Agenda

- DNS Fundamentals
- DNS Security
- Summary

Last night, Jidong (at home, sitting in front of his laptop), opened his browser, typed www.youtube.com in the address bar, in the hope of watching the 2018 American Music Awards. However, he ended up opening www.porntube.com. Which of following, if happended, could cause this incident? (Choose all that apply.)

- A. Jidong's laptop was hacked.
- B. Jidong's home router was hacked.
- C. Youtube was hacked.
- D. Porntube was hacked.
- E. The DNS server that Jidong was using was hacked.
- F. Jidong's email account was hacked.
- G. Jidong's Facebook account was hacked.
- H. Google forgot to pay its bill.
- I. Jidong actually typed www.porntube.com in the address bar.

Last night, Jidong (at home, sitting in front of his laptop), opened his browser, typed www.youtube.com in the address bar, in the hope of watching the 2018 American Music Awards. However, he ended up opening www.porntube.com. Which of following, if happended, could cause this incident? (Choose all that apply.)

- A. Jidong's laptop was hacked.
- B. Jidong's home router was hacked.
- C. Youtube was hacked.
- D. Porntube was hacked.
- E. The DNS server that Jidong was using was hacked.
- F. Jidong's email account was hacked.
- G. Jidong's Facebook account was hacked.
- H. Google forgot to pay its bill.
- I. Jidong actually typed www.porntube.com in the address bar.

