**CSE-406**

**Computer Security Sessional**

horizontal line

# 

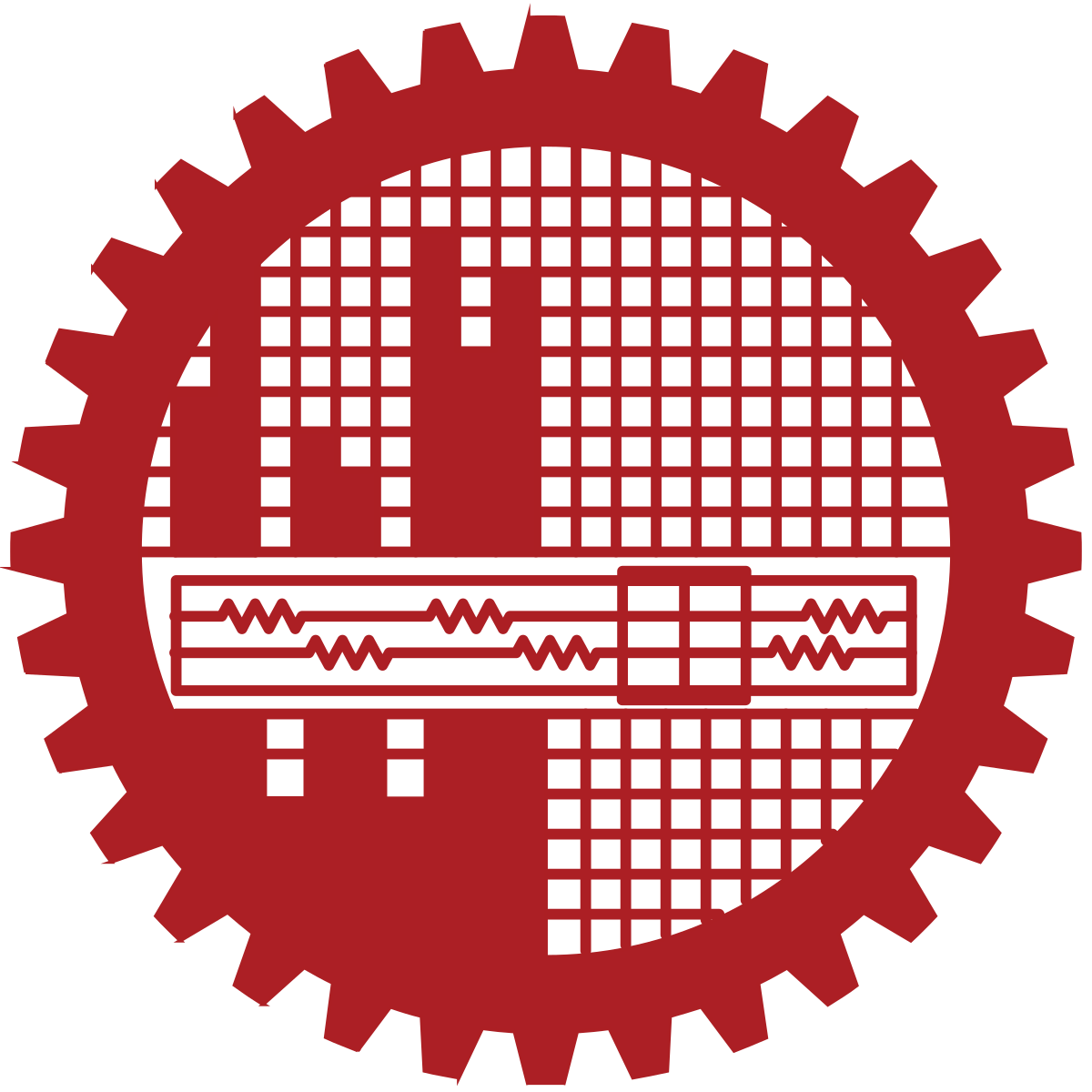
# **DNS Cache Poisoning**

# 

**Submitted by: Submitted to:**

**Md. Imran Hasan Dr. Md. Shohrab Hossain**

**1505026 Nafis Irtiza Tripto**



Department of CSE,

Bangladesh University of Engineering and Technology,

Dhaka-1205.

