**Design Specifications**

*Compiled on 16 April 2021*

**1. Introduction**

This assignment is the first step in the culminating experience for cadets within the 3CES, Cyber Minor and CS/IT programs. To successfully complete the assignment, students will apply concepts from previous coursework in CY300, CY350, and CY450. Each cadet group represents an information technology (IT) response team called in to replace the IT department for a company in one of the 16 critical infrastructure sectors <https://www.cisa.gov/critical-infrastructure-sectors>. We will simply refer to this company as the sector to which it belongs.

Groups will design and build an improved network for their sector according to these network specifications. Cadet groups will then integrate, update, and secure the existing hosts and servers while maintaining prior functionality. Your instructors will role-play as the sole remaining member of the previous IT department. They will answer any direct questions but will not volunteer additional information unless you ask.

**2. Schedule & Grading**

Refer to the schedule in the public folder for dates and tasks. Below is a table summarizing the point value for each of the graded events.

**Table 1: Schedule & Point Values**

|  |  |  |
| --- | --- | --- |
| **Lesson** | **Event** | **Points** |
| 28 | Implementation Design | 30 |
| 30 | Implementation Assessment (IPR) | 60 |
| 32 | Implementation Assessment Continued |
| 34 | Security Assessment (IPR) | 90 |
| 36 | Security Assessment Continued |
| 37 | Incident Response Exercise |  |
| 39 | Incident Response Report | 30 |
| 39 | Group Final Report | 50 |
| 39 | Individual Security Reflections | 100 |

**Implementation Design:** Groups will prepare the following details for their implementation plans:

* Design Plan:
  + Network diagram
  + Subnet chart
  + Service Implementation Plan
  + Initial security considerations (ACLs and other planned controls)
* Team Details
  + Initial user roles within the team
  + Schedule of known disruptive events
  + Sync plan (how and how often the group plans to synchronize their efforts)

**3. Scenario**

Your team is the new IT department for your sector. The previous team was fired after numerous security incidents. Your team will have to start by reestablishing your sector’s critical services and infrastructure, which have been rendered inoperable by the most recent incident. Your instructor, who was previously the junior member of the IT team that no one listened to, proved to be the only competent member of the team. Now, they are your point of contact for continuity and an interface for requests to DHS, your higher headquarters.

Your first task (this assignment) is a design plan for re-establishing your sector. This step focuses on the restoration of service availability, but that will remain a priority throughout the later phases when you will focus on restoring other security CIA+ properties (next assignment). More details will be provided soon, but it is appropriate to begin considering security measures immediately.

**4. Network Architecture**

The entire capstone network is a private network (10.45.128.0/17) and each group is assigned a subnet within this network. Figure 1 depicts the allocation of network addresses in the larger network. Each sector will divide their assigned network into two subnets **internal (LAN)** and **external (DMZ)**. The virtual adapters follow the naming convention **cy450-teamX-LAN** and **cy450-teamX-DMZ** respectively. Table 1 specifies the required number of hosts for each of these subnetworks (make sure you plan for growth). **The actual number of virtual machines you will deploy is less than the total listed in the table but ensure that your subnets are sized appropriately for the requirement.**

**Table 2: IP Ranges, Domains, External Addresses & Subnet Requirements**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Team** | **IP Range** | **Domain** | **Ext. Address** | **LAN Hosts** | **DMZ Hosts** |
| HQ | 10.45.200.0/24 | .cy450, hq.cy450 | 10.45.250.100 | N/A | N/A |
| 1 | 10.45.201.0/24 | chem.cy450 | 10.45.250.1 | 10 | 120 |
| 2 | 10.45.202.0/24 | comms.cy450 | 10.45.250.2 | 20 | 110 |
| 3 | 10.45.203.0/24 | dams.cy450 | 10.45.250.3 | 30 | 100 |
| 4 | 10.45.204.0/24 | defense.cy450 | 10.45.250.4 | 40 | 90 |
| 5 | 10.45.205.0/24 | emergency.cy450 | 10.45.250.5 | 50 | 80 |
| 6 | 10.45.206.0/24 | energy.cy450 | 10.45.250.6 | 60 | 70 |
| 7 | 10.45.207.0/24 | fin.cy450 | 10.45.250.7 | 70 | 60 |
| 8 | 10.45.208.0/24 | gov.cy450 | 10.45.250.8 | 80 | 50 |
| 9 | 10.45.209.0/24 | infotech.cy450 | 10.45.250.9 | 90 | 40 |
| 10 | 10.45.210.0/24 | nuclear.cy450 | 10.45.250.10 | 100 | 30 |
| 11 | 10.45.211.0/24 | transpo.cy450 | 10.45.250.11 | 110 | 20 |
| 12 | 10.45.212.0/24 | water.cy450 | 10.45.250.12 | 120 | 10 |

**Figure 1: Capstone Network**



**5. Virtual Machine Resources**

To implement your sector’s service requirements, each team is resourced with three different virtual machine images. The images were taken from before the series of incidents occurred, but it is unknown whether the machines were ***already compromised*** at that time.

