

GenAI: Cybersecurity Investigation Unit

Due: Tue Jan 13, 2026 3:30pm

Late **20/20 Points**

Attempt 1



Review Feedback

SUBMITTED: Jan 15, 2026 3:33pm

Attempt 1 Score:
20/20

Anonymous Grading: no

2 Attempts Allowed

Available: Jan 13, 2026 10:30am until Jan 31, 2026 11:59pm

▼ Details



Cybersecurity Investigation Unit

GenAI Simulation: Authentication Attack Analysis



Mission Overview

Welcome, Bootcamp Cyber Analyst . You've been assigned to investigate authentication breaches. Your cases will be personalized based on YOUR interests, and you'll need to identify which authentication fact

Activity Type: Investigation | Estimated Time: 35 minutes

What You'll Need



Google Gemini
Access
gemini.google.com



[Simulation Prompt File](https://myncca.instructure.com/files/2564641?wrap=1) (<https://myncca.instructure.com/files/2564641?wrap=1>). [Download](https://myncca.instructure.com/files/2564641/download?download_frd=1) (https://myncca.instructure.com/files/2564641/download?download_frd=1)

[Download from this assignment](https://myncca.instructure.com/files/2564641?wrap=1) (<https://myncca.instructure.com/files/2564641?wrap=1>). [Download](https://myncca.instructure.com/files/2564641/download?download_frd=1) (https://myncca.instructure.com/files/2564641/download?download_frd=1) https://doctreader.readspeal.com/1164dd3c3968%2FActivity_1_1_2.Authentication_Simulation.txt%3Ftoken%3DeyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9eyJpYXQiOjE3NjkwOTU1NjMsInVzZXJfaWQiOm51bGwsInJlc291cmNljoil2ZpbGVzLzhYml5Nzl1LWF1

⚙️ Setup Instructions

1. Download the simulation prompt file attached to this assignment
2. Open Google Gemini at gemini.google.com (https://gemini.google.com)
3. Start a new chat (click "+ New chat" if needed)
4. Upload the prompt file by clicking the attachment icon (📁)
5. Type: **Start the simulation**
6. Follow Agent Williams' instructions throughout

💡 How the Simulation Works

Phase

What Happens

Phase 1

Interest Discovery - AI asks about your hobbies

Phase 2

Case Assignment - 3 personalized scenarios

Phase 3

Investigation - Analyze and identify factors

Phase 4

Summary & Final Question

Phase 5

Completion Screen

📘 Authentication Factors - Quick Reference

Factor

Examples

Something You KNOW

Password, PIN, security question

Something You HAVE

Phone, smart card, security key

Something You ARE

Fingerprint, face scan, retina

 Pro Tips

- Be specific about your interests - it makes better scenarios!
- Read carefully - the attack details reveal which factor was compromised
- Use vocabulary - terms like "brute force" and "social engineering" help
- Think prevention - MFA is usually the best defense
- Screenshot the end - you need the completion screen for submission

 Submission Requirement

Screenshot your completion screen and submit it to this assignment.

 Due: TODAY by 3:30 PM

 CASE FILE: 1 Subject: Jordan, a semi-pro soccer player

Background: Jordan runs a popular Facebook group for local athletes and frequently buys equipment online.

Incident Report: Jordan saw a Facebook ad for "90% off Elite Cleats" and clicked the link. It took him to a login page that looked exactly like his usual sporting goods store. He typed in his username and password. The next day, his account was drained, and the password had been changed by someone else.

 CASE FILE: 2 Subject: Alex, a fantasy football league commissioner

Background: Alex manages large sums of money for the league and uses a mobile app for all transactions and shopping.

Incident Report: While Alex was cheering at a crowded sports bar, he left his smartphone on the table to go to the restroom. When he returned, the phone was gone. An hour later, his bank notified him that a "password reset" code sent via SMS text message was used to access his accounts, even though he never shared his password.

 CASE FILE: 3 Subject: Casey, a high-tech gym member

Background: Casey attends a luxury fitness center that uses advanced biometrics for entry to prevent membership sharing.

Incident Report: To enter the locker room where members store their wallets and shopping bags, Casey scans a fingerprint on a sensor. An attacker managed to lift a latent fingerprint from Casey's water bottle, created a synthetic mold, and used it to bypass the scanner and access the secure area.

◀ Previous

(<https://myncca.instructure.com/courses/6068/modules/items/1586903>)

New Attempt

Next ▶

(<https://myncca.instructure.com/courses/6068/modules/items/1586909>)