Attack Configuration:

In this attack, I used Man-In-The-Middle approach. To simulate this attack I used one ubuntu host machine(attacker) and another one in virtual machine(victim). The network traffic of guest os flows through the host os. So, I placed the attacker in host os to sniff the packets of victim. Figure 1 describes the attack scenario.

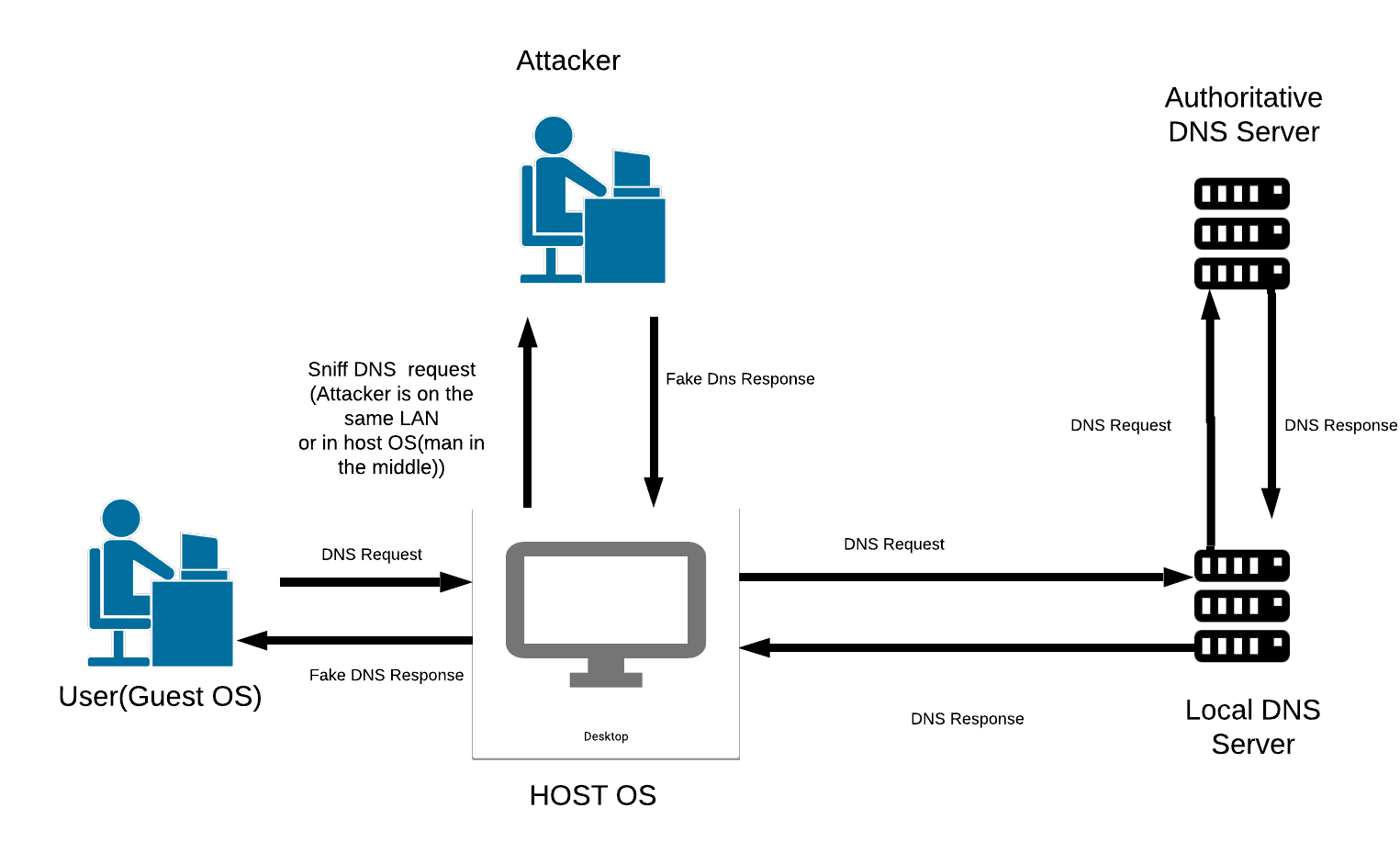


Figure 1: DNS cache poisoning

I used NAT network option of virtual box. Bridged network option is applicable to. We have to ensure that the attacker can sniff the victims network traffic.

Steps of Attack:

In this attack, I followed four steps. The steps are described below:

1. Sniff victims DNS request:

To sniff packet I used pcap library. In attacker machine, the sniffer captured all traffic of victim.

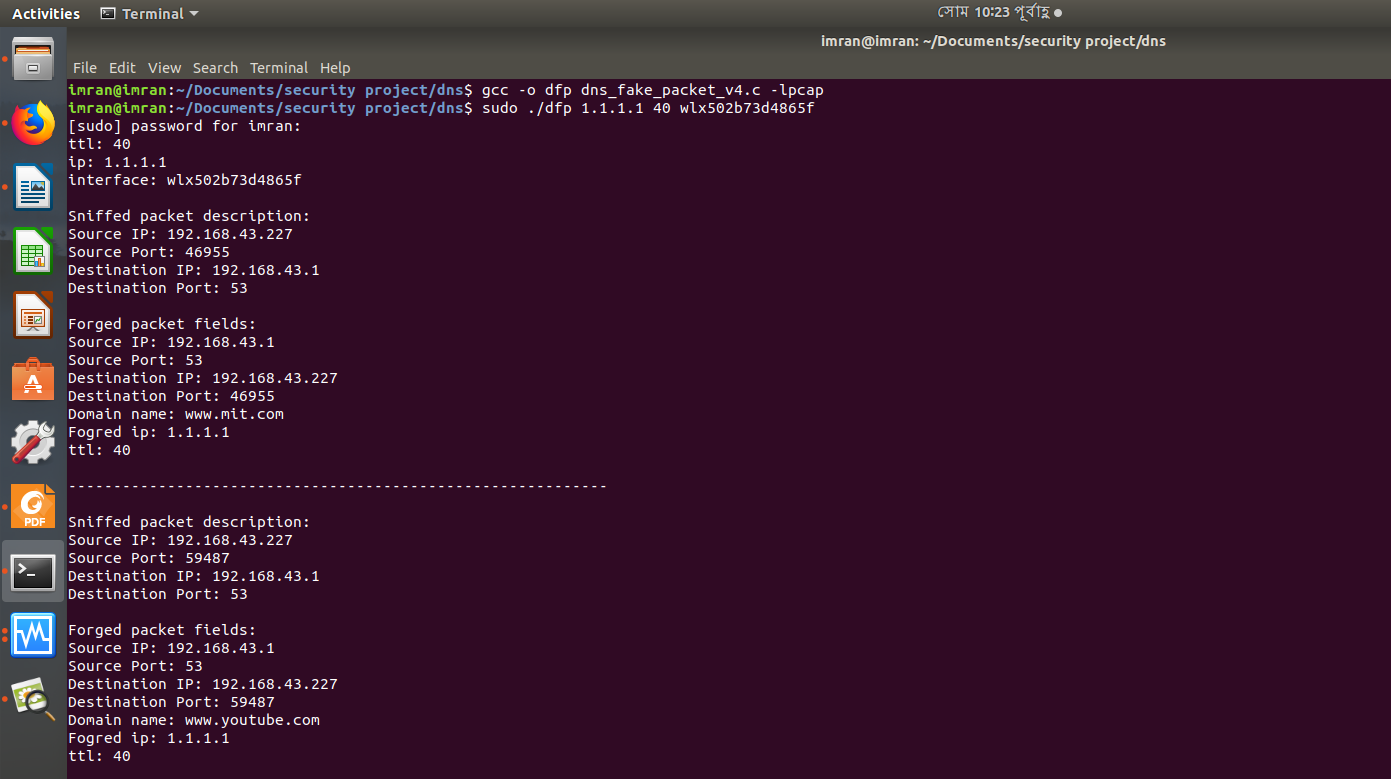


Figure 2: Sniffed DNS packets

In pcap, it is possible to filter network traffic to get specific types of packet. I set filter parameters to get DNS traffic.

1. Parse DNS packet:

I parsed the received packet and retrieved IP, UDP, DNS layers header fields and data. In this step, I checked if received packet is DNS query or not. If not then the packet had been discarded. The DNS layers transaction ID, Question Section and Additional Section had been stored.

