DNS and Attacks

18.1. Instead of referring your own computer as `localhost`, you would like to refer it as `myhost`. What should you do to make that happen?

18.2. Please use the `dig` command to get the nameserver information about the `nsf.gov` domain.

18.3. What protocol and port number does DNS use?

18.4. Please verify that DNS queries can be sent over the TCP protocol. Hint: The `dig` command has a TCP option, which tells `dig` to use TCP to send DNS queries. You can run this command and show the DNS packets captured by Wireshark.

18.5. Your computer wants to get the IP address of `www.example.com`. Please use the `dig` command to emulate what your local DNS server will do in order to get the IP address for you. Please show the result for each emulation step.

18.6. Your computer wants to get the domain name for the IP address `93.184.216.34`. Please use the `dig` command to emulate what your local DNS server will do in order to get the domain name for you. Please show the result for each emulation step.

18.7. How does the DNS client software running on a local DNS server know the IP addresses of the root server?

18.8. What fields of a DNS query packet contain random data that need to be included in the response?

18.9. What is DNS cache poisoning attack?

18.10. What are the fundamental problems of the DNS protocol that makes DNS vulnerable to DNS cache poisoning attacks?

18.11. To launch DNS cache poisoning attacks on remote DNS servers is quite challenging. (1) Please describe what exactly those challenges are. (2) Please describe how the Kaminsky attack solved those challenges.

18.12. Bob wants to launch a Kaminsky DNS cache poisoning attack on a recursive DNS resolver; his goal is to get the resolver to cache a false IP address for the hostname `www.example.com`. Bob knows that during the iterative process, a query will be sent to the root server, then to the `.COM` nameserver, and finally to the `example.com`'s nameserver. He can choose to spoof replies from any of these nameservers, after triggering the iterative process from the resolver. He decides to spoof a reply from the `.COM` server. Please describe whether Bob's attack will be successful or not.

18.13. Bob wants to launch a Kaminsky DNS cache poisoning attack on a recursive DNS resolver. His objective is to poison the cache of the DNS resolver, so his own nameserver can provide answers to any query related to the `bank32.com` domain. Bob needs to spoof DNS replies. Please describe an example of Bob's spoofed reply. Please use the format like the output of the `dig` command to describe your answer.

18.14. Bob wants to launch a Kaminsky DNS cache poisoning attack on a recursive DNS resolver, but his machine does not have a hostname (he launches the attack from a coffee shop using its Wi-Fi). He plans to use a random hostname in the authority section, and then provides his machine's IP address in the additional section. See the following portion of his spoofed reply. Would this approach work?

```
;; AUTHORITY SECTION:
example.com. 259200   IN   NS   ns.ARandomName.net

;; ADDITIONAL SECTION:
ns.ARandomName.net 259200 IN  A  132.2.1.4
```

18.15. The following is a DNS reply received by a local DNS server. Please describe which parts of the answer will not be cached by the DNS server. Please explain why.

```
;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 259200 IN A 129.211.32.34

;; AUTHORITY SECTION:
example.net. 259200 IN NS ns.tklp-server.net
example.com. 259200 IN NS ns.gltd-server.net

;; ADDITIONAL SECTION:
ns.gltd-server.net 259200 IN A 132.2.10.9
ns.tklp-server.net 259200 IN A 130.3.11.39
ns.atfz-server.com 259200 IN A 128.0.31.66
```

18.16. Company XYZ sets up a website `www.example.com` for its internal use only, so only computers inside the company can access it. Instead of setting up a firewall to limit the access, the administrator of the web server decides to use reverse DNS lookup to check whether a client belongs to the company or not. For example, when an HTTP request comes in, the web server extracts the IP address from the request packet, conducts a reverse DNS lookup to get the hostname corresponding to the IP address. If the hostname ends with `example.com`, access is granted; otherwise, access is denied. You are an outsider, can you find a way to access this website?

18.17. DNS root servers use IP Anycast to improve its scalability, which is essential against DDoS attacks. IP Anycast allows many computers to share the same IP address. These computers are typically distributed geographically. Packets to an Anycast IP address will be routed to any one of these computers, selected on the basis of which is the nearest, lowest cost, with the least congested route, or some other distance measure. Please describe how DNS root servers use this technology to achieve scalability.

18.18. If you manage a DNS zone, what would you do to reduce the risk of DDoS attacks on your network?

18.19. In cyberwars between two counties, the root DNS servers of each side will be primary targets. If country A can bring down all the root servers of country B, A can effectively

cut off the communication between B and the outside world. Assume that your job is to manage the root DNS server for country B, which is a small country that does not have sufficient resources to defend against large-scale DDoS attacks from its powerful foe. What can you do?

18.20. Recursive DNS server, if not configured correctly, can be used for DNS amplification attack, which is a type of DDoS attacks, in which attackers can use third-party servers (in this case, DNS servers) to amplify the power of their attacks. Please find the information about this kind of attack from the Internet, and provide a summary of the attack.

18.21. In the DNS rebinding attack example described in the book, what prevents the attacker from directly interacting with the target IoT server?

18.22. In the DNS rebinding attack, how can the attacker's JavaScript code running inside the victim's browser defeat the browser's Same-Origin policy?

18.23. In the DNS rebinding attack, if the victim's browser caches the IP address for any hostname used in HTTP requests for an hour, can the attack still be successful? Why?