Social Engineering

Module 09

Social Engineering

Social engineering is the art of convincing people to reveal confidential information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Source: http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/index.htm

Social engineering is essentially the art of gaining access to buildings, systems, or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. The term "social engineering" can also mean an attempt to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. For example, instead of trying to find software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Shane MacDougall, a hacker/security consultant, duped a Wal-Mart employee into giving him information that could be used in a hacker attack to win a coveted "black badge" in the "social engineering" contest at the Defcon hackers' conference in Las Vegas.

In this year's Capture the Flag social engineering contest at Defcon, champion Shane MacDougall used lying, a lucrative (albeit bogus) government contract, and his talent for self-effacing small talk to squeeze the following information out of Wal-Mart:

- The small-town Canadian Wal-Mart store's janitorial contractor
- Its cafeteria food-services provider
- Its employee pay cycle
- Its staff shift schedule
- The time managers take their breaks
- Where they usually go for lunch
- Type of PC used by the manager
- Make and version numbers of the computer's operating system, and
- Its web browser and antivirus software

Stacy Cowley at CNNMoney wrote up the details of how Wal-Mart got taken in to the extent of coughing up so much scam-worthy treasure.

Calling from his sound-proofed booth at Defcon MacDougall placed an "urgent" call, broadcast to the entire Defcon audience, to a Wal-Mart store manager in Canada, introducing himself as "Gary Darnell" from Wal-Mart's home office in Bentonville, Ark.

The role-playing visher (vishing being phone-based phishing) told the manager that Wal-Mart was looking at the possibility of winning a multimillion-dollar government contract.

"Darnell" said that his job was to visit a few Wal-Mart stores that had been chosen as potential pilot locations.

But first, he told the store manager, he needed a thorough picture of how the store operated.

In the conversation, which lasted about 10 minutes, "Darnell" described himself as a newly hired manager of government logistics.

He also spoke offhand about the contract: "All I know is Wal-Mart can make a ton of cash off it," he said, then went on to talk about his upcoming visit, keeping up a "steady patter" about the project and life in Bentonville, Crowley writes.

As if this wasn't bad enough, MacDougall/Darnell directed the manager to an external site to fill out a survey in preparation for his upcoming visit.

The compliant manager obliged, plugging the address into his browser.

When his computer blocked the connection, MacDougall didn't miss a beat, telling the manager that he'd call the IT department and get the site unlocked.

After ending the call, stepping out of the booth and accepting his well-earned applause, MacDougall became the first Capture the Flag champion to capture every data point, or flag, on the competition checklist in the three years it has been held at Defcon. Defcon gives contestants two weeks to research their targets. Touchy information such as social security numbers and credit card numbers are verboten, given that Defcon has no great desire to bring the law down on its head.

Defcon also keeps its nose clean by abstaining from recording the calls, which is against Nevada law. However, there's no law against broadcasting calls live to an audience, which makes it legal for the Defcon audience to have listened as MacDougall pulled down Wal-Mart's pants.

MacDougall said, "Companies are way more aware about their security. They've got firewalls, intrusion detection, log-in systems going into place, so it's a lot harder for a hacker to break in these days, or to at least break in undetected. So a bunch of hackers now are going to the weakest link, and the link that companies just aren't protecting, which is the people."\

MacDougall also shared few best practices to be followed to avoid falling victim to a social engineer:

- Never be afraid to say no. If something feels wrong, something is wrong
- An IT department should never be calling asking about operating systems, machines, passwords or email systems—they already know

- Set up an internal company security word of the day and don't give any information to anyone who doesn't know it
- Keep tabs on what's on the web. Companies inadvertently release tons of information online, including through employees' social media sites

As an expert **ethical hacker** and **penetration tester**, you should circulate the best practices to be followed among the employees.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Objectives

The objective of this lab is to:

- Detect phishing sites
- Protect the network from phishing attacks

To carry out this lab, you need:

- A computer running Window Server 2012
- A web browser with Internet access

Lab Duration

Time: 20 Minutes

TASK 1

Overview

Overview Social Engineering

Social engineering is the art of convincing people to reveal confidential information. Social engineers depend on the fact that people are aware of certain valuable information and are careless in protecting it.

Lab Tasks

Recommended labs to assist you in social engineering:

- Social engineering
- Detecting phishing using Netcraft
- Detecting phishing using PhishTank

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Detecting Phishing Using Netcraft

Netcraft provides web server and web hosting market-share analysis, including web server and operating system detection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

By now you are familiar with how social engineering is performed and what sort of information can be gathered by a social engineer.

Phishing is an example of a social engineering technique used to deceive users, and it exploits the poor usability of current web security technologies.

Phishing is the act of attempting to acquire information such as user names, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications claiming to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel is almost identical to the legitimate one.

Phishers are targeting the customers of banks and online payment services. They send messages to the bank customers by manipulating URLs and website forgery. The messages sent claim to be from a bank and they look legitimate; users, not realizing that it is a fake website, provide their personal information and bank details. Not all phishing attacks require a fake website; messages that claim to be from a bank tell users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) is dialed, it prompts users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Since you are an expert **ethical hacker** and **penetration tester**, you must be aware of phishing attacks occurring on the network and implement anti-phishing measures. In an organization, proper training must be provided to people to deal with phishing attacks. In this lab you will be learning to detect phishing using Netcraft.

Lab Objectives

This lab will show you phishing sites using a web browser and show you how to use them. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attack

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

To carry out this lab you need:

- **Netcraft** is located at **D:\CEH-Tools\CEHv8 Module 09 Social Engineering\Anti-Phishing Toolbar\Netcraft Toolbar**
- You can also download the latest version of **Netcraft Toolbar** from the link http://toolbar.netcraft.com/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser (Firefox, Internet explorer, etc.) with Internet access
- Administrative privileges to run the Netcraft toolbar

Lab Duration

Time: 10 Minutes

Overview of Netcraft Toolbar

Netcraft Toolbar provides **Internet security services**, including anti-fraud and anti-phishing services, **application testing**, code reviews, automated penetration testing, and **research data and analysis** on many aspects of the Internet.

Lab Tasks

TASK 1

Anti-Phishing Tool bar

1. To start this lab, you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

You can also download the Netcraft toolbar form http://toolbar.netcraft.com

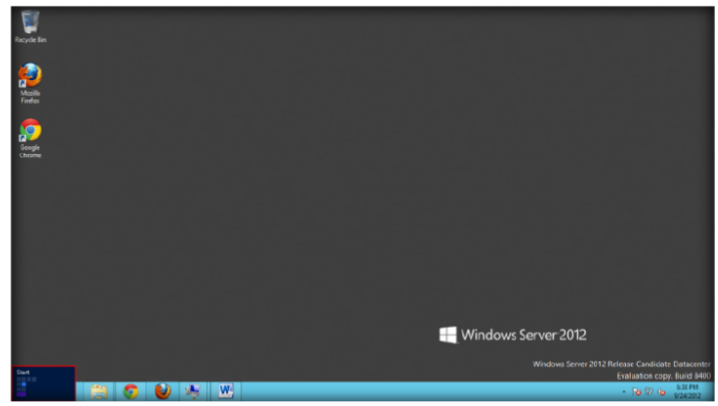


FIGURE 1.1: Windows Server 2012-Start Menu

3. Click the **Mozilla Firefox** app to launch the browser.

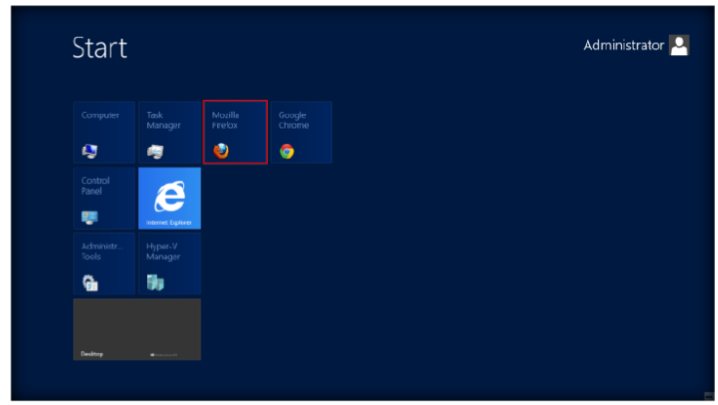


FIGURE 1.2: Windows Server 2012-Start Menu Apps view

4. To download the **Netcraft Toolbar** for **Mozilla Firefox**, enter http://toolbar.netcraft.com in the address bar of the browser or drag and drop the **netcraft_toolbar-1.7-fx.xpi** file in Firefox.
5. In this lab, we are downloading the toolbar from the Internet.
6. In Firefox browser, click **Download the Netcraft Toolbar** to install as the add-on.

Netcraft provides Internet security services, including anti-fraud and anti-phishing services.

FIGURE 1.3: Netcraft toolbar downloading Page

7. On the **Install** page of the Netcraft Toolbar site, click the **Firefox image** to continue with installation.

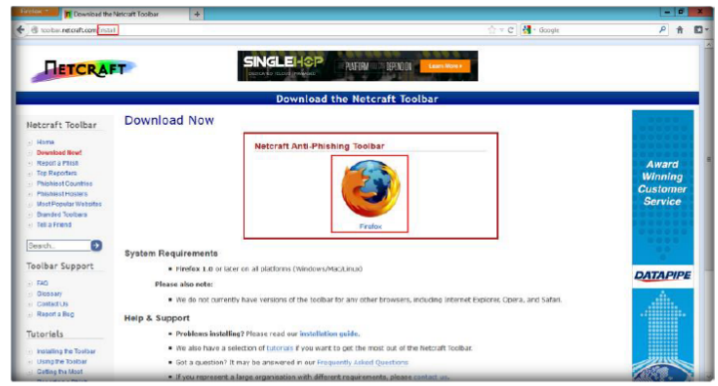


FIGURE 1.4: Netcraft toolbar Installation Page

Netcraft is an Internet services company based in Bath, England.

8. Click **Allow** to download Netcraft Toolbar.

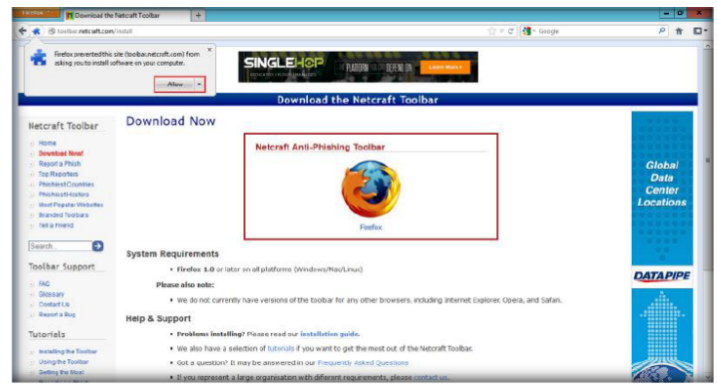


FIGURE 1.5: Netcraft toolbar Installation-Allow button

9. When the **Software Installation** dialog box appears, click **Install Now**.

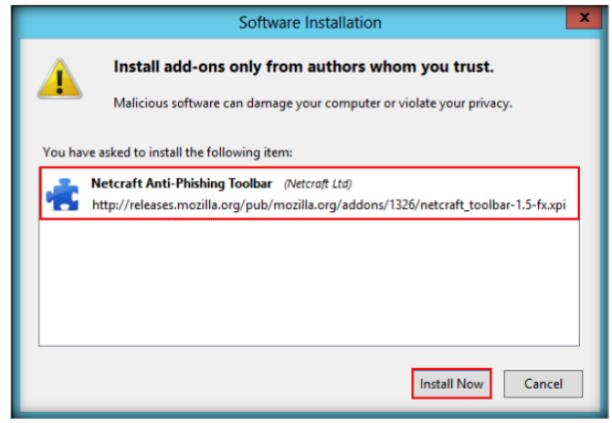


FIGURE 1.6: Installing Netcraft Toolbar

Netcraft Toolbar provides a wealth of information about the sites you visit.

10. To complete the installation it will ask you to restart the browser. Click **Restart Now**.

Risk Rating displays the trustworthiness of the current site.

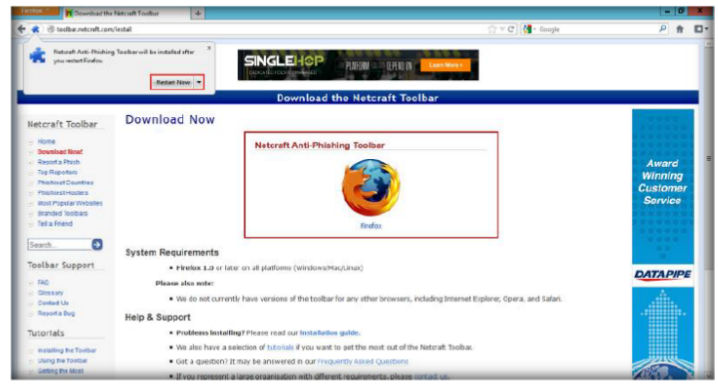


FIGURE 1.7: Restarting Firefox browser

11. **Netcraft Toolbar** is now visible. Once the **Toolbar** is installed, it looks similar to the following figure.

FIGURE 1.8: Netcraft Toolbar on Mozilla Firefox web browser

12. When you visit a site, the following information displays in the Toolbar (unless the page has been blocked): **Risk rating, Rank**, and **Flag**.
13. Click **Site Report** to show the report of the site.

Site report links to a detailed report for the current site.