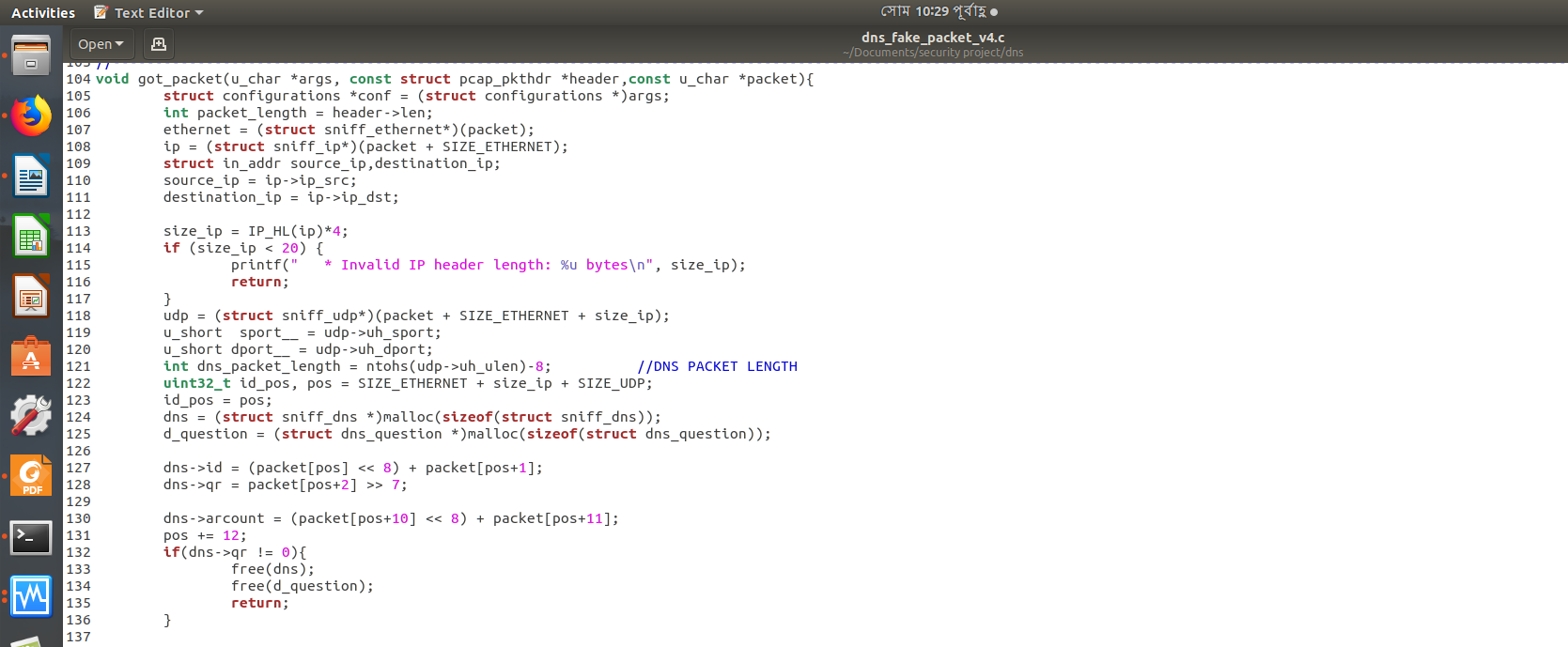


Figure 3: packet parsing code

1. Create forge response packet:

I used RAW SOCKET for sending forged DNS response. That’s why I had to create and configure IP, UDP layers header and data. I created IP, UDP and DNS header by following standard protocols. The received DNS request packets transaction ID, question section and additional section had been copied to DNS response packet. In Answer section, I placed my malicious servers IP where i want the user to be redirected. Other fields associated with answer section had been set properly.

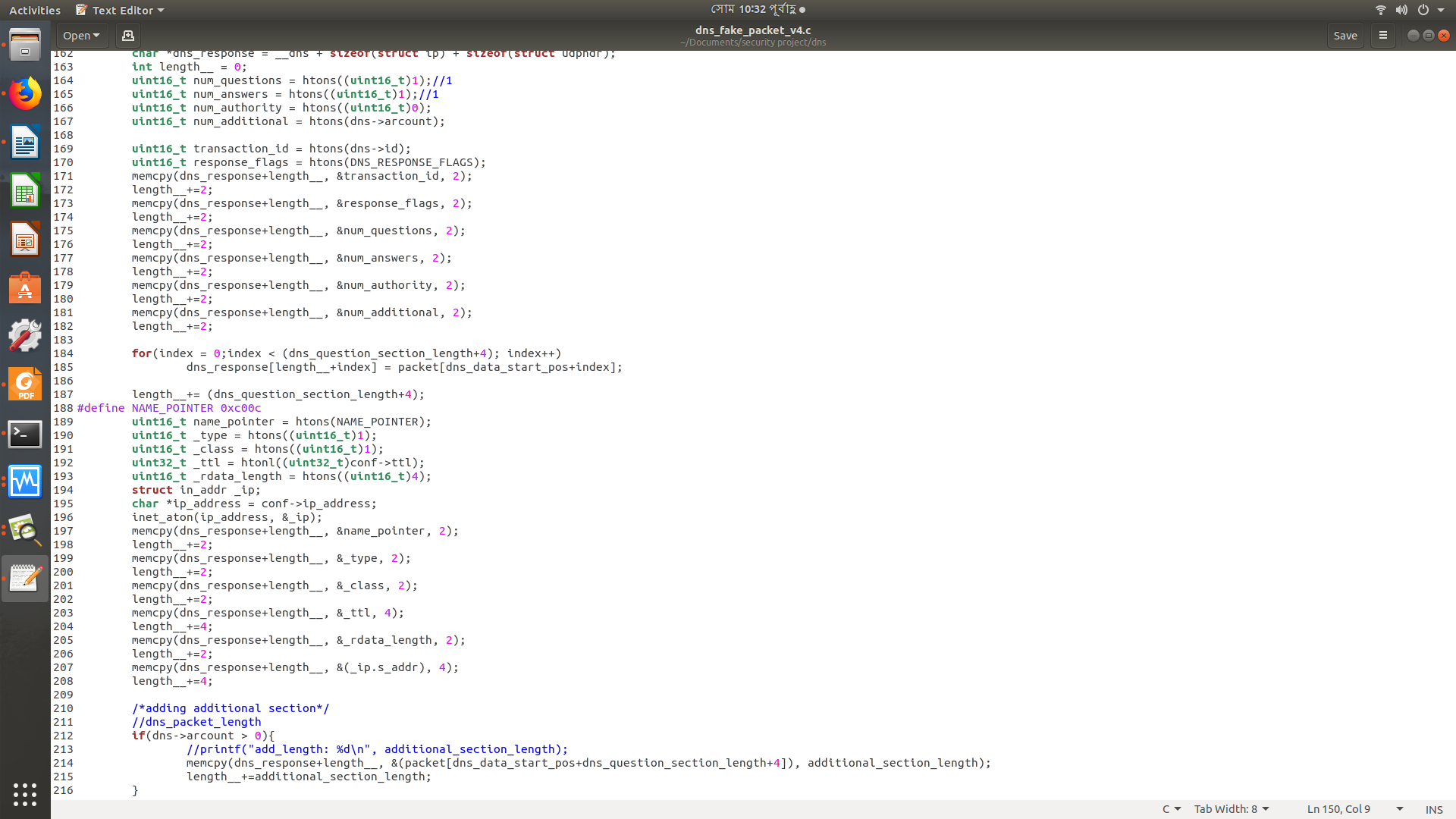


Figure 4: DNS packet creation

1. Send the packet to victim:

To make the attack successful, the created packet had been sent to victim before the original DNS response had been arrived. I used RAW SOCKET to send the packet.

Observed Output in Attacker PC:

In this attack, attacker is a middle man who sends forged packet to victim and if attacker successful, the victim is redirected to attackers ip. But i did not implement any server. But, as a middle man I can capture all traffic and can view if any attempts to session establishment is tried or not.

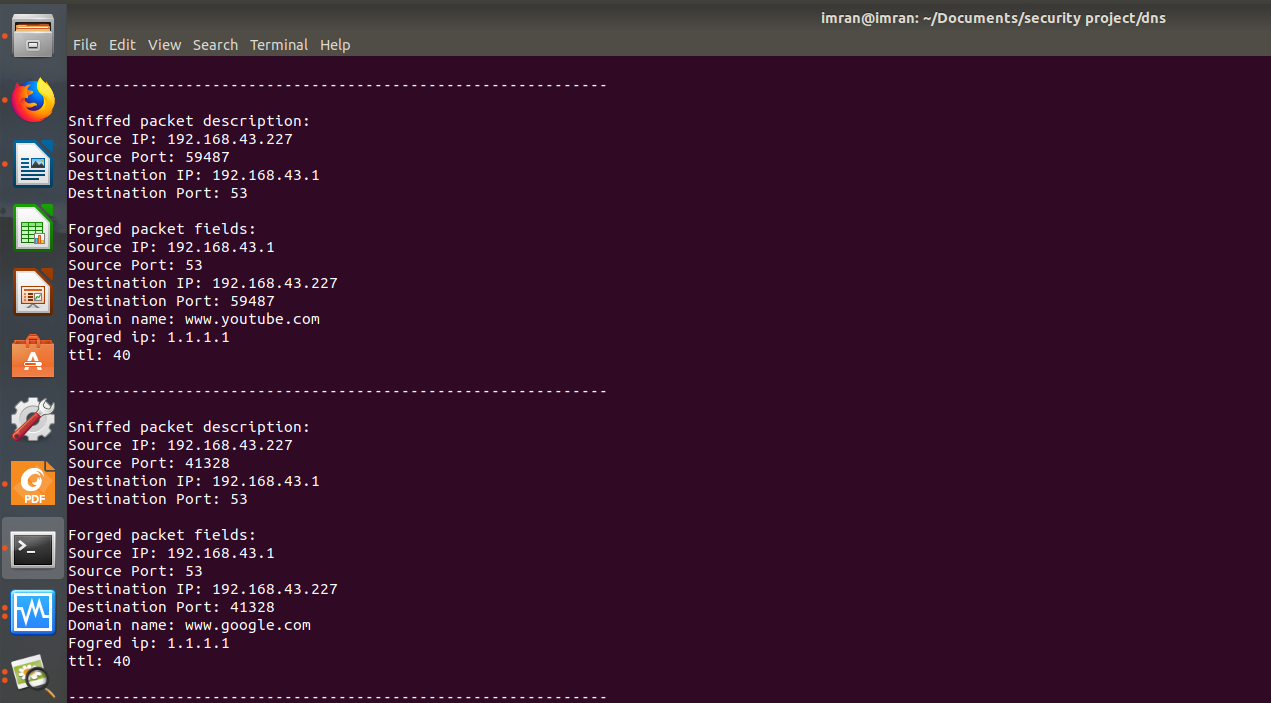


Figure 5: Attacker Window

Attacker can see the output like Figure 5. If attacker sniff’s packet using wireshark then attacker can see output like Figure 6 if the attack is successful.

