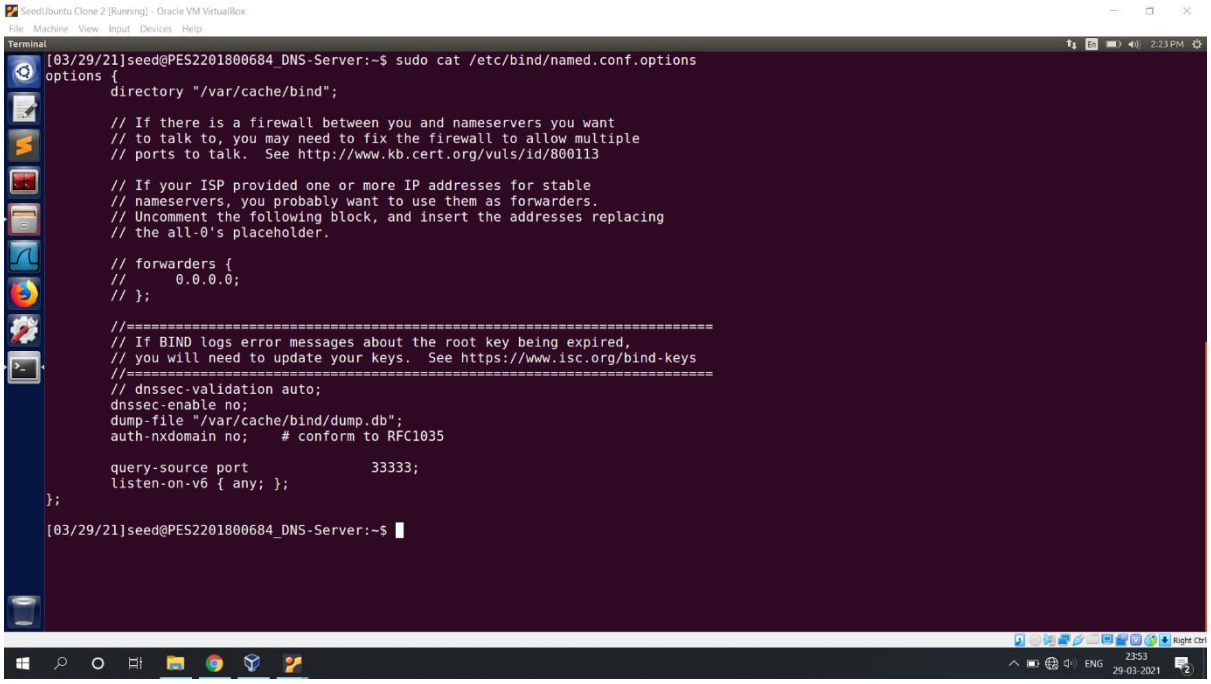
Computer Networks Laboratory
Week-3 Submission

