Response Template for CA #3

Student Name	An Truong
Student ID	1103313636

With reference to the Dyn 2016 DDoS attack,
Question 1: **Describe the type of attack that Dyn experienced.**

On October 21st, 2016, one of the most significant cyber incidents occurred caused a global network infrastructure abuse that brought down more than 1,200 domains contracting with DYN (now is known as Oracle), one of the biggest Domain Name System (DNS) providers. The largest Distributed Denial of Service (DDoS) attack was detected as a reason for the assault of DYN. This DDoS attack, in an untraditional way, violated the network and prevented authorized accesses of users from thousands of websites via the uses of Internet of Things (IoT) devices, such as digital cameras, home routers, internet protocol or DVR players, instead of computers. The attack is considered to be the largest of its kind as it had the involvement of 50,000 to 100,000 internet-connected devices with approximate 1.2 TBPS of the attack strength. Cyber attackers made use of IoT gadgets to assist their abnormal malware or compromised botnet named Mirai that enables the attack to be spread quickly and automatically.

DYN is a DNS provider that is responsible for mapping human-language internet addresses (Domain Network) to corresponding IP Addresses and provide directions for the internet data traffic of routers. As the process of the DYN system relied mostly on the TCP connection organization between users (clients) and servers (protocol communications in Layer 3 and 4), attackers manipulated the vulnerability of the three-way handshake process to cause the half-open state of port 53 in the DNS servers of DYN (aka TCP SYN flood). This DDoS Protocol attack used the Mirai botnet to flood the system of DYN with malicious DNS SYN requests and caused the violation of Availability (one of the CIA Triad principles) that DYN lost its ability to process users' authorized connection requests. According to the research conducted by Flashpoint, there are some similarities in technical indicators and tactics, techniques, and procedures between this attack and previous Mirai incidents, however, the size and the scale of the packets in traffic were outstanding in comparison to the previous ones.

Question 2: **Explain** how this kind of attack is performed.

The incident of DYN was identified as an SYN flood DDoS attack with the participation of Mirai malware that accessed and was installed in thousands of IoT devices. The process of the attack technically happened like any recorded DDoS attacks, however, the use of IoT devices in proceeding with the attack, instead of using computers, made the DYN incident became one of the largest cyber-attack against the DNS provider so far.

The DDoS attack is a sequence of malicious attempts that violates the Availability principles in the CIA Triad concepts of cyber security. Within the networks of Internet-connected machines, DDoS is executed by attackers taking over the malware-infected devices, then remotely control and instruct each bot to direct attacks. Corresponding to the case study, the Mirai DDoS attack controlled thousand of IoT devices to accomplish illegal and malicious tasks. The DYN attack in 2016 introduced the DDoS attack vector named State Exhaustion DDoS attack. The core action of the attack is bombarding and overwhelming the server of the victim by sending illegitimate requests to the target, in order to take down the services (like DNS) and underly network infrastructure. In this case study, attackers used a type of TCP State-Exhaustion Attack named SYN flood to conduct their DDoS attack plan.

First, the attackers identified the workflow of the DYN system that it is a process of providing domain names and corresponding IP addresses and respond to the requests from clients (web browser owners). The three-way handshake process plays an important role in the DYN system, therefore, attackers take advantage of the vulnerable in the workflow then carried out the SYN flood. The SYN flood is a sequence of actions to prevent the completion of the interaction between client and server in a TCP three-way handshake. Unlike other DDoS attacks, DYN attack 2016 using Mirai botnet infecting distributed devices can spoof/mask the IP addresses from which the fraud request packets are sent which make it hard to track back to the source of the attack. To exploit the TCP handshake process, attackers started by sending TCP "Initial Connection Request" SYN packets in a high volume to the targeted server from IoT gadgets infected with Mirai malware. The server acknowledged and responded to the SYN-ACK message broadcast to every falsified request from botnet remotely controlled by attackers, however, would never receive back any ACK messages from these IP addresses with the insecure connections open and available that eventually result in a server crash.

These half-open connections (open in the server but not in other devices) caused by malicious clients obstructed the data traffic of the legitimate user accesses, exhausted the server's open connection resources and eventually exceeded the available resources on the server. Through the combination of the TCP SYN flood attack to port 53 of the DYN server and a subdomain attack (a prepend attack), attackers sent numerous DNS requests to the server with the random prepended domain name or subnet designations that required the server to look them up in the cache and keep maintaining a new open port connection in a period of time until all of them are utilized and disable the normal functionalities of the server. This activity sapped computational resources and prevent the server from reaching and processing the legitimate traffic. The attack and malware kept spreading widely by the path of accessing the nearest DNS server and data centre to efficiently violate the DYN local system.

Question 3: How was Dyn affected?

The victim of the DDoS attack, DYN, has been affected significantly in technical and financial terms both during the incident and its aftermath. In technical aspect, the local server of DYN has been attacked and damaged that more than 175,000 websites along with their domain-name-resolving operations were taken down, suffered from the number 40 to 50 times higher than normal of the spam packets within waves. To be specific, there are 2 waves of malicious attacks against the DYN system: the first one was the assault in 3 DYN data centres named Chicago, Washington DC and New York, which affected the Eastern Coast of the U.S; and the second wave violated 20 DYN data centre around the world. It seemed like each region was set with enough botnets to handle the spread of the attack as the DNS requests were prompted to route to the nearest DNS server and access the data centre within that region. DYN also suffered from the financial impact of the DDoS attack that DYN lost a quarter of their clients within a couple of months and 8% of their client base in the aftermath of the incident.

Question 4: How did Dyn respond and how was the attack mitigated?

During attack:
After being aware of the incident occurring within the system, DYN collaborated with criminal investigation to navigate tens of millions of suspicious and discrete IP addresses sent toward the server and identify the main cause of the attack which was the SYN flood DDoS attack using internet-connected devices along with Mirai malware. While the attack was occurring, "traffic-shaping incoming traffic, rebalancing of that traffic by manipulation of anycast policies, application of internal filtering and deployment of scrubbing services." was a response and mitigation provided from DYN. DYN continued to carry out and demonstrate the analysis of the

attack, investigate the complexity and severity of the incident, therefore, they can take prompt action to come up with solutions, provide protective measures appropriately during the attack, and aggressively extend or scale the provided measures.

Aftermath:
Sharing learning and mitigation methods throughout this DDoS attack by actively contacting and discussing with upstream internet infrastructure providers is one of the first strategies of DYN in dealing with the DDoS incident. To maintain the stability of attack resolution and reduce the impacts of the incident on end-users, clients and servers, DYN and other infrastructure providers cooperated to find out the effective mitigation strategies that merge the condition of the incident. There are not only the mitigation that is needed to apply to the DYN server to handle this problem but also the customers who directly use DYN services and be directly affected by the attack. There should be an alternative plan for any cyber incident that might occur to their domain website in the future that would not rely mostly on the DNS server.

Reference(s) using UniSA Harvard Referencing Style

S. Greenstein, "The Aftermath of the Dyn DDOS Attack," in IEEE Micro, vol. 39, no. 4, pp. 66-68, 1 July-Aug. 2019, doi: 10.1109/MM.2019.2919886.

Woolf, N., 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*, *26*.

Dyn 2016, "How the DYN DDoS attack unfolded"
https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html

CLOUDFLARE (2019). *Cloudflare*. [online] Cloudflare. Available at: https://www.cloudflare.com/en-au/learning/ddos/what-is-a-ddos-attack/.

Cloudflare. (2021). *SYN flood DDoS Attack*. [online] Available at: https://www.cloudflare.com/en-au/learning/ddos/syn-flood-ddos-attack/ [Accessed 15 Oct. 2021].

Greene, T. (2016). *DDoS attack overwhelmed Dyn despite mitigation efforts*. [online] CSO Online. Available at: https://www.csoonline.com/article/3135986/ddos-attack-against-overwhelmed-despite-mitigation-efforts.html [Accessed 14 Oct. 2021].

Lewis, D. (2016). *The DDoS Attack Against Dyn One Year Later*. [online] Forbes. Available at: https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#47df91f41ae9 [Accessed 14 Oct. 2021].

netscout (2019a). *What is a State-Exhaustion Attack?* [online] NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/state-exhaustion-attacks.

netscout (2019b). *What is a SYN Flood Attack?* [online] NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/syn-flood-attacks.

standford (2016). *The 2016 Dyn Attack and its Lessons for IoT Security | MS&E 238 Blog*. [online] mse238blog.stanford.edu. Available at: https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/#_ftnref2 [Accessed 14 Oct. 2021].

Woolf, N. (2016). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. [online] The Guardian. Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.