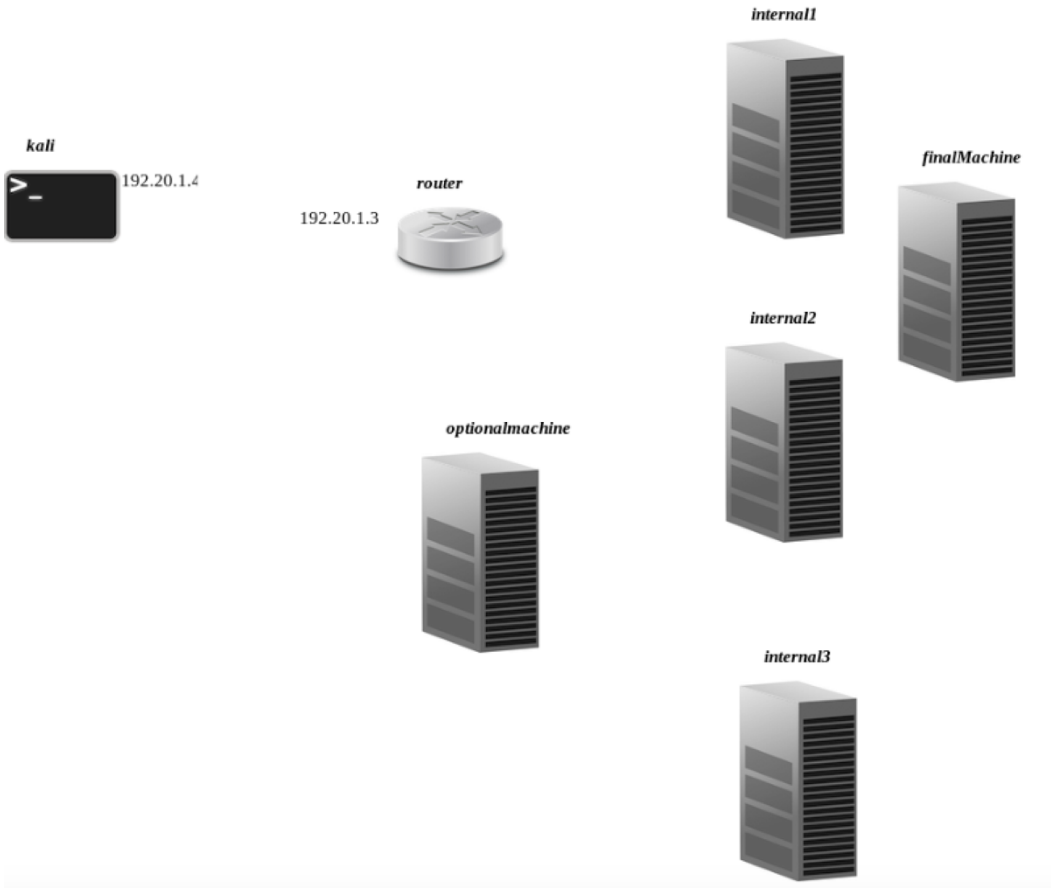
# Hack the Whale Reloaded!

*Mama put my guns in the ground*
*I can't shoot them anymore*
*That cold black cloud is comin' down*
*Feels like I'm knockin' on heaven's door*
*Knock-knock-knockin' on heaven's door*
*Knock-knock-knockin' on heaven's door*
*Knock-knock-knockin' on heaven's door*
*Knock-knock-knockin' on heaven's door...*

This lab is going to be a tough one, so calm down, pour your own coffee and roll up your sleeves!

Here is the scenario:



As you can see in the picture, you'll be sitting behind the "Kali" machine display, facing the target network. The only thing that you know is that you can reach the target through the Internet. You do not even know what set of IP addresses corresponds to the target network's hosts.

So, what action would you take, if you were a real hacker? You'd certainly start with the canonical path: *scanning* and *enumeration*[1]. If you want to access a nice survey of the mentioned techniques, a handy academy-style resource is freely available here:

https://booksite.elsevier.com/samplechapters/9781597496278/Chapter_3.pdf

In terms of tools, you're certainly going to rely on things like:

- *Nmap:* https://nmap.org/
- *Netcat* (the TCP/IP swiss army knife): http://nc110.sourceforge.net/

