**VIP 2023 - INDUSTRY PROBLEM STATEMENT**

**E.GOWTHAM**

**MCA DEPARTMENT**

**SONA COLLEGE OF TECHNOLOGY**

1. **CyberSecurity**

**Problem Statement:**

Choose a university/college campus and analyze its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

**Tasks:**

1. Campus Network Analysis: Choose a university or college campus and conduct an analysis of its existing network topology, including the layout, devices, and connections.

2. Network Mapping: Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and other relevant network components.

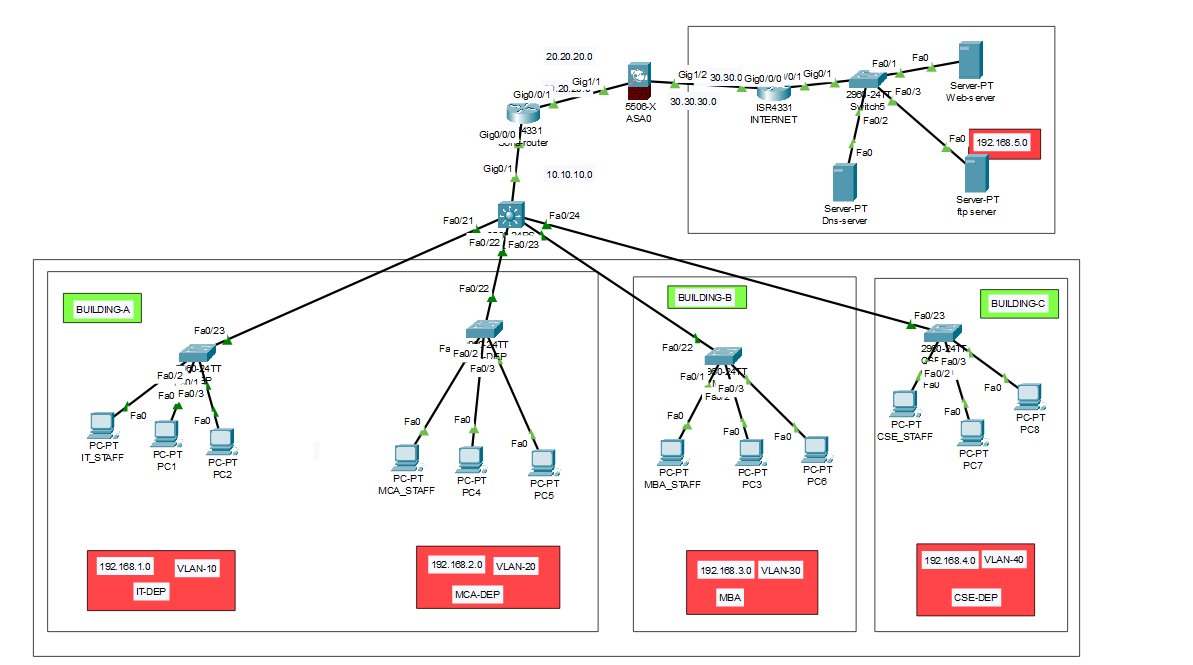
3. Attack Surface Mapping: Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design, considering factors such as unauthorized access, data breaches, and network availability.

4. Secure Access Controls: Incorporate appropriate security controls (e.g., VLANs, IDP/IPS, VPN, Firewalls, password management, vulnerability management etc.) in your design to enhance security posture.

**Deliverables:**

1. Network topology diagram depicting the existing infrastructure and attack surface findings.

2. Security assessment report highlighting identified security risks, proposed solutions, and countermeasures to mitigate attack surface risks.

**SOLUTION:**

* **COLLEGE CAMPUS NETWORK DESIGN**
* **Step-By-Step Guide For The Configuration Of Each Device:**

**STEP-1: COLLEGE-ROUTER:**

* 1. **Password Management:**

1. Configure console and vty (SSH) passwords with “password command”.
2. Enable password encryption with “service password-encryption”.
3. Set the privileged EXEC mode password with “enable secret”.
   1. **Interface And Routing Configuration:**
4. Configure IP addresses on the interfaces with the "ip address" command.
5. Enable the interfaces with "no shutdown".
6. Implement RIP routing protocol and advertise networks with the "router rip" command.
   1. **Access Control List (Acl) Configuration:**
7. Create and configure an ACL with permit statements to allow specific traffic between source and destination IP addresses.
8. Apply the ACL inbound on the GigabitEthernet0/0/0 interface with the “ip access-group” command.

**STEP-2: SERVER-ROUTER:**

**I. Password Management:**

1. Configure console and vty (SSH) passwords with password command.
2. Enable password encryption with service password-encryption.
3. Set the privileged EXEC mode password with enable password.

**II. Interface And Routing Configuration:**

1. Configure IP addresses on the interfaces with the ip address command.
2. Enable the interfaces with no shutdown.
3. Implement RIP routing protocol and advertise networks with the router rip command.

