DNS attacks

Resources:

https://www.infoblox.com/dns-security-resource-center/dns-security-faq/what-are-dns-attacks/

A DNS Attack is any attack targeting the availability or stability of a network's DNS service. Attacks that leverage DNS as its mechanism as part of its overall attack strategy, such as cache poisoning, are also considered DNS attacks. In this article, we will get an overview of the common types of DNS attacks out there.

Generic Attacks Against DNS Service

These attacks focus on attacking the DNS infrastructure itself, either rendering the DNS service itself unavailable or subverting the answers provided by the DNS servers. Keep in mind that DNS is comprised of two (2) separate components, authoritative servers (answer-hosting) and recursive servers (answer-finding), and there are tailored attacks against each component that will be discussed later.

Network Floods

Like any other server, DNS servers are prone to all network-based attacks. There are many ways attackers can cause a large amount of network traffic to the DNS servers, such as TCP/UDP/ICMP floods, rendering the service unavailable to other network users by saturating the network link to the DNS servers.

Software Vulnerability

Attackers can also leverage a specific vulnerability to the DNS server software or host operating system, to either bypass control measures to create rogue entries in the DNS database, or cause the DNS server to crash.

Attacks Against Authoritative Servers

Authoritative name servers maintain the DNS zone and records, similar to a database. These are some common attacks against authoritative DNS servers.

Reconnaissance

DNS data by design is supposed to be for public consumption, making this the ideal first step for an attacker trying to learn more about a target environment. This attack does not directly impact service availability or stability, but it is usually part of a long-term strategy of a larger attack. For example, an attacker could deduce that exchange.example.com listed in the MX record is running Microsoft Exchange, and launch specific attacks against it.

Unauthorized Update

Authoritative name servers can accept dynamic updates, meaning they can essentially create new DNS records on the fly. However, this feature could be exploited by attackers to sneak unauthorized entries into the DNS zone.

Subdomain Attack

This is a type of DoS attack, and its goal is to overwhelm the authoritative name servers to the point that it can no longer respond to legitimate queries. In this attack, the attacker sends a lot of queries for subdomains that probably do not exist, consuming the authoritative server's resources to the point that it causes disruption to other DNS lookups. For example, instead of querying for example.com, the attacker would query for 111aaa.example.com, 111bbb.example.com, 222aaa.example.com, 333ccc.sub.example.com, etc.

Attacks Against Recursive Servers

Cache Poisoning

The main job of a recursive server is to build and hold a rich cache of DNS answers. Cache poisoning aims to corrupt the answers stored in the cache, so any subsequent lookup from other clients will get the corrupted answer. This is discussed in **Cache Poisoning**.

NXDOMAIN and Phantom Domain

Similar to the subdomain attack against authoritative servers, this attack queries recursive name servers that are known to not exist. This will waste the recursive server's time in walking the DNS namespace, only to reach the conclusion that the name does not exist, filling up the cache with useless answers.

Other DNS-based Attacks and Exploits

Amplification + Reflection Attack

Previously discussed DDoS attacks are the variety where attackers target DNS servers within an organization. These types of attacks we address now is where attackers take over DNS servers within an organization as part of a DDoS attack to target someone else. It is discussed in more details in **DDoS**.

Domain Hijacking and Redirection

This category of attack subverts the users to go to a different destination. A well-known example is the domain name paypaI.com (notice the letter "i" is in uppercase), which looks very much like the real domain name paypal.com, spelled with an L. In a similar category, attackers could infect the target client machine with malware that changes the local DNS settings, so that all DNS requests are sent to the DNS server under the attacker's control, such as the case for the DNSChanger worm.

Malware

Speaking of malware, many types of malware today are using DNS as part of their overall function to not only communicate with the command-and-control server but to update and evolve itself. A prime example is the recent WannaCry ransomware, which relies on making an initial successful DNS query before it executes its attack.

Data Exfiltration and Tunneling

DNS Tunneling is a general technique that encodes messages in DNS queries and answers, mostly to evade detection. While there are legitimate uses of DNS Tunneling, where it gets serious is when someone uses it to **exfiltrate sensitive information** out of the target environment. This is extremely difficult to detect, due to the ever-changing domain names, and the encoding-decoding schema chosen.