جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني
DEPARTMENT OF CYBER SECURITY

SUBJECT:

MALICIOUS CODES

CLASS:

THIRD

LECTURER:

DR. SUHA ALHUSSIENY

LECTURE: (8)

DISTRIBUTED DENIAL OF SERVICE ATTACKS , DDOSATTACK DESCRIPTION CONSTRUCTING THE ATTACK NETWORK ,

DDOS COUNTERMEASURES

Distributed Denial of Service Attacks:

Distributed denial of service (DDoS) attacks present a significant security threat to corporations and the threat appears to be growing. In one study, covering a three-week period in 2001, investigators observed more than 12,000 attacks against more than 5000 distinct targets, ranging from well-known ecommerce companies such as Amazon and Hotmail to small foreign ISPs and dial-up connections. DDoS attacks make computer systems inaccessible to servers, networks, with useless traffic so that legitimate users can no longer gain access to those resources.

A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or network node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack.

In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target.

DDoS Attack Description

A DDoS attack attempts to consume the target's resources so that it cannot provide service. One way to classify DDoS attacks is in terms of the type of resource that is consumed. Broadly speaking, the resource consumed is either an internal host resource on the target system or data transmission capacity in the local network to which the target is attacked.

The following examples are one of the popular internal resources for the TCP data structure:

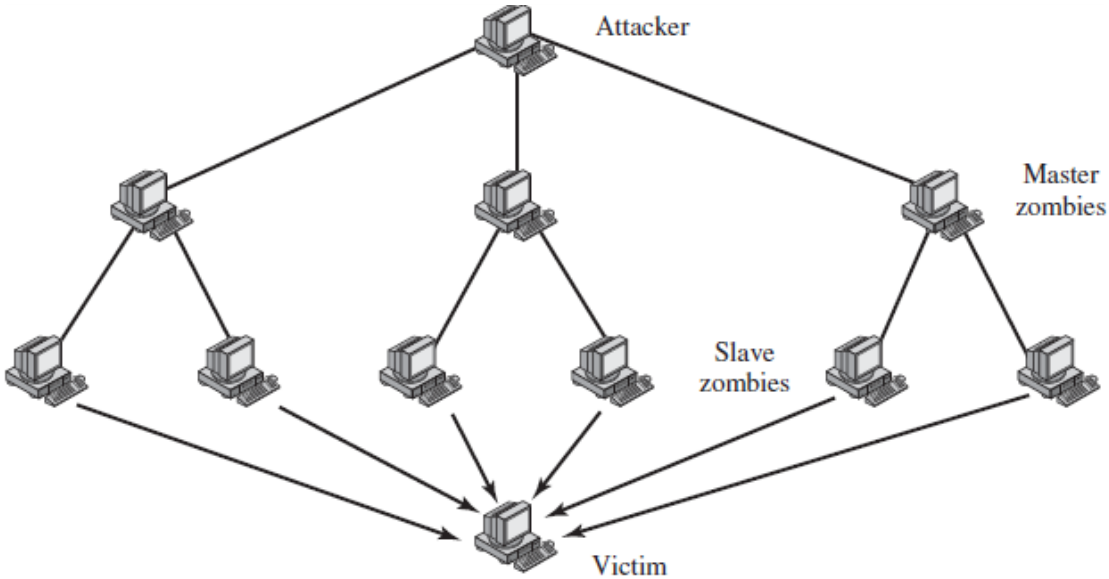
1. In many systems, a limited number of data structures are available to hold process information (process identifiers, process table entries, process slots, etc.). An intruder may be able to consume these data structures by writing a simple program that does nothing but repeatedly create copies of itself.

2. An intruder may also attempt to consume disk space in other ways, including:

- generating excessive numbers of mail messages
- intentionally generating errors that must be logged99999-0
- placing files in anonymous areas or network-shared areas

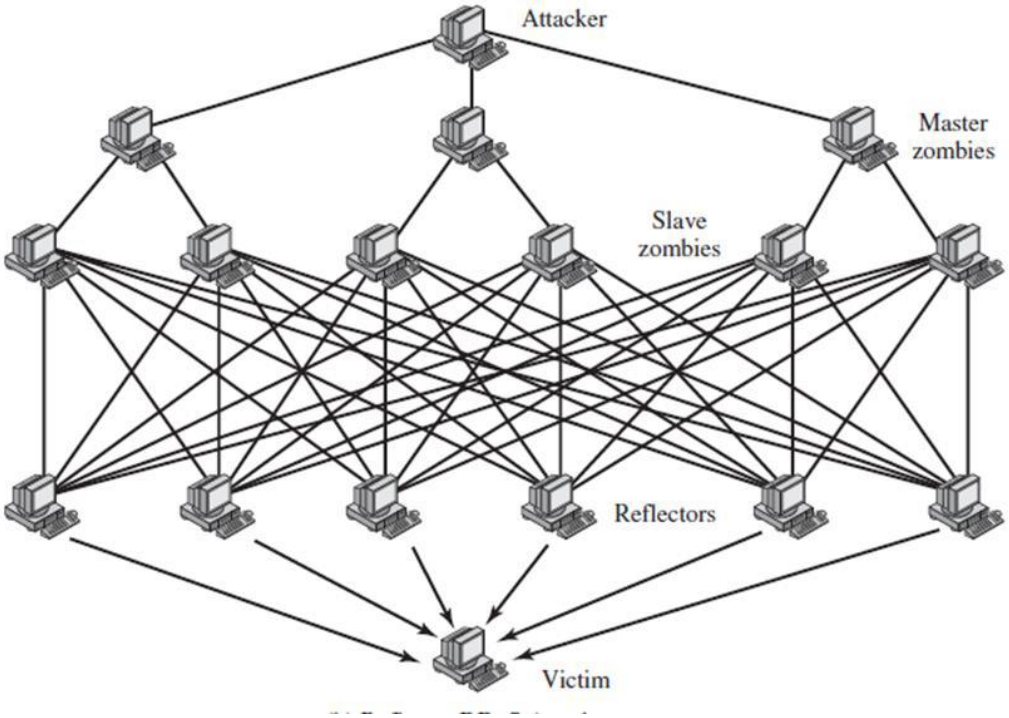
Another way to classify DDoS attacks is as either direct or reflector DDoS attacks.

In a **direct DDoS** attack (Figure 5-a), the attacker is able to implant zombie software on a number of sites distributed throughout the Internet. Often, the DDoS attack involves two levels of zombie machines: master zombies and slave zombies. The hosts of both machines have been infected with malicious code.The attacker coordinates and triggers the master zombies, which in turn coordinate and trigger the slave zombies.The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers.



(Figure 5-a) Direct DDoS Attack

A reflector DDoS attack adds another layer of machines (Figure 5.b). In this type of attack, the slave zombies construct packets requiring a response that contains the target's IP address as the source IP address in the packet's IP header. These packets are sent to uninfected machines known as reflectors. The uninfected machines respond with packets directed at the target machine. A reflector DDoS attack can easily involve more machines and more traffic than a direct DDoS attack and hence be more damaging. Further, tracing back the attack or filtering out the attack packets is more difficult because the attack comes from widely dispersed uninfected machines.