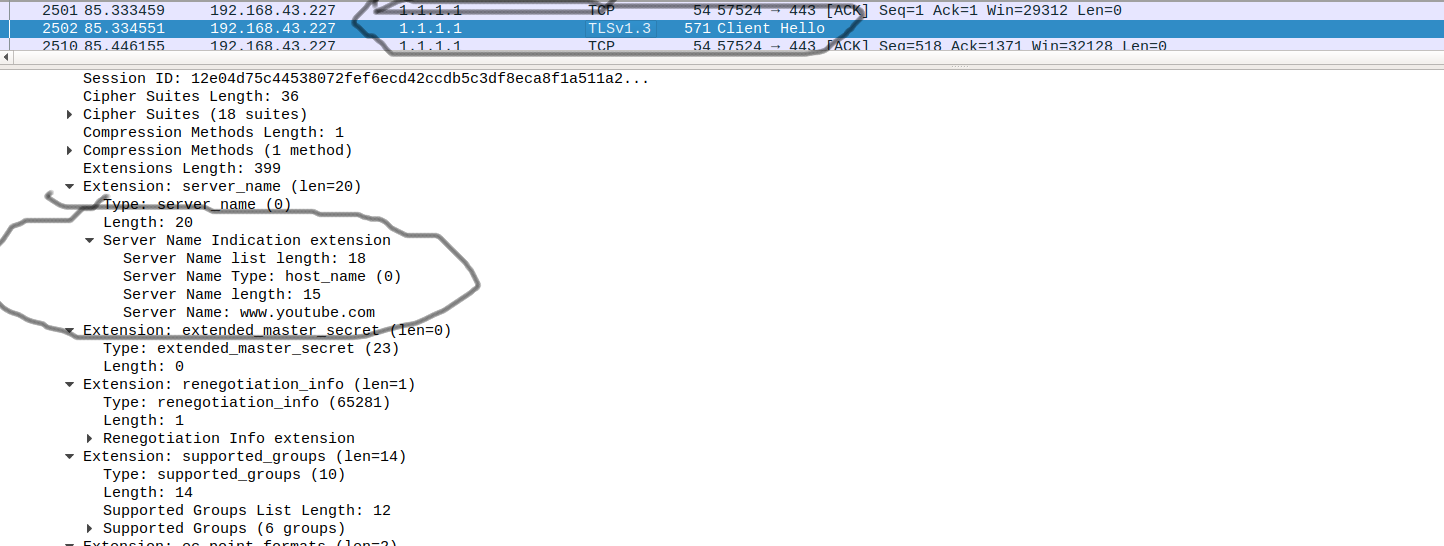


Figure 6: Wireshark Output

Server Name Indication contains the server name to whom i want to connect. In Figure 6, server name is youtube. If we look at the upper circled content, we will see that the servers IP address is 1.1.1.1 which is attackers server ip. So, victim is redirected to attacker’s IP.

Observed Output in Victim’s PC:

In this attack configuration, if the attack is successful the victim will try to connect with attacker’s IP. But if there is no program to listen then victim will see output like Figure 7.

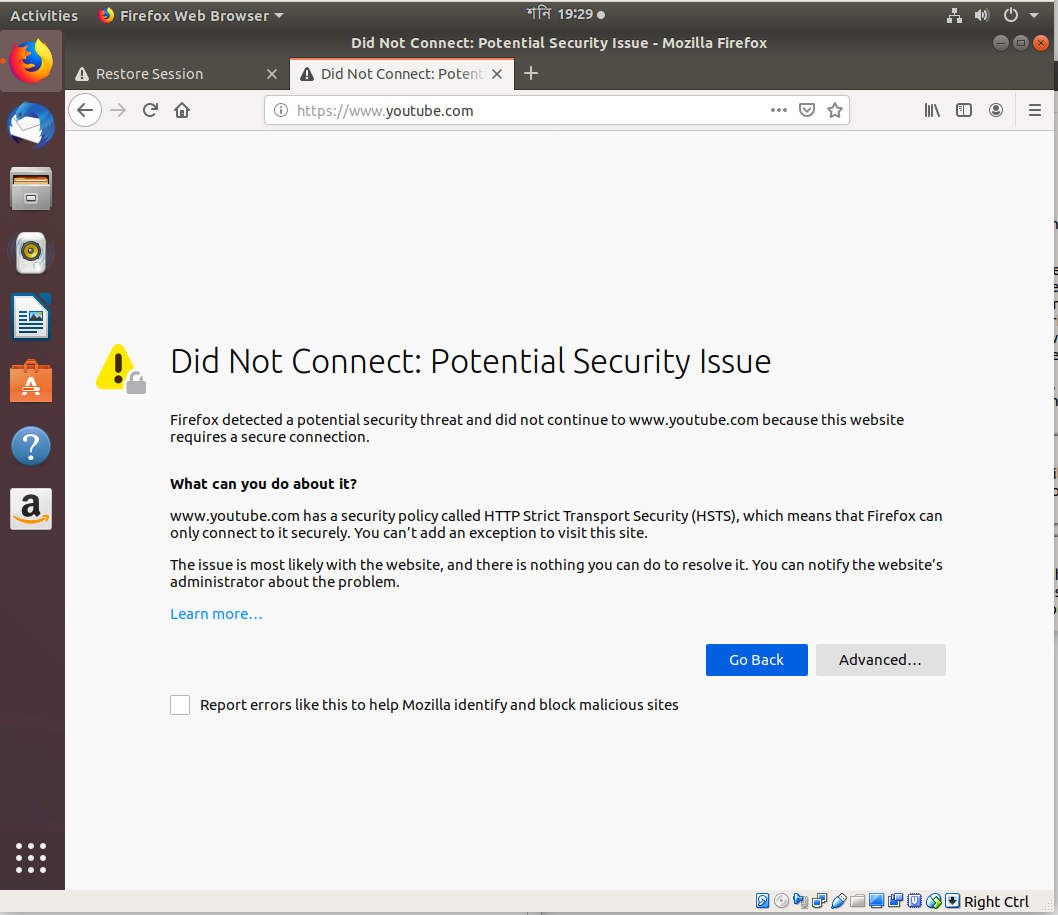


Figure 7: Victim’s Window

In victims machine, if we use dig command then, we can see actual cache poisoning.

