**Case Project 5-1**

[Distributed Denial of Service (DDoS) attacks](https://www.vxchnge.com/blog/how-to-protect-data-centers-from-a-new-generation-of-ddos-attacks) became more common and frequently used strategy from hackers to slow or take down a web site or a server to create chaos and disruption. The companies are targeting to improve their network security accordingly to mitigate the impact of DDOS attacks and to protect their business and their customers.

The most famous recent DDOS attacks are:

1. GitHub (2018)

GitHub is a popular code repository management platform for version control and collaboration that is used by millions of developers, GitHub is used to high traffic and usage. It is flooded with 126.9 million packets of data per second. This attack was recorded as “biggest DDoS attack”. GitHub was down for about 20 minutes. The impact was controlled while GitHub utilized a DDoS mitigation service that detected the attack and quickly was able to minimize the impact.

1. Dyn (2016)

Dyn is a leader DNS provider. It worked with several major companies, such as Netflix, PayPal, Visa, Amazon, and The New York Times. Hackers used a malware called Mirai and created a massive botnet to launch the largest recorded DDoS attack at that time. The attack had a massive impact on Dyn’s customers due to DNS errors when Dyn’s servers went down. The problems were sorted out and service restored at the end but it was as a red flag to alert to the [fragility of network infrastructure](https://www.vxchnge.com/blog/when-servers-go-down).

1. BBC (2015)

A group of hackers called New World Hacking [launched a massive attack](https://thehackernews.com/2016/01/biggest-ddos-attack.html) against BBC’s sites and servers. The servers went down for more than three hours. Also, this attack was the biggest recorded DDoS attack at that time. The hackers used their tools on cloud computing resources (AWS servers) to launch the attack.

The most common targets for DDOS attackers are the Enterprises, the big companies or big organizations to achieve their goals and targets to cause harm and disruption among these big businesses and their massive customers.

According to an article in SecurityWeek, “By combining the direct attacks with the reflection attacks, the researchers discovered that the internet suffers an average of 28,700 distinct DoS attacks every day.

DDOS attacks can be prevented when enterprises and individual users care about security aspects and secure their devices by using strong passwords and installing anti-malware software and firewalls to prevent the devices from being a part of a botnet. Keeping the security software and hardware, operating systems and applications always up to date. Also, using the network monitoring softwares, such as NinjaRMM, Datadog, Obkio to make sure computers/systems are not part of a botnet and to be alerted when that happen.

**Case Project 5-4**

**SQL** stands for Structured Query Language. It is the standard language for relational database management systems. SQL queries are used to perform tasks such as update, insert, search and delete database records.

SQL injection is a common attack that inserts malicious SQL code for the web application database and give the attacker a complete control over it.

* These are the recent and top SQL injection attack examples:
  1. In New York, an attacker used SQL injection attack for hacking into vulnerable e-commerce websites to steal credit card information in May 2020.
  2. Number of government agencies and universities were targeted using SQL injection attack by a hacker who was involved in penetration of the US Election Assistance Commission and subsequent database sale in November 2016.([Help Net Security](https://www.helpnetsecurity.com/2017/02/16/hacker-govt-agencies-via-sql-injection/))
  3. One of the SQL injection attack stole personal information of 156,959 customers from servers of the British telecommunications’ company in October 2015. Attackers exploited vulnerabilities in the system. ([Wikipedia](https://en.wikipedia.org/wiki/SQL_injection#Examples))
* To prevent SQL injection attack, there are many steps and procedures to follow:
  1. Input validation is how to write the code in a way that can prevent and identify the illegitimate user input to enter the information system.
  2. keep the web application software up to date with the latest security patches and leaving to place for vulnerabilities.
  3. Limit the usage of database functionality that is no longer needed to prevent it from being exploited by attackers.
  4. Ensure all the database credentials are encrypted.
  5. The most important is to minimize the vulnerabilities in database system as possible.
  6. On a regular base monitor SQL statements and queries of the database-connected applications.