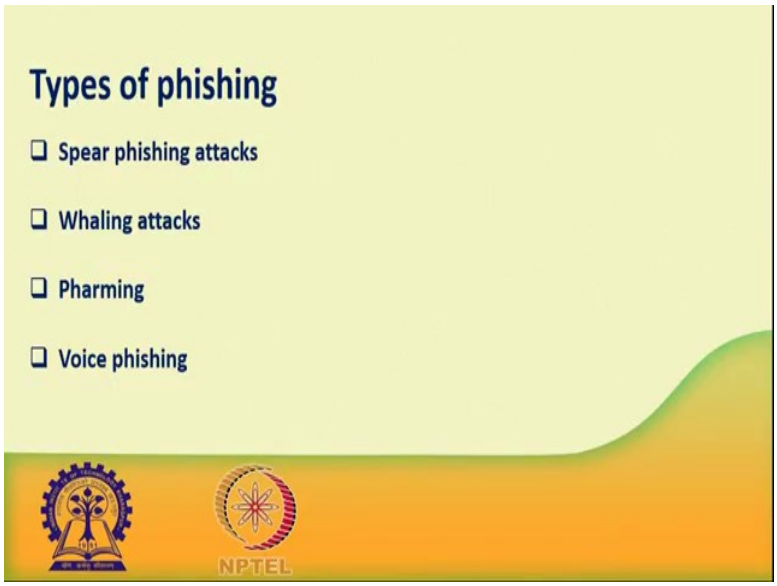
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

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.

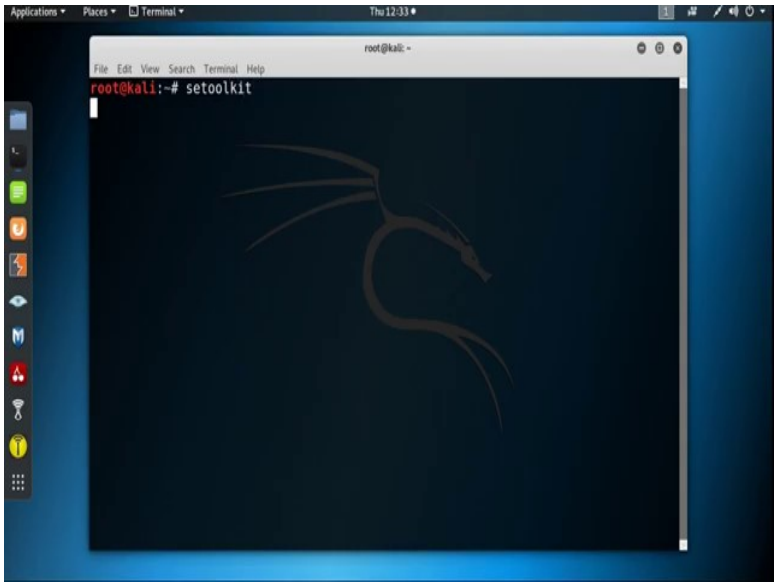
A typical phishing scam uses speech synthesis software to live voicemails to notify the victim of suspicious activity in a bank or credit account and solicits the victim to respond to a malicious phone number to verify his identity. Thus compromising the victims account credential. Now, I am discussing 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, kink 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)

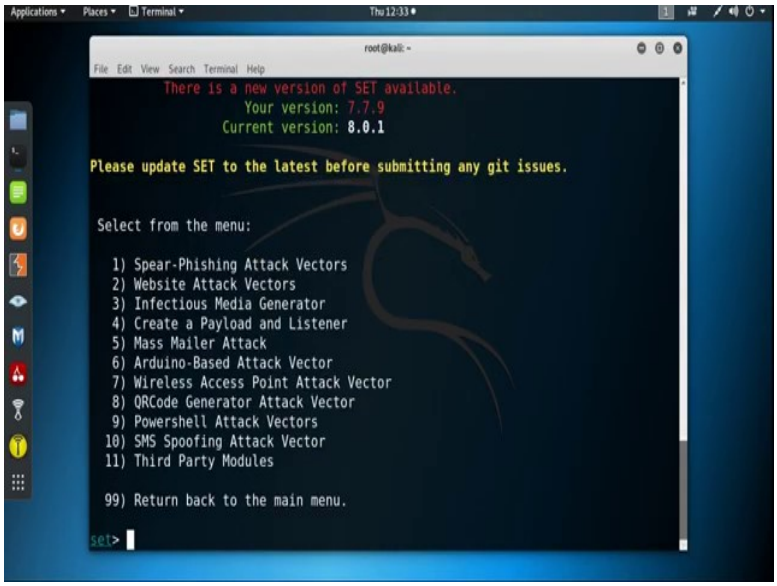
Now, I will show you how to perform phishing attack using social engineering toolkit.

