NMAP and ZenMAP

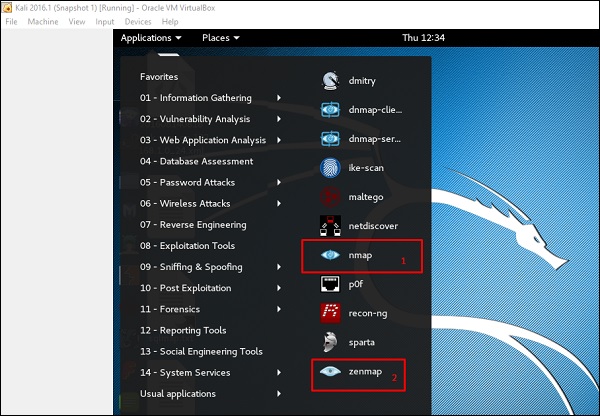
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Now, let’s go step by step and learn how to use NMAP and ZenMAP.

**Step 1** − To open, go to Applications → 01-Information Gathering → nmap or zenmap.

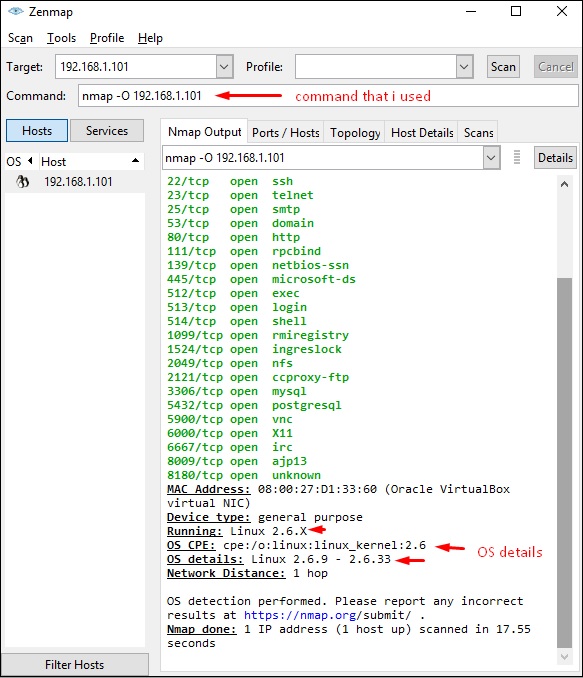


**Step 2** − The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable “-O”. For more information, use this link: <https://nmap.org/book/man-os-detection.html>

The command that we will use is −

nmap -O 192.168.1.101

The following screenshot shows where you need to type the above command to see the Nmap output −

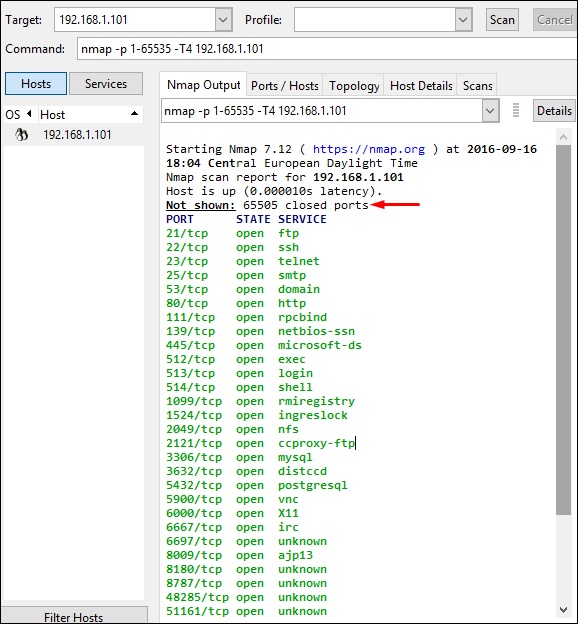


**Step 3** − Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command −

nmap -p 1-65535 -T4 192.168.1.101

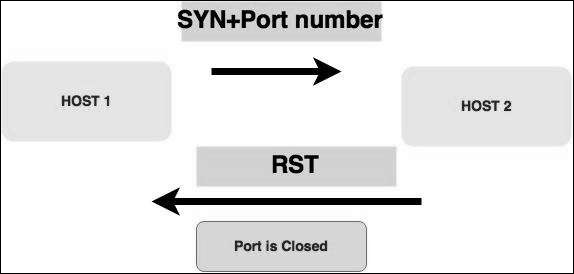
Where the parameter “–p” indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and “-T4” is the speed of scanning at which NMAP has to run.

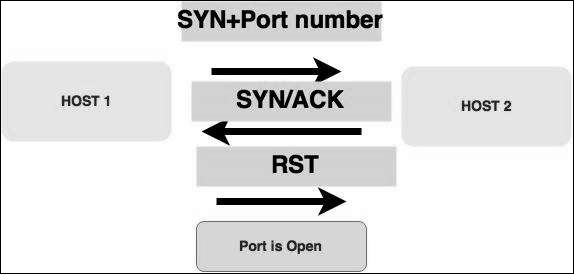
Following are the results. In green are all the TCP open ports and in red are all the closed ports. However, NMAP does not show as the list is too long.



Stealth Scan

Stealth scan or SYN is also known as **half-open scan**, as it doesn’t complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it’s assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn’t active or is closed.

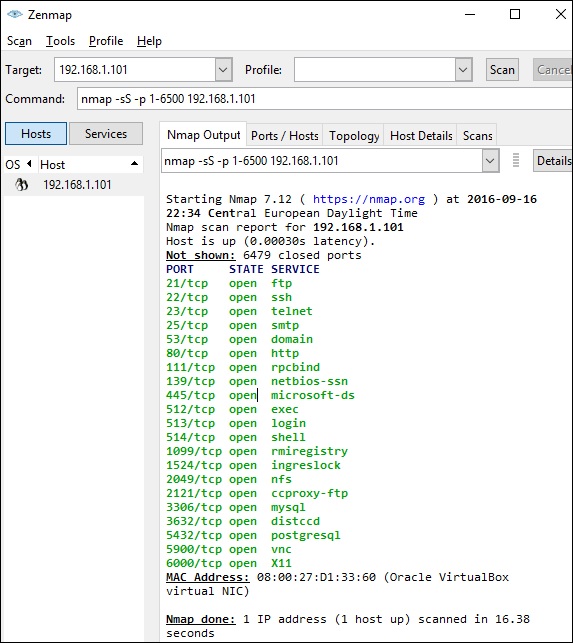




Now to see the SYN scan in practice, use the parameter **–sS** in NMAP. Following is the full command −

nmap -sS -T4 192.168.1.101

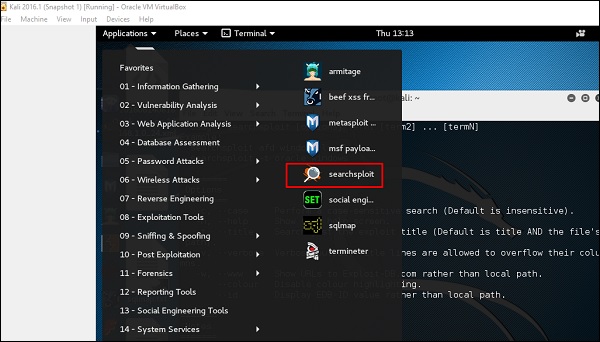
The following screenshot shows how to use this command −



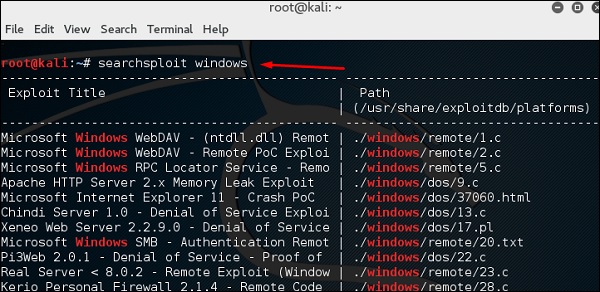
Searchsploit

Searchsploit is a tool that helps Kali Linux users to directly search with the command line from Exploit database archive.

To open it, go to Applications → 08-Exploitation Tools → searchsploit, as shown in the following screenshot.



After opening the terminal, type "**searchsploit exploit index name**".



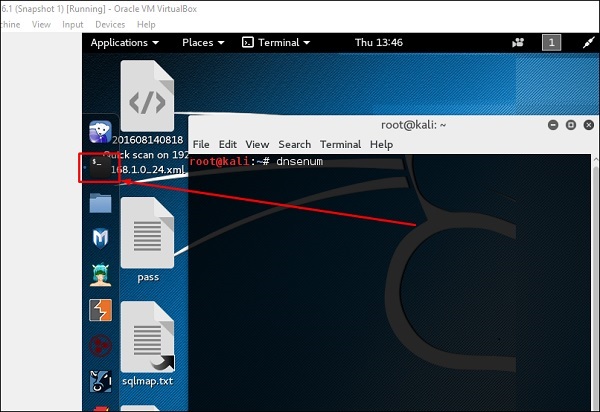
DNS Tools

In this section, we will learn how to use some DNS tools that Kali has incorporated. Basically, these tools help in zone transfers or domain IP resolving issues.

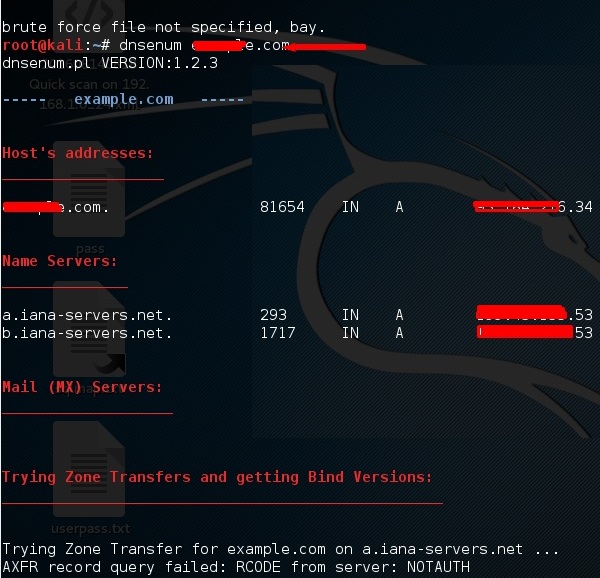
dnsenum.pl

The first tool is **dnsenum.pl** which is a PERL script that helps to get MX, A, and other records connect to a domain.

Click the terminal on the left panel.



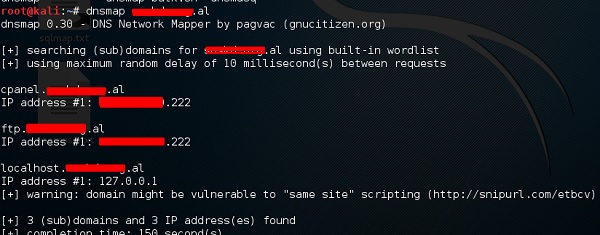
Type **“dnsenum domain name”** and all the records will be shown. In this case, it shows A records.



DNSMAP

The second tool is **DNSMAP** which helps to find the phone numbers, contacts, and other subdomain connected to this domain, that we are searching. Following is an example.

Click the terminal as in the upper section , then write **“dnsmap domain name”**



dnstracer

The third tool is **dnstracer**, which determines where a given Domain Name Server (DNS) gets its information from for a given hostname.

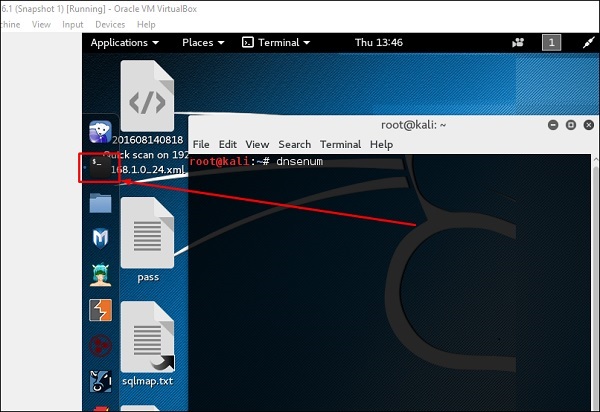
Click the terminal as in the upper section, then type **“dnstracer domain name”**.



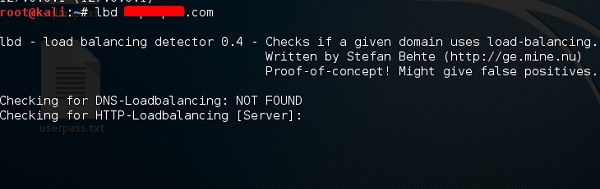
LBD Tools

LBD (Load Balancing Detector) tools are very interesting as they detect if a given domain uses DNS and/or HTTP load balancing. It is important because if you have two servers, one or the other may not be updated and you can try to exploit it. Following are the steps to use it −

First, click the terminal on the left panel.



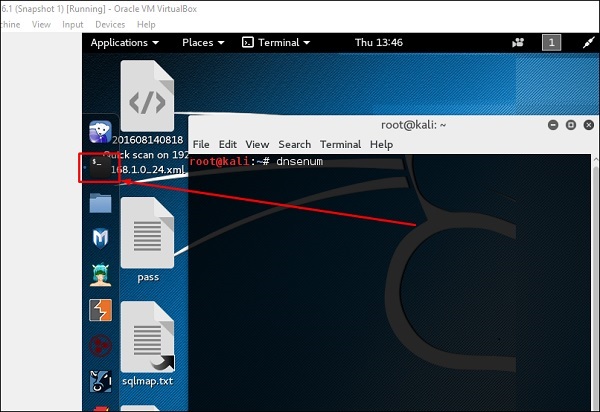
Then, type **“lbd domainname”**. If it produces a result as “FOUND”, it means that the server has a load balance. In this case, the result is “NOT FOUND”.



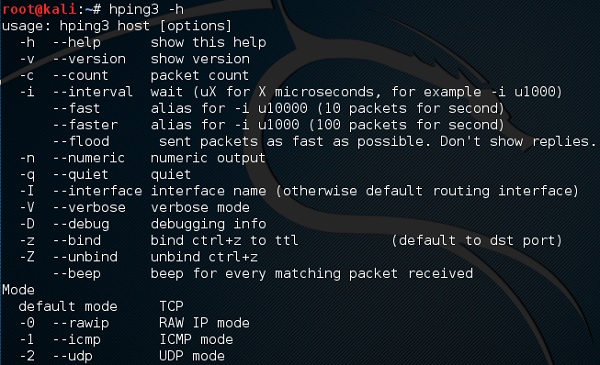
Hping3

Hping3 is widely used by ethical hackers. It is nearly similar to ping tools but is more advanced, as it can bypass the firewall filter and use TCP, UDP, ICMP and RAW-IP protocols. It has a traceroute mode and the ability to send files between a covered channel.

Click the terminal on the left panel.



Type **“hping3 –h”** which will show how to use this command.



The other command is **“hping3 domain or IP -parameter”**

