Name: Kazi Noshin

Student ID: 1605071

Attack Tool 19: DNS cache poisoning + Phishing attack

Contents

Definition of the attack with topology diagram:

Definition of the attack:

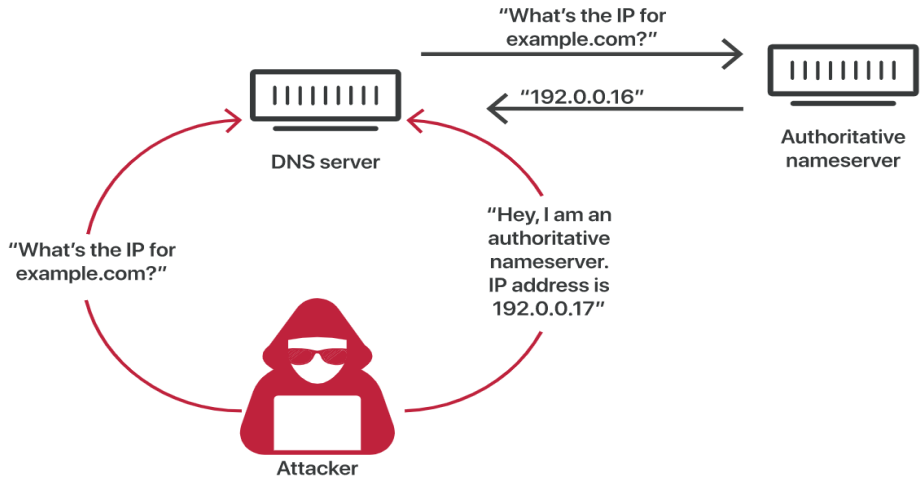
- **DNS cache poisoning** is the act of entering false information into a DNS cache so that DNS queries return an incorrect response and users are directed to the wrong websites.
- **Phishing attack** refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data in order to utilize or sell the stolen information, by pretending as a reputable website with an enticing request.

Relation between DNS cache poisoning and phishing attack:

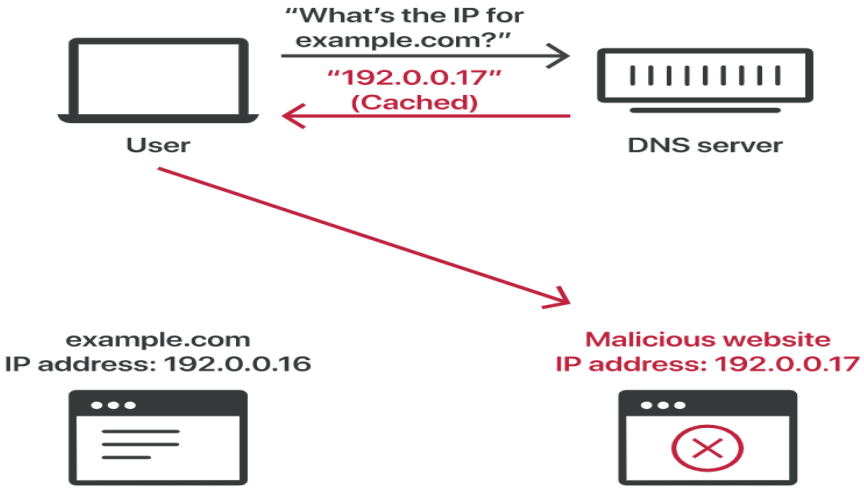
An attacker can poison the DNS cache and direct users to the false website to gain personal information which will be a phishing attack.

Topology Diagram:

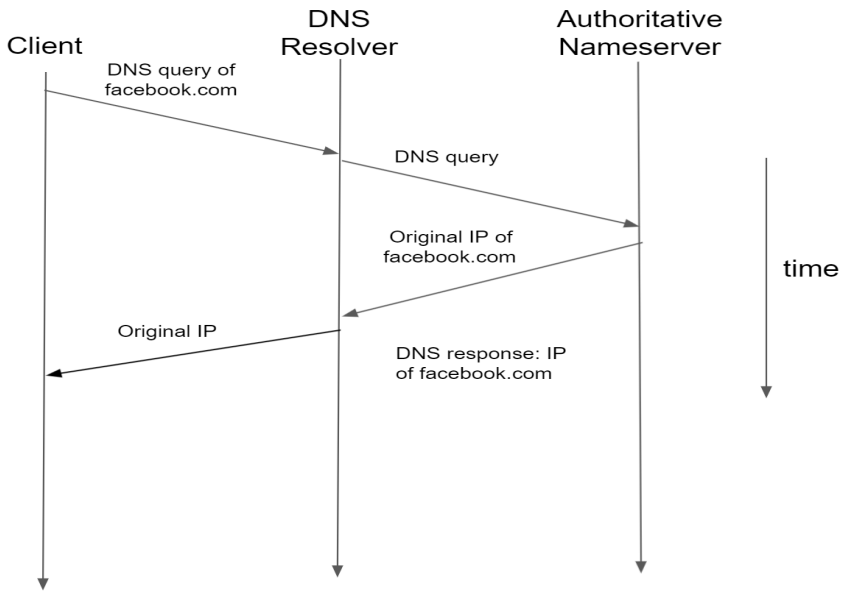
DNS Cache Poisoning Process:



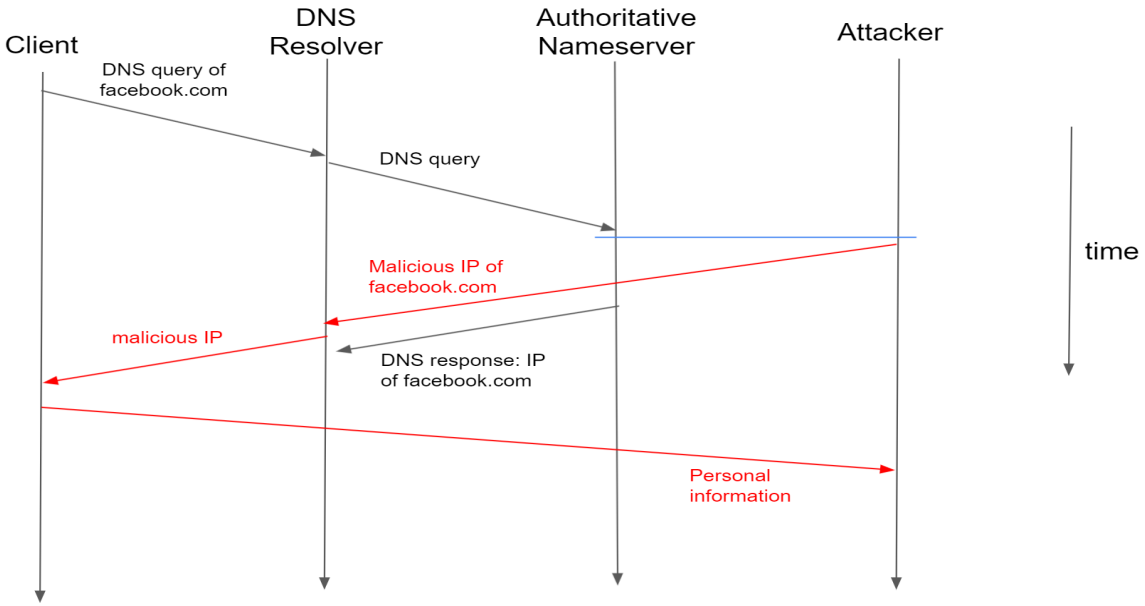
Poisoned DNS Cache:



Timing diagram of the original protocol :



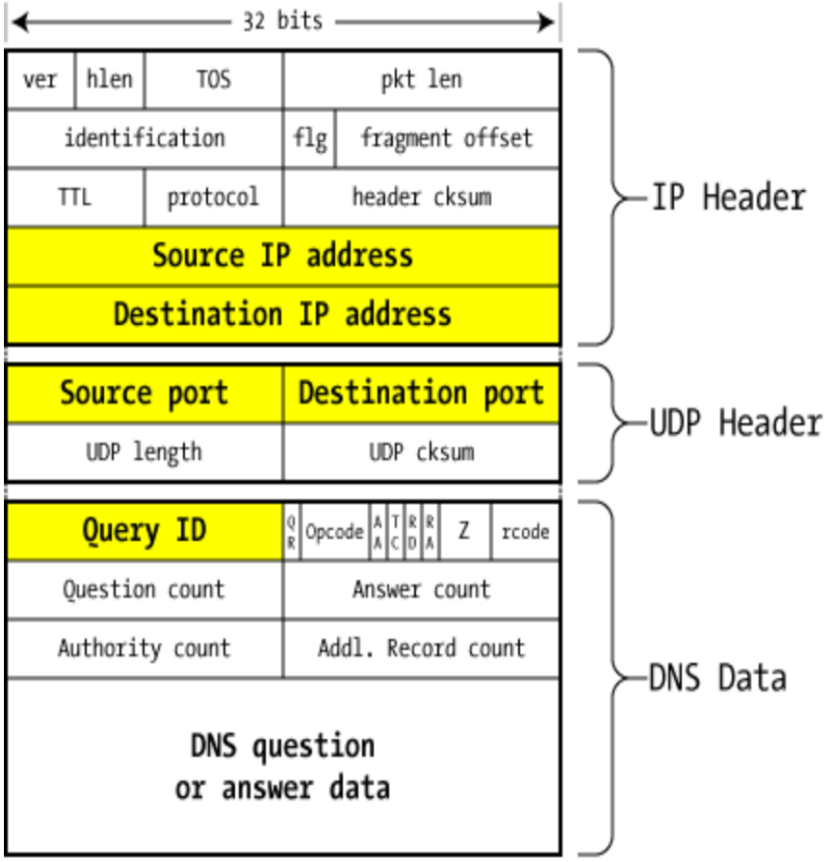
Attack timing diagram with attack strategies:



