Research Week 07

Chaz Davis

February 12, 2020

1 What types of packets are commonly used for flooding attacks?

- **Types of packets:**
  ICMP
  UDP
  TCP SYN

2 What is “backscatter traffic?” Which types of DoS attacks can it provide information on? Which types of attacks does it not provide any information on?

In computer network security, backscatter is a side-effect of a spoofed denial-of-service attack. In this kind of attack, the attacker spoofs (or forges) the source address in IP packets sent to the victim. In general, the victim machine cannot distinguish between the spoofed packets and legitimate packets, so the victim responds to the spoofed packets as it normally would. These response packets are known as backscatter.

If the attacker is spoofing source addresses randomly, the backscatter response packets from the victim will be sent back to random destinations. This effect can be used by network telescopes as indirect evidence of such attacks.

The term ”backscatter analysis” refers to observing backscatter packets arriving at a statistically significant portion of the IP address space to determine characteristics of DoS attacks and victims.

3 Define a distributed denial-of-service (DDoS) attack.

Denial of service attack is a malicious attempt by an individual or group of people to attack any network or website and abrupt the service for the people who are using those network or websites.

It prevents the authorized use of networks, systems or applications with the help of resources such as memory, bandwidth, CPU and disk space.

4 Considering your answer from question 3, is a normal DoS attack from a small number of hosts effective in today’s bandwidth heavy networks? Why or why not?

Yes, if the attacker employs a basic tactic – more resources wins this game. If they can overload your resources, the attack is successful.

It is quite easy for attackers to achieve their goals. Most website owners are leveraging shared hosts and the ones with virtual private server (VPS) environments are often set up in the smallest tiers and configurations.

This attack can be measured in bits per second.

Volume-based DDoS attacks include:

- **UDP floods**
- **ICMP floods**
- **Ping floods**

So, my answer is, no. The larger the network, the larger the botnet to be used.

5 Define a reflection attack.

The attacker sends the network packet with a spoofed source address to service runs on the network server and the server responds back to this packet by sending it to the spoofed address that belongs to authentic attack target.

This is referred to as reflection attack

* I the attacker sends multiple numbers of requests attached all with same spoofed source addresses to the number of servers

* The resulting flood of responses for those requests devastates the targets network link. It is the fact that the normal server systems used with intermediaries and if the handling of packets is entirely predictable. Then, these attacks are easier to deploy and harder to trace back to the actual attacker.

6 Define an amplification attack.

Amplification attack is different from the reflector attack and it is used to transmit a packet with spoofed source address to the target system through mediators.

* After transmission, it generates multiple responses for each original packet transmitted and it is achieved by sending the original request to some other network by broadcasting the address.

Finally, the host on the entire network responds to the request and generates a huge number of responses alternatively it uses service called DNS which generates a longer response than the original request

7 What is the primary defense against many DoS and DDoS attacks, and where is it implemented?

The main critical component of dos attack is the use of spoofed source addresses

The spoofed addresses both makes it difficult to understand the originating system of direct and distributed DDoS attacks and they are used to direct the reflected or amplified traffic to the target system. So, it is recommended to limit the ability of systems to send the packets with spoofed source addresses.

Implementation

The spoofed address filtering must be implemented and needs to be done close to the source packet with the help of routers or gateways by identifying the valid address range of incoming packets.

Normally, this is the ISP that provides the network connection for an organization or users from home

ISP knows which address belongs to which customers

Therefore, it is best to ensure whether all the packets from the customers use valid source addresses

8 What defenses are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?

For an individual or company running a website or service, mitigation options are limited. This comes from the fact that the individual's server, while it might be the target, is not where the main effect of a volumetric attack is felt. Due to the high amount of traffic generated, the infrastructure surrounding the server feels the impact. The Internet Service Provider (ISP) or other upstream infrastructure providers may not be able to handle the incoming traffic without becoming overwhelmed.

- Reduce the total number of open DNS resolvers By having poorly configured DNS resolvers exposed to the internet, all an attacker needs to do is discover it.
- Source IP Verification Because the UDP requests being sent by the attacker's botnet must have a source IP spoofed to the victim's IP address, a key component in reducing the effectiveness of UDP-based amplification attacks is for ISPs to reject any internal traffic with spoofed addresses.

9 What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?

There are various measures used to trace the source of various types of packets used in the DOS attack:

- the organization may wish to ask the ISP to trace the flow of packets to identify the source
- If the packets are used with spoofed addresses then it is difficult and time consuming to trace back the packets whereas if they are used with nonspoofed addresses then it is easy to identify the source

Are packets easier to trace back:
No! Traversing is neither easy nor automated, to trace back the source of various types of packets than other packets. This requires cooperation from the network providers to traverse these packets.

10 Is it always possible to trace the general geographic source of a DDoS attack?

An IP address traceback tasks can be performed in three ways: cache mining mode, online mining mode, and offline mining mode. During this attack, the eight to 12 pieces of DDoS data generated in one hour need to be analyzed and handled at a high speed.

- **High-speed memory mining:** The mined data, saved in the memory, can be quickly invoked and reused for progressive queries.

  Mining a big amount of data consumes a lot of cluster memory. So, the cache mode is applicable only for mining data generated in one day.

  It is recommended that a filter be used to filter the data in advance.
- **Online mining mode:** After mining conditions are typed, a filter will be automatically generated accordingly.

  The filter directly queries the raw flow table without waiting for a cache to be created, thus making query to a specific analysis scenario fast and convenient.

  This mode is applicable to one-time queries of data generated within one day.
- **Offline mining mode:** This can be used for analyzing data generated within more than one day.

  The required data is first queried and then compressed (by combining small files).

  The created physical table is saved in the hard disk for future reuse.

  Due to the big amount of data, conditions should be configured, such as a specified IP address to be queried.