WIFI SSID: `GOhack25`

Password: `90|-|@(X25!`

Register here!
https://htbzh.ch/onboarding.html

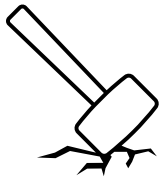
HACKTHEBOX

Hands-On Penetration Testing Training

Your Host

- Hack The Box Ambassador
- Tech Lead Bug Bounty, Swisscom

Antoine Neuenschwander



Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology
Acknowledge there is no 100% security
Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

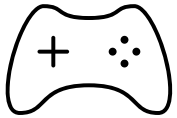
Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorized access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics



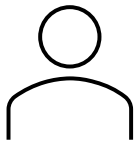
Gamification

Capture the Flag (CTF)
Hacking Competition

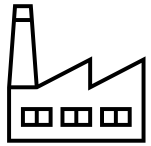
(warning: addictive)

HACKTHEBOX

> 400 virtual machines (boxes)

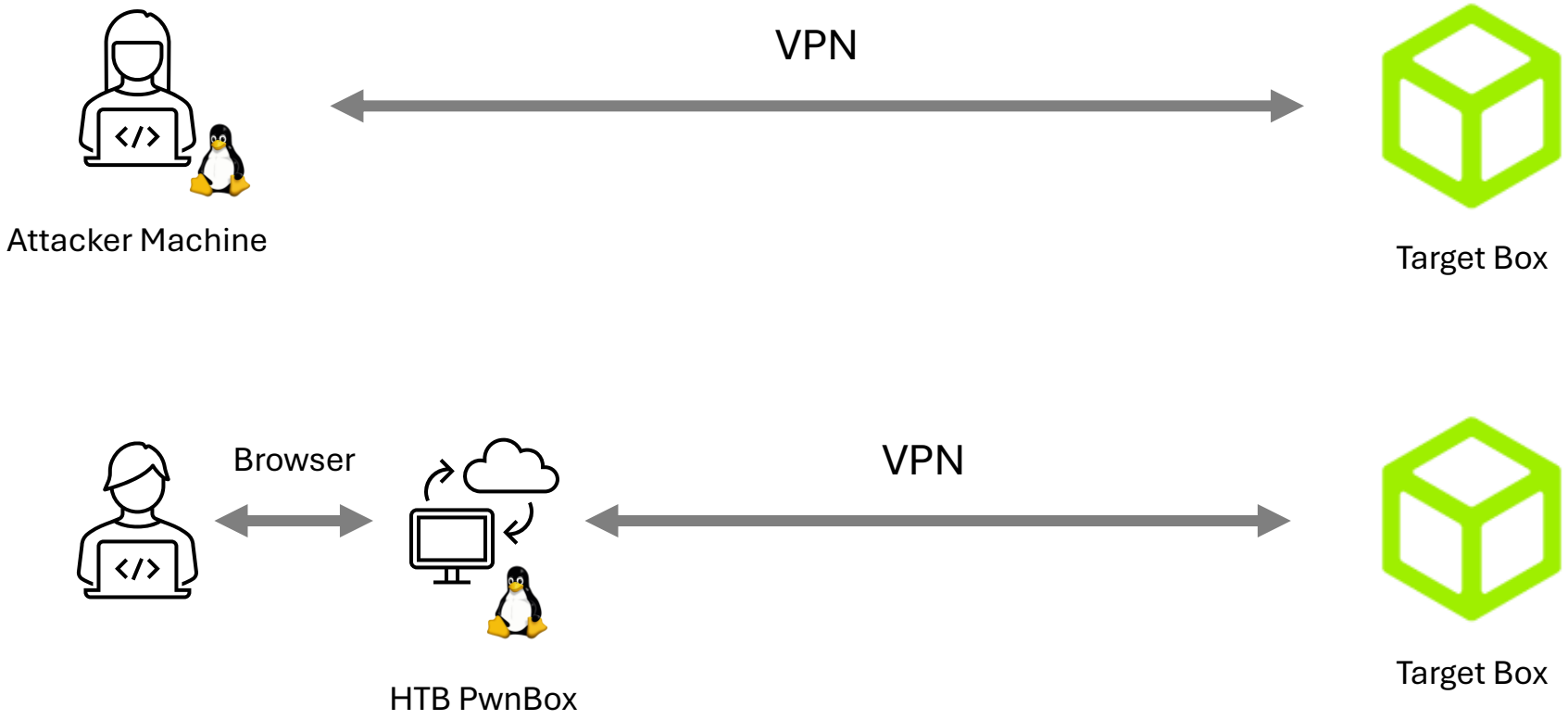


HTB Labs
https://app.hackthebox.com



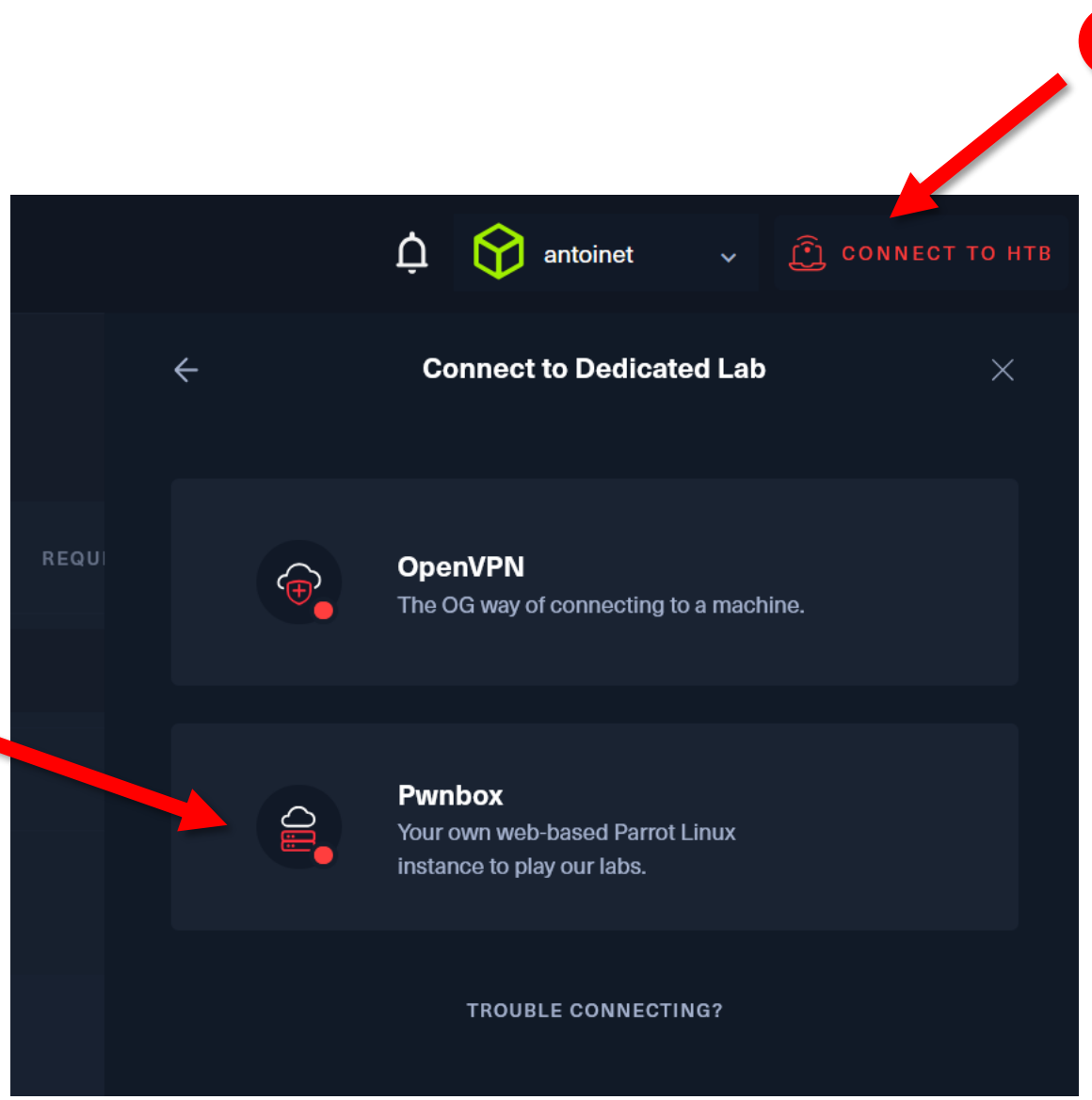
HTB Enterprise Platform
https://enterprise.hackthebox.com

Hacking Setup



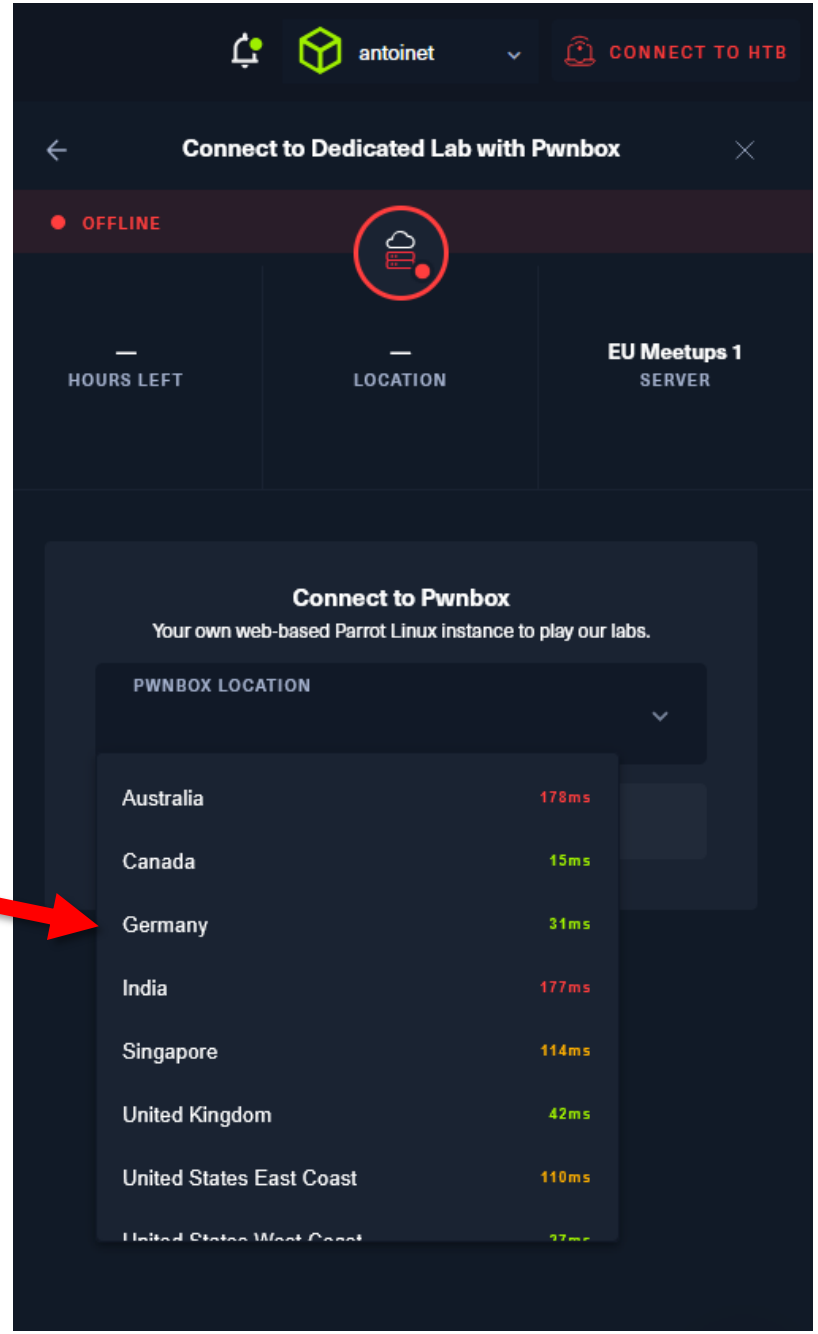
Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