Sathvik Saya
PES2201800684
A-section

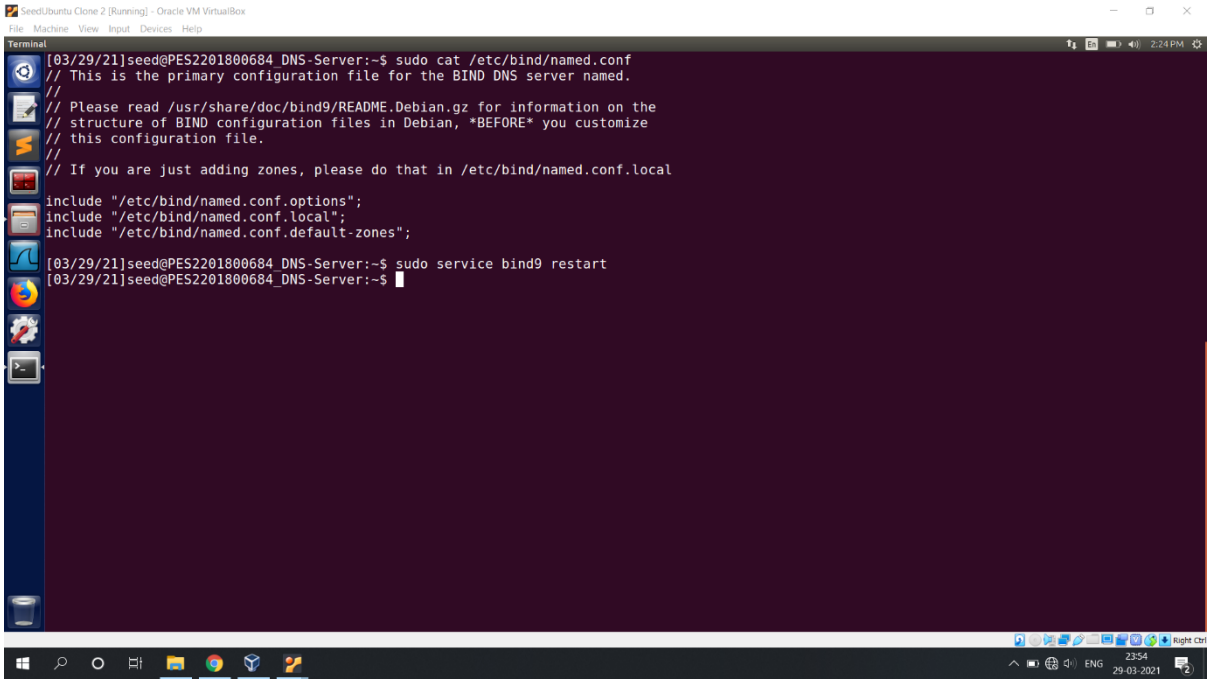
Note: -

Attacker – 10.0.2.12
Victim – 10.0.2.13
DNS Server– 10.0.2.14

Task 1: Configure the Local DNS Server

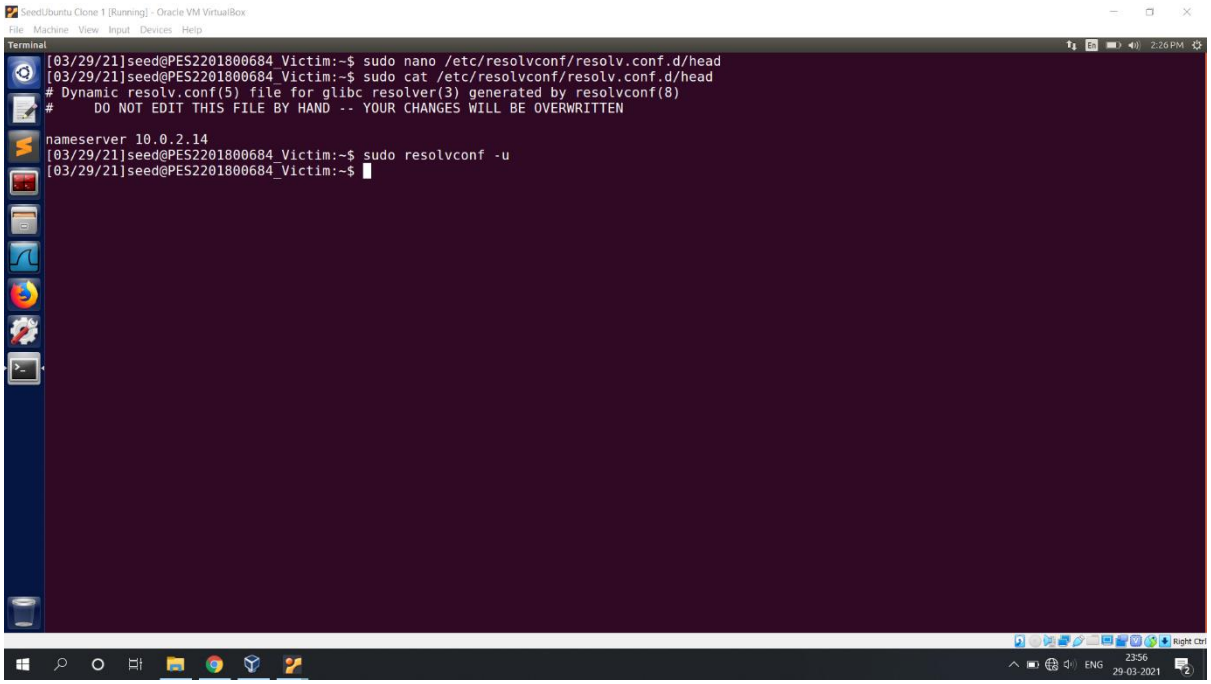


We configure the BIND9 Server in DNS Server machine. Let us first set up an option related to DNS cache by adding a dump-file entry to the options block. We turn the protection against spoofing in