Lab #10: Assessment Worksheet
Part A – Create a CIRT Response Plan for a Typical IT Infrastructure

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 25/3/2023

Overview

The following are the steps required to perform Lab #10 – Create a CIRT Response Plan for a Typical IT Infrastructure:

1. Refer to Figure 6 – "Mock" IT Infrastructure for Lab #10. Your CIRT response plan must address one of the following:
   - Internet ingress/egress
   - Headquarters departmental VLANs on LAN Switch 1 and 2 with clear-text privacy data
   - Remote branch office locations connected through the WAN
   - Data center/server farm

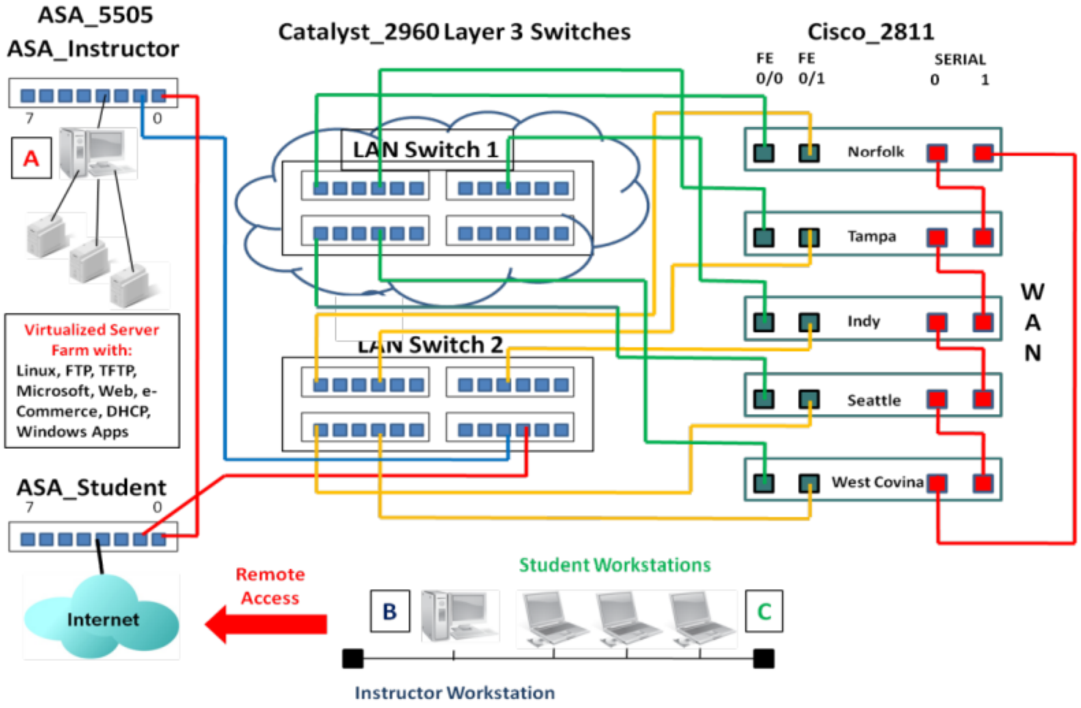

Figure 6 – "Mock" IT Infrastructure for Lab #10

2. For one of the above CIRT response plan items, build a CIRT response plan approach according to the defined 6-step methodology unique to the risks associated with the item:

- Step 1 - Preparation - what tools, applications, laptops, and communication devices are needed to address computer/security incident response for this specific breach?
- Step 2 - Identification - when an incident is reported it must be identified, classified, and documented. During this step, the following information is needed:
  - Validating the incident
  - Identifying its nature, if an incident has occurred
  - Identifying and protecting the evidence
  - Logging and reporting the event or incident
- Step 3 - Containment - the immediate objective is to limit the scope and magnitude of the computer/security-related incident as quickly as possible, rather than to allow the incident to continue in order to gain evidence for identifying and/or prosecuting the perpetrator. For the lab explain how you will solve this challenge.
- Step 4 - Eradication - the next priority is to remove the computer/security related incident or breach’s affects. Explain what you would do for this lab.
- Step 5 - Recovery - recovery is specific to bringing back into production those IT systems, applications, and assets that were affected by the security-related incident. Define what your RTO would be for this lab and explain your reasoning.
- Step 6 - Post-Mortem Review - following up on an incident after the recovery tasks and services are completed is a critical last step in the overall methodology. A post-mortem report should include a complete explanation of the incident and the resolution and applicable configuration management, security countermeasures, and implementation recommendations to prevent the security incident or breach from occurring again. Explain what you would do port-mortem for an incident that occurs within your portion of the network

--------------6-step methodology--------------

To build a CIRT response plan for one of the items, you need to follow the 6-step methodology that consists of:

- **Preparation**: This step involves performing a risk assessment and prioritizing security issues, identifying which are the most sensitive assets and which critical security incidents the team should focus on. You also need to create a communication plan, document roles, responsibilities and processes, and recruit members to the Cyber Incident Response Team (CIRT). You also need to prepare tools, applications, laptops and communication devices that are needed to address computer/security incident response for this specific breach.

