CIS 435 + 535 – Fall 2020

DNS Fundamentals, Attacks, and Countermeasures

- **Read Textbook thoroughly and answer the following questions.**
- **Provide Screenshots whenever applicable.**

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?

   Add"127.0.0.1 myhost"toyour/etc/hostsfile.

2. What protocol and port number does DNS use?

   DNS uses UDP by default, but under certain circumstances, especially when the size of the response is large, DNS switches to TCP. In both cases, the port number used is 53.

3. 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.

   $ dig +tcp www.example.com

```
25090:~ yun$ dig +tcp www.example.com

; <<>> DiG 9.10.6 <<>> +tcp www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43609
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        1440    IN      A       93.184.216.34

;; Query time: 77 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Oct 04 22:06:40 CDT 2020
;; MSG SIZE  rcvd: 60
```

4. 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.

   See Textbook Pages 286 - 287.

```
25090:~ yun$ dig @a.root-servers.net www.example.com

; <<>> DiG 9.10.6 <<>> @a.root-servers.net www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36895
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.example.com.               IN      A

;; AUTHORITY SECTION:
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
```

```
25090:~ yun$ dig @a.gtld-servers.net www.example.com

; <<>> DiG 9.10.6 <<>> @a.gtld-servers.net www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64588
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; AUTHORITY SECTION:
example.com.            172800  IN      NS      a.iana-servers.net.
example.com.            172800  IN      NS      b.iana-servers.net.

;; Query time: 27 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sun Oct 04 21:51:56 CDT 2020
;; MSG SIZE  rcvd: 92
```

```
25090:~ yun$ dig @a.iana-servers.net www.example.com

; <<>> DiG 9.10.6 <<>> @a.iana-servers.net www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17497
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.34

;; Query time: 37 msec
;; SERVER: 199.43.135.53#53(199.43.135.53)
;; WHEN: Sun Oct 04 21:52:40 CDT 2020
;; MSG SIZE  rcvd: 60
```

5. 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.

   See Textbook Page 305 for commands of reverse DNS lookup

```
25090:~ yun$ dig @a.root-servers.net -x 93.184.216.34

; <<>> DiG 9.10.6 <<>> @a.root-servers.net -x 93.184.216.34
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31905
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;34.216.184.93.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
in-addr.arpa.           172800  IN      NS      e.in-addr-servers.arpa.
in-addr.arpa.           172800  IN      NS      f.in-addr-servers.arpa.
```

```
25090:~ yun$ dig @e.in-addr-servers.arpa -x 93.184.216.34

; <<>> DiG 9.10.6 <<>> @e.in-addr-servers.arpa -x 93.184.216.34
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51499
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;34.216.184.93.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
93.in-addr.arpa.        86400   IN      NS      ns3.afrinic.net.
93.in-addr.arpa.        86400   IN      NS      tinnie.arin.net.
93.in-addr.arpa.        86400   IN      NS      ns3.lacnic.net.
```

```
25090:~ yun$ dig @ns3.afrinic.net -x 93.184.216.34

; <<>> DiG 9.10.6 <<>> @ns3.afrinic.net -x 93.184.216.34
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21524
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;34.216.184.93.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
216.184.93.in-addr.arpa. 172800 IN      NS      ns2.edgecastcdn.net.
216.184.93.in-addr.arpa. 172800 IN      NS      ns1.edgecastcdn.net.
```

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

   According to IANA, operators who manage a local DNS server typically need to configure a “root hints file”. This file contains the names and IP addresses of the authoritative name servers for the root zone, so the software can bootstrap the DNS resolution process. For many pieces of software, this list comes built into the software.

7. What is DNS cache poisoning attack?

When a local DNS server sends out a DNS query, attackers can spoof the response and provide false information, such as the IP address and nameserver information in the response. If the response is accepted by the local DNS server, the false information may be kept in the DNS cache for a period of time, and affect future DNS queries. In a sense, it "poisons" the DNS cache.

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

The DNS protocol does not include any mechanism to verify the authenticity of a DNS reply, so after receiving a DNS reply, the client cannot tell whether the reply is authentic or fraudulent. DNSSEC basically solved this fundamental problem using digital signatures.

9. 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.

Challenges

1) Need to guess Transaction ID (16-bit random number)
2) Cache effect: If one attempt fails, the actual reply will be cached by local DNS server; attacker need to wait for the cache to timeout (TTL) for the next attempt.

Kaminsky's Idea:

1) Ask a different question every time, so caching the answer does not matter, and the local DNS server will send out a new query each time.
2) Provide forged answer in the **Authority section**

10. Briefly Describe DNSSEC.

DNSSEC is a set of extension to DNS, aiming to provide authentication and integrity checking on DNS data. With DNSSEC, all answers from DNSSEC protected zones are digitally signed.

By checking the digital signatures, a DNS resolver is able to check if the information is authentic or not. DNS cache poisoning will be defeated by this mechanism as any fake data will be detected because they will fail the signature checking.

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

There are several approaches to reduce the risk of DDoS attacks. One way is to increase the power of the nameservers and the bandwidth of the network. Another way is to outsource the DNS services to other companies specializing in DNS providers. For example, the company Dyn provides DNS services to many companies. Many enterprises, such as Netflix, Twitter, and Linkedin are powered by Dyns DNS solutions.

12. 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
```

In the Authority section, the NS record for example.net will not be accepted, because it is out of the zone of example.com.