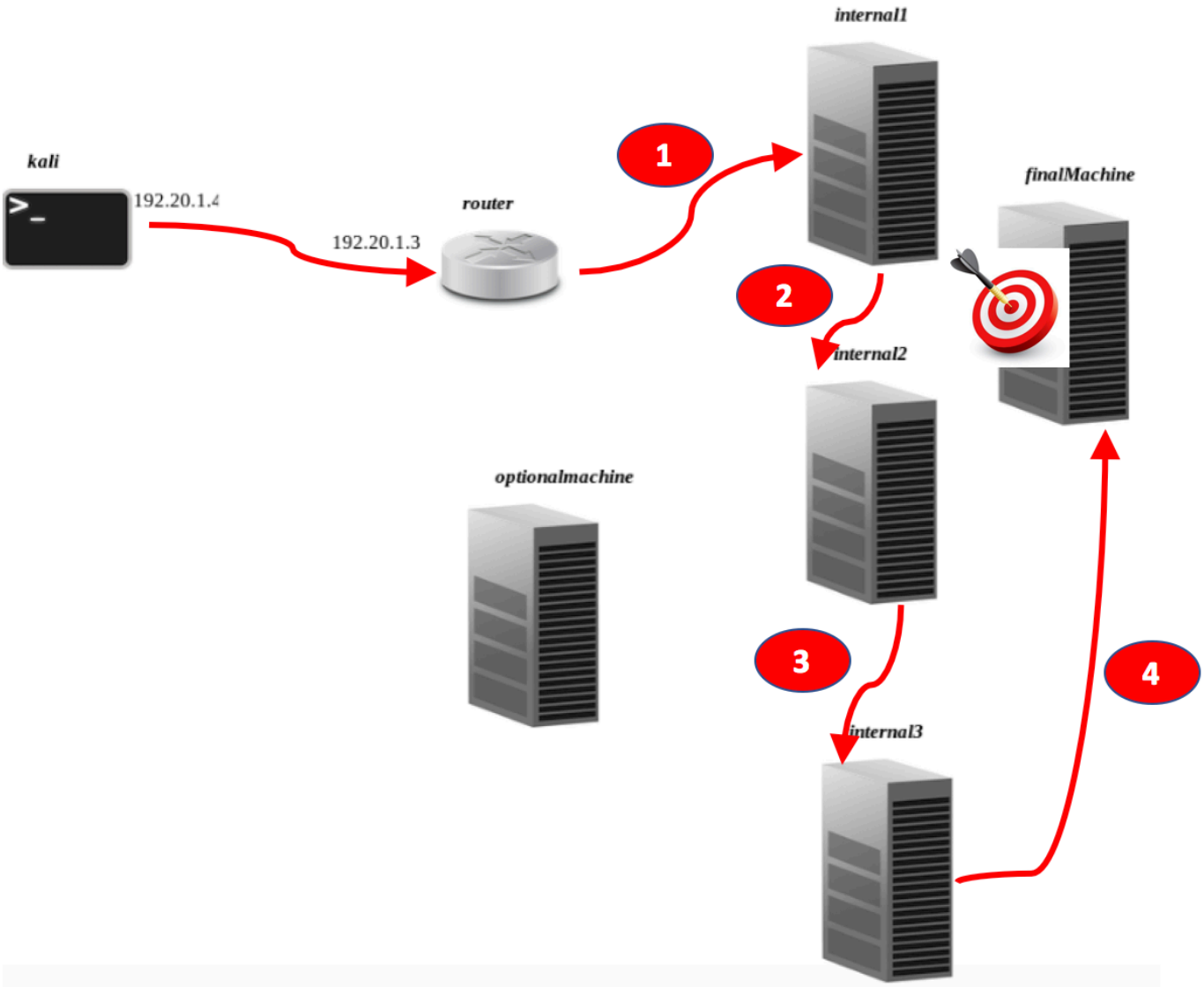
With the help of those tools, once discovered the target subnet address, you can start investigating about the hosts that are up and running, as well as the services they expose. Though, please be warned that we've been harsh when we created this lab! So, **you should not give for granted that if you don't discover a specific service on one of the nodes, that service will never be activated on that node**. The previous sentence will become clearer in a while, believe us.

Indeed, the whole lab has been organized around a well-defined sequence of actions that the wannabe hackers should entail in order to capture that damned flag! If you were real hackers, discovering that sequence would be part of your job. But you're not real hackers, aren't you?! So, today we're giving you a hand and make your life easier. First off, please notice that the target machines have been properly labeled in order to allow you to clearly identify the required hacking sequence. Namely, the final target will obviously be the machine that is called (guess what?) ***finalMachine.*** There's no point in starting directly from there, though. Actually, before being capable of attacking that node, you will be forced to gather precious pieces of information from the other hosts residing on the target network. We have configured "finalMachine" in such a way as to accept properly formatted requests for spawning a remotely exploitable service on the machine itself. This has been done by leveraging the well-known **port knocking** technique (https://en.wikipedia.org/wiki/Port_knocking). The ports you'll have to knock[2] are three and you'll find them on the nodes labeled, respectively, **internal1**, **internal2** and **internal3.**

So, the picture below gives you an idea of the hacking path you'll have to follow if you want to successfully arrive at the final target:

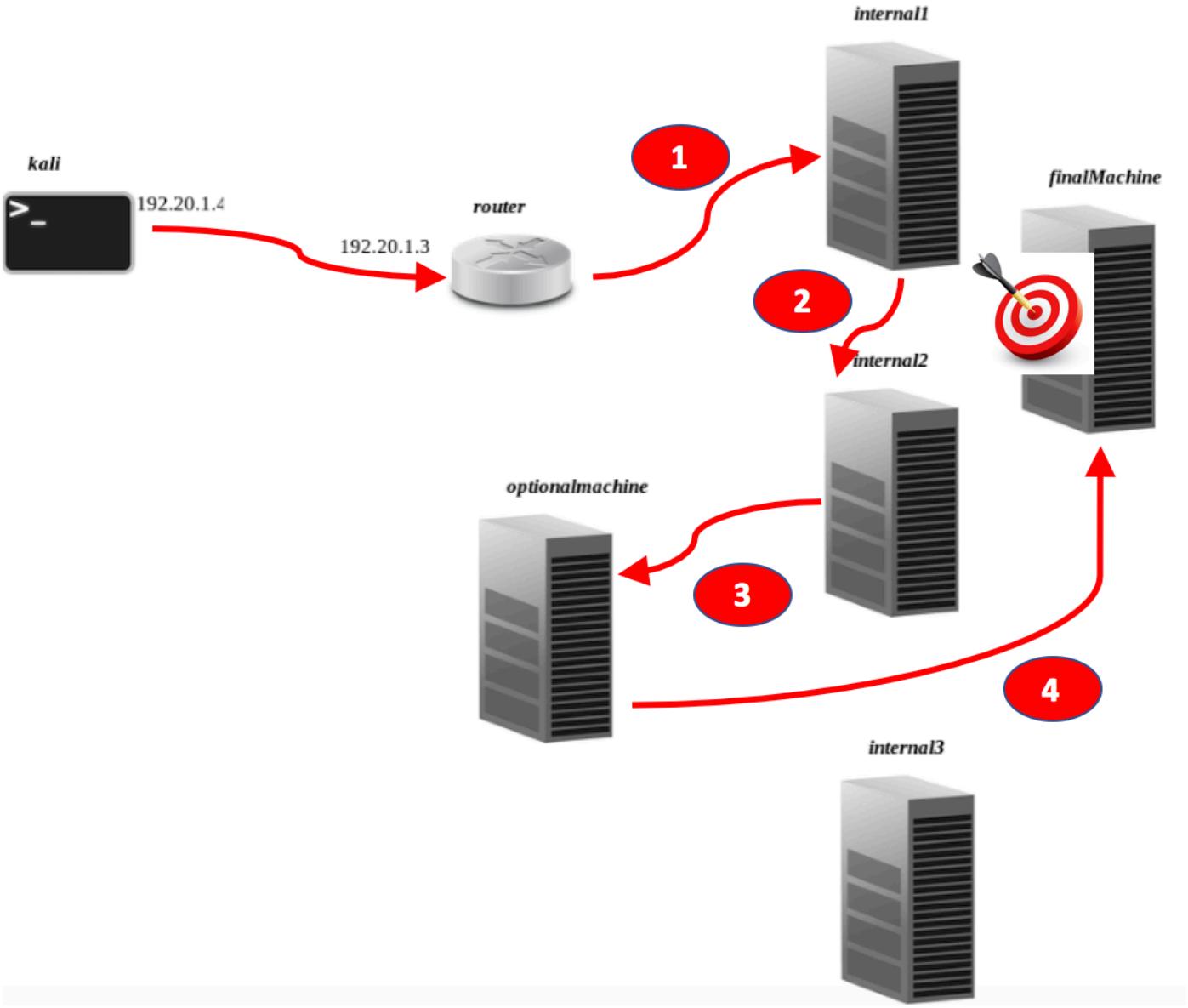
[1] We're not going to play with *footprinting*, for this lab.
[2] See also https://www.systutorials.com/docs/linux/man/1-knockd/

**internal1 → internal2 → internal3 → finaMachine!**




What about that strange further machine called **optionalmachine**? Well, that's a node that you can attack if you want to reach the final target through an alternate path which does not involve node "internal3". This is illustrated in the picture below, which shows the alternative hacking path you can choose:

