Dig for DNS Info

The domain information groper, or [**dig**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-6-networking-basics-0147673/), is a command that is built into every distribution of [Linux](https://null-byte.wonderhowto.com/how-to/linux-basics/) and UNIX. It is designed to be able to grab and display for the user key DNS info. Let's open a terminal and start digging!

With a terminal open, we can type **dig** from any directory as this ubiquitous command is located in the /bin directory in every version of Linux and UNIX. Let's do some digging on our friends at SANS, one of the leading information security training and consulting firms in the world.

**kali > dig sans.org**

[](https://img.wonderhowto.com/img/original/19/17/63546895013958/0/635468950139581917.jpg)

Dig goes out to the Internet and grabs the records from your DNS server as seen above. You can see that it grabs the IP address (66.35.59.202) of the domain sans.org. The next section contains the name servers for this domain:

* dns31b.sans.org
* dns31a.sans.org
* dns21a.sans.org
* dns21b.sans.org

If we want to find their email servers, we simply add an [**mx**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-6-networking-basics-0147673/) to the end of the command like this:

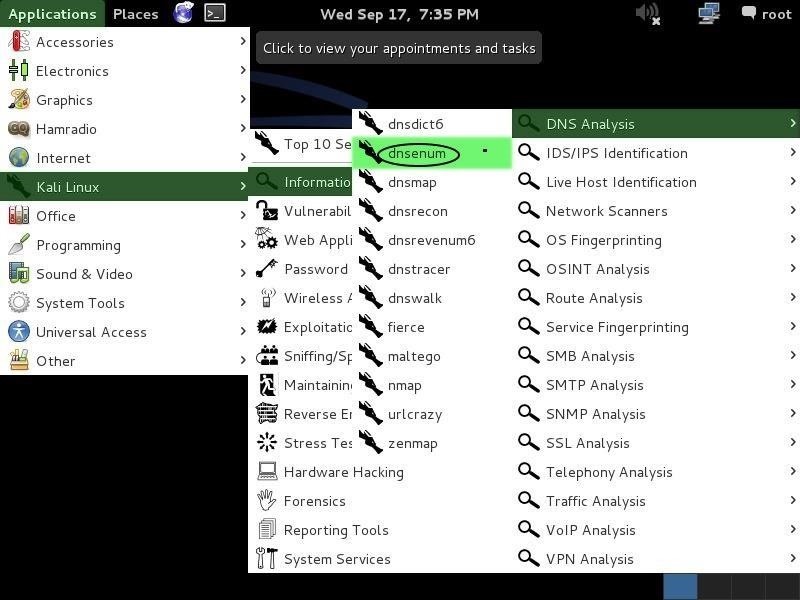
**kali > dig sans.org mx**

[](https://img.wonderhowto.com/img/original/63/63/63546895055645/0/635468950556456363.jpg)

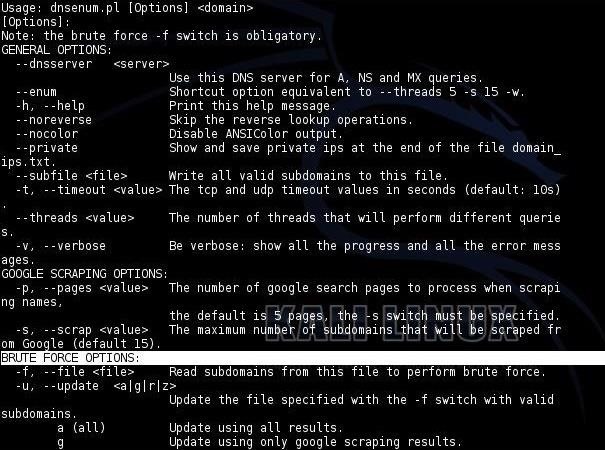
As you can see, this simple query reveals for us the four email servers that SANS utilizes. Hmmmm....very interesting. Anyone want to send anonymous, spoofed, or bulk email?

Step 2Open Dnsenum

[Kali](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/) and [BackTrack](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-backtrack-your-new-hacking-system-0146889/) both have a nice little tool that can do everything dig does and more. It's called **dnsenum**. We can find it by going to Applications -> Information Gathering -> DNS Analysis -> dnsenum.

[](https://img.wonderhowto.com/img/original/46/21/63546895066114/0/635468950661144621.jpg)

When you do, it will open a dnsenum help screen like that below. Among the things that dnsenum can do for us is find subdomains that are not obvious or are hidden from the public. I have highlighted the section in the screenshot that addresses brute-forcing these subdomains.

[](https://img.wonderhowto.com/img/original/33/13/63546895077364/0/635468950773643313.jpg)

Step 3Run Dnsenum

Let's try running this simple, but effective tool against our friends at SANS and see if we can find additional information about their servers and subdomains from querying DNS. It's probably worthwhile to note here that all of this [reconnaissance](https://null-byte.wonderhowto.com/how-to/recon/) is "passive." There is no way for the victim to know we are "casing" their systems because we are not "touching" their systems, just the DNS servers so it looks like normal traffic.

**kali > dnsenum sans.org -f /usr/share/dirbuster/wordlists/directories.jbrofuzz**

You can use any [wordlist](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/) you have available to you that you believe may contain the name of subdomains of the organization, so choose you wordlist carefully, my tenderfoot hackers. You can find all the wordlists built into Kali by typing;

**kali > locate wordlist**

In this case, I chose the */usr/share/dirbuster/wordlists/directories.jbrofuzz* wordlist, as it has many directory names which also are often used in the names of subdomains.

When we run this command, we get the following results. First, we see the name servers and the mail servers (mx) just as we did by using dig. These records also include the IP addresses of these servers. It's interesting to note that SANS is using Google mail servers. I would have thought they would use their own email servers, considering their level of IT expertise.

[](https://img.wonderhowto.com/img/original/76/15/63546895090223/0/635468950902237615.jpg)

Next, dnsenum will attempt to do a zone transfer. In this case, it failed against the DNS server.

Finally, it will try to find subdomains within sans.org. Many times, companies have subdomains such as training.sans.org and admin.sans.org—dnsenum can help us find these by attempting to brute-force these potential subdomains using a wordlist. Of course, as I mentioned, the wordlist you choose will be critical to your success, but generally, these subdomain names are simple dictionary words like training, test, sales, admin, etc.

[](https://img.wonderhowto.com/img/original/18/75/63546895099958/0/635468950999581875.jpg)

Like any brute-force attempt, this can be tedious and time consuming, so be patient. If you choose a good wordlist and are patient, you are likely to find many hidden servers that the company doesn't necessarily want you to know about, but might be juicy targets. Dnsenum will not only find these servers, but will also provide you the IP address which can VERY helpful when we get around to attacking that system.

I ran dnsenum for a few hours and retrieved the subdomains listed above. As you can see, it was about 50% done, having only gone through the letter "L."

Dnsenum is just one more tool in our hacker toolbox that can be useful for [doing reconnaissance on potential targets](https://null-byte.wonderhowto.com/how-to/recon/). The beauty of this tool is its ability to find those hidden servers by simply abusing DNS, and the potential victim is totally unaware of any untoward activity.

I'll keep showing more and more tools and techniques for hacking, so keep coming back, my tenderfoot hackers!