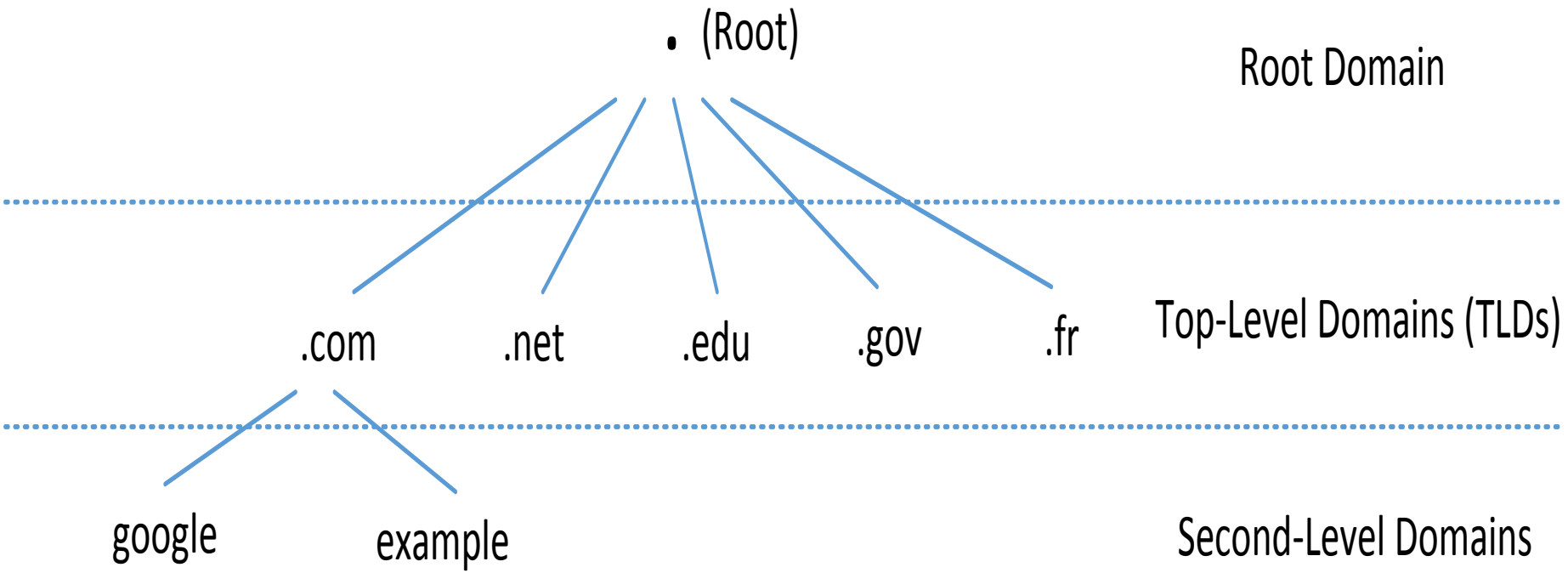
Basic Terminologies

- `DNS`: Domain Name System. A system designed to make computers easier to use for human beings. DNS maps domain names to IP addresses, like a phonebook map people's names to their phone numbers - it's easy to remember (people's and computer's) names than their numbers.
- `DNS nameserver`: A server that stores the DNS records, such as address (A) records, name server (NS) records, and mail exchanger (MX) records for a domain name and responds with answers to queries against its database. (port 53)
- `DNS resolver`: A local server that stores a central database of DNS nameservers and manages DNS requests for all the clients on your network. Sometimes people also use it to represent the client side of DNS, i.e., a component of your OS, which is responsible for initiating the queries.

Basic Terminologies

- `DNS hierarchy`: An inverted tree structure to manage the DNS database system.
- `DNS caching`: After your computer or a local DNS server obtains the query results from another DNS server, it will store the results in its cache for certain period of time.

DNS Hierarchy



Top-level domain: TLD;

Generic top-level domain (gTLD);

Country code top-level domain (ccTLD);

Fully qualified domain name (FQDN); A FQDN = host name + domain name.

DNS Message Format

Two types of DNS messages are used in DNS protocol: queries and replies, (same format). Each message consists of a header and four sections: question, answer, authority, and additional.