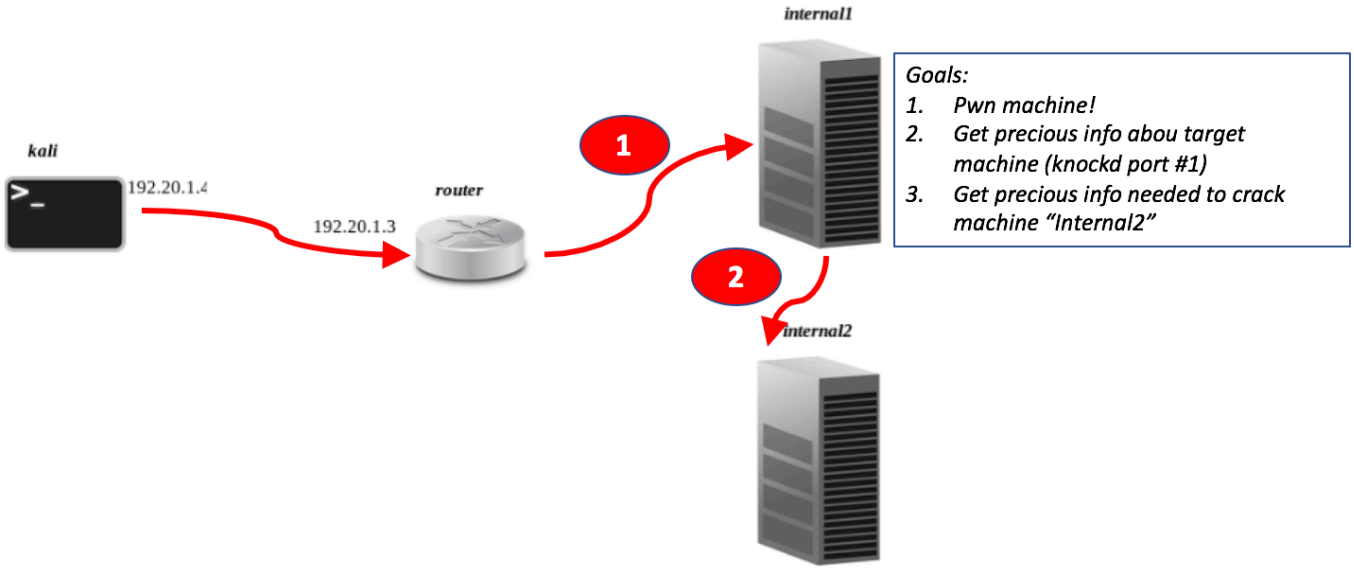
**internal1 → internal2 → optionalmachine → finalMachine!**



