FOOT PRINTING

Date .....

N-MAPS.

- One of the most basic tools for exploiting the services.

ZEN MAP :- Graphical version (GUI) of N-map
Less used.

nmap -h → nmap help.

Take IP from nmap.org (Domain), nirsoft.net.
↳ Major ip blocks.

Copy 1 IP. (Randomly, but yours proxy country preffered)

Type on DDG → who is IP

Use nslookup _ IP.
↳ Gives domain
nslookup _ domain
↳ Gives IP.

nmap Scanme.nmap.org.

Date .....

→ Get your own subnet of IP Address.
Use ifconfig.

Get the range of inet.

use → nmap -oG - 192.168.1.0-255
Generally.

-p 22 -vv > /home/SCAN
Port no. you wish to Scan
Redirect

Open SCAN file using less or cat.

cat SCAN | grep Up
To print lines with word UP.
↳ To check hosts alive.

cat SCAN | grep Up | awk -f " " '{print $2}'
Good command

JAN 2020

sun	mon	tue	wed	thu	fri	sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Date

awk command → awk -f " " '{print $2}'
Delimeter
Printing 2nd thing of each line (IP addr).

Usage:- cat SCAN | grep Up | awk -f " " '{print $2}' > ALIVEHOSTS.

Now, Alive hosts contains only IP(s) of all available open ports (Up).

for exploiting more vulnerabilities,

→ nmap.org/nsedocs.

→ exploitdb.com