VIT®

Vellore Institute of Technology

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

Computer Science & Engineering

CSE3501

Information Security Analysis and Audit

LAB ASSIGNMENT 2

Submitted to **Prof. RAJA SP**

TOPIC: INTRUSION DETECTION SYSTEM

NAME: PUNIT MIDDHA

REG.NO: 19BCE2060

SLOT: L39+L540

DATE: 23/10/2021

Intrusion Detection System using CLI

DESCRIPTION:

1. Place 2 PCs, 2 switches, 1 server and 3 routers.

2. Add serial Interface to routers.

3. Connection:

   PC0 and server with Switch0 through copper straight-through cable.

   Switch 0 with router 0 through copper straight-through cable.

   Connect routers with each other through serial interface wire.

   Router 2 with switch1 and switch 1 with PC1 through copper straight-through wire.

4. IP configurations:

   PC1:
   IPv4 Address – 192.168.4.2
   Default Gateway - 192.168.4.1

   Router 2:
   GigabitEthernet0/0 - 192.168.4.1
   Serial0/1/1 - 192.168.3.2

   Router 1:
   Serial0/1/1 – 192.168.3.1
   Serial0/1/0 – 192.168.2.2

   Router0:
   Serial0/1/0 – 192.168.2.1
   GigabitEthernet0/0 – 192.168.1.1

   Server0:
   IPv4 Address - 192.168.1.2
   Default Gateway – 192.168.1.1

   PC0:
   IPv4 Address - 192.168.1.3
   Default Gateway - 192.168.1.1

5. Set Routing Information path for all the routers.

6. Now the devices are connected and configured. If we ping server from PC1 we get a reply from the server.

7. Install and enable security technology package:

```
Router#show version
Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#exit
Router#reload
Router>enable
Router#show version
```

8. Create an IOS configuration directory ‘flash’.

```
Router#clock set 09:50:00 24 August 2021
Router#mkdir flash
Router#configure terminal
Router(config)#ip ips config location flash:y
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
```

9. Configure the signature:

```
Router(config)#ip ips signature-c
Router(config-ips-category)#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
Router(config)#interface serial 0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#exit
```

10. Modify the signature

```
Router(config)#ip ips signature-d
Router(config-sigdef)#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 prod
Router(config-sigdef-sig-engine)#event-action produce-alert
```

```
Router(config-sigdef-sig-engine)#event-action deny
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
```

11. Now we have successfully attacked the router from CLI. So, if we ping from PC1 to server request, packets are not received.