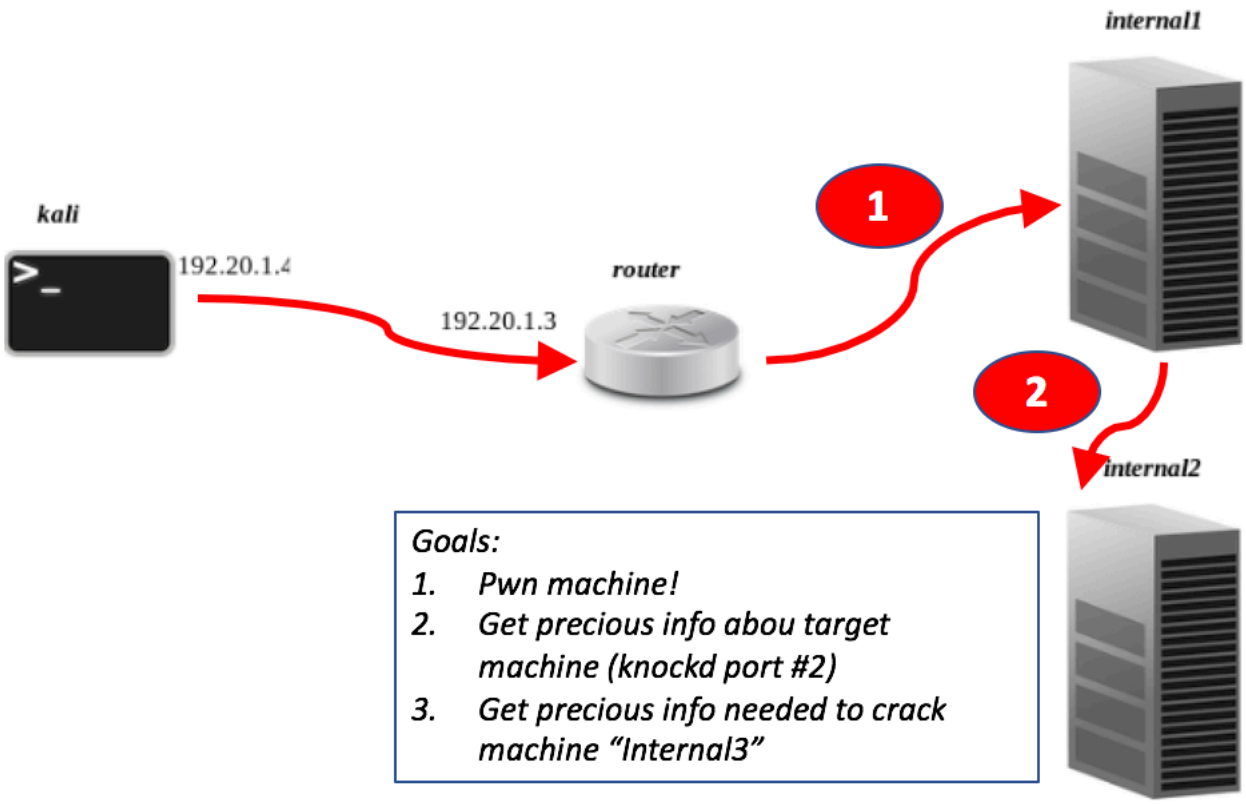

So, what path will you choose? This just depends on your taste and personal inclination!

Let's now start digging a bit more into the details of the single machines. Below you can find a quick summary of the goals you'll have to reach on each and every machine if you want to have any chance of succeeding once you'll confront yourself with the final target.

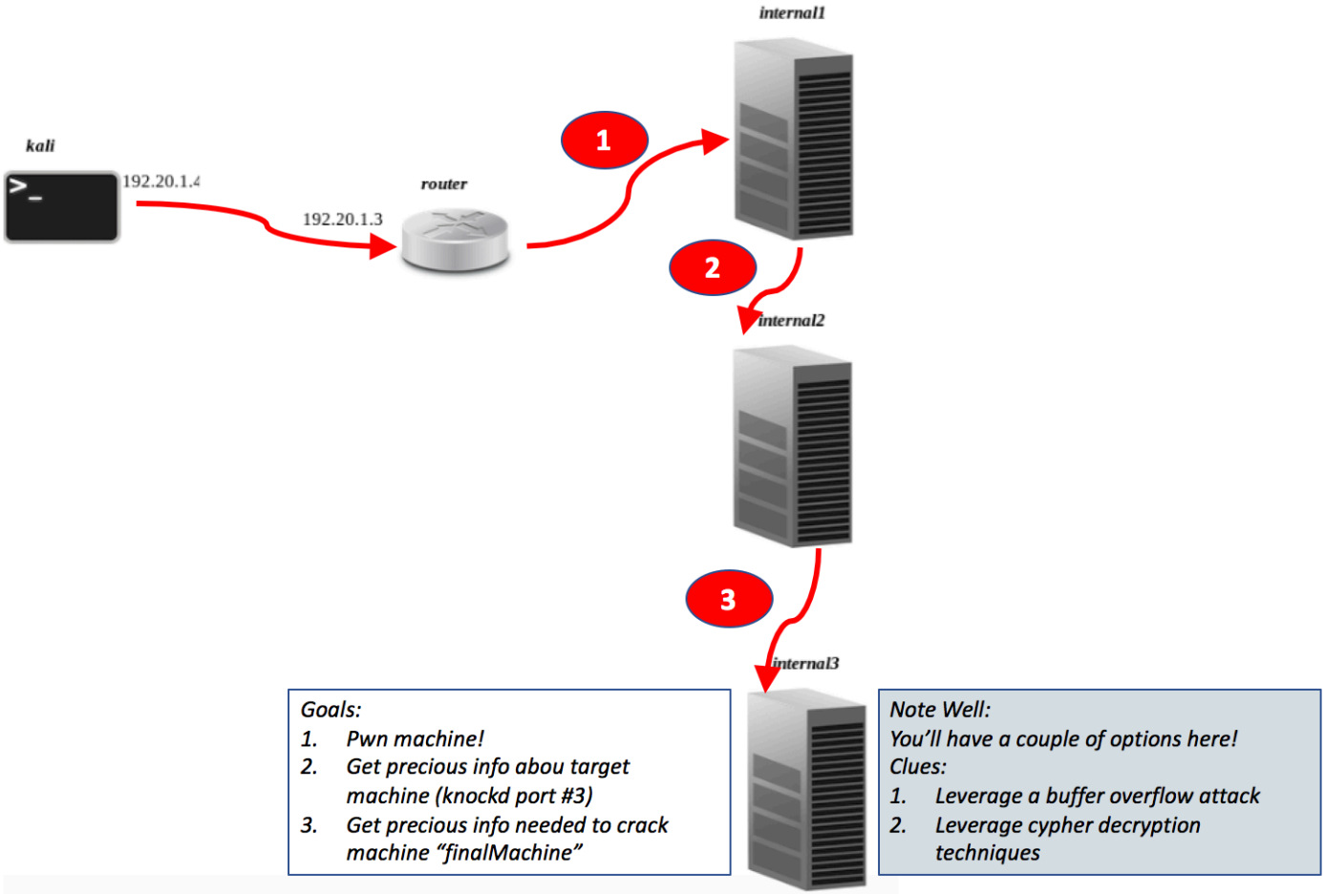
Let's get started with machine **internal1.** Well, in this case, the hint we can give is that you'll necessarily have to play with a bit of web application hacking. Your main objective here will be to somehow grab information about the **first knocking port**. Though, you will find here also some very useful advice on how to exploit the subsequent node.