(Refer Slide Time: 05:35)



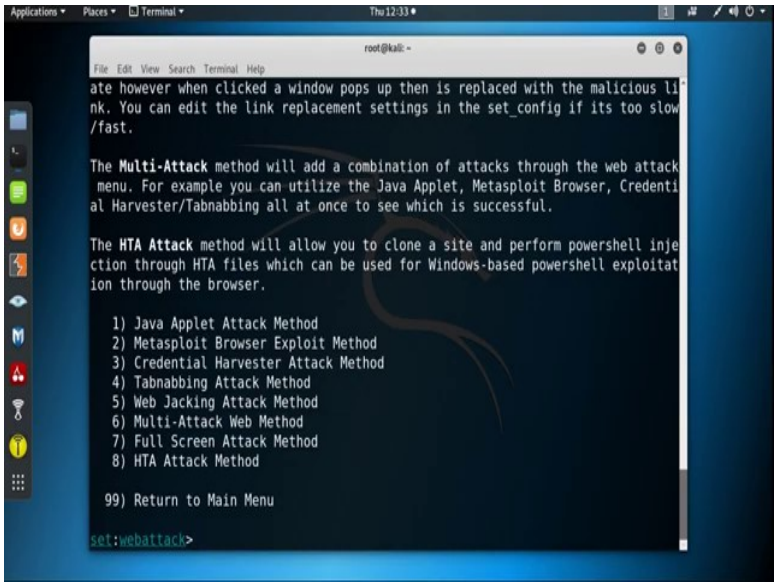
Now, open terminal and go to the social engineering tool by typing $setoolkit$.

(Refer Slide Time: 05:47)



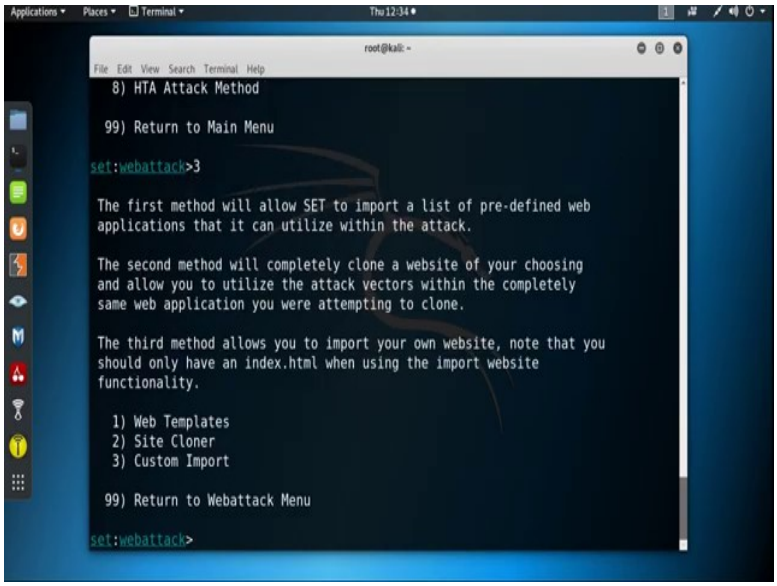
Now, go to the option one social engineering attacks.

(Refer Slide Time: 06:00)



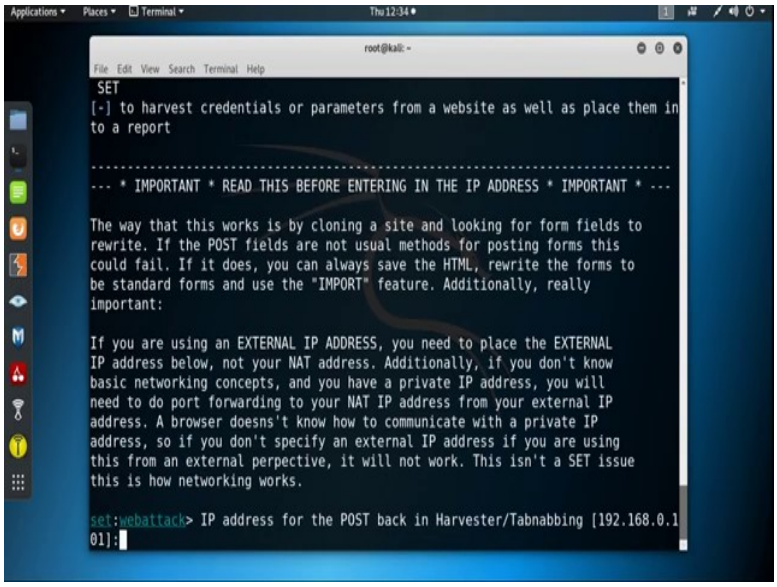
Then go to option 2 website attack vector.

(Refer Slide Time: 06:07)



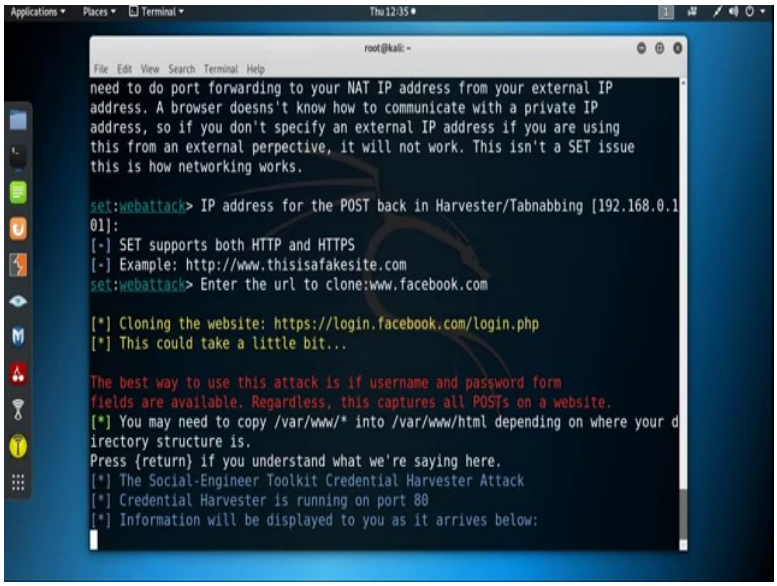
Now, go to option 3, credential harvester attack method.

(Refer Slide Time: 06:12)



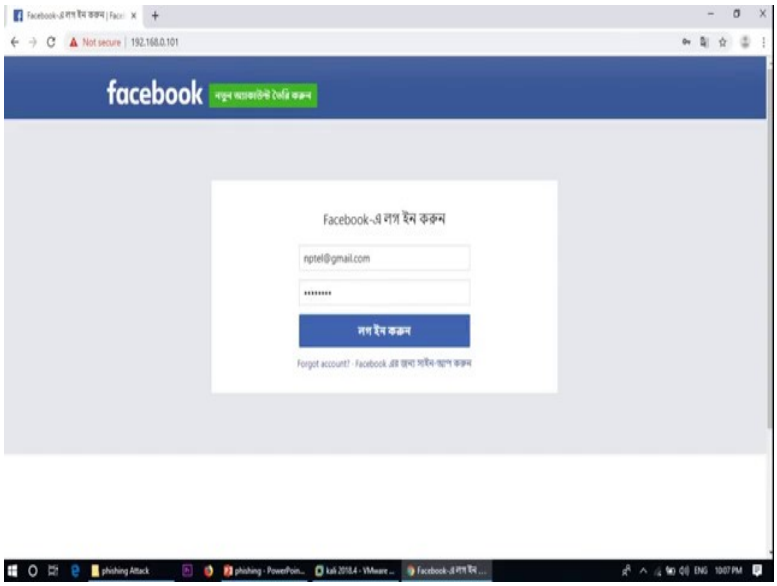
And now go to option 2, site cloner. So, *IP address for the POST back in harvester/tabnabbing* [192.168.0.101]. So, basically I am going to host my phishing page and that particular IP address which is my IP address.

(Refer Slide Time: 06:37)



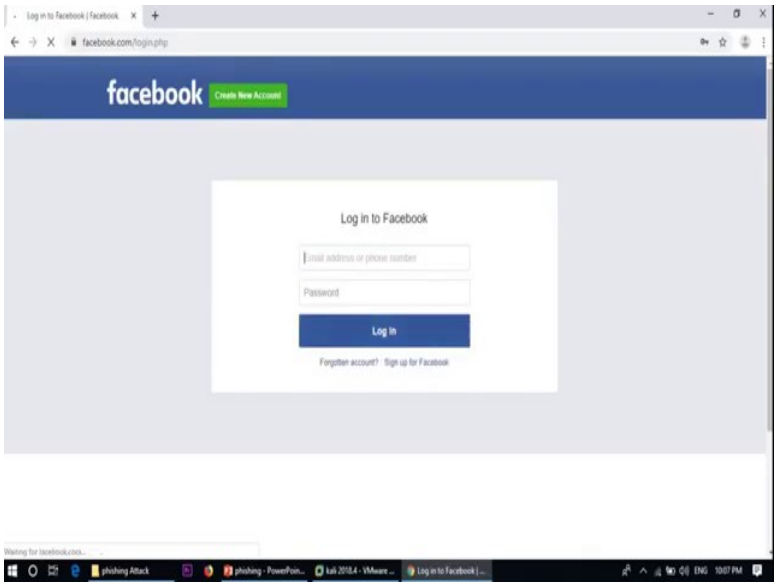
Now, enter the URL to clone. Now, I am going to put the URL $www.facebook.com$. So, I am going to create a phishing page of $facebook.com$, ok. So, information will be displayed to you as it arrives below. Now, send your URL, hosted URL to the victim machine by using some other kind of social engineering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

(Refer Slide Time: 07:31)



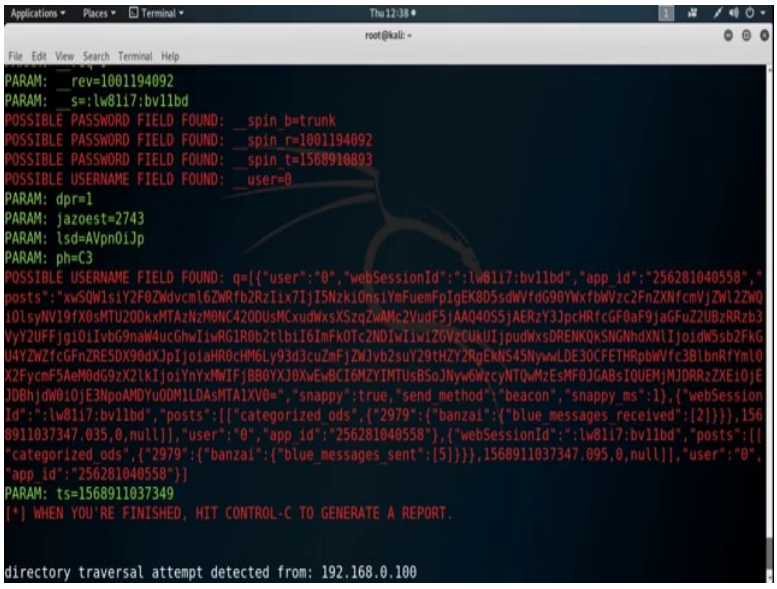
Now, victim open the phishing page in his or her machine. 192.168.0.101; so, it asking for the email and password, password.

(Refer Slide Time: 08:26)

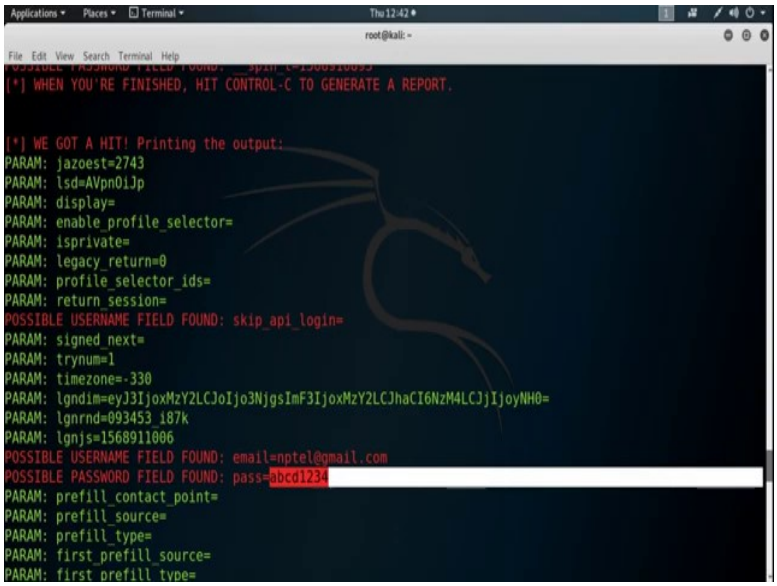


Now, try to login. Now, it will redirect to the actual login page of Facebook, and at the same time the credential already go at the attacker site. Now, check from the attacker machine.

(Refer Slide Time: 08:47)



(Refer Slide Time: 09:05)



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.