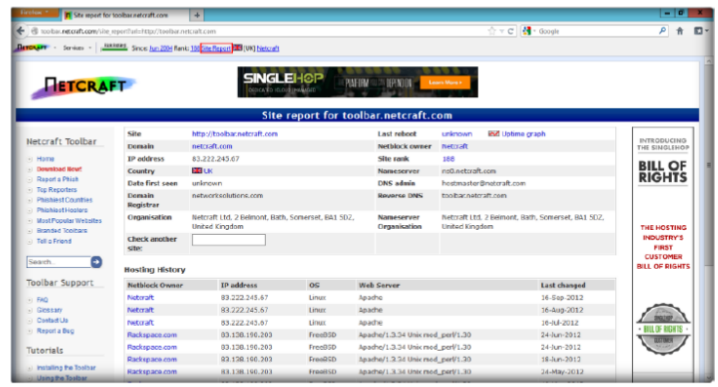


FIGURE 1.9: Report generated by Netcraft Toolbar

14. If you attempt to visit a page that has been identified as a phishing page by Netcraft Toolbar you will see a **warning dialog** that looks similar to the one in the following figure.
15. Type, as an example: http://www.paypal.ca.6551.secure7c.mx/images/cgi.bin

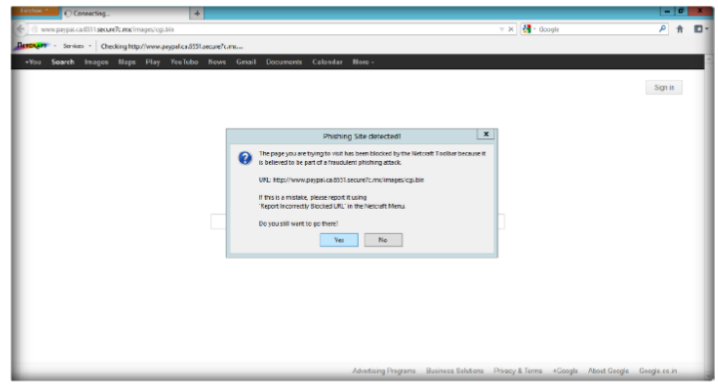


FIGURE 1.10: Warning dialog for blocked site

Phishing a site feeds continuously updated encrypted database of patterns that match phishing URLs reported by the Netcraft Toolbar.

16. If you trust that page click **Yes** to open it and if you don't, click **No (Recommended)** to block that page.
17. If you click **No** the following page will be displayed.

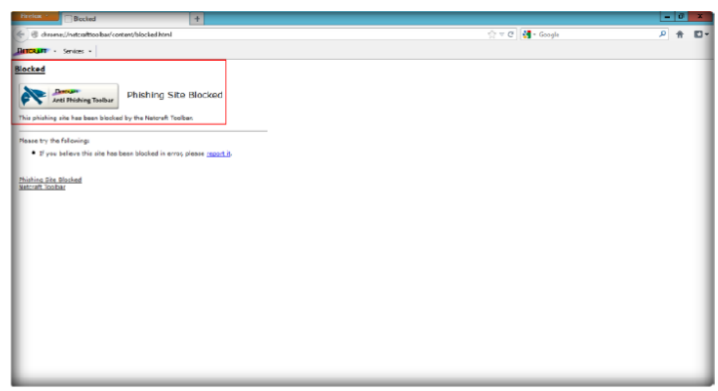


FIGURE 1.11: Web page blocked by Netcraft Toolbar

Lab Analysis

Document all the results and report gathered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Netcraft	▪ Phishing site detected

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate whether the Netcraft Toolbar works if you use a transparent proxy.

2. Determine if you can make the Netcraft Toolbar coexist on the same line as other toolbars. If so, how?
3. How can you stop the Toolbar warning if a site is trusted?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 3

Detecting Phishing Using PhishTank

PhishTank is a collaborative clearinghouse for data and information regarding phishing on the Internet.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information such as account user names and passwords that can further expose them to future compromises. Additionally, these fraudulent websites may contain malicious code.

With the tremendous increase in the use of online banking, online share trading, and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc.) by masquerading as a trusted entity.

In the previous lab you have already seen how a phishing site can be detected using the Netcraft tool.

The usual scenario is that the victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to "a secure page on the bank's website." The victim believes the web page to be authentic and he enters his user name, password, and other information. In reality, the website is a fake and the victim's information is stolen and misused.

Being an administrator or penetration tester, you might implement all the most sophisticated and expensive technology solutions in the world; all of it can be bypassed if your employees fall for simple social engineering scams. It become

your responsibility to educate employees on best practices for protecting information.

Phishing sites or emails can be reported to phishing-report@us-cert.gov

http://www.us-cert.gov/nav/report_phishing.html

US-CERT (United States Computer Emergency Readiness Team) is collecting phishing email messages and website locations so that they can help people avoid becoming victims of phishing scams.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Objectives

This lab will show you how to use phishing sites using a web browser. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attacks

Lab Environment

To carry out the lab you need:

- A computer running Windows Server 2012
- A web browser (Firefox, Internet Explorer, etc.) with Internet access

Lab Duration

Time: 10 Minutes

Overview of PhiskTank

PhishTank URL: http://www.phishtank.com

PhishTank is a **free community site** where anyone can submit, verify, track, and share **phishing data**. PhishTank is a collaborative clearing house for data and information regarding phishing on the Internet. Also, PhishTank provides an **open API** for developers and researchers to integrate anti-phishing data into their applications at no charge.

Lab Tasks

TASK 1

PhishTank

1. To start this lab you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of desktop.

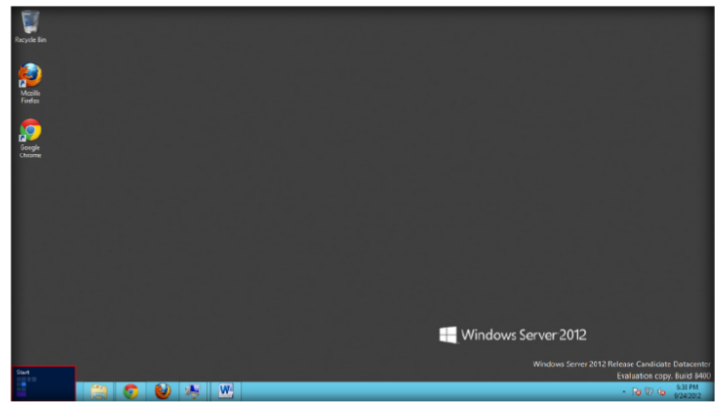


FIGURE 2.1: Windows Server 2012-Start Menu

3. Click the **Mozilla Firefox** app to launch the browser.

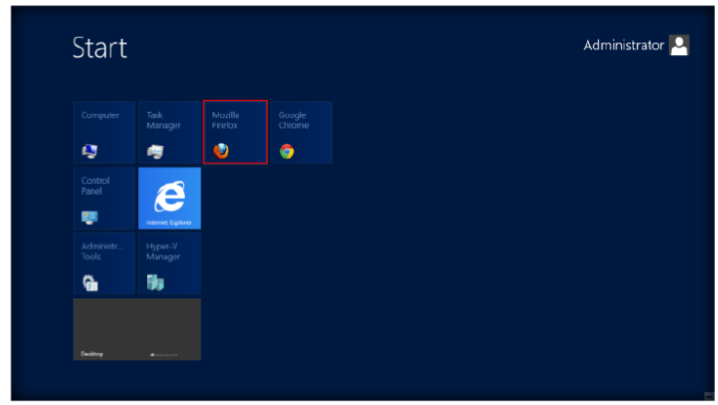


FIGURE 2.2: Windows Server 2012-Start Menu Apps view

PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

4. Type **http://www.phishtank.com** in the address bar of the web browser and press **Enter**.

5. You will see the following **screen**.

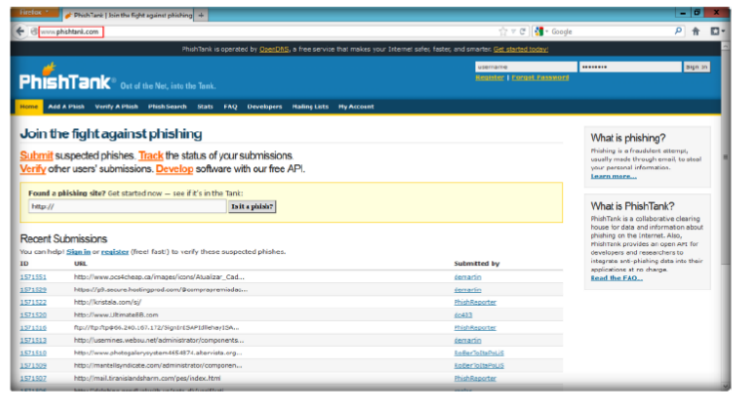


FIGURE 2.3: Welcome screen of PhishTank

PhishTank is operated by Open DNS to improve the Internet through safer, faster, and smarter DNS.

