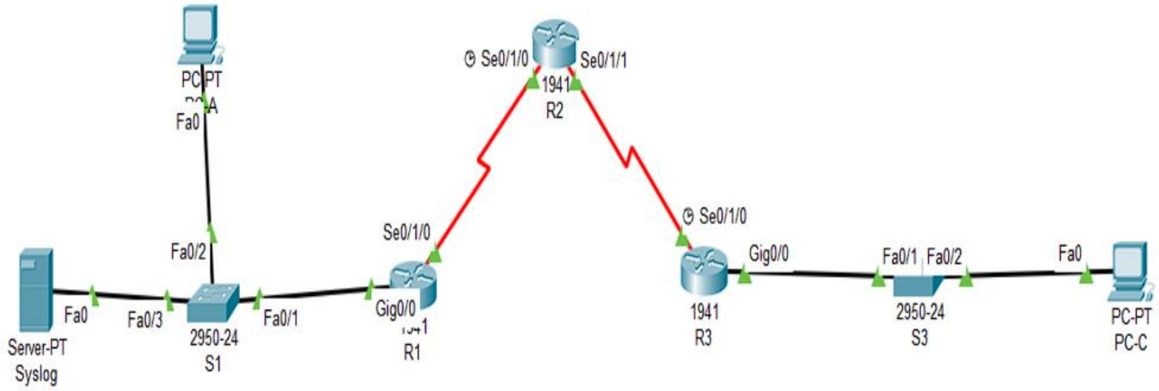
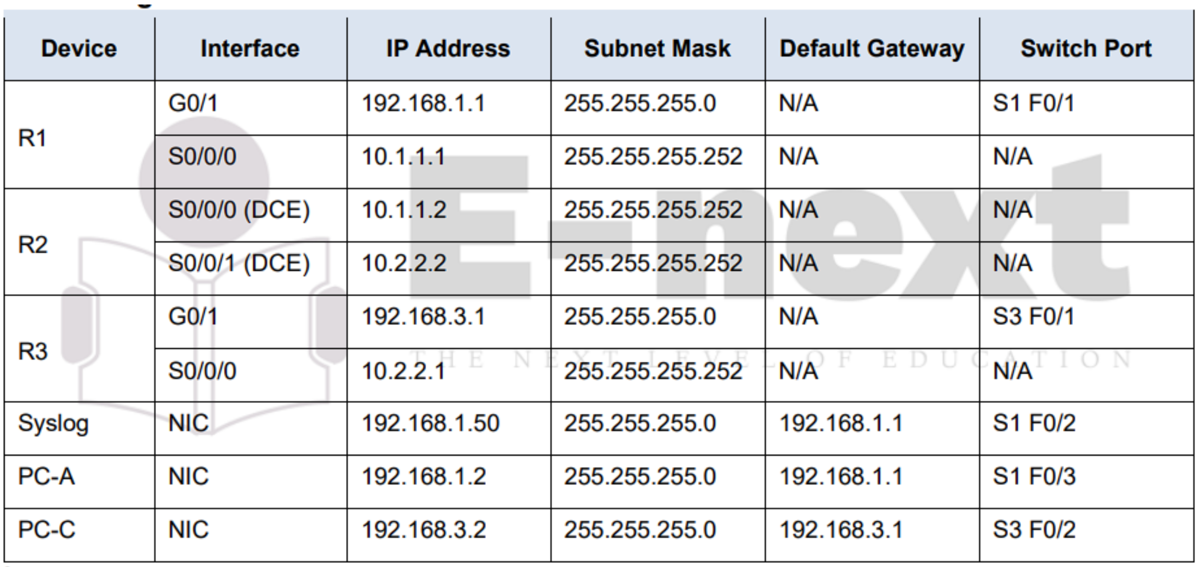
Security In Computing Practical’s

Practical 6: Configure IOS Intrusion Prevention System (IPS) Using the CLI

Topology:



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

Objectives

• Enable IOS IPS.

• Configure logging.

• Modify an IPS signature.

• Verify IPSPart 1: Configure router

Setting Display Name and Hostname

Device - > Config - > Settings
Router -> R1/R2/R3

Switch S1/S3
PC->PC-A/PC-C
Server->Syslog

IP Addressing through CLI

```
R1>en
R1#config t
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit

R2>en
R2#config t
R2(config)#int se0/1/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#int se0/1/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit


R3>en
R3#config t
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#interface Serial0/1/0
R3(config-if)#ip address 10.1.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
```

OSPF Routing

```
R1(config)#router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0..255.255.255 area 0
R1(config-router)#exit


R2(config)#router ospf 1
```

```
R2(config-router)# network 10.2.2.0 0.255.255.255 area 0
R2(config-router)#network 10.1.1.0 0..255.255.255 area 0
R2(config-router)#exit
```

```
R3(config)#router ospf 1
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 10.2.2.0 0..255.255.255 area 0
R3(config-router)#exit
```

Step 1: Configure secret on router

Execute command on all routers

```
R(config)# enable secret enpa55
```

Step 2: Configure console password on router

Execute command on all routers

```
R(config)# line console 0

R(config-line)# password conpa55

R(config-line)# login
```

Step 3: Configure SSH login on router

Execute command on all routers

```
R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024
```

Step 4: Configure OSPF on routers

Execute command on router 1

```
R1(config)#router ospf 1

R1(config-router)# network 192.168.1.0 0.0.0.255 area 0

R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

Execute command on router 2

```
R2(config)#router ospf 1R2(config-router)# network 10.1.1.0 0.0.0.3 area 0

R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Execute command on router 3

```
R3(config)#router ospf 1
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

Part 2: Enable IOS IPS

Step 1: Enable the Security Technology package

```
R1# show version
```

(When command “show version” is given the above result comes, remember for further practical’s)

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

(Type yes)

```
R1# copy run start
R1# reload
R1# show version
```

(When command “show version” is given again the above result comes to check If security is enabled or not, remember for further practical’s)

Step 2: Verify network connectivity

```
PCA> ping 192.168.3.2
```

(Successful)

```
PCC> ping 192.168.1.2
```

(Successful)

Step 3: Create an IOS IPS configuration directory in flash.

```
R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
```

Step 4: Configure the IPS signature storage location.

```
R1(config)# ip ips config location flash:ipsdir
```

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 hr:min:sec date month year

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)# 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.

```
R1(config)# int gig0/0

R1(config-if)# ip ips iosips out
```

Step 9: Use show commands to verify IPS.

```
R1# show ip ips all
```

(Output)

Step 10: View the syslog messages.

Click the Syslog server->Services tab-> SYSLOG

(Output)

Part 3: Modify the Signature

Step 1: Change the event-action of a 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-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Step 2: Use show commands to verify IPS.

```
R1# show ip ips all
```

(Output)

Step 3: Verify that IPS is working properly.

```
PCC> ping 192.168.1.2(Unsuccessful – Request timed out)
PCA> ping 192.168.3.2(Successful)
```

Step 4: View the syslog messages.

Click the Syslog server->Services tab-> SYSLOG