**A. Router/Firewall**

Your router/firewall is the Cisco CSR1000v cloud router. The router provides a traditional Cisco IOS Command Line Interface. Unfortunately, the router image was backed up only in its default state, so none of your sector's configuration survived. Each appliance has three interfaces: WAN, LAN, and DMZ. Login is sector, password: admin, with enable password of : admin.

**B. Server**

The server image is based on Ubuntu 18.04 Desktop. The backup contains a project management database, a project management web application (Collabtive), and the user accounts required to be on **all servers**. Unfortunately, the backup does not include your sector's web server or DNS server configuration. Before the incident, all the services were consolidated on one system, but the backup we have available was taken before this consolidation. As a result, you will receive one server virtual machine to re-establish all of your services, but you may request up to five additional VMs through the change request process. Based on the new guidance from HQ, you will need at least three servers to implement a defensible set of external services. Be sure to request specific virtual machines that are named according to the function you would like them to perform. The default administrative credentials for the server VM image are user: sector, password: admin.

**C. Client**

The client image is also based on Ubuntu 18.04 Desktop. The backup contains the user accounts required for **all clients**. You may audit the accounts and request changes to those accounts, but unless you explicitly request otherwise, **all user accounts** must remain available throughout the duration of the exercise. You will receive one client VM which will represent multiple systems for your internal users. You may request additional client VMs if you would like to use them for specialized purposes (such as compliance or penetration testing) on your capstone network. The default administrative credentials for the client VM are user: sector, password: admin.

**D. Change requests**

You may request changes to the default system configurations; **all change requests and deviations from this specification must be requested to and approved by Headquarters. Additionally, you will also need to request support from Headquarters for some of your services to be accessible by external entities**. For example, Headquarters and other sectors will not be able to resolve any of your domain names unless you register your external DNS server’s address with HQ. For internal requests such as renaming your team’s VMs or making other changes to your team’s VMs, use your team's Teams channel. For requests that require external support, use the rfcs channel in Teams.

**6. Sector Service Requirements**

The following sections specify the required services that must be available on each team’s network. Many of these services must be available both to local users and external users on the 10.0.0.0/8 network. Each team must decide how to implement these services to achieve the required CIA+ properties.

**A. Routing**

Traffic must flow between each team’s local network and the greater CY450\_Capstone network. Each team’s external network must be accessible from its internal network and the greater capstone network as depicted in Figure 1. Each team must also advertise their networks to the CY450\_Capstone network via OSPF area 450. The CY450\_Capstone network implements OSPF using MD5 message-digest authentication with the following authentication key: cy450-capstone and key-id: 1. The default route is advertised by the core router depicted in Figure 1.

**B. Remote Access**

To improve usability and allow HQ to audit your services, you must implement **secure remote terminal access for all systems** including your clients, servers, and router. Successfully implementing remote terminal access will also enable you to remotely administer your systems.

**C. Domain Name Service**

Each team must enable domain name resolution for all systems within their network. Each team should enumerate the domain names for all clients, servers, and network devices as part of your design. Refer to Table 2 for the required host names. For HQ to properly configure its DNS server, each team must submit an RFC to HQ with the address of their external DNS server. Your DNS servers should forward requests to the HQ DNS shown in Figure 1. Your internal client devices should use your group’s internal DNS server as their primary DNS server and your external DNS as their secondary DNS. Several components of your DNS configuration should closely resemble the DNS lab. Your internal zone does not need a reverse zone, but your external zone should have one. All external zone names should be authoritatively resolved by the Internal DNS.

**Table 3: Host Names (Replace** SECTOR **with your sector).**

|  |  |  |
| --- | --- | --- |
| **Description** | **Zone** | **Host Name** |
| External DNS | External | ns1.SECTOR.cy450 |
| Router | External | router.SECTOR.cy450 |
| Web Server | External | www.SECTOR.cy450 |
| Internal DNS | Internal | ns2.int-SECTOR.cy450 |
| Client | Internal | client.int-SECTOR.cy450 |

**D. Web Server**

You must reestablish your sector's web server, which includes several components. The home page (e.g., http://www.SECTOR.cy450/) for your sector should be descriptive and professional. You must have at least two additional pages: team\_info.html and sector\_info.html that contain the following information: a team summary that includes your team names, photo(s), and very short bios that relate to the roles on your team; and a sector summary that summarizes pertinent information about your sector. The homepage must link to these two pages as well as the Collabtive project management web application. The supporting database for the Collabtive application is provided on the Server VM image. Your web server should primarily use HTTPS and redirect HTTP requests to HTTPS. Your certificate should also be signed by HQ to prevent a certificate warning for your users.

**E. Client (User) Workstation(s)**

The client VM could be used by many user workstations that would be found within an organization. Your team should do everything possible to secure these hosts while preserving the legitimate user accounts that are on them. Additionally, your team could request to minimize the client VM in many ways if it were used for a specialized purpose other than as a general-purpose client.

**7. Deliverables**

Given the scenario and the requirements, you must devise an initial implementation plan that contains, at a minimum, the elements specified in the 1.1 Design Template document.