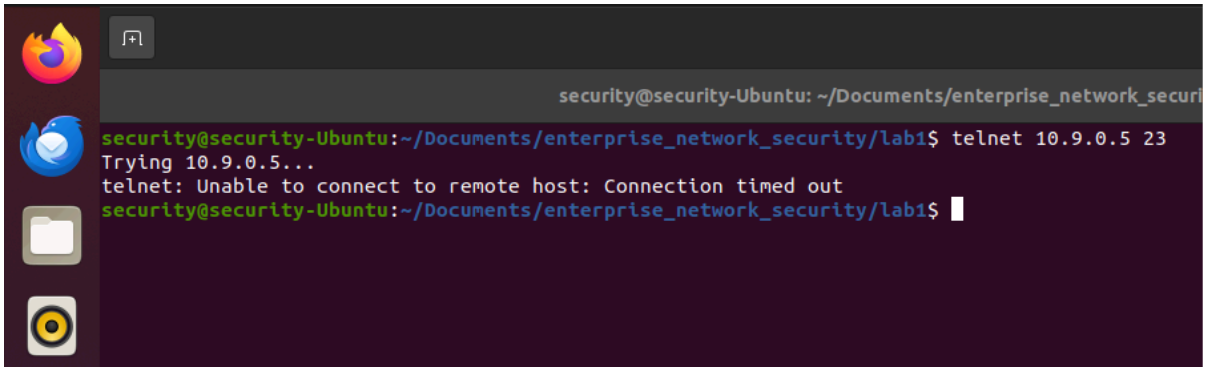
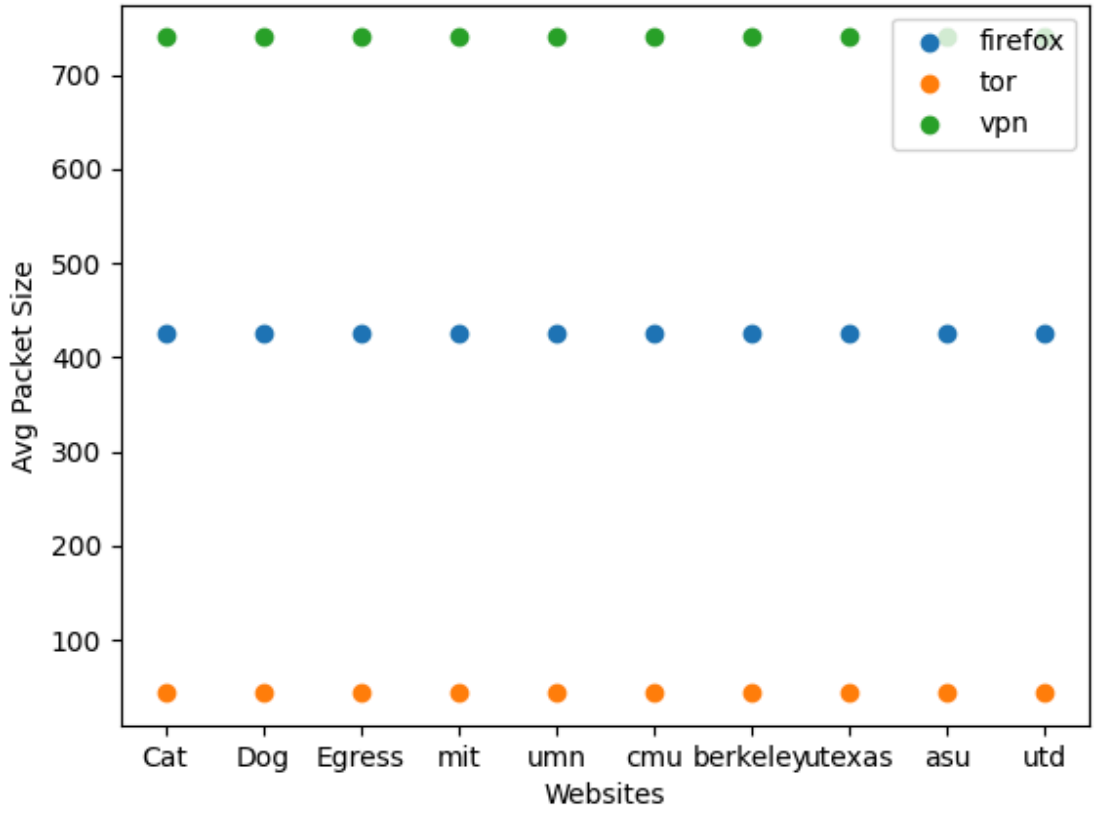
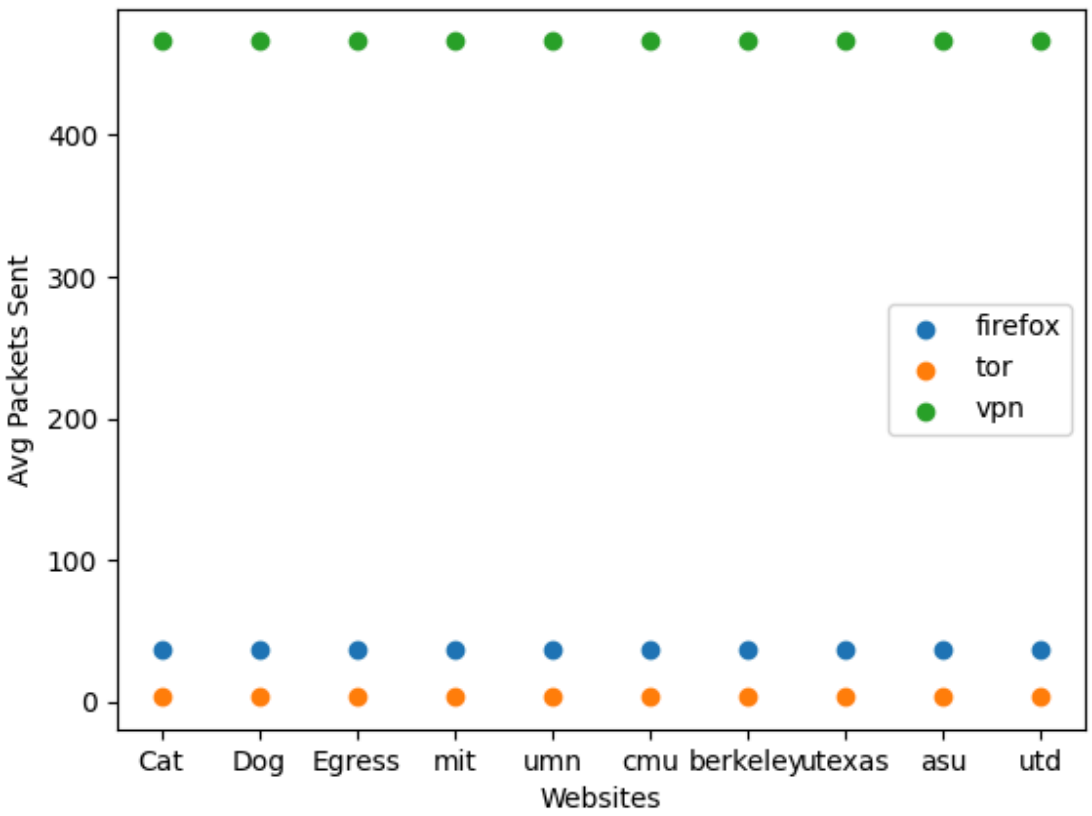
Parts 0-2