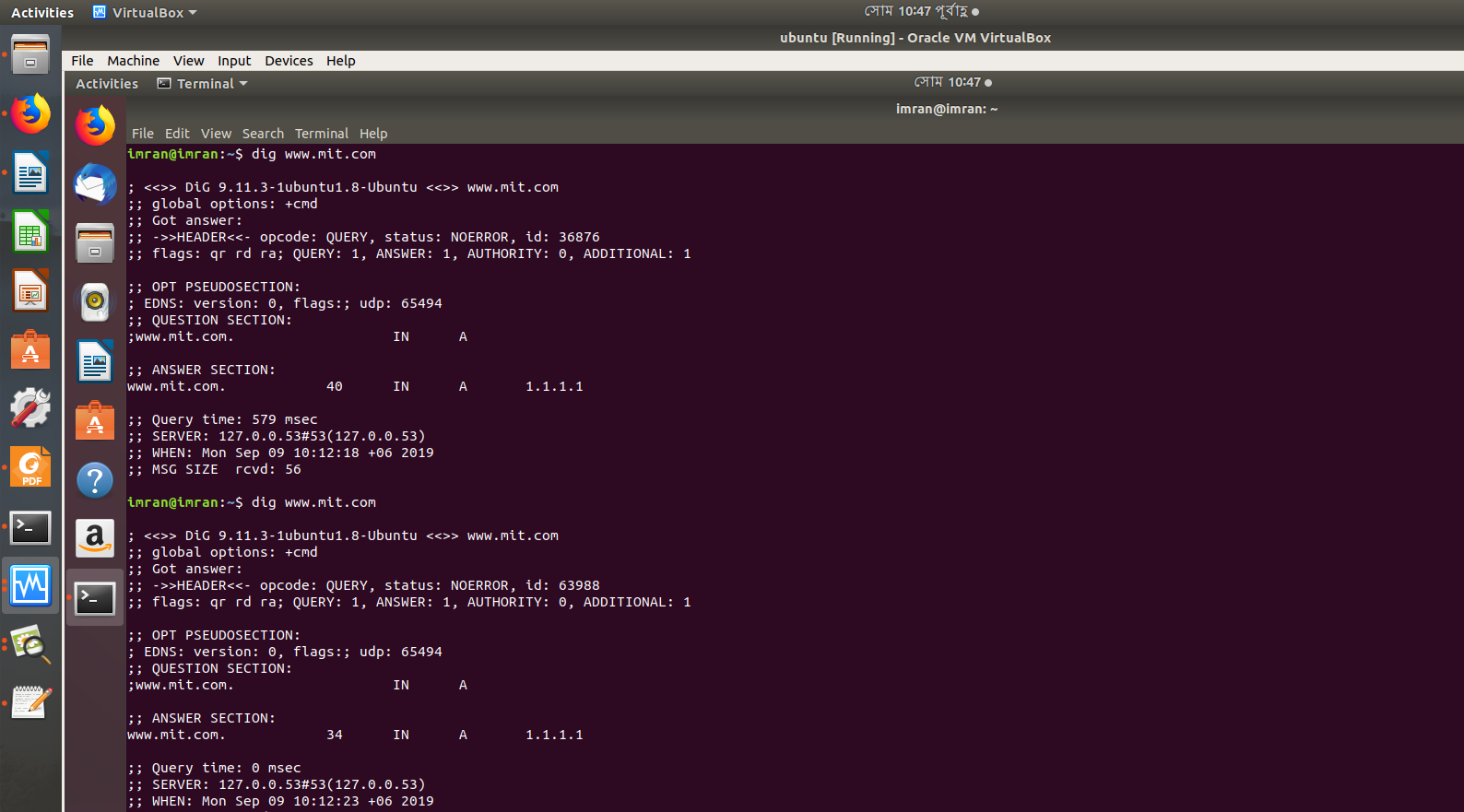


Figure 8: Cache Poisoning in Victims Machine

Attack Success Rate:

When a user wants to connect with a server, it sends(if not cached) a DNS query to DNS server and waits for DNS response. DNS server sends back response to user. And this happens within a small time.

My attack strategy worked for me. I captured DNS packet, parsed it, created new packet and sent it back in real time. As DNS servers are placed near users of an ISP and users PC cache DNS entries, the attack success rate is low.