**DAY 21**

Why attack happens:

1. Not having a rate limit for number of requests for connection within a stipulated time (say 60 sec)

2. The application layer which is not having a rate limit of number of request to the resources also makes a DOS/DDOS attack

3. Blocking the user account for more number of login requests received.

4. Not having a strong firewall rules.

Slow DOS attack:

Github script: slowlorris

DOS/DDOS counter measures:

1. Rate limiting for connections and application layer resource requests.

2. Active profiling

3. Establishing honeypots and redirecting the malicious traffic to the honeypots

4. Using packet filters

5. Establishing IDS and IPS

6. Absorbing the attack (Anti DDoS protection) like cloudfare, OVH anti DDOS

Hacking web servers:

🡪Web servers are the programs used for hosting

🡪Web servers may be deployed on a web server hardware or installed as cloud service.

🡪Web servers use a protocol called HTTP in order to deliver the contents

Web server security issues:

1. Network level attacks

2. Operating level attacks

Few vulnerabilities regarding the web server security issues:

1. Improper permission of the file directories

2. Default configuration

3. Enabling unnecessary services

4. Lack of security

5. Bugs

6. Misconfigured SSL certificates

7. Enabling debugging at the client side

Intitle:Index.of intext:admin.zip

-Advanced IP scanner