VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE 3502

Information Security Management

Winter Semester 2022-23

Lab Report – 4

Configuration of IOS Intrusion Prevention System (IPS)

Name:Aditya Krishna

Reg No.:20BCE0456

Guided by: Prof. Lavanya K

24th Feb, 2023

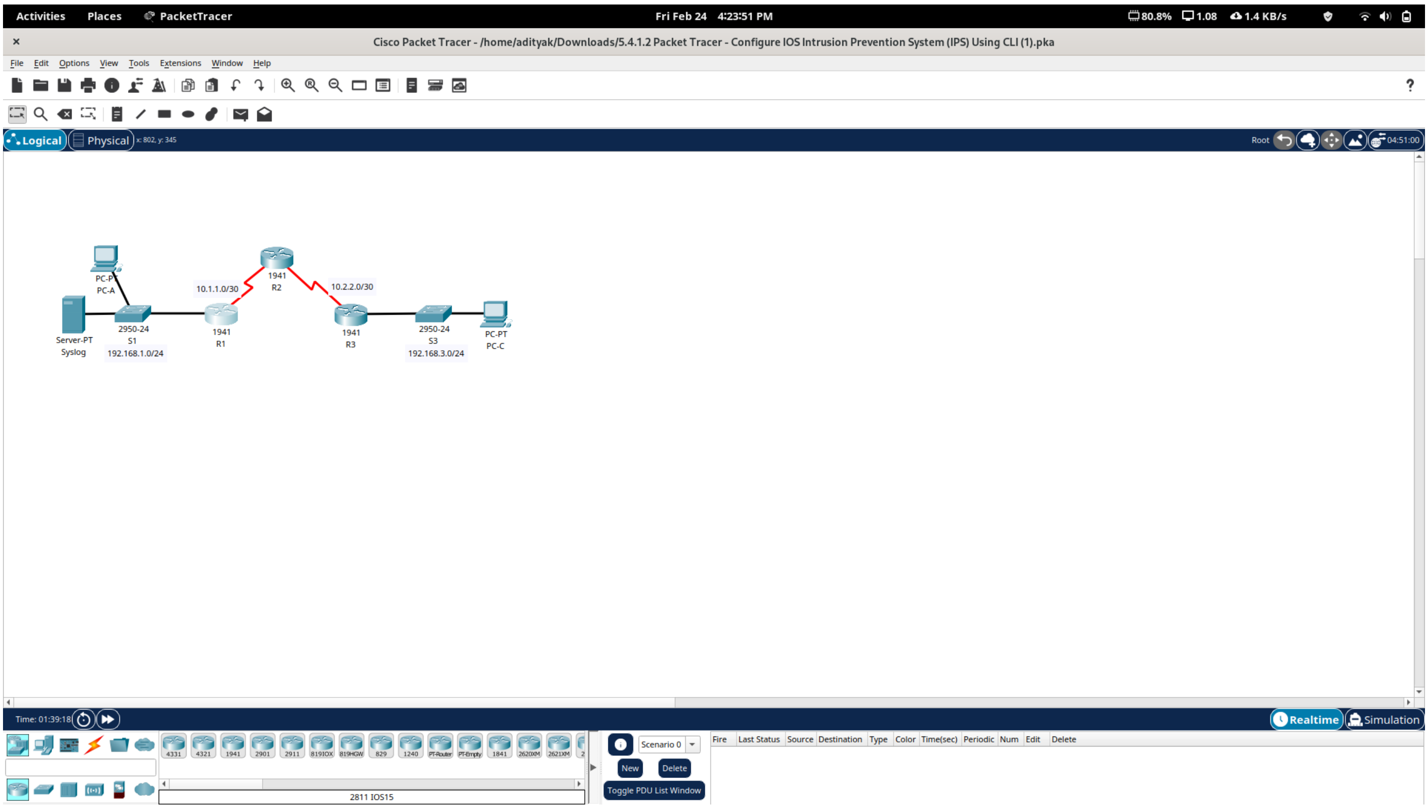
Introduction :

An IOS Intrusion Prevention System (IOS IPS) is a security technology designed to detect and prevent various types of network attacks, including network-based and application-based attacks, from penetrating and exploiting vulnerabilities in a network. It is implemented as a software module within the Cisco IOS software running on routers and switches. The IOS IPS performs real-time traffic analysis of network traffic passing through the device, compares it against predefined attack signatures, and takes action to block the traffic that matches these signatures.The IPS can operate in inline mode, where it actively blocks suspicious traffic, or in promiscuous mode, where it only monitors traffic and sends alerts to the network administrator for further analysis. By proactively identifying and blocking potential threats, an IOS IPS helps to improve the overall security posture of a network and minimize the risk of security breaches

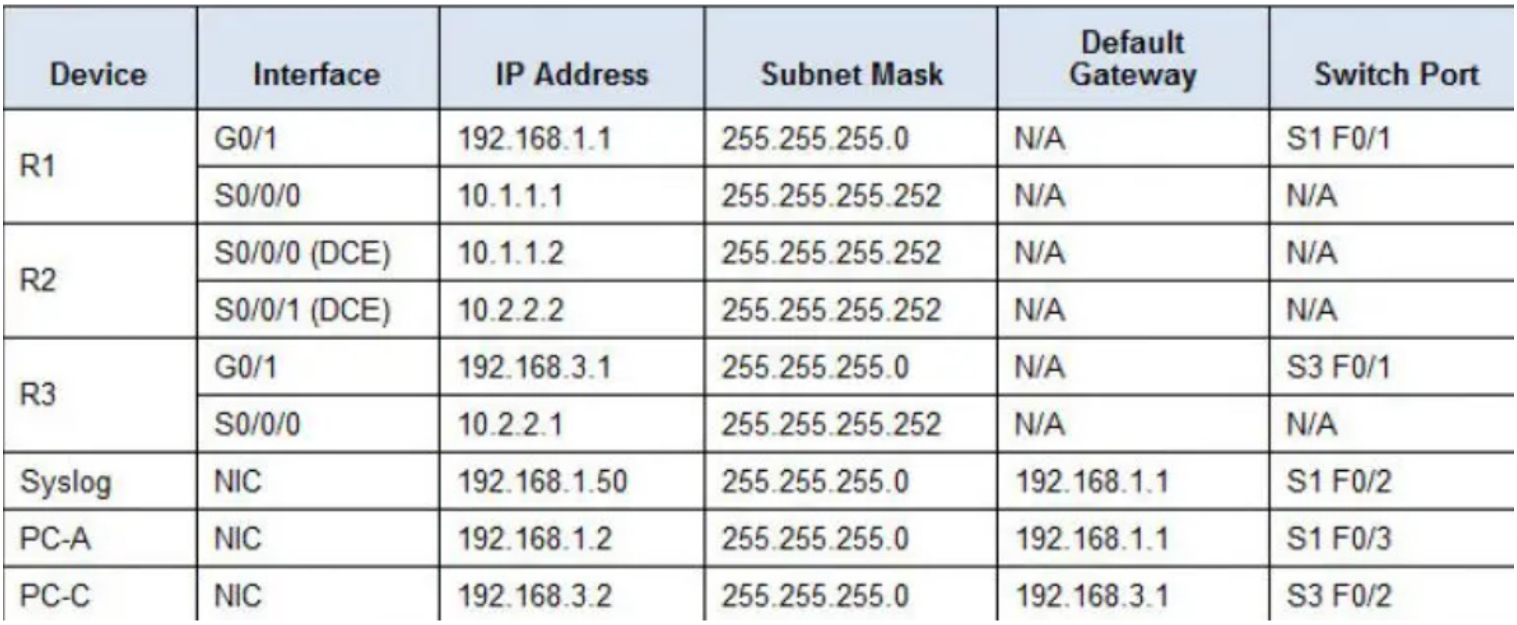
Objectives/AIM

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

Step 0: Make the topology



IP Addressing Table



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

Assign IP's respectively & enable the connections.