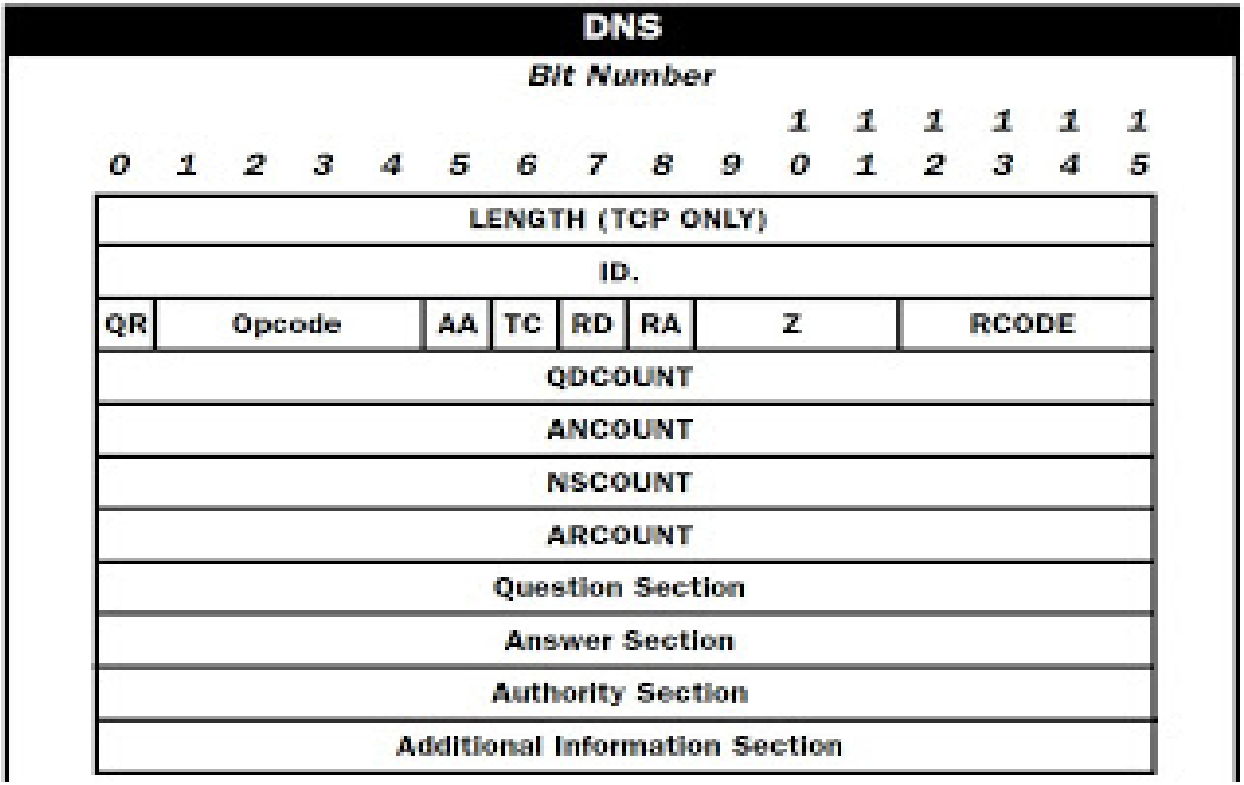


Image sources:
http://icanhazsecurity.ondrejdavid.com/2013/04/pentesting101-5-basic-protocols-overview.html

DNS Queries

- Recursive queries: the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message stating that the record or domain name does not exist. The DNS server cannot just refer the DNS client to a different DNS server. Thus, if a DNS server does not have the requested information when it receives a recursive query, it queries other servers until it gets the information, or until the name query fails.
- Iterative queries: when a DNS client allows the DNS server to return the best answer it can give based on its cache or data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral.

