CSE 3502

INFORMATION SECURITY MANAGEMENT

Lab Assessment – 3

L19+L20 | SJT516
Dr. Lavanya K

WINTER SEMESTER 2021-22

by

SHARADINDU ADHIKARI
19BCE2105

Exp 3. IPS Configuration

Introduction to IPS

IPS, the abbreviation for Intrusion Prevention System, is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to our configuration. System supports license-controlled IPS, i.e., the IPS function will not work unless an IPS license has been installed on the security device that supports IPS.

IPS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, system will update the signature database automatically everyday to assure its integrity and accuracy.

The Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based Intrusion-Prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

Objectives

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

Scenario

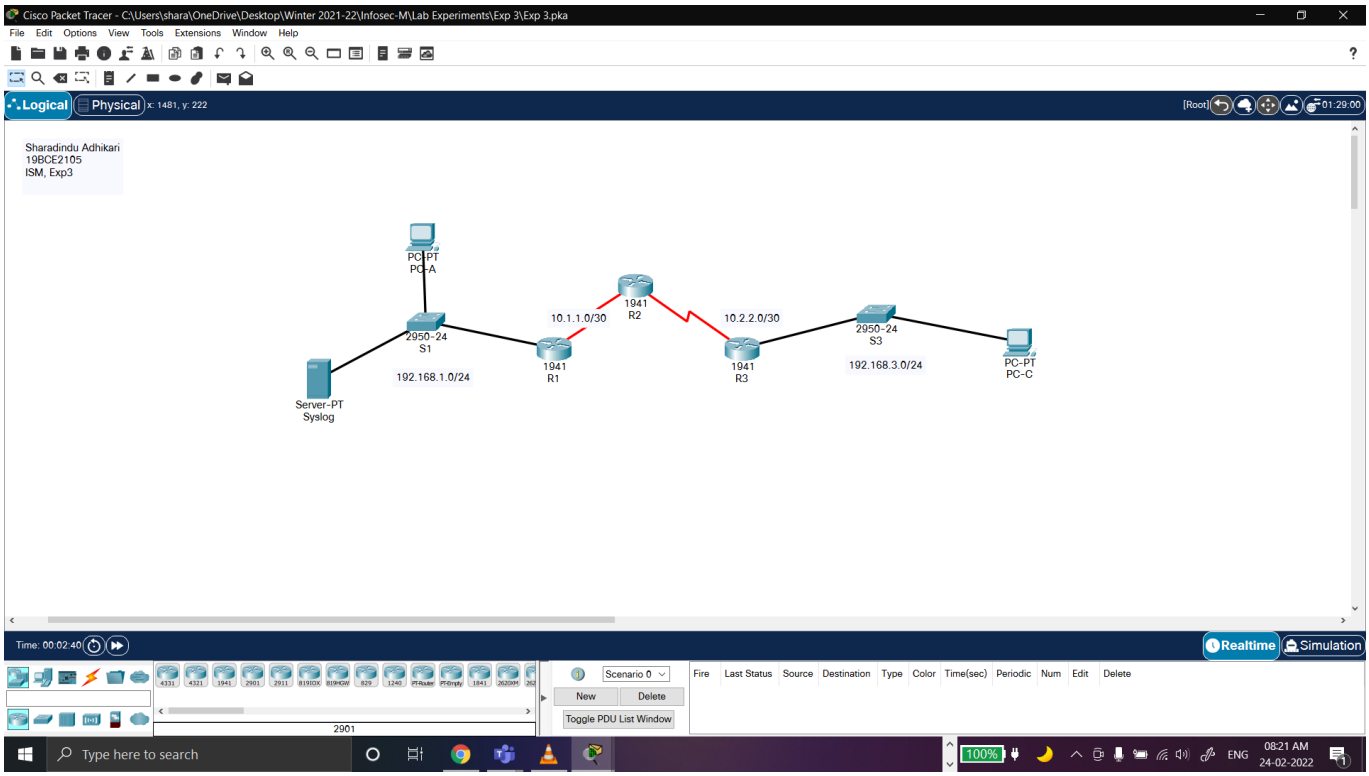
My task is to enable IPS on R1 to scan traffic entering the 192.168.1.0 network. The server labelled Syslog is used to log IPS messages. I've to configure the router to identify the syslog server to receive logging messages. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. I also have to set the clock and configure the timestamp service for logging on the routers. Finally, I also need to enable the IPS to produce an alert and drop ICMP echo reply packets inline.

Components

Component/ Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

Routers: Cisco 1941 Integrated Services Router. 3 in number.
Switches: WS-C2950-24 switch, 24 port, 10/100 auto-sensing and auto-negotiating. 2 in number.
PCs: Regular PC-PTs. 2 in number.
Server: Syslog Server-PT. Only 1.

