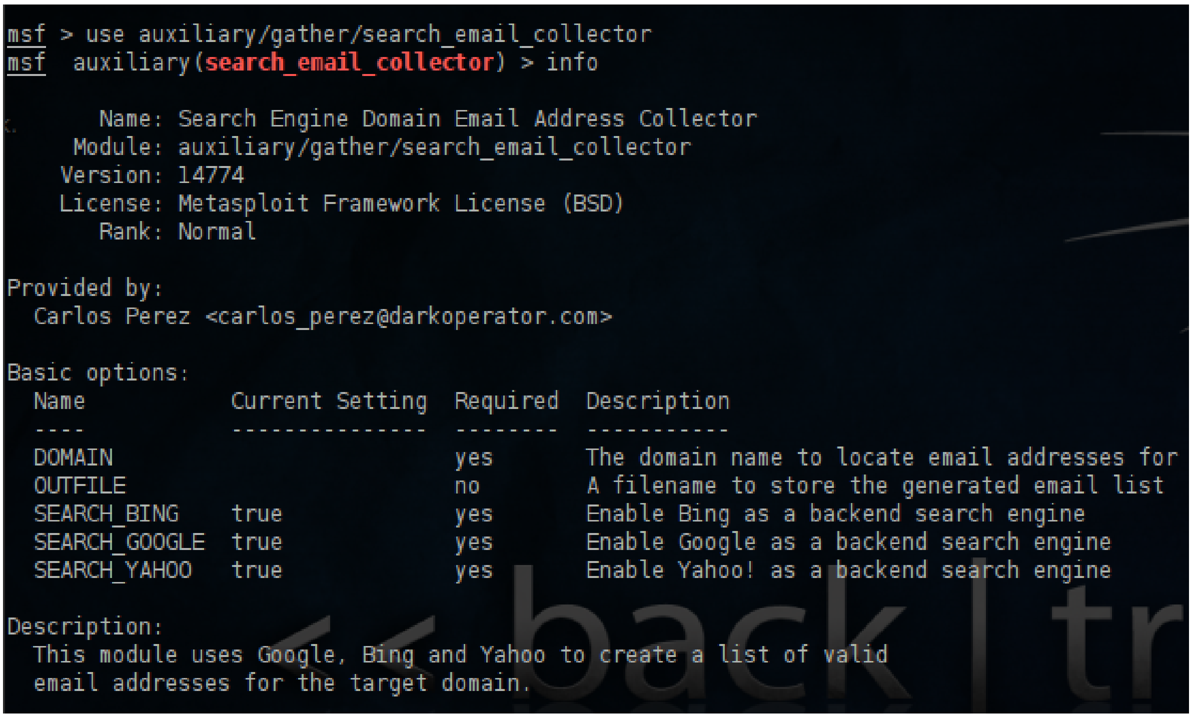
Building Profiles for a Social Engineering Attack

April 19, 2012

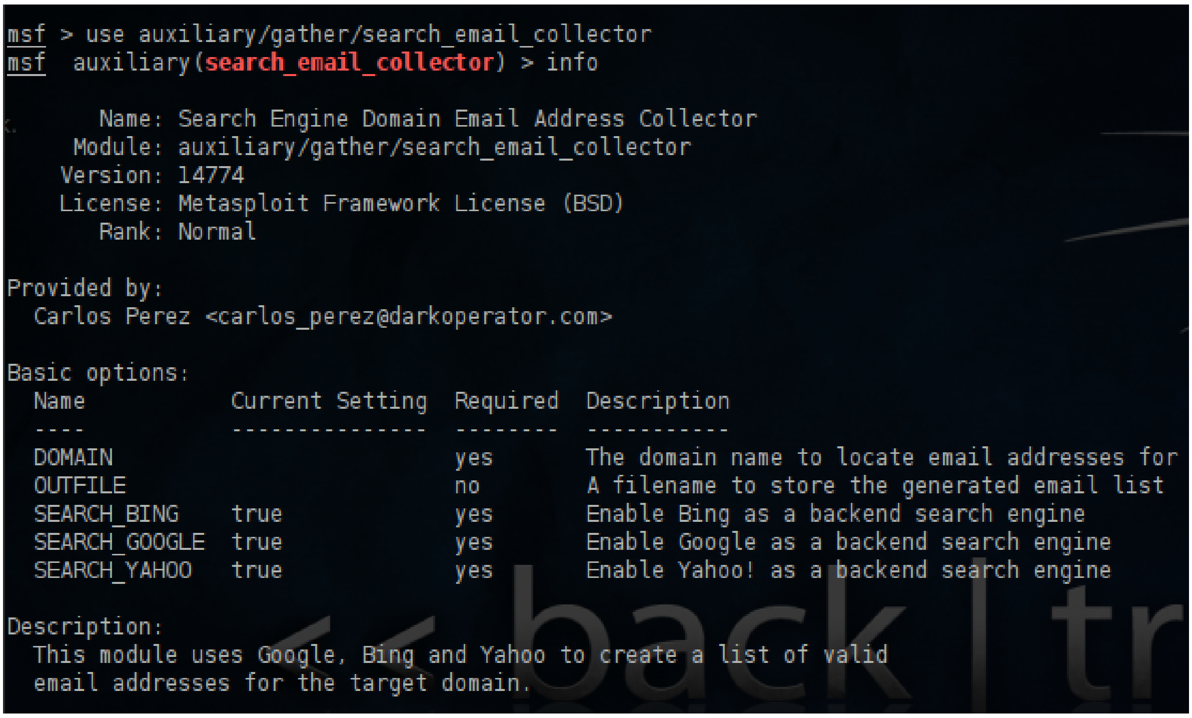


```
msf > use auxiliary/gather/search_email_collector
msf  auxiliary(search_email_collector) > info

       Name: Search Engine Domain Email Address Collector
     Module: auxiliary/gather/search_email_collector
    Version: 14774
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  DOMAIN                          yes       The domain name to locate email addresses for
  OUTFILE                         no        A filename to store the generated email list
  SEARCH_BING    true             yes       Enable Bing as a backend search engine
  SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
  SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

Description:
  This module uses Google, Bing and Yahoo to create a list of valid
  email addresses for the target domain.
```

The key to a successful social engineering engagement is trust.If you are able to win the trust of someone else easily then you can obtain any information you want.Also people are suspicious when they don’t know someone and they are not so open when you are going to ask for something about them or their company.However if you have done your research and you are giving them information that have valid grounds then you might be able to convince them and win their trust faster.In this article we will see how we can create a profile for someone who we don’t know.

Let’s say that our client is the MIT(Massachusetts Institute of Technology) and we don’t have any information about them.As a first step is to discover email addresses and profiles that exist on social media networks.We have two options in this step.We can use either the tool **theHarvester** or we can use the metasploit module called **search_email_collector**.

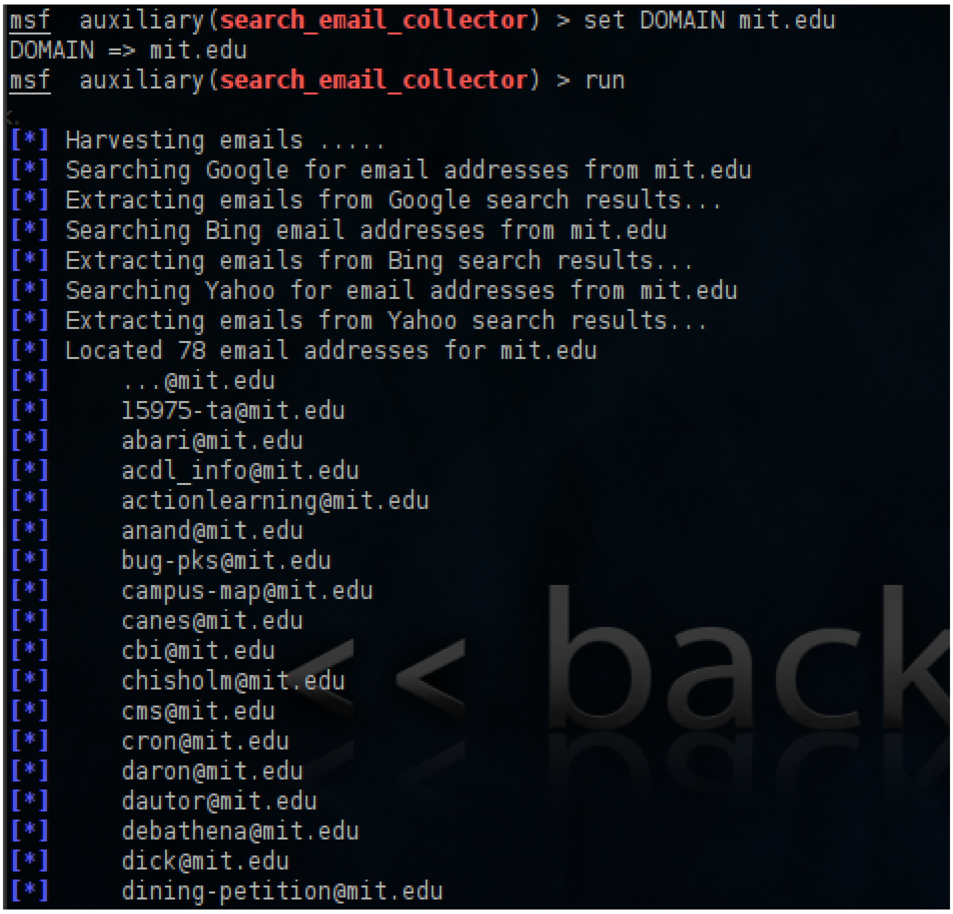
The use of the email collector module of the metasploit framework is pretty simple.We just need to set the domain of our target and it will automatically search through Bing,Yahoo and Google for valid email addresses.



```
msf > use auxiliary/gather/search_email_collector
msf  auxiliary(search_email_collector) > info

       Name: Search Engine Domain Email Address Collector
     Module: auxiliary/gather/search_email_collector
    Version: 14774
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  DOMAIN                          yes       The domain name to locate email addresses for
  OUTFILE                         no        A filename to store the generated email list
  SEARCH_BING    true             yes       Enable Bing as a backend search engine
  SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
  SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

Description:
  This module uses Google, Bing and Yahoo to create a list of valid
  email addresses for the target domain.
```

