

COMPUTER NETWORKS SECURITY

LABORATORY

ASSIGNMENT 4

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

SECTION: C

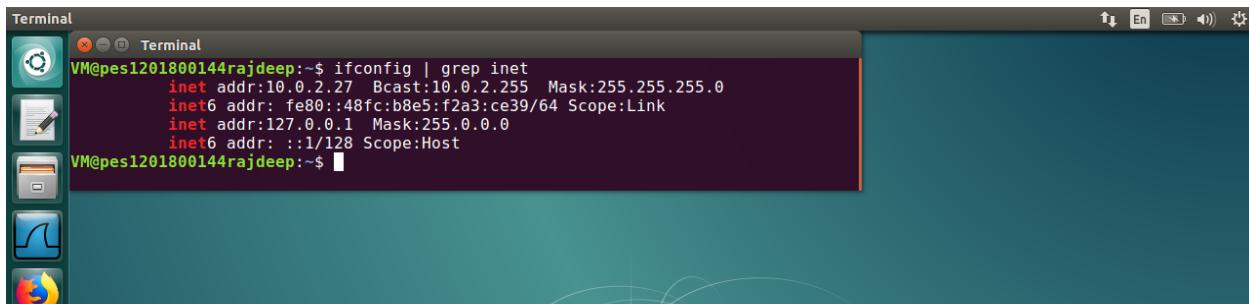
NOTE: Please find my SRN 'PES1201800144rajdeep' as the terminal username.
Also find the description and result analysis and observation of each task in RED FONT following the screenshots for each task.

MY CONFIGURATION:

VM DNS Server: 10.0.2.28

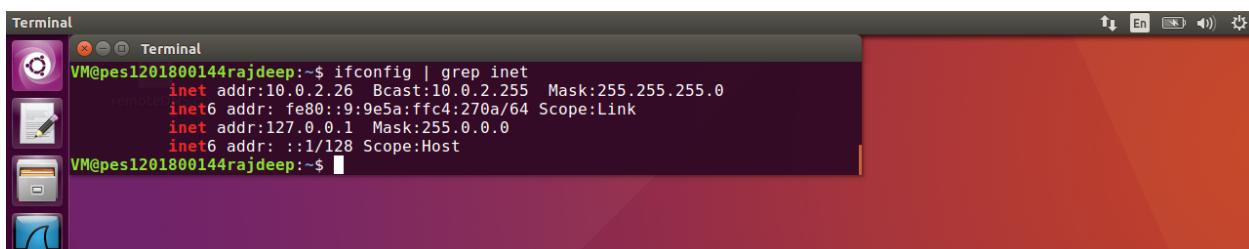
VM Client: 10.0.2.27

VM Attacker: 10.0.2.26



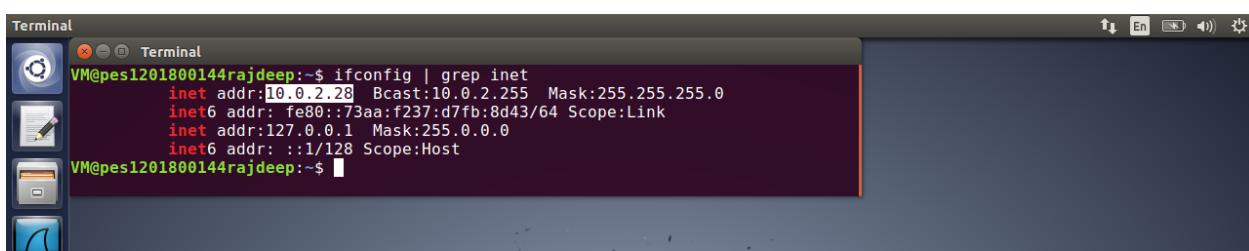
```
Terminal
VM@pes1201800144rajdeep:~$ ifconfig | grep inet
    inet  addr:10.0.2.27  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::48fc:b8e5:f2a3:ce39/64 Scope:Link
            inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
VM@pes1201800144rajdeep:~$
```

Screenshot Client IP address: 10.0.2.27



```
Terminal
VM@pes1201800144rajdeep:~$ ifconfig | grep inet
    inet  addr:10.0.2.26  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::9:9e5a:fffc4:270a/64 Scope:Link
            inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
VM@pes1201800144rajdeep:~$
```

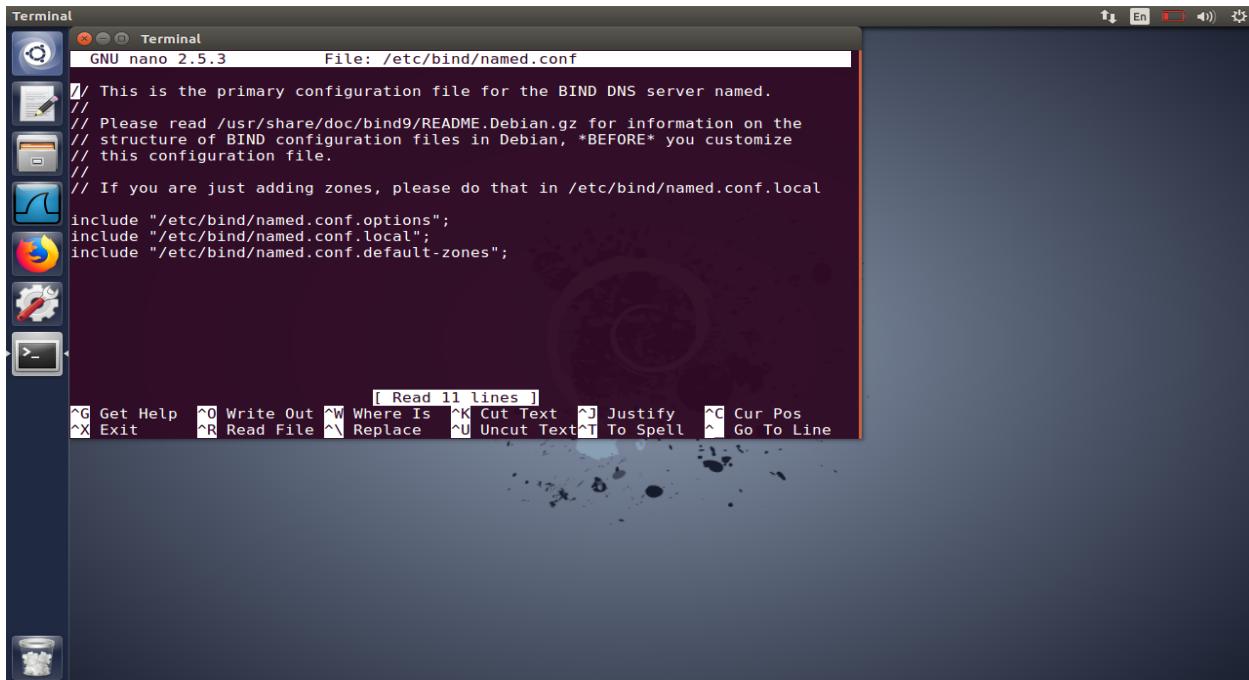
Screenshot Attacker IP address: 10.0.2.26



```
Terminal
VM@pes1201800144rajdeep:~$ ifconfig | grep inet
    inet  addr:10.0.2.28  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::73aa:f237:d7fb:8d43/64 Scope:Link
            inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
VM@pes1201800144rajdeep:~$
```