DNS Recursive and Iterative Queries

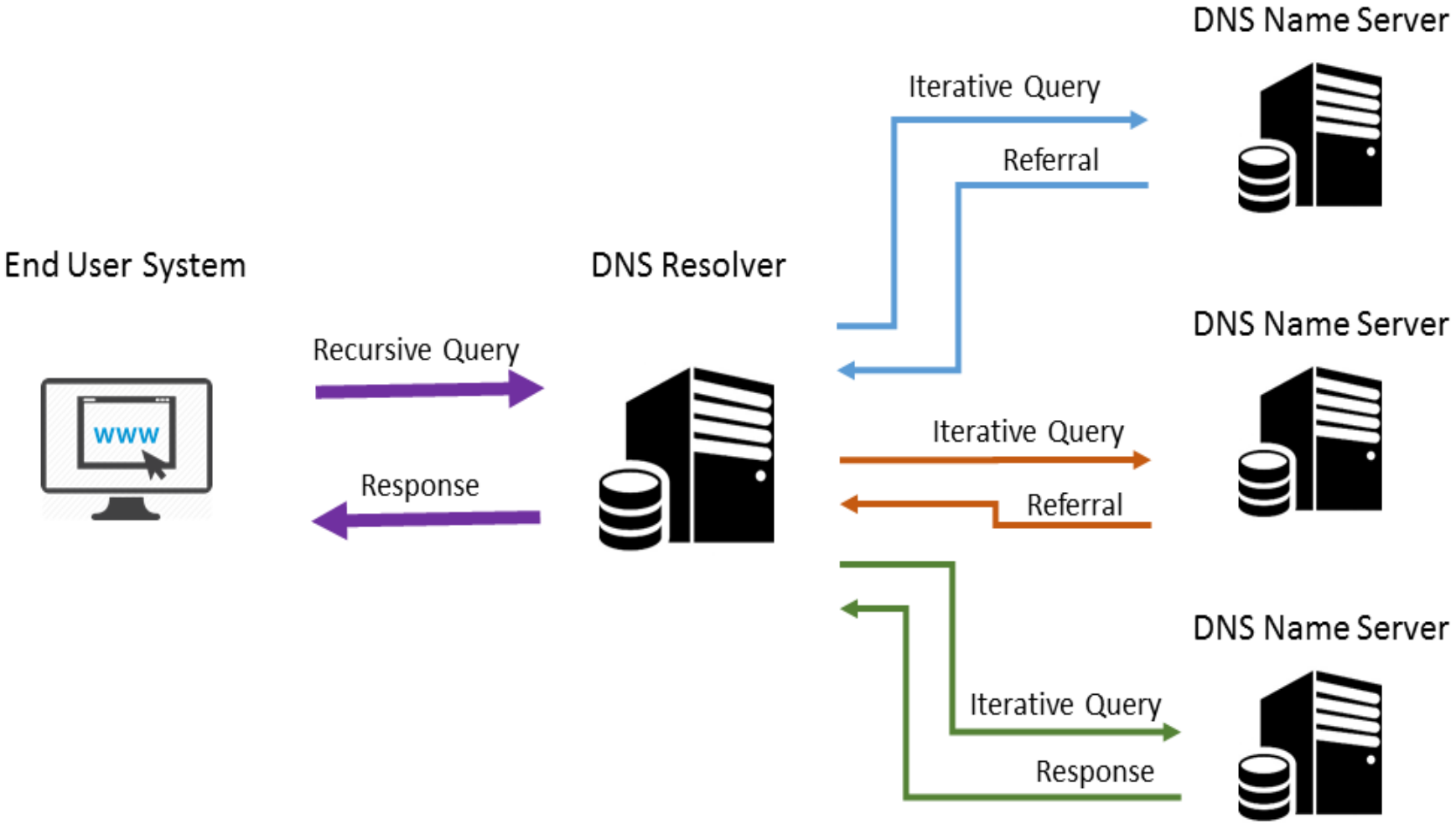
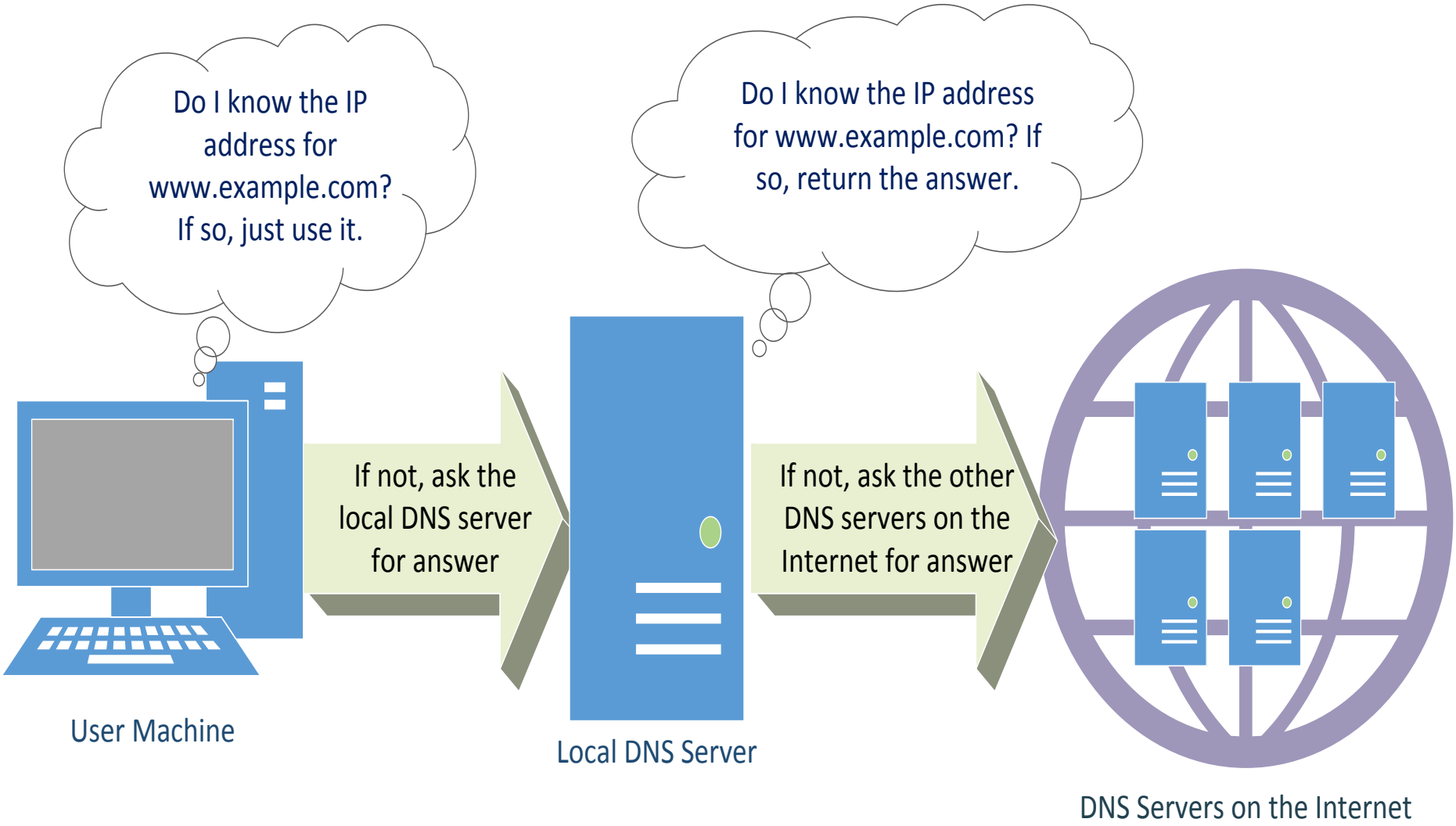
