Scenario: A medium-sized financial institution in Australia has recently suffered from a series of cyber attacks. The company's management has decided to evaluate and improve its cybersecurity posture by conducting a theoretical analysis of potential offensive cyber operations that a threat actor could employ, focusing on offensive cyber security tradecraft using the MITRE ATT&CK framework.

Hypothetical Target: The target is a medium-sized financial institution with branches across Australia. They offer a wide range of financial services, including personal and corporate banking, credit cards, loans, and investment products. The company has a hybrid IT infrastructure, consisting of on-premises and cloud-based systems, and employs a variety of cybersecurity tools and measures, such as firewalls, intrusion detection systems, and anti-malware software.

Step-by-step process to complete the assignment:

Step1.

Refine the target-goal combination: Analyse the target's environment and defences using MITRE ATT&CK framework techniques to identify potential vulnerabilities that could be exploited by a threat actor. Your goal is to understand and assess the potential cyber offensive operations that could be executed against the financial institution.

Step 1: Refine the target-goal combination

In this step, you will analyse the target's environment and defences using the MITRE ATT&CK framework techniques to identify potential vulnerabilities that could be exploited by a threat actor. The goal is to understand and assess the potential cyber offensive operations that could be executed against the financial institution, allowing the company to proactively address these vulnerabilities and improve its cybersecurity posture.

1.1 Identify the target's assets: Analyse the financial institution's key assets that might be attractive to threat actors. These could include customer data, sensitive financial information, intellectual property, and critical infrastructure components.

1.2 Assess the target's environment: Study the target's IT infrastructure, including on-premises and cloud-based systems, to understand their network topology, applications, and protocols in use. This information will help you determine potential attack vectors and vulnerabilities.

1.3 Evaluate the target's defences: Examine the financial institution's current cybersecurity measures, such as firewalls, intrusion detection systems, and anti-malware software. Evaluate their effectiveness in protecting the organization's assets and identify potential weaknesses that could be exploited.

1.4 Map vulnerabilities to MITRE ATT&CK techniques and Cyber Kill Chain stages: Using the information gathered about the target's environment and defences, identify relevant MITRE ATT&CK techniques that could be employed by threat actors to exploit these vulnerabilities. For example, if the target's email system is vulnerable to phishing attacks, you might consider techniques like spearphishing (T1566) or phishing for information (T1598).

1.5 Set the goal: Based on the identified vulnerabilities and potential attack vectors, establish a goal for your theoretical offensive strategy. The goal could be to exfiltrate sensitive data, disrupt the financial institution's operations, or gain unauthorized access to critical systems. Make sure the goal aligns with the learning outcomes of the course.

(now in this scenario let's assume that Technique_ID T1566 was successful and an employee interacted with a phishing email on their personal computer. and the 'Condition' was malware placed in an employee's personal computer. this leads to the Action 'Input capture' Technique_ID T1056)

1.6 Develop the integrated Attack Flow: Combine the Cyber Kill Chain stages and the MITRE ATT&CK techniques to create a structured representation of the steps an adversary might take to execute a cyber attack against the target, utilizing both methodologies..

At the end of Step 1, you should have a clear understanding of the target's environment, defences, and potential vulnerabilities, as well as a defined goal for your theoretical offensive strategy. This information will be crucial for developing your offensive strategy in Step 4.

Step 2

2. Conduct theoretical reconnaissance: Gather open-source intelligence about the target organization to gain insights into its network topology, systems, applications, and potential vulnerabilities. Apply techniques like OSINT (T1597) and network service scanning (T1046) to collect information.

2.1 Review MITRE ATT&CK techniques and Cyber Kill Chain stages related to the identified vulnerabilities: Revisit the vulnerabilities you discovered during Step 1 and review the associated techniques and stages in the MITRE ATT&CK framework and Cyber Kill Chain to better understand the potential attack paths.

2.2 Analyze the techniques and stages in the context of the target's environment and defenses: Assess how the identified techniques and stages could be applied in the context of the target's environment and existing defenses. Determine if any additional techniques or stages should be considered.

2.3 Select appropriate techniques and stages for each part of the integrated Attack Flow: Based on your analysis, choose the most relevant and effective techniques and stages to include in the integrated Attack Flow. This will provide a more detailed representation of the adversary's potential actions throughout the cyber attack.

By the end of Step 2, you will have refined and improved the integrated Attack Flow, providing a more accurate and comprehensive representation of the adversary's potential actions during a cyber attack against the target organization.

Step 3

Step 3 is to develop a theoretical offensive strategy, as you've described. I'll provide a summary of the sub-steps:

3.1 Design attack scenarios: Describe how the selected MITRE ATT&CK techniques and Cyber Kill Chain stages can be applied in each part of the integrated Attack Flow.

3.2 Determine resources and capabilities: Identify the resources and capabilities needed to execute the attack scenarios.

3.3 Assess countermeasures and challenges: Evaluate potential countermeasures and challenges in executing the attack scenarios.

3.4 Discuss strengths and weaknesses: Analyze the strengths and weaknesses of both the Cyber Kill Chain and MITRE ATT&CK methodologies in the context of the attack scenarios.

In this step, you will create a theoretical offensive strategy by designing attack scenarios, determining the resources and capabilities needed, assessing potential countermeasures and challenges, and discussing the strengths and weaknesses of both methodologies.

Step 4

Step 4: Analyze the impact on the target and potential defensive measures

4.1 Evaluate the potential impact of the attack scenarios on the target's assets and operations

4.2 Identify artifacts and signatures generated by the cyber offensive activities

4.3 Suggest improvements to the target's security posture by addressing vulnerabilities and implementing effective countermeasures

4.4 Provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships

This step focuses on understanding the consequences of the attack scenarios, identifying evidence of the cyber offensive activities, recommending improvements to the target's security posture, and providing strategic guidance to policy makers.

Step 5

5. Document your findings: Prepare a comprehensive documentation of the potential vulnerabilities, offensive strategies, and outcomes using the MITRE ATT&CK framework. Include any additional steps that would be taken if not bound by legal constraints.

5.1 Write the executive summary

5.2 Write the introduction, including scoping and document structure

5.3 Describe and justify the chosen target, goal, and integrated Attack Flow

5.4 Detail the chosen strategy and approach using the MITRE ATT&CK techniques and Cyber Kill Chain stages

5.5 Present the results of your analysis, including attack scenarios, impact, and defensive recommendations

5.6 Discuss the strengths and weaknesses of both methodologies in relation to your work

5.7 Relate your work to the course material and learning outcomes

5.8 Write the conclusions

5.9 Compile and format the references using the APA referencing system

Step 6

6. Relate your work to the course material: Analyse your findings in the context of the course material, addressing the four learning outcomes (LO1, LO2, LO3, and LO4) and emphasizing the use of offensive cyber security tradecraft from the MITRE ATT&CK framework.

Step 7

7. Write the report: Prepare a technical report that includes an executive summary, introduction, target/goal description and justification, chosen strategy/approach, results of your activities, a section on how your work relates to the course material, conclusions, and references. Adhere to the maximum word count and formatting guidelines.

Step 8

8. Review and edit: Proofread your report and ensure it is well-structured, logical, and concise. Ensure that all references are cited correctly using the APA referencing system.

Step 9

9. Submit your assignment: After completing all the steps and ensuring that your report adheres to the guidelines, submit your assignment by the specified deadline.