DNS and DNS Snooping

T Naishitha

- The Internet Protocol is the core protocol the Internet uses. Each computer with Internet access has an assigned IP address so that other systems can send traffic to it.
- Each IP address consists of four numbers between 0 and 255 separated by periods, such as **74.125.45.100.**
- These numbers are perfect for computers that always deal with bits and bytes but are not easy for humans to remember.
- To solve this problem, the DNS was invented in 1983 to create easy-to-remember names that map to IP address.

- The primary goal that the designers of the DNS had in mind was scalability. This goal grew from the failure of the previous solution that required each user to download a multi thousand-line file named hosts.txt from a single server.
- To create a truly scalable system, the designers chose to create a hierarchy of “domains.” At the top of the hierarchy is the “root” domain under which all other domains reside.
- Just below the root domain are top-level domains (TLD) that break up the major categories of domains such as .com, .gov, and the country code TLDs.
- Below the TLDs are second-level domains that organizations and individuals can register with the registry that manages that TLD. Below second-level domains are the third-level domains and so forth, with a maximum of 127 levels.

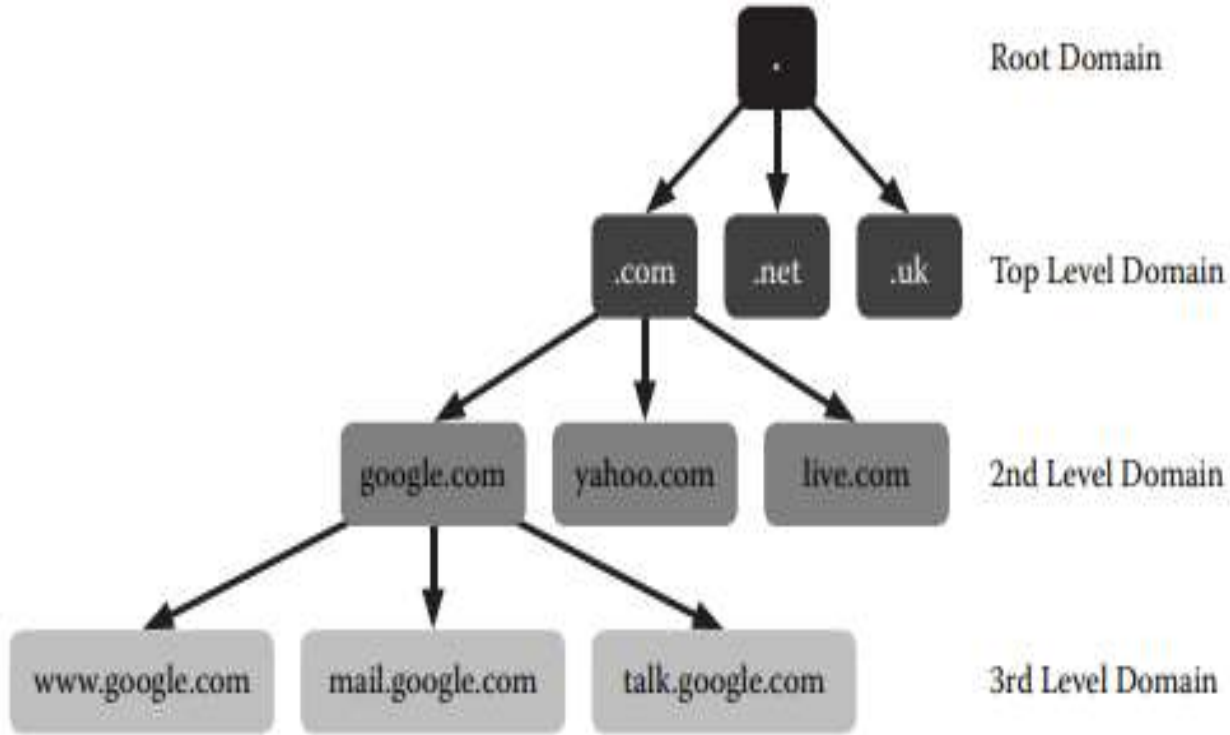


Exhibit 1-10 The hierarchical structure of the domain name system (DNS).

