Cybersecurity

Operations and Incident Response

4.1.7 Password Cracking Tools

What do password crackers use to determine a password?

Overview
Given a scenario, the student will use the appropriate tool to assess organizational security.

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 4.1

- Given a scenario, use the appropriate tool to assess organizational security.
    - Password crackers

Password Cracking Tools

Password crackers use dictionaries, rainbow tables, and brute force attempts to determine a password. Weak passwords are usually the primary target of malicious attempts. Security-minded system administrators will occasionally audit their users' passwords and attempt to crack easy passwords. The administrator will take the password hashes, run them through a password cracker tool, and see which passwords were easily solved/cracked. Those users can then be notified to use stronger passwords.

One example of a password cracker is John the Ripper (JTR). JTR is a free and open source tool for Linux and macOS; however, there is a pro version which contains extra features that users can pay for. A default JTR attack will take a set of password hashes and run them through three tests in an attempt to crack/solve the passwords. It will first simply try the username as the password, then it will run the passwords through a dictionary of thousands of commonly used passwords, and then finally it will begin a brute force attack. A similar tool to JTR for Windows and Android OS is the Hash Suite tool. Similarly, this is a free and open sourced tool that also has a pro version that is not free, but contains extra features. Other password crackers include Medusa, Ncrack (or just Crack), Hashcat, Mimikatz, and many more.