**STEP-3: COLLEGE MULTI-LAYER SWITCH:**

**I. VLAN And IP Address Configuration:**

1. Create VLANs and assign names to them with the vlan command.
2. Configure IP addresses for VLAN interfaces with the interface vlan command.
3. Enable IP routing with the ip routing command.

**II. Rip Routing:**

1. Implement RIP routing protocol and advertise networks with the router rip command.

**STEP-4: COLLEGE DEPARTMENT SWITCHES:**

**I. It-Dep Switch:**

1. Set the IT-DEP switch ports as access ports in VLAN 10.
2. Configure the remaining ports as trunk ports.

**II. Mca-Dep Switch:**

1. Set the MCA-DEP switch ports as access ports in VLAN 20.
2. Configure the trunk port to allow all VLANs.

**III. Mba-Dep Switch:**

1. Set the MBA-DEP switch ports as access ports in VLAN 30.
2. Configure the trunk port to allow all VLANs.

**IV. Cse-Dep Switch:**

1. Set the CSE-DEP switch ports as access ports in VLAN 40.
2. Configure the trunk port to allow all VLANs.

* **CONFIGURATION AND COMMANDS FOR EACH DEVICE:**

1. **COLLEGE-ROUTER:**
2. **PASSWORD MANAGEMENT:**

Sona-router(config)#line console 0

Sona-router(config-line)#password sona

Sona-router(config-line)#login

Sona-router(config-line)#exit

Sona-router(config)#exit

Sona-router(config)#line vty 0 15

Sona-router(config-line)#password virtualsona

Sona-router(config-line)#login

Sona-router(config-line)#exit

Sona-router(config)#enable secret sonaprivilege

Sona-router(config)#service password-encryption

Sona-router(config)#exit

1. **INTERFACE AND ROUTING CONFIGURATION:**

Sona-router(config)#interface g0/0/0

Sona-router(config-if)#ip address 10.10.10.254 255.255.255.0

Sona-router(config-if)#no sh

Sona-router(config-if)#exit

Sona-router(config)#interface g0/0/1

Sona-router(config-if)#ip address 20.20.20.1 255.255.255.0

Sona-router(config-if)#no sh

Sona-router(config-if)#exit

Sona-router( (config)#interface loopback 0

Sona-router( (config-if)#ip address 1.1.1.1 255.255.255.255

Sona-router( (config-if)#no sh

Sona-router( (config-if)#exit

**//RIP ROUTING**

Sona-router(config)#router rip

Sona-router(config-router)#network 10.10.10.0

Sona-router(config-router)#network 192.168.1.0

Sona-router(config-router)#network 192.168.2.0

Sona-router(config-router)#network 192.168.3.0

Sona-router(config-router)#network 192.168.4.0

Sona-router(config-router)#network 20.20.20.0

Sona-router(config-router)#exit

1. **ACCESS CONTROL LIST-CONFIGURATION:**

Sona-router(config)#access-list 120 permit ip 192.168.1.1 255.255.255.0 192.168.5.3 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.1 255.255.255.0 192.168.5.3 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.1 255.255.255.0 192.168.5.3 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.1 255.255.255.0 192.168.5.3 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.1 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.2 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.3 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.1 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.2 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.3 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.1 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.2 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.3 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.1 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.2 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.3 255.255.255.0 192.168.5.1 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.1 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.2 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.1.3 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.1 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.2 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.2.3 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.1 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.2 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.3.3 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.1 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.2 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#access-list 120 permit ip 192.168.4.3 255.255.255.0 192.168.5.2 255.255.255.0

