basic settings for each router.
       1. Configure the hostnames, as shown in the topology.
       2. Configure the interface IP addresses, as shown in the IP Addressing table.
       3. Configure a clock rate for serial router interfaces with a DCE serial cable attached.

R1(config)# **interface S0/1/0**

R1(config-if)# **clock rate 64000**

* + - 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands.

R1(config)# **no ip domain-lookup**

* + 1. Configure static routing on the routers.
       1. Configure a static default route using a next-hop IPv4 address from R1 to R2 and from R3 to R2.
       2. Configure a static route from R2 to the R1 LAN (192.168.1.0) and from R2 to the R3 LAN (192.168.3.0) using the appropriate next-hop IPv4 address.
    2. Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for syslog , PC-A and PC-C, as shown in the IP Addressing table.

* + 1. Verify basic network connectivity.
       1. Ping from R1 to R3.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

* + - 1. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

**Note**: If you can ping from PC-A to PC-C, you have demonstrated that the static routing protocol is configured and functioning correctly. If you cannot ping, but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to identify routing protocol-related problems.

* + 1. Configure a user account, encrypted passwords, and crypto keys for SSH. Do for all three routers.

**Note**: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

* + - 1. Configure a minimum password length using the **security passwords** command to set a minimum password length of 10 characters.

R1(config)# **security passwords min-length 10**

* + - 1. Configure a domain name.

R1(config)# **ip domain-name ccnasecurity.com**

* + - 1. Configure crypto keys for SSH

R1(config)# **crypto key generate rsa general-keys modulus 1024**

* + - 1. Configure an admin01 user account using **algorithm-type scrypt** for encryption and a password of cisco12345.

R1(config)# **username admin01 algorithm-type scrypt secret cisco12345**

* + - 1. Configure line console 0 to use the local user database for logins. For additional security, the **exec-timeout** command causes the line to log out after five minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

**Note**: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to **0 0**, which prevents it from expiring. However, this is not considered a good security practice.

R1(config)# **line console 0**

R1(config-line)# **login local**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **logging synchronous**

* + - 1. Configure line aux 0 to use the local user database for logins.

R1(config)# **line aux 0**

R1(config-line)# **login local**

R1(config-line)# **exec-timeout 5 0**

* + - 1. Configure line vty 0 4 to use the local user database for logins and restrict access to only SSH connections.

R1(config)# **line vty 0 4**

R1(config-line)# **login local**

R1(config-line)# **transport input ssh**

R1(config-line)# **exec-timeout 5 0**

* + - 1. Configure the enable password with strong encryption.

R1(config)# **enable algorithm-type scrypt secret class12345**

* + 1. Save the basic configurations for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

R1# **write Memory**

1. Configuring IPS Using the Cisco IOS CLI

In Part 2 of this lab, you will configure IPS on R1 using the Cisco IOS CLI. You then review and test the resulting configuration.

* 1. Verify Access to the R1 LAN from R2

In this task, you will verify that without IPS configured, the external R2 can ping the R1 S0/1/0 interface and PC-A on the R1 internal LAN.

* + 1. Ping from R2 to R1.

From R2, ping R1 interface S0/1/0 at IP address 10.1.1.1.

R2# **ping 10.1.1.1**

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

* + 1. Ping from R2 to PC-A on the R1 LAN.

From R2, ping PC-A on the R1 LAN at IP address 192.168.1.2.

R2# **ping 192.168.1.2**

If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

* + 1. Display the R1 running configuration prior to configuring IPS.

Issue the **show run** command to review the current basic configuration on R1. Remove the surplus ! in your result.

R1#sh run

Are there any security commands related to IPS?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Create an IOS IPS configuration directory in flash.

On **R1**, create a directory in flash using the **mkdir** command. Name the directory **ipsdir**.

R1# **mkdir ipsdir**

Create directory filename [ipsdir]? <**Enter**>

Created dir flash:ipsdir

* + 1. Configure the IPS signature storage location.

On **R1**, configure the IPS signature storage location to be the directory you just created.

R1(config)# **ip ips config location flash:ipsdir**

* + 1. Create an IPS rule.

On **R1**, create an IPS rule name using the **ip ips name** *name* command in global configuration mode. Name the IPS rule **iosips**.

R1(config)# **ip ips name iosips**

* + 1. Enable logging.

IOS IPS supports the use of syslog to send event notification. Syslog notification is enabled by default. If logging console is enabled, IPS syslog messages display.

* + - 1. Enable syslog if it is not enabled.

R1(config)# **ip ips notify log**

* + - 1. If necessary, use the **clock set** command from privileged EXEC mode to reset the clock.

R1# **clock set 10:20:00 10 january 2014**

* + - 1. Verify that the timestamp service for logging is enabled on the router using the **show run** command. Enable the timestamp service if it is not enabled.

R1(config)# **service timestamps log datetime msec**

* + - 1. Send log messages to the syslog server at IP address 192.168.1.50.

R1(config)# **logging host 192.168.1.50**

* + 1. Configure IOS IPS to use the signature categories.

Retire the **all** signature category with the **retired true** command (all signatures within the signature release). Unretire the **IOS\_IPS Basic** category with the **retired false** command.

R1(config)# **ip ips signature-category**

R1(config-ips-category)# **category all**

R1(config-ips-category-action)# **retired true**

R1(config-ips-category-action)# **exit**

R1(config-ips-category)# **category ios\_ips basic**

R1(config-ips-category-action)# **retired false**

R1(config-ips-category-action)# **exit**

R1(config-ips-cateogry)# **exit**

Do you want to accept these changes? [confirm] **<Enter>**

* + 1. Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the **ip ips name** *direction* command in interface configuration mode. Apply the rule outbound on the G0/1 interface of **R1**. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

**Note**: The direction **in** means that IPS inspects only traffic going into the interface. Similarly, **out** means that IPS inspects only traffic going out of the interface.

R1(config)# **interface g0/1**

R1(config-if)# **ip ips iosips out**

1. Modify the Signature
   * 1. Change the event-action of a signature.

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature action to alert and drop.

R1(config)# **ip ips signature-definition**

R1(config-sigdef)# **signature 2004 0**

R1(config-sigdef-sig)# **status**

R1(config-sigdef-sig-status)# **retired false**

R1(config-sigdef-sig-status)# **enabled true**

R1(config-sigdef-sig-status)# **exit**

R1(config-sigdef-sig)# **engine**

R1(config-sigdef-sig-engine)# **event-action produce-alert**

R1(config-sigdef-sig-engine)# **event-action deny-packet-inline**

R1(config-sigdef-sig-engine)# **exit**

R1(config-sigdef-sig)# **exit**

R1(config-sigdef)# **exit**

Do you want to accept these changes? [confirm] **<Enter>**

* + 1. Use show commands to verify IPS.

Use the **show ip ips all** command to view the IPS configuration status summary.

Enter the result here:

R1#sh ip ips all

To which interfaces and in which direction is the **iosips** rule applied?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Verify that IPS is working properly.
       1. From **PC-C**, attempt to ping **PC-A**. Were the pings successful? Explain.

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. From **PC-A**, attempt to ping **PC-C**. Were the pings successful? Explain.

C:\>ping 192.168.3.2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. View the syslog messages.
       1. Click the **Syslog** server.
       2. Select the **Services** tab.
       3. In the left navigation menu, select **SYSLOG** to view the log file.