Threats: Dos, SQL and interception

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

Monday, 04 April 2022

Learning Intention

To develop knowledge by Identifying other risks to data and networks

To secure understanding by describing key features of interception, Dos and SQL attacks

To achieve excellence by Transforming key information about these treats into a suitable format

Keywords

Server
a computer or device on a network that manages network resource

Task

S.P.I.R.I.T

✓ Independence

✓ Perseverance

- Create a double page information sheet which explains the **risks** and **ways to stay secure**.
- It should cover:
  - **Technical weakness**:
    - DoS attack
    - SQL injection
    - Interception
  - **Ways to stay secure**

Learning Intention

To develop knowledge by Identifying other risks to data and networks

To secure understanding by describing key features of interception, Dos and SQL attacks

To achieve excellence by Transforming key information about these treats into a suitable format

Data Interception & Theft

Definition

Unauthorised taking or interception of computer-based information.

Each time any communication is **sent** across a network, it is **split** up into **packets** and sent by various routes. As they travel from one part of the network to another, they are at **risk** of being **intercepted, read, altered or deleted**.

How to intercept data

One way data can be intercepted is if someone uses some **hijacking software** and **pretends** to be the destination for communications across a network.

Another way is for a user to use '**packet sniffing**' software to monitor network traffic and **intercept** those packets it is interested in. People using packet sniffers are especially looking for plain text files, **passwords** and set-up information being set across the network, which they can **steal** and extract **information**.

DoS Attack

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

https://www.youtube.com/watch?v=OhA9PAfkJ10

- Denial of service (DoS) attacks
- **do not** attempt to break system security,
- **they attempt to make your website and servers unavailable** to legitimate users, by swamping a system with fake requests—usually in an attempt to exhaust server resources.

- A DoS attack will involve a single Internet connection.

<u>To develop knowledge</u> by
Identifying other risks to data and networks

<u>To secure understanding by</u>
describing key features of interception, Dos and SQL attacks

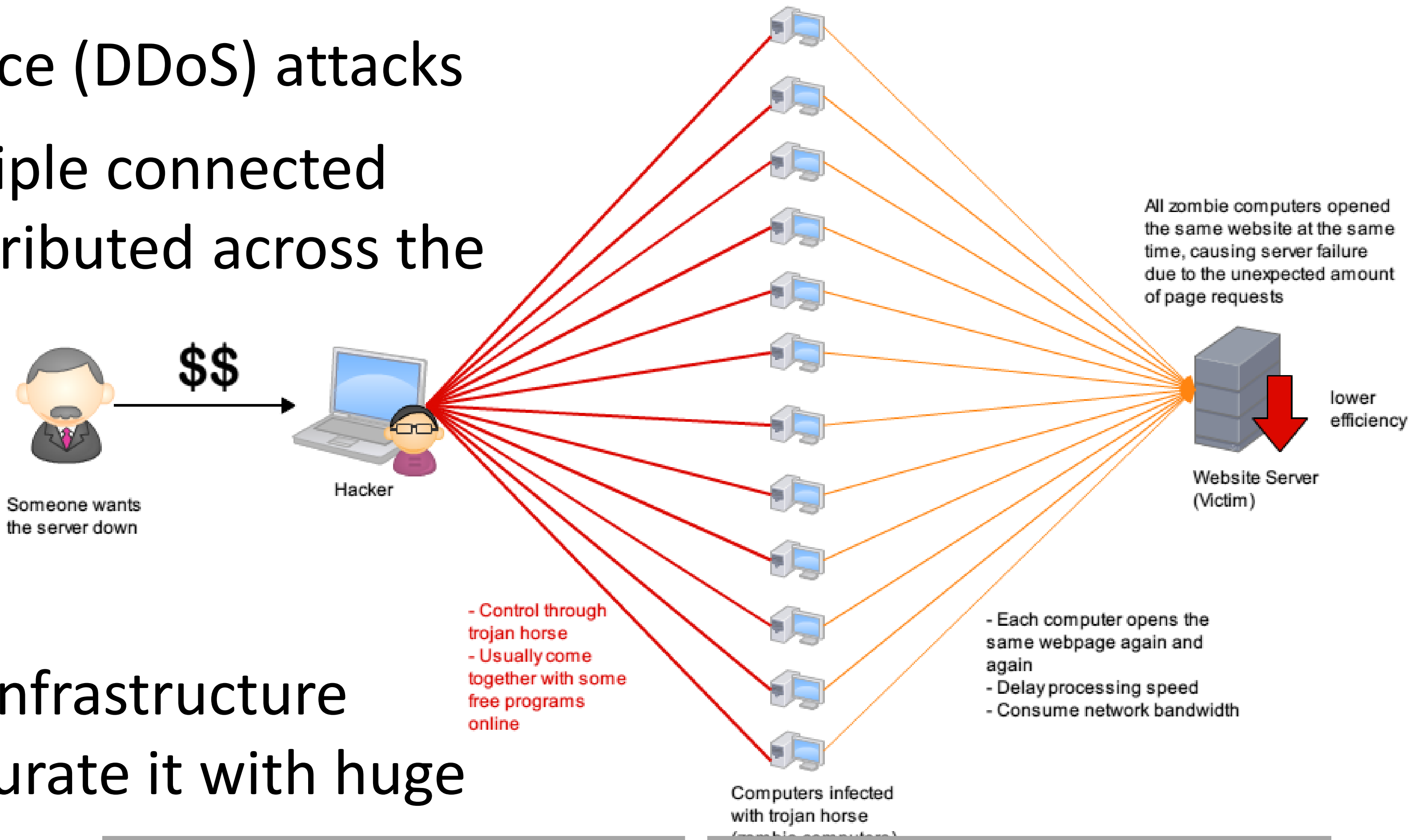
DDoS Attack

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

Distributed Denial of Service (DDoS) attacks

- launched from multiple connected devices that are distributed across the Internet.

- These multi-person, multi-device attacks target the network infrastructure in an attempt to saturate it with huge volumes of traffic.


$$
Someone wants the server down
Hacker
All zombie computers opened the same website at the same time, causing server failure due to the unexpected amount of page requests
lower efficiency
Website Server (Victim)
- Control through trojan horse
- Usually come together with some free programs online
- Each computer opens the same webpage again and again
- Delay processing speed
- Consume network bandwidth
Computers infected with trojan horse

<u>To develop knowledge</u> by
Identifying other risks to data and networks

<u>To secure understanding by</u>
describing key features of interception, Dos and SQL attacks

SQL Injection

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

- SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input.
- Injected SQL commands can alter SQL statements and compromise the security of information held in a database.
- http://www.bbc.co.uk/news/business-13636704

To develop knowledge by
Identifying other risks to data and networks

To secure understanding by
describing key features of interception, Dos and SQL 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.