ECS
Serving Your IT Needs

Types of Cyber Attacks

Cyber-attacks are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others. From installing Spyware on a computer to obliterating a company's entire infrastructure, cyber-attacks can have devastating effects on many.

Password Attacks

Passwords are intended to prevent unauthorized access to your accounts, so it's important to use passwords that are strong in order to prevent threats against the privacy and security of the data associated with your company and customers.

Why is it important to use a strong password?

There is software available to hackers that will allow them to try various passwords in an attempt crack the code of, and infiltrate your system.

How to protect your business:

- Create a password that is easy for you to remember but difficult for someone else to figure out
- Include upper- and lower-case letters, numbers, and symbols
- Craft a password that is long
- Regularly update your password

Denial of Service (Dos) Attacks

Denial of service attacks are just as its name states.Its goal is to make a network unavailable to its intended users.

This type of attack can be used against individuals where they consecutively enter the wrong password enough times that they are locked out of their account. It can also manifest as a network being so overloaded that no one can get in.

Damage caused by denial-of-service attacks:

- Network performs slowly
- A specific website is inaccessible
- No websites are accessible
- Receiving a large amount of spam emails

Passive Attack

A passive attack is conducted to simply find the vulnerabilities of a system, but not change any data at that time. Think of it in terms of a conversation that two people are having and the passive attacker is eavesdropping in on the conversation. Although it may seem like a harmless act at the time, if the intruder is able to obtain the “right” information, they can use that in the future to cause irreparable damage.

A passive attack is different from an active attack, which aims to change data of the system at the time of the attack.

Penetration Testing

Penetration testing can be a positive tool for an organization. It is done to unearth the vulnerabilities of a computer system, then take advantage of those vulnerabilities to get an idea of the impact an actual attack will have on the system.

There are many reasons why a company would utilize penetration testing. Some of these include:

- Establish the likelihood of a specific attack occurring
- Detect high risk vulnerabilities that can result from a grouping of low-risk vulnerabilities that take place in a particular pattern
- Determine the bearing an attack will have on a company
- Assess the company's network risk management capabilities

Practical Illustration

Kurt and Jeff are new hires with Bob's Electronics. They are at their desks, setting up their computer passwords. Kurt tells Jeff he should create a password that is long and includes letter, numbers, and symbols, so it will be difficult for others to figure out. Jeff said he doesn't trust his memory to such a password and will probably create one that just has letters. Three months later, Jeff notices he has started receiving a lot of spam in his inbox. A week after, he tries to login to his system by inputting his password, but it locks him out after several failed attempts, and he has to call technical support for assistance.

Review Questions

1. You should create a password that is:
    a. Easy for you to remember and easy for others to figure out
    b. Difficult for you to remember but easy for others to figure out
    c. Easy for you to remember but difficult for others to figure out
    d. Difficult for you to remember and difficult for others to figure out

2. What should your password include?
    a. Upper- and lower-case letters
    b. Upper- and lower-case letters, numbers, and symbols
    c. Numbers and symbols
    d. Upper case letters, numbers, and symbols

3. What is a denial-of-service attack?
    a. An attack that prevents unintended users from being able to access a network
    b. An attack that prevents users from being able to access a network in the early morning hours only
    c. An attack that prevents users from being able to access a network in the late-night hours only
    d. An attack that prevents intended users from being able to access a network

4. Which of the following is not mentioned in the “Denial of Service Attack” lesson as damage that denial of service attacks can cause?
    a. Network performs slowly
    b. A particular website is inaccessible
    c. Receiving a large amount of spam emails
    d. None of the above

5. What is the purpose of a passive attack?
    a. To find network vulnerabilities and immediately change data
    b. To warn the network user of an impending active attack
    c. To find network vulnerabilities but not change data at the time
    d. To warn the network user of vulnerabilities so the user can fix them

6. In the lesson, passive attacks are likened to:
    a. Eavesdropping
    b. Murder
    c. Downloading
    d. Overloading

7. What is penetration testing used for?
    a. In a controlled environment, to find vulnerabilities in the network, but not exploit them
    b. In a controlled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have
    c. In an uncontrolled environment, to find vulnerabilities in the network and exploit those vulnerabilities to see what impact an actual attack would have
    d. In an uncontrolled environment, to find vulnerabilities in the network, but not exploit them

8. Which of these is discussed in the “Penetration Testing” lesson as a reason that companies implement such testing?
    a. Establish the likelihood of a specific attack occurring
    b. Detect high risk vulnerabilities that can result from a grouping of low-risk vulnerabilities that take place in a particular pattern
    c. Determine the bearing an attack will have on a company
    d. All of the above

9. _____ are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others.
    a. Cyber attacks
    b. Personal attacks
    c. A and B
    d. None of the above

10. Receiving a large amount of spam mail and being locked out of the system after putting in the correct password, but not given access are characteristic of which of the following?
    a. Password attack
    b. Denial of service
    c. Denial of service and password attack
    d. None of the above
11.