



Understanding Social Engineering Attacks/Phishing Attacks and Mobile Operating Systems Lab (Linux Emulator for Android and iOS)

Ethical Guidelines:

-  Always ensure you have permission to gather information on a website.
-  Use this task for educational purposes or in a controlled lab environment.

• Lab Overview

The learning objective of this lab is to gain practical experience and insight into Social Engineering Attacks, with a specific focus on phishing attacks. Participants will explore the tactics used by attackers to exploit human psychology and manipulate individuals into divulging sensitive information or performing actions that compromise security. They exploit human vulnerabilities rather than technical flaws to gain unauthorized access to systems or data. Moreover, we will emulate Linux environments on our phones and perform information gathering. If you are an Android user, you must install **Termux**. If you are an iOS user, you must install **iSH Shell**.

Lab Environment Setup for Task 1

• Zphisher

An automated phishing tool with 30+ templates. The features include the latest and updated login pages, users friendly, multiple tunneling options, localhost, Cloudflared, localXpose, mask URL support, and Docker support.

Lab Environment Setup for Task2

a. Termux (Available for Android OS):

Termux is a powerful terminal emulator for Android OS. It offers a Linux environment on Android devices without the requirement of root access. Termux offers the following features:

1. **Terminal Emulation:** supports bash, zsh etc.
2. **Package Management:** additional packages can be installed using the package manager via APT.
3. **Development:** ideal for developers as languages such as Python, Ruby, Node.js and C are supported. Codes can be compiled with Clang, make and gdb.
4. **Remote Access:** remote computers or servers can be connected via SSH.

Installation and Setup:

1. Termux requires following requirements for installation:
 - a. **Android version:** Android 7.0 or above.
 - b. **Permission:** Storage and Network access should be permitted.
2. Termux can be downloaded from Playstore, F-Droid and GitHub.
3. Install Termux on your phone by giving the required permission.

4. After Installation, open the app.
5. Update the Packages by entering “apt update”.
6. Upgrade the installed packages by entering “apt upgrade”.
7. Enable storage access by entering “termux-setup-storage” and give the required permissions to the application.

For more information, refer to [How to install and Setup Termux on Android: A beginner's guide \(hashnode.dev\)](#) .

b. iSH (Available for iOS):

iSH allows you to emulate Linux shell on iOS devices. It offers an lightweight Alpine Linux environment using usermod x86 emulation to run Linux binaries on iOS. iSH offers following features:

1. **BusyBox Utilities:** iSH includes BusyBox, which combines manu common Unix utilities into single executables.
2. **Package Management:** Software packages can be installed and managed within iSH environment with the help of package manager via APK.
3. **File System Access:** files and directories can be managed with the help of iSH.
4. **Open-sorce:** iSH is open-source and its development is active on GitHub.

Installation and Setup:

1. iSH can be downloaded from the AppStore on iPhone or iPad.
2. Once installed, open iSH app.
3. Update the Packages by entering “apk update”.
4. Upgrade the installed packages by entering “apk upgrade”.

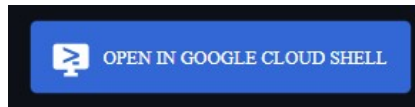
For more information, refer to [iSH - An iOS Linux Shell for Your iPhone or iPad \(bleepingcomputer.com\)](#) .

Lab Tasks 1: For Social Engineering Attack/Phishing attack Using Zphisher

In this lab, you need to conduct social engineering attacks using social media cloning. The attacks are performed on Windows operating systems. However, you can also conduct the same attack on the other operating system and compare the observations after lab classes. You are supposed to use all the different tools for the experiments. However, the required tasks are mentioned as follows:

Steps:

1. Go to this link <https://github.com/htr-tech/zphisher?tab=readme-ov-file>
2. Scroll down find “Open in Google cloud shell”, and click it.



3. Use any Google account. Confirm as “trust repo” and click **Confirm**.
4. Once it is successfully compiled you find the below interface

```
cloudshell x + v
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project cloudshell_open --repo_url "https://github.com/htr-tech/zphisher.git" --page "e
zamwallet@cloudshell:~$ cloudshell_open --repo_url "https://github.com/htr-tech
2024/09/23 00:09:03 Cloning https://github.com/htr-tech/zphisher.git into /home
Cloning into '/home/zamwallet/cloudshell_open/zphisher'...
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 1801 (delta 6), reused 9 (delta 3), pack-reused 1786 (from 1)
Receiving objects: 100% (1801/1801), 28.69 MiB | 13.93 MiB/s, done.
Resolving deltas: 100% (808/808), done.
zamwallet@cloudshell:~/cloudshell_open/zphisher$
```

5. For installation: Just, Clone this repository –

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git
```

6. Now go to cloned directory and run zphisher.sh –

```
$ cd zphisher
$ bash zphisher.sh
```

7. Now the environment ready to use.
8. Select the template, select the localhost, select the port, then go to the localhost link, and then check.

Challenge:

1. Create a different fake site (i.e. any).
 2. Try to create a phishing email (**Optional**)
For details: <https://caniphish.com/email-phishing-simulator>
- (**Screenshot required**)
 1. Provide your **“UTS email”** as the login username and enter **“Student-ID”** as the password.

- Please shortly summarize what you get from this lab and try to answer the following question below (**mandatory**):

1. What happens when I get a phishing link and input my details?
2. How to defend yourself?

Task 2 (For Android User): Information Gathering for Any Website Using Termux.

Steps:

- Check your version

`uname -a`

```
$ uname -a
Linux localhost 4.14.180-perf+ #1 SMP PREEMPT Tue Dec 13 15:34:06 CST 2022 aarch64 Android
```

- Update Termux Packages: First, ensure that all your packages are updated:

`pkg update && pkg upgrade`

```
Report issues at https://bugs.termux.com
$ pkg update && pkg upgrade
Get:1 https://termux.net stable InRelease [1088 B]
Get:2 https://termux.net stable/main aarch64 Packages [233 kB]
Fetched 234 kB in 1s (166 kB/s)
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
Hit:1 https://termux.net stable InRelease
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
Upgrading:
```

You need to give permission to download some dependencies

```
Continue? [Y/n] yy
Get:1 https://termux.net stable/main aarch64 coreutils aarch64 9.5-1 [766 kB]
Get:2 https://termux.net stable/main aarch64 findutils aarch64 4.10.0 [252 kB]
Get:3 https://termux.net stable/main aarch64 libbug-error aarch64 1.50 [115 kB]
Get:4 https://termux.net stable/main aarch64 libassuan aarch64 2.5.7-1 [71.8 kB]
Get:5 https://termux.net stable/main aarch64 libgcrypt aarch64 1.10.3-2 [438 kB]
```

Install python

```
$ pkg instal git python
Installing:
git python

Installing dependencies:
clang libsqlite
gdbm libxml2
libz libidn2
```

- Install Necessary Tools: Install the following packages to perform information gathering:
 - **nslookup**: For gathering DNS information.
 - **Whois**: To gather domain information.
 - **curl**: To identify technologies used on a website.
 - **Wget**: To download files or pages from a website (optional)

To install tool use

`pkg install <name of the tool>`

```

$ pkg install nmap
Installing=
nmap

Installing dependencies=
liblua54 libpcap nmap-ncat resolv-conf

Summary=
Upgrading= 0. Installing= 5. Removing= 0. Not Upgrading= 0
Download size= 5146 kB
Space needed= 28.4 MB

Continue? [Y/n]

```

Do the same process to install other tools.

- Perform a WHOIS Lookup: A WHOIS lookup provides information about the domain name owner, IP address, and other registration details.

`whois example.com` (Screenshot required)

Replace example.com with the target website. This command will return details like the domain registrar, registration dates, and contact information (if publicly available).

- Use Nslookup for DNS Information: Termux supports the nslookup command, which is useful for DNS querying.

`nslookup example.com` (Screenshot required)

This command will perform a basic SYN scan. It will help you determine which ports are open and the types of services running on the server.

- Use Curl to Fetch HTTP Headers: Curl is a powerful tool that can be used to fetch HTTP headers and see what technologies and security measures the website uses (e.g., server type, HTTP methods, etc.).

`curl -I example.com` (Screenshot required)

This will return information about the platform (e.g., WordPress, Apache, PHP) that the website uses.

- Download a Webpage Using Wget: You can download a webpage's source code to analyze it further.

`wget http://example.com` (Screenshot required)

This downloads the HTML page, which you can then examine for comments, metadata, or links.

Task 2: (For iPhone User): Information Gathering for Any Website Using iSH

- Launch iSH and Update the System: Once you have the iSH shell up and running, the first step is to update the system and install necessary tools. Run the following command to ensure everything is up-to-date:

`apk update && apk upgrade`

- Install Basic Tools for Information Gathering: iSH supports apk, the package manager for Alpine Linux, which allows you to install basic tools like whois and wget.

Install Whois (for domain information):

`apk add whois`

Install Wget (for web page download):

`apk add wget`

- Install Nmap (for port scanning and network mapping): Nmap is not available directly in the Alpine repositories on iSH, but if you have a separate device running Nmap (or want to use a cloud VM), you can use it alongside iSH.
- Install Curl (to check website headers and response):

`apk add curl`

- Perform a WHOIS Lookup: WHOIS can provide details about the domain name, including registrar information, registration dates, and other publicly available information.

`whois example.com` (Screenshot required)

Replace example.com with the target website. This will return information like the domain owner, registration dates, and DNS details.

- Run Wget to Download a Webpage: You can use wget to download the homepage or specific pages of the target website for offline analysis. (optional)

`wget http://example.com` (Screenshot required)

- Use Curl to Fetch HTTP Headers: Curl is a powerful tool that can be used to fetch HTTP headers and see what technologies and security measures the website uses (e.g., server type, HTTP methods, etc.).

`curl -I http://example.com` (Screenshot required)

- This will return HTTP headers such as:
- Server: Tells you the web server software (e.g., Apache, Nginx).

- X-Powered-By: Provides information about the technology stack (e.g., PHP).
- Content-Type: Shows the type of data being served (e.g., HTML, JSON, etc.).
- Use Nslookup for DNS Information: iSH supports the nslookup command, which is useful for DNS querying.

`nslookup example.com` (Screenshot required)

This will return the IP addresses and DNS details associated with the domain, allowing you to understand its network configuration.

Example Workflow:

- First, run a **WHOIS** lookup to get basic information about the domain:

`whois example.com`

- Next, use **nslookup** to get the DNS information for the domain:

`nslookup example.com`

- After that, use **curl** to fetch HTTP headers and analyze the server and technology stack:

`curl -I http://example.com`

- Finally, download the webpage using **wget** for further analysis:

`wget http://example.com`

(Using Cloud Servers: You can combine iSH with a VPS (Virtual Private Server) running Linux for a more complete toolset.)

References:

1. [Github - Termux APP](#)
2. [ish an ios Linux shell for your iPhone or iPad](#)
3. [iSH Shell | Hacker News](#)
4. [Termux Installation - YouTube](#)
5. [how to install and setup Termux on android a beginner's guide](#)
6. [how to use Termux as a beginner](#)

Alternative way (Optional)

Alternative Method (Not mandatory for submission)

To conduct this lab, we do not need a virtual environment, this task can be done with any operating system such as Windows, MacOS, and Linux. The tools being used for this lab are Namecheap, 000webhost, basic PHP script, Notepad++, and social media.

For Social Engineering Attack/Phishing attack

▪ Namecheap

“Namecheap, an ICANN Accredited Domain Registrar, offers domain registration, web hosting, SSL certificates, and more. By using this site, you will be able to learn about Homoglyphs or Homographs attacks. Homograph attacks exploit the visual similarity between characters from different writing systems to deceive users. ([Ref](#)).

▪ 000webhost

000webhost is a free web hosting service that enables individuals and small businesses to create and manage websites without incurring expenses. Users can utilize 000webhost to host personal blogs, portfolios, and small business websites, among other types of sites. The platform also supports popular web technologies like PHP and MySQL, allowing for the development of dynamic and interactive web pages ([Ref](#)).

▪ POST PHP

POST PHP is a server-side scripting language commonly used for processing form data submitted by a web browser. When a user fills out a form on a website and submits it, the data is sent to the server using the HTTP POST method. POST PHP scripts are crucial components of phishing websites because they enable attackers to intercept and process the data entered by victims. By crafting PHP scripts to handle form submissions, attackers can capture the information submitted by users and store it on a server under their control. They can perform actions such as logging the stolen information, sending it to remote servers, or automatically redirecting users to legitimate websites after capturing their data to avoid detection ([Ref](#)).

▪ Social Media Cloning

In phishing attacks targeting social media platforms, attackers often create clones or replicas of legitimate social media websites or apps to deceive users into divulging their login credentials and other sensitive information.

Step 0: Create a homograph sample

These attacks exploit visual similarities between characters in different alphabets (e.g., Roman and Cyrillic). By using similar-looking characters, attackers create deceptive URLs or login pages to trick victims into revealing sensitive information ([Ref](#)). These rely on URLs that look very similar to the real website. **However, this is an optional task the reason for this task is to understand the concept of homograph attack.**

“faecbook.com” (fake) vs. “facebook.com” (legitimate)

“instaqram.com” (fake) vs. “instagram.com” (legitimate)

Sub-Steps:

1. Create or buy a Domain name (**Optional**), based on your selective social media, but in this lab, you do not have to buy the domain name.



Step 1: Creating a phishing website

000webhost can be used to execute social engineering attacks in many ways. Firstly, they could construct deceptive phishing websites, mimicking legitimate login pages of banks or email services, where unsuspecting users might input their credentials, unknowingly providing them to the attacker. Another method involves malicious redirects; the attacker might create a seemingly harmless website on 000webhost but redirect visitors to malicious sites without their knowledge. Furthermore, they might exploit popular social media platforms by hosting phishing pages to entice users into disclosing their login credentials ([Ref](#)). In this task, you need to create a phishing site. Remember, ethics matter. **Use your knowledge for positive purposes, such as securing systems and educating others about cybersecurity.**

Sub-Steps:

1. Create an account using your email address.
2. Select a website name based on the selected social media.
3. Provide your website name, and confirm with your password.
4. Once you created the website, go to the file > manager and Select Upload site.
Prepare relative documents, with the following next task.

Step 2: Creating a POST.PHP file to capture sensitive information

We will use the POST PHP file to capture and manipulate sensitive information submitted by unsuspecting users. POST PHP scripts are crucial components of phishing websites because they enable attackers to intercept and process the data entered by victims. By crafting PHP scripts to handle form submissions, attackers can capture the information submitted by users and store it on a server under their control.

Sub-Steps:

1. Create a file with the name POST.PHP, and copy the below code.