Part 1: Enable IOS IPS

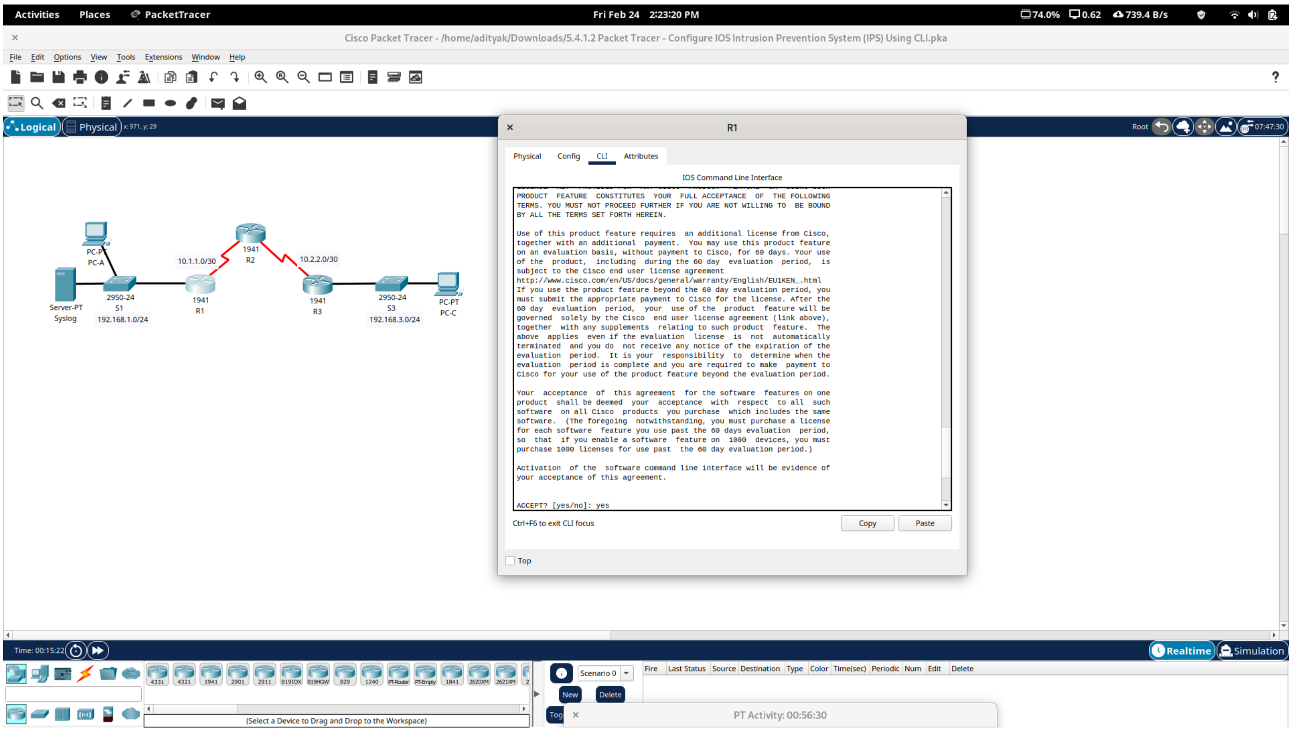
Step 1: Enable the Security Technology package.

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
```

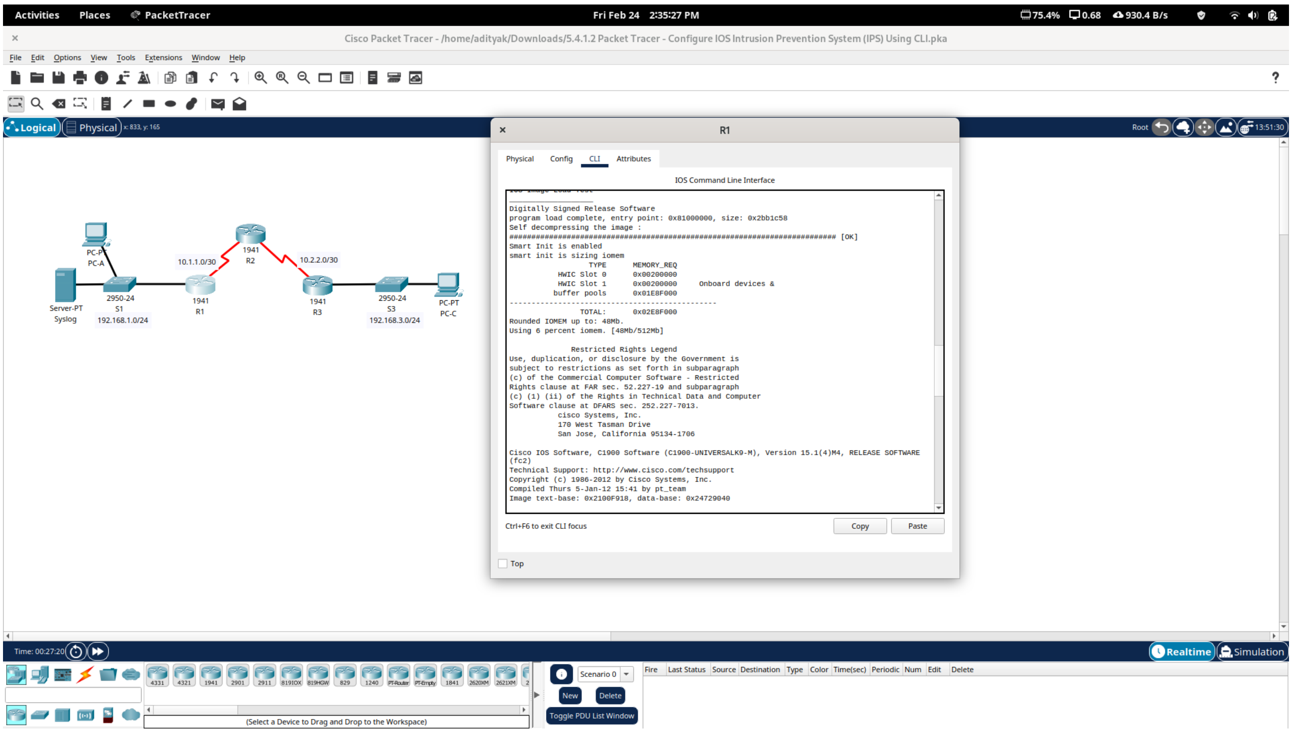
c. Accept the end user license agreement.



