Practical 7: Configure IOS Intrusion Prevention System (IPS) Using the CLI

The routers have also been preconfigured with the following: o Enable password: ciscoenpa55

Console password: ciscoconpa55

SSH username and password: SSHadmin / ciscosshpa55

OSPF 101

**Write the commands for the above**

Part 1: Enable IOS IPS

Step 1: Enable the Security Technology package.

R1(config)#Show version

R1(config)# license boot module c1900 technology-package securityk9

Accept the end user license agreement.

Do copy run start

R1(config)#Show version

Step 2: Verify network connectivity.

Step 3: 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

Step 4: Configure the IPS signature storage location

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

Step 5: Create an IPS rule.

R1(config)# ip ips name iosips

Step 6: Enable logging.

R1(config)# ip ips notify log

R1(config)# service timestamps log datetime msec

R1(config)# logging host 192.168.1.50

Step 7: Configure IOS IPS to use the signature categories.

R1(config)# ip ips signaturecategory

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]

Step 8: Apply the IPS rule to an interface.

R1(config)# interface g0/1

R1(config-if)# ip ips iosips out

Part 2: Modify the Signature

Step 1: Change the event-action of a signature.

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-sigdefsig-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]

Step 2: Use show commands to verify IPS.

show ip ips all

Step 3: Verify that IPS is working properly

1. From PC-C, attempt to ping PC-A

The pings should fail. T

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

The ping should be successful. T

Step 4: View the syslog messages. a. Click the Syslog server. b. Select the Services tab. c. In the left navigation menu, select SYSLOG to view the log file.