COMPUTER NETWORKS LABORATORY

PROJECT SYNOPSIS

November 12, 2016

DDoS ATTACK SIMULATION

A Project to simulate Distributed Denial of Service attack

By

Harshil Gupta | Tuhin Khare | Bhumika Hasija

Introduction

What does **DDoS** stands for?

DDOS is an abbreviation for Distributed Denial of Service.

What does **DDoS** do?

DDoS Attack is a network attack preventing legitimate users from using a specified network resource such as a website, a computer or any specific web-service.

What does a **DDoS** Attack aim?

A Distributed Denial of Service Attack is mainly aimed at the availability of services of a target system or network that is launched indirectly through many compromised systems known as bots.

What are the types of **DDoS** Attacks?

Two types of DDoS Attacks are as follows:

* **Agent Handler Model**

The Agent Handler Model of a DDoS Attack consists of clients, handlers and agents.

Clients are where the attacker communicates with the rest of the DDoS System.

Handlers are the software packages located throughout the internet that the attacker’s client uses to communicate with the agents

Agent software exists in the bot system which will eventually carry out the attack.

* **Internet Relay Chat (IRC) Model**

The IRC based DDoS attack architecture is like the Agent-Handler Model except that instead of using the handler program installed on a network server, an IRC (Internet Relay Chat) is used to connect to the client program.

What Model did we use?

We mainly focused on using the Agent-Handler Model where

* Client Software is used to communicate with the bots/agents
* Agent Searching is done through a particular tool
* Handler is installed in the compromised system
* Agent Software is performing the attack

++++++TO ADD ABOUT RESOURCE DEPLETION++++++++

PROBLEM DEFINITION

To Demonstrate a clean and proper simulation of a Distributed Denial of Service Attack using some host computers as intermediate bots between the attacker and the victim.

OBJECTIVES

* Demonstrate the simulation of a DDoS Attack using the Agent Handler Model
* Search for all the possible bots in a network using Nmap.
* Configure the bots for launching a DDoS Attack on the victim using C++ Socket Programming and POSIX Threads
* Launch the Attack on the victim’s IP through the bots and see the packet transmission using Wireshark
* Learn the Basic Concept behind a DDoS Attack, Socket Programming and Linux Environment.

BACKGROUND AND IMPLEMENTATION

The main programming language used in the project is C++ and Python.

* **Sockets**

Sockets are the end point of the communication which exist in the same network in order for the computers to exchange data.

Sockets are the way two computers talk together, which is mainly achieved by the use of file descriptors.

* **BotSearcher**

The bot searcher code written in python mainly uses the nmap tool in order to predict all the IPs connected to a particular network. These IPs are first parsed into an XML file and then written to a text file named IP.txt.

* **BotMaker**

The Botmaker file is used to configure the hosts in the network in order to launch an attack against the victim PC . The BotMaker mainly uses the C++ Socket Programming and POSIX threads in order to achieve the purpose and is the most important part in the simulation of the DDoS as this makes the attack a “DISTRIBUTED” Denial of Service attack.

* **TCPSyn**

The TCPSyn file is the attack file which is launched by the

Bot in order to attack the victim’s PCs resources thereby preventing legitimate user’s to access the same. This fulfils the major aim of the DDoS Attack.

HOW IS THE ATTACK DONE ?

**$ sudo python botSearcher.py**This code will search for the IP addresses in the local network using the nmap tool.

The IP addresses are written into an IP.txt file

**$ gcc -pthread botMaker.c**

**$ ./a.out**

BotMaker code will take the username and the password of the bots and will also take the input as name of the python code for the implementation of the attack i.e **TCPSyn.py**

Upon Execution of the Attacking file a DDoS will be launched from the bot to the victim thereby preventing all its resources to be accessed by the legitimate users.