```
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.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
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
```

d.Save the running-config and reload the router to enable the security license.

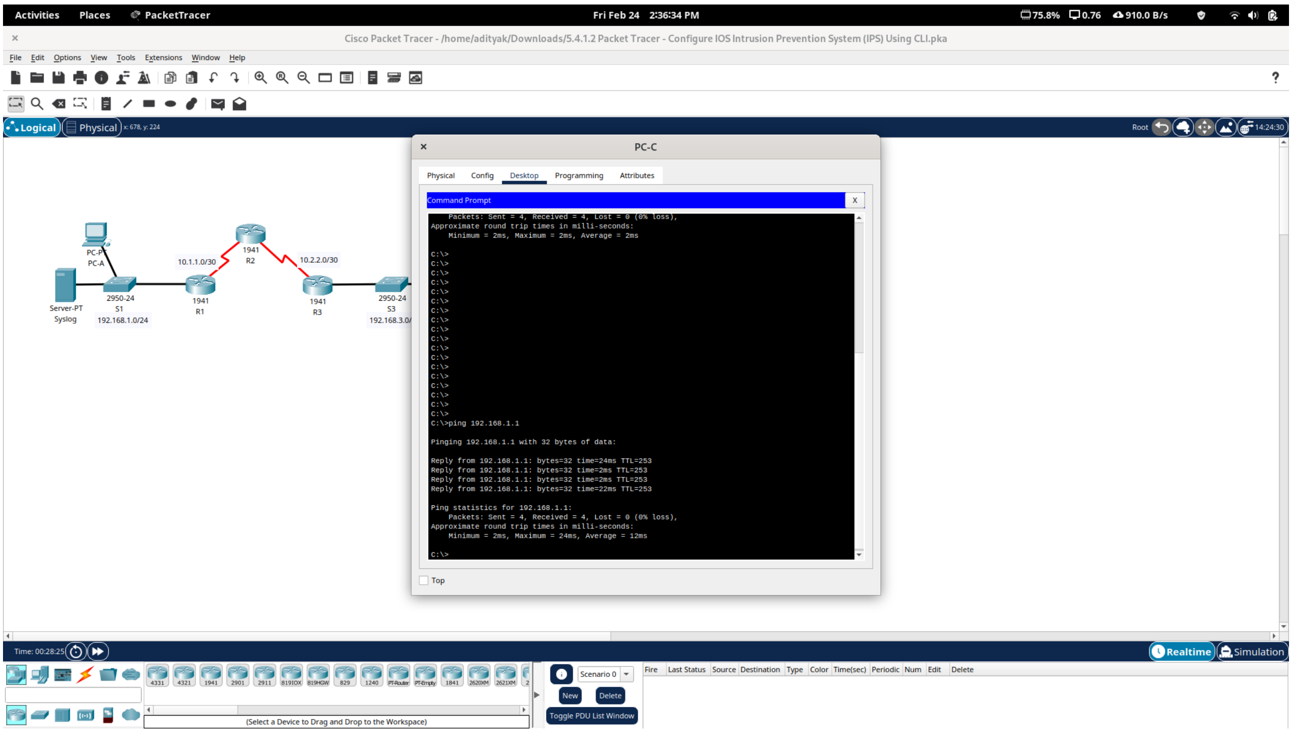
e.Verify that the Security Technology package has been enabled by using the **show version** command.



```
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
           HWIC Slot 0      0x00200000
           HWIC Slot 1      0x00200000     Onboard devices &
          buffer pools      0x01E8F000
-----------------------------------------------
                TOTAL:      0x02E8F000
Rounded IOMEM up to: 48Mb.
Using 6 percent iomem. [48Mb/512Mb]

              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

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) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040
```

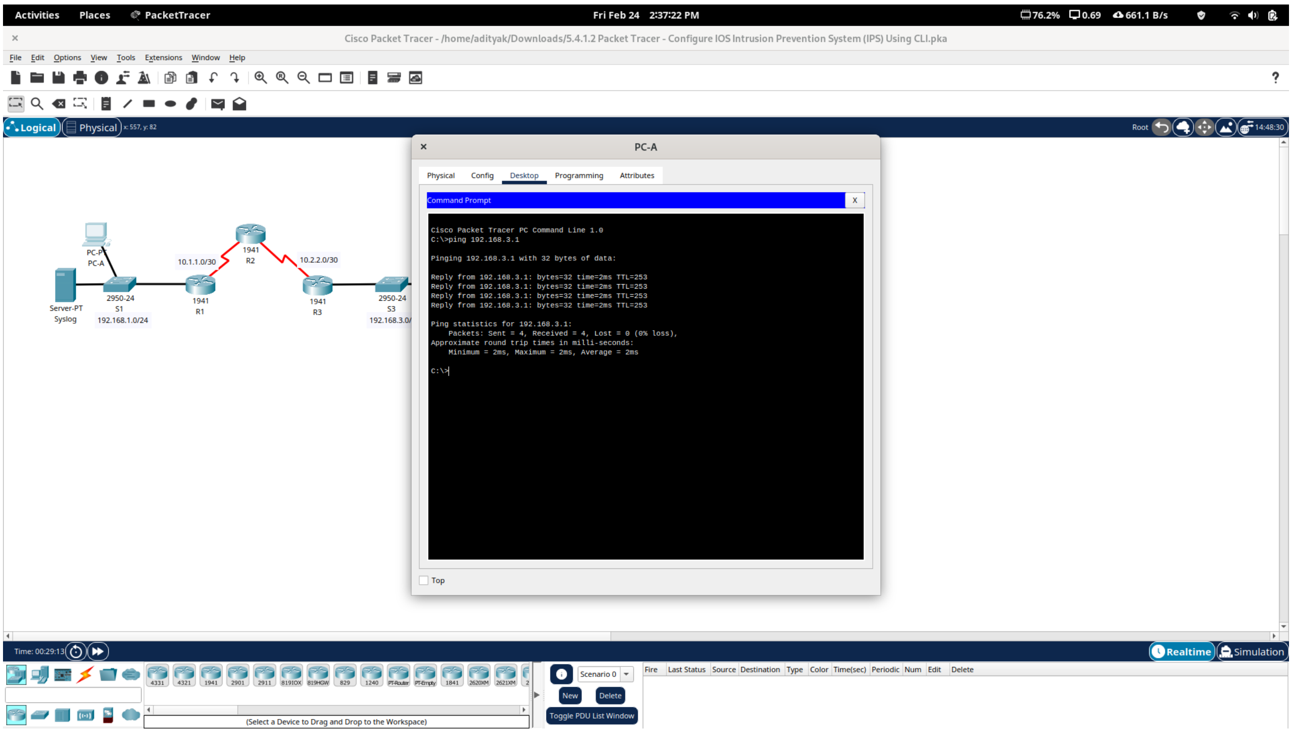
Step 2: Verify network connectivity.

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



```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=24ms TTL=253
Reply from 192.168.1.1: bytes=32 time=2ms TTL=253
Reply from 192.168.1.1: bytes=32 time=2ms TTL=253
Reply from 192.168.1.1: bytes=32 time=22ms TTL=253

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 24ms, Average = 12ms

C:\>
```

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

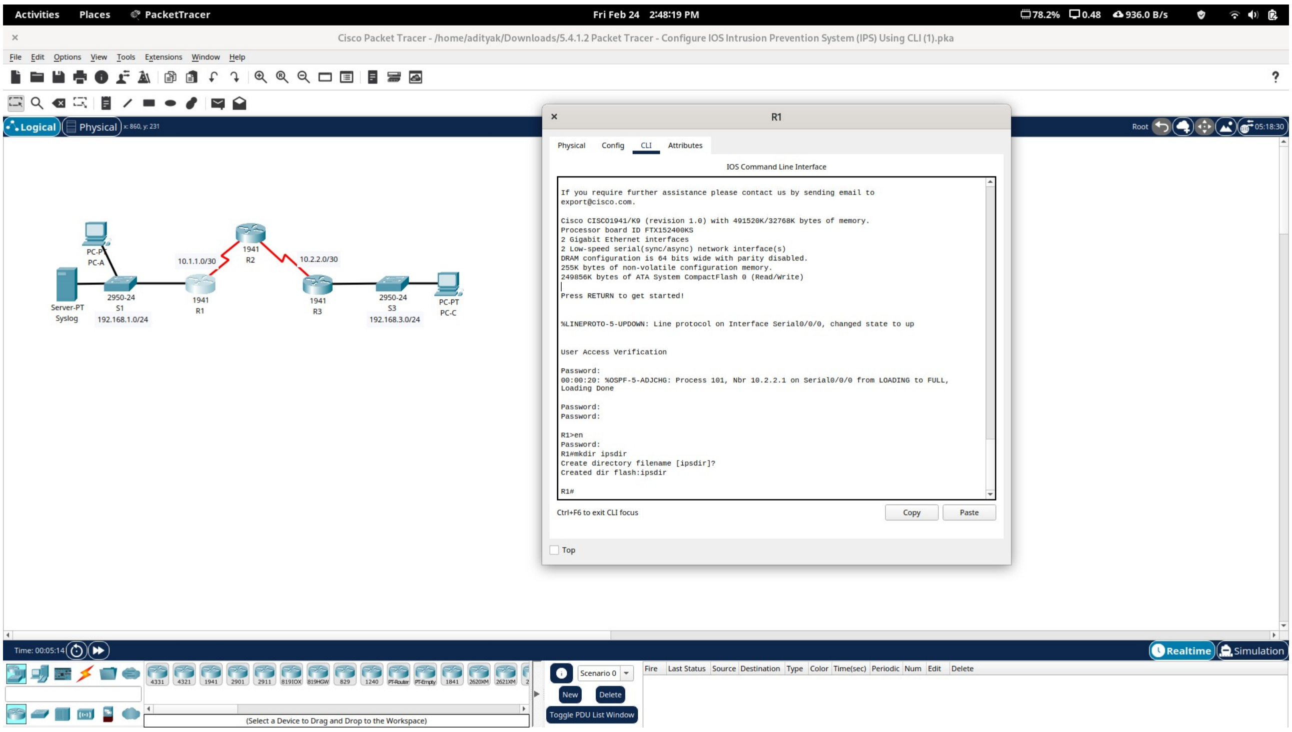


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
```

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



Activities
Places
PacketTracer
Fri Feb 24 2:48:19 PM
Cisco Packet Tracer - /home/adityak/Downloads/5.4.1.2 Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI (1).pka
File Edit Options View Tools Extensions Window Help
Logical
Physical
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
PC-PT
PC-A
Server-PT
Syslog
2950-24
S1
192.168.1.0/24
1941
R1
10.1.1.0/30
1941
R2
10.2.2.0/30
1941
R3
2950-24
S3
192.168.3.0/24
PC-PT
PC-C
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)

```
If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


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:
Password:

R1>en
Password:
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1#
```

Step 4: Configure the IPS signature storage location.

On **R1**, configure the IPS signature storage location to be the directory you just created.

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**.

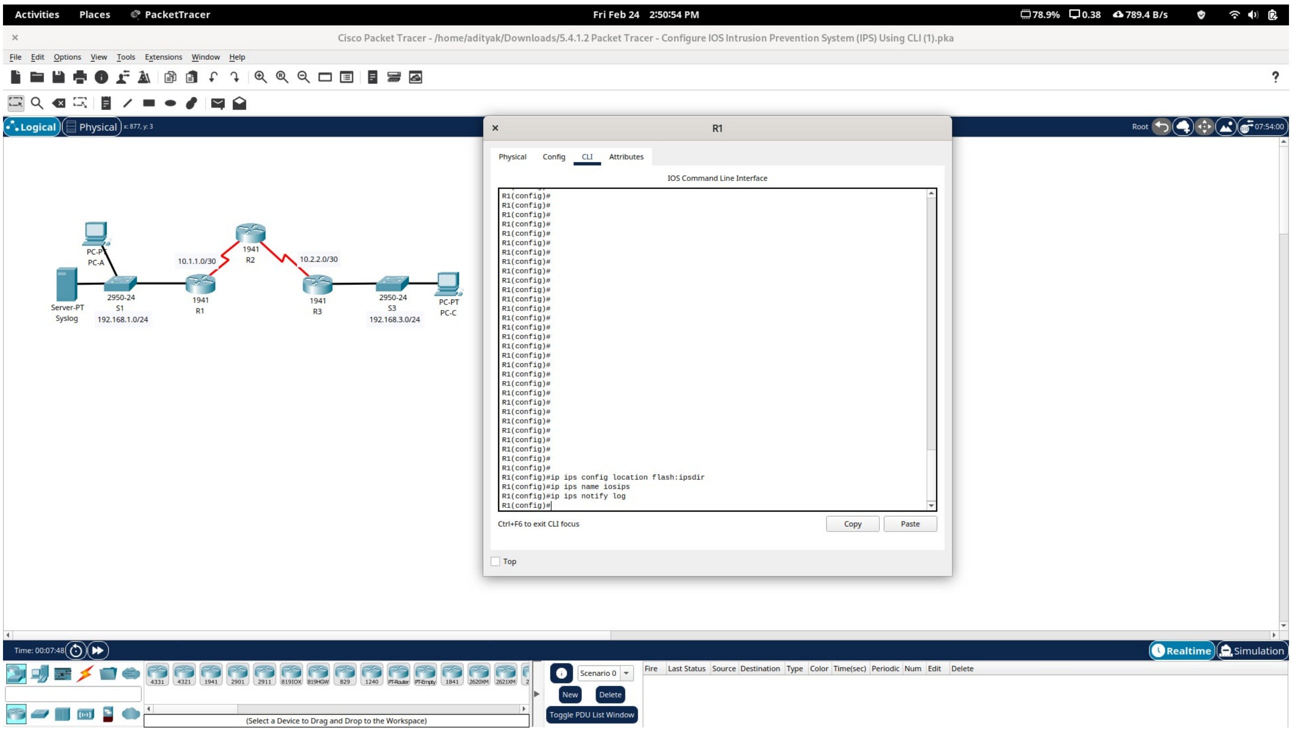
ip ips name iosips

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

`ip ips notify log`



```
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#
```

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

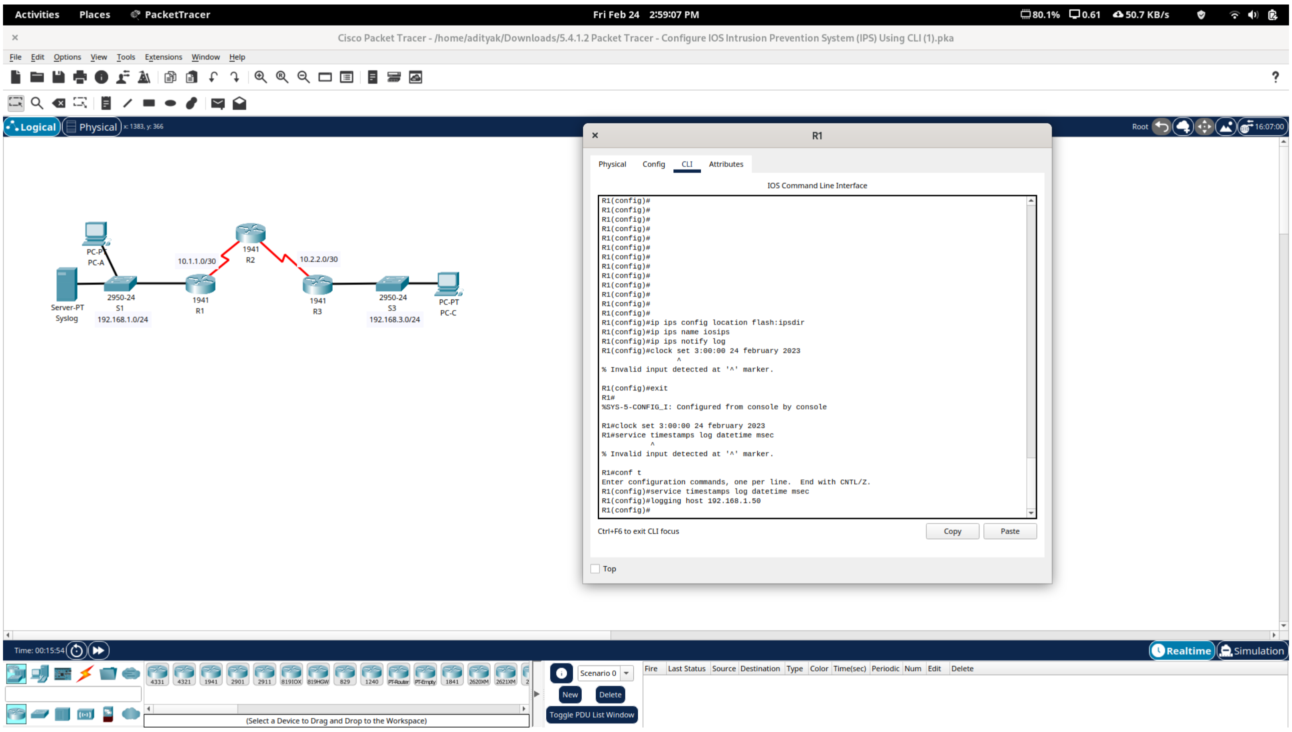
R1# clock set 10:20:00 10 january 2014

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

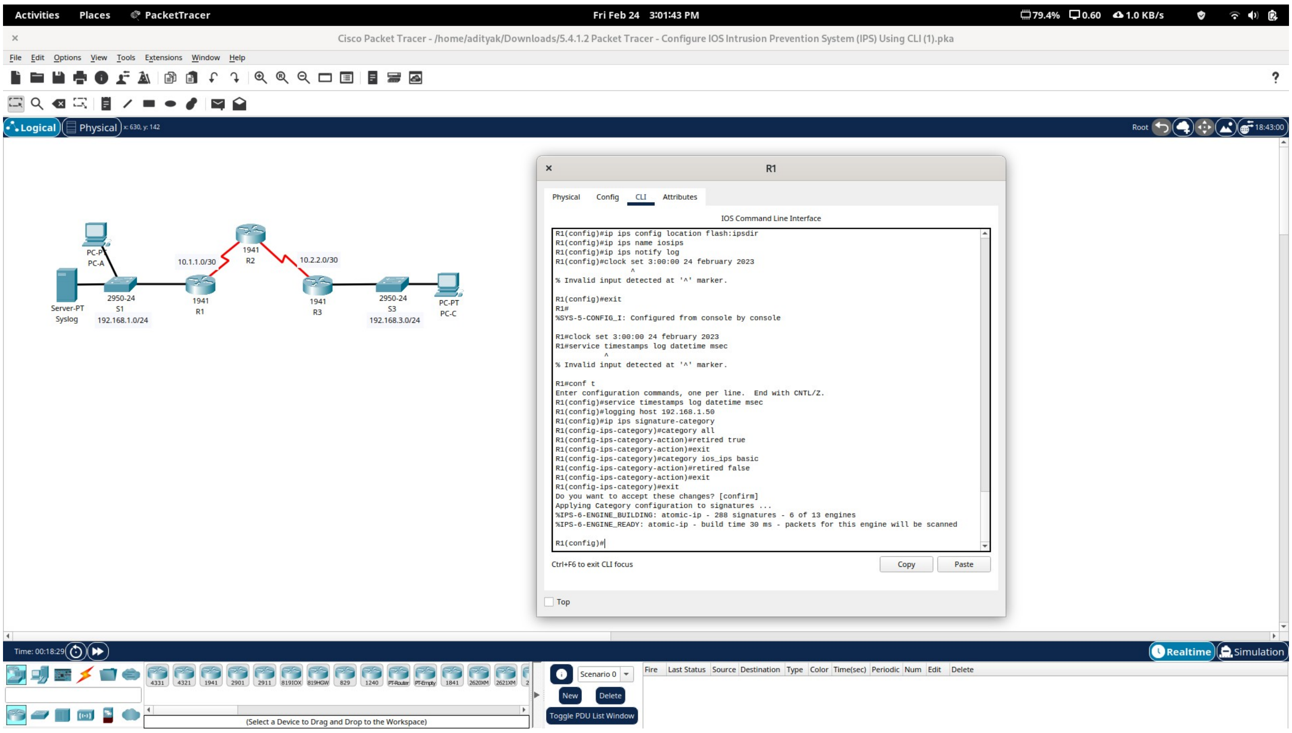


```
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#clock set 3:00:00 24 february 2023
                 ^
% Invalid input detected at '^' marker.

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

R1#clock set 3:00:00 24 february 2023
R1#service timestamps log datetime msec
           ^
% Invalid input detected at '^' marker.

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)#
```

Step 7: Configure IOS IPS to use the signature categories.

Retire the **all** signature category with the **retired true** command. Unretire the **IOS_IPS Basic** category with the **retired false** command.

```
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>
```


Activities Places PacketTracer
Fri Feb 24 3:01:43 PM
Cisco Packet Tracer - /home/adityak/Downloads/5.4.1.2 Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI (1).pka
File Edit Options View Tools Extensions Window Help
Logical
Physical
PC-PT PC-A
Server-PT Syslog
2950-24 S1
192.168.1.0/24
10.1.1.0/30
1941 R1
1941 R2
10.2.2.0/30
1941 R3
2950-24 S3
192.168.3.0/24
PC-PT PC-C
R1
Physical Config CLI Attributes
IOS Command Line Interface
Ctrl+F6 to exit CLI focus
Copy Paste
Top
Time: 00:18:29
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)

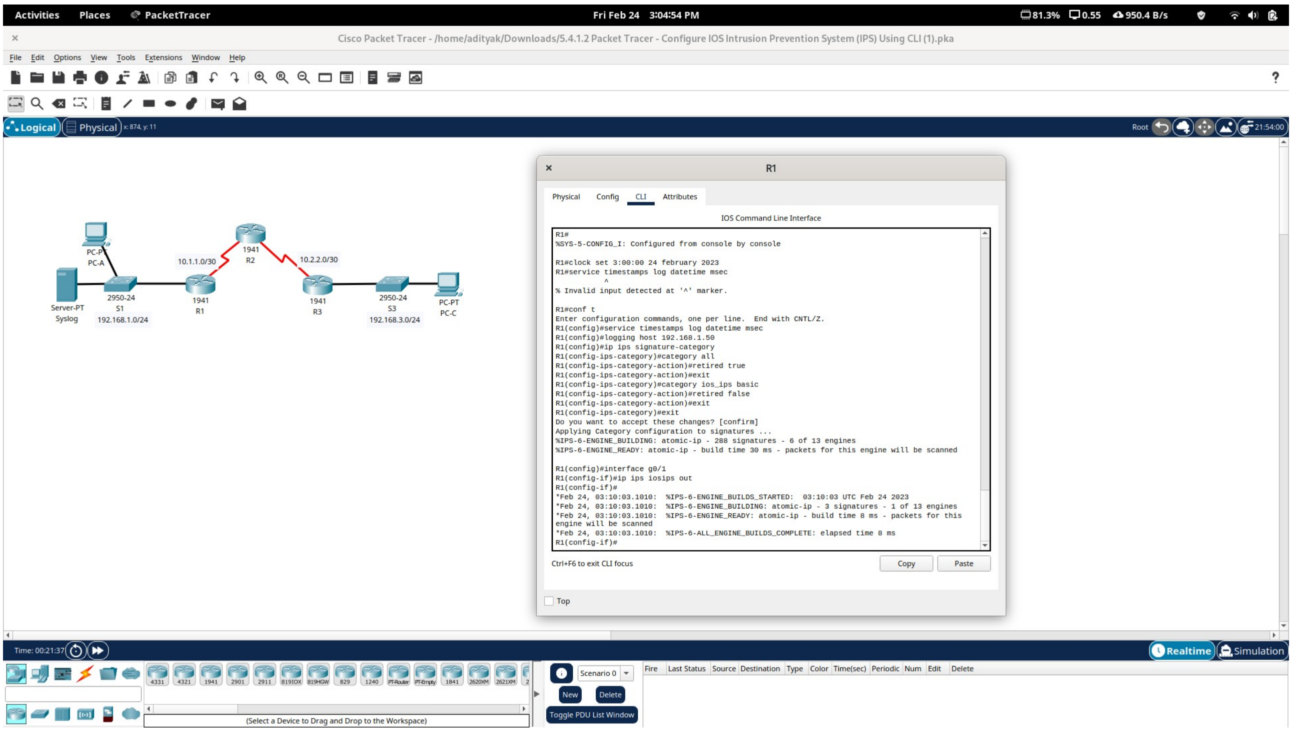
```
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#clock set 3:00:00 24 february 2023
                  ^
% Invalid input detected at '^' marker.

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

R1#clock set 3:00:00 24 february 2023
R1#service timestamps log datetime msec
            ^
% Invalid input detected at '^' marker.

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)#
```

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.

