# Quiz 4

CSE-644 INTERNET SECURITY

DR. SYED SHAZLI

2/12/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

1) What is DNS, why do we need DNS?

The Domain Name System (DNS) translates domain names with their IP addresses. It is necessary so that humans can access domains using their domain names, which are easier to remember than their IP addresses.

2) How does DNS do its query? What does it check the first, what does it check next etc.?

When a user requests access to a domain using its domain name, the local domain name server will search its local cache memory for the IP address first. The local cache contains a file with static mapping between domain names and their IP addresses. If there is no match found, the local DNS will query the internet by sending a request to the root server. Based on the domain name, the root server will redirect the local DNS request to another DNS that owns that domain name.

3) What is DNS cache? What is it used for?

DNS cache is a file containing a static table of domain names and their IP addresses. It is used as a quick look-up table for recently visited domains so that the local DNS does not have to query the root server for each request. Performance is improved by having a DNS cache.

4) What is DNS cache poisoning?

When a local DNS sends a request to another server over the internet, it is susceptible to a DNS cache poisoning attack. The attacker may spoof a reply to the local DNS ahead of the authentic reply from the other server. Then the DNS cache on the local machine will store the attacker's IP address with the searched domain name. The attacker's IP address leads to the attacker's domain, which may have malicious content.

5) What is necessary for your spoofed packet to successfully spoof attack the DNS?

To launch a DNS cache poisoning attack, the attacker must spoof the response to the local DNS using UDP packets. The parts of the UDP packet that must match are the Source/Destination IP addresses, Source/Destination port numbers, and the transaction ID (a randomly generated 16-bit number). If the attacker is on the local network, sniffing and spoofing techniques may be used to obtain the destination port number. If the local DNS accepts the spoofed reply, it will be cached in the DNS cache for as long as the attacker specified in the packet (1 day, 1 month, etc.).

6) What is Kaminsky attack?

What if the attacker is not on the local network? What if the attacker is remote? Remember that the attacker needs the destination port number (16-bit number) and the transaction ID (16-bit number). 16+16 = 32. 2^32 number of guesses (achievable). The attacker spoofs the reply. If the guesses are incorrect, the reply is dropped by the DNS. The real (correct) reply will be accepted. The cache stores the correct information for a long time (possibly days). The attacker must wait for the cache to clear (days) before attempting to guess again.

The Kaminsky attack involves launching an attack without waiting for the DNS cache to clear. The attacker triggers a request for a random website. The local DNS will trigger the request to the root server or domain server. The attacker will send a spoofed reply to this query to the local DNS. The IP address in the spoofed reply does not matter. In the authority section, fake information is provided in

the name server. Example authority section: “example.com nameserver.attacker.com”. The nameserver.attacker.com is obviously fake, but it looks legitimate because it is quite common for a domain to be hosted by a 3rd party computer’s DNS. Therefore, the attacker does not need to be in the same domain as the queried domain name to launch the attack.

If the spoofed reply fails, the IP address in the answer section was incorrect, and the UDP packet is dropped. The authentic reply is cached in the local DNS. However, it does not really affect the attacker’s approach as they will try “a2.example.com” next. Then they will try “a3.example.com”. The attacker will keep changing the domain name until the IP address in the answer section is correct. Once the answer is accepted by the local DNS server, whenever someone wants to visit the example.com domain, they will be redirected to the attacker’s domain.

To protect against the Kaminsky attack, encrypt all UDP packets.

7) What is Denial-of-Service attack on DNS servers?

If an attacker can bring down the root server, they will bring down the entire internet. When a query is sent out, the root server is the starting point for all queries. The root server is very robust because there are duplicate locations with many computers servicing each location. But the attacker can target one level lower than the root server. There are major servers at this level, and they too are robust.

An attacker can target a DNS server at these lower levels by flooding the network with many queries. Other servers that use the targeted DNS will not be able to access the domain names belonging to that server.

The most famous internet incident in China involved two rival gaming companies in which one launched a DOS attack on the other’s DNS. The attacker did not realize that the Chinese version of YouTube also relied on this DNS. When the DNS crashed, it flooded the internet with query requests from the Chinese YouTube, causing the worst internet incident in China. The entire Chinese DNS crashed due to this denial-of-service attack.