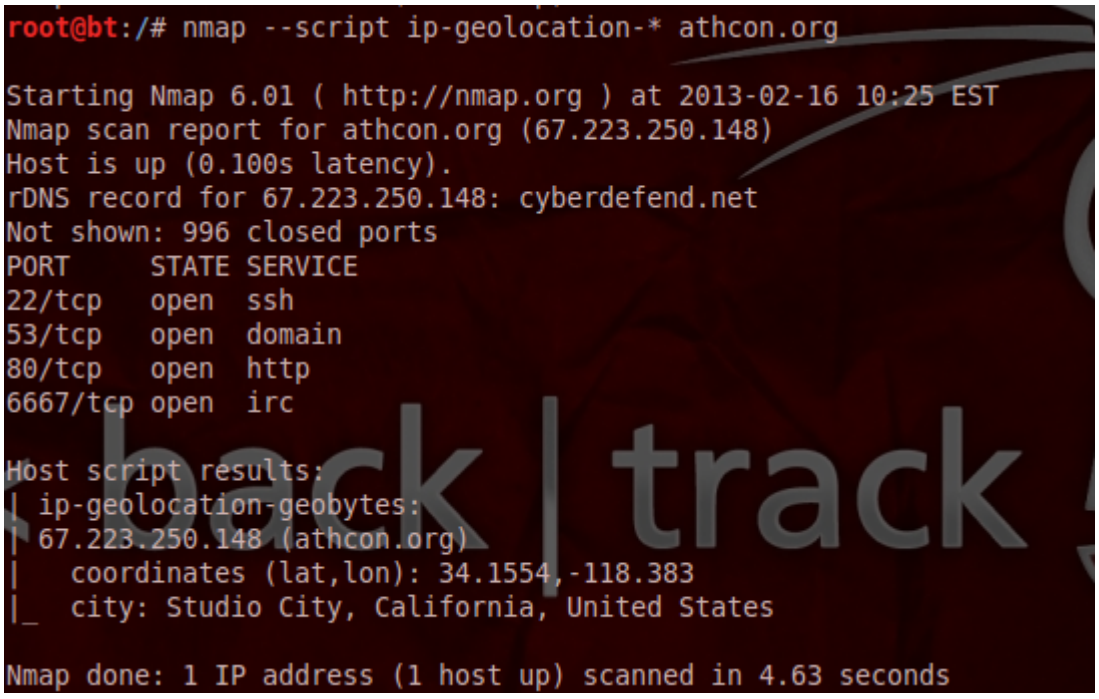
Information Gathering With Nmap

pentestlab.blog/category/information-gathering/page/3

February 16, 2013

Nmap is tool that can perform various activities in a penetration test.The function of NSE (Nmap Scripting Engine) and the scripts that have written so far they can transform Nmap to a multi purpose tool.For example we can use Nmap during the information gathering stage of a penetration test just by using the appropriate scripts.In this article we will examine those scripts and the information that we can extract.

One of our first steps it can be to determine the origin of the IP address that our client has given to us.Nmap includes in his database a couple of scripts for this purpose.If we want to run all these scripts we can use the following command as it can be seen in the image below:

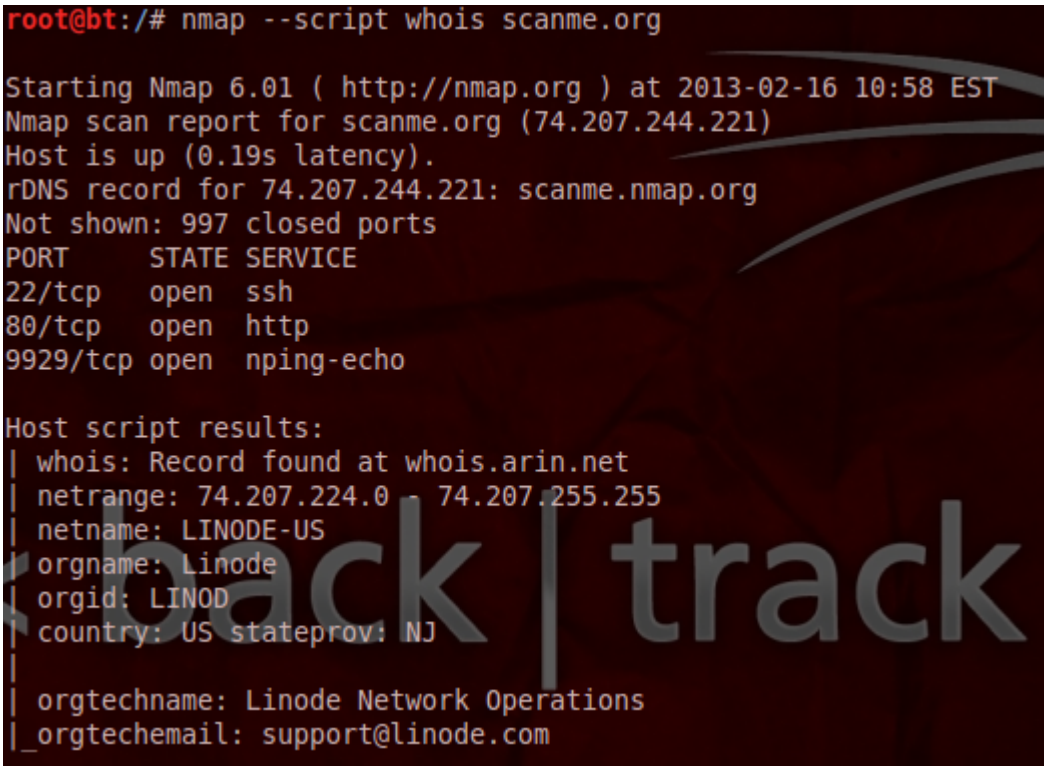


Nmap – IP Geolocation

As we can see the script called an external website (geobytes) in order to determine the coordinates and location of our target.

Whois

The command Whois can be run directly through the console in Linux environments.However there is a specific script for Nmap that performs the same job and it can be used.This script will return information about the registrar and contact names.



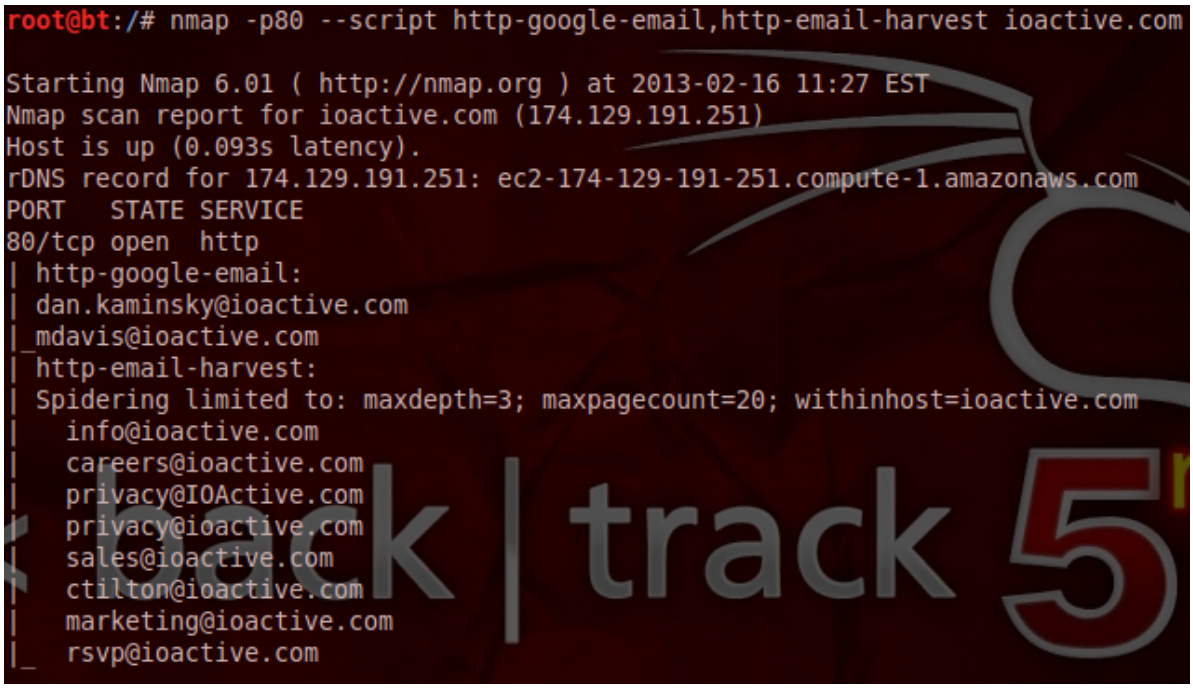
Nmap – Whois

Email Accounts

Email accounts can prove also important in a penetration test as it can be used as usernames,in social engineering engagements (i.e Phishing Attacks)or in a situation where we have to conduct brute force attacks against the mail server of the company.There are two scripts available for this job:

- http-google-email
- http-email-harvest

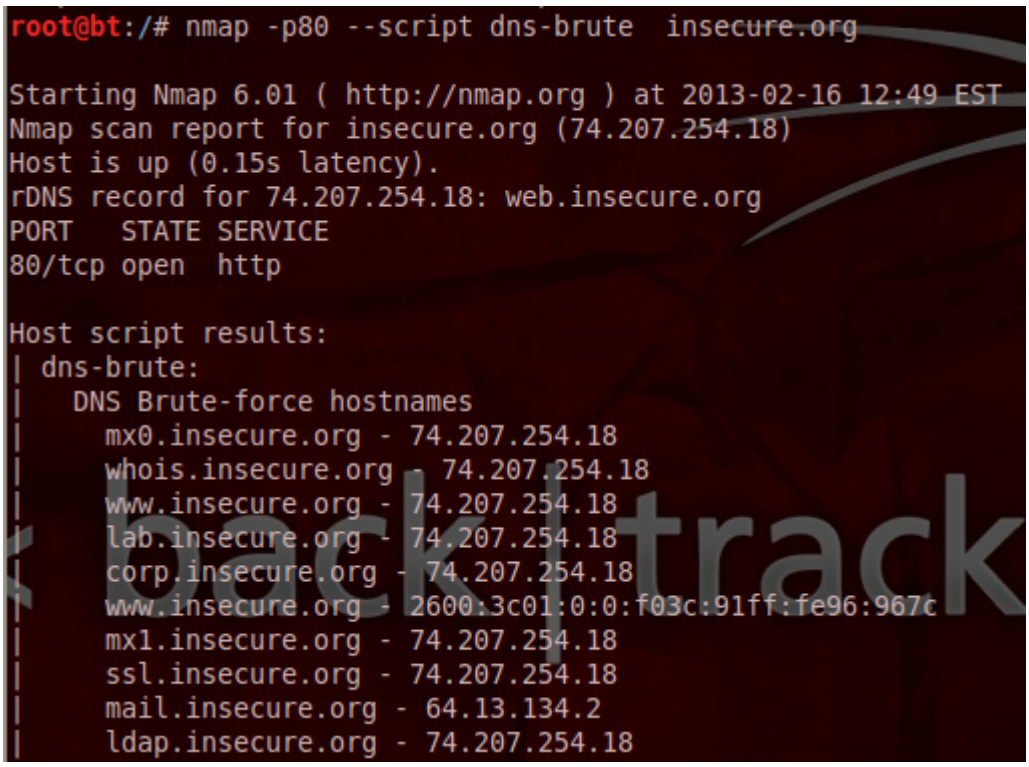
The http-google-email script uses the Google Web and Google Groups in order to search for emails about the target host while the http-email-harvest spiders the web server and extracts any email addresses that it discovers.The http-email-harvest is in the official repository of Nmap and the http-google-email script can be downloaded from here.



Nmap – Discover Email Accounts

Brute Force DNS Records

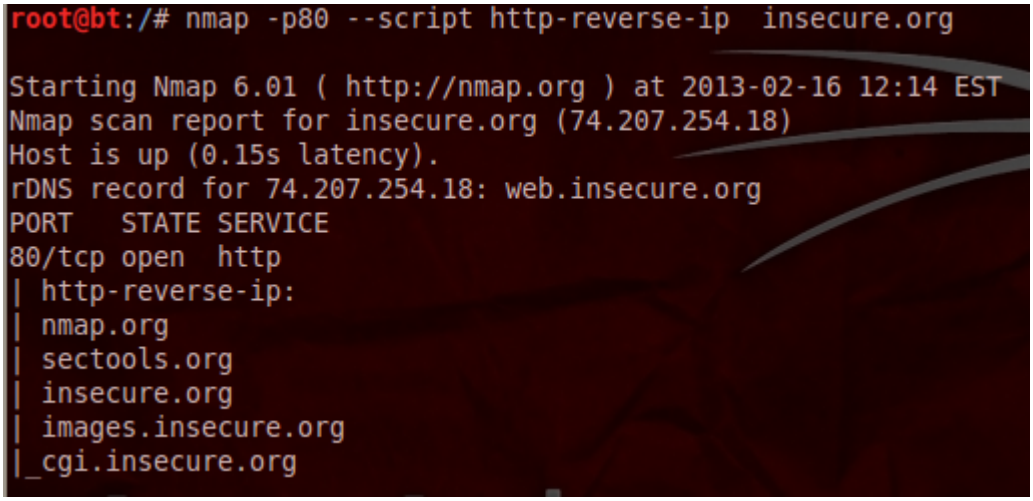
DNS records contains a lot of information about a particular domain which cannot be ignored.Of course there are specific tools for brute forcing DNS records which can produce better results but the dns-brute script can perform also this job in case that we want to extract DNS information during our Nmap scans.



Nmap – Brute Forcing DNS

Discovering Additional Hostnames

We can discover additional hostnames that are based on the same IP address with the nmap script **http-reverse-ip**.This script can help us to find other web applications that exist on the same web server.It is an external script that can be downloaded from here.



Nmap – Reverse IP

Conclusion

In this article we examined some Nmap scripts (internal and external) that can be used during the information gathering stage of a penetration test and before we start the actual scanning.The information that we have obtained proves that Nmap can perform almost any task with his scripts.If it cannot do something that you want then it is time to write your own Lua scripts and to contribute to the community.