CYBERSECURITY LAB #1

Giacomo Gori – Tutor didattico

g.gori@unibo.it

Exercises

Complete the exercises, taking notes of all the steps that you take

Write a small report and upload it on Virtuale

Remember: write name, surname and the number of the lab session on the report!

Evaluation

The laboratory part consist of a maximum of 8 points out of the final mark

Of course, points will be given from the evaluation of your reports :)

You can work in group of **2/3 people**. In the report, try to explain in a short and clear way, the steps that you take

Deadline

You can do the exercise and the report now, or later at home

Every project must be submitted within a month from the day of the practice exercise.

Prerequisites

For this lesson:

- Just a pc with a shell and TOR browser and some basic knowledge of bash scripting :)

For next lessons:

- Virtualbox and the configured Kali VM. **Instructions are on Virtuale!**

Telegram group!

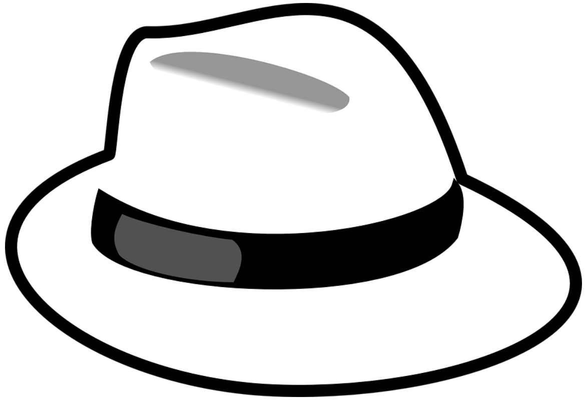
Ethical Hacking

What does "HACKER" mean?

"A **hacker** is a person skilled in information technology who **uses their technical knowledge to achieve a goal or overcome an obstacle**, within a computerized system by non-standard means. "

Source: Wikipedia

It depends on the side that you choose….



White hat

Black hat

Ethical Hackers (aka White hat)

They help companies, organizations and developers to check and improve their security.

With **bug bounty programs** OR being "hired" by them, performing **VAPT**

hackerone

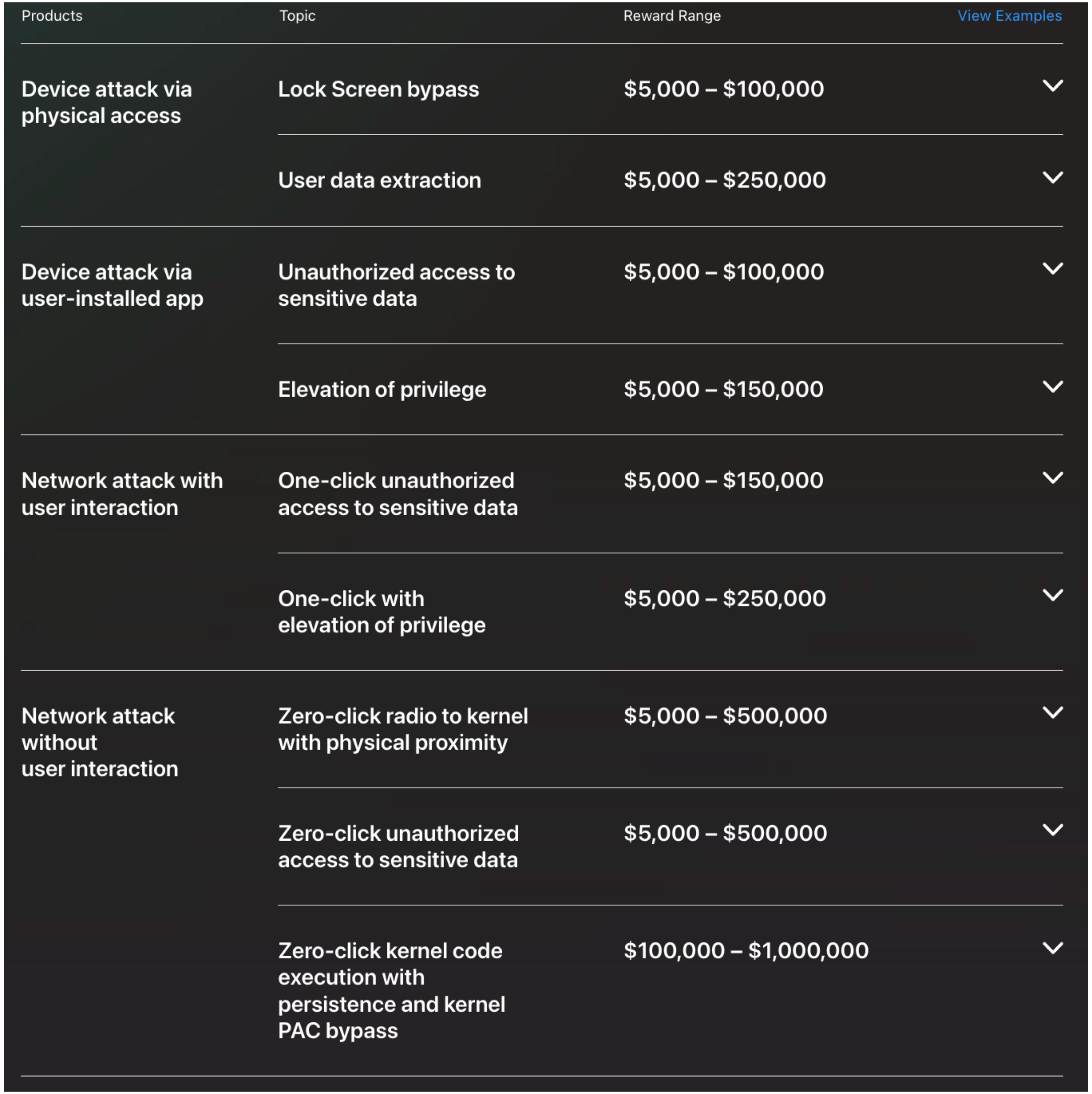
bugcrowd

Bug Bounty programs

Offering a reward to hackers that find undisclosed security bugs

An example

Apple Security Bounty program



Products	Topic	Reward Range	View Examples
Device attack via physical access	Lock Screen bypass	$5,000 – $100,000	⌄
	User data extraction	$5,000 – $250,000	⌄
Device attack via user-installed app	Unauthorized access to sensitive data	$5,000 – $100,000	⌄
	Elevation of privilege	$5,000 – $150,000	⌄
Network attack with user interaction	One-click unauthorized access to sensitive data	$5,000 – $150,000	⌄
	One-click with elevation of privilege	$5,000 – $250,000	⌄
Network attack without user interaction	Zero-click radio to kernel with physical proximity	$5,000 – $500,000	⌄
	Zero-click unauthorized access to sensitive data	$5,000 – $500,000	⌄
	Zero-click kernel code execution with persistence and kernel PAC bypass	$100,000 – $1,000,000	⌄

VAPTs

Performing Vulnerability Assessment and Penetration Testing requires some phases:

Scope and plan

Information gathering

Vulnerability analysis

Exploitation

Reporting

Getting experience..

- Trying to attack deliberately vulnerable VMs
- Participating to Capture The Flag (CTF)

CYBER CHALLENGE.IT

- But **NEVER TRY WITH REAL TARGETS!**
  - Unless you have the authorizations :)

Part 1: overthewire.org

- It's a site with a lots of challenges to do, helping you to learn and practice security concepts in the form of games.

- **Objective of this lesson: Try *Bandit* levels, from Level 0 to 10.**

Tips

- The exercises on the website will suggest you the command to use, together with some useful link on the web
- The "*man*" command is your friend :)
- **Try to resolve them on your own!!**

Connecting with ssh

Use the *ssh* command to connect, with user bandit0 (0 stand for the first level):

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Notice: if you are using almawifi, instead use this command:

```
ssh -J jump@130.136.3.69
 bandit0@bandit.labs.overthewire.org -p 2220
```