- Separating domains in this way allows different registries to manage the different TLDs. These registries are responsible for keeping the records for their assigned TLD and making infrastructure available to the Internet so users can map each domain name to its corresponding IP address
- The DNS uses computers known as name servers to map domain names to the corresponding IP addresses using a database of records. Rather than store information for every domain name in the system, each DNS server must only store the information for its domain. For instance, the name server gotgoogle.com keeps information for www. google.com and mail.google.com but not for www.yahoo.com. Name servers are granted authority over a domain by the domain above them, in this case .com.

- The hierarchical nature that defines the DNS is also a key to the resolution process.
- Resolution is the process of mapping a domain to an IP address, and resolvers are the programs that perform this function. Due to the nature of the resolution process, resolvers fall into two categories: recursive and nonrecursive.
- Exhibit 1-11 shows the steps required for a resolver to complete this process. The first step in resolving www.google.com is contacting the root name server to find out which name server is authoritative for .com.
- Once the resolver has this information, it can query the .com name server for the address of the google.com name server.
- Finally, the resolver can query the google.com name server for the address of www.google.com and pass it on to a Web browser or other program

- Fig depicts the most common way for systems to resolve domain names: by contacting a recursive DNS server and allowing it to do the work.
- A nonrecursive resolver (like the one used by a home PC) will only make a single request to a server, expecting the complete answer back.
- Recursive resolvers follow the chain of domains, requesting the address of each name server as necessary until reaching the final answer.
- Using recursive DNS servers also makes the system much more efficient due to caching.
- Caching occurs when a DNS server already knows what the answer to a question is, so it does not need to look it up again before responding to the query. The addresses of the root server and the .com server are usually cached due to the frequency with which systems request them.