DNS server off. This is done by modifying the named.conf.options file. We comment out the dnssec-validation entry, and add a dnssec-enable entry. Fix the Source Ports, we assume that the source port number is a fixed number. We can set the source port for all DNS queries to 33333.

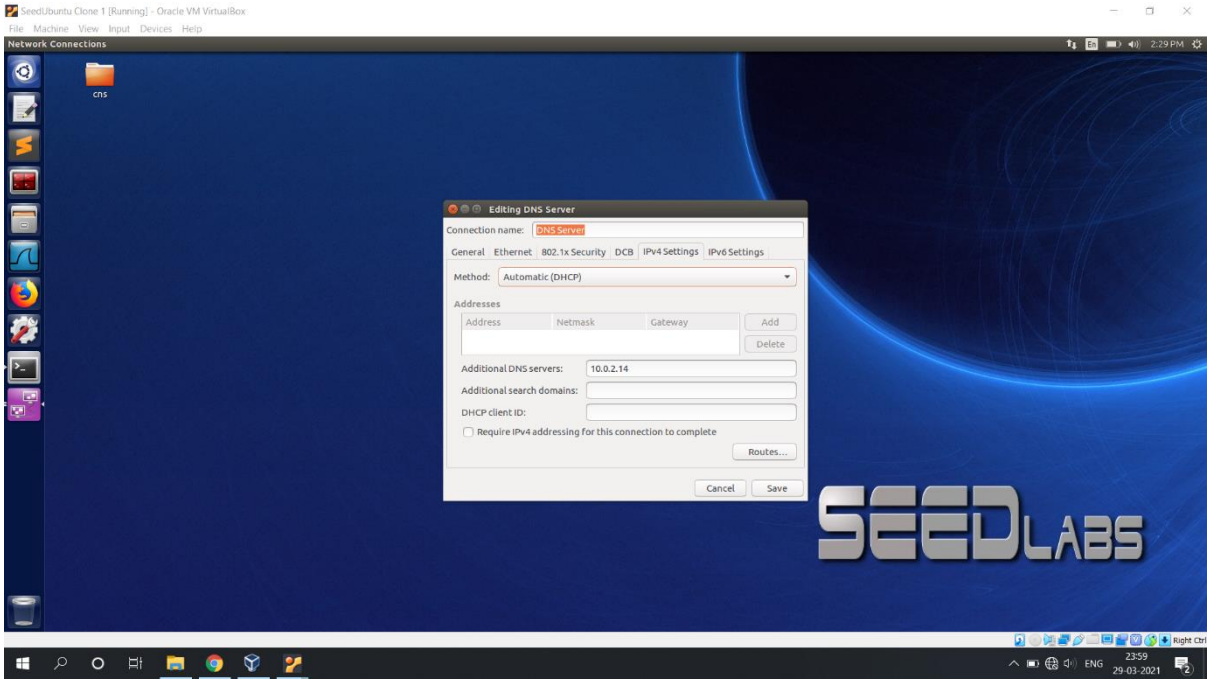


Remove the example.com zone in /etc/bind/named.conf and restart the bind9 server in the DNS Server machine.

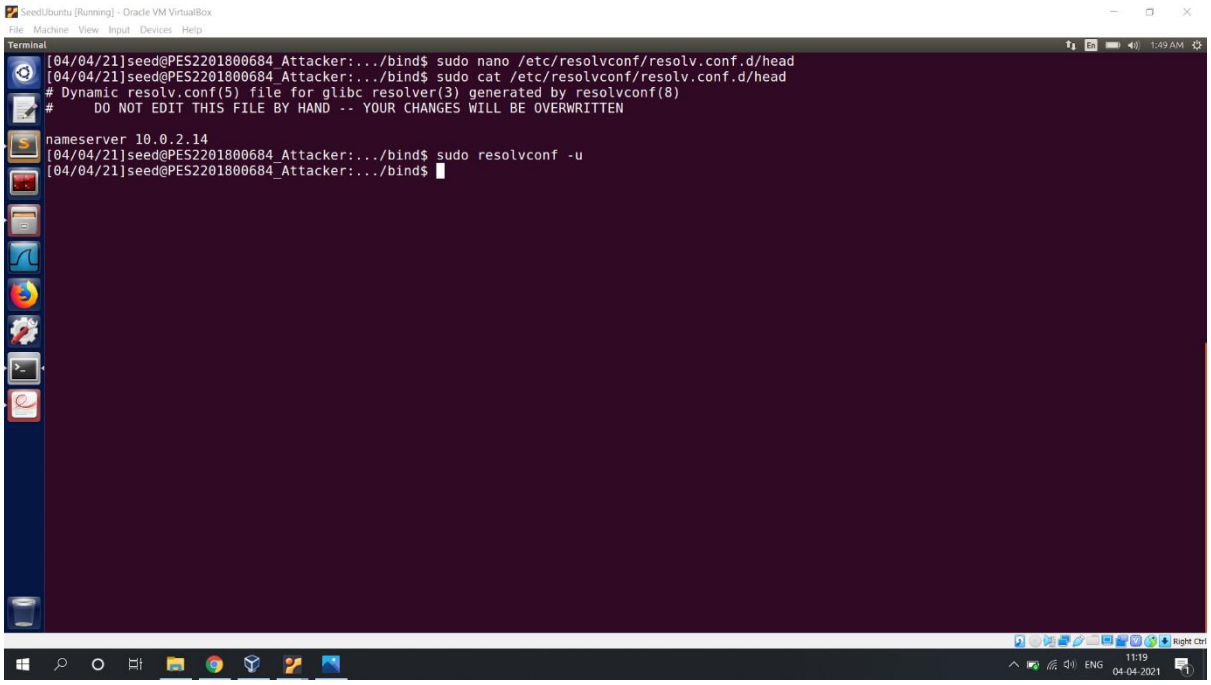
Task 2: Configure the Victim and Attacker Machine



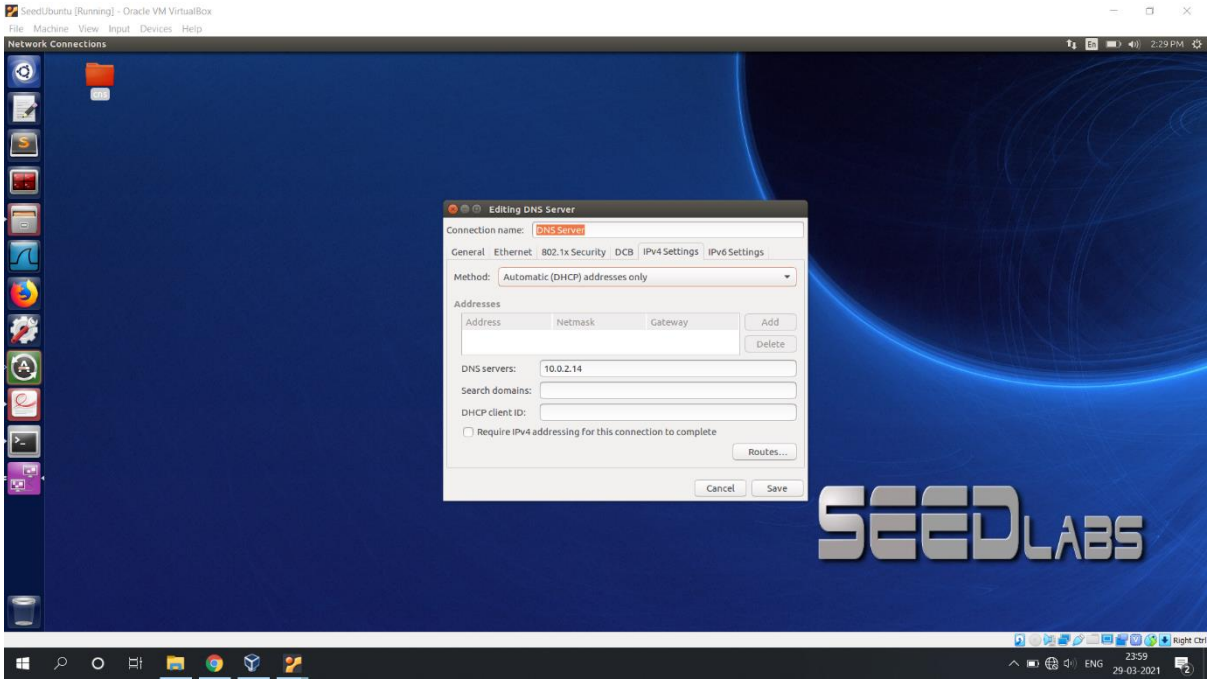
We add a nameserver in /etc/resolvconf/resolv.conf.d/head file in Victim's machine.



We open edit connections in network setting and add a new entry for DNS Server with 10.0.2.14 as IP Address and Automatic (DHCP) as method in Victim Machine.



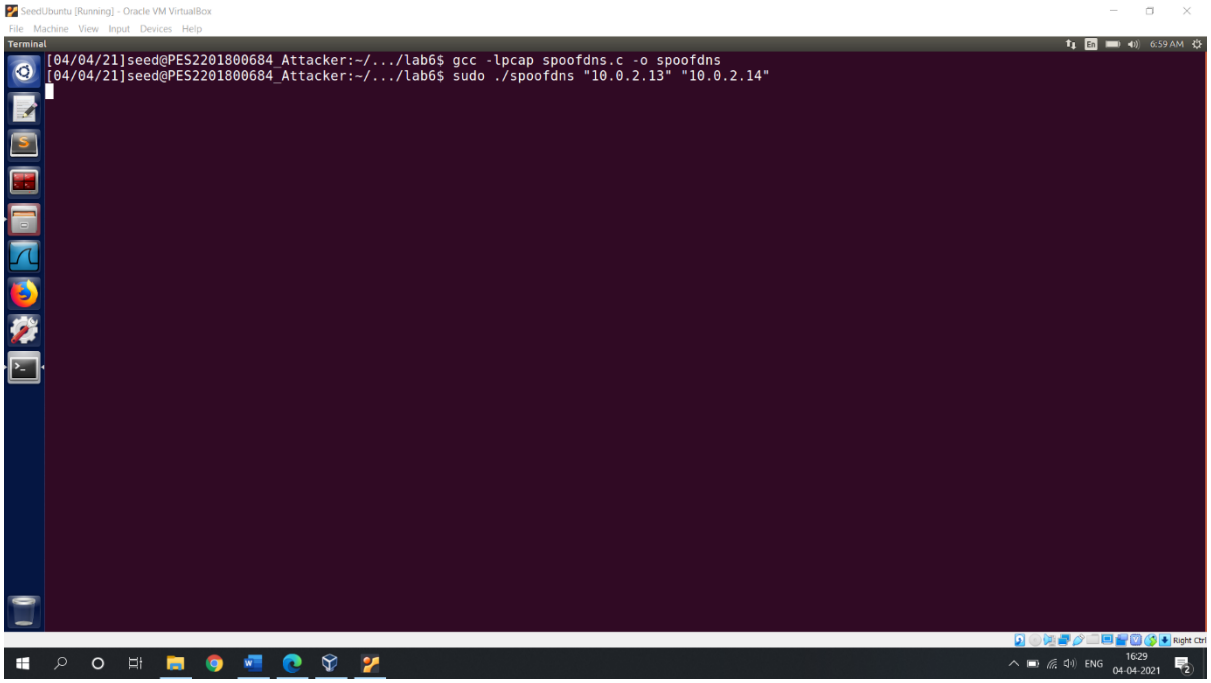
We add a nameserver in /etc/resolvconf/resolv.conf.d/head file in Attacker's machine.



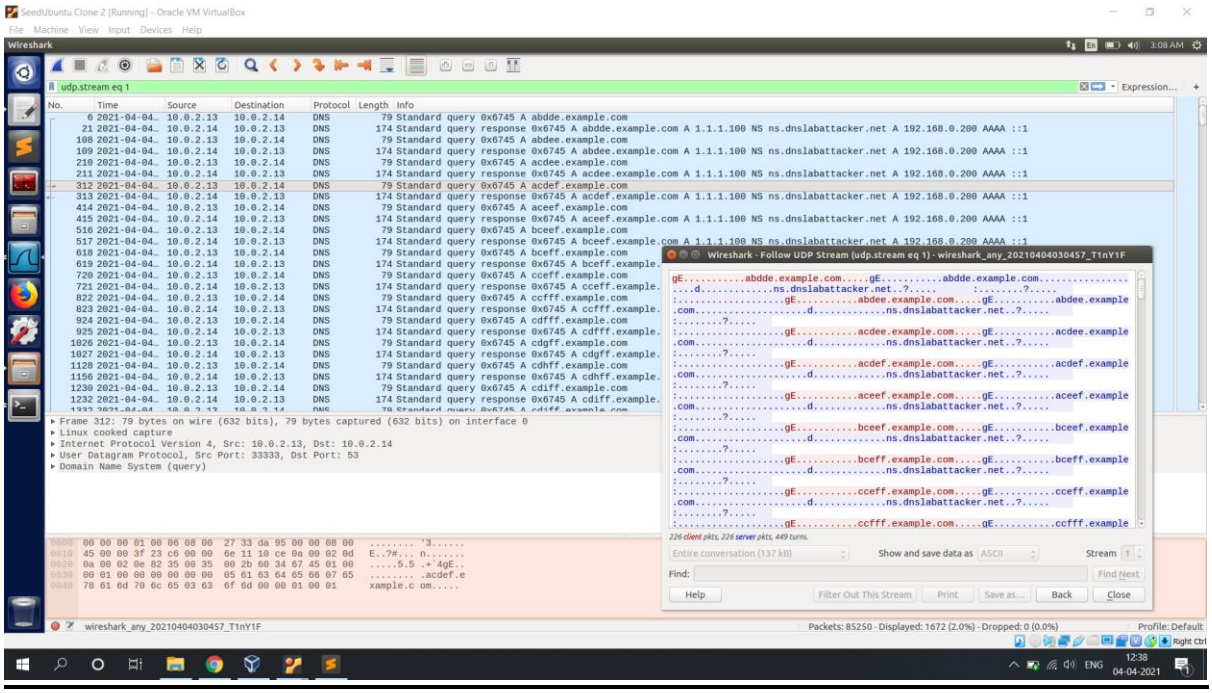
We open edit connections in network setting and add a new entry for DNS Server with 10.0.2.14 as IP Address and Automatic (DHCP) as method in Attacker Machine.

Task 3.1: - The Kaminsky attack

We configure the attacker machine, so it uses the targeted DNS server as its defaults DNS Server as its default DNS server. The attacker machine is on the same NAT network.

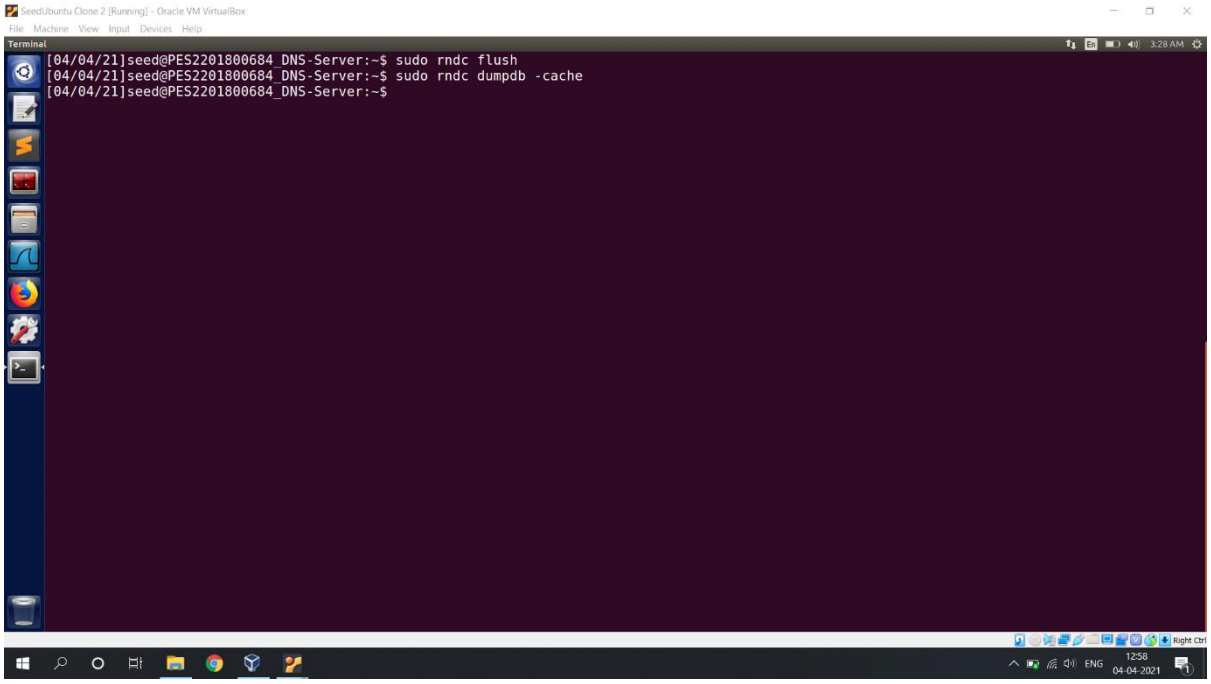


We will spoof DNS Requests that trigger the target DNS server to send out DNS queries, so we can spoof DNS replies. We will spoof DNS Responses to the local DNS Server for each query. We will create a DNS Header with DNS Payload with the Answer, Authority and Additional section. The answer section will give the IP address of the query domain, the authoritative section fills the authoritative nameserver for the query domain. So, after the attack is successful, any query with the domain name will be directed to the Attacker's nameserver "ns.dnslabattacker.com". Lastly, we will fill the additional section with the IP Address of the name server.