Topology Diagram



PART 1: Enabling the IOS Intrusion Prevention System Using CLI

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 thepackage.

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

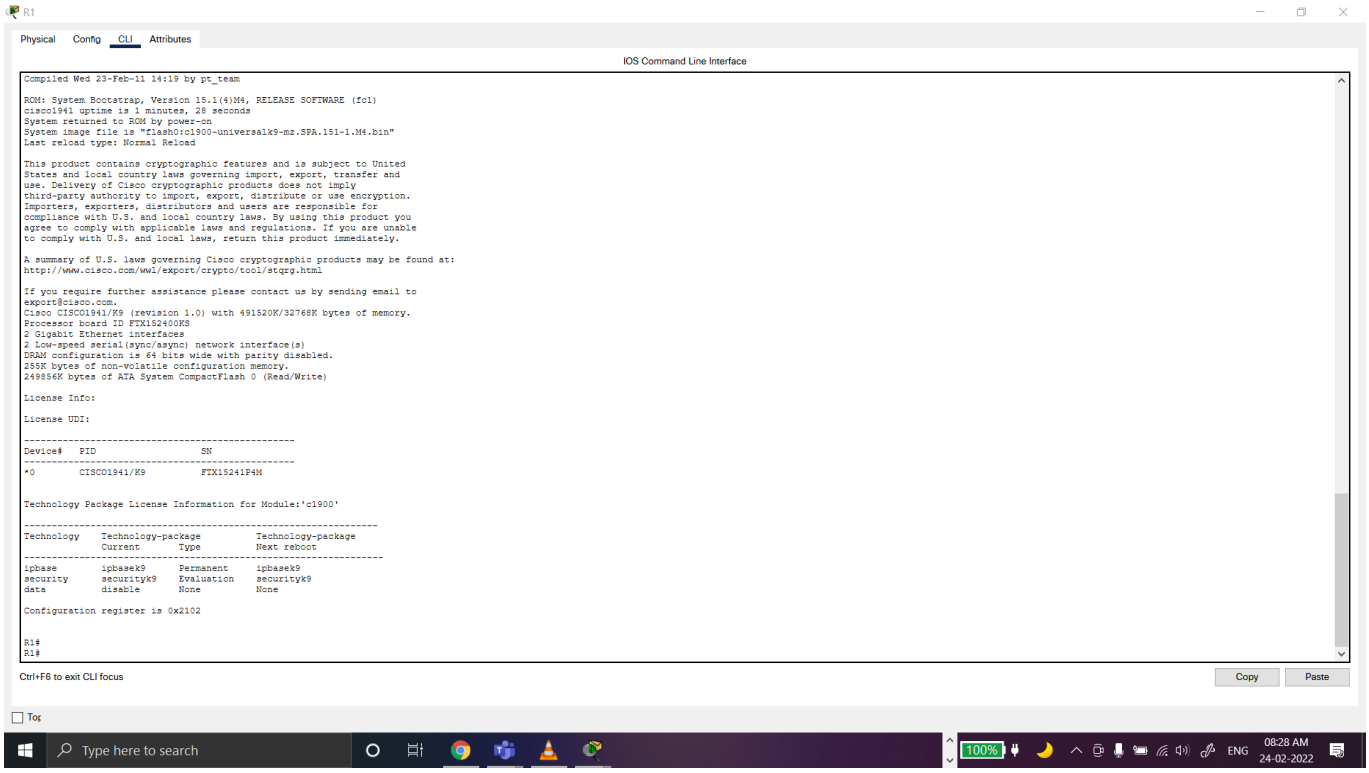
c. Accept the end user license agreement.

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.

```
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9

R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 KBytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
####################################################################### [OK]
Smart Init is enabled
smart init is sizing iomem
                TYPE     MEMORY_REQ
```

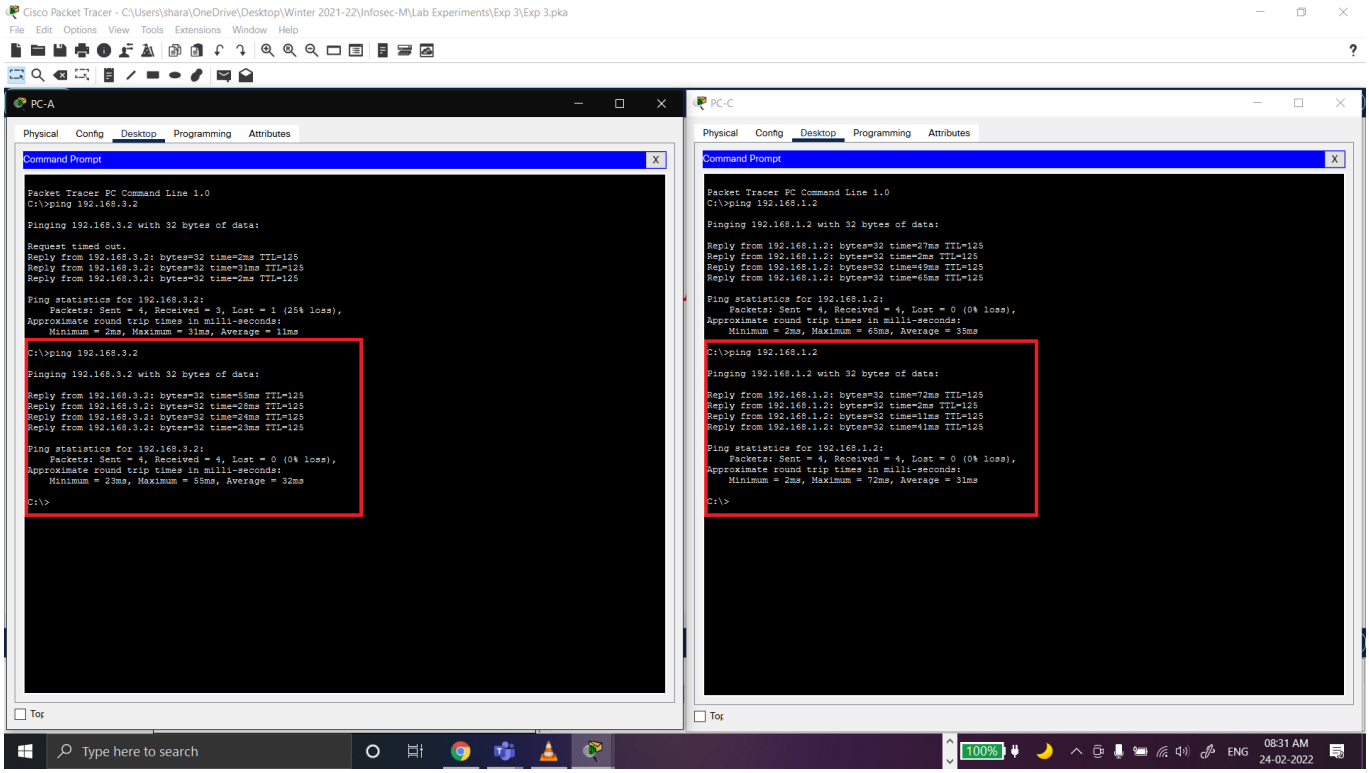
```
R1
Physical   Config   CLI   Attributes
                    IOS Command Line Interface

User Access Verification

Password:
00:00:20: %OSPF-5-ADJCHG: Process 101, Nbr 10.2.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done

Password:

R1>en
Password:
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 17 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 28 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

Ctrl+F6 to exit CLI focus                                   Copy   Paste
Top
Type here to search                 100%  ENG  08:27 AM  24-02-2022
```



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 I 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. Namethe 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. Iflogging 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 8:40:59 24 February 2022
```

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.

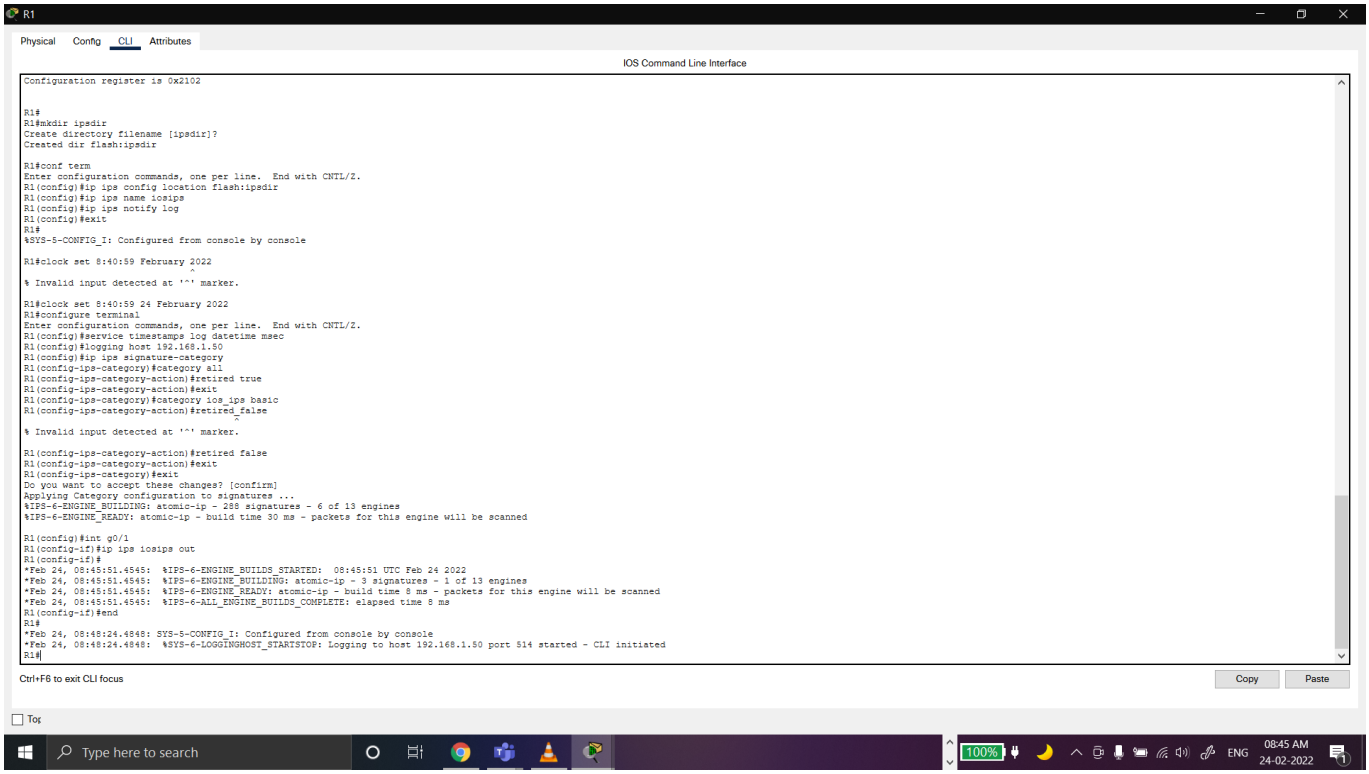
```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-cateogry)# 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 enabling the IPS, some log messages will be sent tothe 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 thatIPS inspects only traffic going out of the interface.

