Group 1I PHANG: Relationship Between Strength of Cybersecurity Laws in Different Geographic Locations and Extent of Attacker Penetration

We aim to determine how the strength of cybersecurity laws in different geographic locations affects the extent of attacker penetration. Our honeypot setup will consist of 5 honeypot containers each hosted from a different geographic location. An OpenSSH server will make the container securely accessible by attackers. The honeypot will be seeking to mimic an employee server that contains personally identifiable information. We will have a banner that every attacker sees upon entry to each of the honeypots that notifies the attacker that they are in the employee system for X reputable company. This makes it more lucrative for attackers to explore the honeypot and also allows us to explore the real-world implications of the data we collect. We will obtain publicly facing external IP's from different geographic locations via AWS EC2 instances and use 1:1 NAT mapping to map the geographic external IP from the EC2 instance to the internal IP we set up the container with. We do not plan to use the UMD publicly facing external IP since we want all external IPs to be standard and don't want to risk attackers being able to see that it's actually on the UMD network. However, we do want to keep our external IPs as a backup for now. Additionally, will use the MITM server to log attacker commands and crontab for recycling containers and performing iptables persistence.

Honey:

- Usernames
- Passwords
- Names
- Birthdays
- Social Security Numbers
- Past Employment Records