Name: Coral S. Schmidt Montilla ID: 148830

Assignment instructions

Objective:

Upon completion of this activity, you will be able to create an attack tree technique to analyze a given threat.

Student Instructions:

Please complete the assignment. This activity is worth 30 points. You will have only one opportunity to complete the activity.

1. [You will build your own attack tree. It may be textual or graphic. You will Identify a cybersecurity-relevant goal (it must be different than the ones presented in class). Then, you will need to identify the possible attacks, identify the measures or tasks needed for the goal or attack to take place.](#_1.)
2. [In your work describe:](#_2.)

* [The asset or objective your analysis tends to and its context, i.e. database in a cloud system for a coffee store.](#_2.)
* [The attacker’s motivations you included in your analysis.](#_2.)
* [Briefly, offer reasoning for your overall analysis.](#_2.)

# 1.

Text Format:

Goal: Gain access to Blackboard portal – Polytechnic University of Puerto Rico

├── Phishing attack

│ └── Create fake university login page

│ └── Send email pretending to be university IT

│ └── User submits credentials

├── Credential stuffing

│ └── Use leaked university emails

│ └── Attempt login with commonly reused passwords

├── Social engineering

│ └── Impersonate student on phone call to IT support

│ └── Request password reset or account info

├── Exploit software vulnerability

│ └── Scan Blackboard login for weaknesses (e.g., SQL injection)

│ └── Inject malicious code

├── Public Wi-Fi attack

│ └── Set up fake Wi-Fi near campus

│ └── Capture login credentials through MITM attack

Graphic Format:

# 2.

The focus of this analysis is the Blackboard portal used at the Polytechnic University of Puerto Rico, San Juan campus. As a cloud-based academic platform, Blackboard manages everything from grades and assignments to communication between students and professors. Because it handles sensitive student data and academic records, it’s a high-value target for attackers looking to exploit personal information, manipulate grades, or disrupt university operations. Since it's accessed constantly by both students and faculty, it's also one of the most exposed entry points into the university’s digital infrastructure.

From an attacker’s perspective, the motivations could range from personal gain to curiosity or even clout-chasing. A student might want to alter grades or due dates, while a more experienced hacker might target the portal to gather login credentials for phishing campaigns, identity theft, or to explore internal systems. Social engineering, phishing, and credential stuffing are especially attractive because they don’t require advanced technical skills—just some creativity and good timing.

Overall, this attack tree highlights how different tactics can be used depending on the attacker’s skill level and goal. Low-effort attacks like phishing or password reuse are more likely to succeed due to common human errors, while higher-effort methods like exploiting software vulnerabilities take more skill but could have a bigger payoff. Recognizing these paths helps us as future professionals design smarter defenses like MFA, tighter user verification, and awareness campaigns that actually stick.