**Security Vulnerabilities Concerning DNS And Its Prevention**

DNS or Domain Name System is a hierarchical database that converts domain names to IP addresses for the network devices to comprehend. But this mechanism is subject to various malpractices.

To cite an example, the tunneling techniques used in DNS can be hacked by malpractice, thereby posing threat to the network connectivity and getting access to the remote device.

**What is meant by DNS vulnerability and why does it happen?**

The primary reason for DNS vulnerability is the resolvers that issue the DNS query trust the responses that are received after they send out a query.IT can also contain unwanted responses that are unrelated to the query.

**What are some of these types?**

Given below are some of the methods used for DNS attacks.

**1. Man In The Middle(MITM) attacks**

The receiver of the data has no means by which they can check the authenticity of the data because the DNS server by no means provides a mechanism for showing the details. Only the DNS reply data packet can be authenticated. Hackers and attackers can take this opportunity to build a DNS server response packet that resolves queries with wrong information and there will be no choice left but to trust the data.

**2. DNS Flood Attacks**

This is a type of DDoS (Distributed Denial of service attack where more than one DNS server possesses the risk of getting attacked and their record resources subject to hampering so that the website or API is unable to respond to traffic.

**3. Cache Poisoning Using Name Chaining**

This attack is associated with giving incorrect and false information to DNS caches. These false data along with DNS names can be infused into the target’s cache. Attackers can provide any name of their choice and provide information that is related to these names.

**4. DNS Spoofing**

Also known as DNS cache poisoning, this is a method by which different DNS records are used to redirect it to a deceptive website that imitates the destination. Once the user reaches the website, they are required to log in with their credentials which enables the attackers to hijack the credentials and also confidential information.

**5. Packet Sniffing**

DNS sends a query to UDP packets that are not encrypted and this can be captured by the attackers and wrong answers can be generated fast enough.

**Vulnerability Prevention**

There are several ways by which DNS attacks can be muted. Some of them are as follows.

1)DNS Resolver should always be private and only network users should have access to this.

2)Applications and APIs must be checked regularly to mitigate the risk of DNS attacks. The generated reports help to find out which area needs more focus.

3) If someone’s own DNS server is not used and a third-party service is involved, two-factor authentication must be kept on.

4) Understand the DNS architecture to secure it properly.

5)Protect servers from access when not required through different enhancements.

**References**

1)<https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/>

2)<https://www.cloudflare.com/en-in/learning/dns/dns-security/>

3)<https://hackernoon.com/what-is-a-dns-attack-and-how-can-you-protect-against-it>

4)<https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks>

5)<https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them>

6)<https://www.geeksforgeeks.org/types-of-dns-attacks-and-tactics-for-security/>

7)<https://web.mit.edu/6.033/www/papers/dnssec.pdf>