



# SANS ISC InfoSec Forums

Keyword, Domain, Port, IP or Header

Search

Log In

[Sign Up for Free!](#)[Forgot Password?](#)

## Contact Us

## Diary

## Podcasts

## Jobs

## News

## Tools

## Data

## FORUMS

[Auditing](#)[Diary Discussions](#)[Forensics](#)[General Discussions](#)[Industry News](#)[Network Security](#)[Penetration Testing](#)[Software Security](#)[← Next Thread](#) [Previous Thread →](#)

Does your organization have an InfoSec opening? [Post a job listing](#) with the SANS Internet Storm Center

## DNS Reconnaissance using nmap



In a penetration test (PenTest) a thorough reconnaissance is critical to the overall success of the project.

DNS information for the target network is often very useful reconnaissance information. DNS information is publicly available information and enumerating it from DNS servers does not require any contact with the target and will not tip off the target company to any activities.

A tool that can be used to assist with DNS information gathering is nmap. Nmap has a parallel reverse DNS resolution engine that is normally employed as part of an nmap scan, but can also be used independently of the scan function to do DNS enumeration.

Let's pretend we were hired to do a pentest against SANS. [www.sans.org](http://www.sans.org) is 66.35.59.202. According to ARIN whois 66.35.59.202 is part of a /24 range allocated to the SANS (66.35.59.0/24). ARIN also shows another /24 network range allocated to SANS (204.51.94.0/24).

From <http://whois.arin.net/rest/org/SANSI-1/nets/>

Network Resources	
TERRENAP-0-20 (NET-204-51-94-0-1)	204.51.94.0 - 204.51.94.255
NET-66-35-59-0-1 (NET-66-35-59-0-1)	66.35.59.0 - 66.35.59.255

The nmap command to be used in this case is:

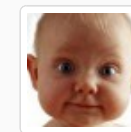
```
# nmap --dns-servers 8.8.8.8,8.8.4.4 -sL 204.51.94.0/24 66.35.59.0/24
```

By default nmap will use your system's configured DNS. If you are enumerating a large address space nmap can generate a high volume of queries. While this shouldn't cause an issue for your DNS servers, being paranoid, I use publicly available servers that I know can handle the volume. In this case Google's public DNS at 8.8.8.8 and 8.8.4.4 or OpenDNS. These servers are specified using the `--dns-servers` parameter.

`-sL` specifies a list scan, which means nmap will only do a DNS resolution, not actually scan the target.

204.51.94.0/24 66.35.59.0/24 is the target networks we want to enumerate. In nmap if multiple address ranges are to be part of the target they are space separated.

Rick



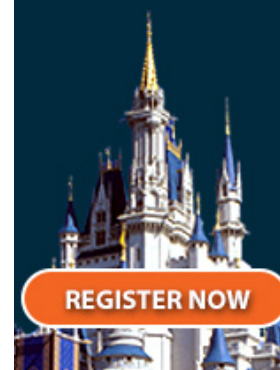
223 POSTS

ISC HANDLER

# SANS 2016

More Than 35  
World-Class  
Information  
Security  
Courses

Orlando, FL  
March 12 - 21



The output is one line per IP in the range (heavily edited for space). Notice that every IP with a reverse DNS entry has that entry listed. IPs without reverse DNS entries just show the IP.

Starting Nmap 5.51 ( <http://nmap.org> ) at 2015-11-08 13:39 EST

Nmap scan report for 204-51-93-0.clp.sans.org (204.51.94.0)

Nmap scan report for router31-int.clp.sans.org (204.51.94.1)

Nmap scan report for fw 31.clp.sans.org (204.51.94.2)

...

Nmap scan report for 204.51.94.43

Nmap scan report for 204.51.94.44

...

Nmap scan report for portal.sans.org (204.51.94.201)

Nmap scan report for mail.sans.org (204.51.94.202)

Nmap scan report for exams.giac.org (204.51.94.203)

Nmap scan report for w w w .giac.org (204.51.94.204)

...

Nmap scan report for w w w .sans.org (66.35.59.202)

Nmap scan report for exams.giac.org (66.35.59.203)

Nmap scan report for w w w .giac.org (66.35.59.204)

...