- **Identification**: This step involves validating the incident, identifying its nature and scope, identifying and protecting the evidence, logging and reporting the event or incident. You need to use tools such as network monitoring systems, intrusion detection systems (IDS), antivirus software etc. to detect anomalies and alerts. You also need to classify the incident according to its severity and impact.

- **Containment**: This step involves limiting the scope and magnitude of the computer/security-related incident as quickly as possible by isolating or disconnecting affected systems from the network. You need to consider short-term containment (such as blocking ports or IP addresses) and long-term containment (such as patching vulnerabilities or changing passwords) strategies.

- **Eradication**: This step involves removing the computer/security related incident or breach's effects by deleting malicious files or code, restoring backups or reinstalling systems etc. You also need to identify root causes of the incident and determine how it was exploited.

- **Recovery**: This step involves bringing back into production those IT systems, applications and assets that were affected by the security-related incident by testing them for functionality and security before reconnecting them to the network. You also need to define your recovery time objective (RTO), which is how long it will take you to restore normal operations after an incident.

- **Post-Mortem Review**: This step involves following up on an incident after recovery tasks are completed by analyzing what happened, what worked well and what didn't work well during each phase of response. You also need to create a post-mortem report that includes a complete explanation of the incident and resolution along with recommendations for improving security measures and processes.

Overview

The best risk mitigation strategy requires building and implementing a CIRT response plan. This means you are preparing for potential computer/security incidents and practicing how to handle these incidents. Like any kind of remediation, the more you can plan, prepare, and practice, the more prepared you are to handle any risk situation. This lab presented how to apply the computer/security incident response methodology to handling incidents specific to a portion of the network infrastructure.

Lab Assessment Questions

1. What risk mitigation security controls or security countermeasures do you recommend for the portion of the network that you built a CIRT response plan? Explain your answer.

- Answer: A CIRT response plan typically includes the following elements:

- Implementing firewall rules, network segmentation and encryption to protect data in transit and at rest
- Following security best practices proposed by vendors to harden their products and give priority to the secure management of high-privileged accounts and key assets
- Applying patches and updates regularly to fix known vulnerabilities
- Adopting the CIS Critical Security Controls as a framework for improving cybersecurity posture
- Conducting regular backups, audits and tests to ensure data integrity and availability

2. How does a CIRT plan help an organization mitigate risk?

- Answer: A CIRT plan helps an organization mitigate risk by:

- Providing a trusted point of contact and a coordinated response for computer incidents
- Reducing the potential damage and impact of computer incidents by following predefined steps and procedures
- Enhancing the security awareness and preparedness of the organization and its stakeholders
- Improving the recovery time and restoring normal operations as soon as possible
- Learning from past incidents and improving security controls and policies accordingly

3. How does a CIRT response plan help mitigate risk?

- Answer: A CIRT response plan can help mitigate risk by providing clear roles and responsibilities, communication channels, procedures and tools for responding to different types of incidents. A CIRT response plan can also help reduce the impact and cost of an incident by enabling faster detection, containment, analysis and recovery.

4. How does the CIRT post-mortem review help mitigate risk?
- Answer: A CIRT post-mortem review can help mitigate risk by providing valuable insights and lessons learned that can be used to update policies, procedures, tools, training and prevention measures. A CIRT post-mortem review can also help foster a culture of learning and collaboration among team members.

5. Why is it a good idea to have a protocol analyzer as one of your incident response tools when examining IP LAN network performance or connectivity issues?
- Answer: A protocol analyzer can be useful for an incident response when examining IP LAN network performance or connectivity issues because it can help identify anomalies, malicious activities, misconfigurations, vulnerabilities and evidence of compromise. A protocol analyzer can also help reconstruct network events, verify compliance and support forensic investigations.

6. Put the following in the proper sequence:
Identification: 2
Containment: 3
Post-Mortem Review: 6
Eradication: 4
Preparation: 1
Recovery: 5

7. Which step in the CIRT response methodology relates back to RTO for critical IT systems?
- Answer: Recovery

8. Which step in the CIRT response methodology requires proper handling of digital evidence?
- Answer: Containment

9. Which step in the CIRT response methodology requires review with executive management?
- Answer: Post-Mortem Review

10. Which step in the CIRT response methodology requires security applications and tools readiness?
- Answer: Preparation