Did you get rid of the first machine? Well done! You're now ready for step number two. This node (**internal2**) is a challenging one. Here, you'll have to play with both password guessing and password cracking, with the twofold objective of retrieving the **second knocking port**, as well as crucial information for penetrating the subsequent node.

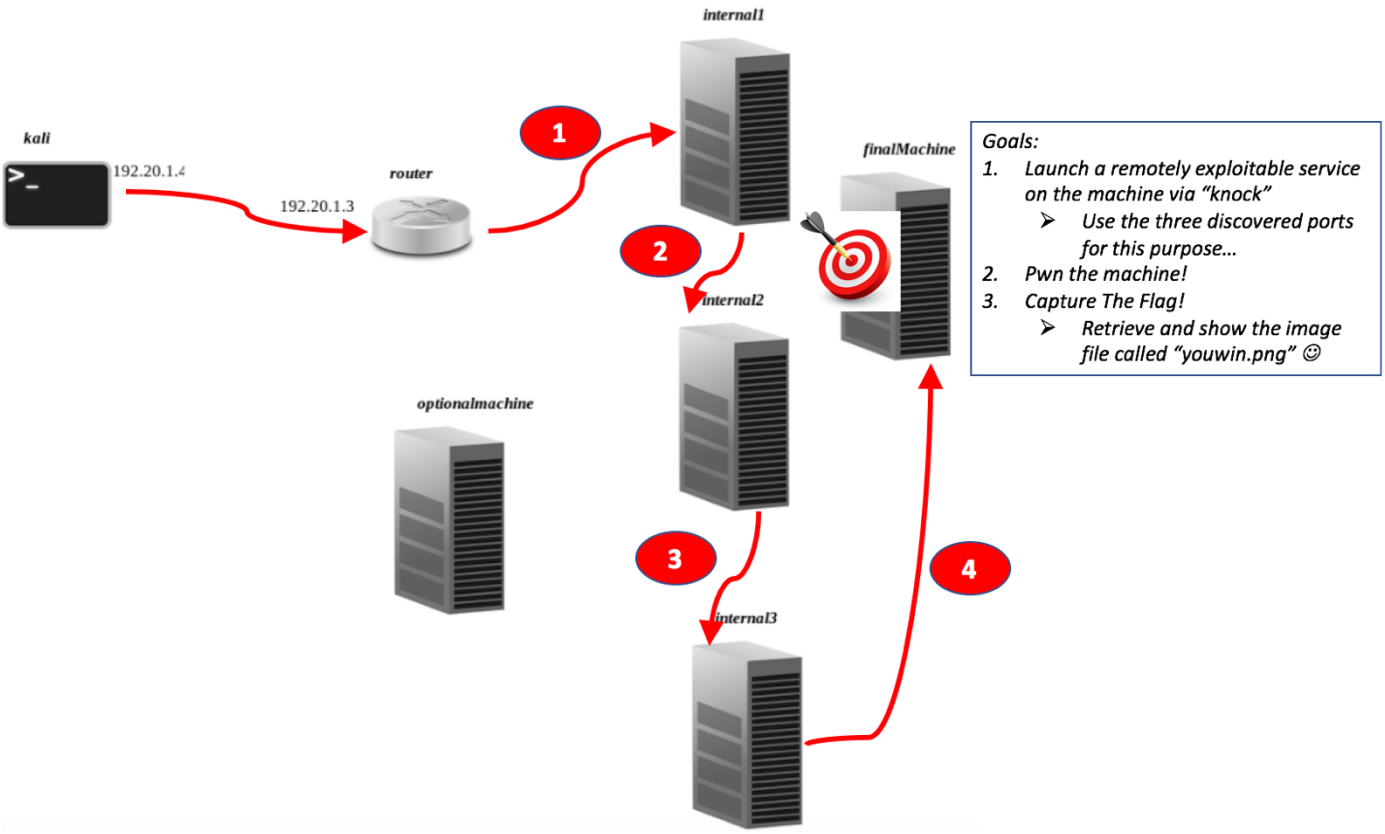


If you're here, this means that you're halfway to the target. Machine **internal3** is full of surprises. As briefly indicated in the picture below, here you'll have a chance to experiment with either "buffer overflow" or "cypher decryption" techniques[3] (or both!). The goal is, as usual, twofold: (i) grab info about the **third and last knocking port**; (ii) get precious info needed in order to penetrate the final machine.



