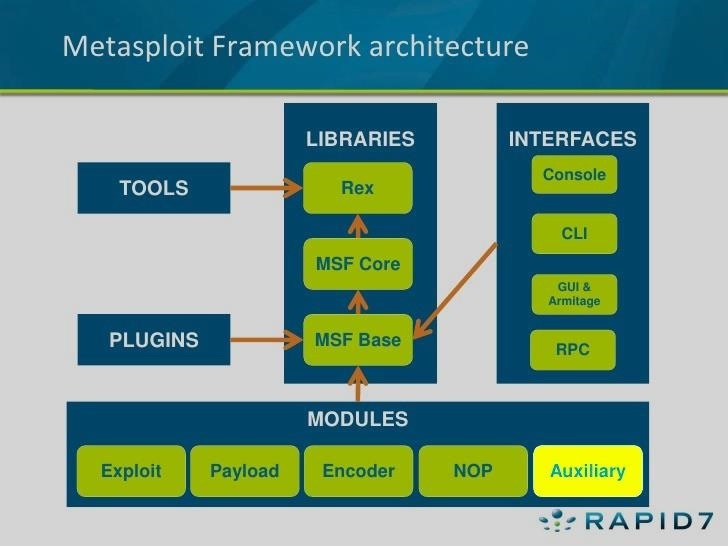
[Metasploit for the Aspiring Hacker, Part 10 (Finding Deleted Webpages)](https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-10-finding-deleted-webpages-0165555/)

* BY [**OCCUPYTHEWEB**](https://creator.wonderhowto.com/occupythewebotw/)
* 11/12/2015 3:34 AM
* [METASPLOIT BASICS](https://null-byte.wonderhowto.com/how-to/metasploit-basics/)

Welcome back, my greenhorn hackers!

Throughout [this series on Metasploit](https://null-byte.wonderhowto.com/how-to/metasploit-basics/), and in most of my hacking tutorials here on Null Byte that use Metasploit (there are many; type "[metasploit](https://null-byte.wonderhowto.com/search/metasploit/)" into the search bar and you will find dozens), I have focused primarily on just two types of modules: exploits and payloads. Remember, Metasploit has [six types of modules](https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-1-primer-overview-0155986/):

1. Exploit
2. [Payload](https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-3-payloads-0157032/)
3. Auxiliary
4. NOP (no operation)
5. Post (post exploitation)
6. Encoder

[](https://img.wonderhowto.com/img/original/33/33/63582835778126/0/635828357781263333.jpg)

Although most hackers and pentesters focus on the exploits and payloads, there is significant capability in the auxiliary modules that is often overlooked and ignored. About one-third of all of Metasploit—measured by lines of code—is auxiliary modules. These auxiliary modules encompass the capabilities of many other tools that a hacker requires, and include various types of scanners (including [Nmap](https://tag.wonderhowto.com/nmap/)), [denial-of-service](https://null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699/) modules, fake servers for capturing (admin) credentials, [fuzzers](https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploring-metasploit-auxiliary-modules-ftp-fuzzing-0155574/), and many more.

In this tutorial, I want to explore and illuminate one of the auxiliary modules that can make hacking with Metasploit much more effective and efficient.

Step 1List the Modules

First, let's fire up [Kali](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/) and open a terminal. In Kali, Metasploit modules are stored at:

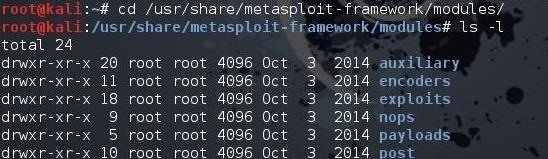
**/usr/share/metasploit-framework/modules**

Let's navigate there:

**kali > cd /usr/share/metasploit-framework/modules/**

Then, let's list the contents of that directory:

**kali > ls -l**

[](https://img.wonderhowto.com/img/original/97/17/63582837765641/0/635828377656419717.jpg)

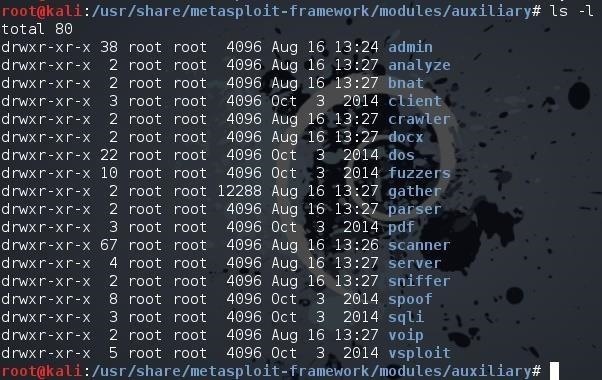
As you can see, there are six types of modules in Metasploit, as mentioned before. Let's focus our attention on the auxiliary modules.

Step 2List the Auxiliary Modules

First, navigate to the auxiliary module directory and list its contents:

**kali > cd auxiliary**

**kali > ls -l**

[](https://img.wonderhowto.com/img/original/68/27/63582837778110/0/635828377781106827.jpg)

As you can see, there are numerous subdirectories of auxiliary modules. In [an earlier tutorial](https://null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699/), I pointed out that there are hundreds of auxiliary modules for DoSing in Metasploit. In this tutorial, we want to work with the scanner modules. Metasploit has scanning modules of just about every type, including [Nmap](https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-active-reconnaissance-and-dos-attacks-with-nmap-0146950/) and website vulnerability scanning.

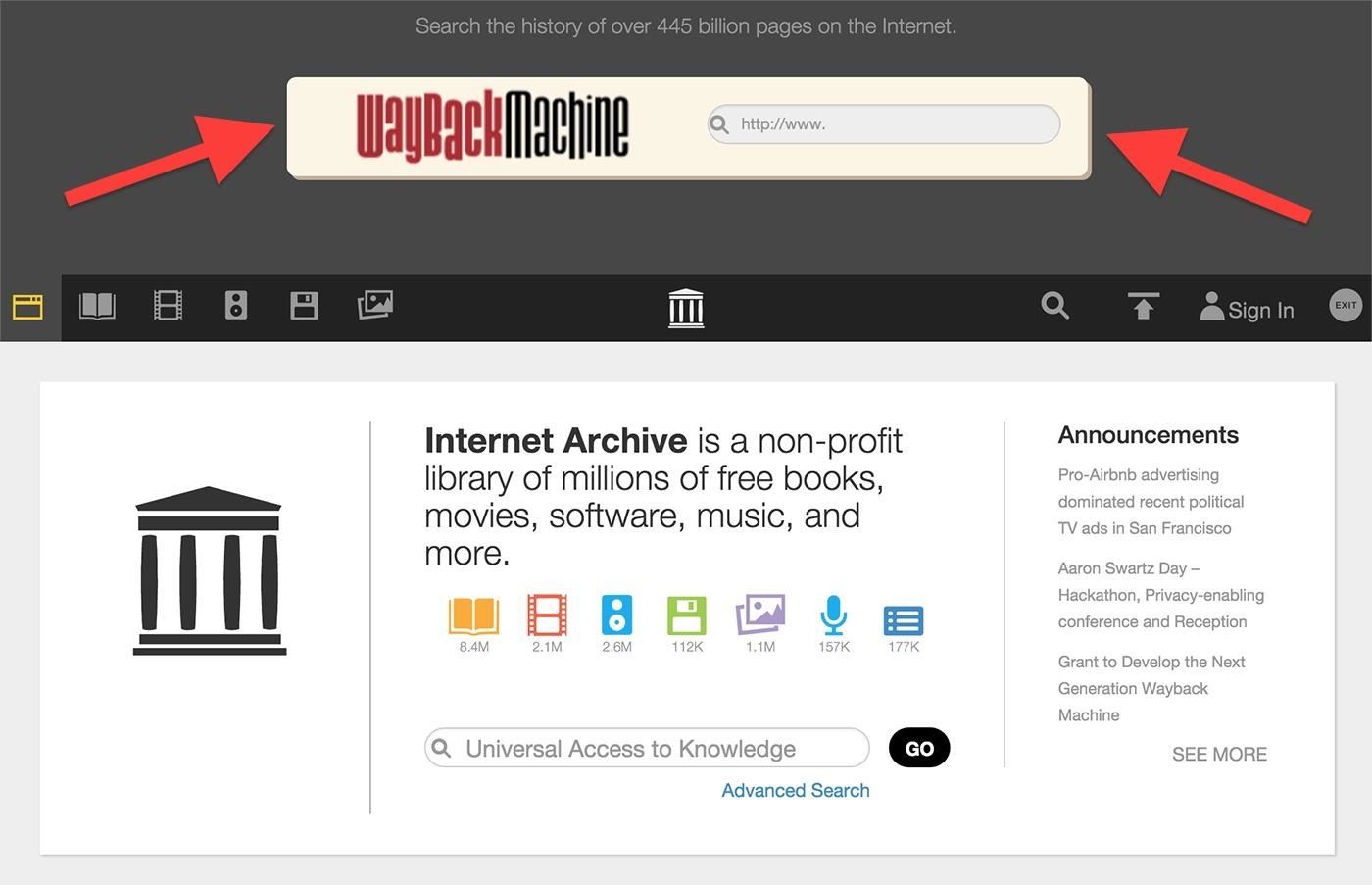
Step 3The Wayback Machine

As many of you know, recent years have seen an increased emphasis on information security. Webmasters and IT security personnel are more vigilant about what goes onto their website, trying to make certain that information that might be used to compromise their security is not posted.

If we go back just a few years, that was not the case. Companies often would post email addresses, passwords, vulnerability scans, network diagrams, etc. on their website, not aware that someone might find these and use them for malicious purposes. Although I still occassional find a company listing email addresses and passwords on their website, this has become much less common.

Fortunately for us, nothing ever disappears from the web. If it's here today, it will be here 20 years from now (keep that in mind when posting on Facebook or other social media sites).

The Internet Archive ([Archive.org](https://archive.org/)) was established to save free books, movies, music, software, along with all of the old web information via its [Wayback Machine](https://archive.org/web/" \t "_blank)tool (which is a reference to an old cartoon where the main characters, Mr. Peabody and Sherman, would travel back in time in a time machine they called the "[WABAC Machine](https://en.wikipedia.org/wiki/WABAC_machine)"). This means that if a company had, at one time, stored email addresses and passwords on their webpages, or Nessus scans, it is still around somewhere on Archive.org.

[](https://img.wonderhowto.com/img/original/96/59/63582838594516/0/635828385945169659.jpg)

Step 4Use Metasploit to Retrieve Deleted Webpages

Fortunately for us, Metasploit has an auxiliary module that is capable of retrieving all of the old URLs from Archive.org that are stored for a particular domain. Since the Internet Archive's website tool is referred to as the [Wayback Machine](https://archive.org/web/" \t "_blank), Metasploit has a module called **enum\_wayback**, short for "enumerate wayback" machine.

Let's start the Metasploit console and load it:

**kali > msfconsole**

When the msfconsole opens, let's load the wayback module by typing:

**msf > use auxiliary/scanner/http/enum\_wayback**

[https://img.wonderhowto.com/img/76/19/63582840309485/0/hack-like-pro-metasploit-for-aspiring-hacker-part-10-finding-deleted-webpages.w1456.jpg](https://img.wonderhowto.com/img/original/76/19/63582840309485/0/635828403094857619.jpg)

This module basically has just two parameters to set:

1. The domain we want to search for on archive.org
2. The file we want to save the information in

Since we will be using the [SANS.org](http://www.sans.org/) as our target, let's set the output to a file named **sans\_wayback**:

**msf > set OUTFILE sans\_wayback**

[https://img.wonderhowto.com/img/32/97/63582840321001/0/hack-like-pro-metasploit-for-aspiring-hacker-part-10-finding-deleted-webpages.w1456.jpg](https://img.wonderhowto.com/img/original/32/97/63582840321001/0/635828403210013297.jpg)

Next, let's set the domain to our favorite IT Security domain:

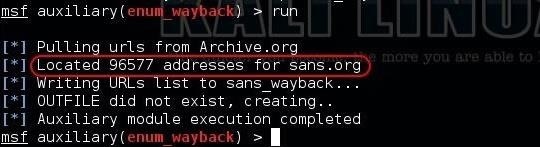
**msf > set DOMAIN sans.org**

[https://img.wonderhowto.com/img/57/47/63582840333157/0/hack-like-pro-metasploit-for-aspiring-hacker-part-10-finding-deleted-webpages.w1456.jpg](https://img.wonderhowto.com/img/original/57/47/63582840333157/0/635828403331575747.jpg)

Step 5Start the Wayback Machine

Unlike exploits in Metasploit where we type **exploit** to start them, auxiliary modules are initiated by typing **run** instead:

**msf > run**

[](https://img.wonderhowto.com/img/original/34/41/63582840513470/0/635828405134703441.jpg)

This module will now go to Archive.org and begin to retrieve every saved URL of SANS.org over the years. In the case of SANS.org, it is over 96,000 URLs! Since we told this module to store all of the URLs in a file named "sans\_wayback," all these URLs are written to this file.

When the module is done running, we can look inside this file by typing:

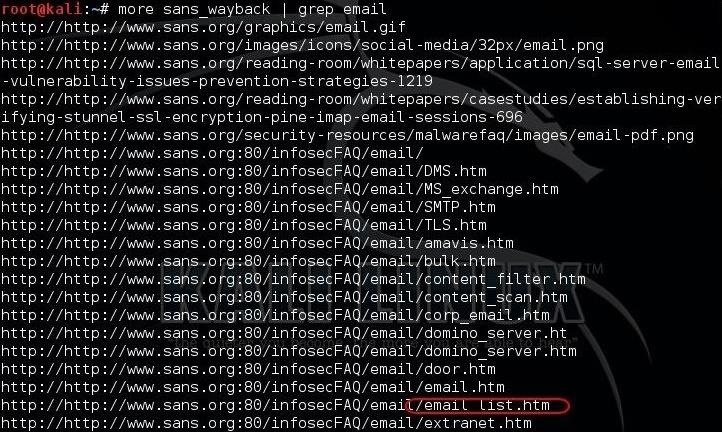
**kali > more sans\_wayback**

[](https://img.wonderhowto.com/img/original/10/53/63582840523970/0/635828405239701053.jpg)

When we do, we can see that Archive.org has stored the first URL from 1998. With over 90,000 URLs, visual inspection looking for interesting information is not really practical. Fortunately, god gave us the **[grep](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-10-manipulating-text-0148539/)** command.

If we want to find the URLs with emails stored in them, we can type:

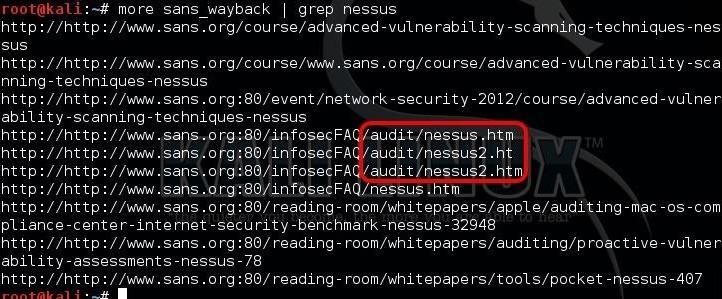
**kali > more sans\_wayback | grep email**

[](https://img.wonderhowto.com/img/original/80/97/63582840533188/0/635828405331888097.jpg)

As you can see in the screenshot above, there are quite a few URLs pertaining to email. The one I have circled in red looks particularly interesting, **email\_list.htm**.

It is not unheard of for companies to put their vulnerability scans on their website for the security and network personnel to view (and the rest of us). As Nessus is the world's most widely used vulnerability scanner, let's see whether we can find it among these old webpages.

**kali > more sans\_wayback | grep nessus**

[](https://img.wonderhowto.com/img/original/81/57/63582840543688/0/635828405436888157.jpg)

As you can see above, we have found three webpages with Nessus in them in the "audit" directory. Hmmm... that might be interesting... maybe some Nessus scan reports from the past?

This approach to finding deleted information is limited to the information in the URL. We could actually take these URLs and view them in our browser at Archive.org to see whether we can find text information on the page that might be useful. Maybe a better approach would be to download the interesting URLs that this module enumerated directly to a hard drive using [HTTrack](https://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/), then do a text search on the entire web content.

Keep coming back, my greenhorn hackers, as we explore the workings of the hacker's best friend, [Metasploit](https://null-byte.wonderhowto.com/how-to/metasploit-basics/)!