Metasploit Email Collector Description

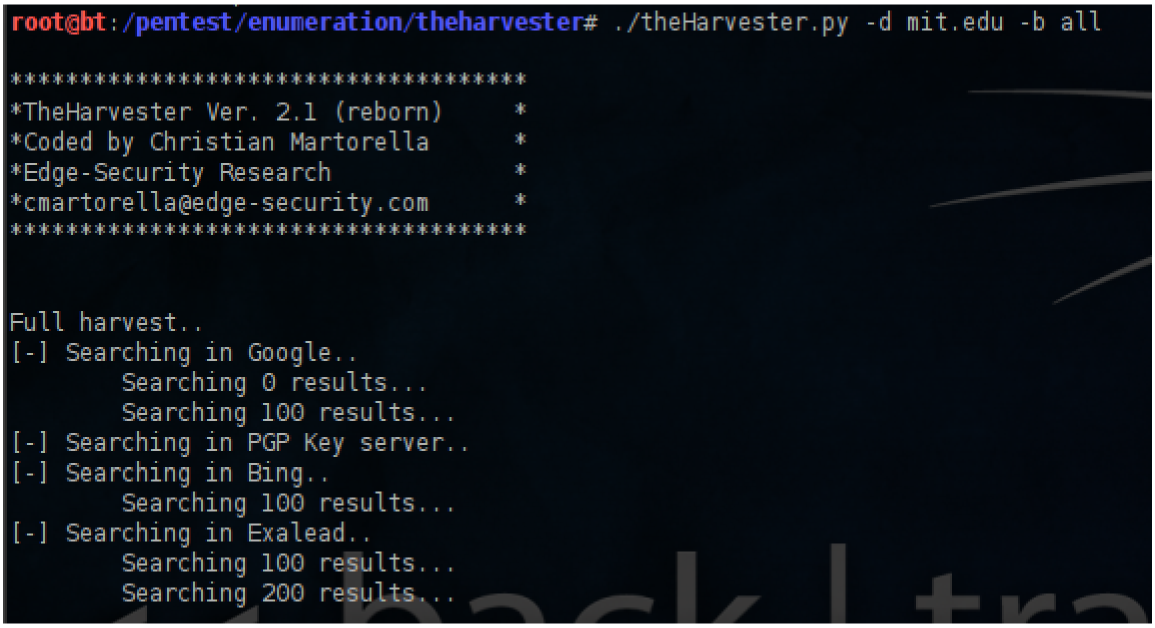
Our target in this case is the MIT so the domain that we want to set is the mit.edu.Below is a sample of our results.



```
msf  auxiliary(search_email_collector) > set DOMAIN mit.edu
DOMAIN => mit.edu
msf  auxiliary(search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from mit.edu
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from mit.edu
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from mit.edu
[*] Extracting emails from Yahoo search results...
[*] Located 78 email addresses for mit.edu
[*]     ...@mit.edu
[*]     15975-ta@mit.edu
[*]     abari@mit.edu
[*]     acdl_info@mit.edu
[*]     actionlearning@mit.edu
[*]     anand@mit.edu
[*]     bug-pks@mit.edu
[*]     campus-map@mit.edu
[*]     canes@mit.edu
[*]     cbi@mit.edu
[*]     chisholm@mit.edu
[*]     cms@mit.edu
[*]     cron@mit.edu
[*]     daron@mit.edu
[*]     dautor@mit.edu
[*]     debathena@mit.edu
[*]     dick@mit.edu
[*]     dining-petition@mit.edu
```

Discovery of valid mit.edu email addresses

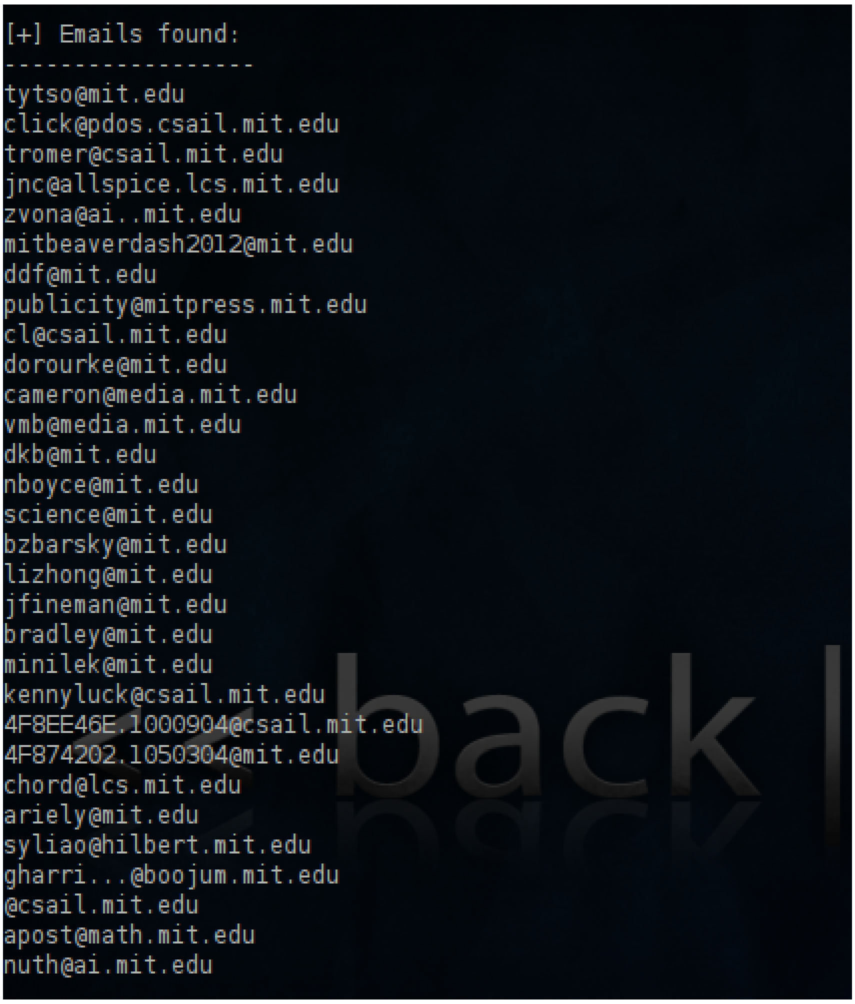
From the other hand the tool theHarvester is providing us with more options.So except of the fact that we can scan for email addresses,we can scan also for profiles in social media like Google+ and Linkedin.In the next image you can see the command that we have executed in the tool.



```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d mit.edu -b all

*************************************
*TheHarvester Ver. 2.1 (reborn)     *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 100 results...
[-] Searching in Exalead..
        Searching 100 results...
        Searching 200 results...
```

