1. B
2. D
3. A
4. C
5. A
6. A
7. D
8. B
9. B
10. B
11. C
12. B
13. D
14. B
15. B
16. B
17. D
18. C
19. C
20. C

<u>Case Study</u>

Some of widely publicized DoS attacks are:

1. Amazon Web Service February 2020 impact:
   The attackers employed a susceptible third-party server to increase the amount of data delivered to a victim's IP address, with 2.3 Tbps. It mostly relied on CLDAP servers to magnify its traffic. Since 2016, ZDNets noted that attacks have been carried out utilizing this protocol, which is generally used to browse and edit directories shared over the internet.

2. GitHub February 2018 impact:
   The DDoS attackers utilized a memcaching approach, in which a spoofed request is forwarded to a susceptible server. It subsequently floods a chosen victim with magnified traffic with 1.3 Tbps that flooded its servers with 126.9 million packets of data each second.

3. Dyn October 2016 impact:
   Unidentified hackers used a software called Mirai to build a vast botnet that included internet of things (IoT) devices and launched the largest-ever DDoS attack using the botnet. After the attack, many of Dyn's clients' websites were crippled by DNS problems, resulting from the downtime of Dyn's servers. Even though the issues were resolved, and service was restored by the end of the day, it served as a sobering reminder of the brittleness of network infrastructure.

DDoS attacks are directed towards the following targets:

On-line systems, from commercial enterprises to government institutions, are subject to DDoS attacks. As a result of this, numerous online services have been rendered unusable. While targeted attacks are rarer, they can nonetheless occur because of a third party's instruction. The types include IP spoofing, DNS amplification attack, and SYN flood attack. Short attacks lasting only a few minutes can net you less than five euros. For a day-long attack, the client must pay at least 50 euros. The victim is frequently subjected to a variety of attacks over the course of several days or weeks.

How to defend the website against DoS attacks:

1. strengthen the infrastructure's redundancy:
   To avoid DDoS attacks, the most fundamental step people can take to make the infrastructure "DDoS obstructive" is to ensure that they have sufficient bandwidth to accommodate any spike in traffic produced by malicious activities. Thus, network monitoring software can assist in determining whether a system has become a botnet member or not. Additionally, they must always update the default password for any Internet of Things device that we install.
2. install anti-DDoS hardware and software components:
   Businesses may assist prevent their computers from becoming a botnet by implementing anti-malware software, deploying firewalls, maintaining software updates, and requiring users to use strong passwords.