Email Scraping and Maltego – Hackers Arise

Archived: 2026-04-05 22:42:30 UTC

For more on the email scraping tool, the Harvester, click here.

As a pentester/hacker, gathering email addresses from potential victims can have multiple uses. When we have the email addresses of key personnel, we can launch attacks by email to get people to click on a malicious link or direct them to our malicious website where we can send XSS attacks and other browser-based attacks. In recent years, some of the highest-profile hacks have been launched via one employee clicking on a link sent by email (RSA, NT Times, etc). In addition, when we have the emails of our potential victims, we might attempt social engineering attacks to gain information, etc. from our potential victims. Whatever form our attack might eventually take, gathering email addresses can be a valuable initial step before launching our attack.

In this tutorial, we will examine a few tools that are useful for scraping websites for available email addresses. One of the lessons of this unit is that we might have multiple tools to do the same task with different effectiveness.

I. goog- mail

One tool that has been around for a while is goog-mail. Goog-mail is a Python script for scraping email addresses from Google's cached pages from a domain.

To get started with goog-mail, create a directory named goog-mail, then navigate to that directory like in the screenshot below.

Next, use the Linux command wget to download this Python script.

wget http://dl.dropbox.com/u/10761700/goog-mail.py

As you can see in the screenshot below, we have successfully downloaded goog-mail and now we must permit ourselves to execute it.

kali > chmod 755 goog-mail.py

Now, let's point it this little tool at our favorite hacking training site, hakin9.org, to see whether it can extract any email addresses for us.

kali > goog-mail hakin9.org

As you can see in the screenshot below, it has successfully extracted three (3) email addresses for us from hakin9.org. Not bad, but I think we can do better than that. Let's look at some other email harvesting tools to see whether we can do better.

II. Maltego

Maltego is an excellent tool for information gathering from our targets from the web with multiple capabilities. In this lesson, we will use only its email scraping capabilities, but in a subsequent lesson, we will look more at using more of Maltego's many information-gathering capabilities.

Kali Linux has a free edition of Maltego built in. We can access it by going to;

Applications –> Top 10 Security Tools –> maltego

Maltego will begin to open with a splash screen like that below.

To use the community/free edition of Maltego, you will need to register.

After we register, we can begin to use this powerful tool to gain information about our target
We need to login and begin our information harvesting. Maltego describes each attempt at gathering information as a "machine". As you can see in the screenshot below, we have numerous choices of what we want Maltego to do. In this lesson, we will simply be doing the first choice, "Company Stalker" which gathers all the email addresses it can from a particular domain, so select the first radio button.

Next, we need to tell Maltego what domain we want to target. In this case, I'm targeting SANS training institute. As many of you know, SANS is a leading information security training firm in the U.S. Let's see whether we can gather any email addresses from their website.

As you can see below, we were able to harvest quite a few email addresses from SANS.org and we can then display them in the screen below. Pretty good!

When I ran Maltego against our friends here at hakin9.org, I harvested ten (10) email addresses, much better than with gogg-mail.

III. The Harvester

Kali Linux, for those new to hacking, has a powerful tool built-in, named Metasploit. Metasploit is best known as an exploitation framework, but it has a multitude of other capabilities to assist with hacking. In it auxiliary modules, it has numerous information and scanning tools integrated into this wonderful tool.

Let's start Metasploit by opening a terminal and typing;

kali > msfconsole

When we come to the msf > prompt, type ;

msf > use gather/search_email_collector

Then type the name of the domain you want to collect emails from, in this case, we will use hakin9.org.

msf >set domain haking.org

Finally, type exploit.

msf > exploit

When we do so, this email harvesting tool will begin its work of scraping the domain for any email addresses it can find. As you can see in the screenshot above, our email collector module searches through Google, then Bing, and Yahoo for email addresses within the domain we specified. In this case, it found just five (5) emails there, better than goog-mail, but far fewer than Maltego.

One key lesson here, besides the obvious lesson that information gathering is critical to a successful hack, is that different tools with the same capabilities can have different effectiveness. At least in this short lesson here, Maltego appears to be far more effective at harvesting email addresses than either goog-mail or Metasploit email gathering module. This may not always the case in all domains and circumstances, so in your exercise below, you will test their capabilities on your own and other domains.
