Fun and Games 2 Submission

Name: Jasper

1. The destination is all the same at ’23.203.162.12’ via HTTP from different sources suggested a DDoS attack. This attack will overwhelm the destination server.
2. The source and destination IP address within the same subnet which can suggest internal transmission of data via the Telnet. As Telnet is not a secured protocol, this can be a man in middle attack.
3. This can be a SYN flood attack as it shows many SYN packets from different IPs, but they did not complete the 3 way SYN ACK handshake.
4. DNS Spoofing as the user (supposedly) wanted to be directed to the official DBS website but was directed to another website that is not affiliated with DBS due to the 6.6.6.6 which is not DBS IP
5. Possibly an FTP brute force attack which is most likely trying to download files from the websites as it uses FTP.
6. Most likely a TCP SYN flood attack which is like one of the previous cases. Specifically, the attacker is trying to open as many ports as possible without ever fulfilling the 3-way handshake. This exhaust the resource of the destination servers.