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



PART 2: Modifying the Signature

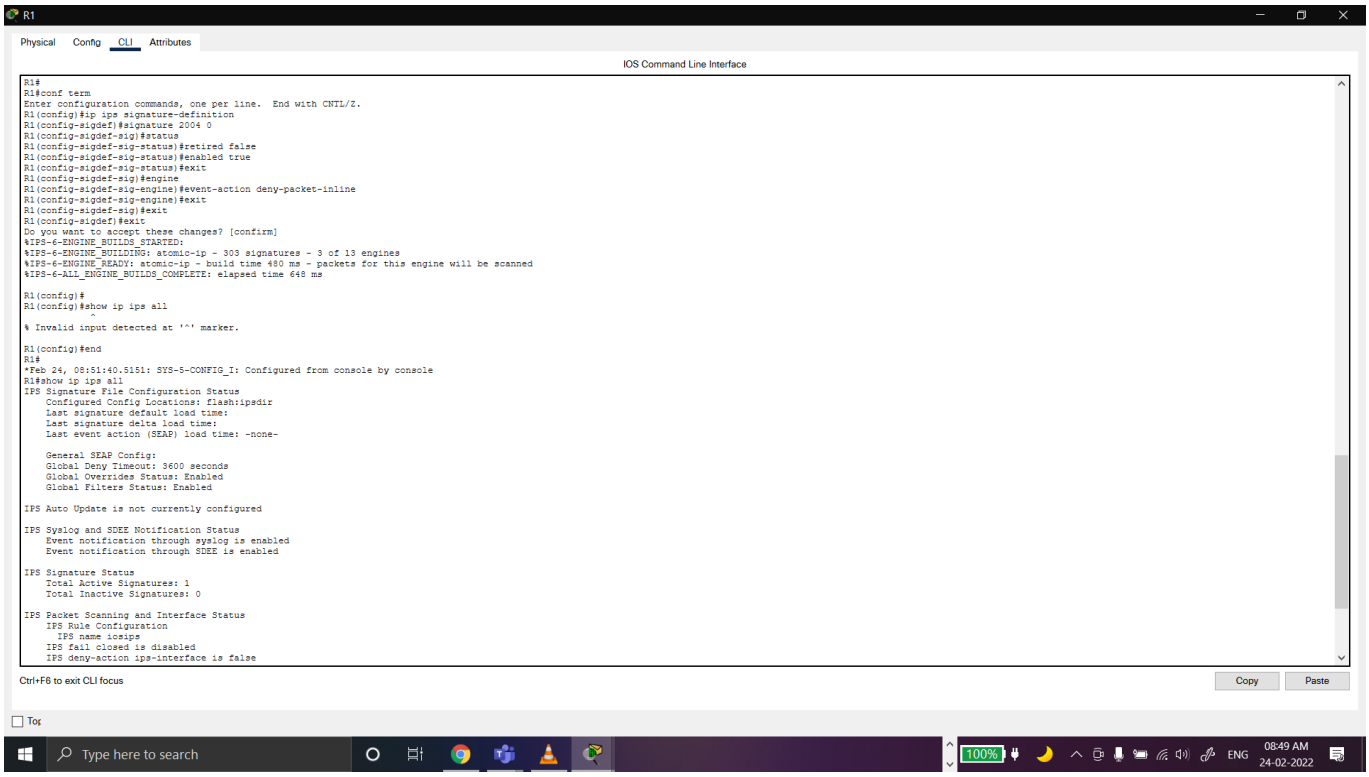
Step 1: Change the event-action of a signature.

