

Foot PRINTING

JK Cement LTD.

JK SUPER
CEMENT
BUILD SAFE

JK SUPER
STRONG
BUILD SAFE

JK SUPER
STRONG
BUILD SAFE
Weather Shield

JK
WHITE
CEMENT
PERFECT WHITE

JK CEMENT
WallMaxX
White Cement Based Putty

Date

N-MAPS.

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

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

`nmap -h` → `nmap help`.

Take IP from `nmap.org`, `microsoft.net`.
↳ Major IP blocks.
Domain

Copy 1 IP. (Randomly, but your proxy country preferred)

Type on DDG → who is IP

Use `nslookup - IP`.

↳ Gives domain

`nslookup domain`

↳ Gives IP.

`nmap Scanme.nmap.org`.

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	



JK CEMENT
ShieldMaxX
Universal Waterproof Putty

JK CEMENT
GypsoMaxX
Premium Gypsum Plaster

JK CEMENT
TileMaxX
Premium Adhesives and Grouts

JK CEMENT
PrimaxX
White Cement Based Primer

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
↓
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 \$1}'
↓
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}'
 Delimiter
 ↓
 Printing 2nd thing of each line (IP address).

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/nse/docs.

→ exploitdb.com

FEB							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	

