# Practical 7

Configuring IOS Intrusion Prevention system (IPS) using CLI

## Part 1 - Enable IOS IPS

### Step 1 - Enable the security technology package

R1 # show version
R1 # conf t
R1 (config) # license boot module c900 technology-package security k9

R1 (config) # end
R1 # copy run start
R1 # reload
R1 # show version

### Step 2 - Create an IOS IPS configuration directory in flash

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

### Step 3 - Configure IPS Signature storage Location

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

### Step 4 - Create an IPS rule

R1(config)# ip ips name iosips

Step 5 - Enable logging

R1(config)# ip ips notify log
R1# clock set 21:00:00 13 March 2019
R1# conf t
R1(config)# service timestamps log datetime msec
R1(config)# logging host 192.168.1.3

Step 6 - Configure IOS IPS to use 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)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] (Enter)

Step 7 - Apply the IPS rule to an interface

R1(config)# interface g0/1
R1(config-if)# ip ips iosips out

Task 2 - Modify the signature.

Step 1 - Change the event action of a signature

```
F1 (config) #ips sig signature = definition
F1 (config-sigdef) # signature 2004 0
F1 (config-sigdef-sig) # status
F1 (config-sigdef-sig-status) # retired false
F1 (config-sigdef-sig-status) # enabled true
F1 (config-sigdef-sig-status) # exit
F1 (config-sigdef-sig) # engine
F1 (config-sigdef-sig-engine) # event-action produce-alert
F1 (config-sigdef-sig-engine) # event-action deny-packet-inline
F1 (config-sigdef-sig-engine) # exit
F1 (config-sigdef-sig) # exit
F1 (config-sigdef) # exit
```

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

Step 2 - Verify that IPS is working properly

R1# show ip ips all

a) Ping from PC-C to PC-A, it should fail because the IPS rule for ivent-action of an echo was sent to deny-packet-inline

PC> ping 192.168.1.3

b) Ping from PC-A to PC-C, it should succeed.

PC > ping 192.168.3.3

Step 3 - View the messages

a) Click the syslog server

b) Select the services tab

c) In the left menu, select SYSLOG to view the log file.