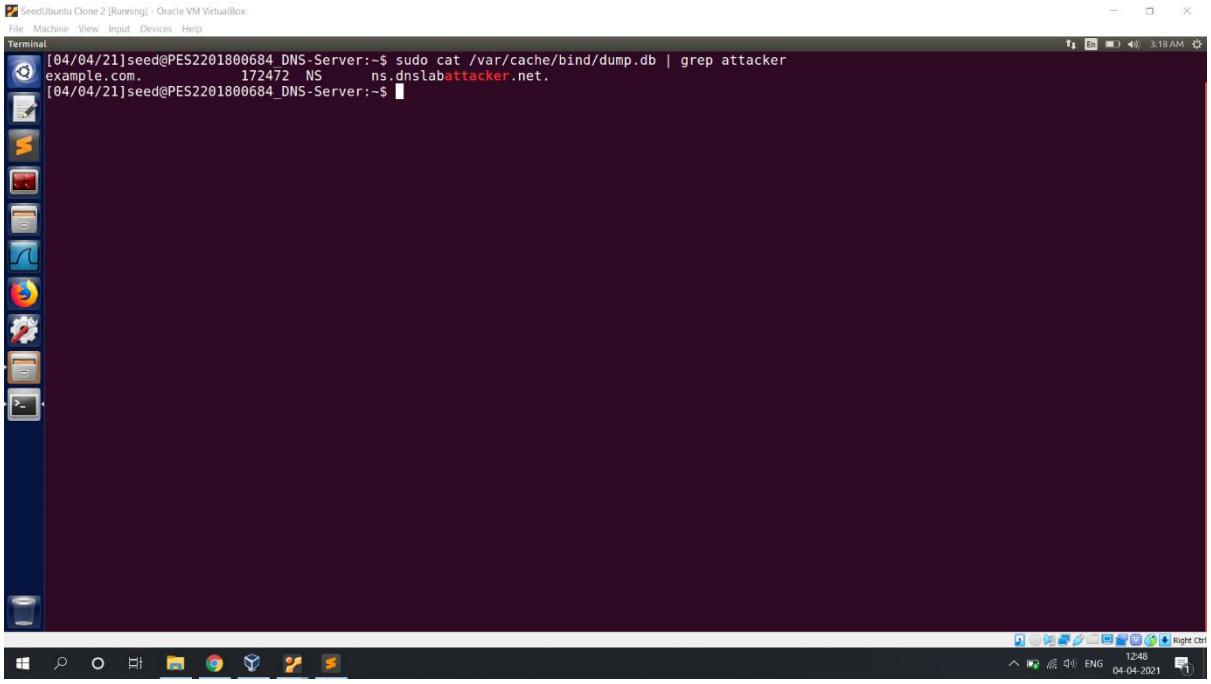


We can see that requests are sent from Victim to the Server and the replies with ns.dnslabattacker.net are sent from Server to Victim.

Task 3.2: - The Kaminsky Attack



We first clear out the cached contents in the server before the attack and dump the cache after the attack.



We can see the dump.db file in the /var/cache/bind directory for the cached content and we can observer that the ns.dnslabattacker.net as nameserver for example.com.

```
[04/04/21]seed@PES2201800684_Victim:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 336
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

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

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.0.200
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 3 msec
;; SERVER: 10.0.2.14#53(10.0.2.14)
;; WHEN: Sun Apr 04 03:20:32 EDT 2021
;; MSG SIZE  rcvd: 139

[04/04/21]seed@PES2201800684_Victim:~$
```

We now dig www.example.com and we can see the in authority section from the reply that the nameserver for example.com is ns.dnslabattacker.net.

Task 3.3: - Result Verification

```
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo nano named.conf.default-zones
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo cat named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

zone "ns.dnslabattacker.net" {
        type master;
        file "/etc/bind/db.attacker";
};
```

We first configure the victim's DNS server Apollo. In the file named.conf.default-zones in the /etc/bind/ directory, we add the dnslabattacker.net zone in it.

```
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo nano db.attacker
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo cat db.attacker
$TTL 604800
@       IN      SOA   localhost. root.localhost. (
                2
                604800
                86400
                2419200
                604800)

@       IN      NS      ns.dnslabattacker.net.
@       IN      A       192.168.0.200
@       IN      AAAA    ::1
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$
```

We create a new file in the bind folder and add the content to it as show in the screenshot.

```
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo nano named.conf.local
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "example.com"{
        type master;
        file "/etc/bind/example.com.db";
};
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$
```

In the file named.conf.local in the /etc/bind/ directory, we add the example.com zone in it.

```
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo nano example.com.db
[04/04/21]seed@PES2201800684_DNS-Server:.../bind$ sudo cat example.com.db
$TTL 3D
@       IN      SOA   ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS    ns.dnslabattacker.net.
@       IN      MX    10 mail.example.com.

www     IN      A     1.1.1.1
mail    IN      A     1.1.1.2
*.example.com.  IN      A       1.1.1.100

[04/04/21]seed@PES2201800684_DNS-Server:.../bind$
```

We create a new file in the bind folder and add the content to it as show in the screenshot.

```
[04/04/21]seed@PES2201800684_DNS-Server:~$ sudo service bind9 restart
[04/04/21]seed@PES2201800684_DNS-Server:~$
```

Now we restart the server to take the changes effect.