Exp NO: 8 | Experimat on Outliving the procedes in
DOTE: 11.09.25 | NMAP before port scanning to find offline system

AIM:

To attempt to port scan offline systems and recognize the wante time and the created unneeded network (because it is active recon)

The ARP Scan:

This scan uses ARP requests to discover live hosts 3.

ICMP Scan:

This scan uses ICMP requests to identify live hosts 3.

There will be 2 scanners introduced:

1) arp-scan
2) nmap scan

NMAP (network mapper) It is a well known tool for mapping networks, locating live hosts and detecting running services. NMAP's scripting engine can be used to extend it capabilities such as finger printing services and exploiting flaws. The scans typically follow the steps represented in the image below, but several are optional and are conditional on the "command-line" options pro

step 1 : Enumerate the targets
step 2 : Discover live hosts
step 3 : Reverse DNS lookup
step 4 : Scan ports
step 5 : Detect versions
step 6 : Detect OS
step 7 : traceroute
step 8 : scripts
step 9 : Write output

Result: Hence the experiment- an outline
The proven in NMAP port scanning
is done successfully

Exp No: 9

Aim :-
To im
simulator.
Closedun
for no
for subn
mocks
Con
Subnets.
have
need
Step
(i) C
(ii) A
(iii)
To
R