R1(config)#interface g0/1

R1(config-if)#ip ips iosips out


Activities Places PacketTracer
Fri Feb 24 3:04:54 PM
Cisco Packet Tracer - /home/adityak/Downloads/5.4.1.2 Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI (1).pka
File Edit Options View Tools Extensions Window Help
Logical
Physical
PC-PT PC-A
Server-PT Syslog
2950-24 S1
192.168.1.0/24
10.1.1.0/30
1941 R1
1941 R2
10.2.2.0/30
1941 R3
2950-24 S3
192.168.3.0/24
PC-PT PC-C
R1
Physical Config CLI Attributes
IOS Command Line Interface
Ctrl+F6 to exit CLI focus
Copy Paste
Top
Time: 00:21:37
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)

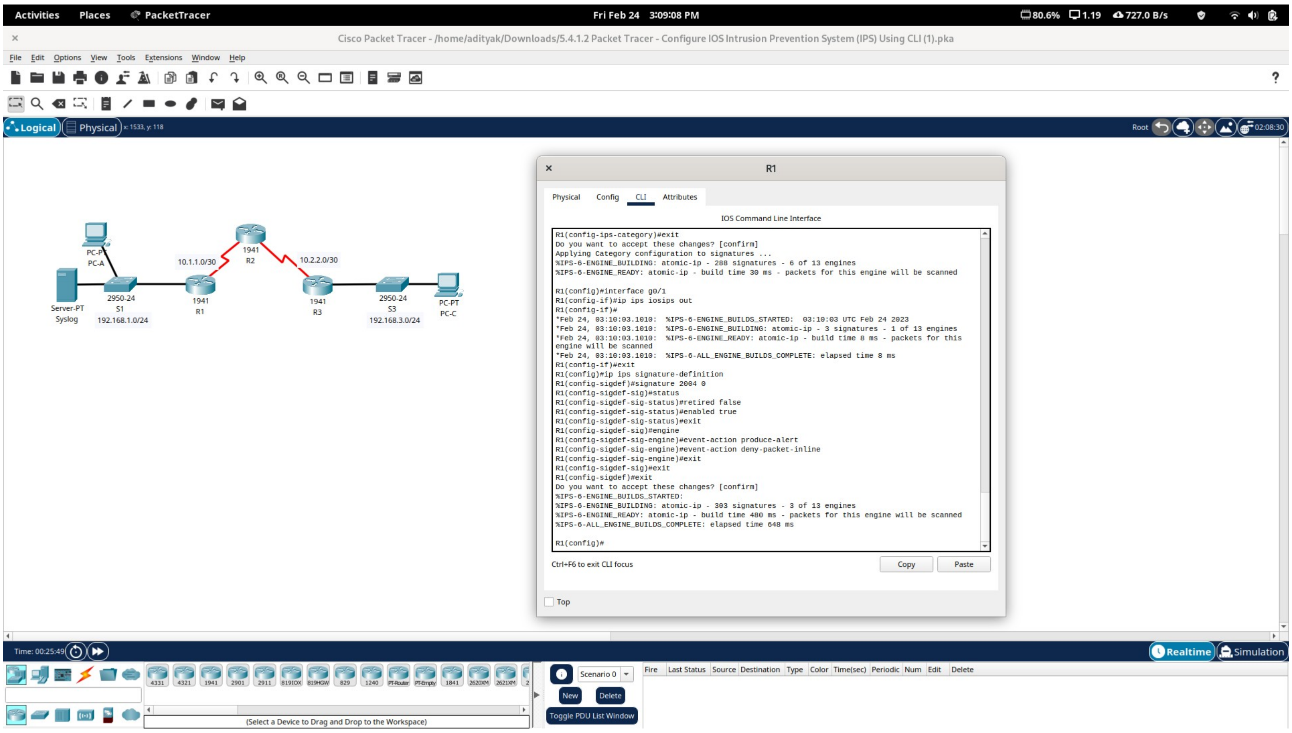
```
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 3:00:00 24 february 2023
R1#service timestamps log datetime msec
            ^
% Invalid input detected at '^' marker.

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)#interface g0/1
R1(config-if)#ip ips iosips out
R1(config-if)#
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_BUILDS_STARTED:  03:10:03 UTC Feb 24 2023
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this
engine will be scanned
*Feb 24, 03:10:03.1010:  %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.

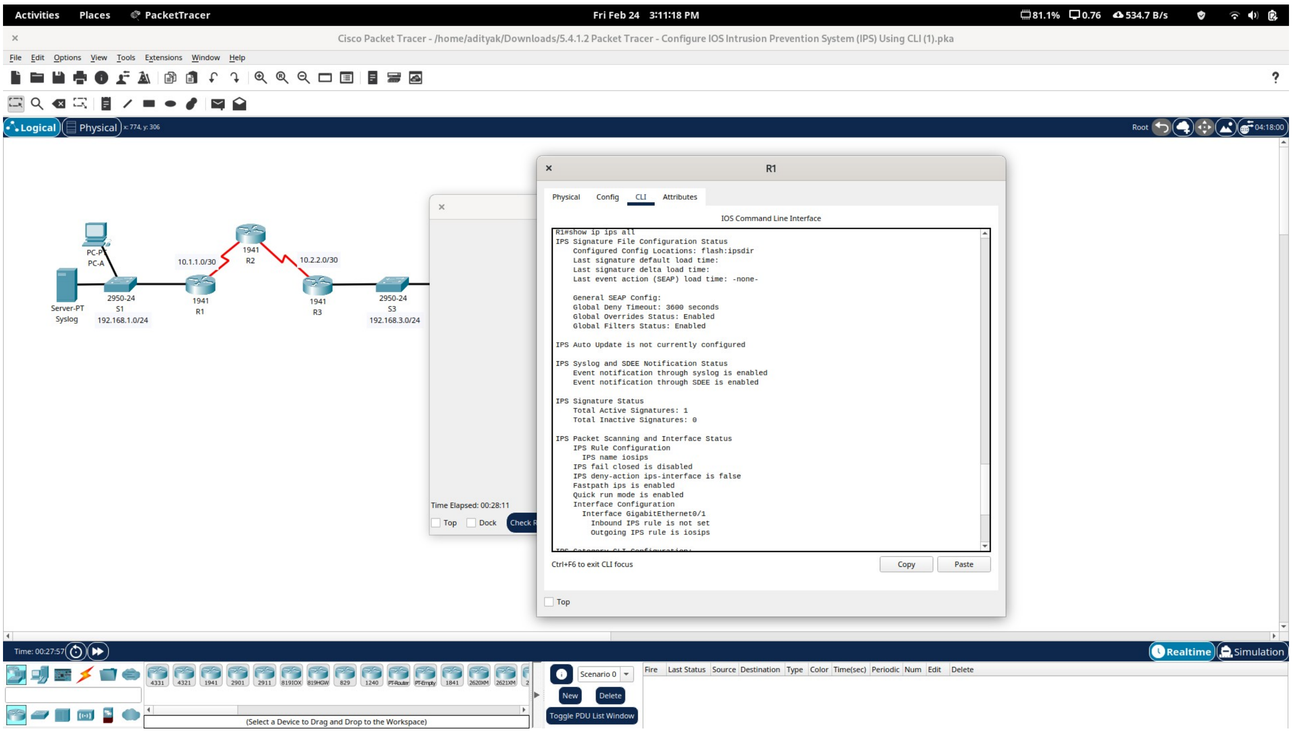
```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action 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>
```