Synflood attack in C working, seen in telnet connection failing





Questions:

1. There are many things that can be observed by passive devices on the network. Information such as packet length, number of packets, the port number, from which IP address to which IP address packets are being sent to, the type of packet (UDP vs. TCP) can all be observed as evidenced by the information in .pcap files.
2. Just based on average connection statistics such as average packet length and size, it cannot be determined which websites are being observed. However, it is possible to distinguish between different connection types such as VPN, firefox, and TOR. Besides just seeing IP addresses, is it possible to “fingerprint” the identity of the websites being accessed from purely connection statistics?

Part 3

6162 networks discovered, 58009 IP addresses probed

Top ten largest networks by number of probed IP addresses associated with them. The remaining networks are attached in a file called `network_count.txt` in the submitted tarball file.

7936 AMAZON-02 - Amazon.com, Inc., US
5478 AKAMAI-AS - Akamai Technologies, Inc., US
2259 AMAZON-AES - Amazon.com, Inc., US
1775 GOOGLE-CLOUD-PLATFORM - Google LLC, US
1475 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US
1332 ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd., CN
1206 DIGITALOCEAN-ASN - DigitalOcean, LLC, US
818 CLOUDFLARENET - Cloudflare, Inc., US
817 OVH, FR
782 KIXS-AS-KR Korea Telecom, KR

Unsurprisingly, the largest networks are cloud providers/internet service providers such as Amazon for AWS, Google Cloud, Digital Ocean, etc. These cloud providers have a huge number of servers/devices in their data centers associated with their network and therefore, have the largest number of IP addresses associated with them.

If the number of machines responding is the number of IP addresses gathered, there were 58009 IP addresses that responded. The total number of machines probed is estimated to be 7,650,000 machines which was calculated by 8,500 packets/second * 900 seconds (15 minutes). This gives us a hit rate of 0.76% over the duration of the scan (58,009 / 7,650,000).

For AS AMAZON-02 US, there were 7,936 probed IP addresses associated with this network. Of these IP addresses, 102 IP addresses responded to probes on Port 443 or the HTTPS port. Of these IP addresses, 1002 IP addresses responded to probes on Port 22 or the TCP port. Of these addresses, only 59 IP addresses responded to probes on both ports.

As AMAZON-02 is associated with Amazon Web Services, it provides backend services for many applications such as cloud computing or hosting web applications. When considering that some IP addresses were included twice due to having both ports open, there are a total of 1045 unique IP addresses that responded to ports 22 or 443. Machines that responded to port 22 are likely available for SSH and used purely for backend purposes while machines that responded to port 443 are likely specific to hosting websites that use the HTTPS protocol. Considering that 13% of the total probed addresses associated with AMAZON-02 have either port open, a large percentage of their machines seem to be associated with cloud computing. I don't know what I'm saying at this point.

AMAZON-02 also constituted the largest network out of all scanned IP addresses with 7,936 addresses. This statistic seems reasonable as Amazon Web Services and Amazon's public cloud infrastructure power a very large segment of the Internet as indicated by their infamous outage three months ago with services in just about every aspect of our daily lives being impacted. Should Internet infrastructure move away from being solely dependent on the services of one company that could prove to be unreliable in the future?