P6(: Configure IOS Intrusion Prevention System (IPS) Using the CLI)

GO to the RIP

check ping in PC1 AND PC0 (ko server ke IP Address se)

PART1: Enable the IOS IPS (on Router1)

Type the following command in the CLI mode of Router1

```
Router#show version
```

As seen above the security package is not enabled, to enable the security feature, type the following command in Router1

```
Router#configure terminal
Router(config)#license boot module c1900 technology-package
securityk9 ACCEPT? [yes/no]: y
```

Press enter key

```
Router#
Router#reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm] Press Enter key
Press RETURN to get started! Press Enter key
Router>enable
Router# Router#show version
```

We will get a message informing whether the security package is enabled or not

As seen above now the security package has been enabled

Now type the following commands in the CLI mode of Router1

```
Router#
Router#clock set 10:30:45 march 3 2022
Router#mkdir smile
Create directory filename [smile]? Press enter key
Created dir flash:smile
Router#
Router#configure terminal
```

```
Router(config)#ip ips config location flash:smile
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
Router(config)#interface Serial0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#
Press enter key
Router(config-if)#exit
Router(config)#
```

Part 2: Modify the Signature

Type the following commands in the CLI mode of Router1

```
Router(config)#
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
Router(config)#
```

Now we need to verify the above IPS configuration, we do it first by pinging PC1 to SERVER and then from SERVER to PC1

PC1 to SERVER – The ping fails,

Server to PC1 – The Ping is successful

We check the Syslog service on the server to check the logging activity, by typing the following commands in Router0

```
Router>enable
Router#configure terminal
Router(config)#logging 192.168.1.2
Router(config)#
Router(config)#
Router(config)#exit
Router#
Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
Router#
```

Hence, we set the IPS and also verified it on Router1