Nmap Cheatsheet

Here is the list of most popular nmap commands that Dhound team use.

This cheatsheet first of all for us during security analysis, but you can also find here something interesting.

If you run nmap on linux, don't forget to run it with root permissions.

Port scanning

- Quick scan

  nmap -Pn dhound.io

- Full TCP port scan using with service version detection

  nmap -p 1-65535 -Pn -sV -sS -T4 dhound.io

- Scan particular ports

  nmap -Pn -p 22,80,443 dhound.io

- Find linux devices in local network

  nmap -p 22 --open -sV 192.168.10.0/24

Trace traffic

- Trace trafic

  nmap --traceroute -p 80 dhound.io

- Trace trafic with Geo resolving

  nmap --traceroute --script traceroute-geolocation.nse -p 80 dhound.io

Get Ip Info

- ISP, Country, Company

  nmap --script=asn-query dhound.io

Test SSL

- Get SSL Certificate

  nmap --script ssl-cert -p 443 -Pn dhound.io

- Test SSL Ciphers

  nmap --script ssl-enum-ciphers -p 443 dhound.io

Brute Force

- Ftp Brute force

  nmap --script ftp-brute --script-args userdb=users.txt,passdb=passwords.txt -p 21 -Pn dhound.io

- HTTP Basic Authentication Brute force

  nmap --script http-brute -script-args http-brute.path=/evifile-bb-demo,userdb=users.txt,passdb=passwords.txt -p 80 -Pn dhound.io

- Wordpress Bruteforce

  nmap -sV --script http-wordpress-brute --script-args userdb=users.txt,passdb=passwords.txt,http-wordpress-brute.hostname=dhound.io,http-wordpress-brute.threads=10 -p 80 dhound.io

- SSH Brute Force

  #use other tools like ncrack

Attacks

- Find vulnerabilities in safe mode

  nmap --script default,safe -Pn dhound.io

- Find vulnerabilities in unsafe mode

  nmap --script vuln -Pn dhound.io

- Run DDos attack

  nmap --script dos -Pn dhound.io

- Exploit detected vulnerabilities

nmap --script exploit -Pn dhound.io