Social engineering and password based attacks

S.P.I.R.I.T
- ✓ **Independence**
- ✓ **Perseverance**

Monday, 04 April 2022

Learning Intention

To develop knowledge by social engineering and give examples

To secure understanding by being able to explain password strength and how it affects attacks

To achieve excellence by using the brute force formula to calculate how long it would take to guess a password

Keywords

Web browser
a software application for accessing information on the World Wide Web
e.g internet explorer, Safari, Chrome

Tier 2 word – deception
the action of deceiving someone

Social Engineering

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

- Uses deception to gain information from someone
- Social engineering involves tricking a user into giving out sensitive information such as a password, by posing as a legitimate system administrator.

Examples:

- **Phishing** - an attempt to acquire users' details using fake emails and websites

https://www.youtube.com/watch?v=opRMrEfAIiI

To develop knowledge by social engineering and give examples

Passwords

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

- **Passwords** are commonly used to **prove a person's identity** to a computer system, thus allowing them access to relevant data.

- Most computer programs require users to use
  - **upper and lower case** alphanumeric
  - **non-alphanumeric** characters such as @ ! ~ - / \ %, for example 'P@55word/1234!'.

To secure understanding by
being able to explain password strength and how it affects attacks

Password-Based Attack

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

Dictionary attack	This **uses a simple file containing words found in a dictionary**. This attack uses exactly the kind of words that many people use as their password.
Brute force attack	Works through **all possible alphanumeric combinations** from aaa1 to zzz10. ***It's not quick, but it will uncover your password eventually.***
Guess ???	A user-generated password is unlikely to be random. Passwords are likely to be based upon our interests, hobbies, pets, family etc. **Educated guesses often work.**

To secure understanding by being able to explain password strength and how it affects attacks

Passwords: Brute Force attack

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

- A hacker may have access to programs that have the ability to try multiple guesses in quick succession.

- This is known as a **brute force attack**.

To secure understanding by
being able to explain password strength and how it affects attacks

- Passwords that use a combination of upper and lower case alphanumeric characters as well as other non-alphanumeric character, will be much harder to guess and will take longer to 'brute force'.

Passwords : Brute Force attack

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

- The following formula can be used to determine the number of attempts it would take to *brute force* a password.

$$Attempts = Number\ of\ characters^{Password\ length}$$

- So a password, such as 'computer' (8 characters), which only contains lower case characters from the 26 letter English alphabet will take:

$$Attempts = 26^8 = 208{,}827{,}064{,}576$$

(on a typical 3.5GHz computer, this would take less than 6 seconds to brute force)

To secure understanding by being able to explain password strength and how it affects attacks

Passwords: Brute Force attack

S.P.I.R.I.T
- ✓ Independence
- ✓ Perseverance

- Whereas a password that contains upper and lower case alphanumeric characters, such as ‘Computer1’ (9 characters),
- has 26 (upper) + 26 (lower) + 10 (numbers) = 62 possible characters. This will take:

$$Attempts = 62^9 = 13{,}537{,}086{,}546{,}263{,}552$$

(on a typical 3.5GHz computer, this would take just over 1 hour to brute force)*

To secure understanding by being able to explain password strength and how it affects attacks

Ways to Protect

S.P.I.R.I.T
- ✓ **Independence**
- ✓ **Perseverance**

- **Keep your operating system up to date**.
  New ways to bypass the operating system's built-in security are often discovered and can be covered ***by installing the security patches*** issued by the operating system manufacturer.

*A **patch** is a set of changes to a computer program or its supporting data designed to update, fix, or improve it*

- **Use the latest versions of web browsers**.
  The manufacturers of web browsers seek to continually improve their products and remove possible security vulnerabilities. Most browsers will download updates automatically, but will need a restart for the update to be installed.

- **Look out for phishing emails**. Emails that ask you to confirm personal details are usually fakes. They should be caught by the spam filter, but be suspicious and do not provide any sensitive information.

- If you suspect you have malware on your computer you will need to download and run a **malicious software removal tool** that should detect and remove malware not blocked by the anti-virus software.

Social engineering Task

S.P.I.R.I.T
- ✓ **Independence**
- ✓ **Perseverance**

Write a <u>short guide</u> about Social engineering

- **It should cover**
  - What is Social engineering?
  - What is Phishing.
  - How you can prevent a criminal from getting your data from phishing (see slide 9)

<u>To develop knowledge</u> by social engineering and give examples

Password tasks

S.P.I.R.I.T
- ✓ **Independence**
- ✓ **Perseverance**

1. Use slide 2 to explain and give examples for passwords
2. Explain what a Brute force attack is.
3. Write the formula which is used to determine the number of attempts it would take to brute force a password
4. **Using Brute Force, write the formula** out for the following passwords:

   (Don't need to calculate it just tell me how it would be worked out)

   1. Password
   2. pAssWord232
   3. qwertyuiop

   example:

   password = computer
   is 8 characters long with 26 possible lower case letters

$$26^8$$

Excellence: *use this formula to calculate the number of attempts*

To secure understanding by being able to explain password strength and how it affects attacks

To achieve excellence by using the brute force formula to calculate how long it would take to guess a password