Sona-router(config)#interface g0/0/0

Sona-router(config-if)#ip access-group 120 in

Sona-router(config-if)#exit

1. **SERVER-ROUTER:**
2. **PASSWORD MANAGEMENT:**

internet>enable

internet#configure terminal

internet(config)#line console 0

internet(config-line)#password server

internet(config-line)#login

internet(config-line)#exit

internet(config)#line vty 0 15

internet(config-line)#password server-vty

internet(config-line)#login

internet(config-line)#exit

internet(config)#enable password serverprivilege

internet(config)#service password-encryption

1. **INTERFACE AND ROUTING CONFIGURATION:**

internet(config)#interface gigabitethernet0/0/0

internet(config-if)#no shutdown

internet(config-if)#ip address 30.30.30.254 255.255.255.0

internet(config-if)#exit

internet(config)#interface gigabitethernet0/0/1

internet(config-if)#no shutdown

internet(config-if)#ip address 192.168.5.254 255.255.255.0

internet(config-if)#exit

internet(config)#interface loopback 0

internet(config-if)#ip address 2.2.2.2 255.255.255.255

internet(config-if)#no sh

internet(config-if)#exit

internet(config)#router rip

internet(config-router)#network 30.30.30.0

internet(config-router)#network 192.168.5.0

internet(config-router)#exit

1. **COLLEGE MULTI-LAYER SWITCH:**
2. **VLAN AND IP ADDRESS CONFIGURAION:**

core-switch >enable

core-switch #configure terminal

core-switch(config)#no ip domain-lookup

core-switch(config)#ip routing

core-switch(config)#vlan 10

core-switch(config-vlan)#name IT

core-switch(config-vlan)#vlan 20

core-switch(config-vlan)#name MCA

core-switch(config-vlan)#vlan 30

core-switch(config-vlan)#name server

core-switch(config-vlan)#vlan 40

core-switch(config-vlan)#name cse

core-switch(config-vlan)#exit

core-switch(config)#interface range fa0/21-24

core-switch(config-if-range)#switchport mode access

core-switch(config-if-range)#switchport mode trunk

core-switch(config)#interface vlan 10

core-switch(config-if)#ip address 192.168.1.254 255.255.255.0

core-switch(config-if)#exit

core-switch(config)#interface vlan 20

core-switch(config-if)#ip address 192.168.2.254 255.255.255.0

core-switch(config-if)#exit

core-switch(config)#interface vlan 30

core-switch(config-if)#ip address 192.168.3.254 255.255.255.0

core-switch(config-if)#exit

core-switch(config)#interface vlan 40

core-switch(config-if)#ip address 192.168.4.254 255.255.255.0

core-switch(config-if)#exit

core-switch(config-if-range)#switchport trunk encapsulation dot1q

core-switch(config-if-range)#exit

core-switch(config)#vtp mode server

core-switch(config)#vtp version 2

core-switch(config)#vtp domain cisco

core-switch(config)#interface g0/1

core-switch(config-if)#no switchport

core-switch(config-if)#ip address 10.10.10.1 255.255.255.0

core-switch(config-if)#no sh

core-switch(config-if)#exit

1. **RIP ROUTING:**

core-switch(config)#router rip

core-switch(config-router)#network 192.168.1.0

core-switch(config-router)#network 192.168.2.0

core-switch(config-router)#network 192.168.3.0

core-switch(config-router)#network 192.168.4.0

core-switch(config-router)#network 10.10.10.0

core-switch(config-router)#exit

1. **COLLEGE DEPARMENT SWITCHES:**
2. **IT-DEP SWITCH:**

IT-DEP>enable

IT-DEP#configure terminal

IT-DEP(config)#inter fa0/23

IT-DEP(config-if)#switchport mode trunk

IT-DEP(config-if)#exit

IT-DEP(config)#vlan 10

IT-DEP(config-vlan)# name IT

IT-DEP(config-vlan)#exit

IT-DEP(config)#vtp mode client

IT-DEP(config)#interface range fa0/1-5

IT-DEP(config-if-range)#switchport mode access

IT-DEP(config-if-range)#switchport access vlan 10

IT-DEP(config-if-range)#exit

1. **MCA-DEP SWITCH:**

MCA-DEP>enable

MCA-DEP#configure terminal

MCA-DEP(config)#interface fa0/22

MCA-DEP(config-if)#switchport mode trunk

MCA-DEP(config-if)#exit

MCA-DEP(config)#vlan 20

MCA-DEP(config-vlan)#name mca

MCA-DEP(config)#interface range fa0/1-5

MCA-DEP(config-if-range)#switchport mode access

MCA-DEP(config-if-range)#switchport access vlan 20

MCA-DEP(config-if-range)#exit

MCA-DEP(config)#vtp mode client

MCA-DEP(config)#no ip domain-lookup

MCA-DEP(config)#exit

MCA-DEP(config)#interface fa0/22

MCA-DEP(config-if)#switchport mode trunk

MCA-DEP(config-if)#switchport trunk allowed vlan all

MCA-DEP(config-if)#exit

1. **MBA-DEP SWITCH:**

MBA-DEP>enable

MBA-DEP#configure terminal

MBA-DEP(config)#interface fa0/22

MBA-DEP(config-if)#switchport mode trunk

MBA-DEP(config-if)#exit

MBA-DEP (config)#vlan 30

MBA-DEP(config-vlan)#name mba

MBA-DEP(config-vlan)#exit

MBA-DEP(config)#vtp mode client

MBA-DEP(config)#interf range fa0/1-5

MBA-DEP(config-if-range)#switchport mode access

MBA-DEP(config-if-range)#switchport access vlan 30

MBA-DEP(config-if-range)#exit

1. **CSE-DEP SWITCH:**

CSE-DEP>enable

CSE-DEP#configure terminal

CSE-DEP(config)#vlan 40

CSE-DEP(config-vlan)#name cse

CSE-DEP(config-vlan)#end

CSE-DEP(config)#vtp mode client

CSE-DEP(config)#interface fa0/22

CSE-DEP(config-if)#switchport mode trunk

CSE-DEP(config-if)#switchport trunk allowed vlan all

CSE-DEP(config-if)#exit

CSE-DEP(config)#inter range fa0/1-5

CSE-DEP(config-if-range)#switchpor mode access

CSE-DEP(config-if-range)#switchport access vlan 40

CSE-DEP(config-if-range)#exit