**DNS Spoofing**

**Other names: the definition has overlap with description of Cache Poisoning**

**Description 1**

**Domain Name Server (DNS) poisoning or spoofing is a type of cyber-attack that exploits system vulnerabilities in the domain name server to divert traffic away from legitimate servers and directs it towards fake ones.** DNS poisoning poses several risks, starting with [**data theft**](https://usa.kaspersky.com/resource-center/threats/data-theft)**.** **Banking websites and popular online retailers are easily spoofed, meaning any password, credit card or personal information may be compromised. Also, if spoofed sites include Internet security providers, a user's computer may be exposed to additional threats such as viruses or Trojans, because legitimate security updates will not be performed**. Finally, eliminating DNS cache poisoning is difficult, since cleaning an infected server does not rid a desktop of the problem, and clean desktops connecting to an infected server will be compromised again. If necessary, users can flush their DNS cache to solve the issue. [1]

**Description 2**

Since DNS names can be easily spoofed or misreported, and it may be difficult for the software to detect if a trusted DNS server has been compromised, DNS names do not constitute a valid authentication mechanism. When the software performs a reverse DNS resolution for an IP address, if an attacker controls the server for that IP address, then the attacker can **cause the server to return an arbitrary hostname**. As a result, **the attacker may be able to bypass authentication,** **cause the wrong hostname to be recorded in log files to hide activities, or perform other attacks.** Attackerscan spoof DNS names by either (1) compromising a DNS server and modifying its records (sometimes called DNS cache poisoning), or (2) having legitimate control over a DNS server associated with their IP address. [2] one consequences is that Malicious users can fake authentication information by providing false DNS information.

**Description 3**

Is an attack that seeks to introduce false DNS address information into the cache of a DNS server, where it will be served to other users **enabling a variety of attacks such as Phishing attack**. [3]

**Reference**

**[1]** [**https://usa.kaspersky.com/resource-center/definitions/dns**](https://usa.kaspersky.com/resource-center/definitions/dns)

**[2]** [**https://cwe.mitre.org/data/definitions/350.html**](https://cwe.mitre.org/data/definitions/350.html)

**[3]** [**https://www.owasp.org/index.php/Category:Attack**](https://www.owasp.org/index.php/Category:Attack)