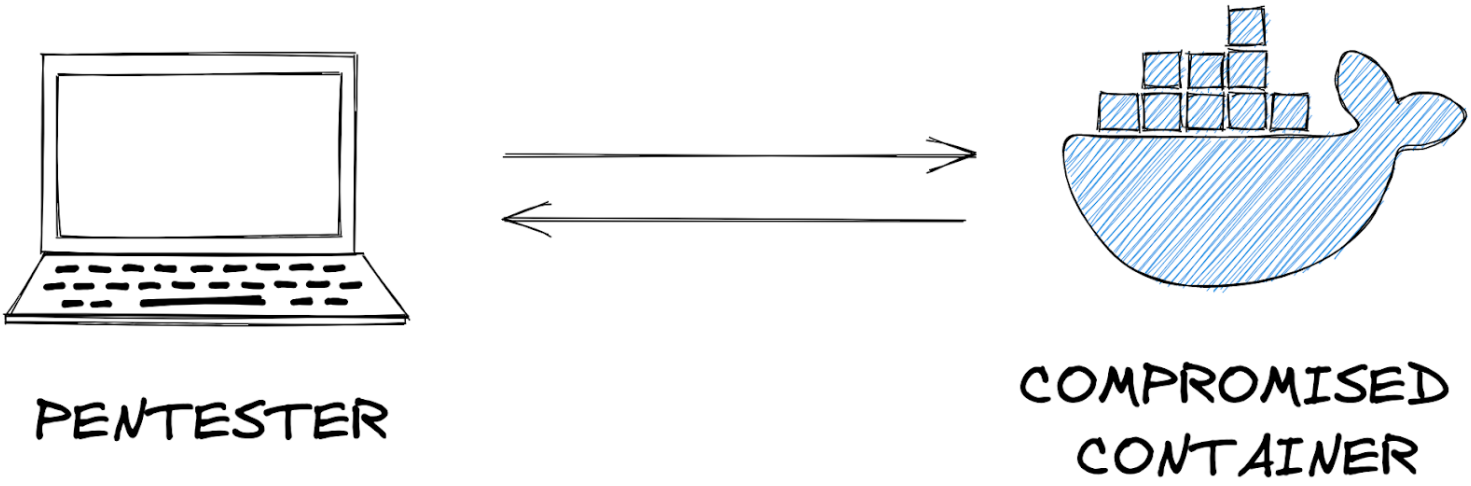
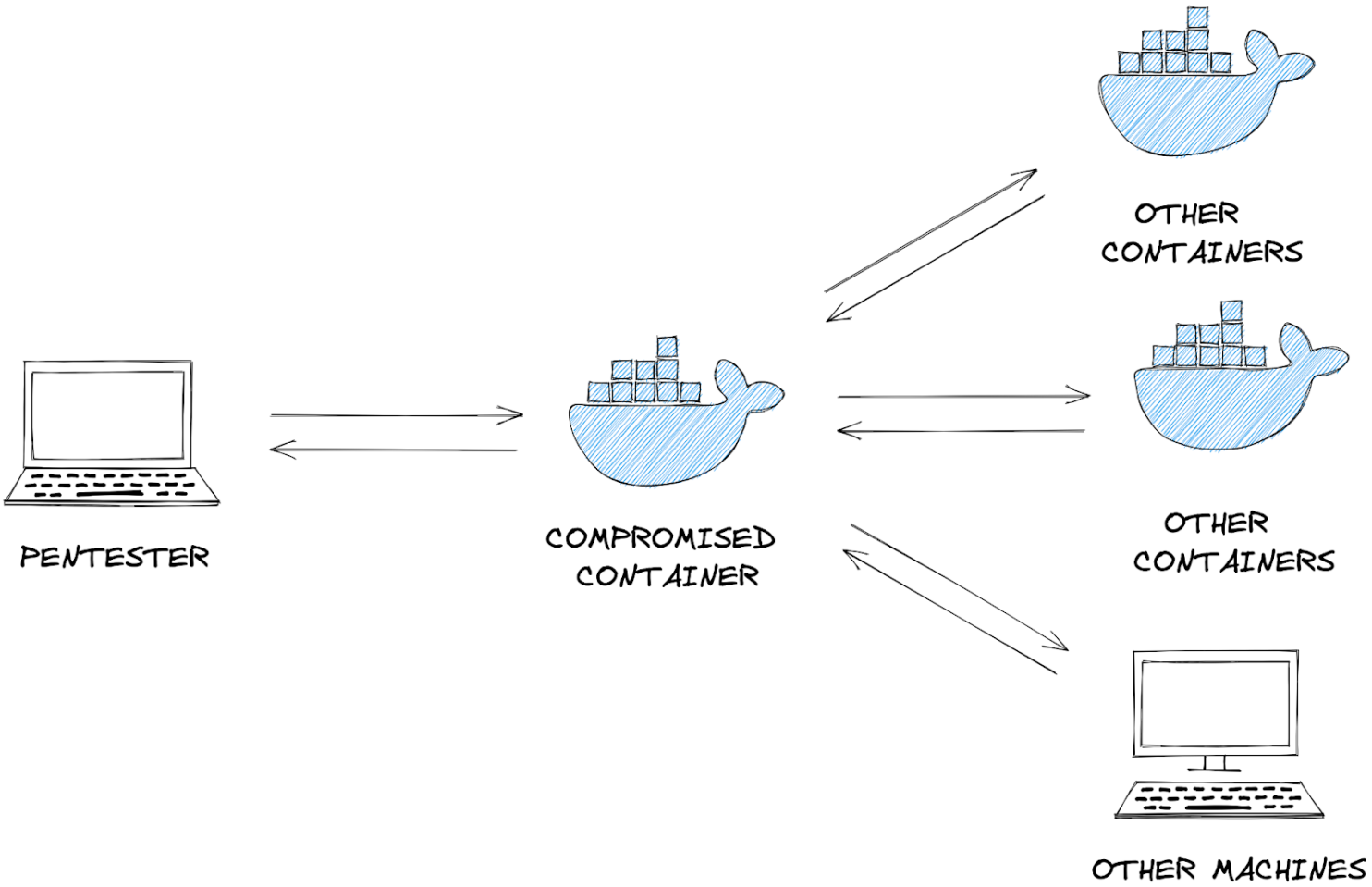
Pivoting