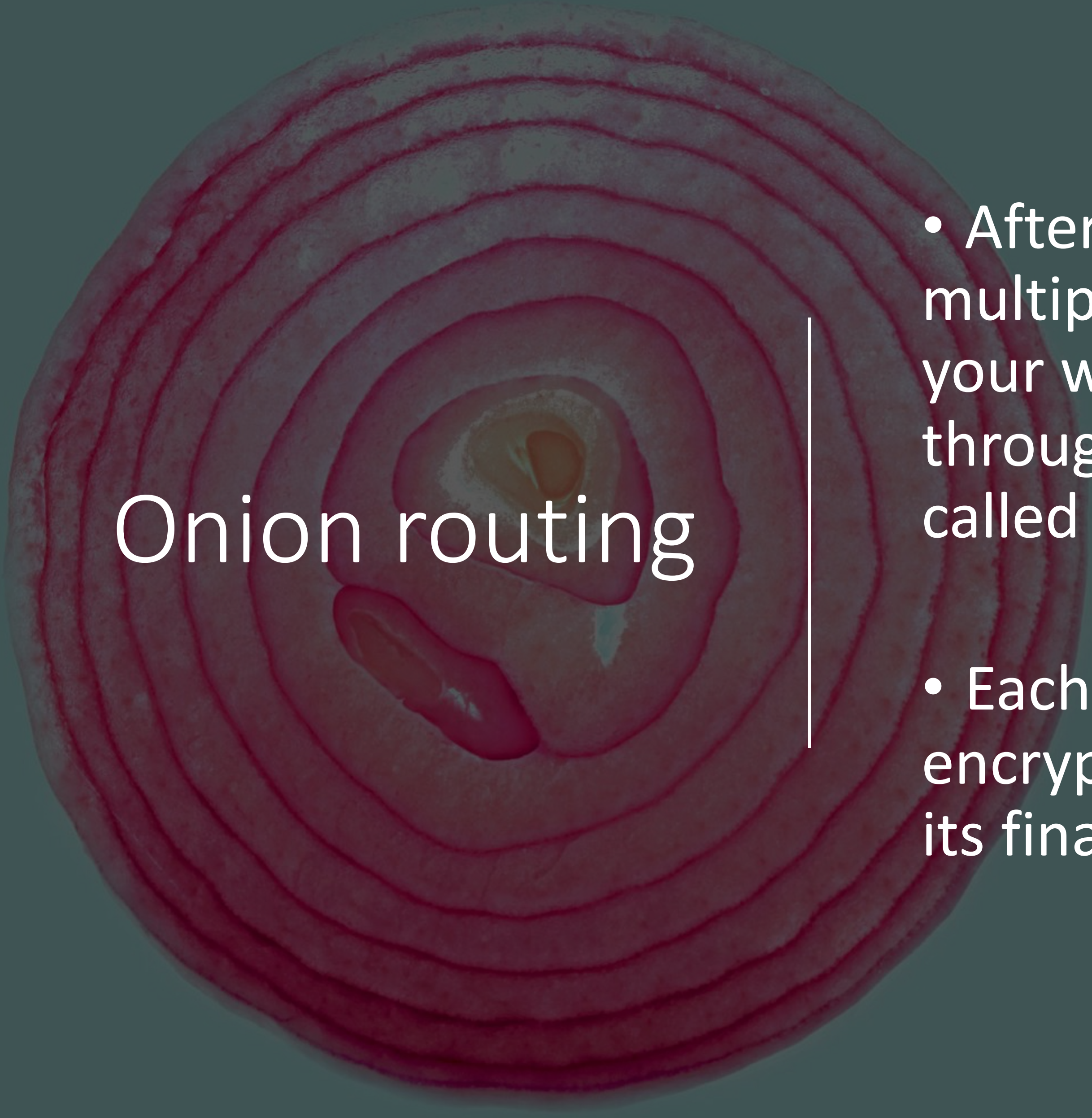
Exercise 1 : www.overthewire.org

Complete the levels, from 0 to 10, **taking notes of all the steps**

Write a small report

Remember : write name, surname and number of the lab session **on the report!**

Hidden services

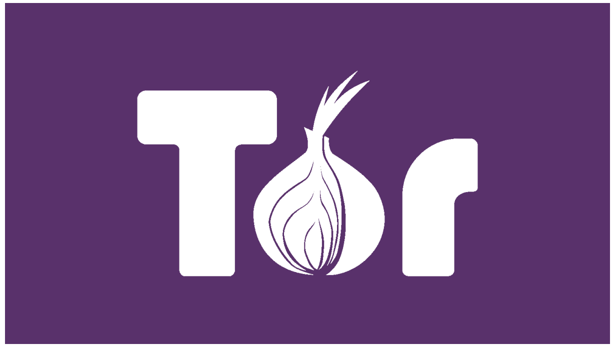


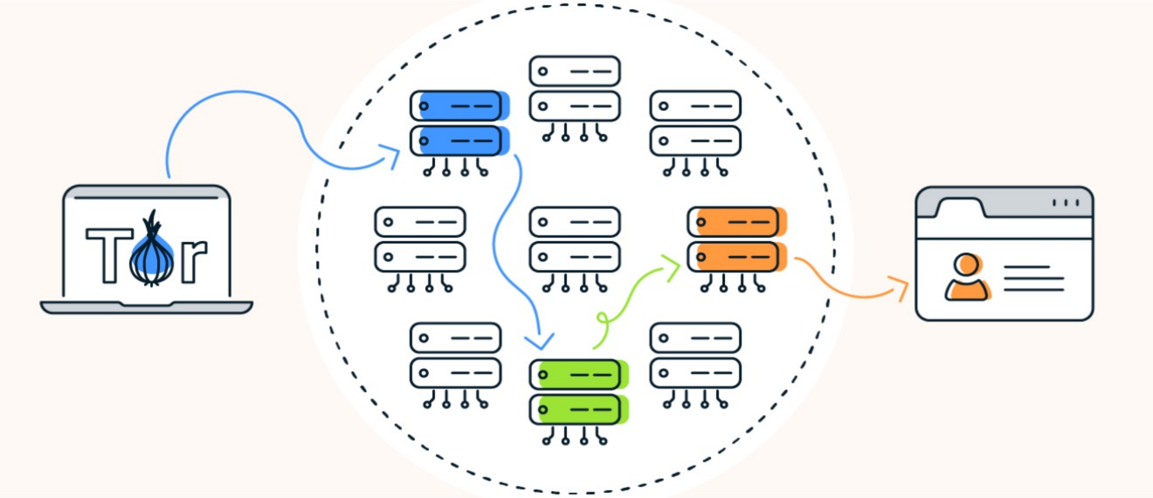