```
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)#interface g0/1
R1(config-if)#ip ips iosips out
R1(config-if)#
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_BUILDS_STARTED:  03:10:03 UTC Feb 24 2023
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Feb 24, 03:10:03.1010:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this
engine will be scanned
*Feb 24, 03:10:03.1010:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
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)#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:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

R1(config)#
```

Step 2: Use show commands to verify IPS.

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

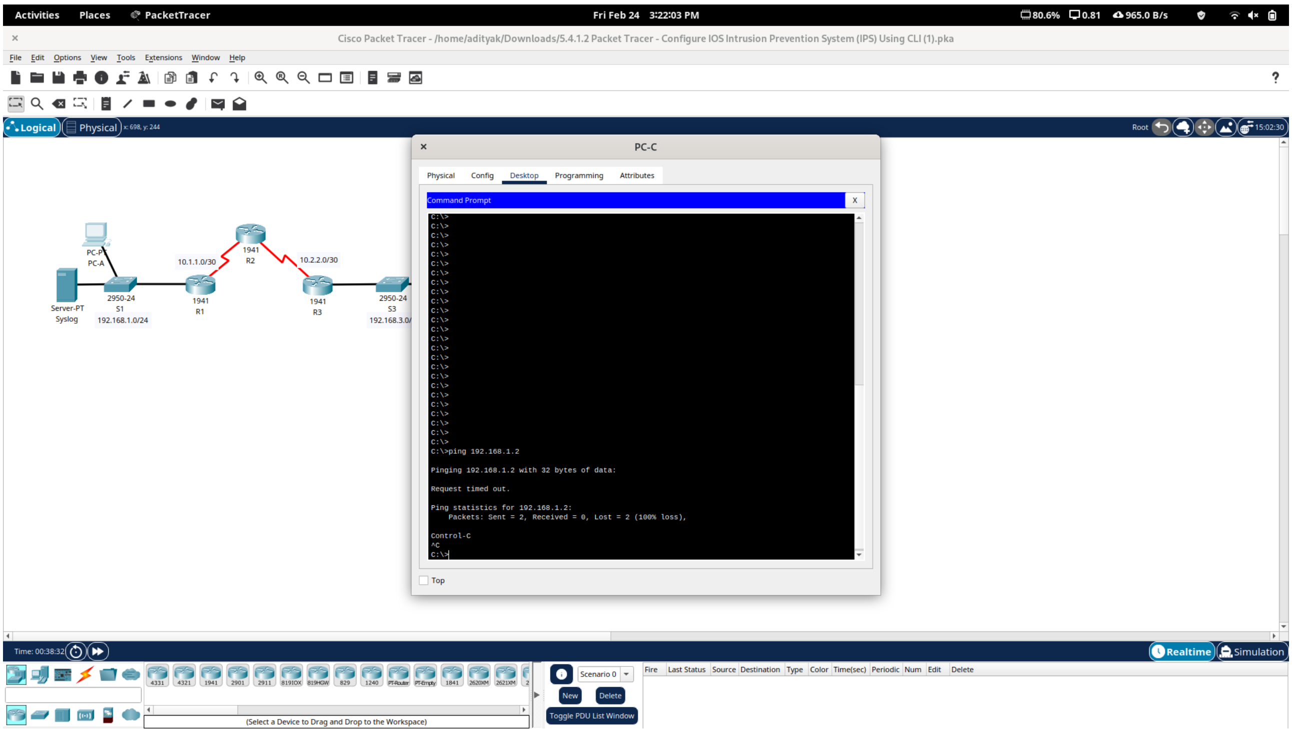


```
R1#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    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

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips
```

Step 3: Verify that IPS is working properly.

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

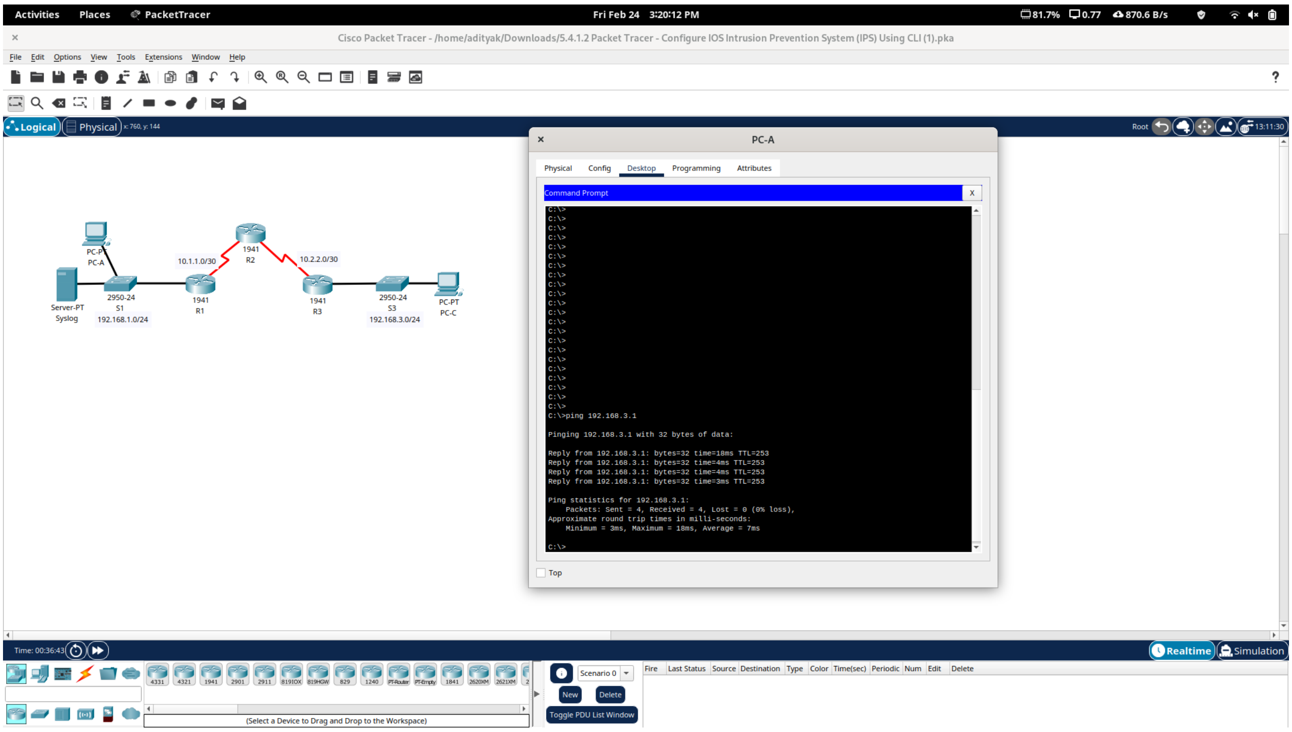
The pings should fail. This is because the IPS rule for event-action of an echo request was set to “denypacket-inline”.



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>
```

b.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.



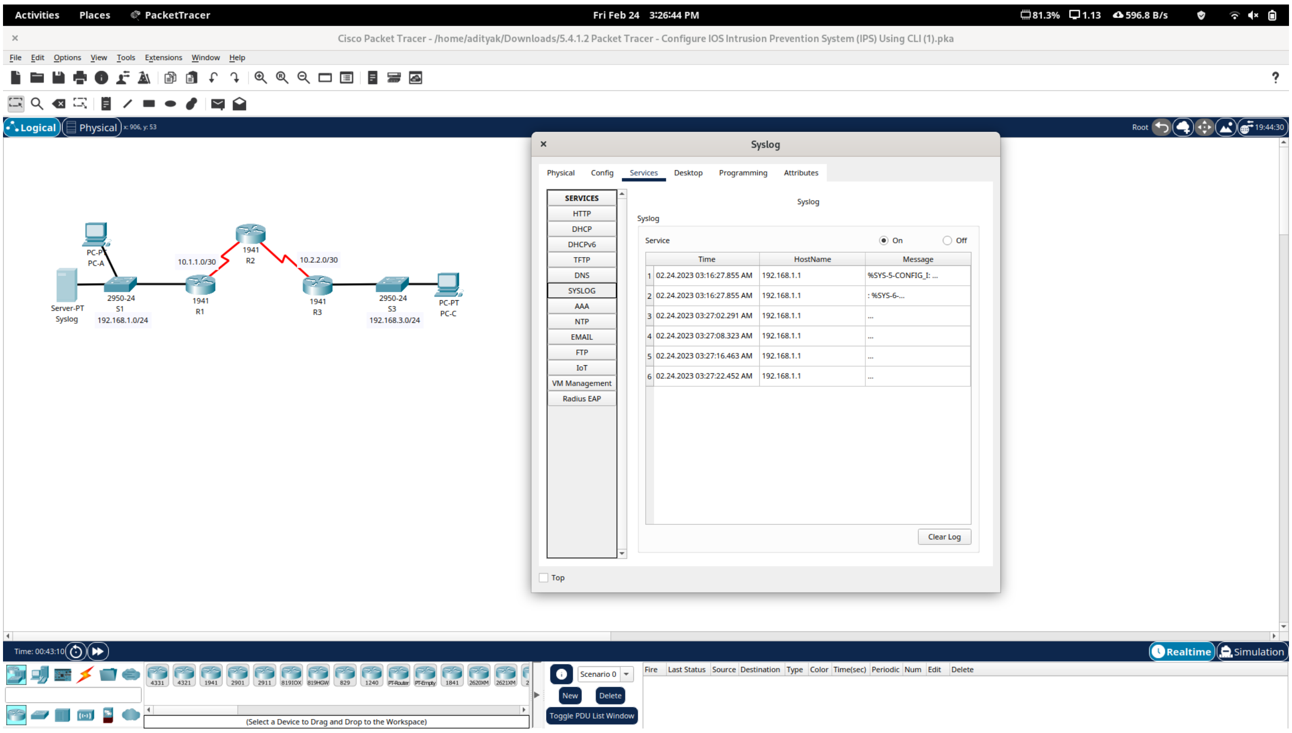
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=18ms TTL=253
Reply from 192.168.3.1: bytes=32 time=4ms TTL=253
Reply from 192.168.3.1: bytes=32 time=4ms TTL=253
Reply from 192.168.3.1: bytes=32 time=3ms TTL=253

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 18ms, Average = 7ms

C:\>
```

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.



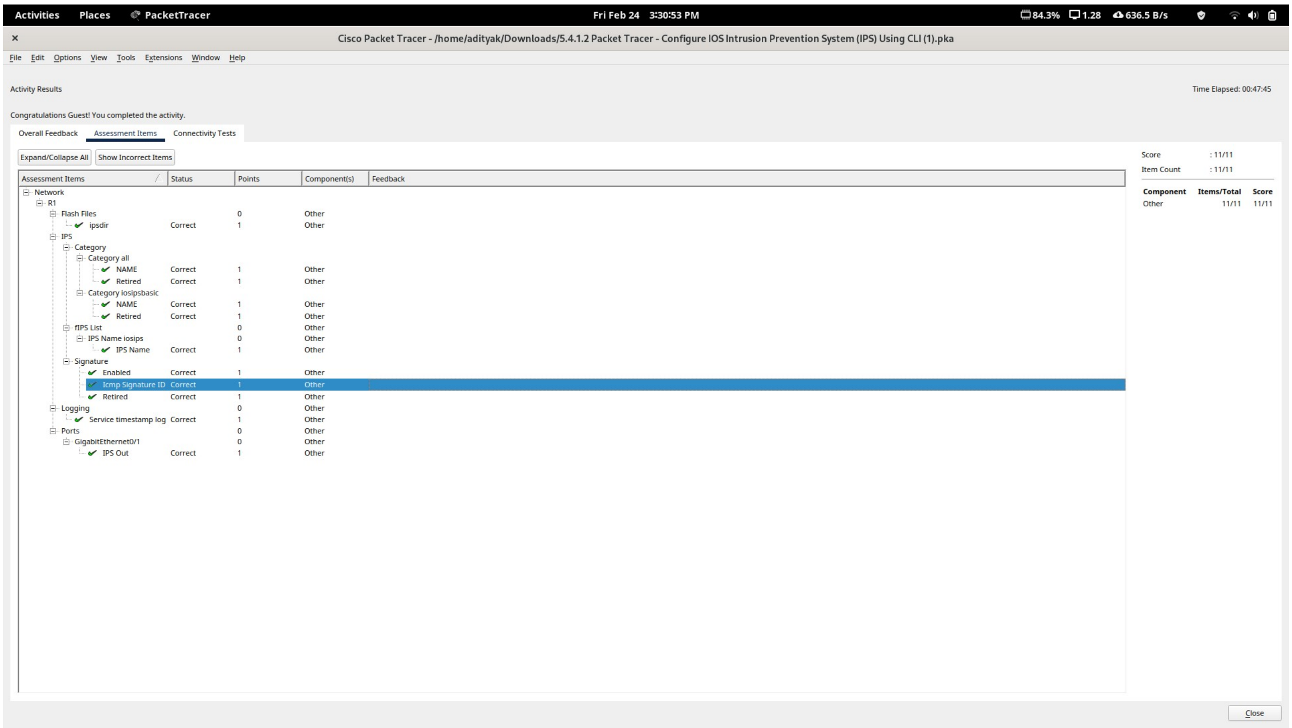
Syslog

Service ● On ○ Off

	Time	HostName	Message
1	02.24.2023 03:16:27.855 AM	192.168.1.1	%SYS-5-CONFIG_I: ...
2	02.24.2023 03:16:27.855 AM	192.168.1.1	: %SYS-6-...
3	02.24.2023 03:27:02.291 AM	192.168.1.1	...
4	02.24.2023 03:27:08.323 AM	192.168.1.1	...
5	02.24.2023 03:27:16.463 AM	192.168.1.1	...
6	02.24.2023 03:27:22.452 AM	192.168.1.1	...

Step 5: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.



Cisco Packet Tracer - /home/adityak/Downloads/5.4.1.2 Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI (1).pka

Activity Results

Time Elapsed: 00:47:45

Congratulations Guest! You completed the activity.

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	
fIPS 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

Configuring IPS (Intrusion Prevention System)

Step 1: Enable the security Technology package

```
R1 (config) # license boot module c1900 techonology 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: ips dir
```

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-sidyf)# exit
Do you want to accept these changes? [Confirm]<Enter>
```

Information Security Alert

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 assessments, penetration testing.