CNS Project Report
Mass Mailer Attack
(Using email harvesting)

SUBMITTED BY:
TWINKAL PARMAR 2016UCP1700 B(3,4)
BHAWANA SANKHLA 2016UCP1457 B(1,2)
SHUBHAM ARORA 2016UCP1399 A(3,4)

0.1 Understanding the mass mailer attack

Mass Mailer attack is a type of social engineering attack. Large number of spam mails are sent to different harvested e-mail addresses usually containing malicious links/scripts. The attack is also used to send a large number of spam e-mails to a single e-mail address possibly trying to crash the inbox. Even if the attack doesnt crash the inbox service of a user it does fill the inbox of a user to an extent that it is difficult for him/her to access important emails. It is also called E-Bombing or SMS Attack. The mass mailer attack has two variations, which are given as follows:

1. E-mail attack on a single e-mail address.
2. E-mail attack using a mass mailer.

A mass mailer is commonly used to send a phishing page link to the e-mail ID of the target. The attacker needs to be aware of the e-mail harvester technique to be efficient in this attack.A mass mailer is also used to perform a Distributed Denial of Service (DDoS) attack through the creation of zombie "bots" and by controlling the bots through the control center.

0.2 Email harvesting

Email harvesting is the process of obtaining a large number of email addresses through various methods. The purpose of harvesting email addresses is for use in bulk emailing or for spamming.

The most common method of email harvesting is by using specialized harvesting software known as harvesting bots, or harvesters.

0.3 Example

Suppose an important email is come into your device but you dont know about that but another person who is a hacker know about that. He can send large amount of spam emails in your inbox. When you open the inbox if the email server is not good first of all your inbox is crashed. If the email server is good. You can see the inbox there are thousands of emails in it. You can read only some emails but you dont read the important email because first of all you dont know about that and the second is that the spam emails are in such a large amount that the important email is hide between them.

0.4 Prerequisites

- MSF CONSOLE
- SE-TOOLKIT
- METASPLOIT FRAMEWORK
- EMAIL COLLECTOR
- PLATFORM : KALI LINUX

0.5 Steps Involved

Step 1: Harvesting e-mail addresses

Commands for e-mail harvesting in KALI linux are:-

- msfconsole
- search collector
- use gather/search email collector
- set DOMAIN mnit.ac.in
- set OUTFILE emailList
- show options
- exploit

Step 2: Get the list

First, we have to get the victim's email lists, so the program knows which to send.

Step 3: Opening the program

Now, we have to open the SE toolkit. SE toolkit is pre-installed in your kali linux, so you don't have to download it. To execute the program, type :

setoolkit

In the terminal. You should see it at the left of the screen in kali linux.Now, lots of thing should have appeared. Like this :

Step 4: Select Social Engineering Attack

Now, type "1" in the terminal, because we want to do a Social-engineering Attack. (Don't forget to enter!)

Step 5: Select Mass Mailer Attack

After you select option 1, type "5" in the terminal, which will say mass mailer attack.

Step 6: Select the type of attack

Select "1" to attack a single person or "2" to attack multiple users. Hit Enter.

Step 7: Specfying the path of harvested list of emails and spamming them

Enter "

Type the name that the victim will see, then type the password of the email since the program has to use that password to login your account and send emails.

Type "no" in the terminal because we don't want to send as high-priority.

After you decide the name of the email and whether you are going to attach a file, then in the html or plain thingy, choose plain by typing : p

Now, type the email and if you finished, type "END" on a new line and press enter. Then the script will send the emails.