Why is Cybersecurity Training Important?

Cyber Security Training

- Training can simulate realistic cyber-attacks in a controlled environment, allowing students to practice responding to various types of security threats
- The accessibility of the cloud gives users the access virtual machines and other resources without having to invest in hardware or infrastructure
- a cloud-based training range can be easily scaled up or down, depending on the number of students or the complexity of the exercises
- this makes it easy for instructors to provide personalized training to individual students or groups of students, without having to worry about resource limitations.

Why is it important for a cyber security training range to feature offensive security?

- Users can gain a better understanding of how attackers think and operate, allowing them to develop more effective defensive strategies to protect against attacks

- by simulating attacks in a controlled environment, users can test the effectiveness of their defenses and identify potential weaknesses, and make improvements to their security measures before an actual attack occurs

- requires users to think creatively and critically to identify vulnerabilities and exploit them – these skills can be applied to other areas of cyber security such as incident response and threat analysis

Password Crackers

What are Password Crackers?

Password cracking tools are applications designed with the purpose of revealing or recovering password authentications used for access to networks, web applications, files and more.

Why were they created?

As technology advanced, so did the techniques used by cyber criminals to crack passwords. Security professionals developed various password cracking tools to test the security of password systems.

Password Crackers

Who pioneered password cracking technology?

One of the earliest password cracking tools was Crack, developed in the 1990s by Alec Muffett.   As computer systems evolved, security professionals developed more advanced password cracking tools that used more sophisticated techniques to crack passwords.

Password Crackers

How do password crackers work?

To guess or crack passwords, cracking tools employ use various techniques, such as:

- brute force: a technique in which the password cracking tool tries all possible combinations of characters to guess the correct password
- dictionary attack: a technique in which the password cracking tool uses a pre-built list of words to guess the correct password
- hybrid attack: a technique that combines the brute force and dictionary attacks
- a rule based attack: a technique that involves creating custom rulesets that define the structure of the password, such as the length, character set, and position of specific characters

Password Cracking: Statistics

According to a study by Verizon, weak or stolen passwords are responsible for 81% of hacking related breeches.

The same study also reported that the most commonly used password is “12345” followed by the word “password.”

In 2019, NordPass analyzed over 500 million passwords and found that the average person has 70-80 passwords, and 54% of them are weak.

In 2020, the Cybersecurity and Infrastructure Security Agency (CISA) reported a 2,000% increase in brute-force attacks against Remote Desktop Protocol (RDP) systems, which allow remote access to computers.

In the same year, a researcher found that a botnet called "Perfected Password Guessing" had compromised over 100,000 Microsoft Exchange servers by using a password cracking tool.

Password Cracking: Why use it?

Password crackers can be used as a part of a penetration testing exercise to identify vulnerabilities in computer systems and networks.

By attempting to crack passwords, security professionals can determine if there are any weak passwords that could be exploited by attackers.

Password crackers can be used to audit the strength of passwords in a computer system or network.

Password crackers be used to recover lost or forgotten passwords.

In situations where a password has been lost or forgotten, password cracking tools can be used to recover the password by attempting to guess or crack it.

Password Cracking: John the Ripper

John the Ripper is a popular password cracking tool used by security professionals to test the strength of passwords. It is capable of cracking a wide variety of password hashes, including those used by UNIX, Windows, and other operating systems.

How does John the Ripper work?

John the Ripper uses different hashing algorithms, including MD5, SHA-1, and bcrypt.

The program needs to be provided with a password file, which contains hashed passwords.

Password Cracking: Hashcat

Hashcat is a free, open-source password cracking tool that uses multiple techniques, including brute-force attacks, dictionary attacks, mask attacks, and hybrid attacks, to crack passwords.

How does Hashcat work?

Hashcat cracks passwords from various operating systems, including Linux, macOS, and Windows, and can use different hashing algorithms, including MD5, SHA-1, and bcrypt.

Hashcat also supports advanced features, such as distributed cracking, which allows multiple computers to work together to crack passwords more quickly, and session management, which allows users to save and resume cracking sessions.

Types of Network Scanning

Passive Scanning/Packet Sniffing

Passive scanning or packet sniffing, which captures and tracks the traffic moving over the network in the form of data packets. Passive scan tools are a type of security tool that monitor network traffic and identify vulnerabilities without actively interacting with the system.

Active Scanning

Active network scanning tools are a type of security tool that actively probes and interacts with the system to identify vulnerabilities and security issues in your AWS environment.

AWS Inspector

- AWS inspector is an automated and continuous vulnerability scanning service that assesses applications deployed on AWS.

- Inspector uses a set of predefined rules to assess the security of your applications, including network configuration, operating system vulnerabilities, and application security.

- Generates a report with a list of security issues and recommendations for remediation.