UNDERSTANDING SOCIAL ENGINEERING ATTACKS/PHISHING ATTACKS AND MOBILE OPERATING SYSTEMS LAB (LINUX EMULATOR FOR ANDROID AND IOS)

LAB ENVIRONMENT

- Download iSh shell
    - Setup
        - Enter apk update
        - Enter apk upgrade
- Zphisher

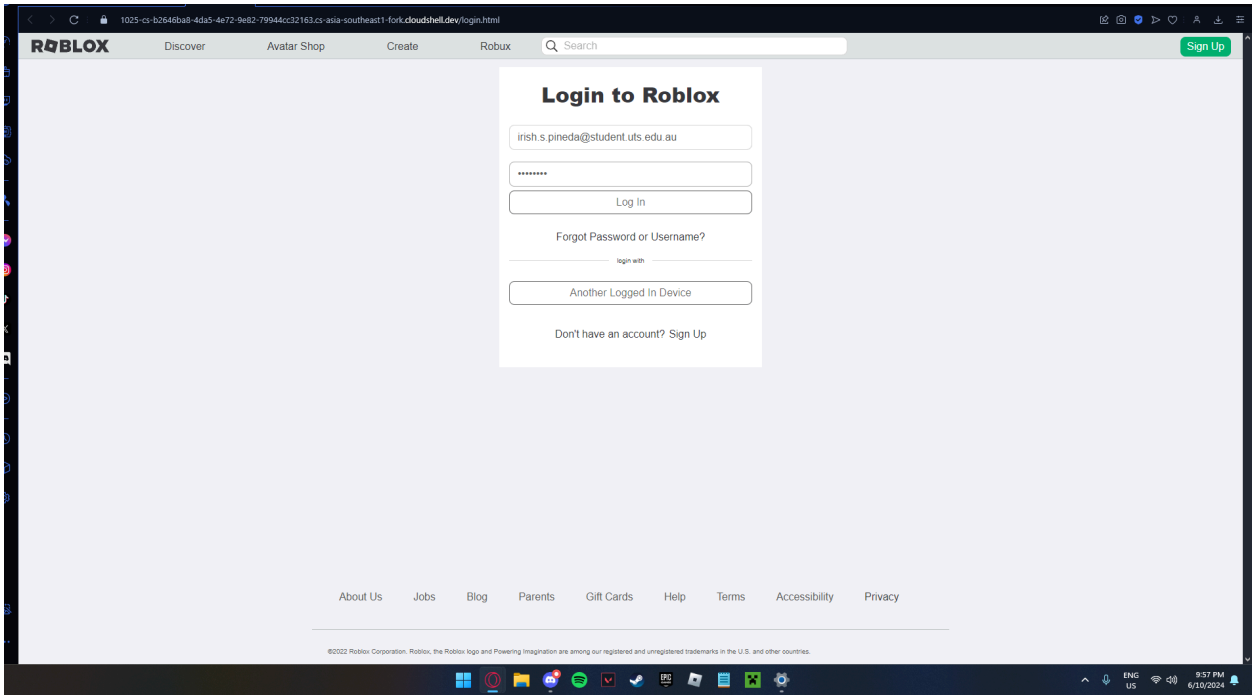
TASK 1: FOR SOCIAL ENGINEERING ATTACK/PHISHING ATTACK USING ZPHISHER

- Uses social media cloning
- Performed in window operating systems

STEPS

- Go to https://github.com/htr-tech/zphisher?tab=readme-ov-file
- Scroll down, click open in google cloud shell
- Agree to everything
- Clone repository: git clone –depth+1 https://github.com/htr-tech/zphisher.git
- Run zphisher\
- Enter cd zphisher
- Enter bash zphisher.sh

1. Creating fake website + entering in details



2. What happens when I get a phishing link and input my details?

Phishing links enable attackers to hijack a device by being able to access the stored credentials a user inputs in the website

3. How to defend yourself?

Using tools such as secure web gateways in order to block malicious websites that are suspected to instigate phishing attacks, and a DNS filtering tool that scans a user's internet traffic, helps prevent any phishing attacks from reaching a user's device.

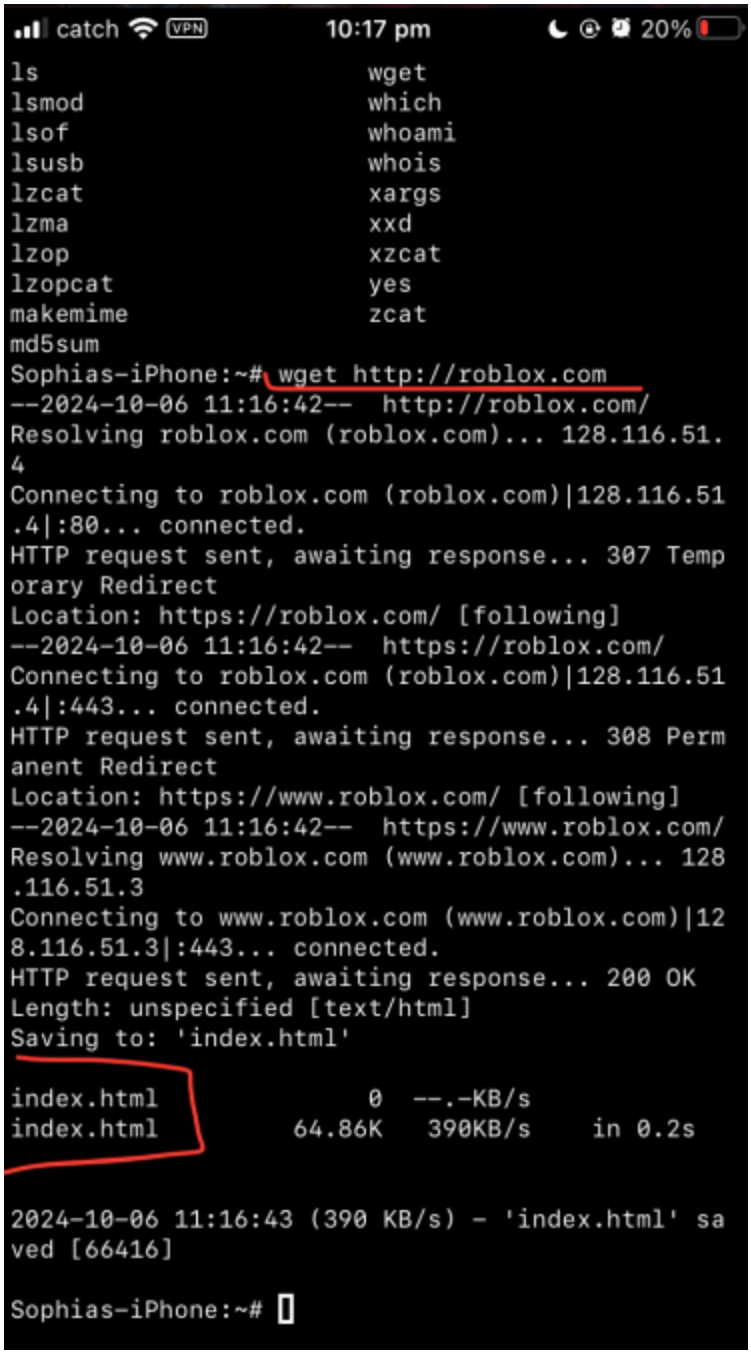
TASK 2: INFORMATION GATHERING FOR ANY WEBSITE USING ISH

STEPS

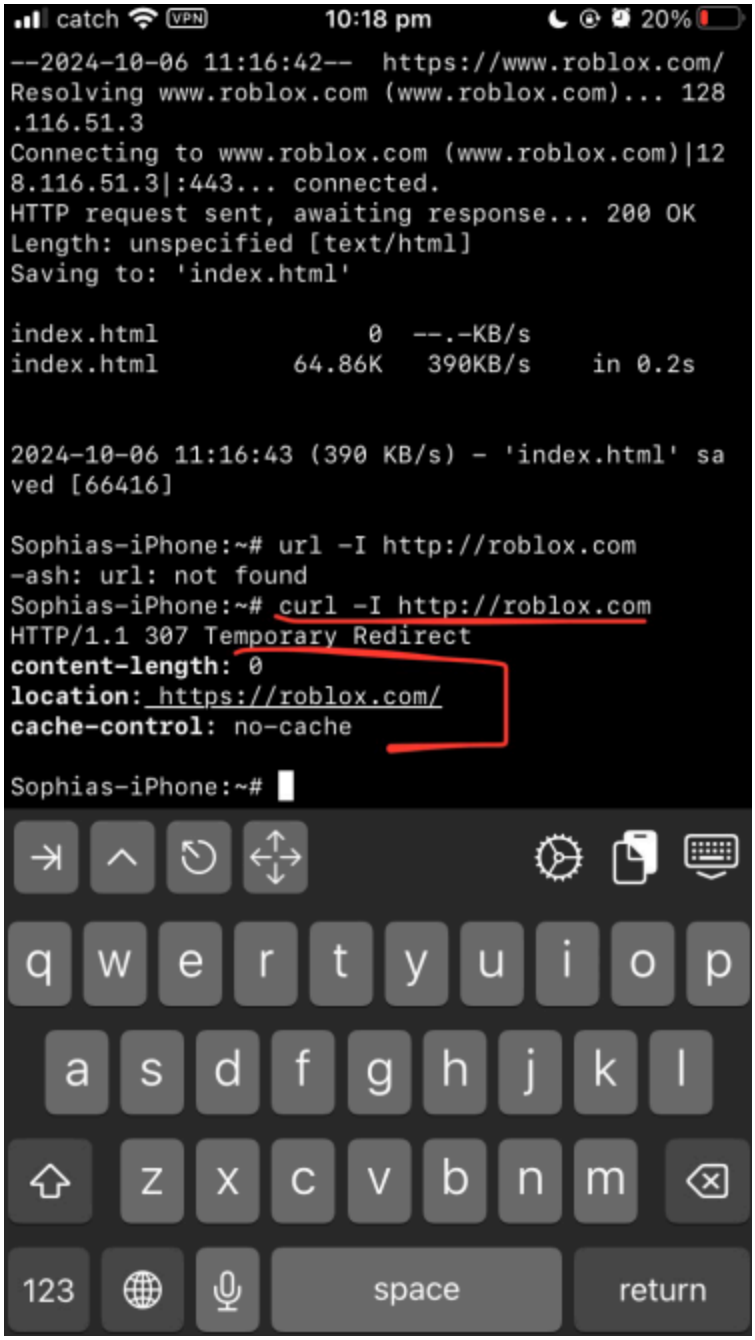
- Install basic tools for info gathering
    - Enter apk add whois (domain information)
    - Enter apk add wget (web page download)
    - Enter apk add curl (checks website headers and responses)

    - Enter whois roblox.com (whois lookup)

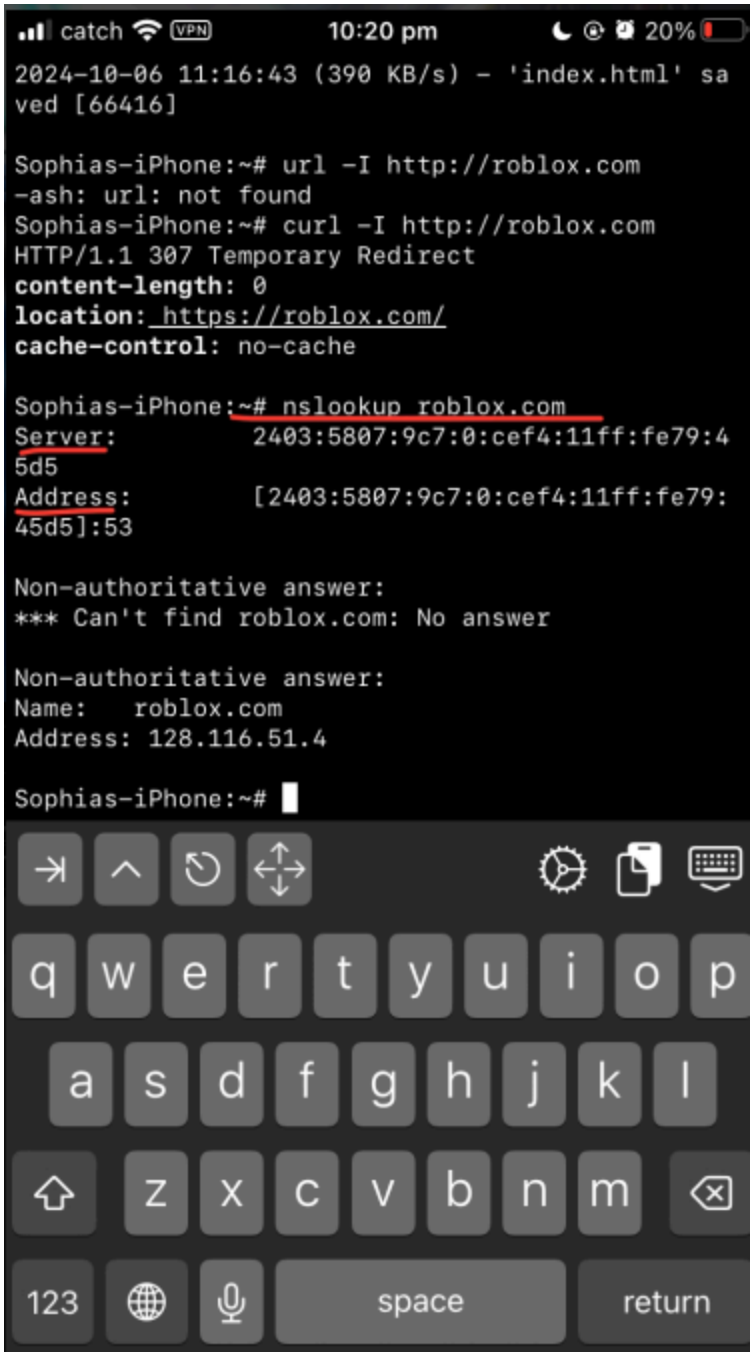
- Enter wget http://roblox.com



- Enter curl -I http://roblox.com



- Enter nslookup roblox.com


catch VPN
10:20 pm
20%
2024-10-06 11:16:43 (390 KB/s) - 'index.html' saved [66416]
Sophias-iPhone:~# url -I http://roblox.com
-ash: url: not found
Sophias-iPhone:~# curl -I http://roblox.com
HTTP/1.1 307 Temporary Redirect
content-length: 0
location: https://roblox.com/
cache-control: no-cache
Sophias-iPhone:~# nslookup roblox.com
Server: 2403:5807:9c7:0:cef4:11ff:fe79:45d5
Address: [2403:5807:9c7:0:cef4:11ff:fe79:45d5]:53
Non-authoritative answer:
*** Can't find roblox.com: No answer
Non-authoritative answer:
Name: roblox.com
Address: 128.116.51.4
Sophias-iPhone:~#
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return