Gathering Web Server Information With Nmap NSE

Information gathering is one of the most crucial steps when pentesting a web server. We can use some of the latest Nmap NSE scripts to collect information and use it to effectively perform a security assessment of a web server and of resident web applications.

The Nmap Scripting Engine offers a robust and flexible framework to develop scripts that perform tasks using host information available to Nmap. Since web security have been drawing a lot of attention, open source collaborators started submitting more HTTP scripts turning Nmap into an extremely powerful tool for web scanning.

From advanced version detection to vulnerability exploitation, Nmap has a wide range of scripts that are useful when conducting penetration tests to web servers and web applications. For a complete list of HTTP scripts visit: *http://nmap.org/nsedoc/*.

Getting Nmap

It is highly recommended that you download the latest stable version from Nmap's official repositories:

```
$svn co --username guest --password
                    „” svn://
                    svn.insecure.org/nmap/
```

If you feel like experimenting with the latest creations of the Nmap's development team, download the experimental branch. Note that this is the developer's sandbox and nothing is guaranteed to work:

```
$svn co --username guest --password „” svn://
                    svn.insecure.org/nmap-exp/
```

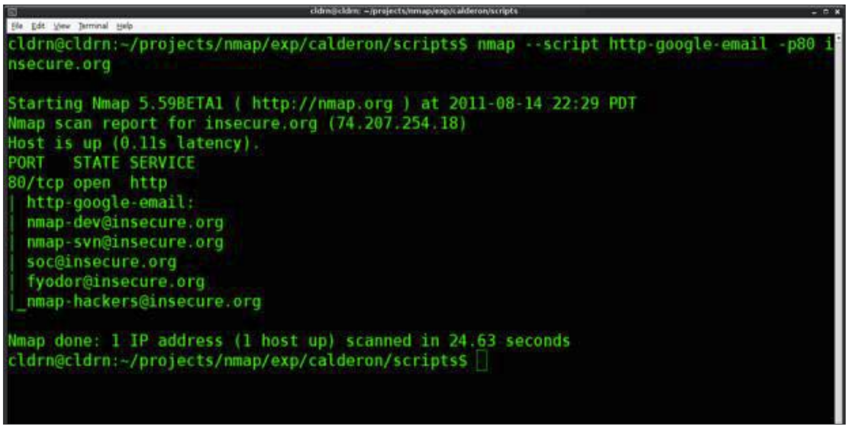
To update after you downloaded a working copy:

```
$svn up
```

You can find other NSE scripts that for different reasons are not going to be included in official releases at: *https://secwiki.org/w/Nmap/Script_Vault*.

Nmaping Search Engines

Search engines contain all sorts of useful information that could be handy during a web penetration test. The following

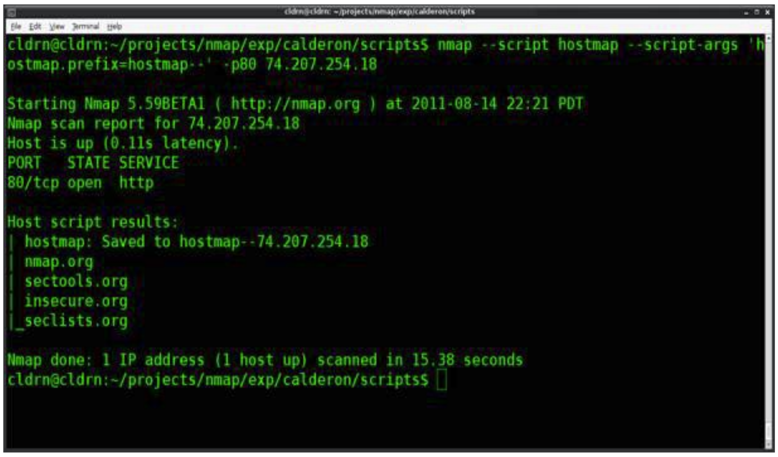

cldrn@cldrn: ~/projects/nmap/exp/calderon/scripts
File Edit View Terminal Help

```
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$ nmap --script http-google-email -p80 i
nsecure.org

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-14 22:29 PDT
Nmap scan report for insecure.org (74.207.254.18)
Host is up (0.11s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-google-email:
| nmap-dev@insecure.org
| nmap-svn@insecure.org
| soc@insecure.org
| fyodor@insecure.org
|_nmap-hackers@insecure.org

Nmap done: 1 IP address (1 host up) scanned in 24.63 seconds
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$ 
```

Figure 1. *Carving email addresses from a web page*



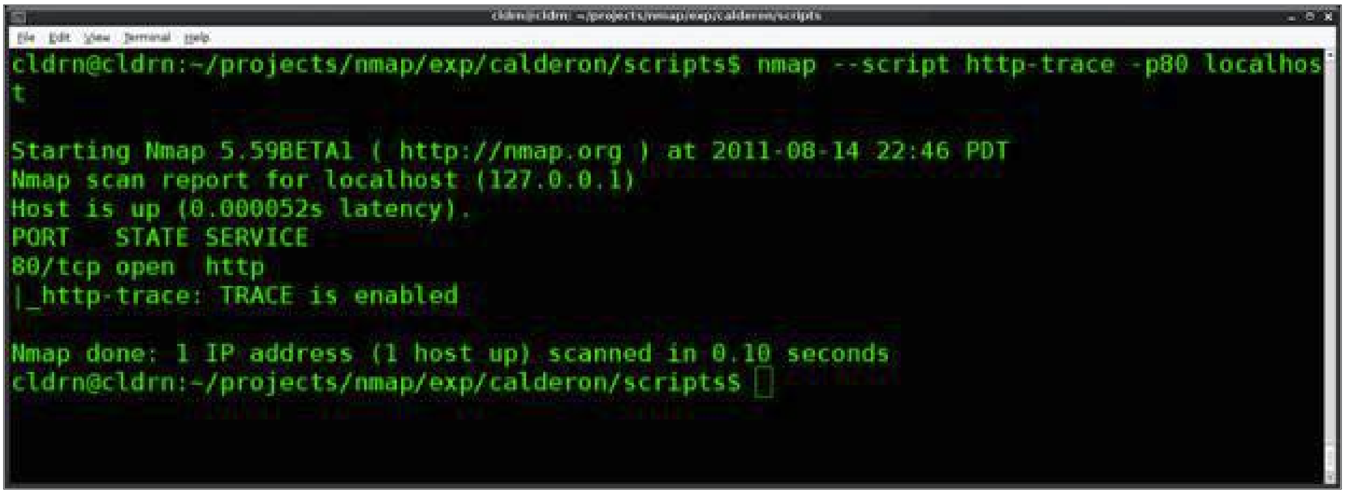
```
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$ nmap --script hostmap --script-args 'h
ostmap.prefix=hostmap--' -p80 74.207.254.18

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-14 22:21 PDT
Nmap scan report for 74.207.254.18
Host is up (0.11s latency).
PORT   STATE SERVICE
80/tcp open  http

Host script results:
| hostmap: Saved to hostmap--74.207.254.18
| nmap.org
| sectools.org
| insecure.org
|_seclists.org

Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$
```

Figure 2. *Discovering virtual domains hosted on the same IP*



```
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$ nmap --script http-trace -p80 localhos
t

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-14 22:46 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000052s latency).
PORT   STATE SERVICE
80/tcp open  http
|_http-trace: TRACE is enabled

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
cldrn@cldrn:~/projects/nmap/exp/calderon/scripts$
```

Figure 3. *Detecting a vulnerable server that uses the TRACE method*

are examples of scripts using search engines to gather valid user accounts and discover new attack points.

Email Account Harvesting with http-google-email

To find email addresses that could be used as valid usernames in web applications we use the script *http-google-email*. It queries Google Groups and Google Search to find public email accounts from the given host:

```
$nmap --script http-google-email
                    <host>
```

If we run this script against Nmap's *insecure.org* domain we obtain the following valid email accounts:

```
nmap-dev@insecure.org
nmap-svn@insecure.org
nmap-hackers@insecure.org
soc@insecure.org
fyodor@insecure.org
```

You need to consider the amount of queries allowed per hour because Google has strict policies about automated tools and if you go over this limit your requests will be blocked.

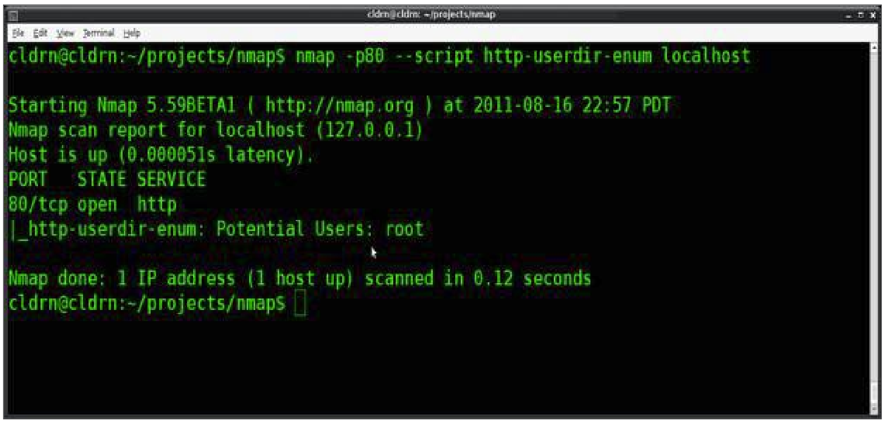
Discovering virtual domains with hostmap

The upcoming version of hostmap uses Bing results to try to list all hostnames pointing to the same IP address. This may reveal additional web applications and increase our attack surface since HTTP servers respond according to the hostname used in the requests:

```
$nmap --script hostmap <host>
```

To save hostmap's output in a separate file you can use the script argument `prefix`:

```
$nmap --script hostmap --script-args
                    hostmap.prefix=hostname_output_ <ip>
```



```
cldrn@cldrn:~/projects/nmap$ nmap -p80 --script http-userdir-enum localhost

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-16 22:57 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000051s latency).
PORT   STATE SERVICE
80/tcp open  http
|_http-userdir-enum: Potential Users: root

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
cldrn@cldrn:~/projects/nmap$
```

Figure 4. *Enumerating users with http-userdir-enum*

HTTP response analysis with Nmap

Widely used protocols are always at the mercy of the developers implementing it and HTTP is no exception. Specially crafted requests make web servers behave in its own way and this allow us to do some nifty tricks to fingerprint them.

Detecting HTTP TRACE

To check if a web server has the method 'TRACE' enabled you can use the script `http-trace`:

```
$nmap -p80 --script http-trace <host>
```

Listing user accounts with http-userdir-enum

If Apache's `mod_userdir` is enabled we can list valid usernames using the script `http-userdir-enum`:

```
$nmap -p80 --script http-userdir-enum <host>
```

Checking if web server is protected by a WAF/IPS

To determine if a web server is behind a web application firewall use the script http-waf-detect:

```
$nmap -p80 --script http-waf-detect --script-args=
  "http-waf-detect.uri=/testphp.vulnweb.com/artists.php,
    http-waf-detect.detectBodyChanges" www.modsecurity.org
```

Note that this script only detects products and configurations that alter the HTTP traffic.

Application discovery

When conducting a black box pentest we face the challenge of finding all the applications running on the web server. Fortunately for us, there are some Nmap NSE scripts for that too.

Enumerating common web applications

To enumerate common directories of web applications and many other interesting files:

```
$nmap --script http-enum -p80 <host>
```

http-enum detects a lot of popular web applications that are known to be vulnerable, it actually includes *exploit-db.com* 's archives of the last two years.

If you are lucky, it can even find an exact web application version or a vulnerability including its proof of concept.

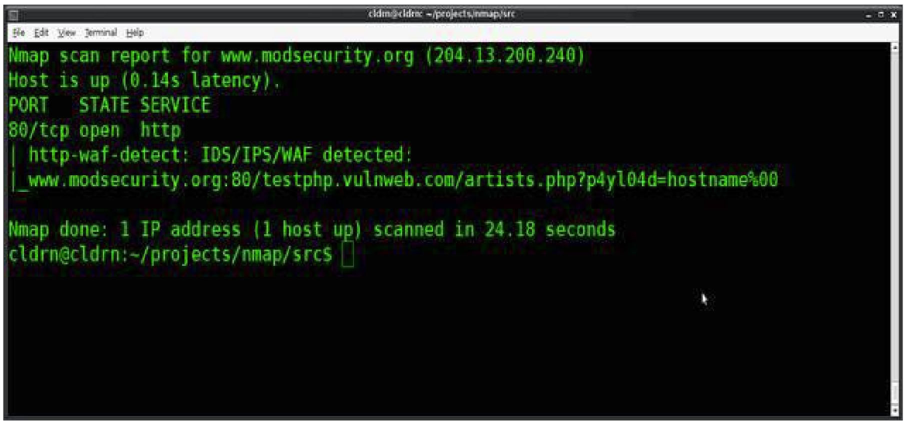
Getting robots.txt

To download r*obots.txt*'s entries with Nmap use the script *http-robots.txt:*

```
$nmap -p80 --script http-robots.txt
<host>
```

Robots.txt's entries will be displayed after *http-robots.txt.* In this case the web server returned:

```
/script-kiddies/
/h4x0rs/
/hackers/
```

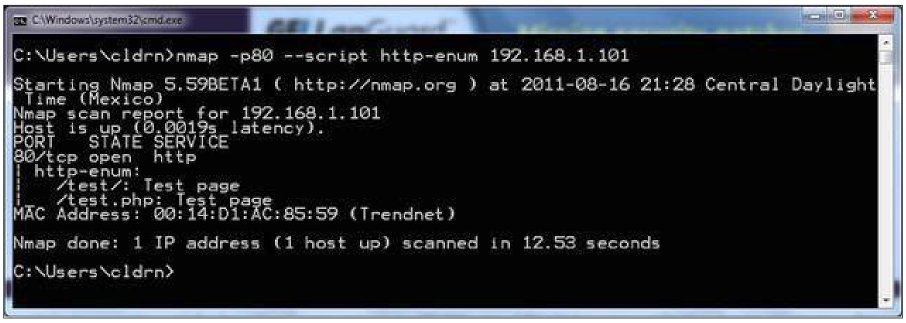


cldrn@cldrn: ~/projects/nmap/src
File Edit View Terminal Help

```
Nmap scan report for www.modsecurity.org (204.13.200.240)
Host is up (0.14s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.modsecurity.org:80/testphp.vulnweb.com/artists.php?p4yl04d=hostname%00

Nmap done: 1 IP address (1 host up) scanned in 24.18 seconds
cldrn@cldrn:~/projects/nmap/src$
```

Figure 5. *http-waf-detect checking if a Web Application Firewall is present*



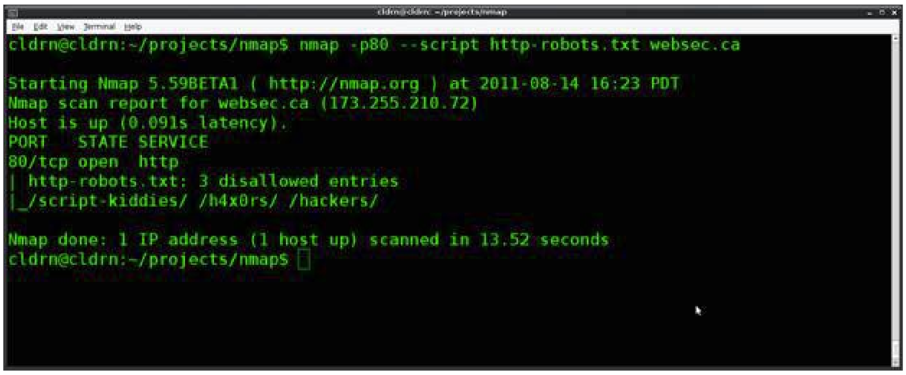
```
C:\Users\cldrn>nmap -p80 --script http-enum 192.168.1.101

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-16 21:28 Central Daylight
 Time (Mexico)
Nmap scan report for 192.168.1.101
Host is up (0.0019s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /test/: Test page
|   /test.php: Test page
MAC Address: 00:14:D1:AC:85:59 (Trendnet)

Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds

C:\Users\cldrn>
```

Figure 6. *Running Nmap's http-enum under Windows*



```
cldrn@cldrn:~/projects/nmap$ nmap -p80 --script http-robots.txt websec.ca

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-08-14 16:23 PDT
Nmap scan report for websec.ca (173.255.210.72)
Host is up (0.091s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-robots.txt: 3 disallowed entries
|_/script-kiddies/ /h4x0rs/ /hackers/

Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
cldrn@cldrn:~/projects/nmap$
```

Figure 7. *Displaying robots.txt entries*

Resources

- *http://nmap.org*
- *http://nmap.org/nsedoc/*
- *https://secwiki.org/w/Nmap/Script_Ideas*
- *https://secwiki.org/w/Nmap/Script_Vault*

Web Crawling And Nmap

Nmap's development team is working on a new spidering library that will allow script writers to create powerful utilities like:

- Cross Site Scripting Scanner
- SQL Injection Scanner
- RFI Scanner
- Backup Scanner
- Redirect Finder

You can find more information about this library and its progress at *https://secwiki.org/w/Nmap/Spidering_Library*.

Conclusion

I only showed you a small subset of the great scripts that are available. I encourage to go ahead and check out the complete list. People submit new scripts almost every week and the Nmap Scripting Engine is constantly being improved so you will be very happy if you keep an updated copy under your penetration testing toolbox.

PAULINO CALDERÓN

Paulino Calderón (@calderpwn) is a passionate software developer and penetration tester. He is one of the founders of WEBSEC[1] and works as the Director of IT Infrastructure. He is experienced in hardening, administering and pentesting IT infrastructures and web applications. He participated in Google's Summer of Code 2011 with the Nmap project as a NSE script developer. You can find his other open source contributions at his personal website [2].

[1] – http://websec.mx and http://websec.ca

[2] – http://calderonpale.com