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature actionto 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.



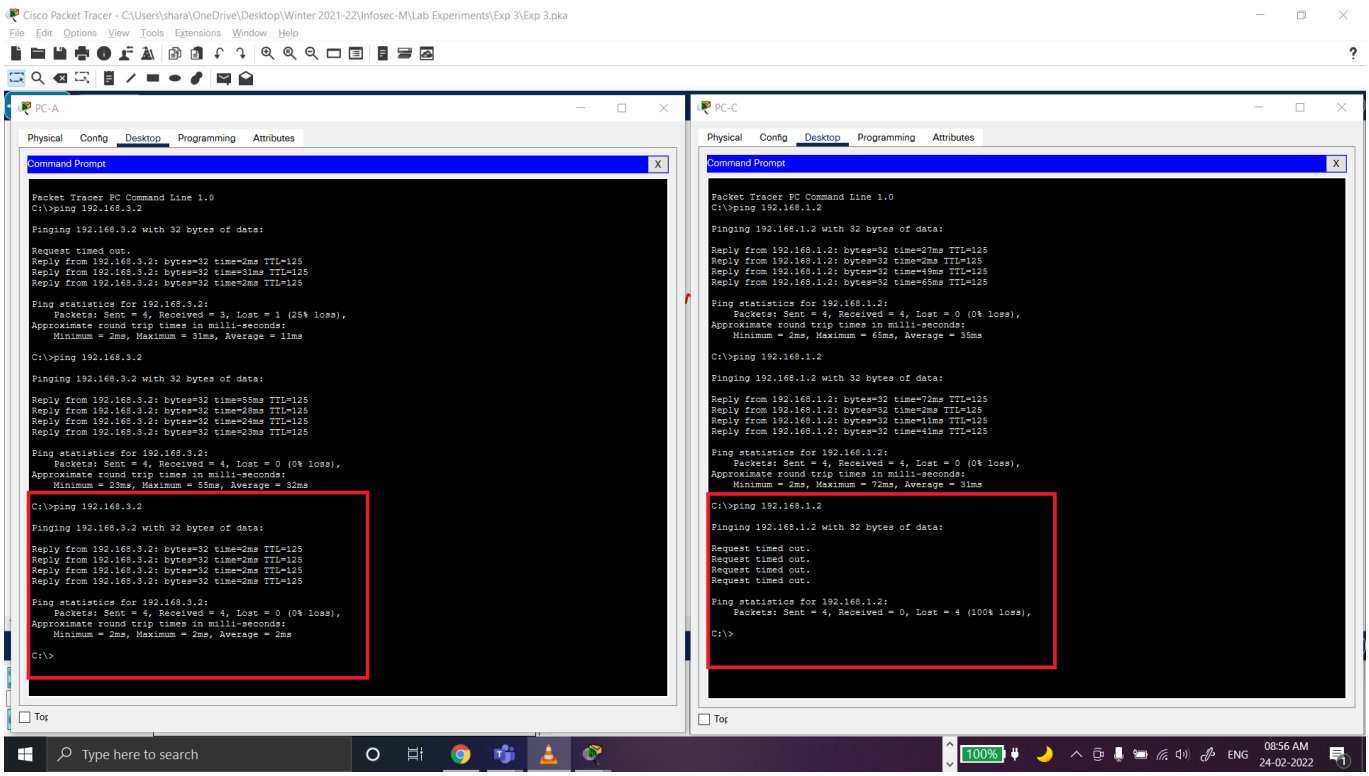
Step 3: Verify that IPS is working properly.

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

   The pings failed. This is because the IPS rule for event-action of an echo request was set to “deny- packet-inline”.

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

   The ping was 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.