Screenshot DNS Server IP address: 10.0.2.28

TASK 1: SETTING UP DNS SERVER CONFIGURATIONS

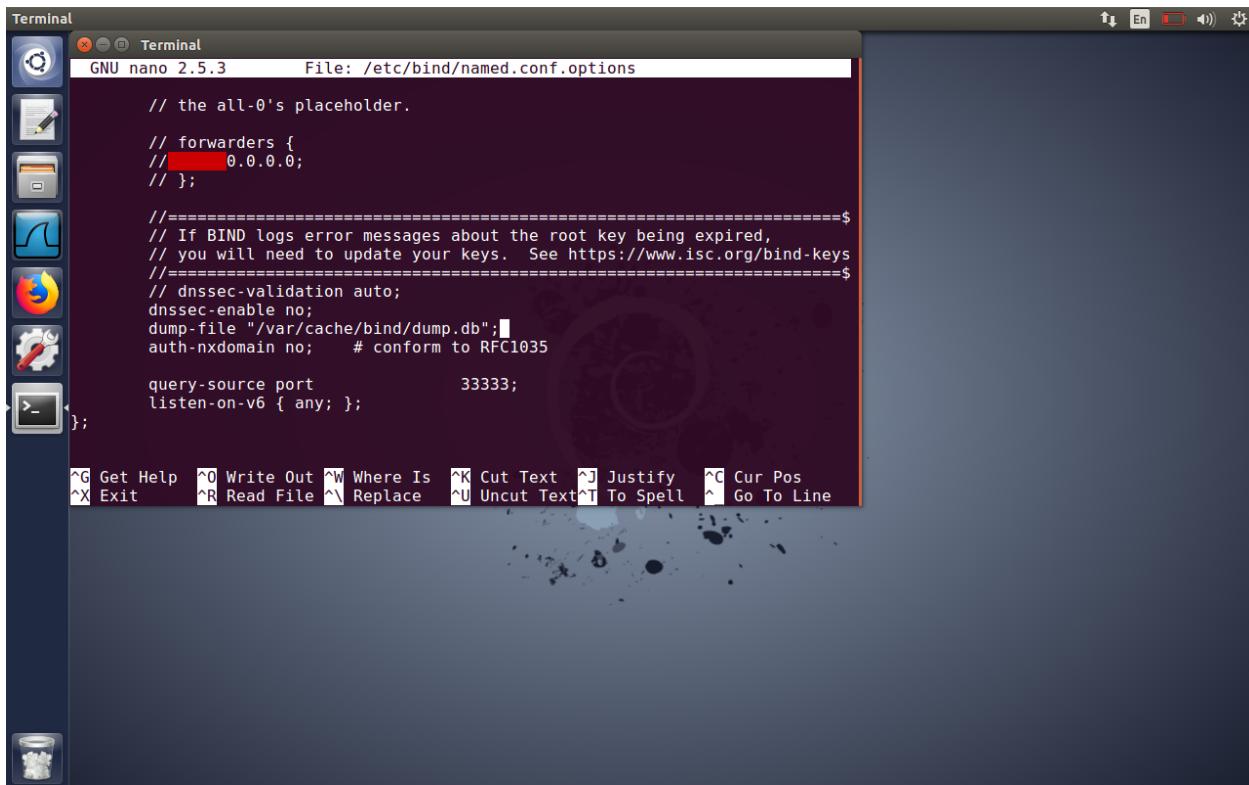


```
Terminal
GNU nano 2.5.3      File: /etc/bind/named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
//
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

[ Read 11 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^L Go To Line
```

Screenshot 1.1: Including named.conf.options in /etc/bind/named.conf file



```
Terminal
GNU nano 2.5.3      File: /etc/bind/named.conf.options

// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

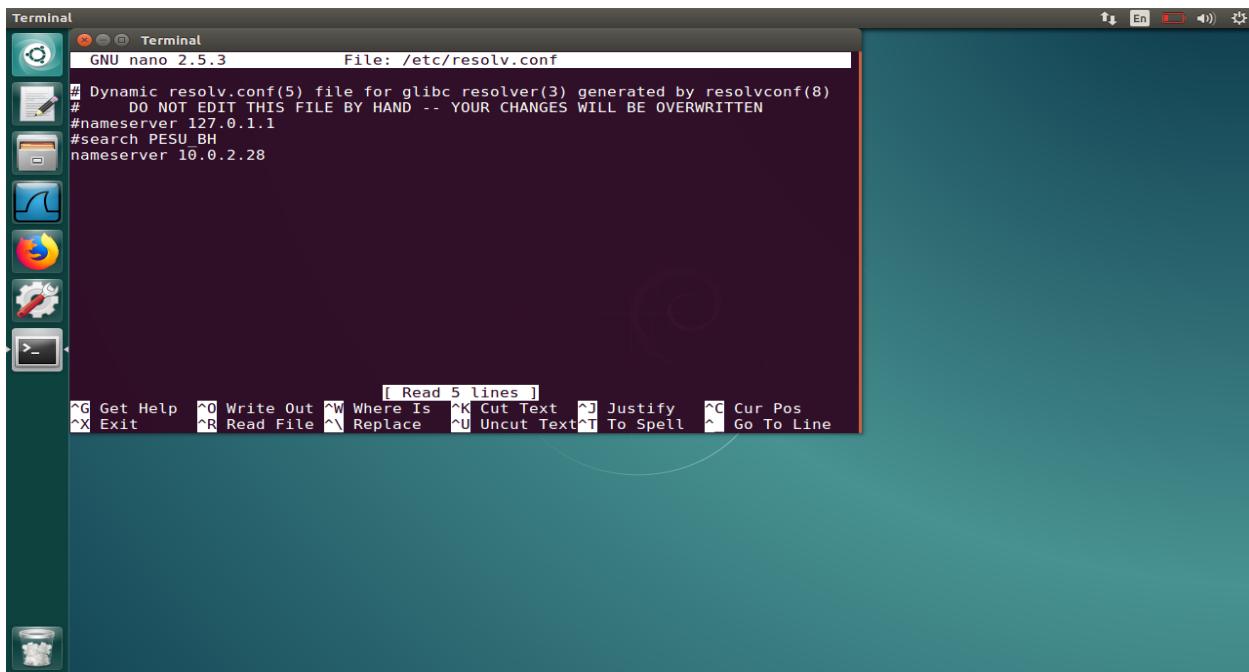
//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
// dnssec-validation auto;
dnssec-enable no;
dump-file "/var/cache/bind/dump.db";#
auth-nxdomain no;    # conform to RFC1035

query-source port      33333;
listen-on-v6 { any; };

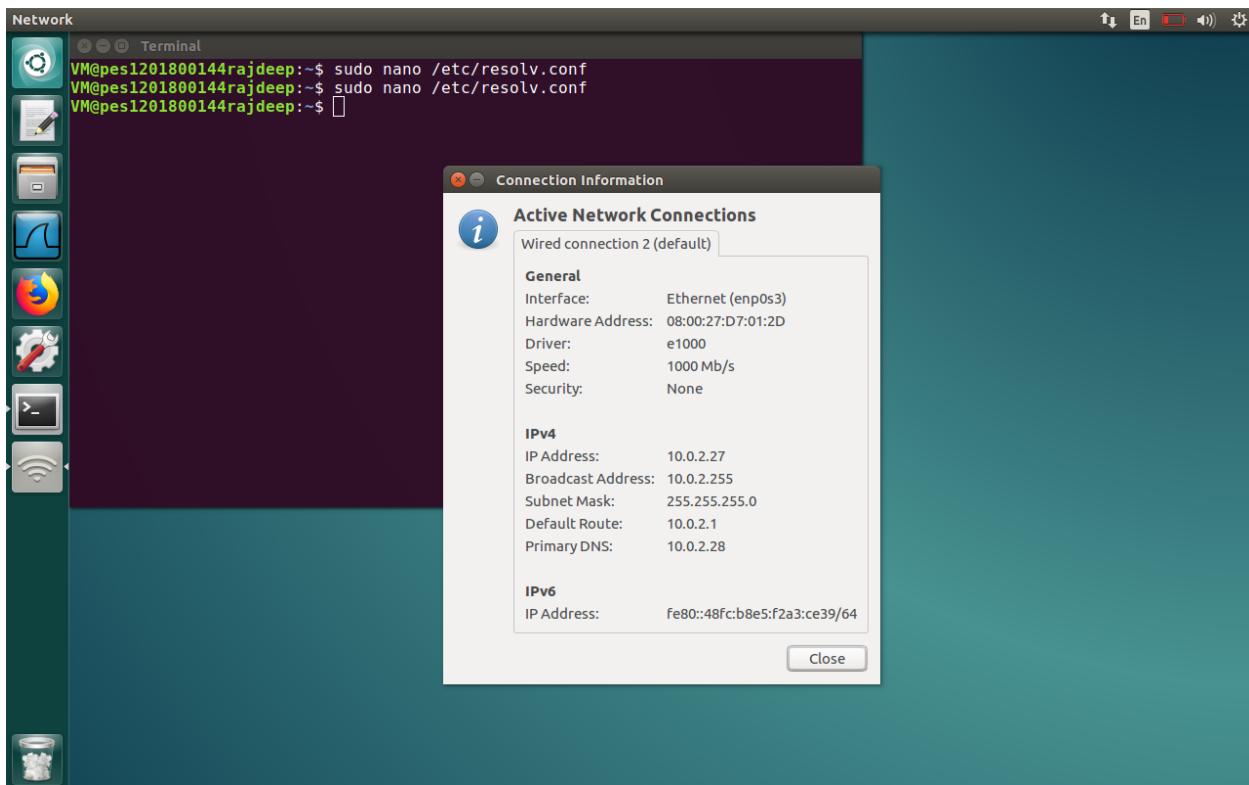
[ Read 11 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^L Go To Line
```

Screenshot 1.2: turning off DNS security, setting query port to 33333 and adding dump file location in named.conf.options file

TASK 2: SETTING UP CLIENT MACHINE CONFIGURATIONS

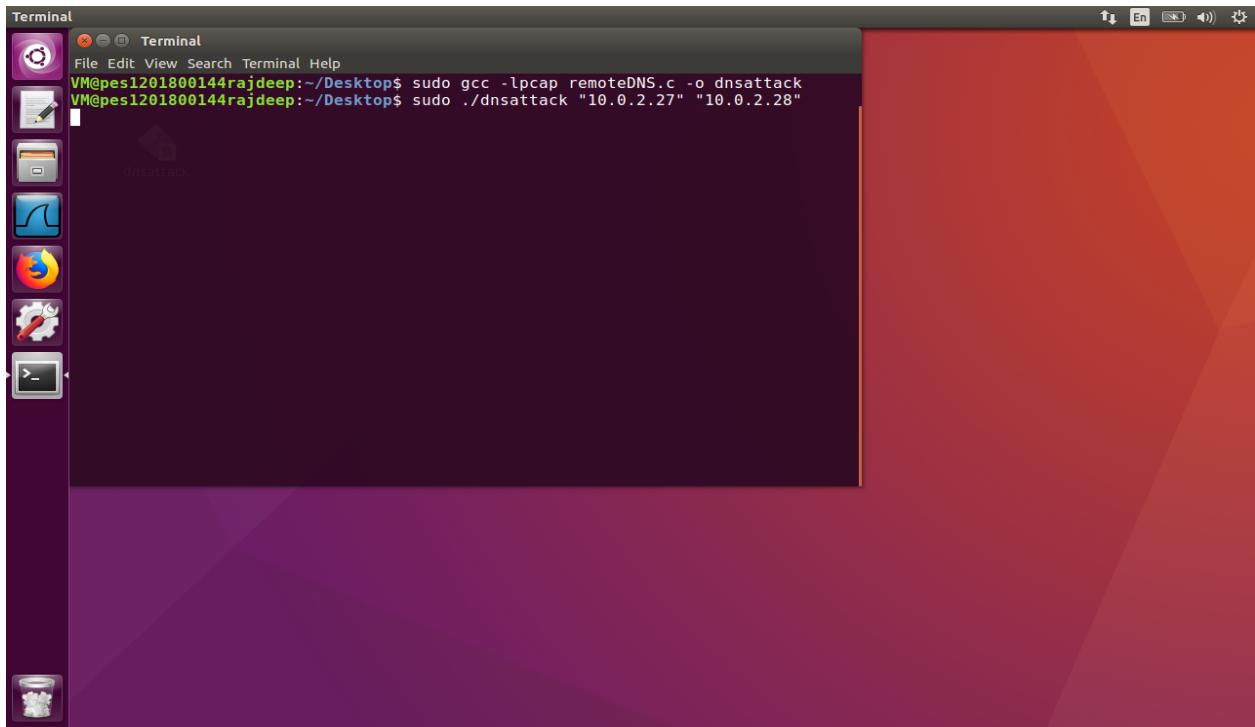


Screenshot 2.1: Setting DNS server for client machine as VM DNS server's IP address 10.0.2.28

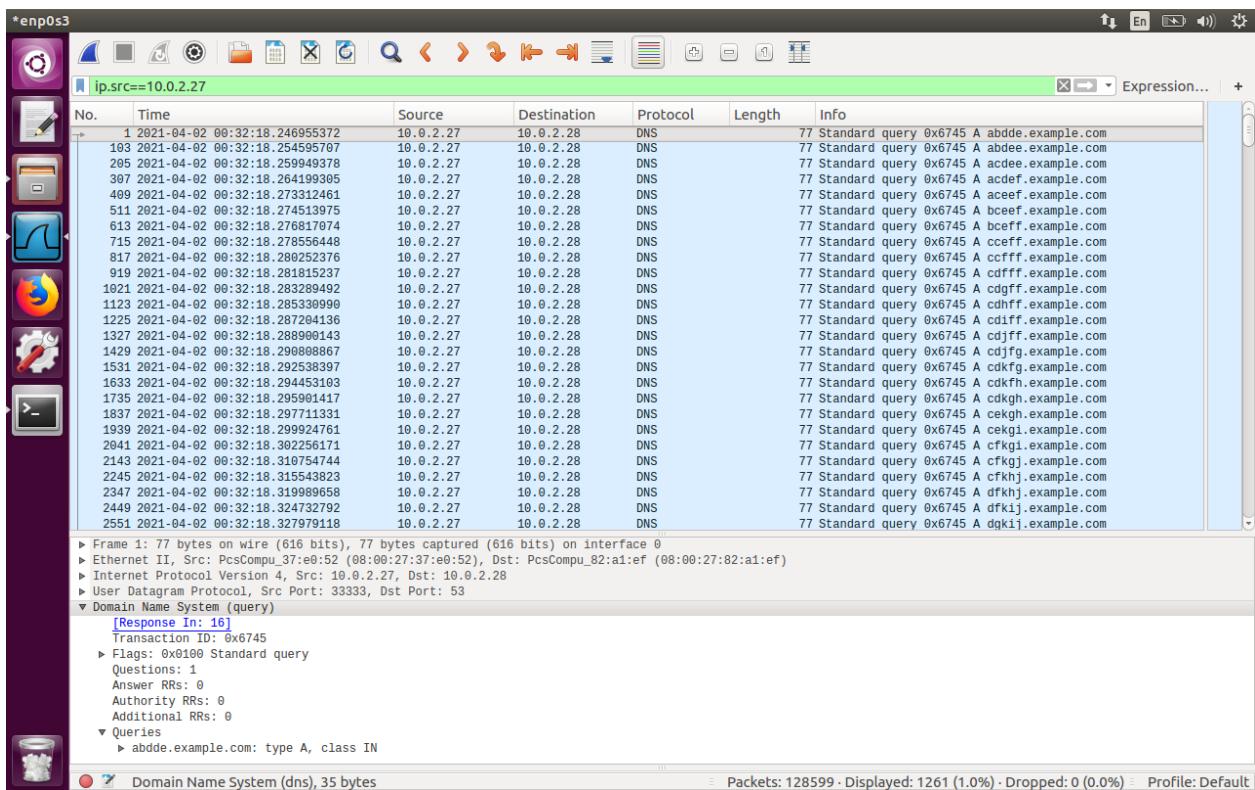


Screenshot 2.2: Setting DNS server as 10.0.2.28 in "edit connections" setting and displaying final configurations of client machine

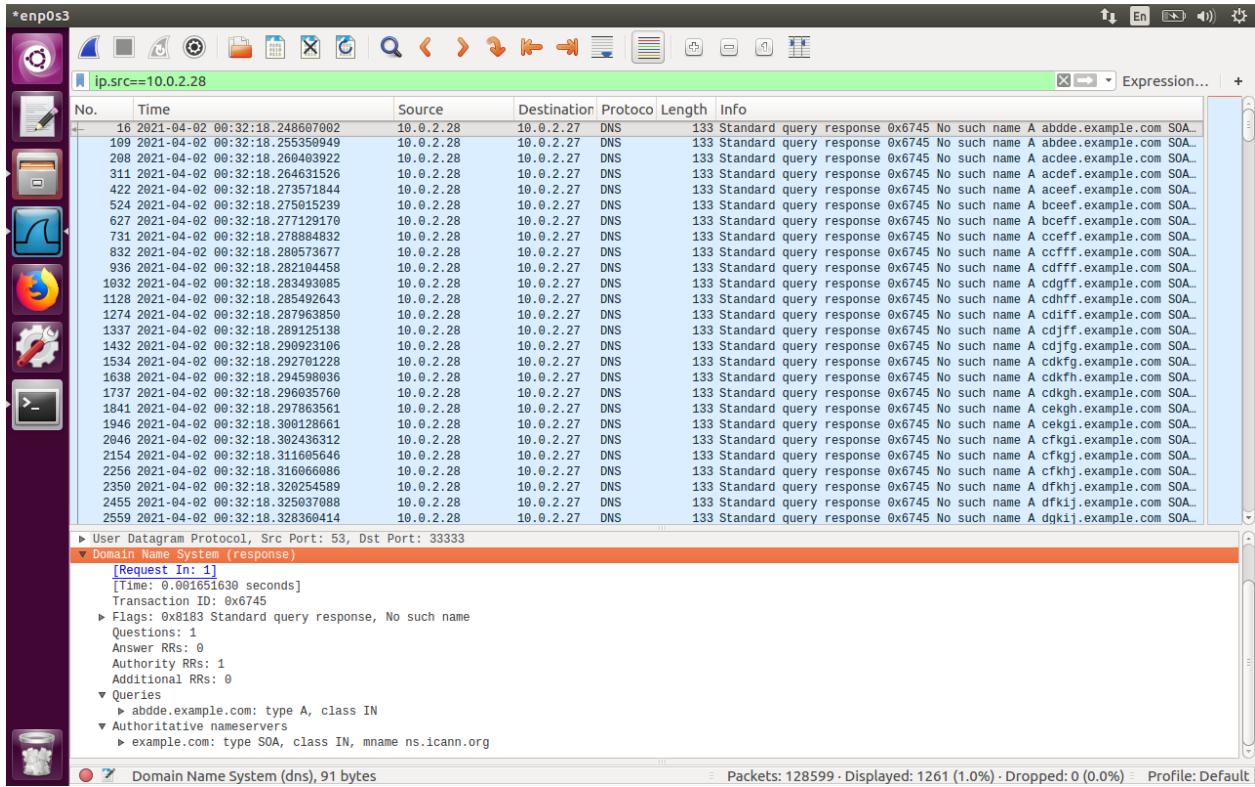
TASK 3: KAMINSKY ATTACK



Screenshot 3.1.1: Compiling and executing the dns spoofing file



Screenshot 3.1.2: DNS requests on wireshark



Screenshot 3.1.3: DNS replies on wireshark

```
dump.db (/var/cache/bind) - gedit
dump.db
/var/cache/bind

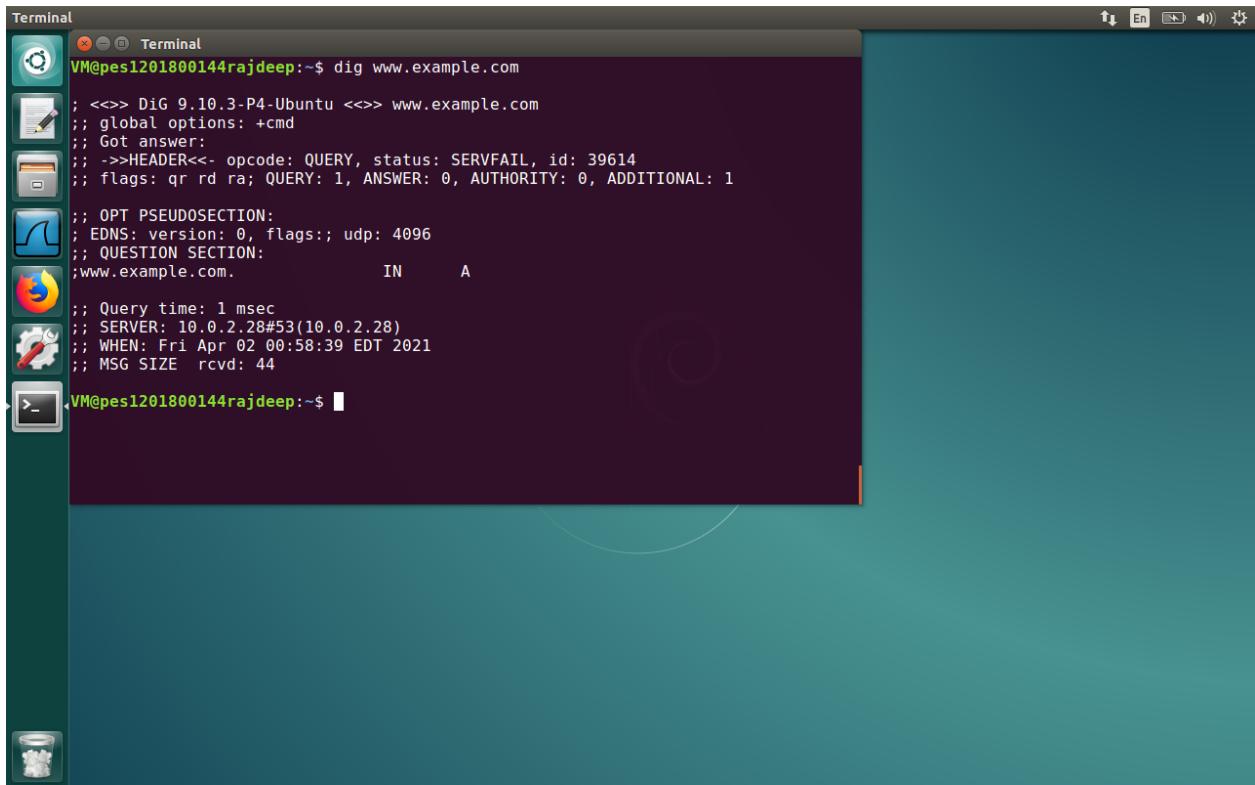
; authauthority
example.com.          108    NS      ns.dnslabattacker.net.
; additional
86293    DS      31406 8 1 (
189968811E6EBA862DD6C209F75623D8D9ED
9142 )
86293    DS      31406 8 2 (
F78CF3344F72137235098ECBBD08947C2C90
61C7F6A085A17F518B5D8F6B916D )
86293    DS      31589 8 1 (
3490A6806D47F17A34C29E2CE80E8A999FFB
E4BE )
86293    DS      31589 8 2 (
CDE0D742D6998A554A92D890F8184C698CF
AC8A26FA59875A990C03E576343C )
86293    DS      43547 8 1 (
B6225AB2CC613E0DCA7962BDC2342EA4F1B5
6083 )
86293    DS      43547 8 2 (
615A64233543F66F44D68933625B17497C89
A70E858ED76A2145997EDF96A918 )

; additional
86293    RRSIG   DS 8 2 86400 (
20210409041715 20210402030715 58540 com.
IgB57FVPTWYUmG48GIWWhQWn20+Rd6xxp8V
84TeTbPQHEYEZNptVykzTCFy10MSY7091fN
IRPPsxX40HT5/m30U0MVHfHyjavfxpq92chZ
U7CE0gYok/TsaqcD6xCLyxjT1cv0YcqkqmA4
UkPxhdRqwusWJfe43JYcNImD0fC2aUBFGZ/8
1UEfwtdc83h8F40XBfnVGTNUqzf7yLNQ== )

; answer
\000\006#\030+.example.com. 3495 \-ANY ;-$NXDOMAIN
```

Detailed description: This screenshot shows a dump file for the BIND DNS server. The file contains several DNS resource records (RRs) for the example.com domain. It includes NS records pointing to ns.dnslabattacker.net, DS (Delegation Signer) records for key signing, and RRSIG (Resource Record Signature) records for the zone. The file is displayed in a terminal window with syntax highlighting for DNS record types.

Screenshot 3.1.4: Dump file in DNS server VM



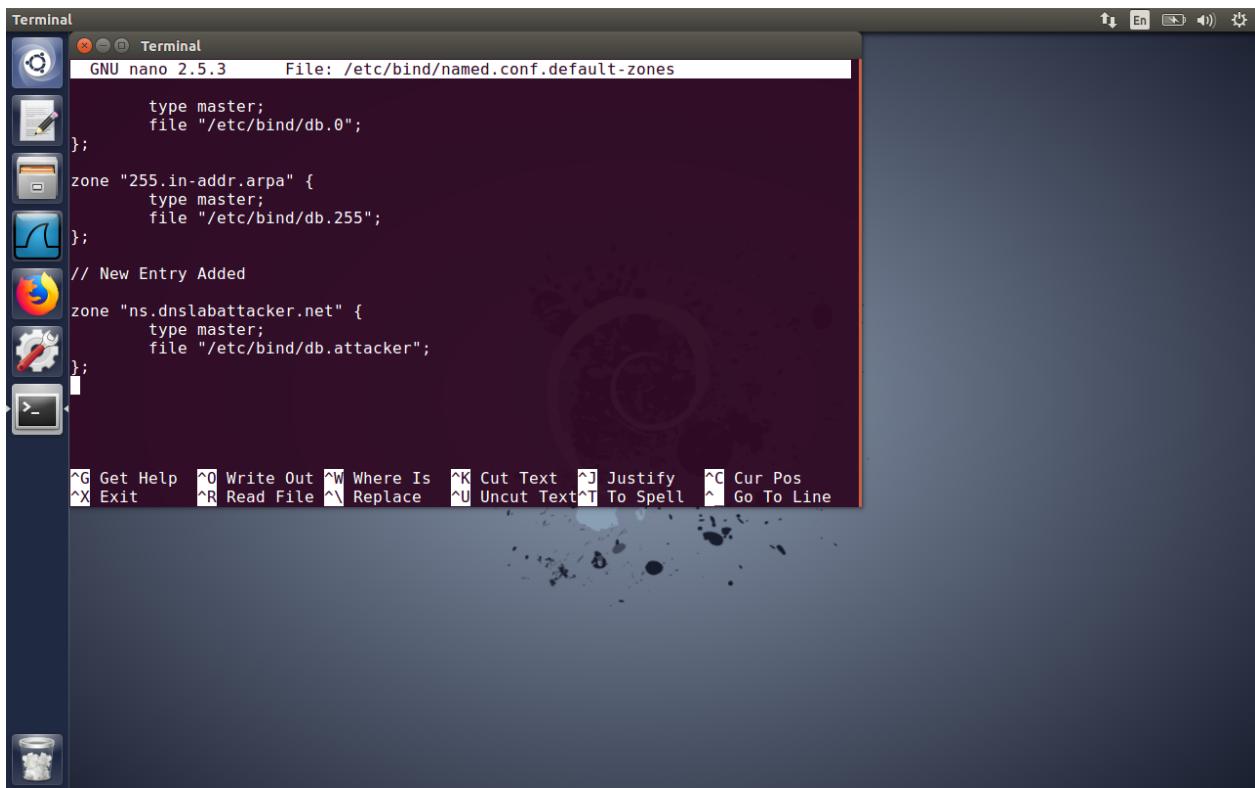
Screenshot 3.1.5: dig command on client machine

In Kaminsky attack, the attacker machine runs a spoofing program which sends different queries to the DNS server VM each time as it can be seen in Screenshot 3.1.2. Since the names are different, the DNS server VM queries example.com domain for the names each time. Before the reply arrives from the example.com nameserver, the attacker floods DNS server VM with spoofed replies. In the spoofed reply, the attacker sends ns.dnslabattacker.net as the authoritative nameserver. If transaction ID matches for the spoofed reply, the Kaminsky attack is successful and the DNS server VM's cache is poisoned.

Sending different queries each time prevents caching effect. The result of the cache poisoning can be verified in the cache dump file as shown in Screenshot 3.1.4.

But in the dig command on the client machine, the IP address cannot be found in the Answer Section.

TASK 3.2: RESULT VERIFICATION



```
GNU nano 2.5.3      File: /etc/bind/named.conf.default-zones

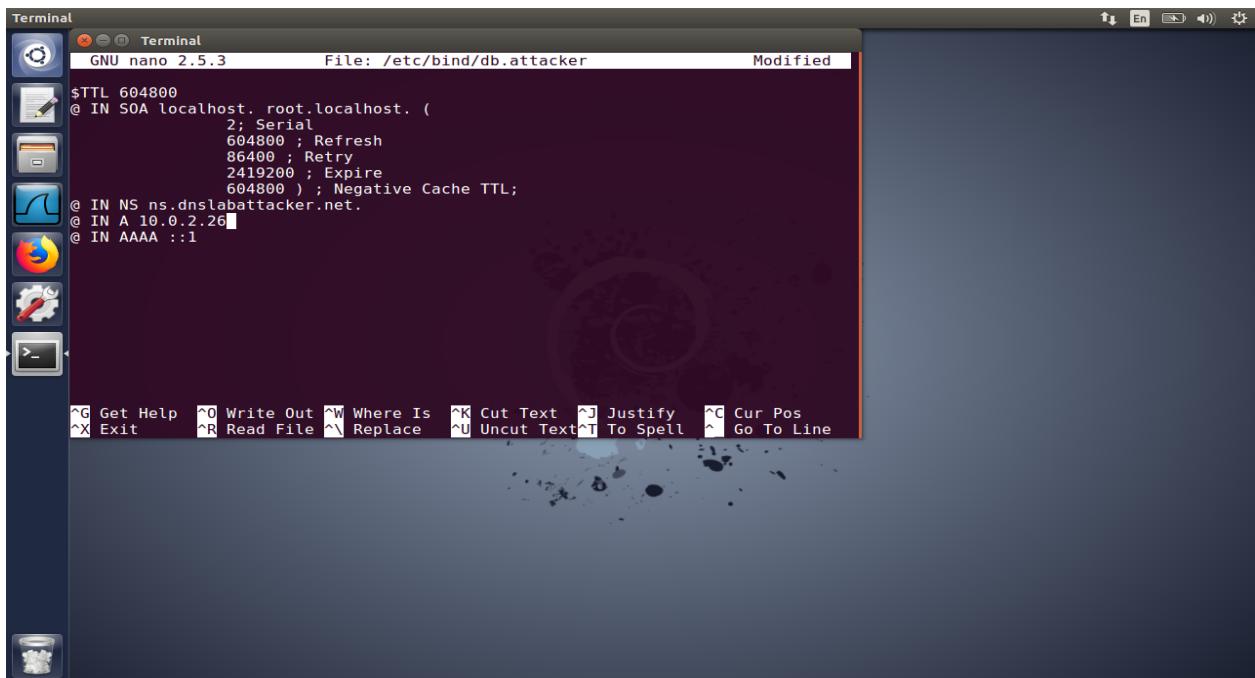
        type master;
        file "/etc/bind/db.0";
};

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

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

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text  ^T To Spell  ^L Go To Line
```

Screenshot 3.2.1: Adding zone file entry in DNS server VM in named.conf.default-zones file

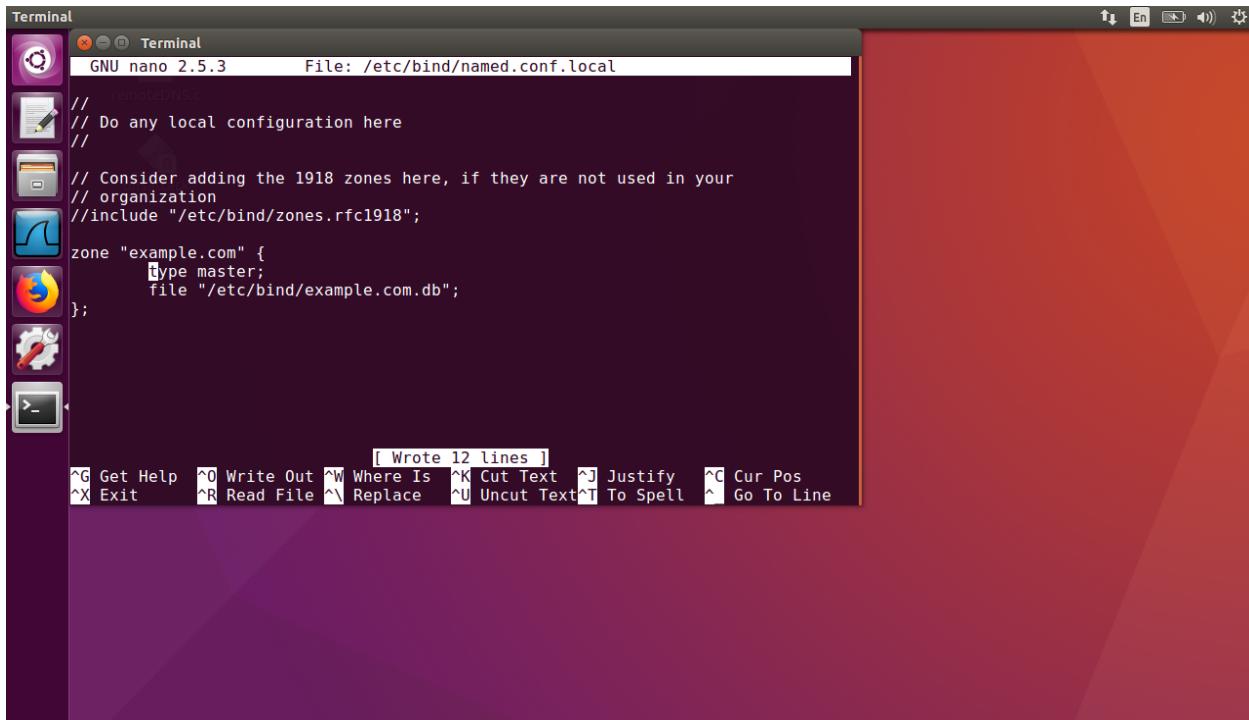


```
GNU nano 2.5.3      File: /etc/bind/db.attacker          Modified

$TTL 604800
@ IN SOA localhost. root.localhost. (
        2; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL;
@ IN NS ns.dnslabattacker.net.
@ IN A 10.0.2.26
@ IN AAAA ::1

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text  ^T To Spell  ^L Go To Line
```

Screenshot 3.2.2: Adding the db.attacker zone file in /etc/bind directory



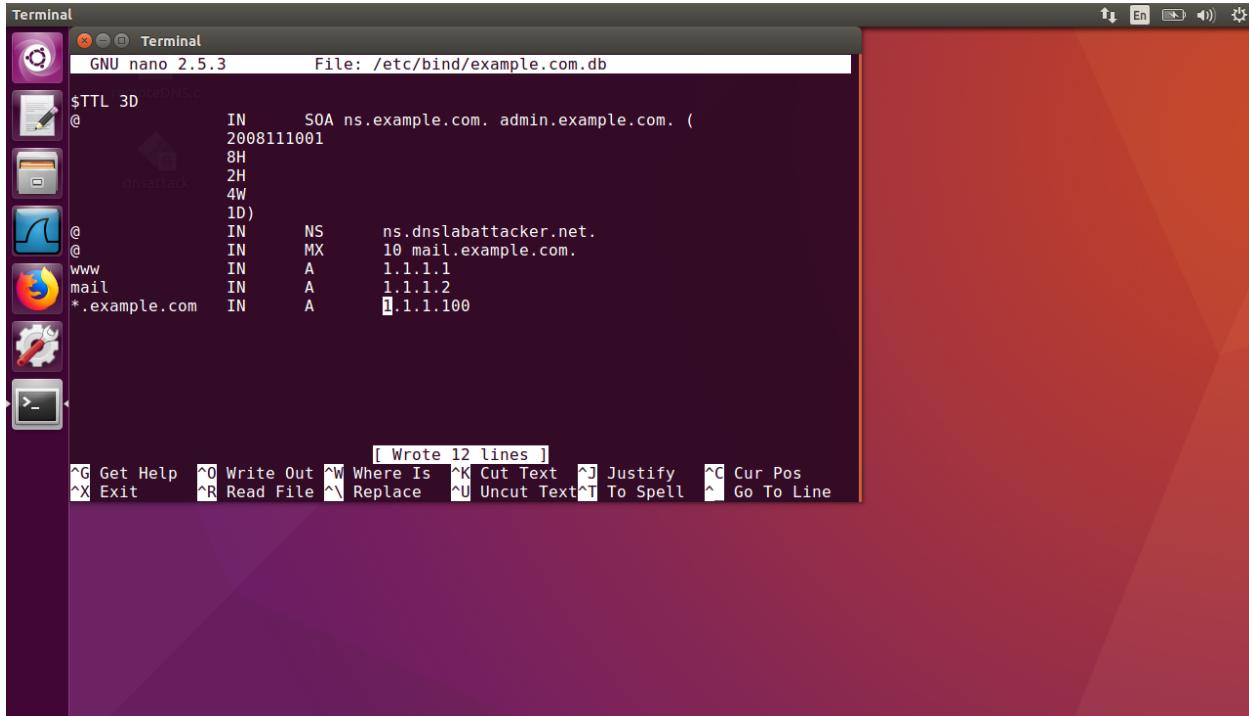
The screenshot shows a terminal window titled "Terminal" running the "GNU nano 2.5.3" editor. The file being edited is "/etc/bind/named.conf.local". The content of the file is as follows:

```
// remoteDNSc
// 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";
};
```

At the bottom of the terminal window, a status bar displays "[Wrote 12 lines]" and a series of keyboard shortcuts.

