https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
http://knoxd3.blogspot.com/2013/06/how-to-use-dnsrecon-in-kali-linux.html
https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
http://tools.kali.org/tools-listing

apt-get install nmap dnsrecon dnsenum

0. Generalne info - wszystko w jednym: nmap -A 172.16.8.129
1. Otwarte porty: map —top-ports 10 172.16.8.129
2. Informacje o systemie: nmap -v -O —osscan-guess 172.16.8.129
3. Wersje uruchomionych serwisów: map -sV 172.16.8.129
4. Najczęściej używane porty TCP: nmap -sA 172.16.8.129
5. Najczęściej używane porty UDP: nmap -sU 172.16.8.129
6. Sprawdza dziury w zaporze: nmap -sX 172.16.8.129
7. Sprawdza DNS na serwerze: dnsrecon -d google.com -t std —xml plik.xml
8. DNSy: dnsenum —noreverse -o plik.xml google.com
9. Przeskanuj wszystkie porty: nmap -p- 172.16.8.129
10. Czy jest podatny na atak UDP DDOS: nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr
11. Tytuły stron opartych na HTTP: nmap —script=http-title 172.16.8.129
12. Headery serwisów HTTP: nmap —script=http-headers 172.16.8.129
13. Sprawdzanie czy ma bezpieczne SSL (Heartbleed test): nmap -sV -p 443 —script=ssl-heartbleed 172.16.8.129
14. Sprawdzanie jakie domeny maja ip z przedziału: dnsrecon -r 172.16.8.129 172.16.8.130