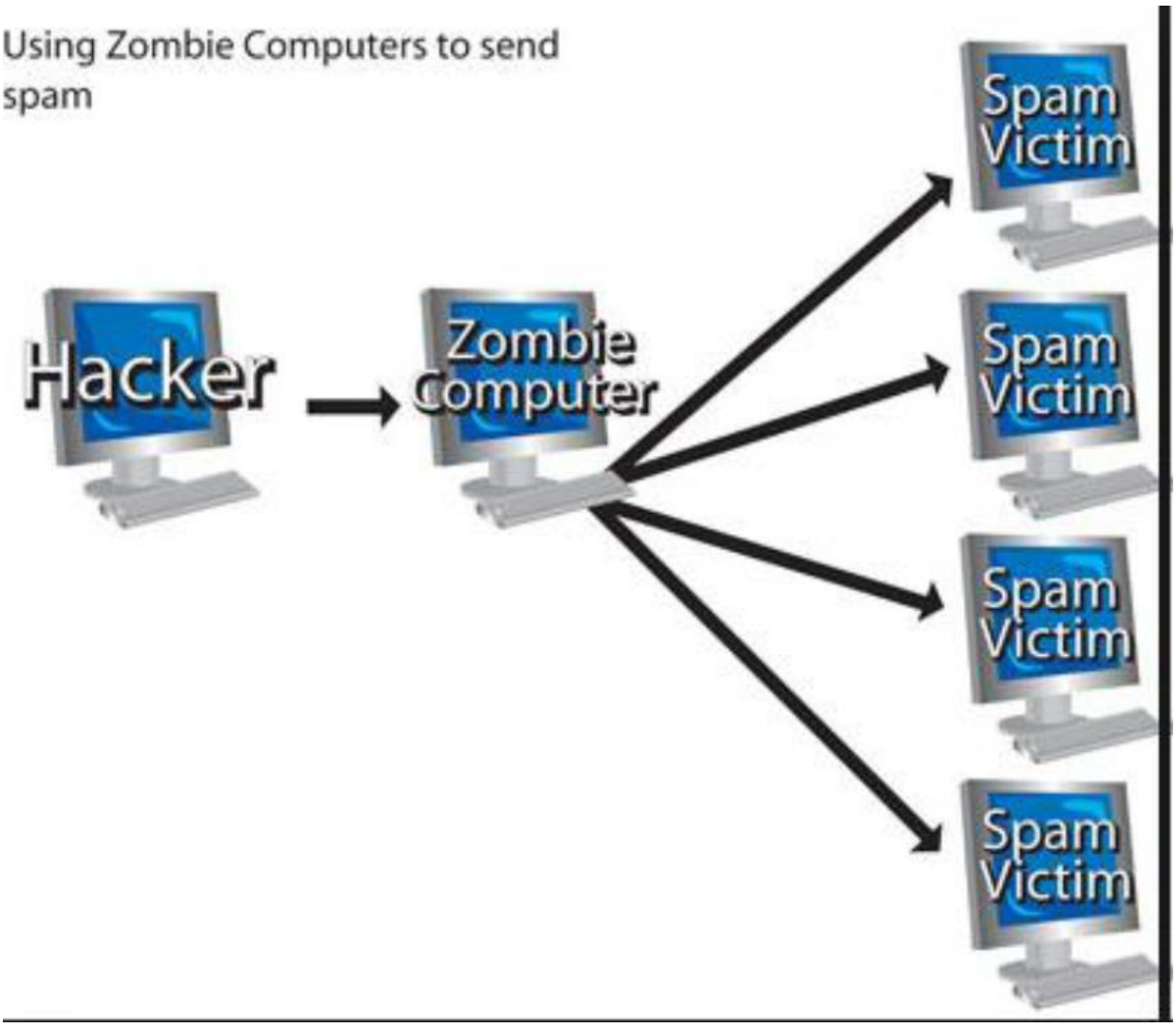


(Figure 5-b) Reflector DDoS Attack

Note: In computing, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse program and can be used to perform malicious tasks under remote direction. A zombie (also known as a bot) is a computer that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the Internet.(figure 6)

The zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies. Compared to programs such as viruses or worms that can eradicate or steal information,

zombies are relatively benign as they temporarily cripple Web sites by flooding them with information and do not compromise the site's data.



(Figure 6) Zombie connection in internet

Constructing the Attack Network

The first step in a DDoS attack is for the attacker to infect a number of machines with zombie software that will ultimately be used to carry out the attack.

The essential ingredients in this phase of the attack are the following:

1. Software that can carry out the DDoS attack.The software must be able to run on a large number of machines, must be able to conceal its existence, must be able to communicate with the attacker or have some sort of time-triggered mechanism, and must be able to launch the intended attack toward the target.

2. A vulnerability in a large number of systems.The attacker must become aware of a vulnerability that many system administrators and individual users have failed to patch and that enables the attacker to install the zombie software.

3. A strategy for locating vulnerable machines, a process known as scanning.

In the scanning process, the attacker first seeks out a number of vulnerable machines and infects them. Then, typically, the zombie software that is installed in the infected machines repeats the same scanning process, until a large distributed network of infected machines is created.

Types of scanning strategies:

- **Random:** Each compromised host probes random IP address. This technique produces a high volume of Internet traffic, which may cause generalized disruption even before the actual attack is launched.
- **Hit-List:** The attacker first compiles a long list of potential vulnerable machines. This can be a slow process done over a long period to avoid detection p-0that an attack is underway. Once the list is compiled, the attacker begins infecting machines on the list. Each infected machine is provided with a portion of the list to scan. This strategy results in a very short scanning period, which may make it difficult to detect that infection is taking place.
- **Topological:** This method uses information contained on an infected victim machine to find more hosts to scan.

DDoS Countermeasures:

In general, there are three lines of defense against DDoS attacks:

1. **Attack prevention and preemption (before the attack):**

   These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources available on demand. In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks.

2. **Attack detection and filtering (during the attack):**

   These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target. Detection involves looking for suspicious patterns of behavior Response involves filtering out packets likely to be part of the attack.

3. **Attack source trace back and identification (during and after the attack):**

   This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack.

H.W/

1. What is the main goal of a DDoS attack?
2. A DoS attack that originates from multiple hosts is called:
3. In a DDoS attack, compromised machines used by the attacker are called:
4. Which resource is commonly exhausted in DDoS attacks?
5. In a direct DDoS attack, the attacker controls:
6. A reflector DDoS attack uses:

7. Which type of DDoS attack involves spoofed source IP addresses?

8. Zombie machines typically send:

9. The first step in constructing a DDoS attack network is:

10. DDoS attack software must be able to:

11. A hit-list scanning strategy involves:

12. Random scanning produces:

13. Topological scanning uses:

14. DDoS attacks against Amazon and Hotmail were observed in:

15. DDoS prevention focuses on:

16. DDoS detection involves:

17. Filtering in DDoS response aims to:

18. Traceback methods are used:

19. In DDoS, consuming disk space can be done by:

20. Zombie computers are commonly used to:

21. A DDoS attack attempts to consume:

22. The scanning strategy that causes early traffic disruption is:

23. A DDoS attack becomes harder to trace when:

24. Backup resources on demand are part of:

25. Reflector attacks are harder to filter because: