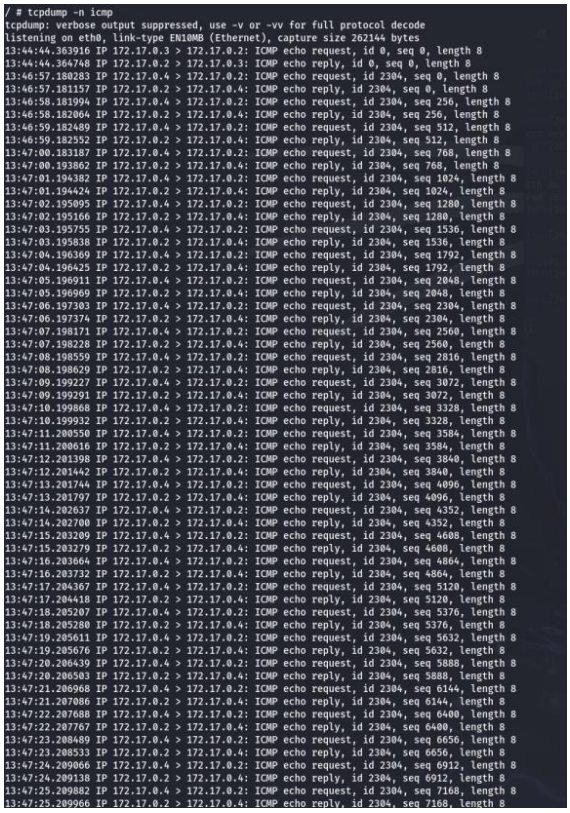
Week 6 Task 6.2C

Question A

1. Include a screenshot of the tcpdump output running on the first Terminal (i.e.,172.17.0.2)



2. In your own words, explain what did just happen?
    - Hear, an ICMP echo request is sent to the first container by the second Docker container, but the packet is masqueraded to looks as though it is from the third container. This results in the generation of a packet with a fabricated source IP address.

Question B

1. What is the password that you have cracked?
    - ‘no replies will be shown’

2. Why would an attacker spoof his IP when running an attack against a victim?
    - An attacker uses a fake IP address to conceal his location on to pretend to be another user.

3. Let’s assume a Web Server was running on the host you targeted (i.e., 172.17.0.2). How could they have prevented their system from being targeted by your ICMP flooding attack?
    - A viable defense against an ICMP flooding assault is available
        - Make sure load balance and redundancy.
        - Setting up firewall rules to restrict or stop ICMP traffic.
        - Setting up ICMP rate limitation.

Question C

Based on the above and your own research about SYN Flood Attack, answer the following questions:

1. What Are the Signs of a SYN Flood DDoS Attack?
    - A SYN flood assault can be identified by keeping an eye on server performance and network traffic for particular signs.
        - One of the main indicators of a SYN flood attack is an abrupt and persistent raise in half-open TCP connections (connections in the SYN_RECEIVED state). Server logs or network monitoring software can be used to see it. Customers may see delays when trying to access services, which is a sign that the server is being overloaded with SYN packets. The sheer volume of pending connections many put a heavy burden on the server's CPU and memory. Crashing or reduced performance may result from this. With the aid of network traffic analysis tools, it may be possible to detect a discernible increase in incoming traffic that is mostly made up of SYN packets. Service outages could occur if legitimate users are unable or unwilling to create new connections to the server. When SYN packets arrive from fictitious or strange IP addresses, monitoring programs may identify them as potential signs of an attack.

2. How to Mitigate and Prevent a SYN Flood DDoS Attack?
    - Using a combination of hardware equipment, software, and network configuration in necessary to mitigate and avoid a SYN flood assault.
        - Get rid of harmful SYN packets by using intelligent firewalls and intrusion prevention systems. These tools have the ability to recognize patterns suggestive of an attack and stop malicious communication. Load balancers can be used to split up incoming traffic among several servers. This makes it less likely that the attack will overwhelm a single server. Determine which IP addresses are sending a lot of SYN messages and block them. This works very well in situations where there are direct attacks and no IP address spoofing. Shorten the timeout period for connections that are partially open. This guarantees that the server releases resources faster by preventing it from waiting too long acknowledgement. Keep a close eye on network traffic for any indications of strange activity. Rapid reaction and mitigation are made possible by early assault detection. Plan your server and network architecture with high availability and redundancy in mind. This makes it possible for other servers to step in and keep service uninterrupted even in the event that one is compromised.

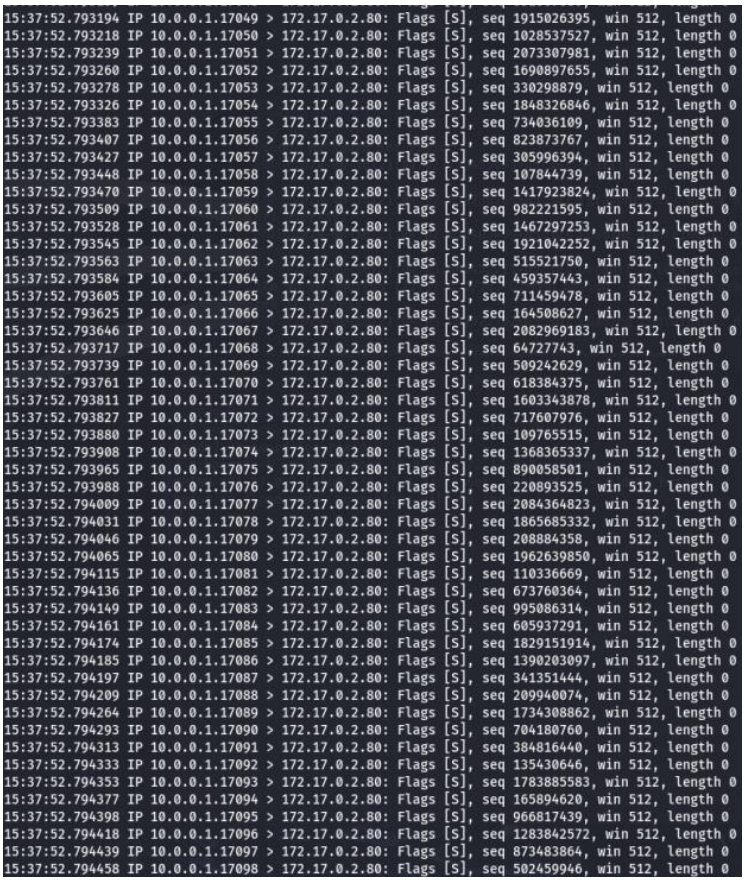
Question D

1. Investigate what is “syn cookie” and explain this in your own words. (1 reference is expected, word count is up to 300 words).
    - Server are shielded from SYN flood attacks, a kind of Denial-of-Service (DoS) attack, by means of SYN cookies. These exploits take use of the TCP handshake procedure to flood a server with partially open connections, preventing it from receiving valid traffic.
    - The SYN cookies solution is for the server to compute a unique sequence number (SYN cookie) using data from the SYN packet and a secret key, rather than devoting resources for each SYN request. SYN-ACK messages contain this sequence number. The sequence number is included in the ACK, if the client provides one. With the use of a reverse function, the server confirms this number. In the event that it is legitimate, it drops the connection and establishes the required resources.
    - A SYN request is sent by the client to establish a connection (TCP Handshake Review) With a SYN-ACK, the server answers. Customer completes the handshake by sending an ACK.
    - Attacker sends a lot of SYN request and does not respond to SYN-ACKs, which leaves connections partially open. This is known as a SYN flood Attack. Each half-open connection requires resource from the server, which fills its buffer and prevents new connections.
    - Benefits: The server guards against resource exhaustion by refusing to allocate resource for connections that are not validated. Service availability is ensured since legitimate connections remain unblocked even in the event severe SYN flooding.

    - Reference: GeeksforGeeks. (n.d.). How SYN cookies are used to preventing SYN Flood attack. Retrieved from GeeksforGeeks

Question E

1. Include a screenshot of the output in the first Terminal showing the huge amount of flooding packets after the attack is executed against the server.



Question F

1. A common interview questions these days is about Mirai Botnet. Investigate this Botnet and in your own words explain how it worked and what was its impact. Is this Botnet still affecting IoT devices? Please ensure that you use references for your answer. The suggested word count is 400-500 words.

    - In 2016, a highly disruptive malware that targeted Internet of Thing (IoT) device surfaced, known as the Mirai Botnet. It was first developed by paras Jha, Josiah white, and Dalton Norman. They used it to perform Distributed Denial of Service (DDoS) assaults against competing servers in the video game Minecraft, giving them an advantage. But the botnet soon became one of the most well-known in cybersecurity history as its capabilities grew.

    - **The operation of Mirai**
      The intrinsic flaws in LoT devices, like default usernames and passwords, were exploited by Mirai. Users frequently forget to modify the default passwords that come with a lot of internet of things devices, such as DVRs, routers and switches, and cameras. After searching the internet for these susceptible gadgets, Mirai used a list of frequently used default credentials to obtain access. Once a device was compromised, Mirai would download its software, thereby turning it into a slave within the botnet.

      Mirai could use this enormous network of compromised devices to overload target systems with traffic after a signification proportion of them were hacked, disrupting services. Because LoT devices are more common than traditional computing devices and frequently have laxer security regulations, they are easy targets for botnet was particularly successful.

    - **The effects of Mirai**
      Considerable and extensive effects were caused by the Mirai Botnet. When a DDoS attack against major DNS provider Dyn was launched using Mirai in October 2016, it was one of the most noteworthy events. Popular websites and services including Twitter, Reddit, Netflix, and Airbnb were all negatively impacted by this attack, which also caused widespread internet disruptions.

      Significant disruption could be possible, as evidenced by Mirai's capacity to enslave a large number of IoT devices into a botnet that could produce terabits of malicious traffic per second. In addition to bringing attention to IoT devices vulnerabilities, the attacks also made clear that the quickly expanding IoT industry needs better security procedures.

- **Present Condition of Mirai**
  There is still a threat from variation of the Mirai Botnet, even after its developers were apprehended and found guilty in 2017. After Mirai's source code was made available to that public in 2016, additional cybercriminals were able to alter and customize it to suit their needs. Consequently, novel strains of Mirai persist in surfacing, focusing on an expanded array of IoT devices and employing increasingly intricate techniques to elude identification and countermeasure initiatives.

  The ongoing existence of Mirai variations suggests that Internet of Things devices are still susceptible. The default password on a lot of Internet of Things devices are still in place, and users frequently forget to install security upgrades. Furthermore, botnets such as Mirai have an ever-growing attack surface due to the growing prevalence of IoT devices.

- To sum up, the Mirai botnet caused a great deal of disruption by talking advantage of poor security in IoT devices, which made it clear how urgently the IoT ecosystem needed stronger security measure. Though its original developers have been captured, Mirai's legacy lives on in the from of continuous variations that pose a threat to global internet services reliability and security

- Reference - Mimoso, M. (2017). Mirai Botnet Authors Avoid Jail Time, Will Assist FBI. Threatpost. Retrieved from Threatpost