Using theHarvester

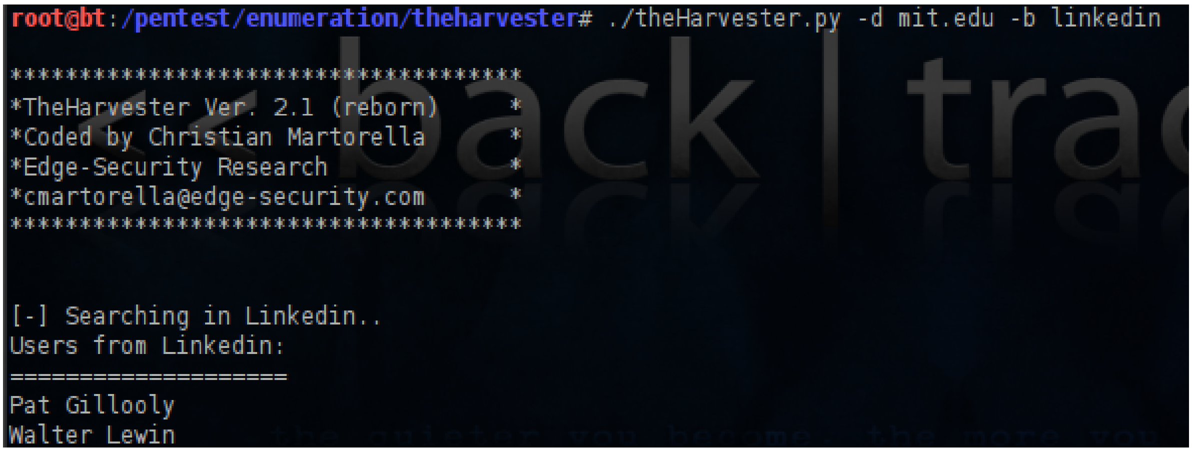
Below is a sample of the email addresses that the tool theHarvester has discovered.Of course we can combine the results with the module of the metasploit if we wish.



```
[+] Emails found:
------------------
tytso@mit.edu
click@pdos.csail.mit.edu
tromer@csail.mit.edu
jnc@allspice.lcs.mit.edu
zvona@ai..mit.edu
mitbeaverdash2012@mit.edu
ddf@mit.edu
publicity@mitpress.mit.edu
cl@csail.mit.edu
dorourke@mit.edu
cameron@media.mit.edu
vmb@media.mit.edu
dkb@mit.edu
nboyce@mit.edu
science@mit.edu
bzbarsky@mit.edu
lizhong@mit.edu
jfineman@mit.edu
bradley@mit.edu
minilek@mit.edu
kennyluck@csail.mit.edu
4F8EE46E.1000904@csail.mit.edu
4F874202.1050304@mit.edu
chord@lcs.mit.edu
ariely@mit.edu
syliao@hilbert.mit.edu
gharri...@boojum.mit.edu
@csail.mit.edu
apost@math.mit.edu
nuth@ai.mit.edu
```

theHarvester - email addresses output

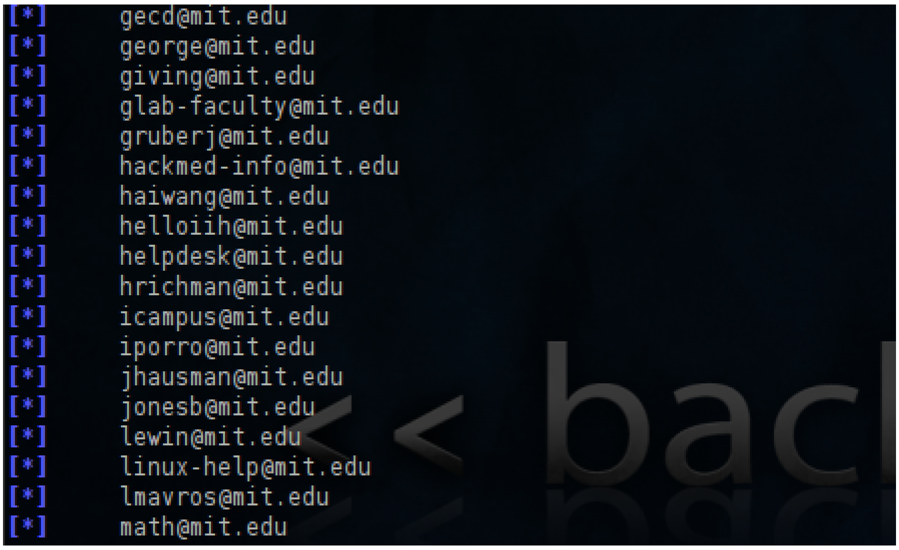
We can try also to scan for profiles related to the mit.edu into professional social networks like Linkedin.We have discovered 2 profiles.



```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d mit.edu -b linkedin

*************************************
*TheHarvester Ver. 2.1 (reborn)     *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


[-] Searching in Linkedin..
Users from Linkedin:
====================
Pat Gillooly
Walter Lewin
```

Discover profiles on the Linkedin

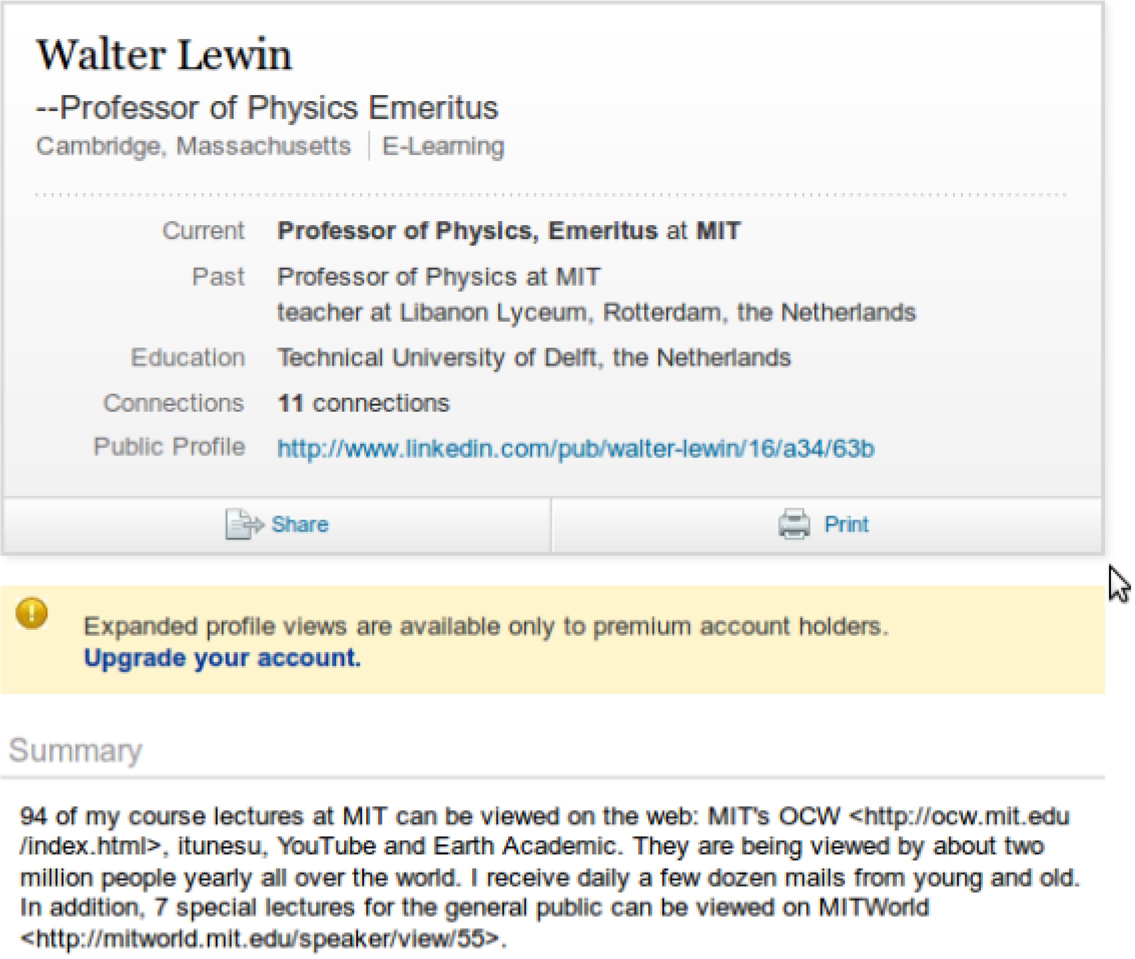
So we have a lot of email addresses and two names.Comparing the results with the metasploit module email collector we have identify that there is an email address that is probably corresponds to the Walter Lewin profile.The email address is **lewin@mit.edu** and you can see it in the results below.



```
[*]     gecd@mit.edu
[*]     george@mit.edu
[*]     giving@mit.edu
[*]     glab-faculty@mit.edu
[*]     gruberj@mit.edu
[*]     hackmed-info@mit.edu
[*]     haiwang@mit.edu
[*]     helloiih@mit.edu
[*]     helpdesk@mit.edu
[*]     hrichman@mit.edu
[*]     icampus@mit.edu
[*]     iporro@mit.edu
[*]     jhausman@mit.edu
[*]     jonesb@mit.edu
[*]     lewin@mit.edu
[*]     linux-help@mit.edu
[*]     lmavros@mit.edu
[*]     math@mit.edu
```

Email addresses output from Metasploit module

Now that we have a name and an email address it is much more easier to search the web in order to collect as much information as possible about this particular person.For example we can start by checking his Linkedin profile.



Walter Lewin

--Professor of Physics Emeritus

Cambridge, Massachusetts | E-Learning

Current	**Professor of Physics, Emeritus** at **MIT**
Past	Professor of Physics at MIT teacher at Libanon Lyceum, Rotterdam, the Netherlands
Education	Technical University of Delft, the Netherlands
Connections	**11** connections
Public Profile	http://www.linkedin.com/pub/walter-lewin/16/a34/63b

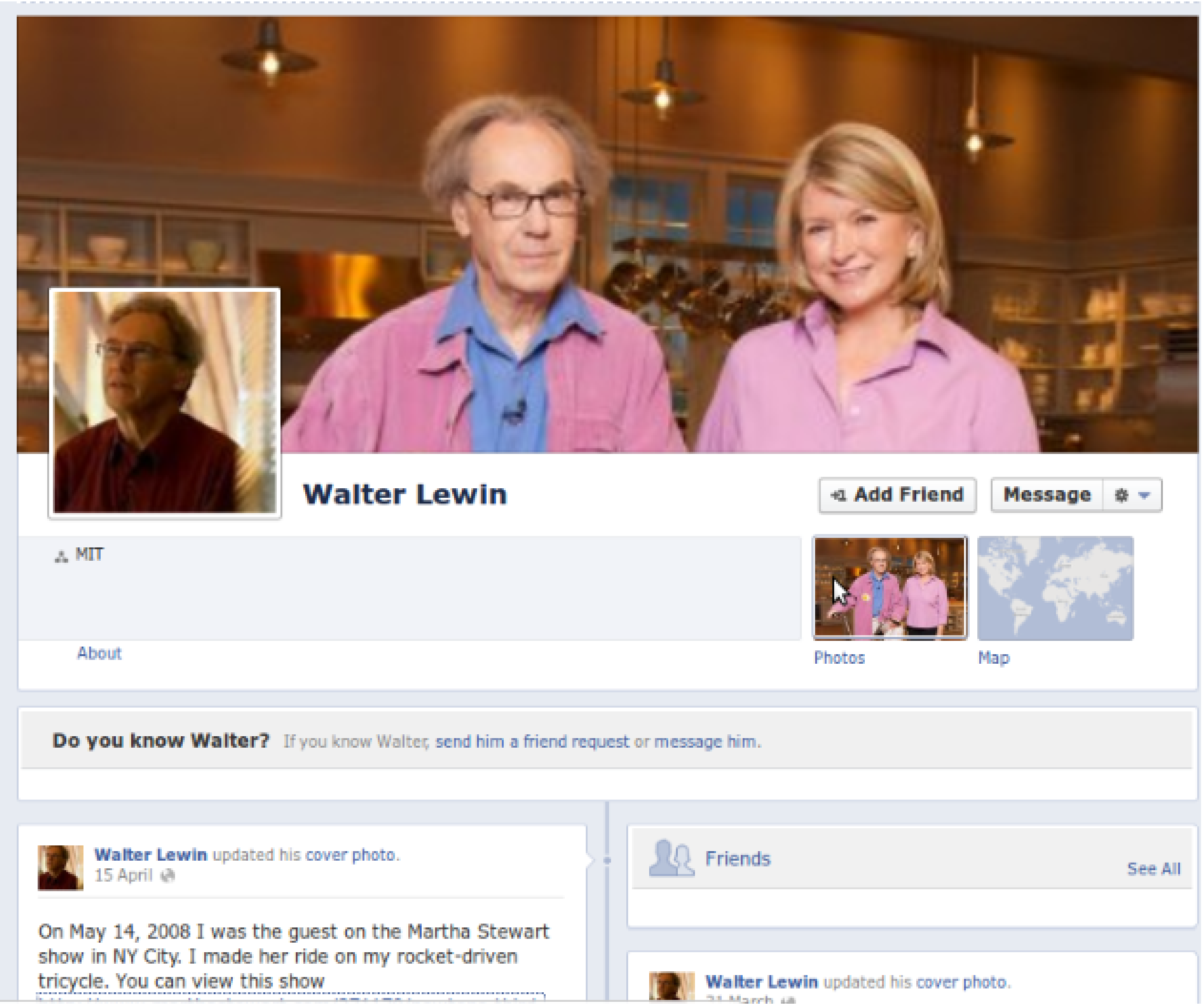
Expanded profile views are available only to premium account holders. **Upgrade your account.**

Summary

94 of my course lectures at MIT can be viewed on the web: MIT's OCW <http://ocw.mit.edu/index.html>, itunesu, YouTube and Earth Academic. They are being viewed by about two million people yearly all over the world. I receive daily a few dozen mails from young and old. In addition, 7 special lectures for the general public can be viewed on MITWorld <http://mitworld.mit.edu/speaker/view/55>.

Linkedin Profile

We can use the email address **lewin@mit.edu** to discover his Facebook profile.



Walter Lewin

Add Friend

Message

MIT

About

Photos

Map

Do you know Walter? If you know Walter, send him a friend request or message him.

Walter Lewin updated his cover photo.
15 April

On May 14, 2008 I was the guest on the Martha Stewart show in NY City. I made her ride on my rocket-driven tricycle. You can view this show

