Assignment No: 02

Title: Implementation and analysis the effect of attack.

a) DDOS Attack

b) IP spoofing

c) DNS Attack

Performance (3)	Understanding (1)	Regularity (1)	Total (5)	Sign of Staff

Assignment No: 02

Aim: Create an attack using python script and implement attack and analyze the effect of attack.

a) DDOS Attack

b) IP spoofing

c) DNS Attack

Objectives: 1) To create and implement attack using Python script

2) To analyze the effect of attack

DDOS attack:

Distributed denial of service (DDoS) attacks is a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

Unlike other kinds of cyber-attacks, DDoS assaults don't attempt to breach your security perimeter. Rather, a DDoS attack aims to make your website and servers unavailable to legitimate users. DDoS can also be used as a smokescreen for other malicious activities and to take down security appliances, breaching the target's security perimeter.

How DDOS attack works?

Cybercriminals carry out DDoS attacks by gaining unauthorized control of a network of computers. With the help of specially designed malware, cybercriminals turn those computers, and other systems (such as IoT devices) into a bot (or zombie). A group of such bot systems is known as a botnet. Cybercriminals will remotely control the botnet to carry out DDoS attacks.

Cybercriminals can direct the devices in the botnet by sending instructions to each bot via a method of remote control. When the botnet targets the IP address of a victim (a website, server or other network resources), each bot will respond by sending repeated connection requests to the target, potentially causing the targeted machine to overflow capacity, resulting in a denial-of-service to normal traffic.

Botnets can be of any size; botnets with tens or hundreds of thousands of compromised machines have become increasingly common, and there are no upper limits to their size. Once a botnet is created, the attacker can use the traffic generated by those compromised devices to attack the targeted website or computer with overwhelming connection requests.

Types of DDOS attack:

1. HTTP Flood

HTTP Flood is a type of DDoS attack which appears to be legitimate GET or POST requests that are exploited by a cybercriminal. This type of attack uses lesser bandwidth than other types of DDoS attacks, but it can force the server (target machine) to use maximum resources.

2. UDP Flood

A UDP flood type of attack targets random ports on a computer system or network with UDP (User Datagram Protocol) packets. It involves sending high volumes of UDP packets to the target machine.

3. SYN Flood

SYN Flood type of attack exploits vulnerabilities in the TCP connection sequence (in a server), known as a three-way handshake. The attacker sends repeated SYN requests (a TCP connection) to the target machine (server).Usually, the server replies with an SYN-ACK response, and then the client system follows up with an ACK signal to establish the connection. In an SYN flood, the ACK is never sent. This leads to the buildup of incomplete connections, leading to the server (target machine) slow down or even crash.

IP spoofing:

Internet Protocol (IP) spoofing is a type of malicious attack where the threat actor hides the true source of IP packets to make it difficult to know where they came from. The attacker creates packets, changing the source IP address to impersonate a different computer system, disguise the sender's identity or both. The spoofed packet's header field for the source IP address contains an address that is different from the actual source IP address.IP spoofing is a technique often used by attackers to launch distributed denial of service (DDoS) attacks and man-in-the-middle attacks against targeted devices or

the surrounding infrastructures. The goal of DDoS attacks is to overwhelm a target with traffic while hiding the identity of the malicious source, preventing mitigation efforts.

How IP spoofing works?

Internet traffic is sent in units referred to as packets. Packets contain IP headers that have routing information about the packet. This information includes the source IP address and the destination IP address. Think of the packet as a package in the mail and the source IP address as the return address on that package.

In IP address spoofing, the attacker changes the source address in the outgoing packet header. That way, the des-tination computer sees the packet as coming from a trusted source -- such as a computer on an enterprise network -- and accepts it.

Attackers may generate fraudulent packet headers by falsifying and continuously randomizing the source address using a tool. They may also use the IP address of another existing device so that responses to the spoofed packet go there instead.

To carry out IP spoofing, attackers need the following:

- A trusted IP address that the receiving device would permit to enter the network. There are numerous ways to find device IPs. One way is Shodan, an online database of IP address-to-device mappings.

Types of DNS attack:

1. DoS and DDoS Attacks
2. DNS Hijacking/DNS Redirection
3. DNS Poisoning/DNS Spoofing
4. DNS Tunneling

How DNS attack works?

When a user types a domain name in the browser, a program available in the operating system known as ‘DNSresolver‘searches for the IP address of that domain name.The DNS resolver searches its own

local cache and check if it already has the IP address for that domain. If it does not find it in the local cache, It queries a DNS server to check if it knows the accurate IP address for that domain.DNS servers work in a loop which means they are able to query each other to find the DNS server that knows the correct IP address of the domain name.As soon as the DNS resolver locates the IP address, it returns the IP address to requesting program. DNS caches domain addresses for future use as well.

Conclusion:

Thus DDOS, IP spoofing and DNS attacks are implemented and analyzed successfully.