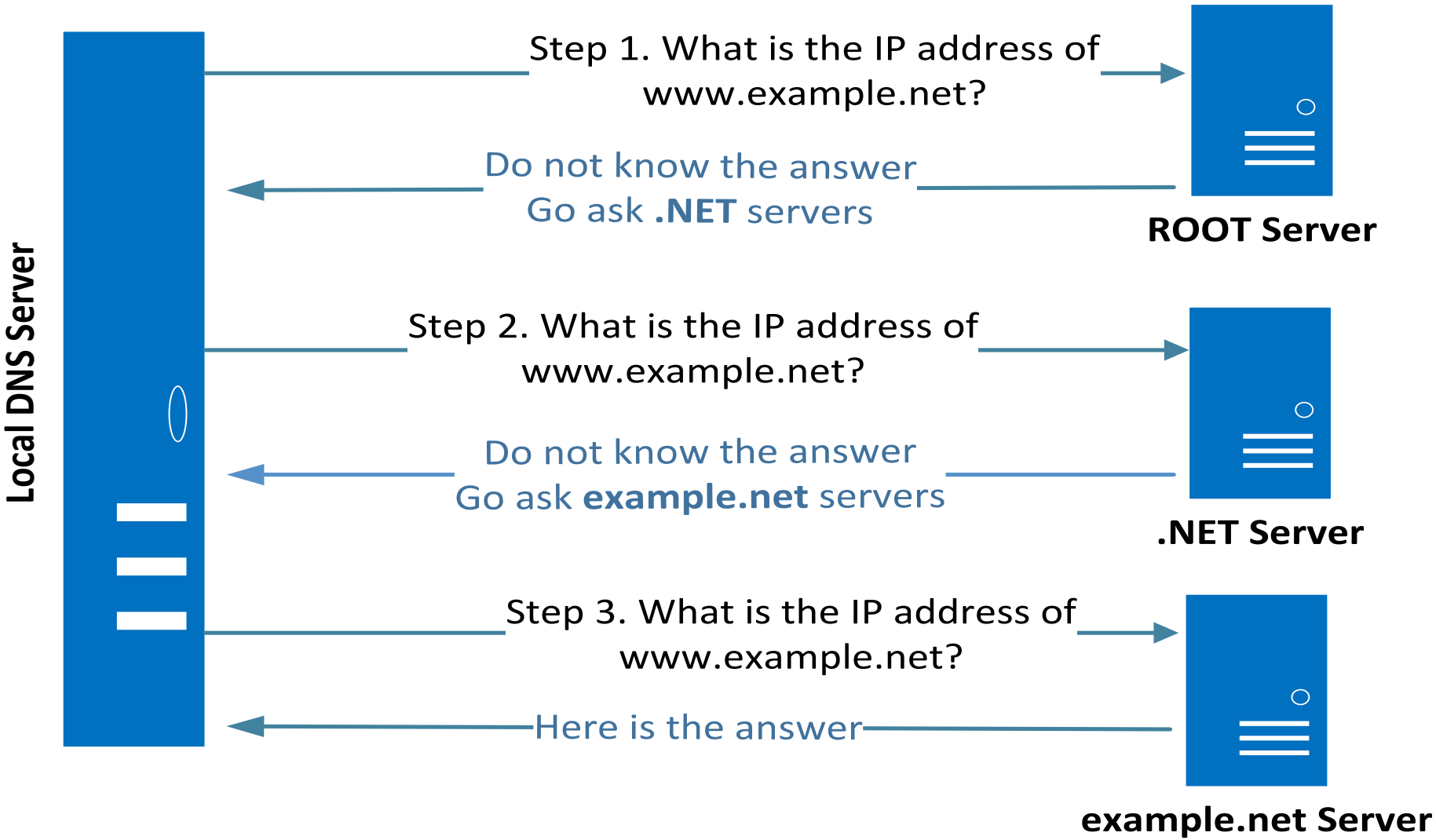


