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

LET ME IN

This lesson follows the "Identity Crisis" lesson and helps students develop an understanding of authentication and authorization. Students will think about how they protect their data and devices through a Think-Pair-Share activity. Definitions of security controls, authentication, and authorization are presented through the PowerPoint slides. Students will explore the most common passwords with the intent of understanding "weak" versus "strong" passwords. Password strength is examined through two websites in which students can "test" passwords. The NIST password guidelines are summarized on a slide. After reviewing a security document on passwords, students will create a digital artifact designed to educate people on password security. Multifactor authentication, authorization, and the principle of least privilege is presented in the remaining PowerPoint slides.

LAB ENVIRONMENT

Students will develop an understanding of ways to protect devices and data, distinguish between authentication and authorization, identify three types of Multifactor authentication (knowledge, possession, inheritance), and describe what defines a strong password. The activities include access to several websites,

- Wikipedia "List of Most Common Passwords".
- How Secure is My Password (Dashlane Password Manager).
- The Password Meter
- "Choosing and Protecting Passwords" Security Tip ST04-002 (CISA).

FILES NEEDED

IdentityAuthenticationAuthorization_LetMeIn_Presentation.pptx

WARM UP ACTIVITY

Present the following prompts to students in the PowerPoint:

- Define authentic.
- List synonyms for authentic.
- List antonyms for authentic.

The prompts help students construct a definition for authentication. The slide deck provides a definition to display after the discussion.

THINK-PAIR-SHARE/STEP 1

Students should think silently and independently on this question, "How do you protect your data and your devices?" After a few minutes, students should pair up and discuss their answers. Students then share their answers with the whole class. A PowerPoint slide provides possible answers. The slides provide definitions of security controls, and examples of authentication and authorization.

RESEARCH THE MOST POPULAR PASSWORDS/STEP 2

The PowerPoint provides a definition of the term, password, and then students research the most popular passwords. Challenge students to look for patterns or similarities in the passwords on the list. Encourage students to examine the list and note similarities such as simplicity, length, lack of uppercase/lowercase and symbols used, dictionary terms, and easily guessed words.

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability. Source: Wikipedia

PASSWORD STRENGTH/STEP 3

Students will visit the How Secure is My Password and The Password Meter websites to explore password strength. Provide students with 5 to 8 minutes to explore both websites. Then ask students to describe password strength. To encourage exploration of password strength, instruct students to enter in a numeric password of 5 characters and report back the results. Then instruct students to enter a single dictionary word password, and report back the results. Finally, instruct students to enter three dictionary words as a password, and report back the results. From this exercise, students should begin to understand the impact of complexity on password strength. Students may want to input

existing passwords in order to test the strength of their passwords. Encourage students to practice good password management. This means implementing strong and unique passwords for each account. Some students may comment that they "don't care" about password security. Emphasize that impersonation, identity theft, and loss of access to your account could occur.

DIGITAL ARTIFACT: ONE-PAGER/STEP 4

Students will review the NIST guidelines for password security as provided in the PowerPoint slides. Students will review a US-CERT Security document on passwords. Equipped with this information, students will create a digital artifact known as a one-pager. Students can use the provided template to either make a digital artifact or it can be created by hand. A one-pager is a combination of words and visual images to clearly and concisely share the key points or takeaways of a topic. The border of the template should contain key terms. The center block should contain a title or heading. The four quadrants should contain examples, details, vocabulary, or illustrations. Students should use the terms authentication and authorization in the one-pager.

WHAT TO SUBMIT

Students submit a one-pager artifact.

ONE PAGER ORGANIZER