Onion routing

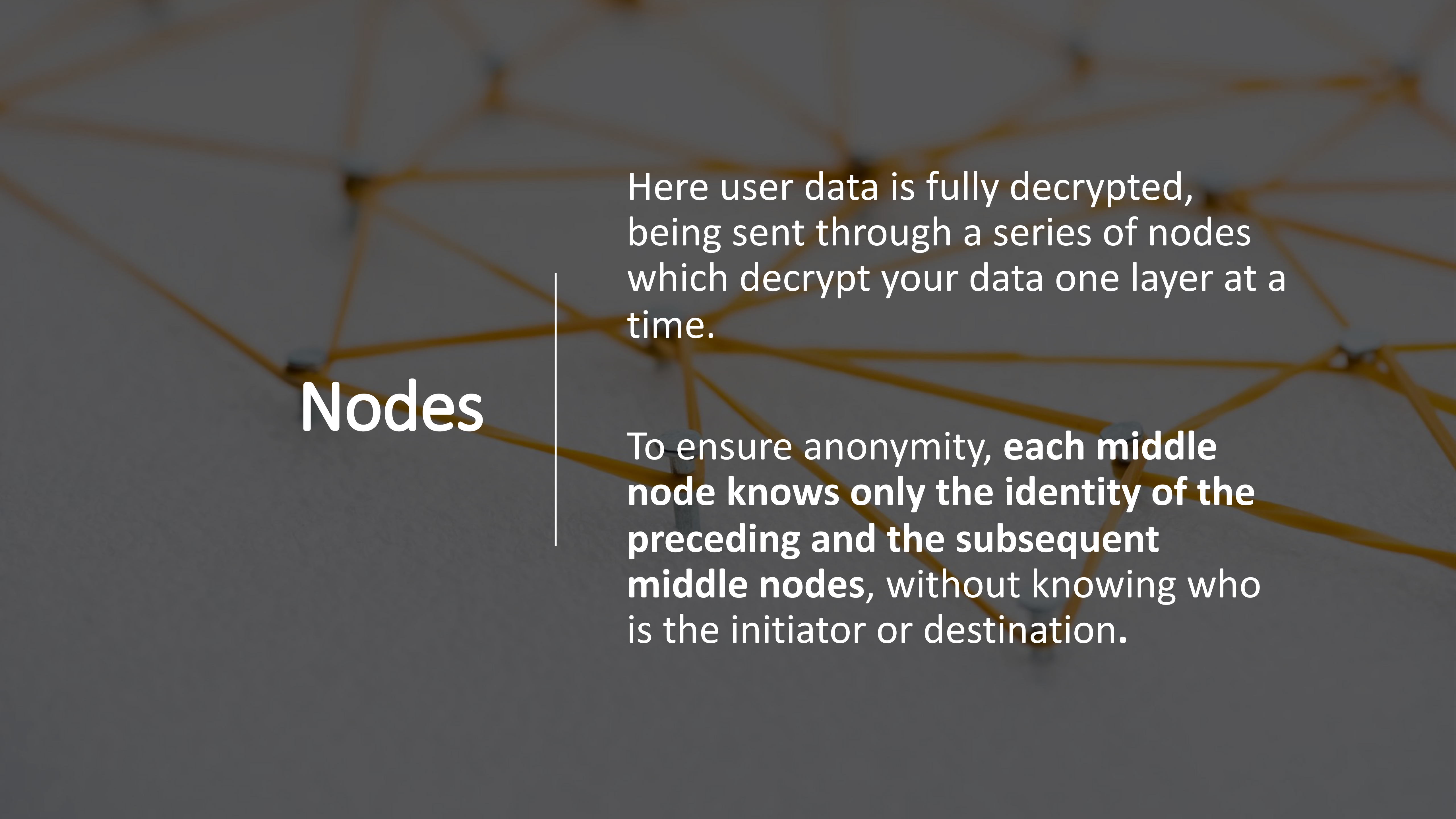
- After your data is secured inside multiple layers of encryption, your web traffic is transmitted through a series of network nodes, called onion nodes.
- Each node “peels away” a layer of encryption until the data reaches its final destination, fully decrypted.