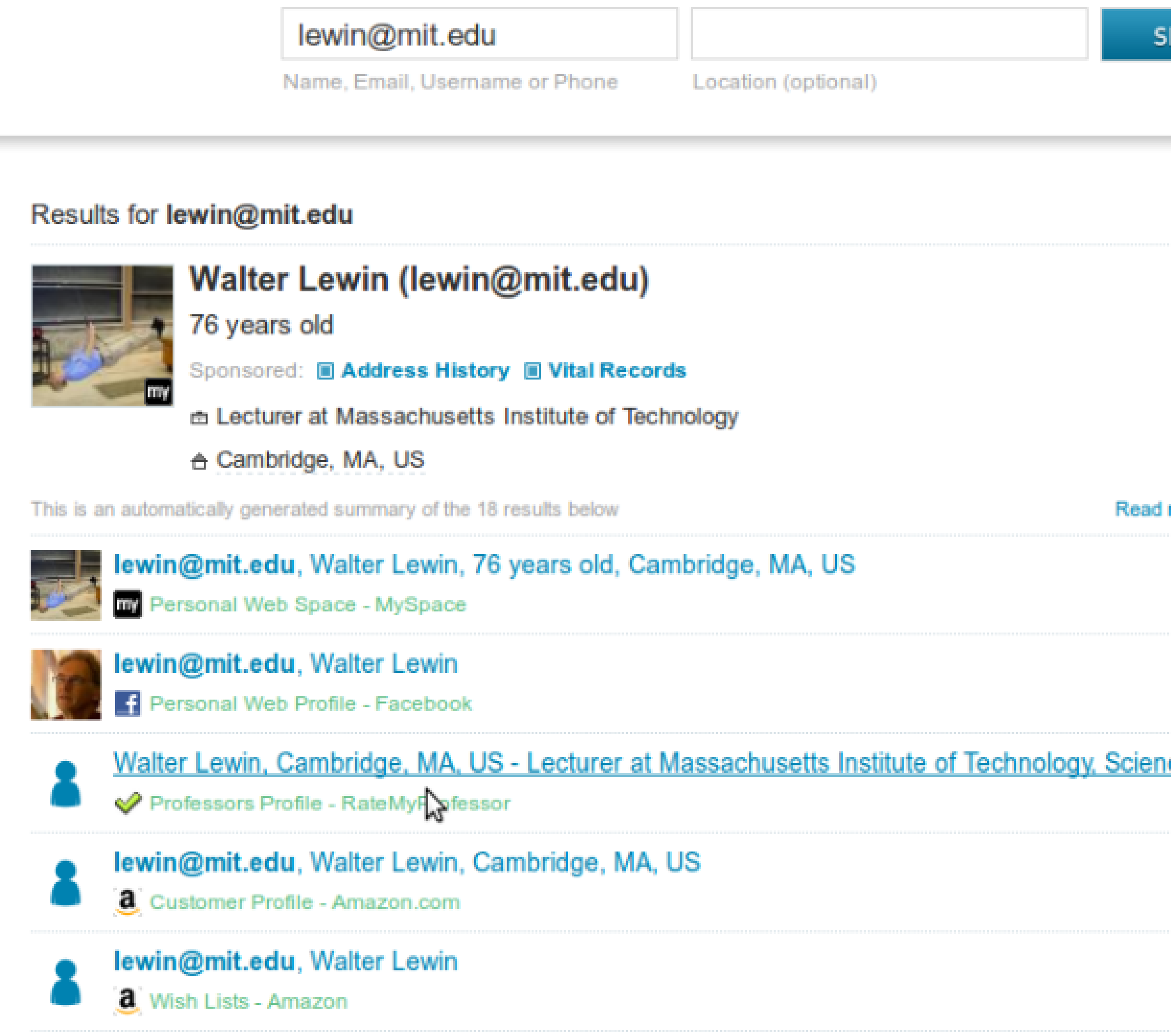
Friends

See All

Walter Lewin updated his cover photo.

Facebook Profile

The information that we can retrieve without being friends on Facebook with is limited.However if we impersonate ourselves as a teacher of MIT we can send a friend request and we might be able to convince him with this way to add us to his friend list so we can have access to much more personal information.Another good tool for obtaining information is through the website pipl.com.



lewin@mit.edu

Name, Email, Username or Phone

Location (optional)

Results for **lewin@mit.edu**

Walter Lewin (lewin@mit.edu)

76 years old

Sponsored: Address History Vital Records

Lecturer at Massachusetts Institute of Technology

Cambridge, MA, US

This is an automatically generated summary of the 18 results below

Read

lewin@mit.edu, Walter Lewin, 76 years old, Cambridge, MA, US
Personal Web Space - MySpace

lewin@mit.edu, Walter Lewin
Personal Web Profile - Facebook

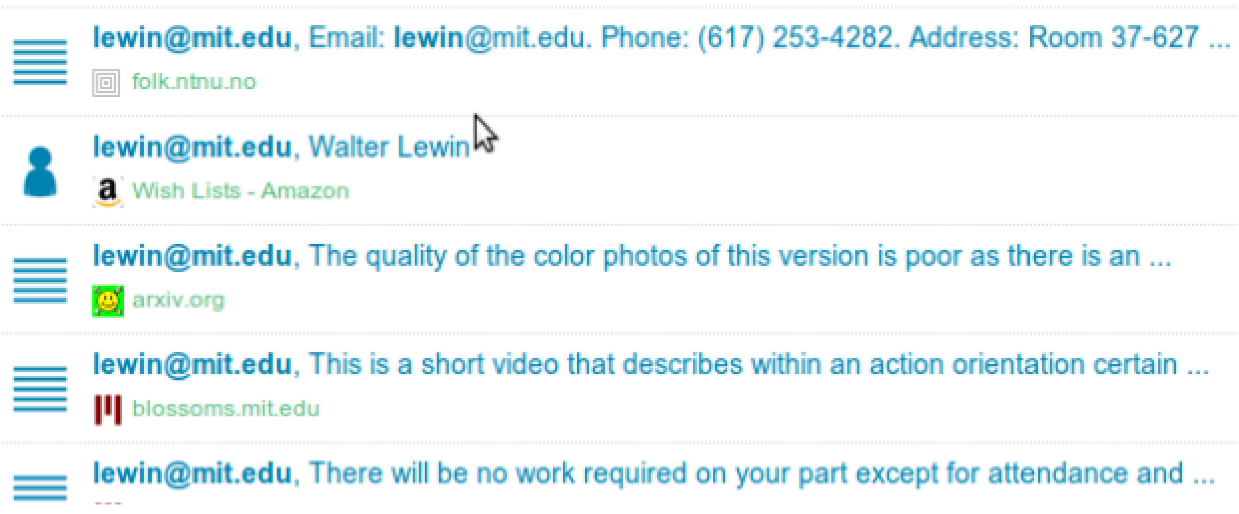
Walter Lewin, Cambridge, MA, US - Lecturer at Massachusetts Institute of Technology, Scien
Professors Profile - RateMyProfessor

lewin@mit.edu, Walter Lewin, Cambridge, MA, US
Customer Profile - Amazon.com

lewin@mit.edu, Walter Lewin
Wish Lists - Amazon

Information gathering on Pipl

As you can see we have discovered information about the age,the job,the personal web space,his Amazon wish list and a website that contains the profile about this professor.Also from the same search we have manage to find his work phone number and his office room.



lewin@mit.edu, Email: **lewin**@mit.edu. Phone: (617) 253-4282. Address: Room 37-627 ...
folk.ntnu.no

lewin@mit.edu, Walter Lewin
Wish Lists - Amazon

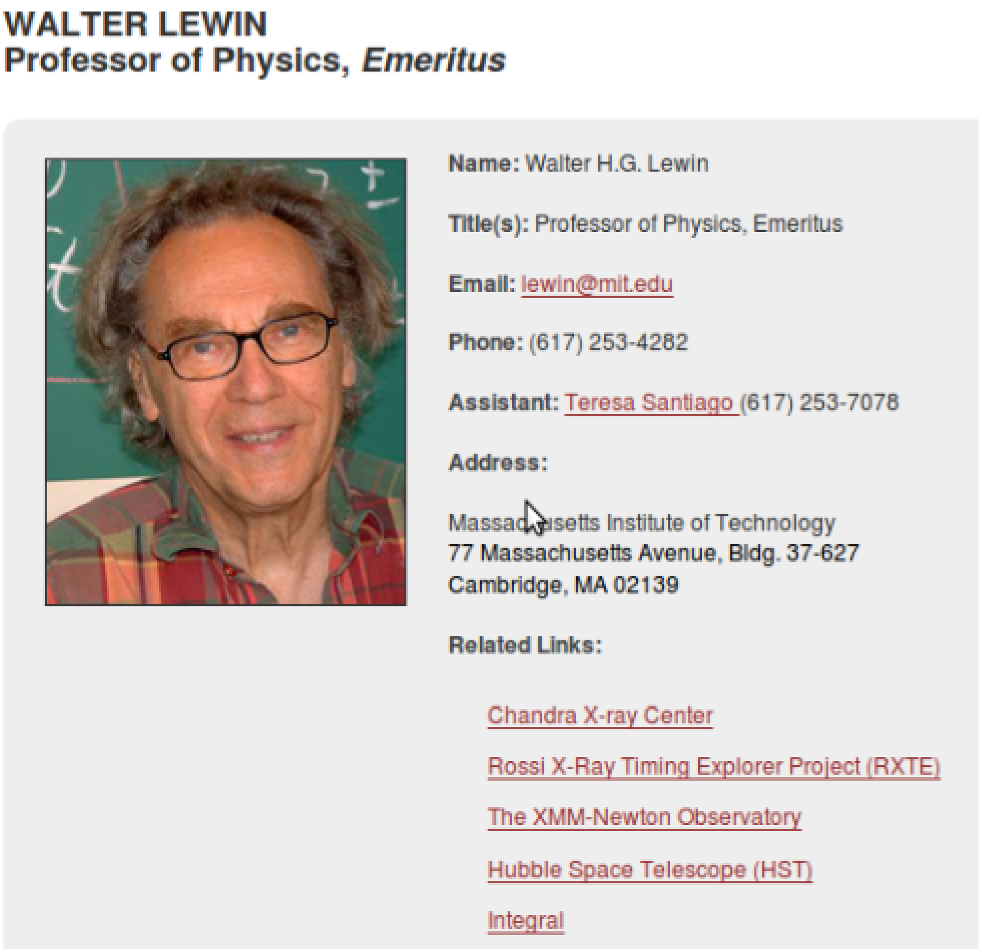
lewin@mit.edu, The quality of the color photos of this version is poor as there is an ...
arxiv.org

lewin@mit.edu, This is a short video that describes within an action orientation certain ...
blossoms.mit.edu

lewin@mit.edu, There will be no work required on your part except for attendance and ...

Work Phone Number and Office Room

We can verify the above details by simply discovering his personal web page of the MIT.



WALTER LEWIN
Professor of Physics, *Emeritus*

Name: Walter H.G. Lewin

Title(s): Professor of Physics, Emeritus

Email: lewin@mit.edu

Phone: (617) 253-4282

Assistant: Teresa Santiago (617) 253-7078

Address:

Massachusetts Institute of Technology
77 Massachusetts Avenue, Bldg. 37-627
Cambridge, MA 02139

Related Links:

- Chandra X-ray Center
- Rossi X-Ray Timing Explorer Project (RXTE)
- The XMM-Newton Observatory
- Hubble Space Telescope (HST)
- Integral

Personal page

From the above image except of the phone numbers and the addresses we have discovered also and the assistant of this professor.This can help us in many ways like:we are sending him an email pretending that it comes from his assistant.The professor will think that it came from a person that he trusts so he will respond to our questions more easily.

Basically the idea when constructing a profile of the person that you will use your social engineering skills is to have as much information as possible about his interests and activities,his friends and colleagues,emails and phone numbers etc.Keeping all that information on your notebook will help you to construct an ideal scenario that will work.

Conclusion

Exposure of personal information is an advantage for every social engineer guy.Every information that you will post on the Internet eventually it will stay forever.So before you post something personal think twice if it is really necessary to allow other people to know about my self and my activities.Also using different email addresses and usernames will make the work of social engineers much more difficult.

Disclaimer

Pentestlab appreciates highly the professor Mr. Walter Lewin and respects his work and contribution to the science and doesn’t encourage in any way his readers to use this personal information in order to perform illegal activities against this person.