

Hackercombat.com

Distributed Denial Of Service (DDoS) Attack Using Kali Linux

SWIPE



DDoS Attacks



What is Distributed Denial of Service Attack(DDoS)?

A distributed denial-of-service (DDoS) attack is an attempt to make a system or network resource unavailable to its intended users. Although the means and motives vary it generally consists of efforts to temporarily or indefinitely interrupt a host connected to the Internet. This article reads on how to carry out a Denial-of-service Attack using Kali Linux.

DDoS attacks have been carried out by different hackers and criminals and even government agencies. This is mainly attributed to poor coding, loose patches or unstable systems. These are the factors that result in DDoS like attacks.

How DDoS Attacks Work?



In a typical DDoS attack, the assailant begins by exploiting vulnerability in one computer system and making it the DDoS master.

The attack master system identifies other vulnerable systems and gains control over them by either infecting the systems with malware or through bypassing the authentication controls (i.e., guessing the default password on a widely used system or device).

DDoS attack normally starts when the criminal looks for the vulnerability in one system and thus making it a DDoS master. The master then looks for other vulnerabilities in the system to get access to the system, so it will either infect the system with a malware by bypassing the admin and taking control.

What is Kali Linux?



Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company. Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

It contains several hundred tools that are intended towards various information security tasks, such as Security research, Penetration Testing, Reverse Engineering, Computer Forensics.

It was in the year 2013 that Kali Linux was released. A complete top-to-bottom BackTrack Linux adhering to Debian development standards was rebuilt.

How To DDOS a Website

Anonymously Using Kali Linux?



- Run etherape root@kali:~# etherape, it prompts a popup window which displays network activity graphically.
- Run TOR Servicenow root@kali:~# service tor start
- Download Goldeneye
<https://github.com/jseidl/GoldenEye>
- Once Downloaded Unzip it as a folder root@kali:~#
unzip GoldenEye-master.zip
- Launch the attack

DDOS Tools

DDOS tools are capable of putting heavy loads on HTTP servers and bring them to their knees by exhausting its resources.

➔ EtherApe

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It can filter traffic to be shown, and can read packets from a file as well as live from the network.

➔ Proxychains

Latest version of Proxychains support SOCKS5, SOCKS4, and HTTP CONNECT proxy servers. Proxychains can be mixed up with a different proxy types.

➔ GoldenEye

GoldenEye a python app designed for Security Testing Purpose only.

➔ Service Tor

Tor allows clients and relays to offer hidden services. That is, you can offer a web server, SSH server, etc., without revealing your IP address to its users.

Follow us



Visit

Hackercombat.com

5 Steps To Prepare For a DDoS Attack

Step 1

Map Vulnerable Assets

Step 2

Assess Potential Damages

Step 3

Assign Responsibility

Step 4

Set Up Detection Mechanisms

Step 5

Deploy a DDoS Protection Solution

Follow us



Visit

[Hackercombat.com](https://hackercombat.com)

**14.5
Million**

Global estimates of the total number of DDoS attacks are anticipated to double to 14.5 million by 2022, according to 2017 data from the Cisco Visual Networking Index (VNI).



Follow us

Hackercombat.com