

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

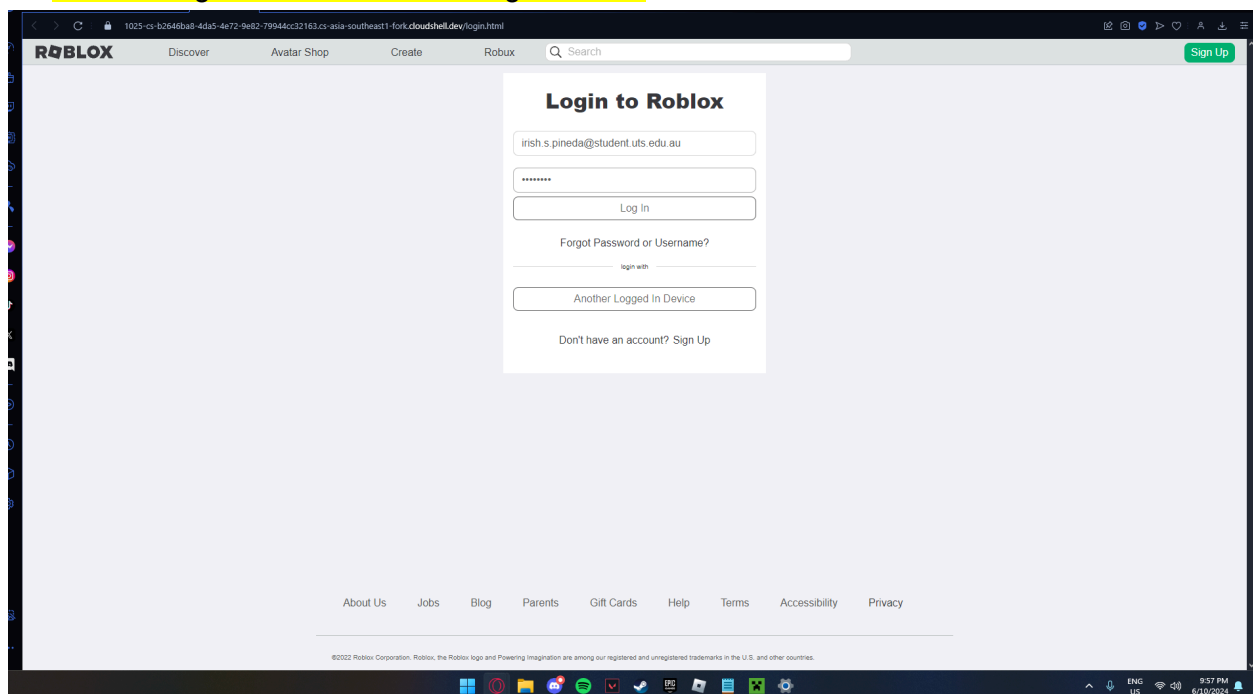
TASK 1: FOR SOCIAL ENGINEERING ATTACK/PHISHING ATTACK USING ZPHISHER

- 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)

catch VPN 10:15 pm 22%

```
Sophias-iPhone:~# whois roblox.com
Domain Name: ROBLOX.COM
Registry Domain ID: 110864800_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-12-29T09:40:58Z
Creation Date: 2004-01-30T00:08:43Z
Registry Expiry Date: 2025-01-30T00:08:43Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: DNS1.P06.NSONE.NET
Name Server: DNS2.P06.NSONE.NET
Name Server: DNS3.P06.NSONE.NET
Name Server: DNS4.P06.NSONE.NET
Name Server: NS01.RBXINFRA.NET
Name Server: NS02.RBXINFRA.NET
Name Server: NS03.RBXINFRA.NET
Name Server: NS04.RBXINFRA.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-06T11:14:36Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

- Enter wget <http://roblox.com>

```

catch 10:17 pm 20%
ls wget
lsmod which
lsof whoami
lsusb whois
lzcat xargs
lzma xxd
lzop xzcat
lzopcat yes
makemime zcat
md5sum
Sophias-iPhone:~# wget http://roblox.com
--2024-10-06 11:16:42-- http://roblox.com/
Resolving roblox.com (roblox.com)... 128.116.51.
4
Connecting to roblox.com (roblox.com)|128.116.51
.4|:80... connected.
HTTP request sent, awaiting response... 307 Temp
orary Redirect
Location: https://roblox.com/ [following]
--2024-10-06 11:16:42-- https://roblox.com/
Connecting to roblox.com (roblox.com)|128.116.51
.4|:443... connected.
HTTP request sent, awaiting response... 308 Perm
anent Redirect
Location: https://www.roblox.com/ [following]
--2024-10-06 11:16:42-- https://www.roblox.com/
Resolving www.roblox.com (www.roblox.com)... 128
.116.51.3
Connecting to www.roblox.com (www.roblox.com)|12
8.116.51.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html      0  --.-KB/s
index.html      64.86K  390KB/s   in 0.2s

2024-10-06 11:16:43 (390 KB/s) - 'index.html' sa
ved [66416]

Sophias-iPhone:~# 

```

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

```
catch VPN 10:18 pm 20%
--2024-10-06 11:16:42-- https://www.roblox.com/
Resolving www.roblox.com (www.roblox.com)... 128
.116.51.3
Connecting to www.roblox.com (www.roblox.com)|12
8.116.51.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html      0  --.-KB/s
index.html      64.86K  390KB/s   in 0.2s

2024-10-06 11:16:43 (390 KB/s) - 'index.html' sa
ved [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:~#
```

- 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:~#
```

