ISM

Configuring IPS (Intrusion Prevention System)

Step 1: Enable the security Technology package

R1(config)# license boot module c1900 technology package security K9

Step 2: Verify network connectivity

a. Ping from PC-C to PC-A

b. Ping from PC-A to PC-C

Step 3: Create an IOS IPS configuration directory in flash.

R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash: ipsdir

Step 4: Configure the IPS signature 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# clock set 13:41:00 14 February 2023

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 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)# ~~exit~~ category IOS-ips basic

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

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

R1(config-ips-category)# exit

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

Step 8: Apply the IPS rule to an interface

R1(config)# interface g 0/1

R1(config-if)# ip ips ios ips out

Modify the 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-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-sidgf)# exit
Do you want to accept these changes? [Confirm]<Enter>

Information Security Audit

Definition: Formal process by certified professionals to measure information systems performance.

Techniques: Personal interviews, policy reviews, vulnerability scans, OS settings, examination, network analysis, data log analysis

Scope: <1> Type of data assets
<2> Value of data & priority
<3> Previous incidents
<4> Time available
<5> Auditor experience

Constraints: <1> Time, <2> 3rd party access, <3> Business operation continuity <4> Techology tools.

Diagnostic measures: Vulnerability assesments, penetration testing.