TOR browser

Tor is a browser that anonymously transmits encrypted data across three layers (*entry – middle – exit nodes*) of international proxies that make up the Tor circuit.





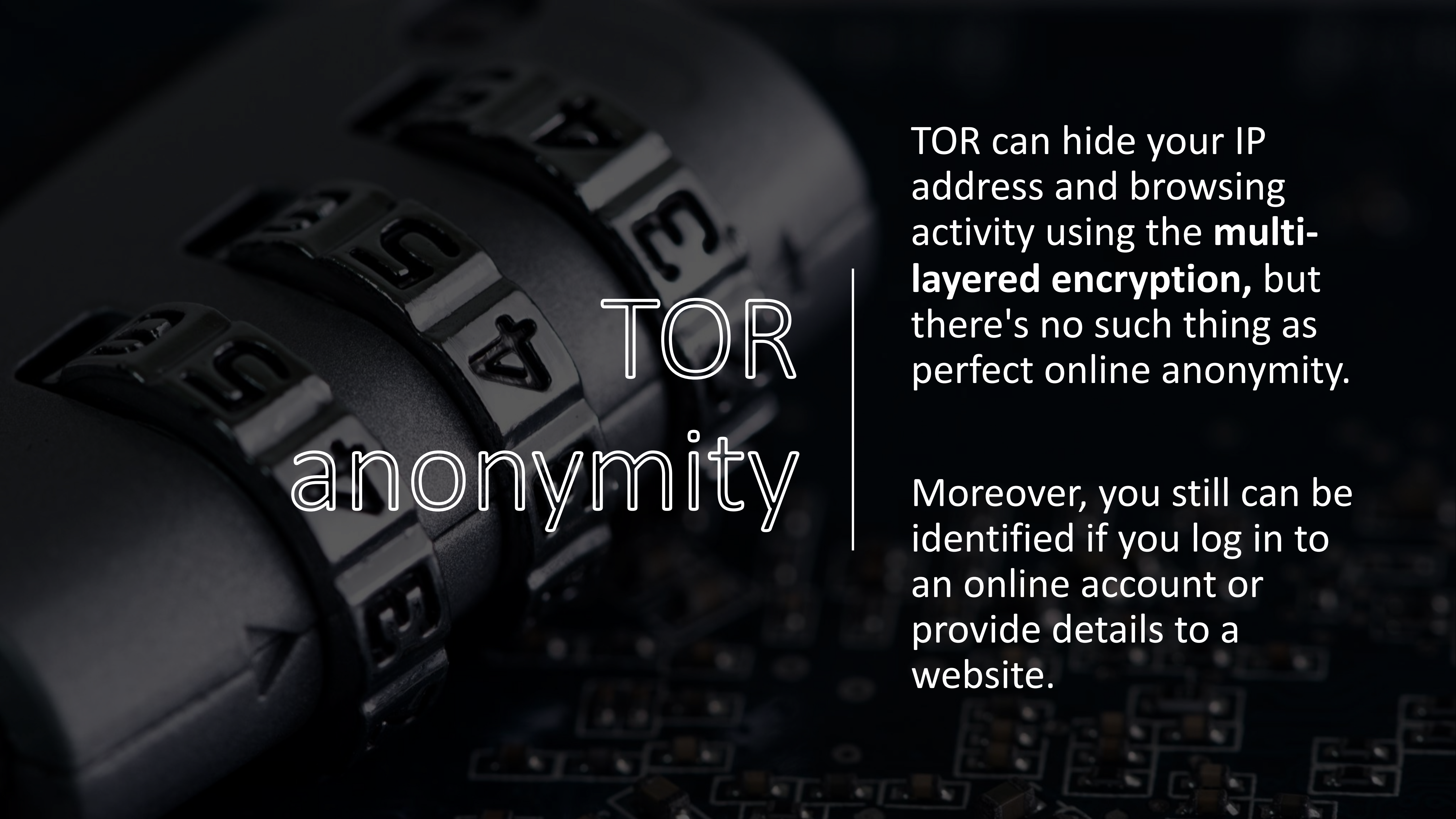


Nodes

Here user data is fully decrypted, being sent through a series of nodes which decrypt your data one layer at a time.

To ensure anonymity, **each middle node knows only the identity of the preceding and the subsequent middle nodes**, without knowing who is the initiator or destination.

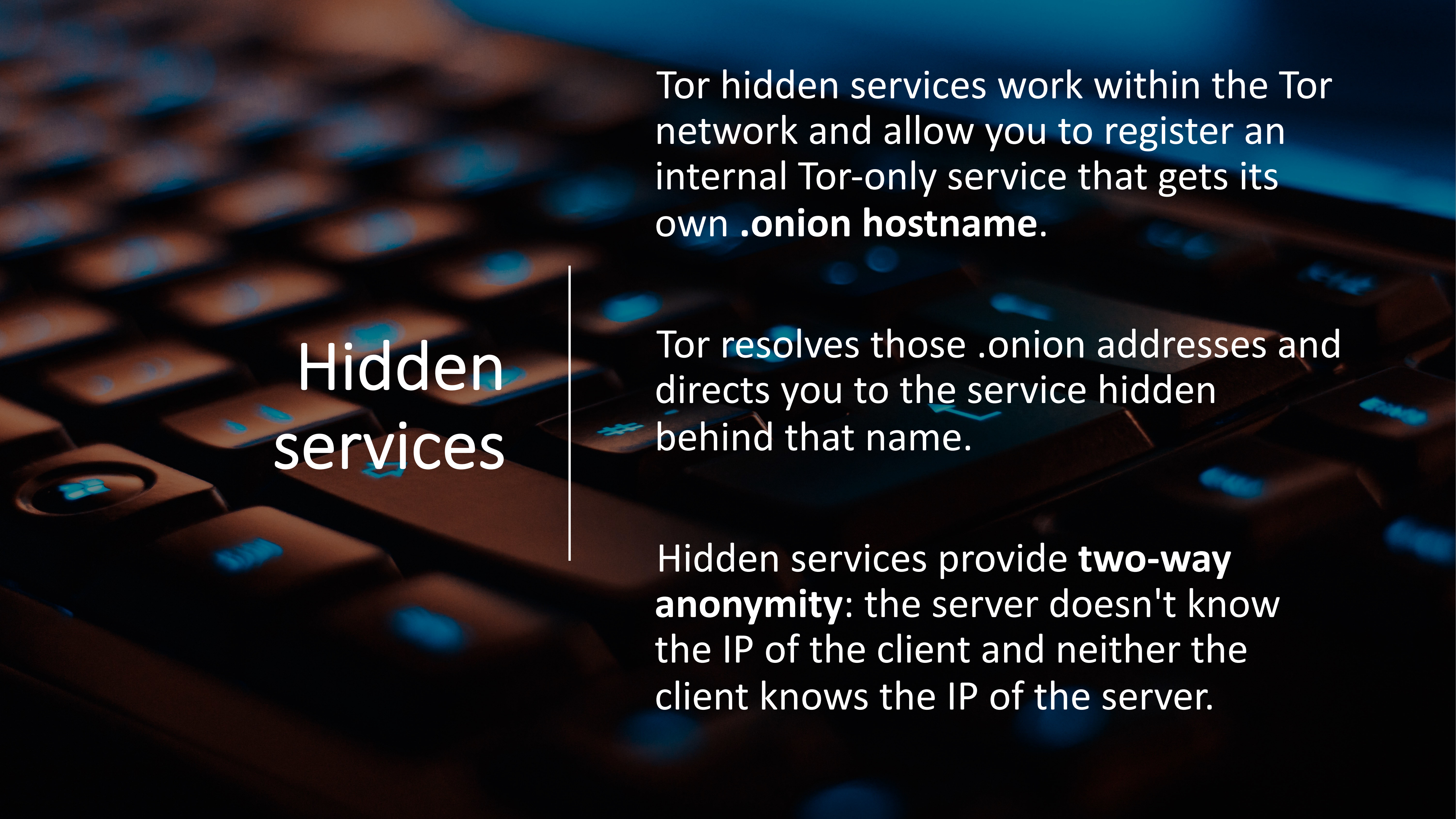
Am I anonymous with TOR?



