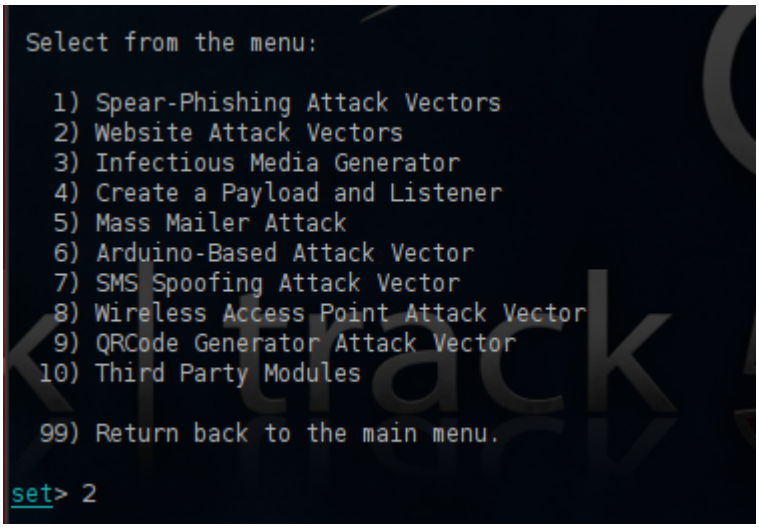
QRCode Attack Vector

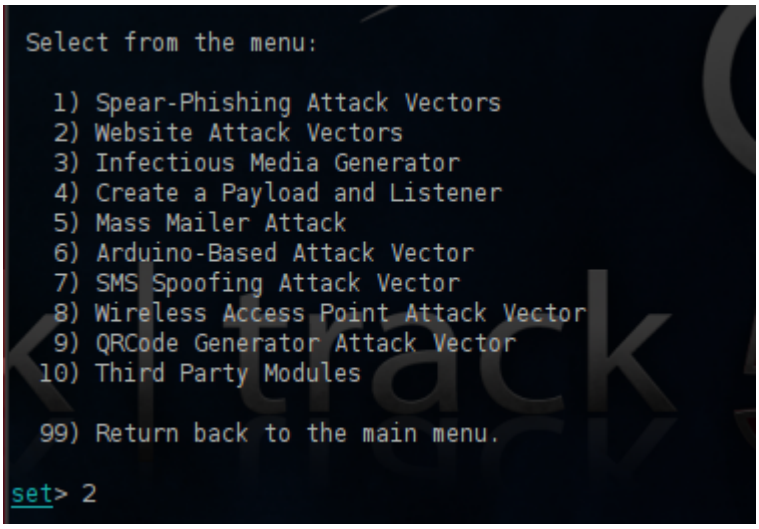
pentestlab.blog/category/social-engineering/page/5

April 17, 2012



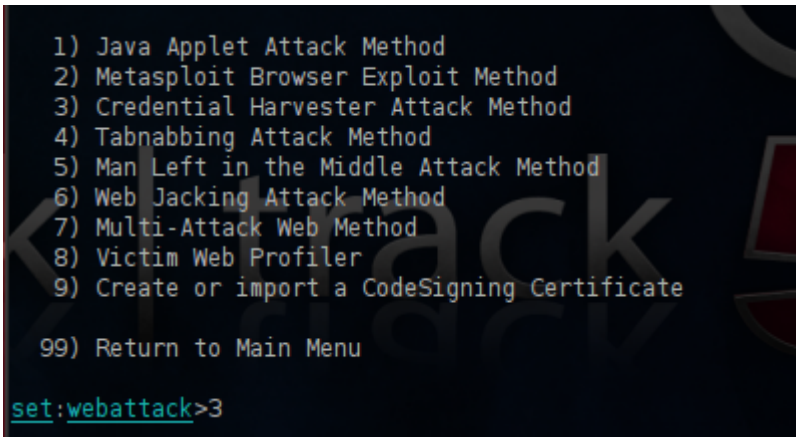
In nowadays QR codes are almost everywhere.You can see them in every product,in concert tickets even in advertisements on the streets.The main purpose of these QR Codes is to be used for marketing purposes or for people who would like to know more information about a specific product or service.However 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 unsuspicious 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**.



Selecting the Website Attack Vector

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

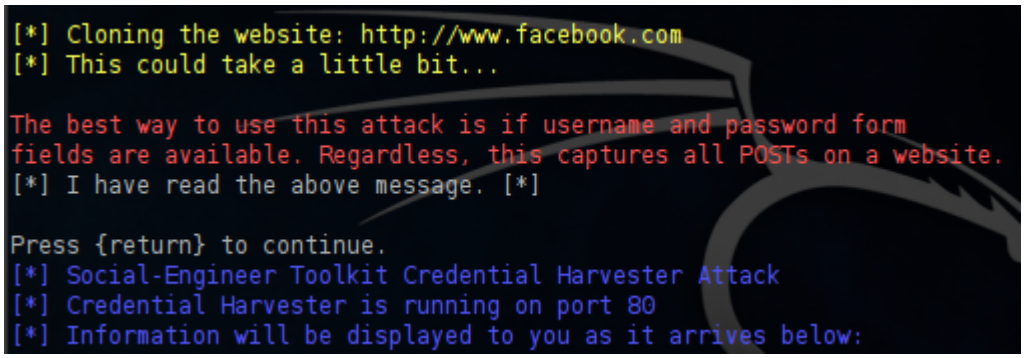


Choosing the Credential Harvester Attack

We will select from the existing templates to clone Facebook.

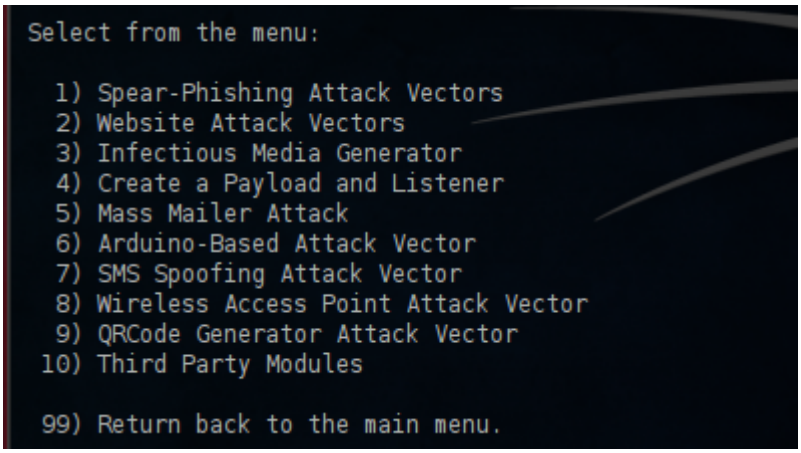
Select from the existing templates Facebook

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



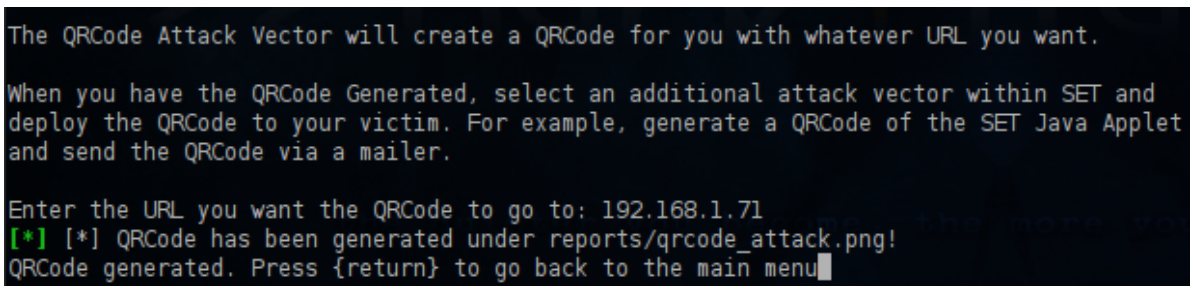
Cloning Facebook

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**.



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.

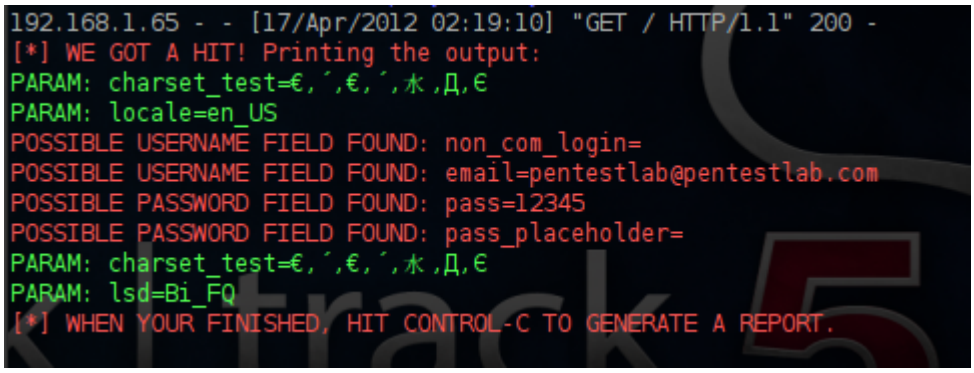


Inserting the malicious link

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 unsuspicious 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 mobiles phones they will redirected to the fake website which in our case is Facebook.If they put their credentials then it will appear to your system.



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 unsuspicious 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.