5.2.6 DNS Attack Facts

A DNS-based attack occurs when stolen DNS records are used to redirect traffic to fake websites for malicious purposes. Below are important facts you should know about DNS:

- Standard DNS is configured with one primary DNS server that maintains a read/write copy of all the computer names and IP addresses registered in DNS for the domain.
- Secondary DNS servers obtain a read-only copy of this data from the primary DNS server or another secondary server.
- The process of copying the records from the primary to the secondary DNS server is called *zone transfer* and is performed in cleartext.

The main methods used to attack DNS servers are explained in the following table.

Attack	Description
Reconnaissance	Reconnaissance is used to gather information for an attack. The goal is to obtain DNS records that identify computer names and IP addresses in a network. This can be accomplished by: ▪ Performing direct queries on DNS servers (using a tool such as **nslookup**) to request individual records. ▪ Attaching to a DNS server as a secondary server and requesting a zone transfer of DNS records. ▪ Using a protocol analyzer to gather zone transfer traffic, which is transferred in cleartext from the primary DNS server to the secondary DNS server. To mitigate reconnaissance attacks: ▪ Configure your DNS servers to only accept queries for zone transfers from specific hosts ▪ Secure zone transfer data using IPSec or a VPN tunnel
DNS Poisoning	*DNS poisoning* (also known as DNS cache poisoning) occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack: ▪ Incorrect DNS data is introduced into the cache of a primary DNS server. ▪ The incorrect mapping is made available to client applications. ▪ Traffic is redirected to incorrect sites (known as *pharming*) for phishing purposes to perform: ▪ Identity theft ▪ Financial theft ▪ Malware downloads (drive-by downloads), which can be used to capture sensitive information, such as passwords and financial information.
Domain Name Kiting	*Domain name kiting* occurs when spammers exploit domain registration by taking advantage of the five-day grace period for a newly registered domain name. This allows spammers to: ▪ Acquire domains and never pay for the registration of domain names by unregistering a domain name just before the grace period is up and then immediately re-registering the domain name. ▪ Generate income through clicks by automatically registering thousands of domains and putting ads on them. They can create *link farms* (multiple domains with automatic hyperlinks to targeted sites) to spam the index of a search engine (such as Google) and trick the search engine into conferring a page ranking on the spammed website.
Domain Hijacking	Unlike the other DNS attacks listed here, which use stolen DNS data to redirect unwitting users, *domain hijacking* is when an attacker gains access to the domain control panel itself. They reconfigure the domain name to point toward another web server. This allows attackers to trick users into thinking they're at a legitimate website, when they're really at a dummy site created by the attacker.

The HOSTS file located on the C: drive at Windows\System32\drivers\etc maps IP addresses to host names. If the host name is not found in this file, then the computer will contact the DNS server. This file can be used to improve security and reduce bandwidth usage by:

- Mapping known malicious sites to the loopback address of 127.0.0.1 to prevent browsers from displaying the malicious sites.
- Using security software to prevent modification of the HOSTS file without your knowledge. This will prevent hackers from placing a mapping in the file to redirect traffic to a fake site.

Other ways to protect your organization from DNS attacks include:

- Using the latest version of DNS software.
- Consistently monitoring traffic going through your network.
- Configuring servers to duplicate, separate, and isolate DNS functions.
- Using Domain Name System Security Extensions (DNSSEC) to secure certain kinds of information provided by DNS. DNSSEC adds cryptographic signatures to existing DNS records, helping the server correctly validate DNS responses.
- Securing and automatically renewing domain registration accounts.