جامـــــعـة المـــــسـتـقـبـل
AL MUSTAQBAL UNIVERSITY

قــســــم الامـــــــــن الـــــــــــــــــســيبرانـــــــــــــــــــــــي
DEPARTMENT OF CYBER SECURITY

SUBJECT:
MALICIOUS CODES
CLASS:
THIRD
LECTURER:
DR. SUHA ALHUSSIENY
LECTURE: (10)
DESCRIPTION CONSTRUCTING THE ATTACK NETWORK ,
DDOS COUNTERMEASURES

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?

A. Steal user credentials B. Make a system unavailable C. Modify system files

D. Gain administrator rights E. Install backdoors

2. A DoS attack that originates from multiple hosts is called:

A. Phishing B. Brute-force attack C. DDoS attack D. Spoofing E. Ransomware

3. In a DDoS attack, compromised machines used by the attacker are called:

A. Agents B. Zombies C. Rootkits D. Proxies E. Firewalls

4. Which resource is commonly exhausted in DDoS attacks?

A. RAM and CPU B. Power supply C. Network cables D. GPU modules E. Keyboard buffer

5. In a direct DDoS attack, the attacker controls:

A. Only reflectors B. Only the target C. Master and slave zombies D. Routers only

E. ISP servers

6. A reflector DDoS attack uses:

A. Encrypted tunnels B. Uninfected machines C. Browser plugins D. Cloud servers only

E. IoT devices only

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

A. Topological attack B. ARP attack C. Reflector attack D. Keylogging E. Sniffing

8. Zombie machines typically send:

A. Encrypted packets B. Authentication codes C. Large volumes of useless traffic

D. System updates E. Email notifications

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

A. Choosing a target B. Scanning vulnerable machines C. Launching the attack

D. Disabling firewalls E. Injecting SQL commands

10. DDoS attack software must be able to:

A. Block antivirus B. Hide its presence C. Change hardware D. Restart systems

E. Delete OS files

11. A hit-list scanning strategy involves:

A. Scanning only local networks

B. Scanning random IPs

C. Pre-compiled list of targets

D. Using ARP tables

E. Hijacking DNS records

12. Random scanning produces:

A. Minimal network traffic

B. High network traffic

C. Encrypted data only

D. Traffic limited to LAN

E. Only IPv6 packets

13. Topological scanning uses:

A. OS logs

B. Browser cookies

C. Information on infected hosts

D. DNS servers

E. IP blacklists

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

A. 1990

B. 2001

C. 2010

D. 2015

E. 2020

15. DDoS prevention focuses on:

A. Tracing attack origin

B. Filtering packets

C. Enduring attack attempts

D. Encrypting data

E. Disabling routers

16. DDoS detection involves:

A. Looking for suspicious patterns

B. Reinstalling the OS

C. Destroying hard drives

D. Disconnecting the internet entirely

E. Modifying BIOS

17. Filtering in DDoS response aims to:

A. Encrypt data

B. Block ordinary users

C. Stop likely attack packets

D. Increase RAM

E. Force reboots

18. Traceback methods are used:

A. Before the attack

B. During and after the attack

C. Only after the attack

D. Only before the attack

E. Never

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

A. Deleting logs

B. Generating excessive mail messages

C. Installing drivers

D. Updating OS

E. Clearing cache

20. Zombie computers are commonly used to:

A. Clean malware B. Improve network speed C. Forward spam and attack traffic D. Protect servers E. Monitor user activity

21. A DDoS attack attempts to consume:

A. User credentials B. Target resources C. CPU temperature logs D. USB storage logs

E. GPU power

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

A. Hit-list scanning B. Topological scanning C. Random scanning D. Selective scanning

E. Host-based scanning

23. A DDoS attack becomes harder to trace when:

A. It uses firewalls B. It uses two levels of zombies C. It uses a LAN D. It uses no malware

E. It uses outdated systems

24. Backup resources on demand are part of:

A. Attack detection B. Attack prevention C. Attack filtering D. Attack traceback

E. Attack reconstruction

25. Reflector attacks are harder to filter because:

A. They use encrypted keys B. Traffic comes from uninfected machines

C. They use only IPv6 packets D. Packets are invisible E. Targets do not log traffic

Correct Answers

1. B

2. C

3. B

4. A

5. C

6. B

7. C

8. C

9. B
10. B
11. C
12. B
13. C
14. B
15. C
16. A
17. C
18. B
19. B
20. C
21. B
22. C
23. B
24. B
25. B