Attack strategy:

- The attacker sends a DNS query to the victim nameserver for the hostname it wishes to hijack.
- The bad guy starts flooding the victim with forged DNS reply packets, knowing that the victim will shortly be asking the authoritative server (through recursion) for an IP address. All purport to be from the real server but include the answer with the IP of the attacker's malicious webserver.
- The victim nameserver asks the real server for the IP address.
- The real nameserver provides a legitimate response to this query, with the appropriate query id. But if the attacker has successfully matched the query ID during flooding, this legal reply arrives too late and is ignored.
- With the false IP address (of the attacker's webserver) in the cache, the victim server provides this poisoned answer to the requesting DNS client.

Packet details for attack:



DNS packet on the wire

Some of the fields that are related to this attack:

Field	Description
Source / Destination IP address	• These reflect the IP addresses of the machines that sent and should receive the packet. It's possible to forge the source address, but pointless to forge the destination.
Source / Destination port numbers	• DNS servers **listen on port 53/udp** for queries from the outside world, so the first packet of any exchange always includes 53 as the UDP destination port. • The **source port varies** considerably, sometimes it's also port 53/udp, sometimes it's a fixed port chosen at random by the operating system, and sometimes it's just a random port that changes every time. • As far as DNS functionality is concerned, the source port doesn't matter as long as the replies get routed to it properly. But this turns out to be the weapon of the poison attack.
Query ID	• This is **a unique identifier created in the query packet that's left intact by the server sending the reply**: it allows the server making the request to associate the answer with the question.

	This is also sometimes called the Transaction ID (TXID).
QR (Query / Response)	• Set to 0 for a query by a client, 1 for a response from a server.
AA (Authoritative Answer)	• Set to 1 in a server response if this answer is Authoritative, 0 if not.
RA (Recursion Available)	• The server sets this to indicate that it will (**1**) or won't (**0**) support recursion.
Question record count	• The client fills in the next section with a single "question" record that specifies what it's looking for: it includes the name (www.facebook.com), the type (A, NS, MX, etc.), and the class (virtually always IN=Internet). • The server repeats the question in the response packet, so the question count is almost always 1.
Answer/authority/additional record count	• Set by the server, these provide various kinds of answers to the query from the client.
DNS Question/Answer data	• This is the area that holds the question/answer data referenced by the count fields above.

Resource Record Types:

Each DNS query or response includes a name, a type, and (for a response) a value.

The resource types represent different purposes.

For example:

Type	Description
A	This is an **IP Address record** and is used to translate from a domain name to an IPv4 address.
NS	It **lists which name servers can answer lookups** on a DNS zone.
MX	This record specifies the mail server used to handle mail for a domain specified in an email address.

Modification in the header:

In the DNS answer data section, the desired IP and TTL(Time To Live) get modified by the attacker.

<table>
<tr><th>Good DNS</th><th>Poisoned DNS</th></tr>
<tr><td>
<table>
<tr><th>Answer</th><th>IP</th><th>TTL</th></tr>
<tr><td>An</td><td>IP of facebook.com</td><td>1 hr</td></tr>
</table>
</td><td>
<table>
<tr><th>Answer</th><th>IP</th><th>TTL</th></tr>
<tr><td>An</td><td>IP of attacker’s malicious website</td><td>2 dy</td></tr>
</table>
</td></tr>
</table>

The attacker usually sets a very high TTL in the poisoning responses so that the victim will keep the bogus data in the cache as long as possible.

Justification:

- **Attackers can poison DNS caches by impersonating DNS nameservers**, making a request to a DNS resolver, and then pretending the response is from a legitimate server by forging the header data of the reply when the DNS resolver queries a nameserver. **This is possible because DNS servers use UDP** instead of TCP, and because currently there is no verification for DNS information.
- Most of the forged answers are dropped because the Query ID doesn't match, but **if just one in the flood of fake responses gets it right, the nameserver will accept the answer as genuine.** And because that satisfies the request, the real answer that arrives later is dropped, because the query is no longer pending.