6. Type the **website URL** to be checked for phishing, for example, http://sdapld21.host21.com.
7. Click **Is it a phish?**.

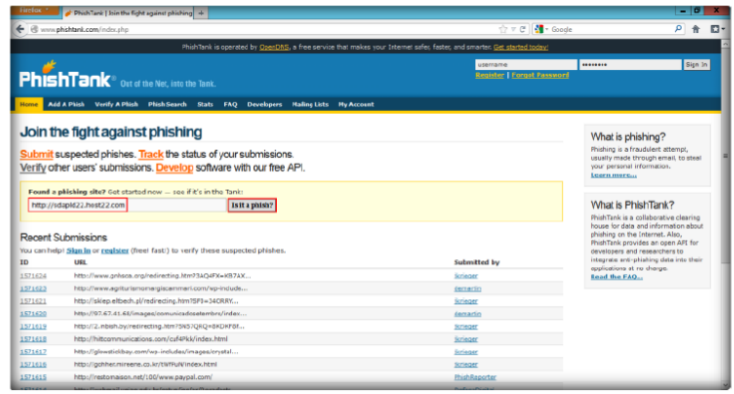


FIGURE 2.4: Checking for site

8. If the site is a **phishing site**, you see the following warning dialog box.

Open DNS is interested in having the best available information about phishing websites.

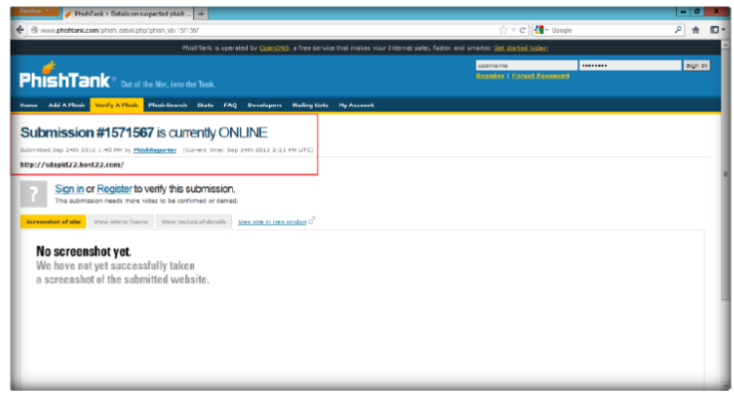


FIGURE 2.5: Warning dialog for phishing site

Lab Analysis

Document all the websites and verify whether they are phishing sites.

Tool/Utility	Information Collected/Objectives Achieved
PhiskTank	▪ Phishing site detected

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate what PhishTank wants to hear about spam.
2. Does PhishTank protect you from phishing?
3. Why is Open DNS blocking a phish site that PhishTank doesn't list or has not yet verified?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 3

Social Engineering Penetration Testing using Social Engineering Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social engineering is an ever-growing threat to organizations all over the world. Social engineering attacks are used to compromise companies every day. Even though there are many hacking tools available with underground hacking communities, a social engineering toolkit is a boon for attackers as it is freely available to use to perform spear-phishing attacks, website attacks, etc. Attackers can draft email messages and attach malicious files and send them to a large number of people using the spear-phishing attack method. Also, the multi-attack method allows utilization of the Java applet, Metasploit browser, Credential Harvester/ Tabnabbing, etc. all at once.

Though numerous sorts of attacks can be performed using this toolkit, this is also a must-have tool for a penetration tester to check for vulnerabilities. SET is the standard for social-engineering penetration tests and is supported heavily within the security community.

As an **ethical hacker**, penetration tester, or **security administrator**, you should be extremely familiar with the Social Engineering Toolkit to perform various tests for vulnerabilities on the network.

Lab Objectives

The objective of this lab is to help students learn to:

- Clone a website
- Obtain user names and passwords using the Credential Harvester method
- Generate reports for conducted penetration tests

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Environment

To carry out the lab, you need:

- Run this tool in **BackTrack** Virtual Machine
- Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Toolkit

Social-Engineer Toolkit is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. The (SET) is specifically designed to perform advanced attacks against the human element. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Lab Tasks

TASK 1

Execute Social Engineering Toolkit

1. Log in to your **BackTrack** virtual machine.
2. Select **Applications → BackTrack → Exploitation Tools → Social Engineering Tools → Social Engineering Toolkit** and click **Set**.

FIGURE 3.1: Launching SET in BackTrack

3. A **Terminal** window for SET will appear. Type **y** and press **Enter** to agree to the terms of service.

SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon.

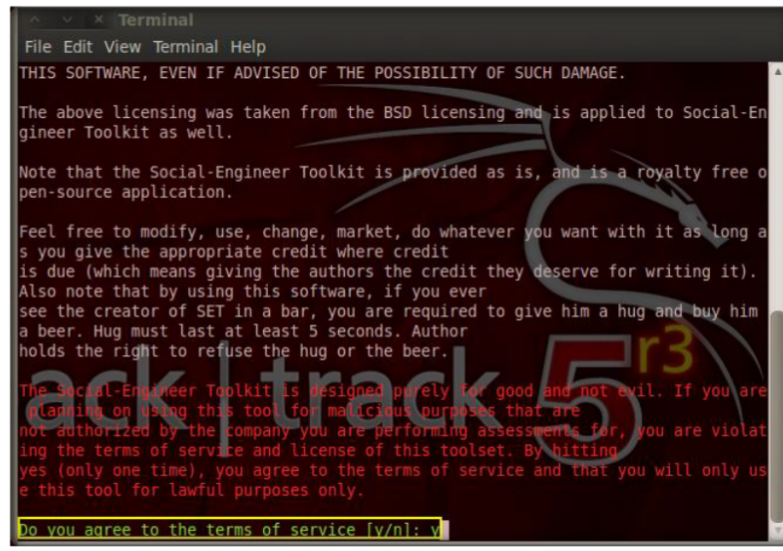
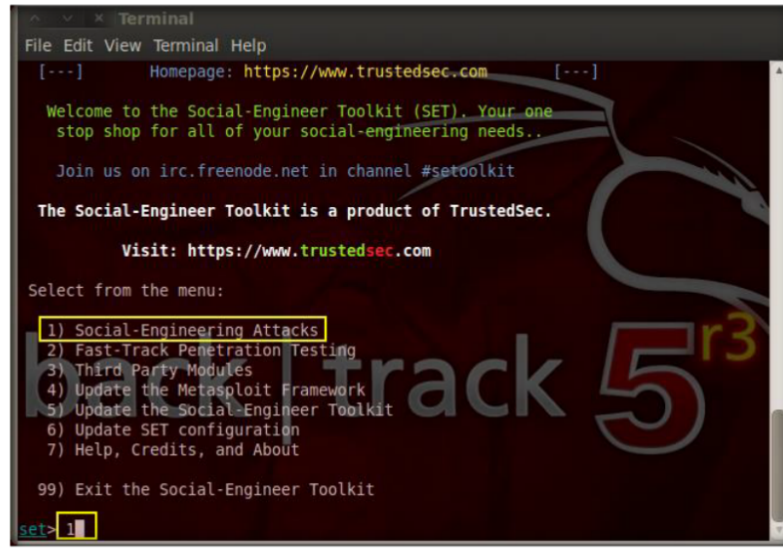


FIGURE 3.2: SET Service Agreement option

The webjacking attack is performed by replacing the victim's browser with another window that is made to look and appear to be a legitimate site.

4. You will be presented will a list of menus to select the task. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.



SET allows you to specially craft email messages and send them to a large (or small) number of people with attached file format malicious payloads.

FIGURE 3.3: SET Main menu

5. A list of menus in Social-Engineering Attacks will appear; type **2** and press **Enter** to select **Website Attack Vectors**.

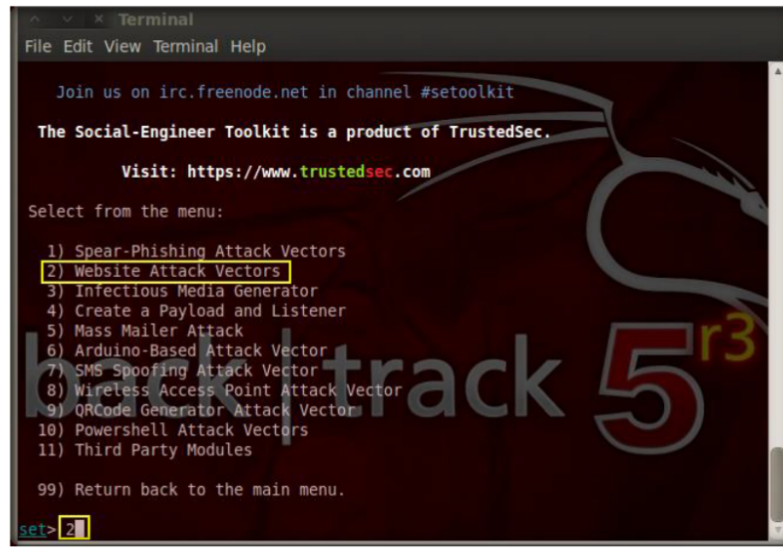


FIGURE 3.4: Social Engineering Attacks menu

The Social-Engineer Toolkit "Web Attack" vector is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

6. In the next set of menus that appears, type **3** and press **Enter** to select the **Credential Harvester Attack Method**.

FIGURE 3.5: website Attack Vectors menu

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

7. Now, type **2** and press **Enter** to select the **Site Cloner** option from the menu.

The Site Cloner is used to clone a website of your choice.

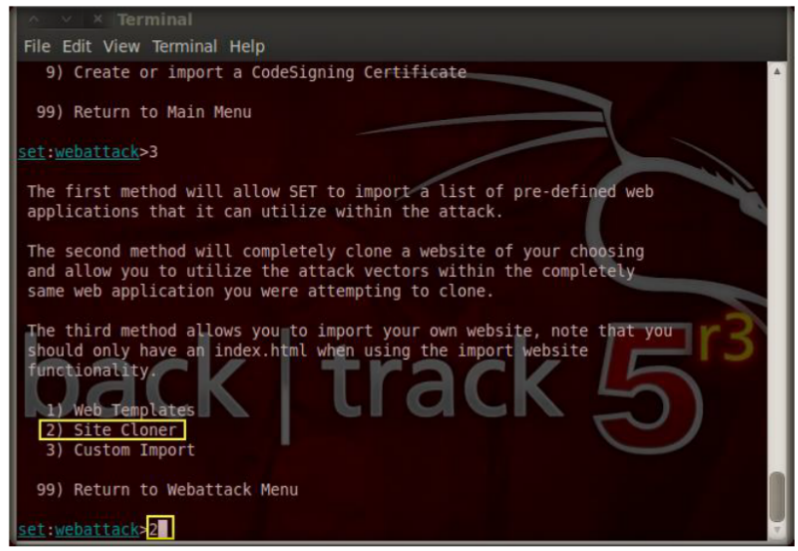


FIGURE 3.6: Credential Harvester Attack menu

8. Type the **IP address** of your BackTrack virtual PC in the prompt for **IP address for the POST back in Harvester/Tabnabbing** and press **Enter**. In this example, the IP is **10.0.0.15**.

The tabnabbing attack method is used when a victim has multiple tabs open, when the user clicks the link, the victim will be presented with a "Please wait while the page loads". When the victim switches tabs because he/she is multi-tasking, the website detects that a different tab is present and rewrites the webpage to a website you specify. The victim clicks back on the tab after a period of time and thinks they were signed out of their email program or their business application and types the credentials in. When the credentials are inserts, they are harvested and the user is redirected back to the original website.

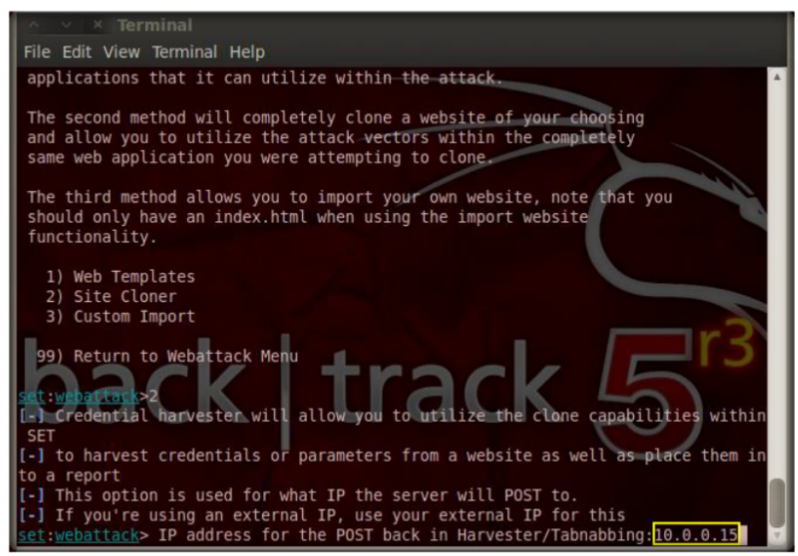


FIGURE 3.7: Providing IP address in Harvester/Tabnabbing

9. Now, you will be prompted for a URL to be cloned, type the desired URL for **Enter the url to clone** and press **Enter**. In this example, we have used **www.facebook.com**. This will initiate the cloning of the specified website.

The web jacking attack method will create a website clone and present the victim with a link stating that the website has moved. This is a new feature to version 0.7.

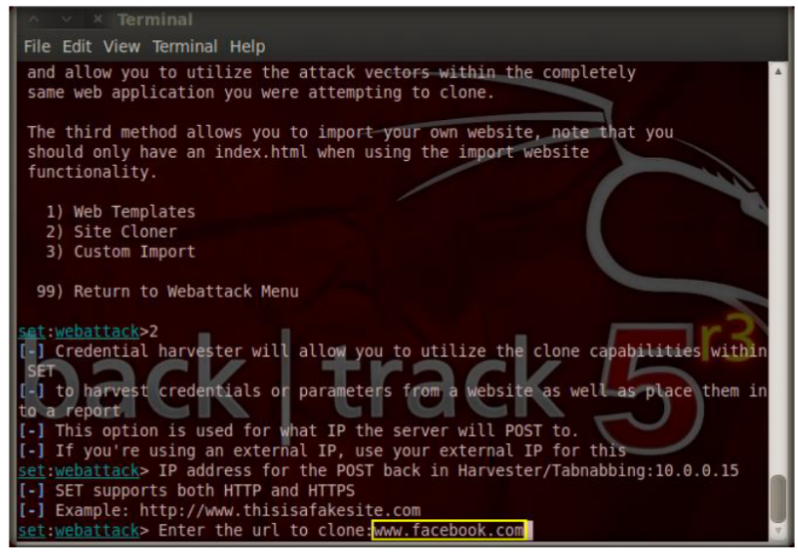


FIGURE 3.8: Providing URL to be cloned

10. After cloning is completed, the highlighted message, as shown in the following screenshot, will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.
11. It will start Credential Harvester.

If you're doing a penetration test, register a name that's similar to the victim, for Gmail you could do gmai1.com (notice the 1), something similar that can mistake the user into thinking it's the legitimate site.

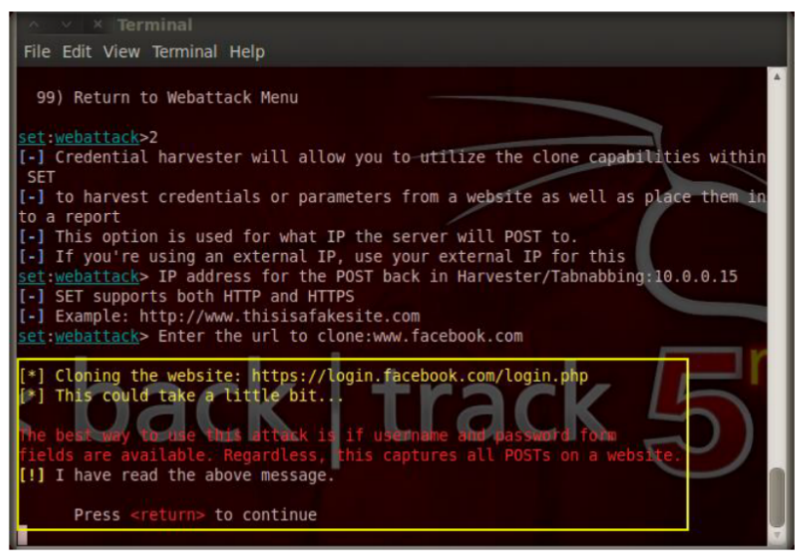


FIGURE 3.9: SET Website Cloning

12. Leave the Credential Harvester Attack to fetch information from the victim's machine.

When you hover over the link, the URL will be presented with the real URL, not the attacker's machine. So for example if you're cloning gmail.com, the URL when hovered over it would be gmail.com. When the user clicks the moved link, Gmail opens and then is quickly replaced with your malicious webserver. Remember you can change the timing of the webjacking attack in the config/set_config flags.

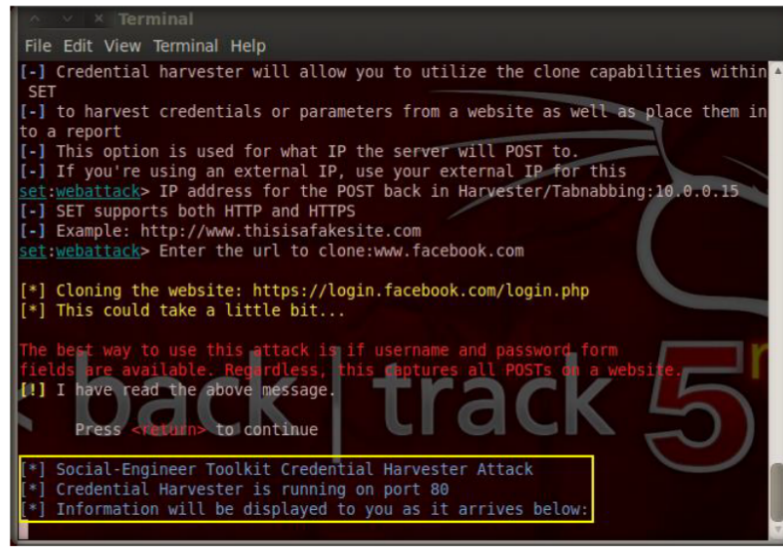


FIGURE 3.10: SET Credential Harvester Attack

13. Now, you have to send the **IP address** of your BackTrack machine to a victim and trick him or her to **click to browse** the IP address.
14. For this demo, launch your web browser in the BackTrack machine; launch your favorite email service. In this example we have used **www.gmail.com**. Login to your gmail account and compose an email.

Most of the time they won't even notice the IP but it's just another way to ensure it goes on without a hitch. Now that the victim enters the username and password in the fields, you will notice that we can intercept the credentials now.

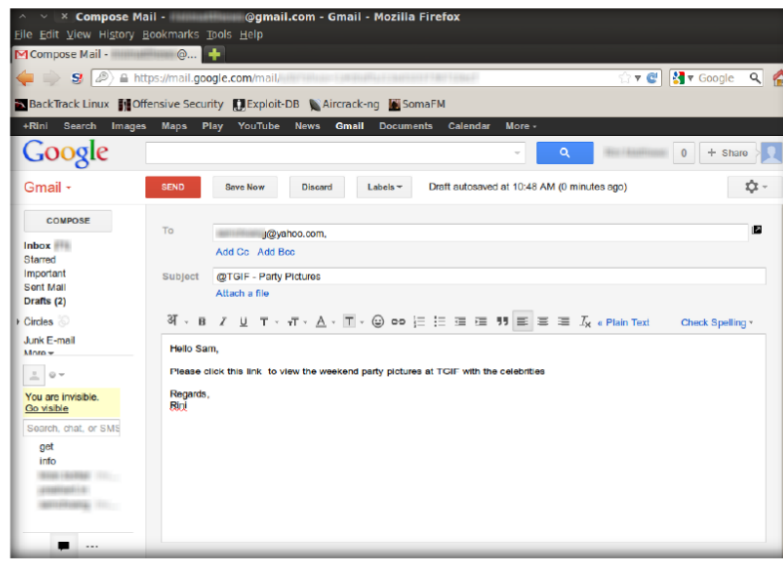


FIGURE 3.11: Composing email in Gmail

15. Place the cursor in the body of the email where you wish to place the fake URL. Then, click the **Link** icon.

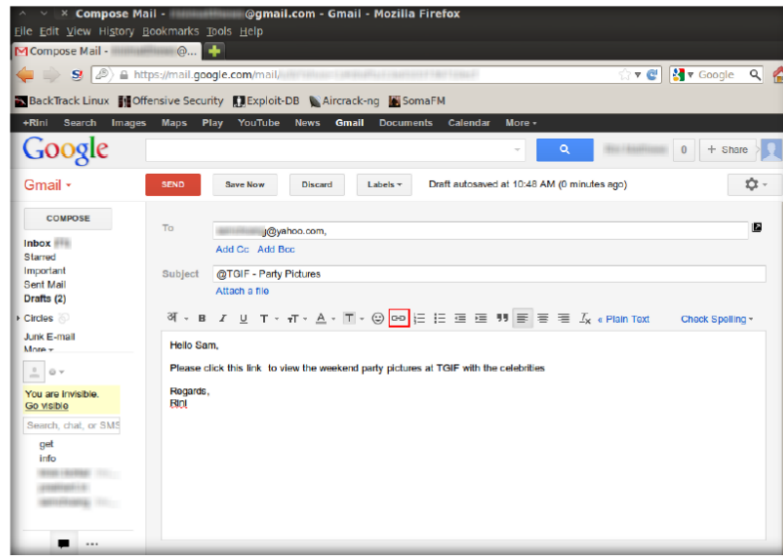


FIGURE 3.12: Linking Fake URL to Actual URL

16. In the **Edit Link** window, first type the actual address in the **Web address** field under the **Link to** option and then type the fake URL in the **Text to display** field. In this example, the web address we have used is **http://10.0.0.15** and text to display is **www.facebook.com/Rini_TGIF**. Click **OK**.

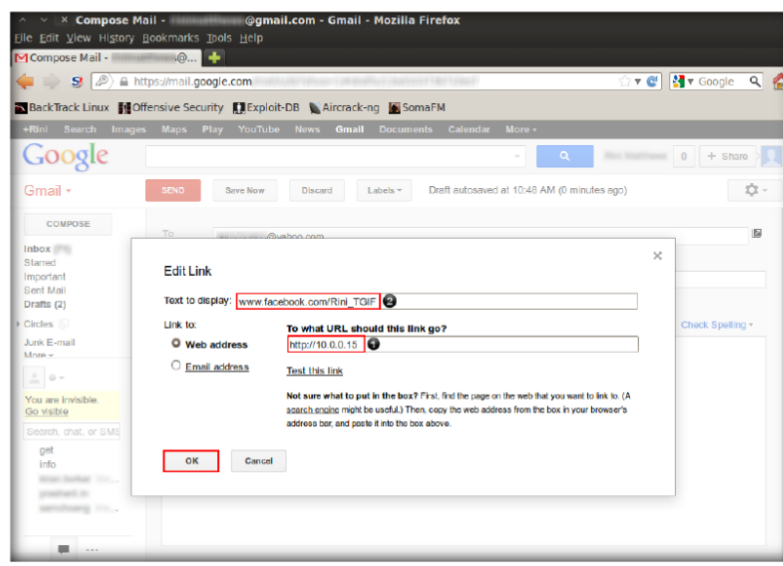


FIGURE 3.13: Edit Link window

17. The fake URL should appear in the email body, as shown in the following screenshot.

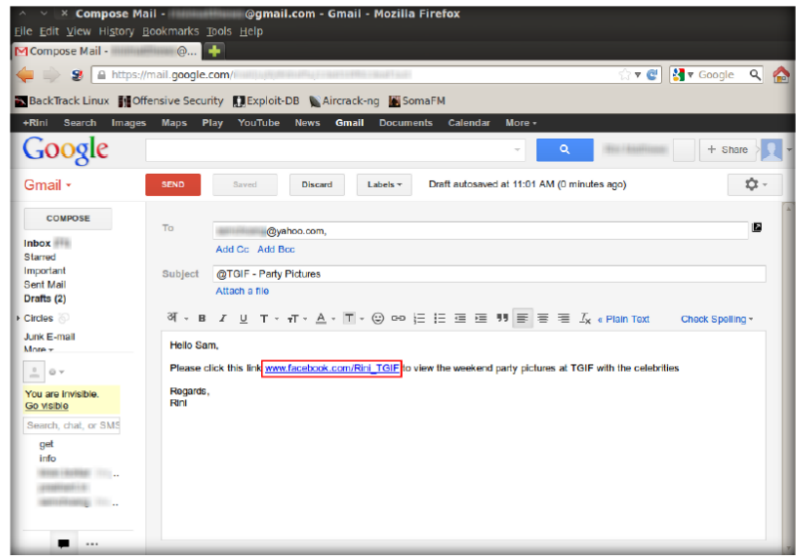


FIGURE 3.14: Adding Fake URL in the email content

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

18. To verify that the fake URL is linked to the actual URL, click the fake URL and it will display the actual URL as **Go to link:** with the actual URL. Send the email to the intended user.

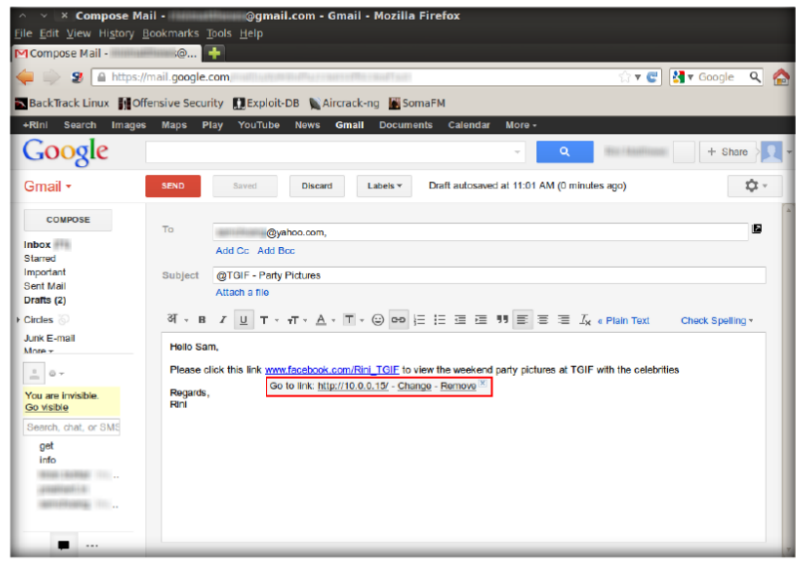


FIGURE 3.15: Actual URL linked to Fake URL

In some cases when you're performing an advanced social-engineer attack you may want to register a domain and buy an SSL cert that makes the attack more believable. You can incorporate SSL based attacks with SET. You will need to turn the WEBATTACK_SSL to ON. If you want to use self-signed certificates you can as well however there will be an "**untrusted**" warning when a victim goes to your website

19. When the victim clicks the URL, he or she will be presented with a replica of **Facebook.com**.

20. The victim will be enticed to enter his or her user name and password into the form fields as it appears to be a genuine website. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects to the legitimate Facebook login page. Observe the URL in the browser.

The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack.

The multi attack vector utilizes each combination of attacks and allows the user to choose the method for the attack. Once you select one of the attacks, it will be added to your attack profile to be used to stage the attack vector. When you're finished be sure to select the 'I'm finished' option.

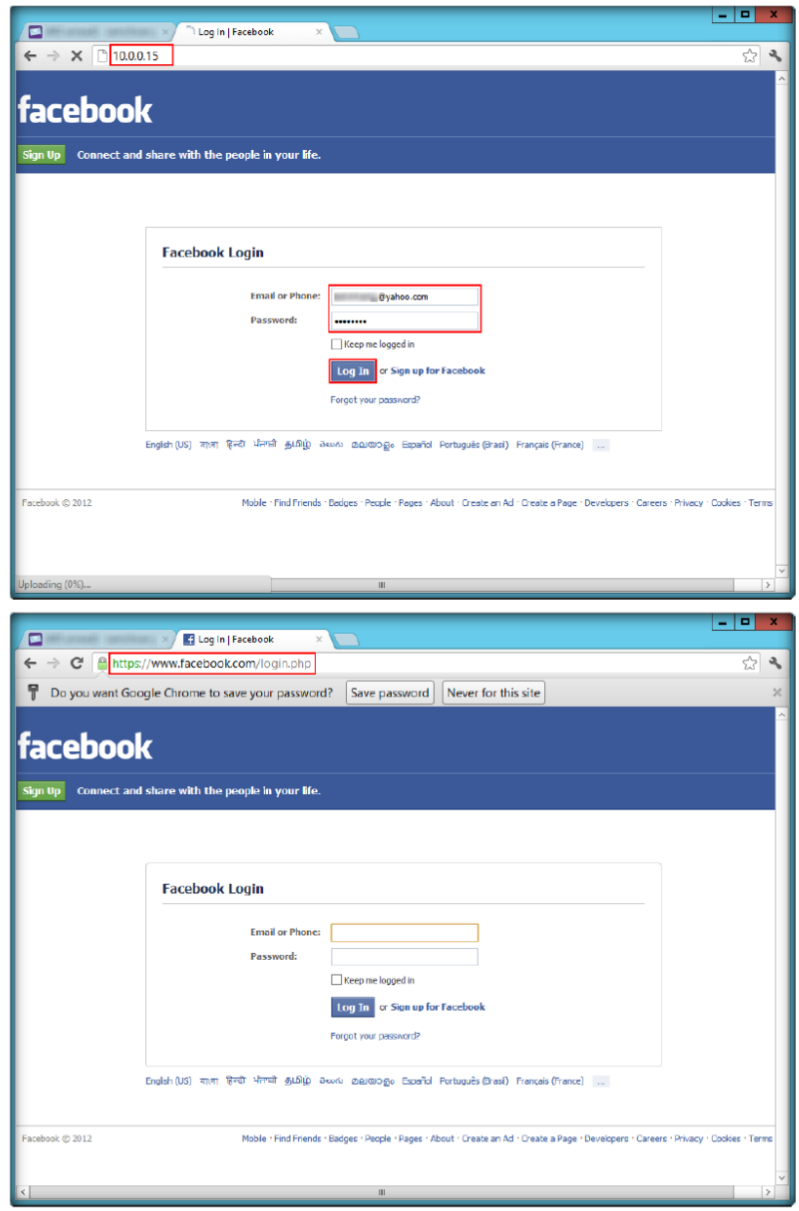


FIGURE 3.16: Fake and Legitimate Facebook login page

21. As soon the victim types in the email address and password, the **SET Terminal** in BackTrack fetches the typed user name and password, which can be used by an attacker to gain unauthorized access to the victim's account.

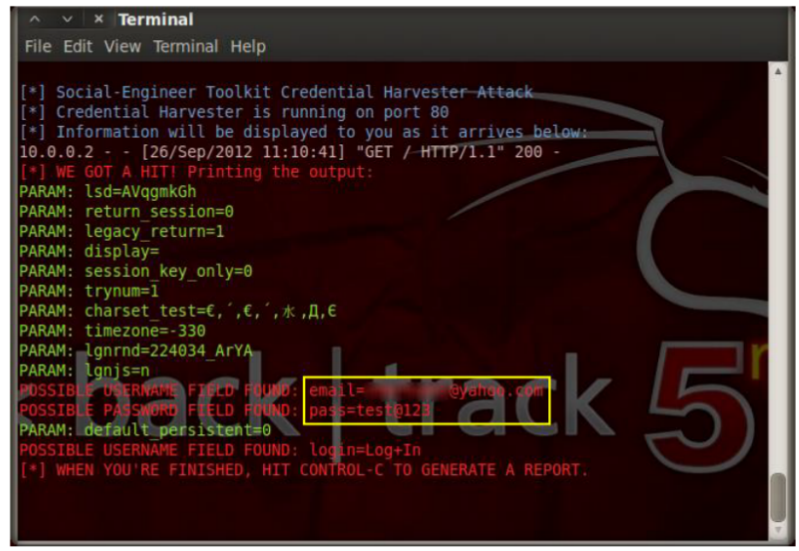


FIGURE 3.17: SET found Username and Password

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer; the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

22. Press **CTRL+C** to generate a report for this attack performed.

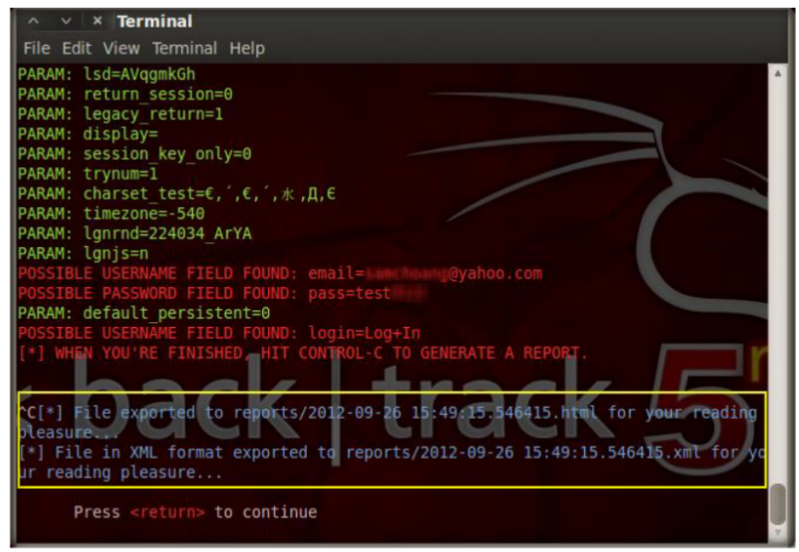


FIGURE 3.18: Generating Reports through SET

The multi-attack will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Social Engineering Toolkit	PARAM: lsd=AVqgmkGh PARAM: return_session=0 PARAM: legacy_return=1 PARAM: display= PARAM: session_key_only=0 PARAM: trynum=1 PARAM: charset_test=€,',€,', PARAM: timezone=-540 PARAM: lgnrnd=224034_ArYA PARAM: lgnjs=n
	email=samchoang@yahoo.com pass=test@123

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate each of the following Paros proxy options:
    a. Trap Request
    b. Trap Response
    c. Continue button
    d. Drop button

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs