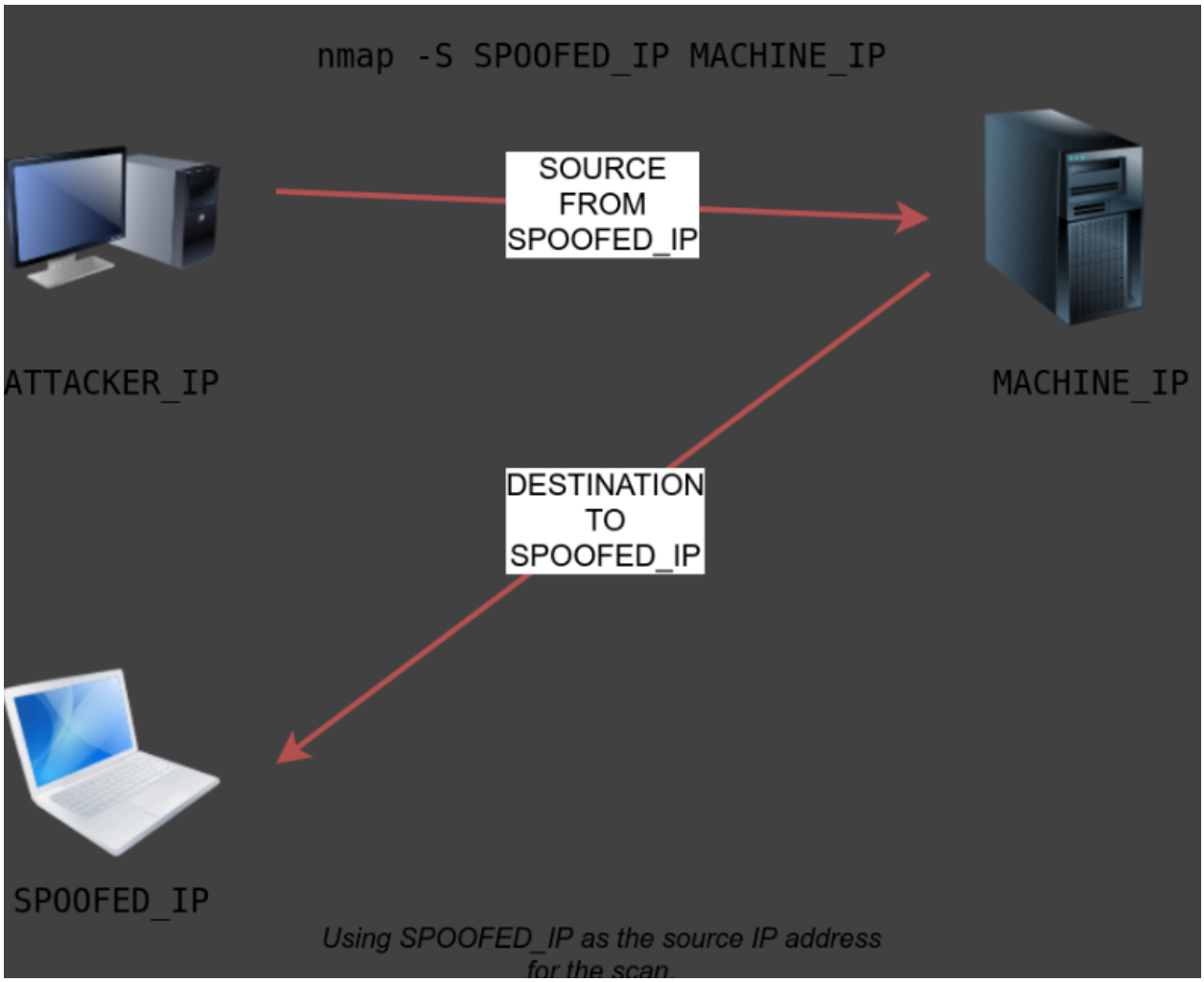
Nmap Spoofing/Decoys

In some network setups you will be able to scan a target system using a spoofed IP address and even a spoofed MAC address. Such a scan is only beneficial in a situation where you can guarantee to capture the response.

If you try scan a target from some random network using a spoofed IP address, chances are you won't have any responses routed to you, also the results could be unreliable.

Use the command = nmap -S 10.10.149.1
This will launch a spoof command. Nmap will craft all the packets using the provided source IP address (spoofed IP). the target machine will respond to the incoming packets sending the replies to the destination IP address (spoofed IP). For this scan to work and give accurate results.
Attacker needs to monitor the network traffic to analyse replies.



3 Steps:

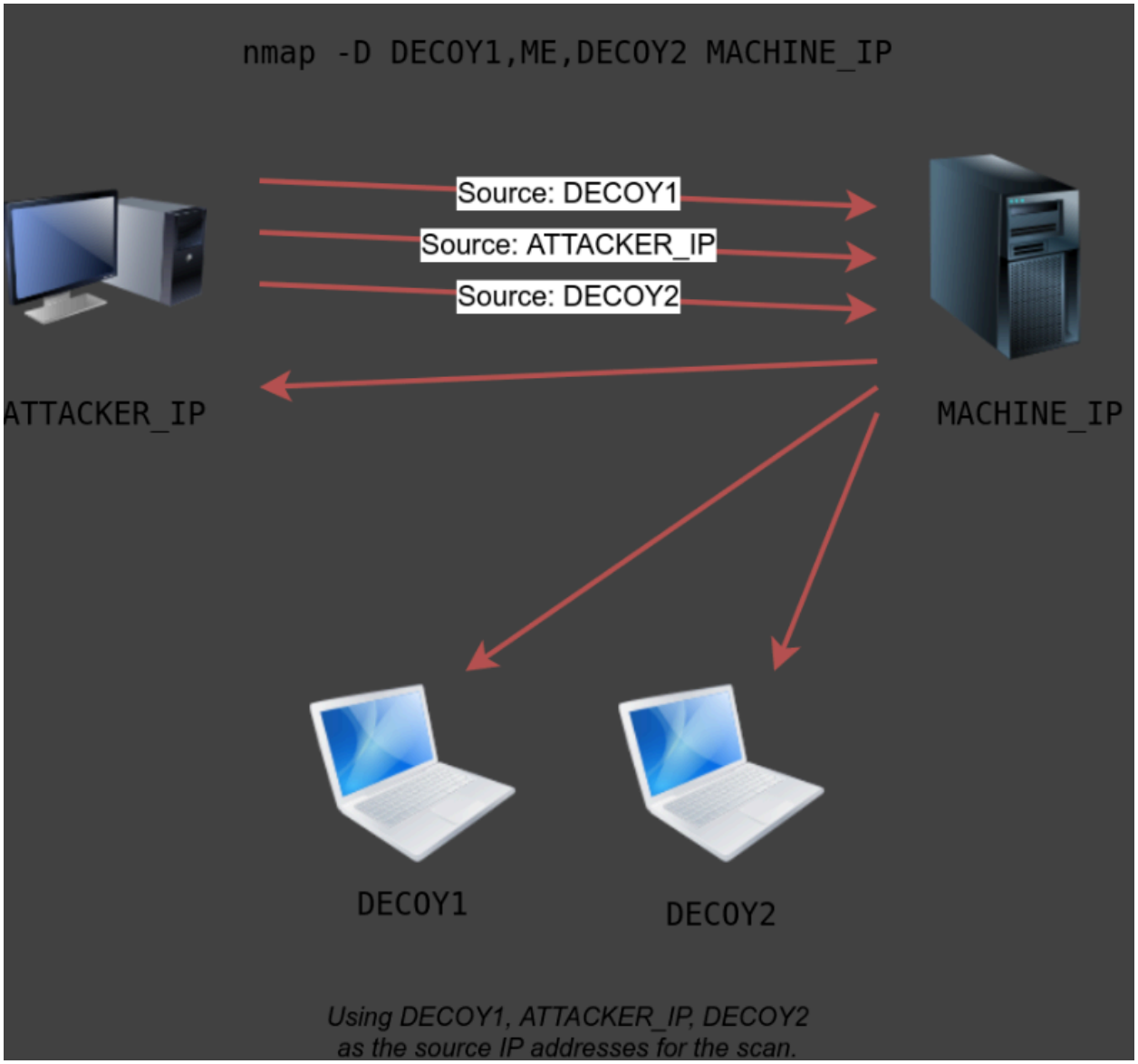
1. Attacker sends packet with spoofed source IP to target machine
2. Target machine replies to spoofed IP as destination
3. Attacker captures the replies to figure out open ports