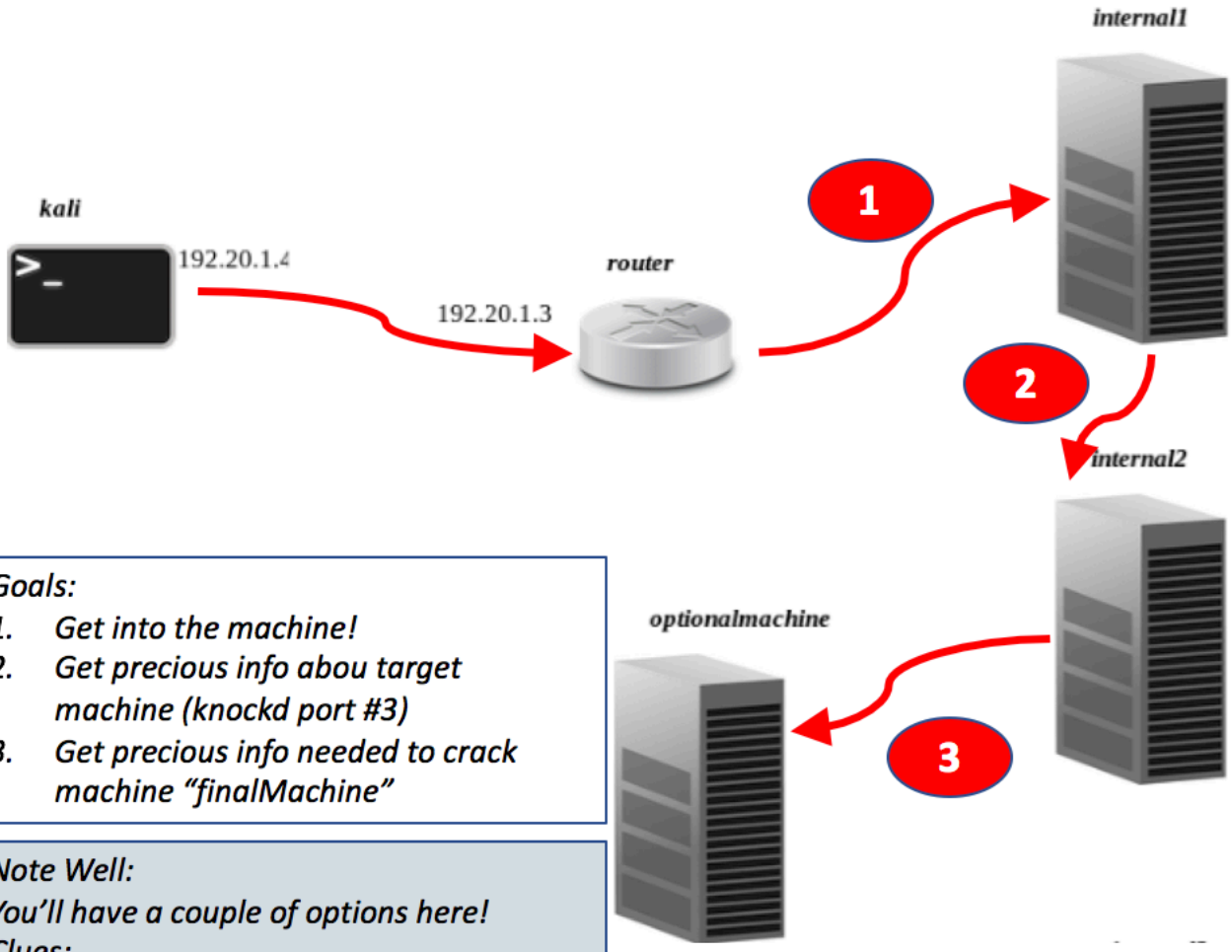

For the last step, you'll have to play with two different services. The former is already active and can be leveraged (after being cracked) to enable pwnage ("pure ownage") of the target. The latter gets unblocked by knocking at the three discovered ports and is the one you'll have to break in order to arrive at the very final stage of the lab, that is retrieving (and showing to us!) the image file called **"youwin.png".** This is briefly sketched in the figure below.

[3] See, e.g., https://tech.pookey.co.uk/non-wp/encoder-decoder.php




If you prefer to take the alternate path (or if you want to try them all and leave no surviving machines behind!) here is what you should expect from the node called **optionalmachine.** Here you will have two options. (i) partially break the node and retrieve info that is needed whem moving the focus towards the final target; (ii) get root access on the machine in order to gather much juicier low hanging fruits providing you with precious information for directly accessing the final target. In both cases, you'll have once again to play with classical web application hacking techniques.

