Shriya Reddy Surusani

DDoS Mid 1

1. Describe how you can use wireshark to verify whether or not a reflection DDoS attack has amplification? How can you find the amplification factor?

Ans. In case of reflection attacks, the attacker writes the victim's IP address to the source address field of the service request packets. So that the service provider sends a response message back to the victim instead of to the attacker. We can detect this in wireshark as follows:

- We need to locate DNS/NTP response for which the system never sends a request. One of the filter that can be used is udp.srcport == <Port number>
- Now, we need to lookout for IP fragmentation cause the response can exceed the maximum size of an Ethernet frame. Filter that we can use for this is "ip.frag_offset".
- Here, the total message will be dissected.

Amplification factor is the ratio between the size of the response message sent to the victim compared to the attackers to perform reflection and amplification attacks. Getting these values from wireshark will give the amplification factor.

2. Describe an influential DDoS attack that happened in the last 32 years. Explain how that attack influenced the evolution of DDoS from that point onward.

Ans. One of the most influential DDoS attacks in last 32-years is the attack carried out by "Mafia boy", where he launched a major DDos attack on Yahoo, Amazon, Dell, ebay, CNN, and other using the alias Mafiaboy. He received rootkit and Dos code from hacker named Sinkhole. He compromised major North American universities, allegedly infecting 40% of the universities. It was a straightforward packet flooding assault on the e-commerce sites of the time.

Because of the huge volume of damage inflicted by this attack. Which is around $1.7 billion to $7.5 million along with the fact that some of the major companies got affected. It caused the consumers to lose confidence in the viability of the e-commerce and thus resulting in increased funds for research in computer and network security and also spiking an interest in the public due to huge media coverage.

3. How good is simulated DDoS attack traffic for analyzing the effectiveness of a DDoS detection approach?

Ans. Simulated DDoS attack traffic is any day less effective than the actual traffic. Factors being, simulated DDoS traffic works on the following required assumptions:

- User's behavior
- Network behavior

- Working systems behavior

The number of packets involved in the simulated DDoS is also way less when compared to the attack using a botnet with million nodes over the world. No matter what the amplification ratio is, simulated DDoS attack can never mimic the actual attack. That being said, it can still be used for initial check of DDoS detection approach used. Such that over time, a real attack can be traced back by the detection approach used in order to improve.

4. Discuss how we use network virtualization and virtual machines in our lab sessions. Explain the differences between the two.

Ans. In lab sessions Operational system data is used to perform real attacks without disturbing the original system. Clemson's background network is used for this. Here, Virtual machines are used to act as sniffer node and virtualized network is used in order to create real time traffic.

Difference,

Network virtualization is a process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network.

Whereas, virtual machines are virtualization of a computer system. It is based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software or a combination.

5. Outline the importance of attack attribution in enforcing antiDDoS laws.

Ans. One of the main problems of DDoS is its global nature, including the role played by botnets in executing DDoS attacks. Since botnet designs provide bad actors with many ways of hiding their actual locations, the ability of any law enforcement agency to find and prosecute the attackers is compromised. It is easy to plant "false flags" that attribute attacks to other players. Hence, tracing back the attack to an accurate geographic location is crucial in order to determine the severity with which antiDDos laws need to be applied. Such that, we could even analyze the patterns of where the most frequent attacks are generated from to come-up with new and better antiDDoS laws. Getting a right location also reduces the chances of triggering a cyber-war against a wrong country.