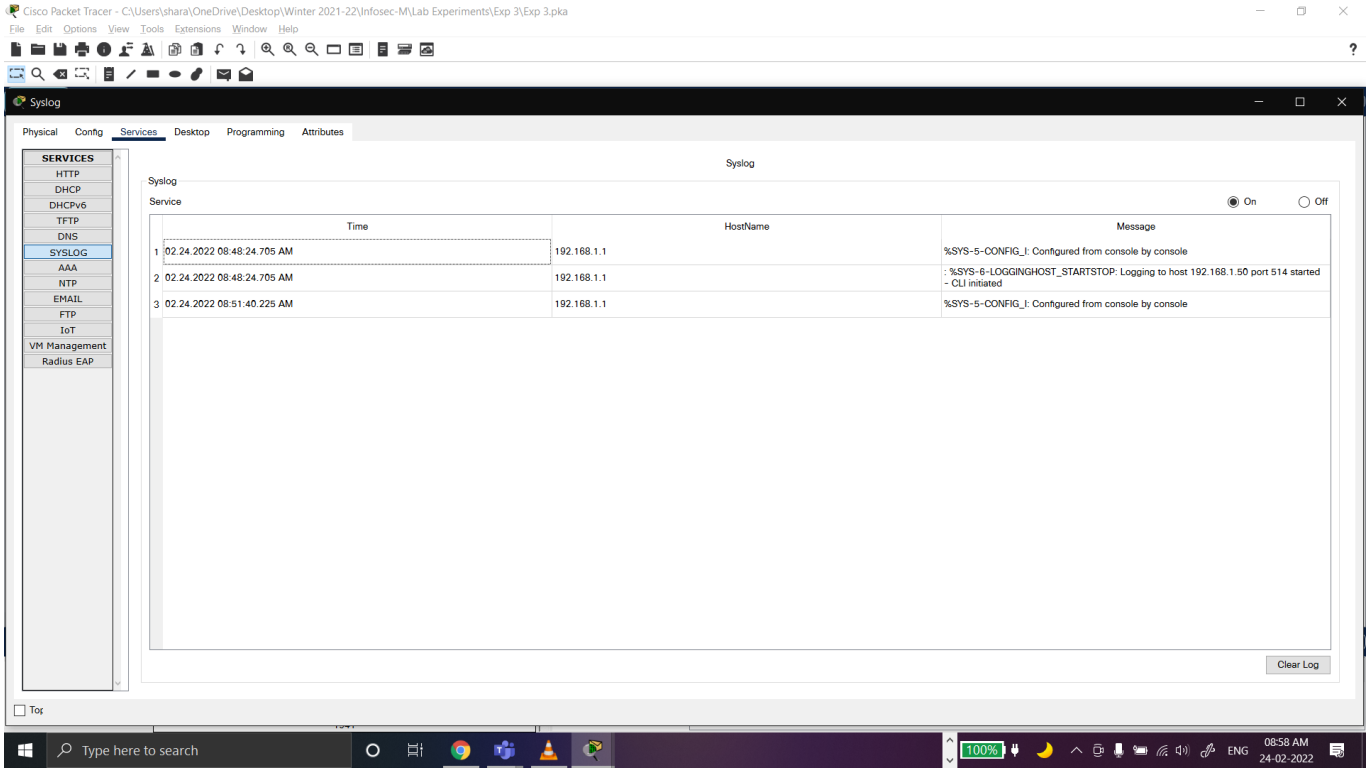


Step 4: View the syslog messages.

a. Click the **Syslog** server.

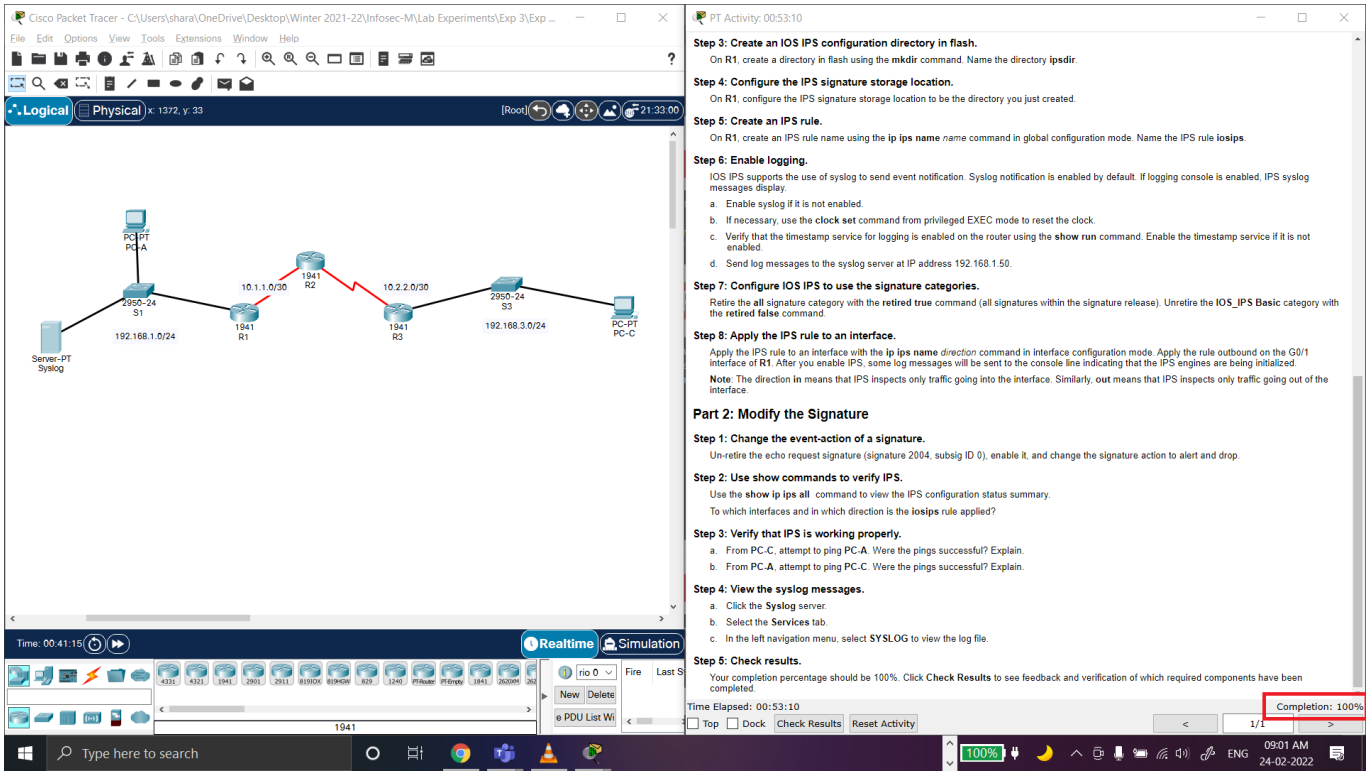
b. Select the **Services** tab.

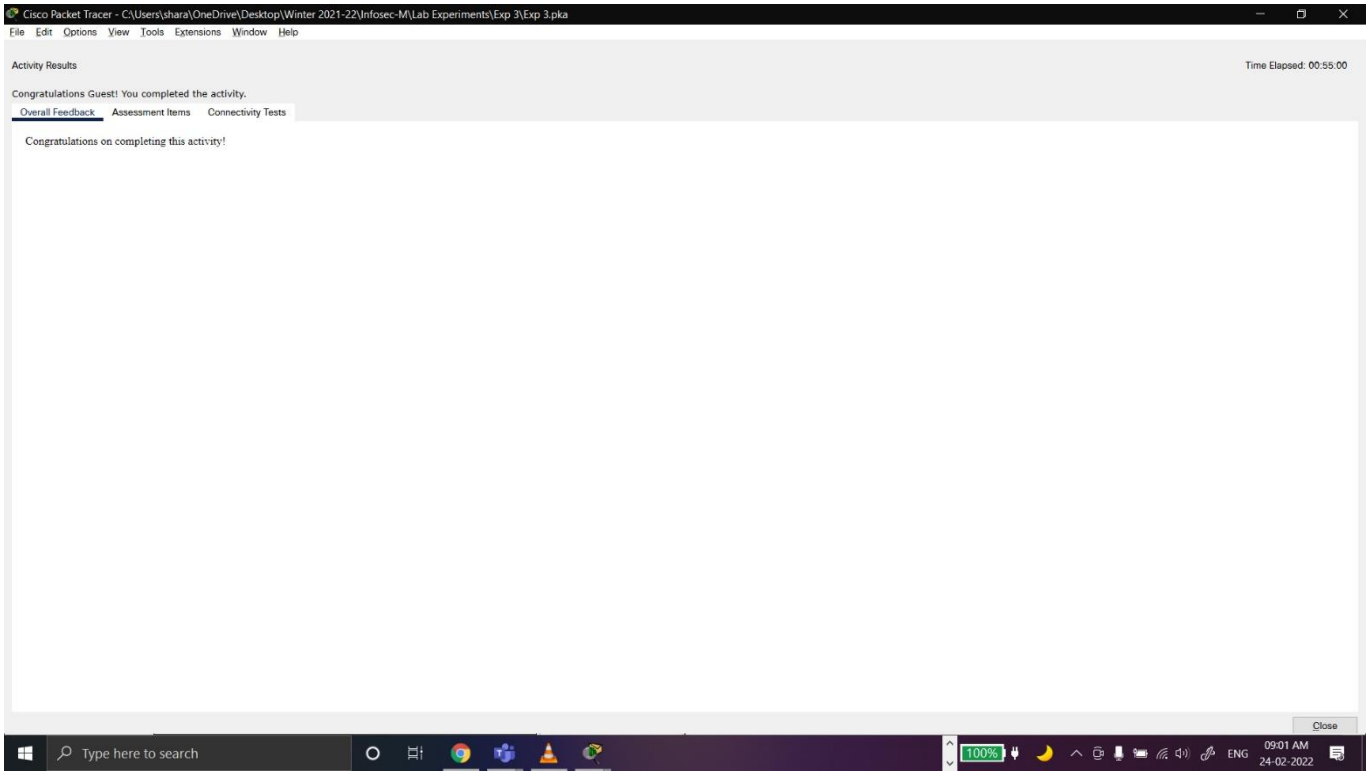
c. In the left navigation menu, select **SYSLOG** to view the log file.

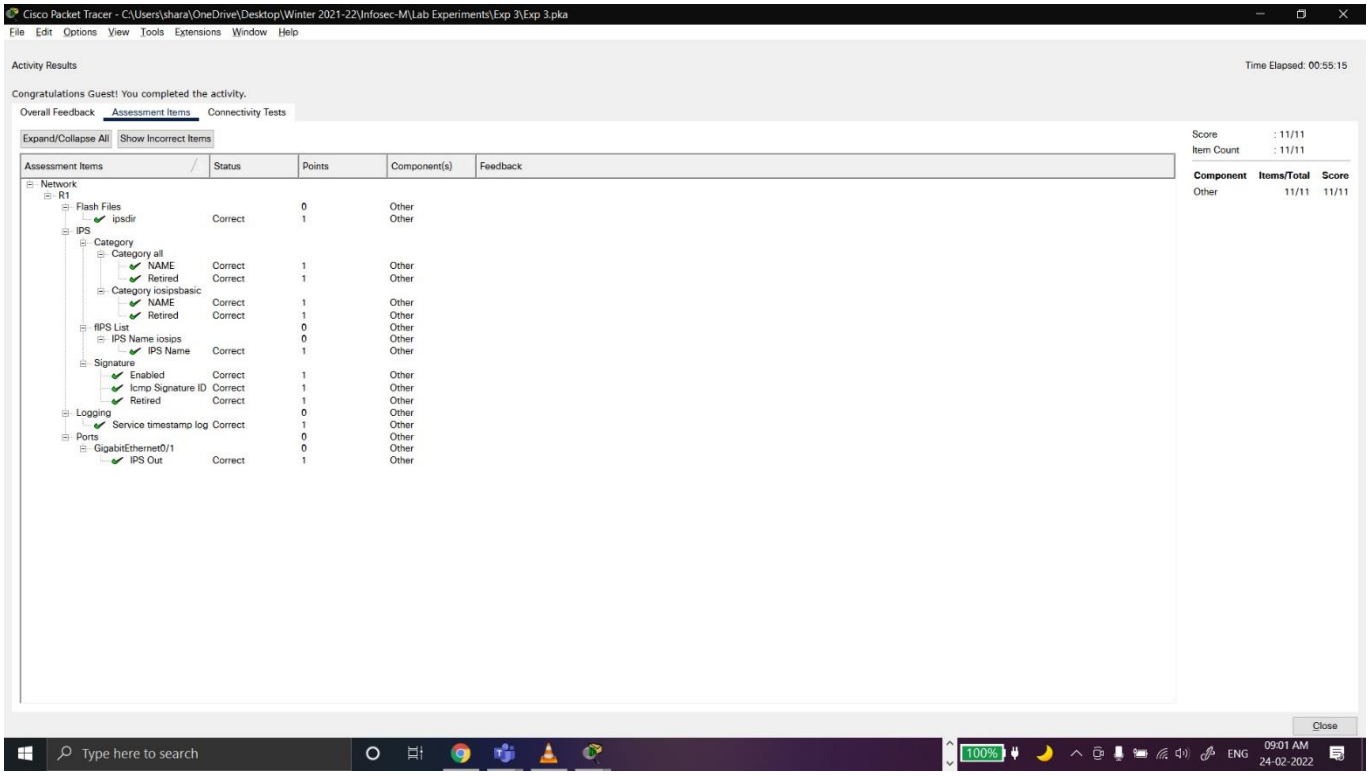


Step 5: Check results.

Completion percentage should be 100%.






Cisco Packet Tracer - C:\Users\shara\OneDrive\Desktop\Winter 2021-22\Infosec-M\Lab Experiments\Exp 3\Exp 3.pka
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:55:15
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Component(s)
Feedback
Network
R1
Flash Files 0 Other
ipsdir Correct 1 Other
IPS
Category
Category all
NAME Correct 1 Other
Retired Correct 1 Other
Category iosipsbasic
NAME Correct 1 Other
Retired Correct 1 Other
IPS List 0 Other
IPS Name iosips 0 Other
IPS Name Correct 1 Other
Signature
Enabled Correct 1 Other
Icmp Signature ID Correct 1 Other
Retired Correct 1 Other
Logging 0 Other
Service timestamp log Correct 1 Other
Ports 0 Other
GigabitEthernet0/1 0 Other
IPS Out Correct 1 Other
Score : 11/11
Item Count : 11/11
Component Items/Total Score
Other 11/11 11/11
Close
Type here to search
100%
ENG
09:01 AM
24-02-2022