DDoS Attack

Pentesting Guide

Table of Contents

Abstract

A [Distributed] Denial of Service ([D]DoS) attack is a malicious attempt to disrupt the regular functioning of a network, service, or website by overwhelming it with a flood of internet traffic. The primary goal is to render the target system inaccessible to legitimate users, causing downtime, financial losses, and potential damage to the target's reputation.

In this report, we are going to describe DOS/DDOS attack, here we will cover What is dos attack; How one can lunch Dos attack on any targeted network and What will be its outcome and How victim can predict for Dos attack for his network.

Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.

Introduction

In our report, we will explore several scenarios of DOS attack and receive alert for Dos attack through the Network Intrusion Detection System (NIDS) Snort. DOS can be performed in many ways either using a command line tool such as Hping3 or GUI based tool. Additionally, pentesters will learn how to Perform Dos attack using GUI tools as well as a command line tool and get an alert through Snort.

For the lab setup, here are the requirements:

Attacker machine: Kali Linux

Victim machine: Ubuntu

Optional: Wireshark (we have added it in our tutorial so that we can clearly confirm all incoming and outgoing packet of the network)

What is DOS/DDOS Attack

From Wikipedia

A **denial-of-service attack** (DoS attack) is a cyber-attack where the attacker looks for to make a machine or network resource unavailable to its deliberated users by temporarily or indefinitely services of disturbing a host connected to the Internet. Denial of service is usually accomplished by flooding the targeted machine or resource with excessive requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a **distributed denial-of-service attack** (DDoS attack), the incoming traffic flooding the victim originates from many different sources. A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

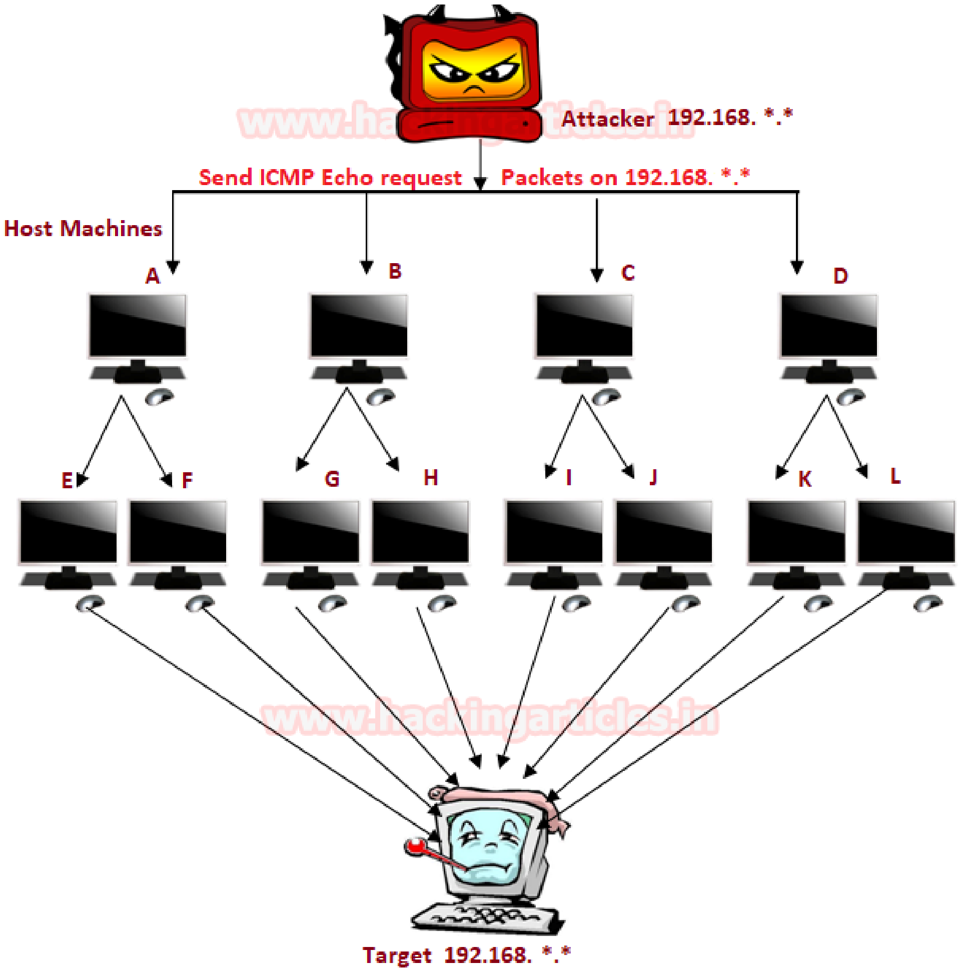
Basically, the attacker machine either himself sends infinite request packets on the target machine without waiting for reply packet form target network or uses bots (host machines) to send request packet on the target machine. Let study more above it using given below image, here you can observe 3 Phases where **Attacker machine** is placed at the **Top** while **Middle** part holds **Host machine** which is control by attacker machine and at **Bottom**, you can see **Target** machine.

From given below image you can observe that the attacker machine want to send ICMP echo request packet on the target machine with help of bots so this will increase the number of attacker and number of request packet on the target network and cause traffic Flood. Now at that time, the targeted network gets overloaded and hence lead some service down then prevent some or all legitimate requests from being fulfilled.

DOS/DDOS Categories

- **Volume Based Attack**: The attack's objective is to flood the bandwidth of the target networks by sending ICMP or UDP or TCP traffic in per bits per second.
- **Protocol-Based Attack:** This kind of attack focus actual target server resources by sending packets such TCP SYN flood, Ping of death or Fragmented packets attack per second to demolish the target and make it unresponsive to other legitimate requests.
- **Application Layer Attack:** Rather than attempt to demolish the whole server, an attacker will focus their attack on running applications by sending request per second, for example, attacking WordPress, Joomla web server by infinite request on apache to make it unresponsive to other legitimate requests.

Distributed Denial Of Service Attack (DDOS)


Attacker 192.168. *.*
Send ICMP Echo request
Packets on 192.168. *.*
Host Machines
A
B
C
D
E
F
G
H
I
J
K
L
Target 192.168. *.*