You expect to specify the network interface using **-e** and explicitly disable ping scan **-Pn** therefore.
You will need **nmap -e NET_INTERFACE -Pn -S SPOOFED_IP** to tell Nmap explicitly which network interface to use and not to expect a ping reply. This scan is useless if repeated, if the attacker system cannot monitor the network for responses.

When using the same subnet as the target machine you would be able to spoof your MAC address too. By doing **–spoof-mac SPOOFED_MAC.** Is possible only if the attacker and the target machine are on the same ethernet (802.3) or wifi (802.11) network.

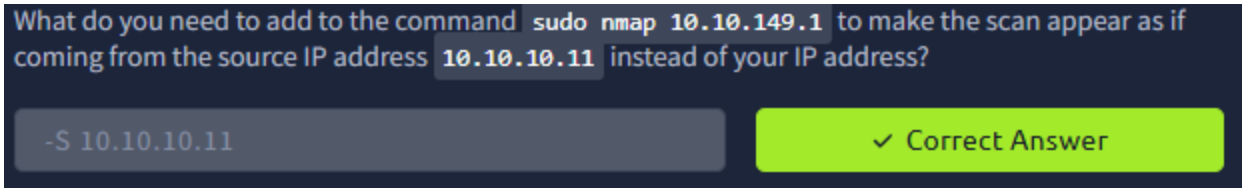
Spoofing only works in a minimal number of cases where certain conditions are met. So the attacker may resort to using decoys. Which makes it more challenging to be pinpointed. How do do this?

Make the scan appear to be coming from multiple IP addresses so the attackers IP would be lost amongst them. EG, the image shows the scan coming from 3 devices.

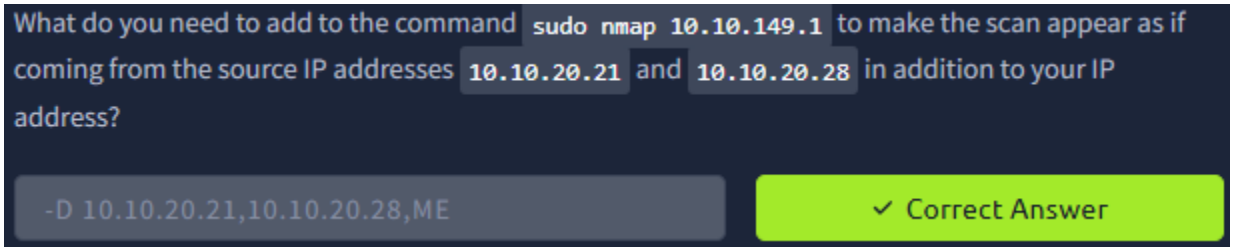


You can launch a Decoy scan from a specific or random IP after **-D** to achieve this.
nmap -D 10.10.0.1,10.10.0.2,ME 10.10.149.1 This will make the scan appear as if it is coming from 10.10.0.1 and 10.10.0.2 and **ME** indicates our IP, alternatively we could automatically randomise the IP by doing this:
nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME 10.10.149.1. This means each time you execute the command, you would expect 2 new random IP addresses to be in the 3rd and 4th decoy sources.

Questions:



-S will craft all the packets to the spoofed IP address, in this case changing our IP of 10.10.149.1 to answer on 10.10.10.11 spoofed IP.



-D = Decoy followed by the 2 decoy addresses we are using, 10.10.20.21 and 10.10.1-20.28 and then followed by ME which would be our own address. But every time we enter this command, it would have to be processed by the decoys first making it harder to track our own IP within.

Conclusion:
So I now understand the importance of stealth attacks, but also ensuring we remain anonymous when/if the defenders come looking it is much harder to identify us, especially if we use decoys as well as randomising the IPs each time makes it very difficult to trace the traffic back to us. Of course it is still possible, but the idea of making it difficult to mitigate the risk of being found!