TOR anonymity

TOR can hide your IP address and browsing activity using the **multi-layered encryption,** but there's no such thing as perfect online anonymity.

Moreover, you still can be identified if you log in to an online account or provide details to a website.



Hidden services

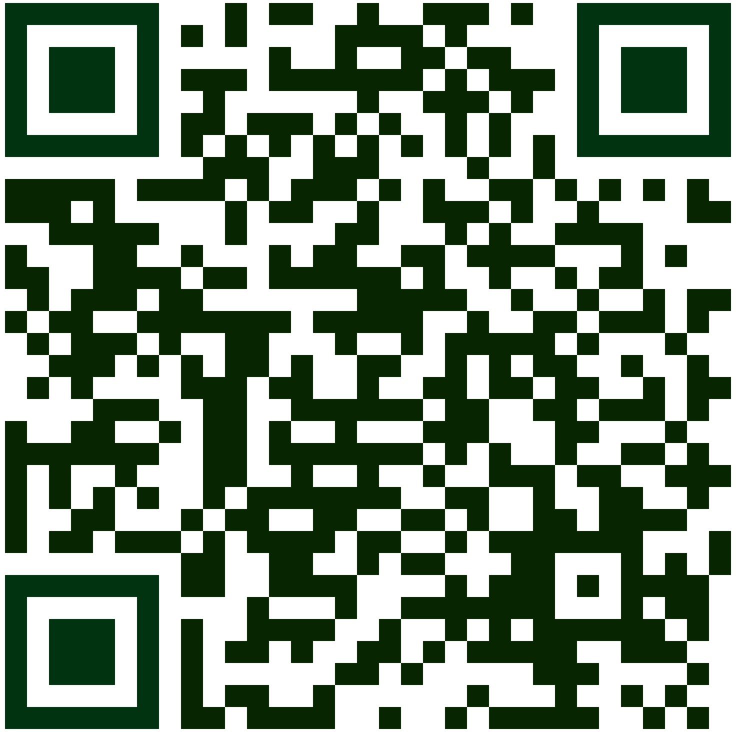
Tor hidden services work within the Tor network and allow you to register an internal Tor-only service that gets its own **.onion hostname**.

Tor resolves those .onion addresses and directs you to the service hidden behind that name.

Hidden services provide **two-way anonymity**: the server doesn't know the IP of the client and neither the client knows the IP of the server.

Part 2: Hidden services

FIND THE FLAG



Exercise 2 : Find the flag

Use the QR code to find the flag, hidden somewhere in the website

Complete the report with this second part and upload it on Virtuale

Remember : write name, surname and number of the lab session **on the report!**