image source:
https://ominouspacket.com/2017/01/13/part-4-dns-address-resolution-the-dns-resolver/

DNS Recursive Queries



DNS Iterative Queries



Useful DNS Tools - dig

- Name resolution: dig boisestate.edu;
- Reverse lookup: dig -x 132.178.214.91
- Find a domain's mail server: dig boisestate.edu MX

Useful DNS Tools - dig

- nslookup
- whois

DNS Security

- DNS spoofing - impact: temporary
- DNS cache poisoning - impact: permanent (or until ttl expires)
- DNS pharming - impact: permanent
- DNS amplification/reflection - impact: temporary

DNS Spoofing

Answering DNS request that intended for another server (a real DNS server).

- Spoofs the DNS server's answer by answering with the DNS server's IP address in the packets source-address field
- client-server exchange or server-server exchange.

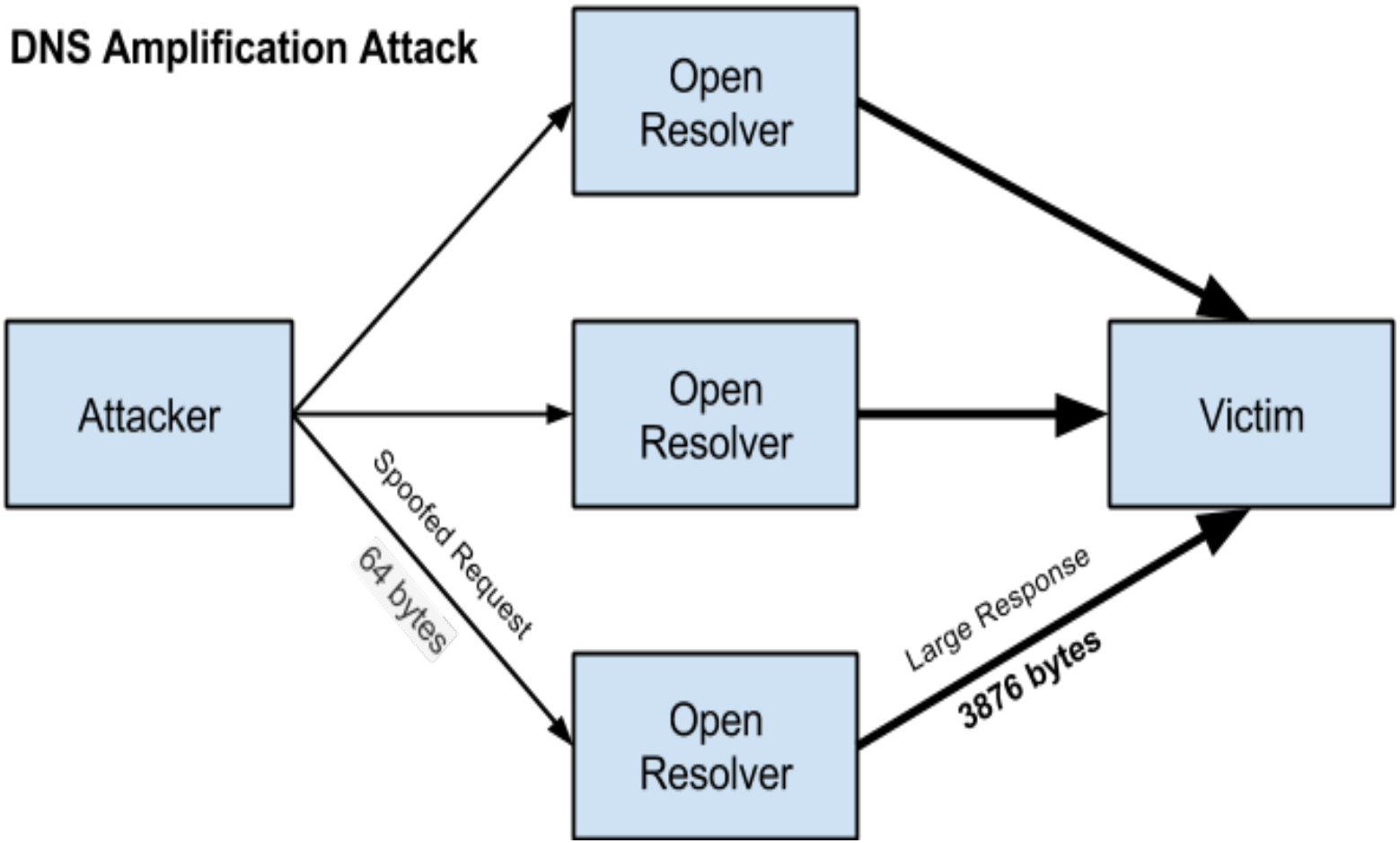
DNS Cache Poison

- Making a DNS server cache false information
- e.g., try to make the ns.defense.gov DNS to answer with the IP of the hacker's computer to any query about the IP of telnetaccess.defense.gov.

DNS Pharming

- Change the DNS server setting on a victim's computer.
- Or change the DNS server setting on the DHCP server.
- DHCP: Dynamic Host Configuration Protocol.

DNS Amplification/Reflection



A type of DoS attack

Image sources: https://blog.opendns.com/2014/03/17/dns-amplification-attacks/

DNS Amplification/Reflection

Three factors that make DNS amplifcation/reflection possible:

- Forgeability of source addresses of DNS messages.
- Availability of open resolvers: A DNS resolver is open if it provides recursive name resolution for clients outside of its administrative domain.
- Asymmetry of DNS requests and responses: "ANY requests ask the DNS resolver for ALL information that it currently knows about the domain which may include where the mail servers are (MX records), what the IP addresses are (A records) and so on. Attackers use this type of query to maximize the size of the response sent to the victim." See more at: https://blog.opendns.com/2014/03/17/dns-amplification-attacks/

Summary

- DNS database: inverted tree structure.
- DNS queries: recursive, iterative.
- DNS attacks: DNS spoofing, DNS cache poison, DNS pharming, DNS Amplification.

References

A large portion of the material is adapted from:

- Security Issues with DNS - SANS Institute
- Top Five DNS Security Attack Risks and How to Avoid Them - Infoblox
- What Are Domain Name System (DNS) Resolvers and How Do They Work? http://smallbusiness.chron.com/domain-name-system-dns-resolvers-work-76639.html
- Computer Security - A Hands-on Approach by Wenliang Du