```
<?php
header(); // Fixed the header function call
$handle = fopen();
for each ($_POST as $variable => $value) {
// Removed invalid characters "[" and "in" and fixed the path
fwrite($handle, $variable . " - " . $value . "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

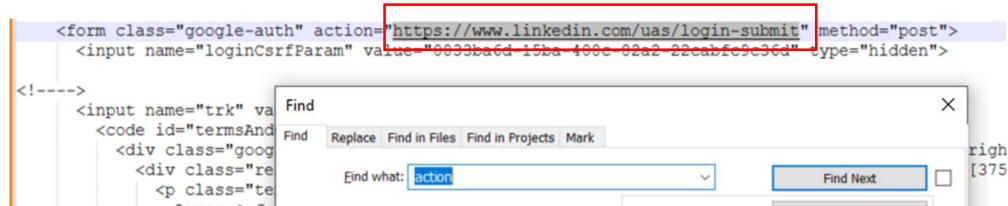
2. Inside the PHP file “header (); input – ‘Location: <https://www.linkedin.com/>’.
3. Then `$handle = fopen(“”);` Create a txt file as “**username.txt**”, “a” where the user input details will be stored.

Step 3: Social Media Cloning.

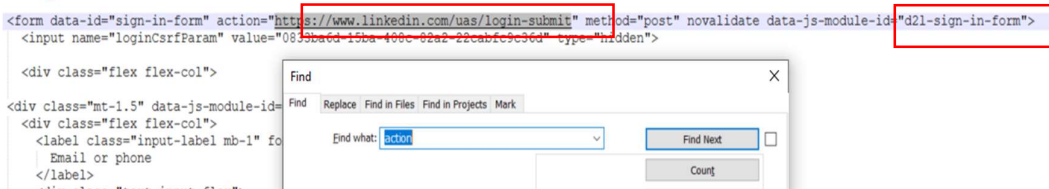
In phishing attacks targeting social media platforms, attackers often create clones or replicas of legitimate social media websites or apps to deceive users into divulging their login credentials and other sensitive information. In this lab, we will choose popular social media platforms such as LinkedIn. The process of creating social media cloning is as follows:

Sub-Steps:

1. We choose LinkedIn, and browse LinkedIn on your browser.
2. Type **Ctrl+Shift+C** or **Ctrl+U** to open source code, select source code **Ctrl+A**, copy **Ctrl+C** (all HTML code), and paste them into **Notepad++**.
3. In Notepad++, type, Ctrl+F, search box type **"action"** find the login link, and rename it with **Post. PHP**.



4. Again, find the text and remove it from the data, this time also remove **"d2l-sign-in-form"**



5. Then, once completed save it as, the file name, **"index.html"**

Step 4- Uploading the files.

This time, you have to upload the "POST.PHP" and "index.html" files on the "000webhost" file manager, that we completed in **Step1**.

1. Upload the "POST.PHP" and "index.html" files on "000webhost"
2. Go back to the Dashboard copy the *URL* and send the link to the victim
3. Once the victim clicks the link it will be redirected to the fake page which will look like the original site
4. Once the victim inputs their credentials, the email and password are saved on the **"000webhost"** site and the victim will be redirected to the original LinkedIn site.
5. You can find the victim details in the following **"usernames.txt"** file.

48730-32548, Cyber Security Week-8

<div>▼ /</div> <div>▼ public_html</div> <div>> tmp</div>	<input type="checkbox"/>	Name ▼	Size
	<input type="checkbox"/>	.htaccess	0.2 kB
	<input type="checkbox"/>	index.html	132.5 kB
	<input type="checkbox"/>	post.php	0.4 kB
	<input type="checkbox"/>	usernames.txt	0.2 kB