VSIT

Security in Computing
Practical #6

Name	Sanjeev Gupta	**Roll Number**	21302B0023
Class	TYBScIT	**Division**	C
Subject/Course	Security in Computing		
Topic	Configure IOS Intrusion Prevention System (IPS) Using the CLI		

Topology and Addressing Table for IPS using CLI

Use the pre-configured topology shared as an attachment with this worksheet. Configure this topology for IPS using CLI

Objectives

- Enable IOS IPS.
- Configure logging.
- Modify an IPS signature.
- Verify IPS.

Background / Scenario

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. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. Set the clock and configure the timestamp service for logging on the routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.

The server and PCs have been preconfigured. The routers have also been preconfigured with the following:

o Enable password: ciscoenpa55
o Console password: ciscoconpa55
o SSH username and password: SSHadmin / ciscosshpa55
o OSPF 101

Part 1: Enable IOS IPS

Step 1: Enable the Security Technology package.

a. On R1, issue the show version command to view the Technology Package license information.
b. If the Security Technology package has not been enabled, use the following command to enable the package.
R1(config)# license boot module c1900 technology-package securityk9
c. Accept the end user license agreement.
d. Save the running-config and reload the router to enable the security license.
e. Verify that the Security Technology package has been enabled by using the show version command.

Step 2: Verify network connectivity.

a. Ping from PC-C to PC-A. The ping should be successful.
b. Ping from PC-A to PC-C. The ping should be successful.

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
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir
```

Step 4: 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
```

Step 5: 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

Step 6: 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.

a. Enable syslog if it is not enabled.

R1(config)# ip ips notify log

b. If necessary, use the clock set command from privileged EXEC mode to reset the clock.

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

c. 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

d. Send log messages to the syslog server at IP address 192.168.1.50.

R1(config)# logging host 192.168.1.50

Step 7: 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>

Step 8: 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

Insert screenshots here

STEP1:

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE
OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING
SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE
FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE
BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

STEP2:

PC C:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=19ms TTL=125
Reply from 192.168.1.2: bytes=32 time=17ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 19ms, Average = 12ms

C:\>
```

PC A:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=5ms TTL=125
Reply from 192.168.3.2: bytes=32 time=13ms TTL=125
Reply from 192.168.3.2: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 8ms

C:\>
```

STEP3:

```
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1#
```

STEP4,5,6,7:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 10:20:00 10 january 2014
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.50
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]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this
engine will be scanned

R1(config)#
```

STEP8:

```
R1(config)#interface g0/1
R1(config-if)#ip ips iosips out
R1(config-if)#
*Jan 10, 10:24:12.2424:  %IPS-6-ENGINE_BUILDS_STARTED:  10:24:12 UTC
Jan 10 2014
*Jan 10, 10:24:12.2424:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3
signatures - 1 of 13 engines
*Jan 10, 10:24:12.2424:  %IPS-6-ENGINE_READY: atomic-ip - build time
8 ms - packets for this engine will be scanned
*Jan 10, 10:24:12.2424:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed
time 8 ms
R1(config-if)#
```

Part 2: Modify the Signature

Step 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>

Step 2: Use show commands to verify IPS.

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

Step 3: Verify that IPS is working properly.

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

The pings should fail. This is because the IPS rule for event-action of an echo request was set to “denypacket-inline”.

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

The ping should be successful. This is because the IPS rule does not cover echo reply. When PC-A pings PC-C, PC-C responds with an echo reply.

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.

Insert screenshots here

```
R1(config-if)#exit
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)#anabled true
                            ^
% Invalid input detected at '^' marker.

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]
%IPS-6-ENGINE_BUILDS_STARTED:
```

```
R1(config)#do show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled
```

STEP3:

PC C:

```
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),

C:\>
```

PC A:

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=7ms TTL=125
Reply from 192.168.3.2: bytes=32 time=16ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=18ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 18ms, Average = 13ms

C:\>
```

STEP 4: