

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] NMAP - Passive Recon Using List Scan](#)

TickTockMan - September 4, 2011, 12:14 am

NMAP – Passive Recon Using List Scan

I'm sure that most of you are familiar with nmap, a port scanner which has been around for a long time. It has numerous features and options, and allows for a high degree of flexibility when conducting port scans.

This tutorial is inspired and influenced by a section of Fyodor's book, "NMAP Network Scanning". It covers how to use the nmap list scan option, -sL, in order to gain more information about a network, by discovering additional hosts which may not be as well protected as the primary target, and could be used in a lateral attack. The functionality of the list scan is very basic. It lists hosts which would be scanned, without sending any port status probes.

Why would you want to do this? What is the use if you don't get any port status information?

The answer to the above questions is simple – DNS. The purpose of DNS is to use human friendly names for network hosts, which are easier to remember than ip addresses. DNS entries can indicate the type of servers in use, giving a general overview of the network, and allowing you to narrow down the machines and services to probe for vulnerabilities.

Here is a scan for a single host:

```
$ nmap -sL www. example.com
```

```
Starting Nmap 5.51 at 2011-09-03 09:48 CST
```

```
Nmap scan report for www. example.com (192.168.1.226)
```

```
Nmap done: 1 IP address (0 hosts up) scanned in 0.17 seconds
```

As you can see nmap, performed a dns lookup get the ip address for the domain. This process will also work the other way, when there is a reverse dns entry for a given ip address.

```
$ nmap -sL 192.168.1.226
```

```
Starting Nmap 5.51 at 2011-09-03 12:00 CST
```

```
Nmap scan report for www. example.com (192.168.1.226)
```

```
Nmap done: 1 IP address (0 hosts up) scanned in 0.17 seconds
```

Now, what if our target is one host in a larger network of related ip addresses? This is where things get more interesting.

Lets do a list scan of the entire Class C subnet (256 ip addresses), containing our target.

```
nmap -sL www. example.com/24
```

Starting Nmap 5.51 at 2011-09-03 12:00 CST

<snip>

Nmap scan report for pptp.example.com (192.168.1.209)
Nmap scan report for 192.168.1.210
Nmap scan report for relay.example.com (192.168.1.213)
Nmap scan report for 192.168.1.214
Nmap scan report for webdev.example.com (192.168.1.216)
Nmap scan report for smtp.example.com (192.168.1.217)
Nmap scan report for 192.168.1.218
Nmap scan report for 192.168.1.225
Nmap scan report for www. example.com (192.168.1.226)
Nmap scan report for ftp. example.com (192.168.1.230)

<snip>

Nmap done: 256 IP addresses (0 hosts up) scanned in 4.69 seconds

Note: nmap will accept variety of formats for scanning multiple ip addresses. We could have used the following and still gotten the same results: `nmap -sL 192.168.1.0-255`

While we we didn't get names for all of the ip addresses, there are clearly others in the same domain which could be points of interest for gaining access to the network.

webdev – Development server? Is it configured at the same security level and the primary web server?

smtp and ftp – Again, how secure are these? Can we brute force accounts on them?

For a given host, you could just scan the relevant standard ports for its services, and lessen the chances of triggering an alert.

When dealing with large ranges of ip addresses, I find it more convenient to have the results output to a file for futher parsing.

```
nmap -sL www. example.com/24 -oN example.txt
```

If your scan shows multiple domains which do not appear to be related, then there is a good chance that are seeing multiple servers at a shared or dedicated hosting environment. This can still work to your advantage if the other machines or sites are not properly secured.

If you are really bored, you could just look for interesting random targets. Sometimes I do this just to get feel for what type of machines might be out there on the Internet.

Now we will also use the `-iR` flag, for a random sampling of ip addresses:

```
nmap -iR 5000 -sL -oN random.txt
```

Depending on your text editor, or comfort using command line tools, there are a number of ways to filter on particular domains, which you may or may not want to stay away from. Or I just glance through the list and see what catches my eye.

For example, are there any .edu domains in my list of random hosts?

```
grep -v -P 'd{1,3}\.d{1,3}\.d{1,3}\.d{1,3}$' random.txt |awk '{print $5}' | grep -P '\.edu$'
```

```
XX.harvard.edu  
XX.usf.edu  
XX.oregonstate.edu
```

And with that, I will wrap things up. Please let me know your thoughts on this tutorial. Hopefully there aren't any spectacularly bad mistakes in it.

toriqq - September 4, 2011, 1:19 am

Appreciated for the tut. So how do I scan for vps ips in my country range? The port is 8080

TickTockMan - September 4, 2011, 5:19 am

(Sep 4, 2011 01:19 AM)toriqq Wrote: [\[CITE\]](#) Appreciated for the tut. So how do I scan for vps ips in my country range? The port is 8080

I do have a method for targeting specific country ip ranges. When I get a chance, I'll see about writing a separate tutorial for that, assuming it hasn't already been done here (I haven't searched yet on that subject).

Ble\$\$eD - September 5, 2011, 4:12 pm

Nice tutorial this ought to help out alot new members here and some that are new to nmap.

bashtem - September 5, 2011, 6:22 pm

nmapis the best port scanner for me it is preety cool

Dialga - September 7, 2011, 2:36 pm

Nice tutorial will use it for sure!! :)

soccer05 - September 7, 2011, 4:10 pm

Nice tutorial. This will def help out some beginners!

EmJay88 - September 7, 2011, 6:18 pm

Thanks mate ! I've been looking for that :)

starcluster - October 7, 2011, 3:33 pm

We novices always appreciate fresh independant discourse.

Developer - October 11, 2011, 9:37 pm

Good job on this basic tutorial but it needs so much added on it.

Clones - October 11, 2011, 10:58 pm

This is really a very nice thread, thanks for sharing with us :)

