Sam Chen
Breesy Reyes

CECS 378 Assignment 4 - Denial of Service

1. **Define a denial-of-service (DoS) attack. How does it differ from a distributed denial-of-service(DDoS) attack?**
   A denial-of-service attack is an attempt to compromise availability by hindering or blocking completely the provision of some service. The attack attempts to exhaust some critical resource associated with the service. The difference between DoS and DDoS is that Dos is an attack done by one computer while DDoS is an attack done by many computers.

2. **What is the primary defense against many DoS attacks, and where is it implemented?**
   The most recommended defense against DoS attacks would be to limit the ability of systems to send packets with spoofed source addresses. It is implemented as close to the source as possible, such as routers or gateways that have knowledge of valid address ranges of incoming packets.

3. **What architecture does a DDoS attack typically use?**
   An attacker uses malware to subvert the system and to install an attack agent, the systems are called zombies. Instead of the attacker commanding each zombie, a control hierarchy is used. In the hierarchy there are a small number of systems that act as handlers, which control a larger number of systems called agents.

4. **What do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?**
   Slashdotted and flash crowd mean huge volumes of legit traffic on a system which will lead to destruction of the systems network connection. An example can happen when a website is overloaded with high popularity. There is a similar situation of an accidental or sudden overload without

affecting the performance of the network. When an overload is predicted in a slashdotted and a DoS attack it will restrict usage of network bandwidth.

5. **What steps should be taken when a DoS attack is detected?**
   The first thing to do would be to identify the type of attack by capturing the packets flowing in then analyzing them. This can be done using network analysis or the ISP to perform capture and analysis. After an attack is analyzed a filter can be designed to block the packets flowing in. However, if the flooding attack of packets is too violent it will not be possible to filter out the packets and restore the network. A possible solution would be to switch to a backup server or install new servers to restore the network.

6. **What measures are needed to trace the source of various types of packets used in a DoSattack? Are some types of packets easier to trace back to their source than others?**
   The ISP can trace the flow of packets to identify the source of a DoS attack. However, if packets are being sent with spoofed addresses, then it is hard to trace back the packets and identify the source compared to having non spoofed addresses. No, because tracing the packets back to the source is difficult. It will require assistance from the ISP to trace the packets.

7. **In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link?Or a10-Mbps link?**
   1 packet = 500 bytes, 1 byte = 8 bits, 1 Mbps = 1,000,000 bits per second
   $0.5\ \text{Mbps} = \frac{500{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte} = 125$ packets per second
   $2.0\ \text{Mbps} = \frac{2{,}000{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte} = 500$ packets per second
   $10\ \text{Mbps} = \frac{10{,}000{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte} = 2{,}500$packets per second

8. **Consider a distributed variant of the attack we explore in the above problem. Assume the attacker has compromised a number of**

broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 128 kbps. What is the maximum number of 500-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a10-Mbps link? Given reports of botnets composed of many thousands of zombie systems, what can you conclude about their controller's ability to launch DDoS attacks on multiple such organizations simultaneously?Or on a major organization with multiple, much larger network links than we have considered in these problems?

The maximum number of 500-byte ICMP echo request packets a single zombie PC can send per second is:

128 kbps = $\frac{128{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte}$ = 32 packets per second

uplink capacity of zombie = 128 kbps = 128,000 bps

0.5 Mbps = 500,000 bps,

500,000 bps $\div$ 128,000 bps = 3.906 $\approx$ 4 zombies

2 Mbps = 2,000,000 bps,

2,000,000 bps $\div$ 128,000 bps = 15.625 $\approx$ 16 zombies

10 Mbps = 10,000,000 bps,

10,000,000 bps $\div$ 128,000 bps = 78.125 $\approx$ 79 zombies

With botnets composed of thousands of zombie systems, it is possible to launch DDoS attacks on multiple organizations or on a major organization with multiple network links. With 1000 zombies and 128 kbps uplink capacity you can flood 128Mbps of network link capacity and with more than 100o zombies you can flood even more.

9. **Assume a future where security countermeasures against DoS attacks are much more widely implemented than at present. In this future network, anti spoofing and directed broadcast filters are widely deployed. Also, the security of PCs and workstations is much greater,making the creation of botnets difficult. Do the administrators of server systems still have to be concerned about, and take further**

countermeasures against, DoS attacks? If so, what types of attacks can still occur, and what measures can be taken to reduce their impact?
Yes, administrators still need to be concerned because there's always a possibility of an attack. They have to worry about potential risks and thinking which DOS defenses to be prioritized. There could be a possibility of special attacks such as buffer overflow and code injections which exploit a weakness in services instead of overrunning their resources. Flash crowds and slash dotting can still occur in networks that have an increase in traffic. Measures to reduce their impact can be using a smart ISP or IDS filters to detect malicious traffic. Using a virtual machine as a sandbox is one way so that if it is compromised then the rest of the network is still secure. The book also mentions that "provision of significant access network bandwidth and replicated distributed servers when the overload is anticipated" is another way to respond to an attack. The four lines of defense against DDoS attacks are prevention and preemption, detection and filtering, traceback and identification, and reaction.

10. **In order to implement a DNS amplification attack, the attacker must trigger the creation of a sufficiently large volume of DNS response packets from the intermediary to exceed the capacity of the link to the target organization. Consider an attack where the DNS response packets are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker trigger to flood a target organization using a 0.5-Mbps link? A2-Mbps link? Or a 10-Mbps link? If the DNS request packet to the intermediary is 60 bytes in size, how much bandwidth does the attacker consume to send the necessary rate of DNSrequest packets for each of these three cases?**
DNS response packet is 500 bytes, 1 byte = 8 bits
0.5 Mbps = $\frac{500{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte}$ = 125 packets per second
2.0 Mbps = $\frac{2{,}000{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte}$ = 500 packets per second
10 Mbps = $\frac{10{,}000{,}000\ bits}{1\ sec} * \frac{1\ byte}{8\ bits} * \frac{1\ packet}{500\ byte}$ = 2,500 packets per second

If DNS request packet is 60 bytes

0.5 Mbps: $\frac{125\ packets}{1\ sec} * \frac{60\ byte}{1\ packet} * \frac{8\ bits}{1\ byte}$ = 60 kbps

2.0 Mbps: $\frac{500\ packets}{1\ sec} * \frac{60\ byte}{1\ packet} * \frac{8\ bits}{1\ byte}$ = 240 kbps

10 Mbps: $\frac{2{,}500\ packets}{1\ sec} * \frac{60\ byte}{1\ packet} * \frac{8\ bits}{1\ byte}$ = 1200 kbps