What is Pivoting?
Once an attacker gains initial entry into a system, the compromised machine can be used to send additional web traffic through - allowing previously inaccessible machines to be reached.
For example - an initial foothold could be gained through a web application running in a docker container or through an exposed port on a Windows machine. This system will become the attack launchpad for other systems in the network.



We can route network traffic through this compromised machine to run network scanning tools such as `nmap` or `arp` to find additional machines and services which were previously inaccessible to the pentester. This concept is called network pivoting.



NOTE this pivoting lesson applies to real machines too, not only Docker.

==========

Proxychains

• If a tool in Linux does not natively support an option for using a socks proxy, ProxyChains can intercept the tool's request to open new network connections and route the request through a socks proxy instead. For instance, an example with Nmap:
proxychains -q nmap -n -sT -Pn -p 22,80,443,5432 MACHINE_IP

==========

You need to Edit your **/etc/proxychains4.conf** file and make the following changes
(NOTE as indicated by the name of the tool you can add as many proxies in your conf folder as you would like just go down one line and add your proxy)

1. Scroll all the way to the bottom
2. Change your proxy whether socks4a or socks5(newer) depending on what version is listening in metasploit.
3. Set your proxychains to use the port that Metasploit will be listening on (you can tell if you show options on the socks_proxy auxiliary module)

4. Set the IP address that Metasploit will be listening on too so that it can redirect your traffic.

==========

Metasploit in Pivoting

Using Meterpreter to pivot
Metasploit has an internal routing table that can be modified with the `route` command. This routing table determines where to send network traffic through, for instance, through a Meterpreter session. This way, we are using Meterpreter to pivot: sending traffic through to other machines on the network. NOTE this doesn't allow other tools on the Linux system to route the traffic through metasploit... {if you would like to acheive routing traffic from a tool on Linux to your target (which may be an internal machine that you don't have access to) you should use the socks_proxy module in metasploit described below in section 2.} after you use this auxiliary module you can use proxychains to route your traffic to metasploit which then will rout it to your target through the shell that you have opened on your initial compromised machine BUT first you have to edit your /etc/proxychains4.conf see Proxychains page to see what needs to be changed.

Note that Meterpreter has a separate route command, which is not the same as the top-level Metasploit prompt's route command described below. If you are currently interacting with a Meterpreter session, you must first `background` it.
Examples:
1. ==========

```
# Example usage route [add/remove] subnet netmask [comm/sid]
route [add/remove] subnet netmask [comm/sid]


# Configure the routing table to send packets destined for 172.17.0.1 to the latest opened session route add 172.17.0.1/32 -1
route add 172.17.0.1/32 -1


# Configure the routing table to send packets destined for 172.28.101.48/29 subnet to the latest opened session route add 172.28.10.48/29 -1
route add 172.28.10.48/29 -1

# Output the routing table route print
route print
```

2. ==========

In Metasploit, to open a socks proxy use `auxiliary/server/socks_proxy` module:

```
use auxiliary/server/socks_proxy

run srvhost=127.0.0.1 srvport=9050 version=4a
```

OR **5**

3. ==========
At the END metasploit will be able to route traffic to an internal target machine hiding THROUGH a machine you have compromised.

==========

Socks Proxy

Socks Proxy

A socks proxy is an intermediate server that supports relaying networking traffic between two machines. This tool allows you to implement the technique of pivoting. You can run a socks proxy either locally on a pentester’s machine via Metasploit, or directly on the compromised server.
There's 2 versions of a socks proxy socks4a which is the older one and socks5

==========
• Tools such as `curl` support sending requests through a socks proxy server via the `--proxy` flag:
curl --proxy socks4a://localhost:9050 http://MACHINE_IP

==========

Docker

A common way to tell if a compromised application is running in a Docker container is to verify the existence of a file at the root directory of the filesystem.

Note that the will contain the HOST that's running docker IP address.
==========
Also laravel uses the **.env** file to store configurations for their system and they save some environment variables for laravel to run with.

==========