**DNS Name Server Attack**

**Description 1**

“This is one of the most common method for attacks, mainly by sending a high number of UDP based DNS requests to a nameserver using a spoof IP address, now any nameserver response is sent back to the destination i.e., to the spoofed IP address and here this IP address is the victim of the DoS attack. So, it is difficult for a nameserver or the victim to determine the true source of the attack.” [1]

**Description 2**

These attacks are aimed at specific DNS servers and can have several objectives, the most common of which is to cause denial-of-service. Another common objective is to obtain all the data stored in a DNS server, in order to study the organization’s network infrastructure. Such study is later used to find effective attack vectors. Yet another attack objective is to get control over the server and server’s data using protocol vulnerabilities and anomalies. While both authoritative and recursive DNS servers are victims to such attacks, different attacks are used with each of them, leveraging the different mode of operation of each to maximize the attack impact. ISPs, hosting providers and any other company that hosts a public DNS server often suffer from such attacks. [2]

**Description 3**

One of the biggest challenges for IT organizations is the varied and ever-changing options for DNS attacks. Common attacks include:

TCP SYN Flood Attacks A DDoS DNS attack, typically leaves “hanging” connections by flooding DNS

server with new TCP connection requests until the target machine fails.

UDP Flood Attack A DDoS DNS attack, sends a large number of UDP packets to a random port on

the targeted host to confuse or overwhelm the target machine until it fails.

Spoofed Source Address/

LAND Attacks

A DDoS DNS attack, sends a spoofed TCP or UDP packet with the target host’s

IP address to an open port as both source and destination. The reason this attack

works is because it causes the machine to reply to itself continuously, therefore

making it essentially unavailable to other applications.

Cache Poisoning Attacks A core DNS attack, poisons DNS cache typically in order to send legitimate

requests to malicious websites.

Man in the Middle Attacks A core DNS attack, a compromised machine in the network can penetrate and

take over the e ntire DNS structure and then route legitimate requests to malicious websites. [3]

**Reference**

[1] <https://www.hostdepartment.com/blog/2014/05/21/ddos-attack/>

[2] <https://blog.radware.com/security/2016/09/dns-and-dns-attacks/>

[3] https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-whitepaper-top5-dns-security-attack-risks-how-to-avoid-them.pdf