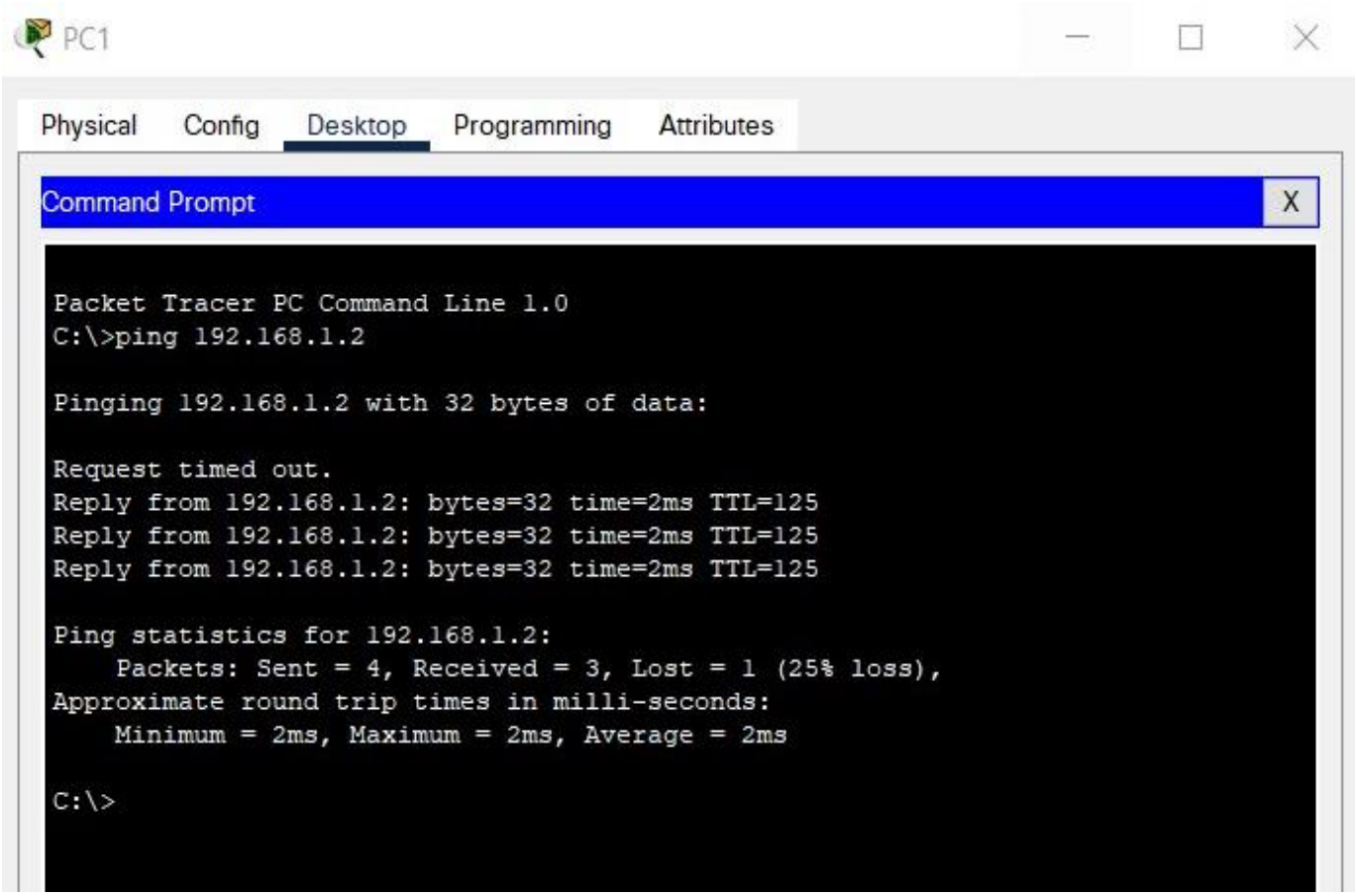
12. See the system log of the server.

13. At router 0(CLI):

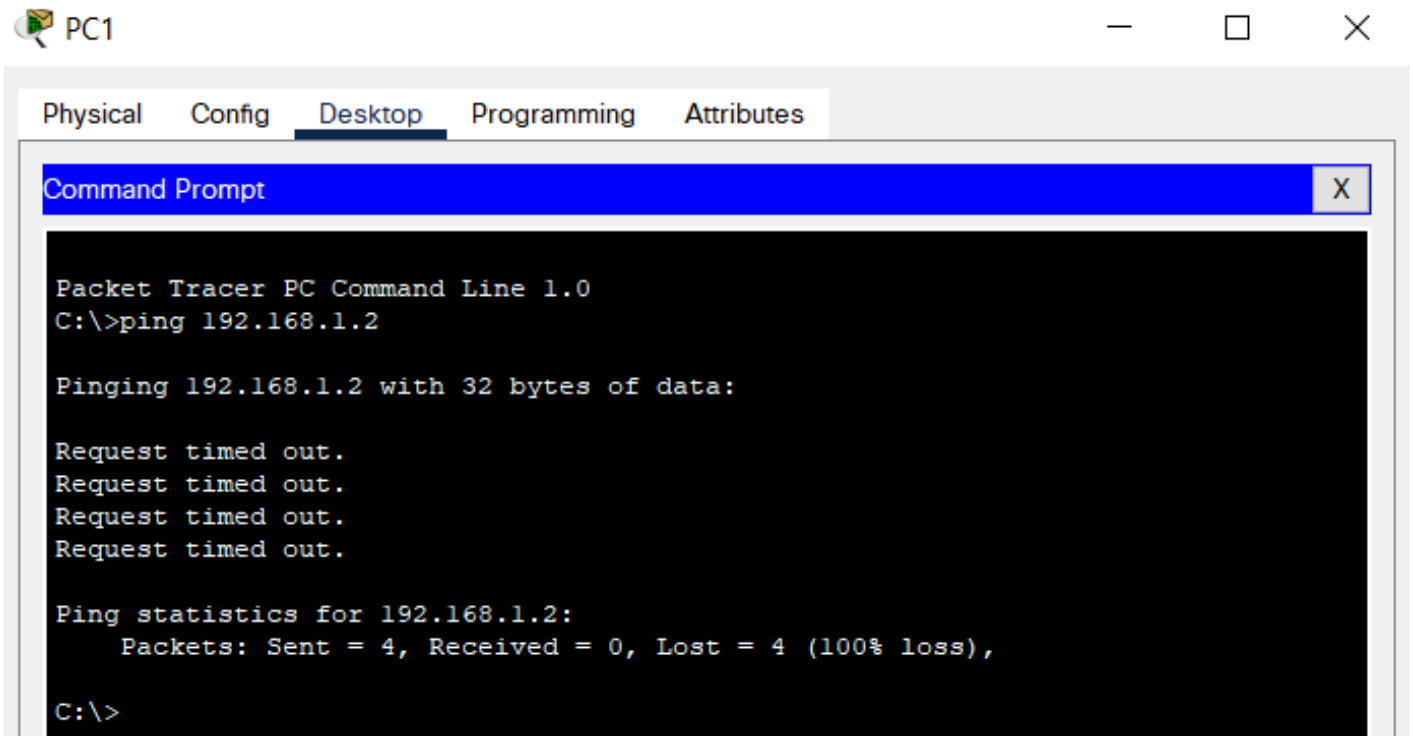
```
Router#configure terminal
Router(config)#logging 192.168.1.2
Router(config)#exit
Router#ping 192.168.1.2
```

SCREENSHOT:

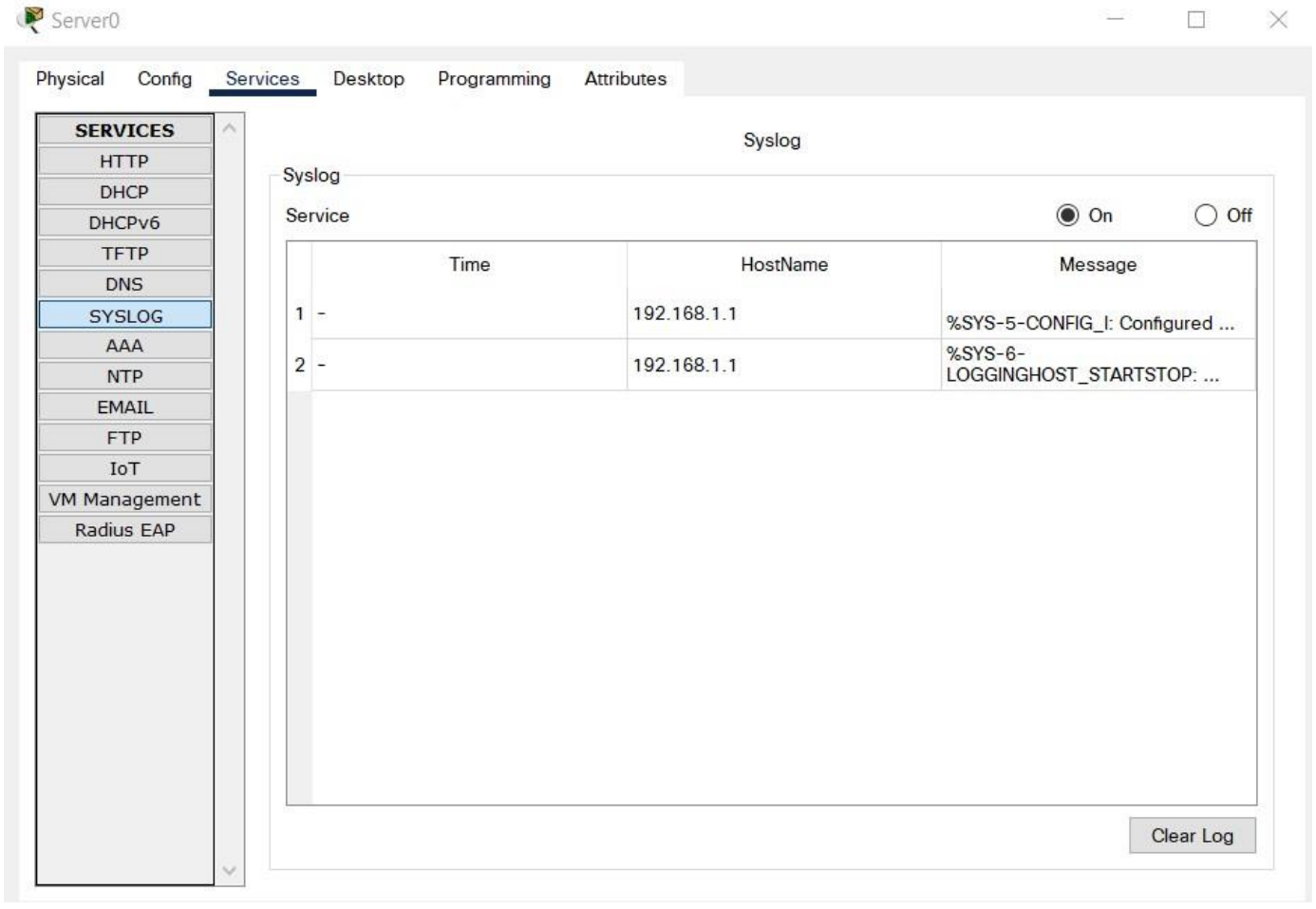
Pinging server from PC1 initially:

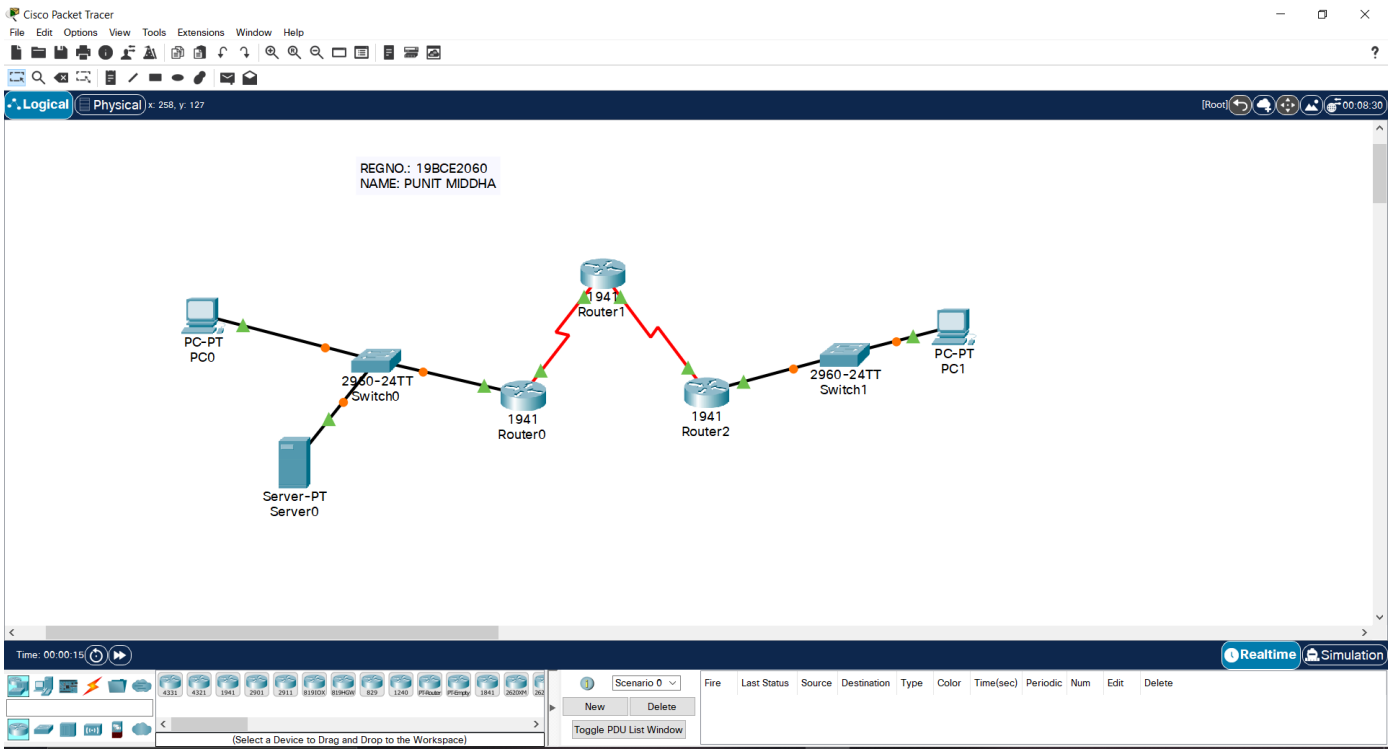


Pinging server from PC1 after attacking on router:



Server0 -> Services -> SYSLOG




Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
REGNO.: 19BCE2060
NAME: PUNIT MIDDHA
1941
Router1
PC-PT
PC0
2960-24TT
Switch0
1941
Router0
1941
Router2
2960-24TT
Switch1
PC-PT
PC1
Server-PT
Server0
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete