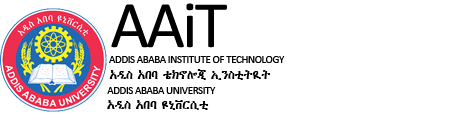
******

***Software Engineering II assignment #2***

***DOS ATTACK ON CLIENT SERVER ARCHITECTURE***

***Submitted by :* kena Wakwoya**

**Id: ATR/4296/08**

**Section 1**

***Assignment #2***

***DENIAL OF SERVICE ATTACKS (DOS) on C-S architecture.***

A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

Denial-of-service (DoS) attacks typically flood servers systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding  attacks can be more difficult to recover from.

TYPES OF DENIAL OF SERVICE ATTACK(DOS)

In addition to differentiating between a single-source denial-of-service attack and a distributed denial-of-service (DDoS) attack,DoS attacks can also be categorized by the methods the attack uses.

* 1 Ping of death: The ping-of-death attack abuses the Packet Inter-Network Groper (ping) protocol by sending request messages with oversized payloads, causing targeted systems to become overwhelmed, stop responding to legitimate requests for service and possibly crashing the victim systems.

## How Ping of Death attack works?

Not all computers can handle data larger than a fixed size. So, when a ping of death packet is sent from a source computer to a target machine, the ping packet gets fragmented into smaller groups of packets.

One fragment is of 8 octets size. When these packets reach the target computer, they arrive in fragments. So, the target computer reassembles the malformed packets which are received in chunks. But, the whole assembled packet causes buffer overflow at the target computer.

This buffer flow often causes the system crash making the system more vulnerable to attack.

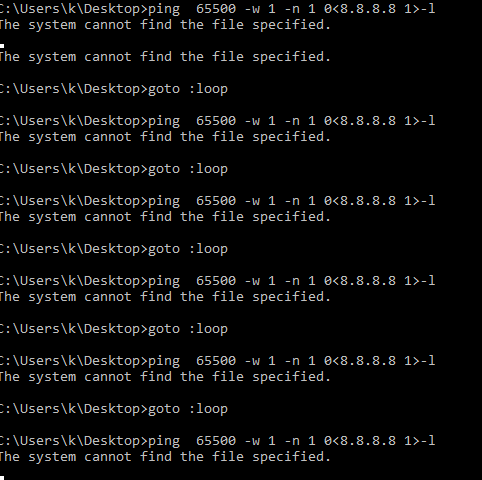
Once the system becomes more vulnerable to attack, it allows more attacks like the injection of a trojan horse on the target machine.

Using cmd and any editor we can do this ping of death as follow:

Write the following code snippet and save it with the .bat extension and then double click on it and you will see alots of ping request running on the cmd.

:loopping <IP Address> -l 65500 -w 1 -n 1goto :loop

And we will see the pinging request like this



When this pinging request is running the server is get flooded and doesn’t response for another requests at that time. This is called denial of service.

Also we can implement this kind of service denial using python is given in the pingofdeath.py and it is connected to this file.

* 2 A sync flooding: A SYN flooding attack abuses TCP's handshake protocol by which a client establishes a TCP connection with a server. In a SYN flooding attack, the attacker directs a high-volume stream of requests to open TCP connections with the victim server, with no intention of actually completing the circuits. The cost of generating the stream of SYN requests is relatively low, but responding to such requests is resource-intensive for the victim. The result is a successful attacker is able to deny legitimate users access to the targeted server. For example we can implement it as follow using python language;

1. Client --SYN Packet--> Server  
2. Server --SYN/ACK Packet --> Client  
3. Client --ACK Packet --> Server

The above 3 steps are followed to establish a connection between source and destination.

This sync flooding is implemented using python programming language and is saved as syncFlooding.py and connected to this folder.

* 3 State exhaustion attack:TCP, or Transmission Control Protocol,-- also called state exhaustion attacks-- occur when an attacker targets the state tables held in firewalls, routers and other network devices by filling them with attack data. When these devices incorporate stateful inspection of network circuits, attackers may be able to fill state tables by opening more TCP circuits than the victim system can handle at once, preventing legitimate users from accessing the network resource.

Using the c programming language we can implement this kinds of attack and it is found in the stateExhaustedAttack.c of this folder.

This is enough to make busy enough the server or maybe crash it down.