Appendix A: Common DDoS Attacks

Name	Description
Slowloris	Attackers exploit the way web servers handle and manage concurrent connections by keeping multiple connections open with a slow and continuous delivery of Hyper Text Transfer Protocol (HTTP) requests. This aims to exhaust the server's resources and may result in slow response times, timeouts, or complete unavailability for legitimate users.
HTTP Flood	Attackers send massive volume of HTTP requests to a web server, overwhelming its capacity to respond. This leads to slower response times, service degradation or server unavailability.
Domain Name System (DNS) Reflection/ Amplification	Attackers utilise open DNS resolvers to deliver the response traffic of their spoofed DNS requests to the target. The response traffic is usually much larger than the request (i.e., amplified) to attempt to overwhelm the target handling the traffic.
Network Time Protocol (NTP) Amplification	Attackers exploit NTP server's functionality through spoofed requests with the aim of overwhelming a target with an amplified amount of UDP traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.
Malformed SSL (Secure Socket Layer)/ TLS (Transport Layer Security) requests	Attackers send malformed SSL/ TLS requests to exploit vulnerabilities in SSL/ TLS handshake process to overwhelm the target server's resources and disrupt its ability to handle legitimate traffic. The massive volume of malformed SSL/ TLS requests from multiple sources causes increased CPU usage and memory consumption of target server.
Telnet DDoS attack	Attackers exploit defects in Telnet by sending many irrelevant data frames to throttle the connection. This prevents legitimate communication to the Telnet server and devices may be prevented from using Telnet to connect.
UDP Flood	An UDP flood involves an attacker flooding a targeted server with a large number of UDP packets with the aim of overwhelming its ability to process and respond, rendering it inaccessible to any legitimate requests.
ICMP (Ping) Flood	A Layer 3 DDoS attack method that uses a large volume of ICMP Echo Request (ping) packets to consume the target network bandwidth, processing resources or to make the target unreachable.
Ping of Death	A ping of death attack that exploits vulnerabilities in certain operating systems which handle oversized or malformed ICMP packets. The attacker sends multiple malformed or oversized packets, each crafted to be larger than the maximum allowed size of an IP packet (including the header) of 65,535 bytes. These malicious packets are fragmented by the attacker when sending the packet. As the victim attempts to reassemble the oversized packet. A buffer overflow or memory-related vulnerability may occur leading to the victim's instability or crashing. The system may then become slow, unresponsive, freeze or reboot.

MAC Flooding	Not a typical DDoS attack but this attack causes a switch infrastructure to fail, resulting in a denial of service. A device, like a network switch, is inundated with many Ethernet frames to overwhelm the switch’s address table with fake MAC addresses. When the table is full, the switch may enter either a “fail open” or “fail close” as it can no longer operate normally, and switch normal function is disrupted.
Jamming or Tampering	Not a typical DDoS attack, but attackers may jam communications or tamper with devices to cause a disruption in services. In a jamming attack, wireless communications are interrupted with jamming nodes, rendering the network nodes out of service. For tampering, these nodes could be attacked with brute force, resulting in the failure of the physical infrastructure and a subsequent disruption in service.