Whatcom COMMUNITY COLLEGE

NCYTE CENTER

IDENTITY, AUTHENTICATION, AND AUTHORIZATION

Nancy Stevens, First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

IDENTITY, AUTHENTICATION AND AUTHORIZATION

IDENTITY CRISIS

This lab introduces problems related to credential-based attacks. The lab presents the scope of these attacks through statistical data and data visualizations. Students research attack methods and understand ways in which attackers gain unauthorized access to systems and data. The lab is the first step in understanding the importance of authentication and authorization, which are examined further in the second lesson.

LAB ENVIRONMENT

Students develop an understanding of identification, authentication, and authorization concepts in cybersecurity. They examine examples of cybercrime and develop an understanding of the magnitude of credentials-based cybercrime. The activities include visiting the website, https://haveibeenpwned.com/ and https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. Students research several attack methods including keyloggers, malware, malicious web links, rogue access points, and other techniques.

LAB FILES NEEDED

- 02.IdentityAuthenticationAuthorization_Presentation.pptx
- 03.IdentityAuthenticationAuthorization_IdentityCrisis_Activity.docx
- 04.IdentityAuthenticationAuthorization_IdentityCrisis_Activity_Solutions.docx

WARM UP ACTIVITY

Students will engage in a Think-Pair-Share activity as they answer these questions: How do people know who you are? How do you prove who you are? What are some examples of access based upon proving your identity?

The warmup activity is designed to get students thinking about the concepts of identification, authentication, and authorization.

Examples of data breaches and credential-based crimes are presented in a series of slides. Definitions are presented to provide the background for the learning activities.

PWNED ACTIVITY/STEP 1

Students visit the Have I Been Pwned website and enter in an email address to see if it has been reported in a data breach or hack. If students' have been involved in a breach, the websites are listed further down the page. Place emphasis on the potential impact of reused passwords once a breach has occurred. A hacker can run a script and brute force attack websites using the usernames and passwords from a successful attack. A guiding question is provided to lead the discussion: What are the possible effects to an individual whose data has been exposed to persons that should not be able to view it?

VISUALIZING DATA BREACHES & HACKS/STEP 2

Students visit the "World's Biggest Data Breaches & Hacks" David McCandless website and examine the timeline and growth of attacks. As students hover over an attack, details of the breach will be displayed. The following guiding questions are provided for this exploration activity:

- **What do you notice?**
- **What do you wonder?** *What are you curious about that comes from what you notice in the graphs?*
- **What might be going on?**

RESEARCH ACTIVITY/STEP 3

Students research attack methods to gain an understanding of how unauthorized access is gained. Some websites are provided for research. A worksheet (located at the bottom of this document) is provided for the research activity. This activity could be jigsawed. Assign groups of students a particular topic, and then students share what they learned with the whole class. This method enables students to gain an understanding of all of the topics.

WHAT TO SUBMIT

Students conduct research and submit a document. A solution is provided in a separate document.

Name:_____

RESEARCH ACTIVITY

How do attackers gain unauthorized access?

Recommended sources for research:

- Open Web Application Security Project (OWASP) List of Attacks
- National Cyber Awareness System (CISA)
  - "Securing Wireless Networks" Security Tip (ST05-003)

1. Keylogger:
2. Credential Stuffing:
3. Shoulder Surfing:
4. Social engineering:
5. Pretexting:
6. Malware:
7. Phishing:
8. Malicious links:
9. Brute force:
10. Piggybacking:
11. Rogue Access Point:
12. Evil Twin Attack:
13. Packet Sniffing:
14. Weak passwords:
15. Physical theft: