CIS 350: AI for Cybersecurity

Activity 2 Worksheet: Hacker101 - Authentication

Activity Overview

In this activity, you will watch the Hacker101 lesson on weak password storage and authentication, then answer questions to deepen your understanding of real-world authentication vulnerabilities. You'll also design a secure password policy for a hypothetical company.

Warm-Up (5 min): Predict, Then Pair-Share

Before watching, write your gut answers. Then compare with a partner - you will revisit these after the lesson to see what changed.
- When you type your password into a website, how do you think the site stores it? Should the company be able to see your actual password?
- One prediction: what is the single biggest mistake you think companies make with passwords?

Task 1: Watch the Hacker101 Lesson

Resource: Hacker101.com - Lessons - 'Weak Password Storage and Authentication'
Duration: ~15 minutes

As you watch, take notes on:
- How passwords should be stored (vs. how they're often stored)
- What 'hashing' means and why it's important
- Why adding a 'salt' to passwords helps
- Real-world examples of authentication breaches

Task 2: Guided Questions

Q1: What is the difference between encryption and hashing?

Q2: Why is plaintext password storage dangerous? (Give two reasons)

Q3: What is a 'salt' in password hashing? Why does it help?

Q4: What is a 'dictionary attack'? How does it work?

Q5: From Lab 1, our dataset showed 77.1% password reuse. If one website is breached, what happens to users who reuse passwords?

Task 3: Analyze Passwords from Lab 1

In Lab 1, you analyzed real password data. Recall the findings:
- Average password length: ~7.4 characters
- Longest password: 25 characters
- 65.7% of passwords were weak (less than 8 characters)

Questions:
1. Why are short passwords (less than 8 characters) weak? What attacks would be effective?

2. If passwords are hashed with bcrypt, does the length matter as much? Why or why not?

3. From the Hacker101 lesson, what's the best way a company can protect users if one of these weak passwords is exposed in a breach?

Checkpoint (2 min): Discuss With a Partner

Before you design your policy, check your understanding out loud with a partner:
- In one sentence each, explain hashing, salting, and why password reuse is so dangerous.
- If you disagree or get stuck, note the question here and bring it to the whole-class discussion.

Task 4: Design a Secure Password Policy

You are a security engineer at a bank. The CEO asks you to design a password policy that balances security and usability. Write a policy with 5-7 requirements.

Your Policy (use numbered list):

Explain your choices: Why did you choose these specific requirements? How do they protect against the attacks from the Hacker101 lesson?

Task 5: Reflection

Q1: What surprised you most about authentication vulnerabilities? Why?

Q2: If you were designing a new social media platform, what would you do differently from the companies mentioned in the Hacker101 lesson?

Q3: What is one thing you'll change about your own password habits after learning about authentication attacks?

Grading Rubric (20 points)

Criterion	Description	Points
Completion	Lesson watched; all tasks and questions attempted	8
Understanding	Q&A answers demonstrate learning from the lesson	7
Application	Password policy is practical, secure, and well-explained	5

Total: 20 points

Scoring: Completion (8) + Understanding (7) + Application (5) = 20 points

How to Submit

1. Complete all tasks in this worksheet
2. Ensure all questions are answered thoughtfully
3. Submit this PDF on Canvas by [DUE DATE]

Questions? Post in the course forum or attend office hours!