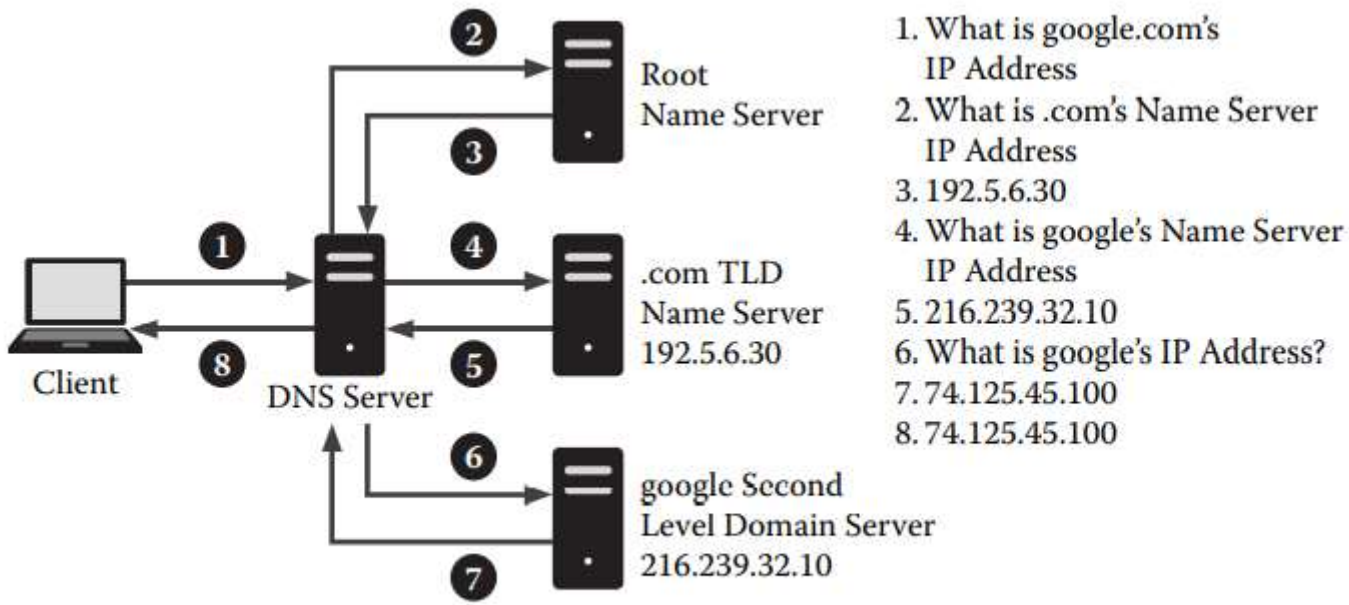


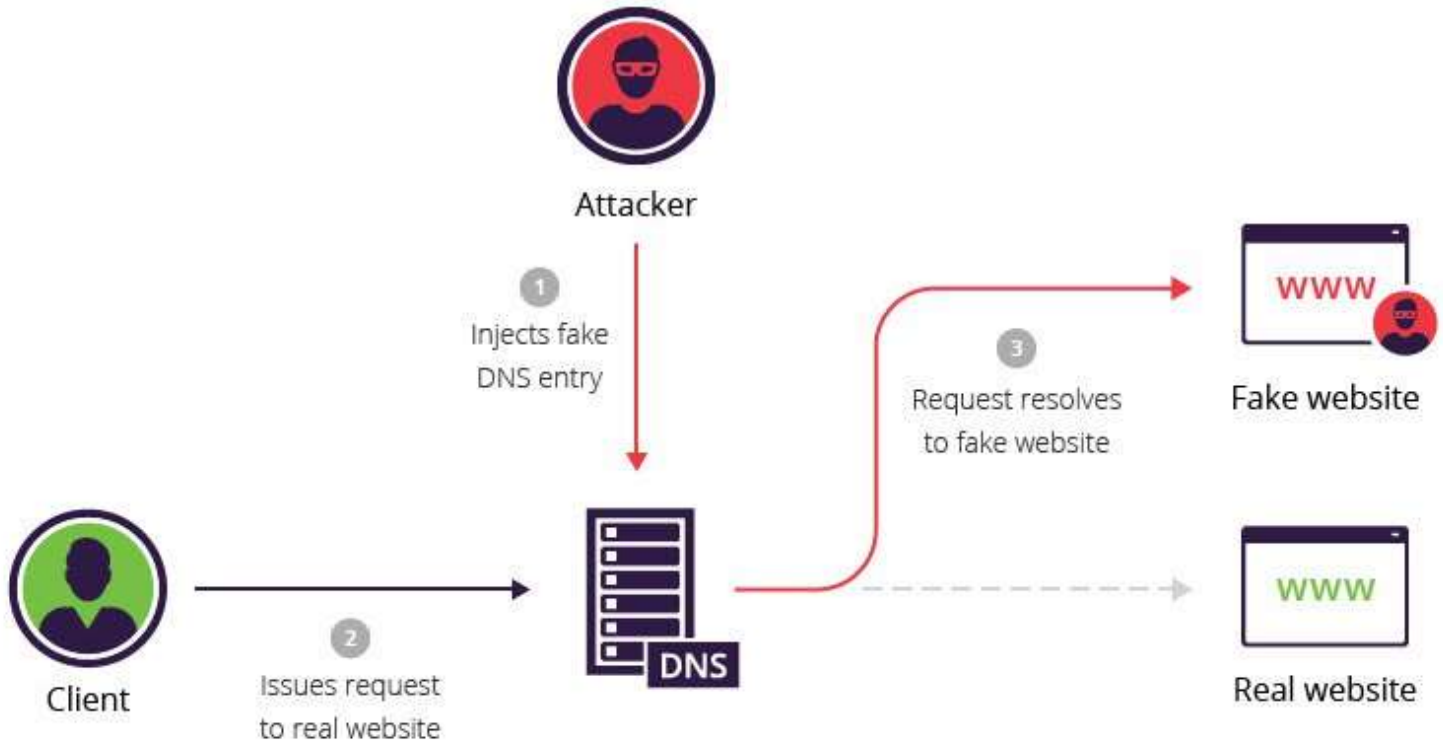
Exhibit 1-11 Resolution of google.com using a recursive DNS server.

DNS Snooping

- Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.
- Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information. Furthermore, the malicious website is often used to install worms or viruses on a user's computer, giving the perpetrator long-term access to it and the data it stores.
- Methods for executing a DNS spoofing attack include:

Man in the middle (MITM) – The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.

DNS server compromise – The direct hijacking of a DNS server, which is configured to return a malicious IP address.


Attacker
1
Injects fake
DNS entry
3
Request resolves
to fake website
www
Fake website
Client
2
Issues request
to real website
DNS
www
Real website