The picture below provides a brief summary of the above discussion.



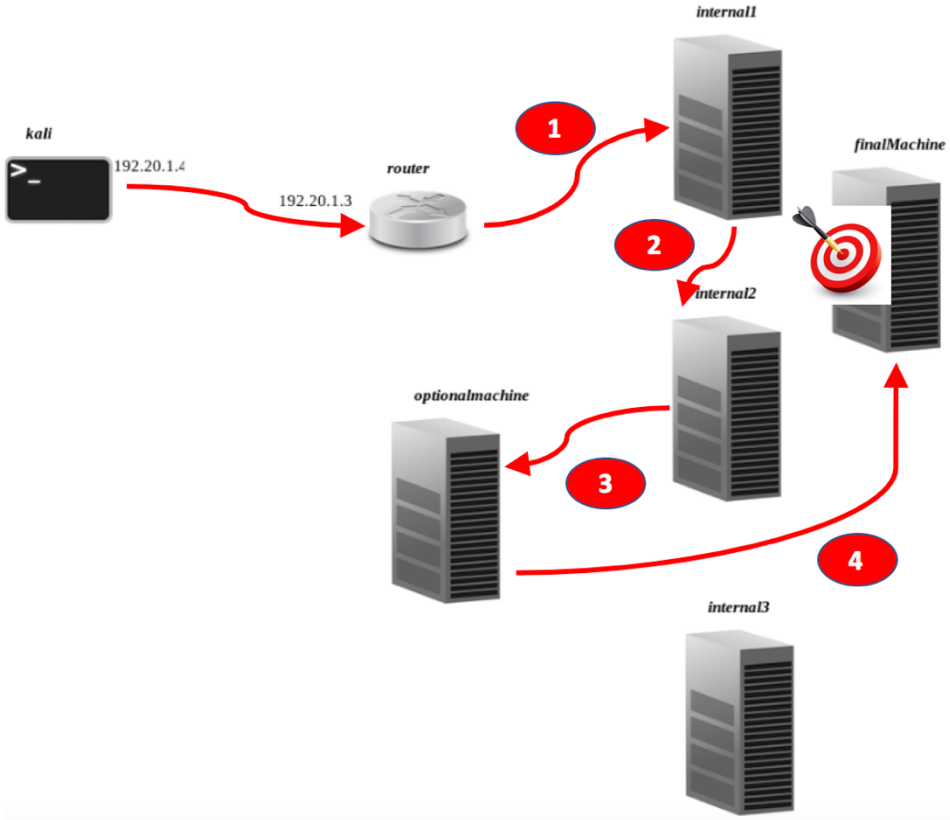

*Goals:*

1. *Get into the machine!*
2. *Get precious info abou target machine (knockd port #3)*
3. *Get precious info needed to crack machine "finalMachine"*

*Note Well:*
*You'll have a couple of options here!*
*Clues:*

1. *Partially break the machine and get useful info for the last step*
2. *Pwn the machine and get enriched info allowing you to directly break the target!*

Once again, if you succeeded in penetrating "optionalmachine", you are now ready to point your guns towards node **"finalMachine",** as illustrated in the picture below.




Goals:

1. Launch a remotely exploitable service on the machine via "knock"
   - Use the three discovered ports for this purpose…
2. Pwn the machine!
3. Capture The Flag!
   - Retrieve and show the image file called "youwin.png" ☺