Screenshot 3.2.3: Adding zone file entry in /etc/bind/named.conf.local on attacker machine

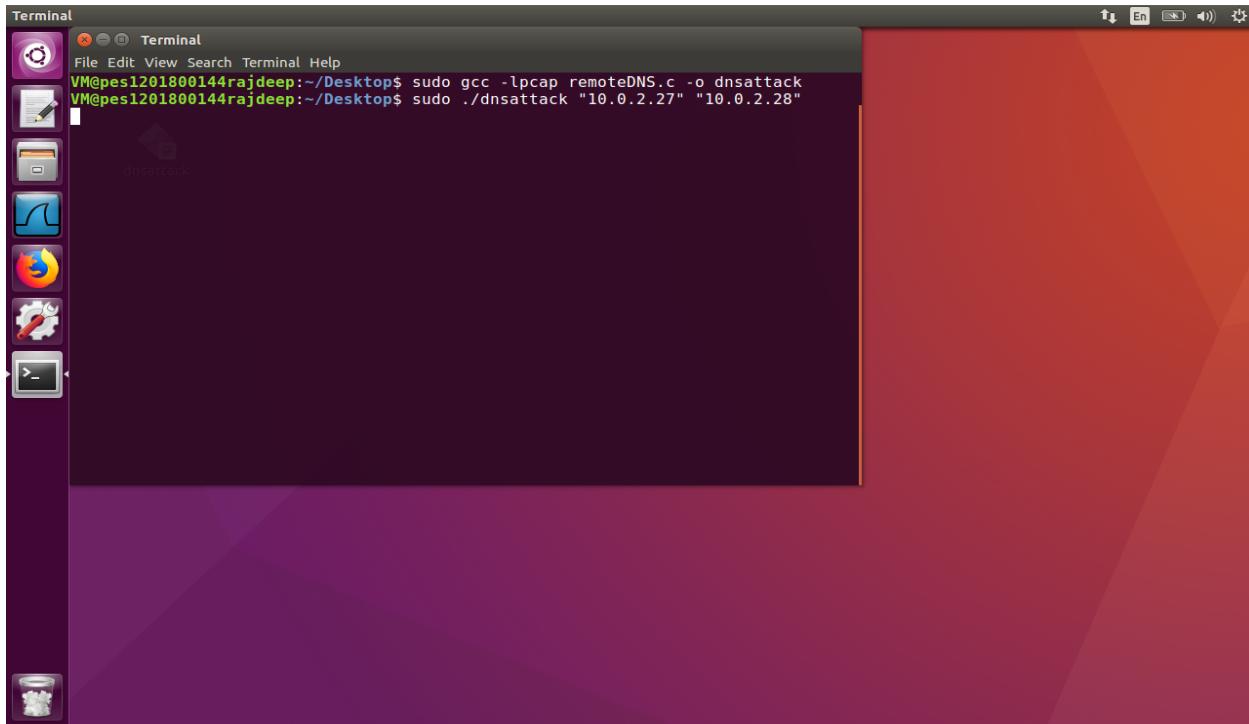


The screenshot shows a terminal window titled "Terminal" running the "GNU nano 2.5.3" editor. The file being edited is "/etc/bind/example.com.db". The content of the file is as follows:

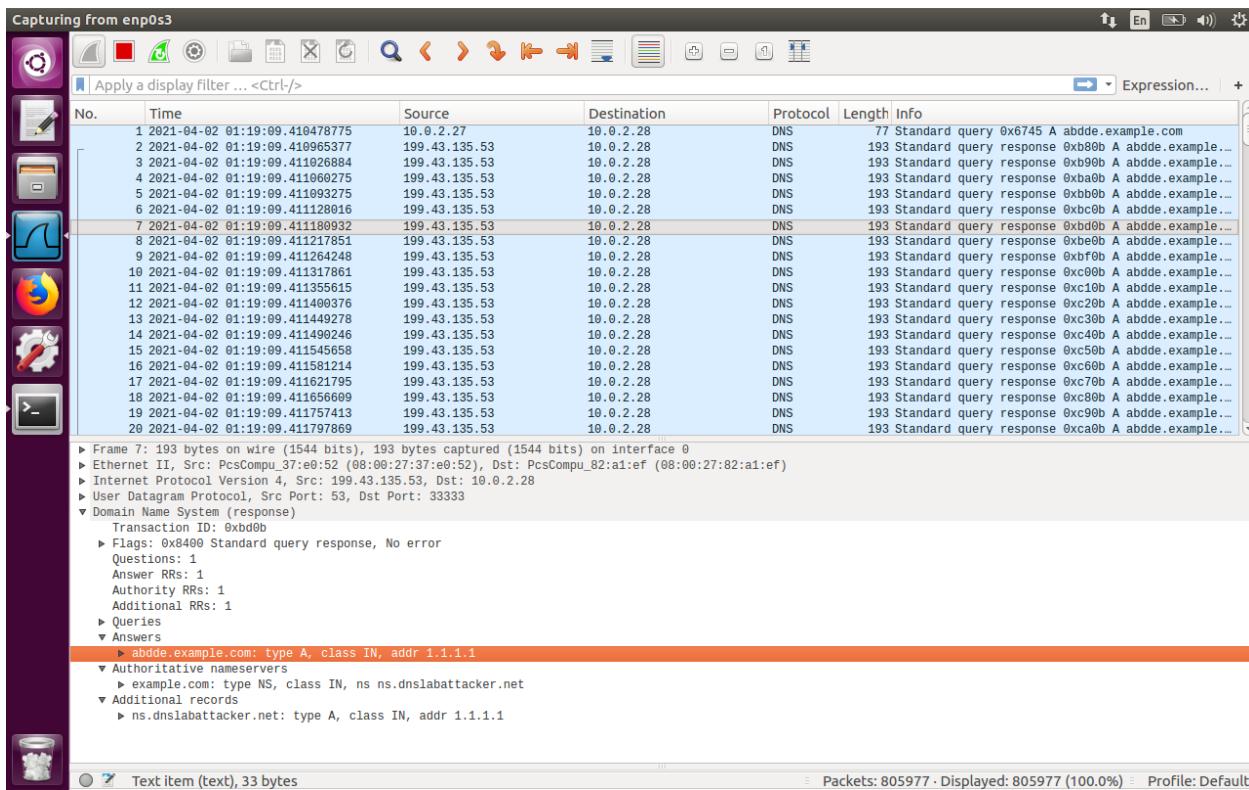
```
$TTL 3D
@       IN      SOA ns.example.com. admin.example.com. (
                  2008111001
                  8H
                  2H
                  4W
                  1D)
@       IN      NS      ns.dnslabattacker.net.
@       IN      MX      10 mail.example.com.
www    IN      A       1.1.1.1
mail   IN      A       1.1.1.2
*.example.com IN      A       1.1.1.100
```

At the bottom of the terminal window, a status bar displays "[Wrote 12 lines]" and a series of keyboard shortcuts.

Screenshot 3.2.4: Adding the example.com.db zone file in /etc/bind directory of attacker machine and restarting bind9 server



Screenshot 3.2.5: Rerunning the spoofing code



Screenshot 3.2.6: We can see Kaminsky attack is successful as in the answer section, we can find ns.dnslabattacker.net

dump.db (/var/cache/bind) - gedit

```

dump.db
/var/cache/bind

; additional
86335 RRSIG DS 8 1 86400 (
20210414210000 20210401200000 14631 .
bCxqa2+YIXBHULMpou81Yo1KPlbHob5I
nm=90dtkXwCTG9MXsWqZ0Tcpt0GyG8tNk/f
s9bg61J3DbtzY8dMB+Cpyy5WxrkBaFohj9q
bXh4j69Ezpv3VBeJ6f8c/LrTYzhIEuur6joa
AzcF2qG25p3khcs4cw00m/0RAjFTkb6xFJLH
IdJDURwsMpZ2A6qT+Re3rZB0evF1eV4/MUy
YKnmY2/2gYoucdPVUl2hdF+QSi5Xzjkv8YS
7n7WD1lWqu1YiyqITbkUFURKAwdhtDLogife
BoClvaJP3b/ToRGDHhv+p3Nhszv92yqwR9FU
MnJu2t/ftysaoJqbCg== )

; authauthority
example.com. 178 NS ns.dnslabattacker.net.

; additional
86336 DS 31406 8 1 (
189968811E6EBA862DD6C209F75623D8D9ED
9142 )
86336 DS 31406 8 2 (
F78CF3344F72137235098ECBBD08947C2C90
01C7F6A085A17F518B5D8F6B916D )
86336 DS 31589 8 1 (
3490A6806D47F17A34C29E2CE80E8A999FFB
E4BE )
86336 DS 31589 8 2 (
CDE0D742D6998AA554A92D890F8184C698CF
AC8A26FAS9875A990C03E576343C )
86336 DS 43547 8 1 (
B6225AB2CC613E0DCA7962BDC2342EA4F1B5
6083 )
86336 DS 43547 8 2 (
61SA64233543F66F44D08933625B17497C89
A70E858ED76A2145997EDF96A918 )

; additional
86336 RRSIG DS 8 2 86400 (
20210409041715 20210402030715 58540 com.
IgB57FP7WYUmG48QWlWhkHQn2D+Rd6xxp8V
84TeTp0HEYEZNptvYkzTBCFy10MSV7091fn
IRPpsX40hT5/m030UMVHFyjavfxp9q2ochZ

```

Plain Text ▾ Tab Width: 8 ▾ Ln 40, Col 1 ▾ INS

Screenshot 3.2.7: Dump file on DNS server VM

dump.db (/var/cache/bind) - gedit

```

dump.db
/var/cache/bind

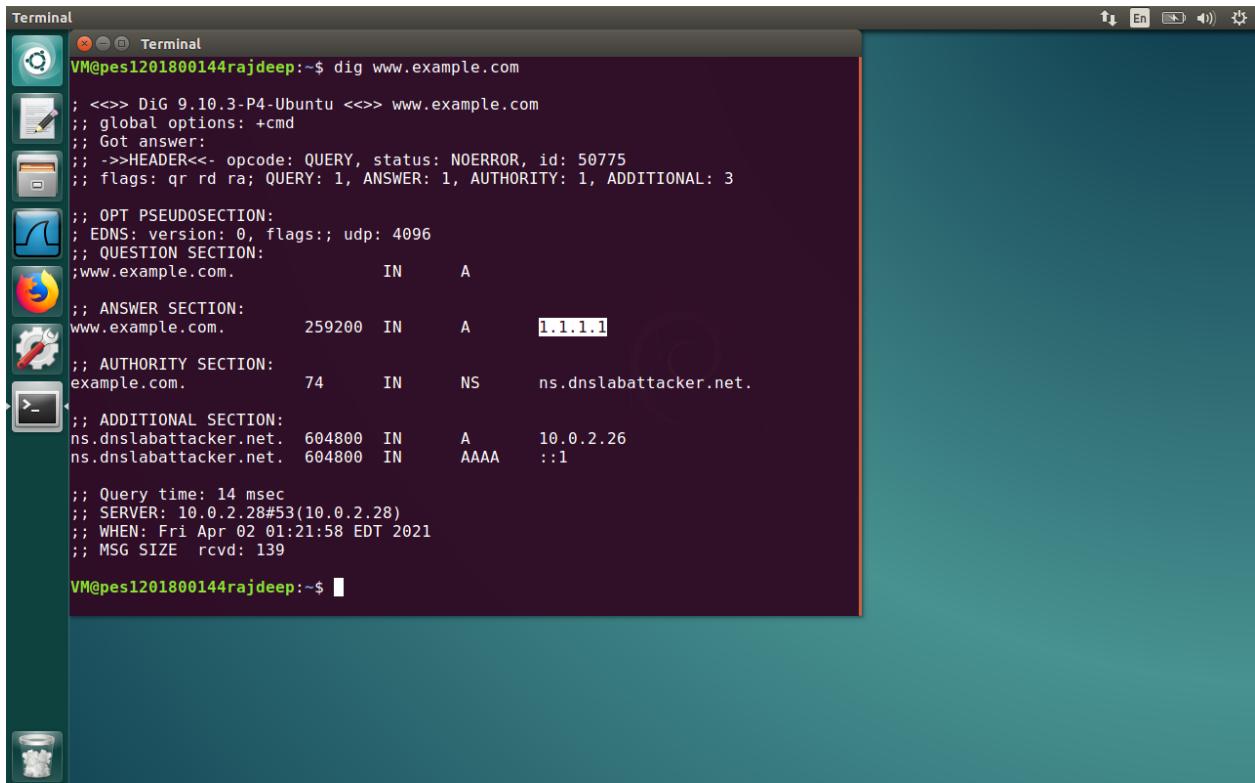
; answer
!w141U\156.example.com. 3560 \-ANY ;-$NXDOMAIN
example.com. SOA ns.icann.org. noc.dns.icann.org. 2021022314 7200 3600 1209600 3600
example.com. RRSIG SOA ...
example.com. RRSIG NSEC ...
example.com. NSEC www.example.com. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
answer
!\157\147\166.example.com. 3566 \-ANY ;-$NXDOMAIN
example.com. SOA ns.icann.org. noc.dns.icann.org. 2021022314 7200 3600 1209600 3600
example.com. RRSIG SOA ...
example.com. RRSIG NSEC ...
example.com. NSEC www.example.com. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
answer
!\162\140\162.example.com. 3571 \-ANY ;-$NXDOMAIN
example.com. SOA ns.icann.org. noc.dns.icann.org. 2021022314 7200 3600 1209600 3600
example.com. RRSIG SOA ...
example.com. RRSIG NSEC ...
example.com. NSEC www.example.com. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
authanswer
!\162\140\163.example.com. 178 A 1.1.1.1
answer
!\162\140\164.example.com. 10770 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer
!\162\141\164.example.com. 10771 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer
!\162\142\164.example.com. 10771 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer
!\163\142\164.example.com. 10771 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer
!\163\143\164.example.com. 10771 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer
!\164\143\164.example.com. 10771 \-ANY ;-$NXDOMAIN
example.com. SOA ns.example.com. admin.example.com. 2008111001 28800 7200 2419200 86400
answer

```

Plain Text ▾ Tab Width: 8 ▾ Ln 11377, Col 1 ▾ INS

Screenshot 3.2.8: In the dump file, example.com can be seen with IP address

1.1.1.1



```
Terminal
VM@pes1201800144rajdeep:~$ dig www.example.com
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50775
;; flags: qr 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.            74      IN      NS      ns.dnslabattacker.net.
;; ADDITIONAL SECTION:
ns.dnslabattacker.net. 604800  IN      A      10.0.2.26
ns.dnslabattacker.net. 604800  IN      AAAA   ::1
;; Query time: 14 msec
;; SERVER: 10.0.2.28#53(10.0.2.28)
;; WHEN: Fri Apr 02 01:21:58 EDT 2021
;; MSG SIZE rcvd: 139
VM@pes1201800144rajdeep:~$
```

Screenshot 3.2.9: Dig command replies 1.1.1.1 for www.example.com as desired

In the Kaminsky attack, when the dig command for www.example.com is sent to the DNS server VM, it searches its cache and finds ns.dnslabattacker.net.

Further, it sends a query to ns.dnslabattacker.net but gets no valid IP address. Therefore it's not a fullproof since it has a flaw which will easily be recognized and flagged by the DNS server since it doesn't have a valid IP address.

To prevent this, DNS server VM machine is configured to recognize dnslabattacker.net as real domain. This is done by creating a zone file in the server machine. By doing this, DNS server VM machine won't query the dnslabattacker.net domain and refer to the attacker machine. The domain dnslabattacker.net is looked on the attacker machine because in db.attacker file, the IP address of the attacker VM machine is given(Screenshot 3.2.2).

In the attacker VM machine, a zone file is created for example.com with the IP address 1.1.1.1 (Screenshot 3.2.4).

Hence, when the client VM machine queries dig command for www.example.com, the DNS server VM queries attacker VM which in turn returns 1.1.1.1 which is displayed in the Answer Section of dig command of client VM.