Nmap scan report for dshield.org (66.35.59.248)

Nmap scan report for isc.sans.org (66.35.59.249)

Nmap scan report for isc.sans.org (66.35.59.250)

Nmap scan report for isc.sans.org (66.35.59.251)

...

Nmap done: 512 IP addresses (0 hosts up) scanned in 58.98 seconds

DNS information is publicly available information, so enumerating it is not a crime in any jurisdiction that I am

aware of. If you really feel the need to go further than this, please remember that the difference between an attack and a pentest is permission.

-- Rick Wanner MSISE - [rwanner@isc.sans.edu](mailto:rwanner@isc.sans.edu) - <http://namedeplume.blogspot.com/> -  
Twitter:namedeplume (Protected)

Tags: DNS, nmap

[Reply](#) [Subscribe](#)

2 months ago

Using NMAP for DNS recon means doing PTR record queries of the current DNS, which can be deleterious in three ways. First, not all address assignments are covered by PTR records, and often times the only registration is the A record (or AAAA, for IPv6). PTR is sometimes called "reverse lookup" whereas A and AAAA are called "forward lookup". Simply put, a reverse lookup does not have to work in order for a domain name to be usable as a service locator.

Second, the current DNS may be inaccurate, since malicious domains and networks are under constant threat of takedown. It's valuable therefore to see the history of prior registrations rather than just those registrations which still exist at the time of your recon work. Third and finally, the name servers responsible for the registration data may be under control or surveillance by your opponents, who can either feed you false data, or know from your queries when your recon work has begun, or both.

For those reasons, recon work should also include passive DNS lookups. Here is a short shell-level demo for the two networks you used in your examples. Note that the real data is in JSON form, but that I've converted it to CSV here for readability purposes.

```
$ ./dnsdb_query -p csv -i 204.51.94.0/24 | wc -l
475
$ ./dnsdb_query -p csv -i 204.51.94.0/24 | head
time_first,time_last,zone_first,zone_last,count,bailiwick,rrname,rrtype,rdata
,,2011-02-24 17:10:31,2015-11-07 17:15:32,1707,,,"ns1.counterhackchallenges.com.,"A","204.51.94.78"
,,2011-04-15 14:03:36,2015-11-08 16:04:48,1656,,,"dns31a.sans.org.,"A","204.51.94.7"
,,2011-04-15 14:03:36,2015-11-08 16:04:48,1656,,,"dns31b.sans.org.,"A","204.51.94.8"
2011-02-07 19:05:02,2015-11-08 16:41:14,,,"37795633","dns31a.sans.org.,"A","204.51.94.7"
2011-02-07 19:05:02,2015-11-08 16:41:14,,,"37771267","dns31b.sans.org.,"A","204.51.94.8"
2011-04-20 14:13:09,2015-11-08 14:34:30,,,"369108","smtp31a.sans.org.,"A","204.51.94.13"
2011-04-20 14:13:09,2015-11-08 09:55:54,,,"363539","smtp31b.sans.org.,"A","204.51.94.14"
2010-11-05 19:42:58,2013-11-05 22:54:30,,,"31860","mass31a.sans.org.,"A","204.51.94.25"
2011-09-30 16:16:31,2011-11-04 02:18:49,,,"245","elm.sans.org.,"A","204.51.94.26"
```

```
$ ./dnsdb_query -p csv -i 66.35.59.0/24 | wc -l
2421
$ ./dnsdb_query -p csv -i 66.35.59.0/24 | head
time_first,time_last,zone_first,zone_last,count,bailiwick,rrname,rrtype,rdata
,,2012-09-12 14:10:09,2015-11-08 16:04:48,1140,,,"dns21a.sans.org.,"A","66.35.59.7"
,,2012-09-12 14:10:09,2015-11-08 16:04:48,1140,,,"dns21b.sans.org.,"A","66.35.59.8"
```

Anonymous



2 POSTS

```
2012-11-01 14:32:08,2015-08-11 09:04:19,,382,,,"dns1a.den.giac.net.", "A", "66.35.59.7"
2012-11-01 14:35:59,2012-11-02 11:00:01,,69,,,"dns1b.den.giac.net.", "A", "66.35.59.7"
2012-09-11 21:29:50,2015-11-08 17:11:22,,22167360,,,"dns21a.sans.org.", "A", "66.35.59.7"
2012-11-01 14:32:08,2015-10-26 00:15:48,,93,,,"dns1c.den.giac.net.", "A", "66.35.59.8"
2012-10-29 23:48:53,2015-11-08 17:11:22,,22167343,,,"dns21b.sans.org.", "A", "66.35.59.8"
2012-08-29 23:15:03,2015-11-08 19:01:44,,321206,,,"smtp21a.sans.org.", "A", "66.35.59.13"
2012-08-29 22:34:01,2015-11-08 16:23:24,,302389,,,"smtp21b.sans.org.", "A", "66.35.59.14"
```

There are dozens of passive DNS projects around the Internet. The above examples come from Farsight DNSDB, which is free for purely academic, unpaid and unfunded, no-fee-charged work, and which is available commercially for other work including self defense, customer defense, or commercial research.

For a deeper demonstration, I've uploaded the following files:

```
http://family.redbarn.org/~vixie/sans1.txt
http://family.redbarn.org/~vixie/sans1.json
http://family.redbarn.org/~vixie/sans1.csv
http://family.redbarn.org/~vixie/sans2.txt
http://family.redbarn.org/~vixie/sans2.json
http://family.redbarn.org/~vixie/sans2.csv
```

Vixie


[Reply](#) [Quote](#)

2 months ago

Thanks Vixie! Everything you say is absolutely correct. nmap should not be the only tool in an experienced pentester's drawer, but it is but one of the many tools at the pentester's disposal. Passive DNS is another excellent source of information.

[Reply](#) [Quote](#)

**Rick**



223 POSTS

ISC HANDLER

2 months ago

One other caveat, is that DNS queries that aren't answered by a cached entry will ultimately propagate back to an authoritative server. If you do have some type of query logging running, then you will be able to see these DNS scans.

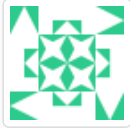

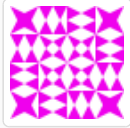


That was exactly the case for me. I detected someone querying every PTR record on my network, and by tracking back, I identified the network they were coming from. Subsequently after a few more enquiries I was given the contact details for the person responsible.

When I contacted them, their response was one of surprise. They informed me that nobody else had ever detected them conducting DNS scans. However, there's a first time for everything I suppose?

**Ian B**



5 POSTS

<a href="#">Reply</a> <a href="#">Quote</a>	2 months ago
<p>DNS is not always available to the public: see split-horizon DNS!</p>	<b>Anonymous</b>  67 POSTS 2 months ago
<a href="#">Reply</a> <a href="#">Quote</a>	2 months ago
<p>@IAN: How would you enable DNS query logging for your company domain?</p>	<b>AAInfoSec</b>  33 POSTS 2 months ago
<a href="#">Reply</a> <a href="#">Quote</a>	2 months ago
<p>There's also a module in recon-ng (recon/netblocks-hosts/reverse-resolve that can be used to perform reverse lookups of netblocks obtained from ARIN. You can set global options in recon-ng to change to the Google DNS.</p>	<b>Anonymous</b>  4 POSTS 2 months ago
<a href="#">Reply</a> <a href="#">Quote</a>	2 months ago
<p>I looked at using Farsight's DNS database <a href="https://www.dnsdb.info/">https://www.dnsdb.info/</a> but found it much too expensive for a small .edu to use for self defense. It would have been most helpful. I'm assuming Vixie is Dr. Paul Vixie, CEO of Farsight <a href="https://www.farsightsecurity.com/Team/">https://www.farsightsecurity.com/Team/</a></p>	<b>John</b>  70 POSTS 2 months ago
<a href="#">Reply</a> <a href="#">Quote</a>	2 months ago
<p>I've found that DNSDumpster.com gives relatively complete information for quick recon as well. It's likely not as advanced as Farsight's offering by any means, but it typically gives complete information and even does some nice tree maps.</p>	<b>Diamond187</b> 

[Reply](#) [Quote](#)

1 POSTS

2 months ago

[← Next Thread](#) [Previous Thread →](#)

[Sign Up for Free](#) or [Log In](#) to start participating in the conversation!



[Shop](#) [Link To Us](#) [About Us](#) [Handlers](#) [Privacy Policy](#) [Back To Top](#)

**Developers:** We have an [API](#) for you!