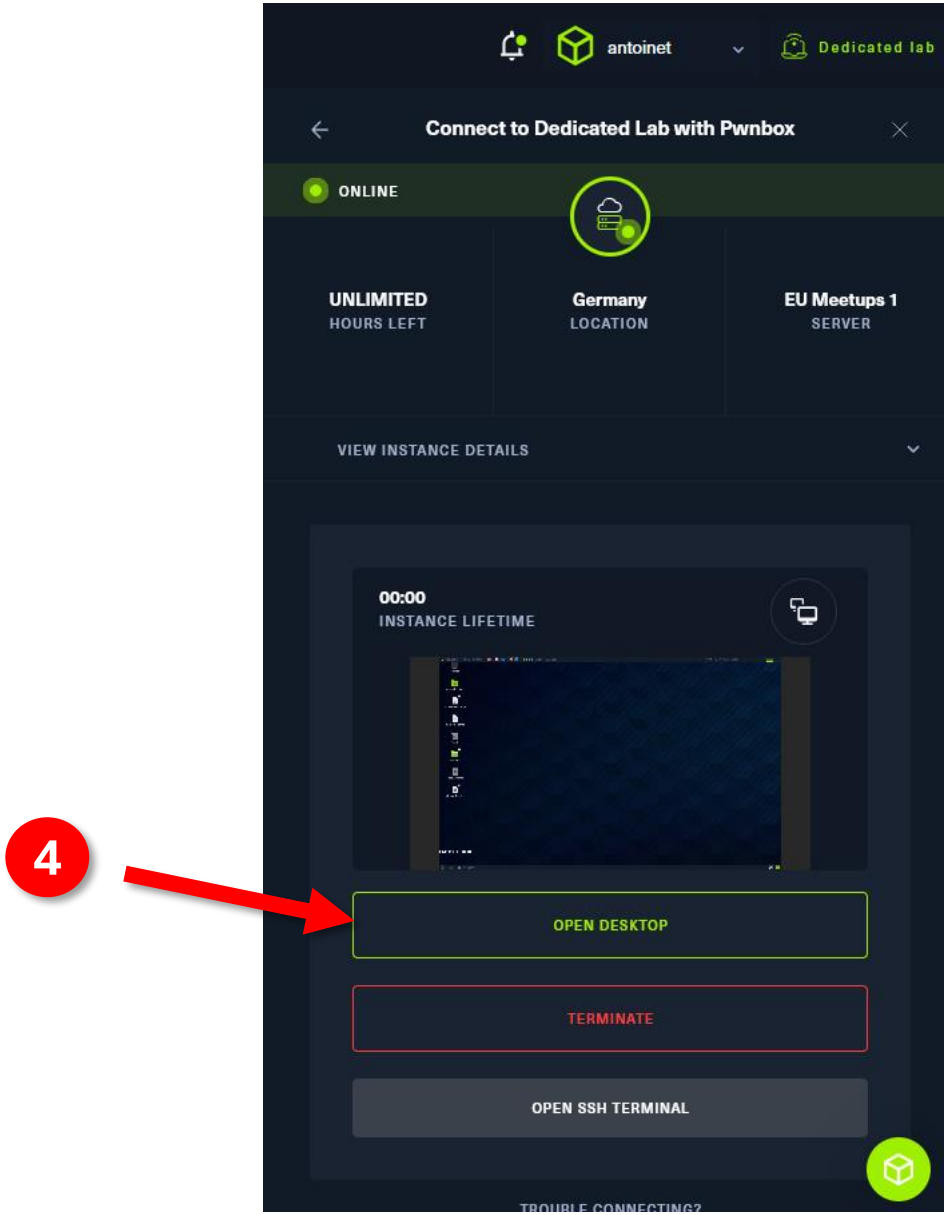
Connect to the Lab via HTB PwnBox

Choose the nearest location



Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop

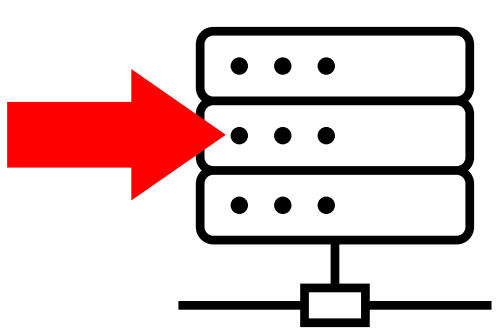


Mirai

- Improperly configured IoT device
- Network scanning with nmap
- Search engines for connected devices
- Web-fuzzing / Forced Browsing
- Basic filesystem forensics

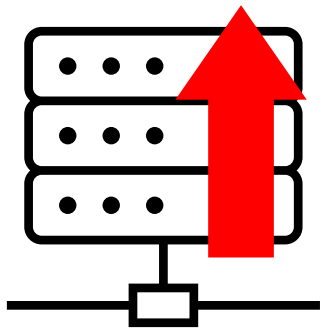
Attack Phases

Initial Access



`user.txt`

Privilege Escalation



`root.txt`

/etc/hosts file

- Add the domain **mirai.htb** to the **/etc/hosts** file
- Overrides DNS resolution

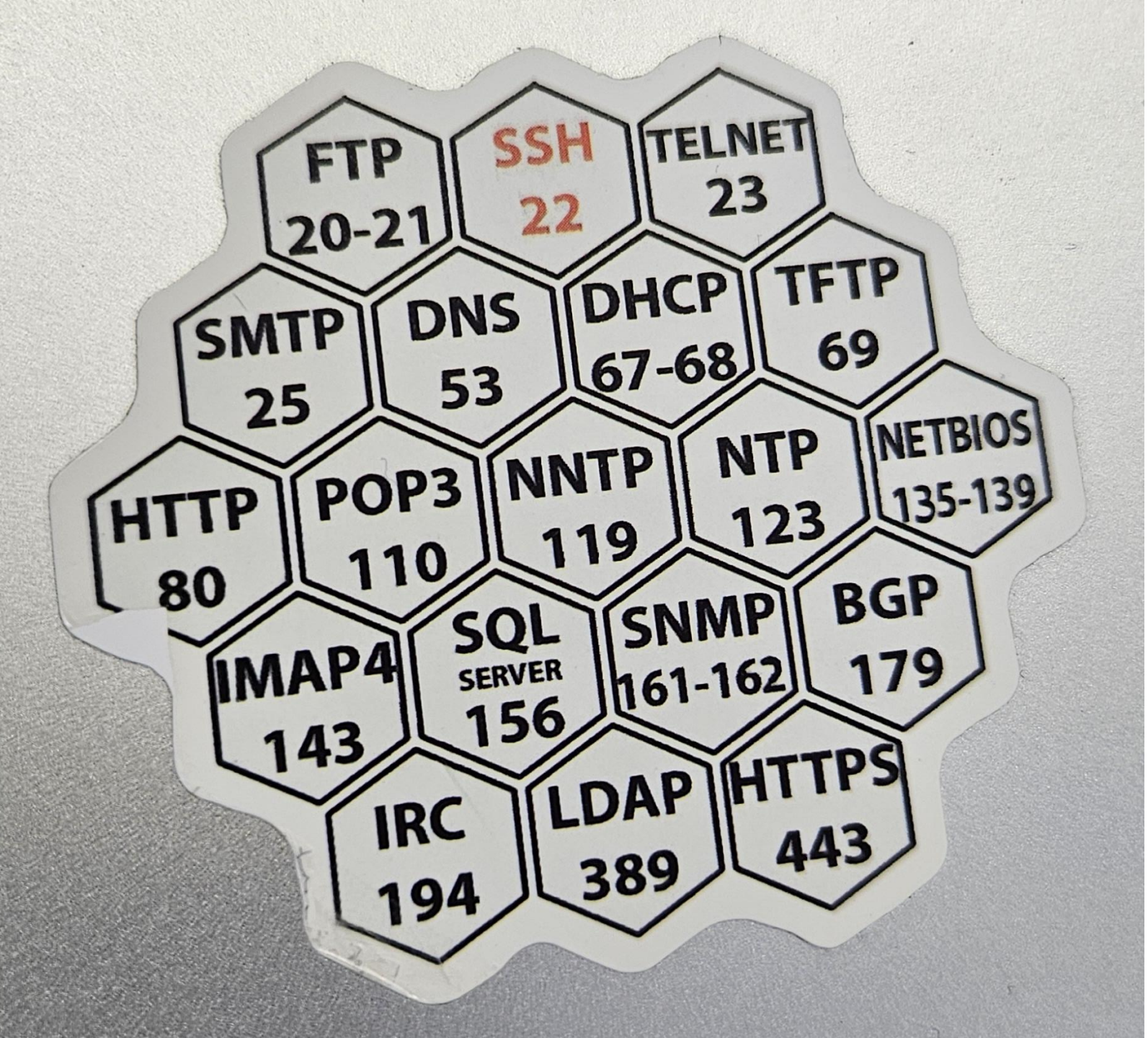
```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX mirai.htb
```

Network Scanning & Service Enumeration

Application	Provides **network services** to applications	HTTP, FTP, SMTP, SSH, etc.
Transport	Ensures **reliable data transfer** between devices	TCP Port 1337
Internet	**Routing** of data packets within and between networks	IP Address 203.0.113.45
Network Access	**Physical Transmission** of Data • Ethernet (LAN cable) • Wi-Fi	MAC Address 48:2C:6A:1E:59:3F



TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

Advanced nmap options

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

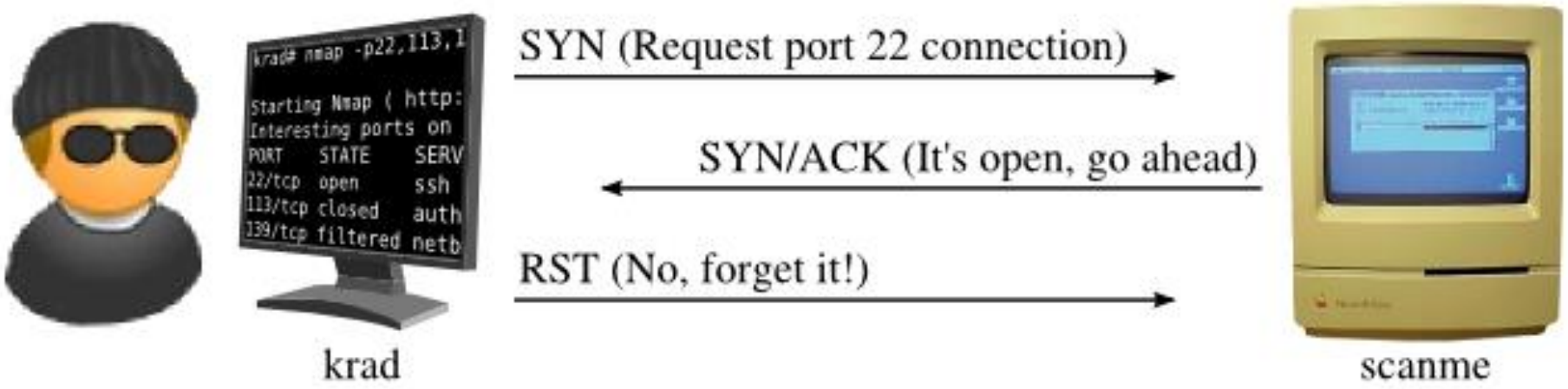
```
$ nmap -sV <ip-address>
```

Script scan (default nmap scripts)

```
$ nmap -sC <ip-address>
```

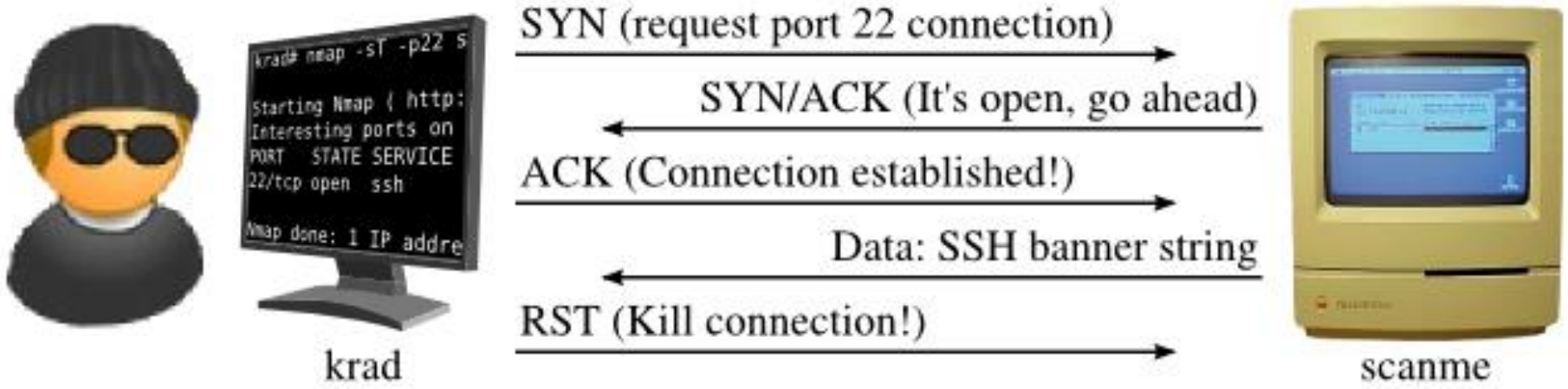
Scanning Techniques - SYN Scan

```
nmap -sS --max-retries=0 -p <port> <target>
```



Scanning Techniques - Connect Scan

```
nmap -sT --max-retries=0 -p <port> <target>
```



Enumeration

Check all open ports

```
$ nmap -p- -T4 mirai.htb
```

Detailed scan

```
$ nmap -p 22,53,80 -sC -sV mirai.htb
```

README | Code of conduct | Contributing | License | Security

Pi-hole®

Network-wide ad blocking via your own Linux hardware

The Pi-hole® is a DNS sinkhole that protects your devices from unwanted content without installing any client-side software.

- **Easy-to-install**: our dialogs walk you through the simple installation process in less than ten minutes
- **Resolute**: content is blocked in *non-browser locations*, such as ad-laden mobile apps and smart TVs
- **Responsive**: seamlessly speeds up the feel of everyday browsing by caching DNS queries
- **Lightweight**: runs smoothly with minimal hardware and software requirements
- **Robust**: a command-line interface that is quality assured for interoperability
- **Insightful**: a beautiful responsive Web Interface dashboard to view and control your Pi-hole
- **Versatile**: can optionally function as a DHCP server, ensuring *all* your devices are protected automatically
- **Scalable**: capable of handling hundreds of millions of queries when installed on server-grade hardware
- **Modern**: blocks ads over both IPv4 and IPv6
- **Free**: open source software that helps ensure *you* are the sole person in control of your privacy

One-Step Automated Install

Sponsor this project

pi-hole Pi-hole

https://pi-hole.net/donate

patreon.com/pihole

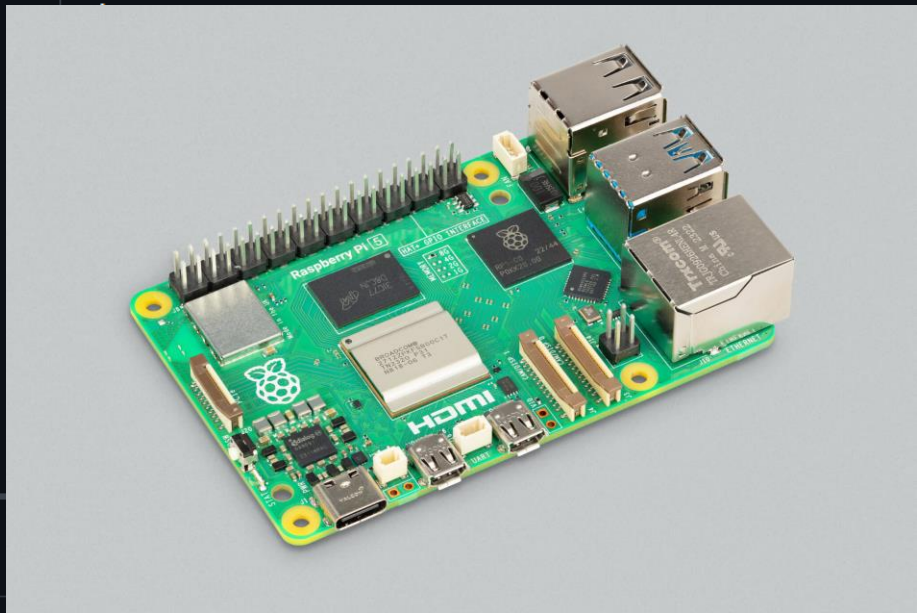
Learn more about GitHub Sponsors

Packages

No packages published

Contributors 238

+ 224 contributors



TOTAL RESULTS

10

TOP PORTS

53	9
9000	1

TOP ORGANIZATIONS

Swisscom (Schweiz) AG	5
Bluewin is an LIR and ISP in Switzerland.	3
Swisscom (Schweiz) AG is an internet service provider in CH.	1
Swisscom AG is a full service provider in CH	1

144.2.104.115

bbcs-104-115.pub.wingo.ch
Swisscom (Schweiz) AG
Switzerland, Zürich

```
dnsmasq-pi-hole-v2.92test13
Recursion: enabled
```

92.106.24.224

224.24.106.92.dynamic.cust.swisscom.net
Swisscom (Schweiz) AG is an internet service provider in CH.
Switzerland, Yverdon-les-Bains

```
dnsmasq-pi-hole-v2.92test13
Recursion: enabled
```

92.105.53.84

84.53.105.92.dynamic.cust.swisscom.net
Bluewin is an LIR and ISP in Switzerland.
Switzerland, Rupperswil

```
dnsmasq-pi-hole-v2.90+1
Recursion: enabled
```

83.173.213.89

censys

Hosts | ("pi-hole") and autonomous_system.asn:3303 | Search

Register
Log In

Results | Report | Docs

Host Filters

Labels:

17 jquery
16 bootstrap
7 remote-access
4 angularjs
4 network.device.vpn
More

Autonomous System:

22 SWISSCOM Swisscom Switzerland Ltd

Location:

22 Switzerland

Service Filters

Service Names:

90 HTTP
8 DNS
5 SSH
4 SMB
4 UNKNOWN
More

Ports:

18 443
17 80
8 53
5 22

Hosts

Results: 22 Time: 0.06s

144.2.104.115 (bbcs-104-115.pub.wingo.ch)

SWISSCOM Swisscom Switzerland Ltd (3303) Zurich, Switzerland

managed-file-transfer | remote-access | webshell | shellinabox | bootstrap | jquery | angularjs

22/SSH 53/DNS 80/HTTP 81/HTTP 443/HTTP
4200/HTTP 5900/VNC 7880/HTTP 8080/HTTP 8443/HTTP
9000/HTTP 9082/HTTP 9443/HTTP

92.106.24.224 (224.24.106.92.dynamic.cust.swisscom.net)

Linux SWISSCOM Swisscom Switzerland Ltd (3303) Vaud, Switzerland

bootstrap | jquery | remote-access | proxy

22/SSH 53/DNS 80/HTTP 443/HTTP 9080/HTTP
9443/HTTP

144.2.69.200 (bbcs-69-200.pub.wingo.ch)

Ubuntu Linux SWISSCOM Swisscom Switzerland Ltd (3303) Geneva, Switzerland

file-sharing | bootstrap | jquery | angularjs | remote-access | network-administration

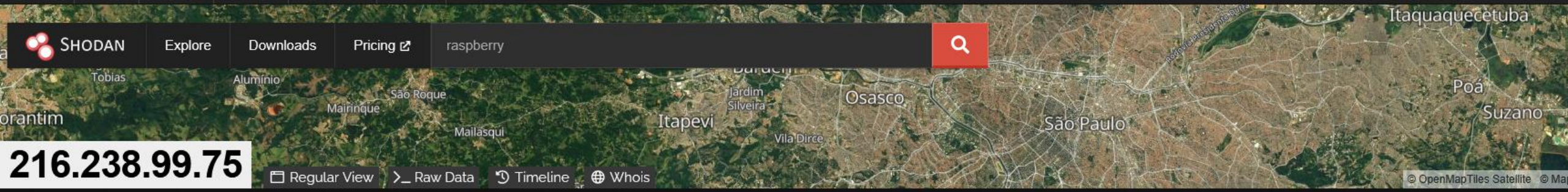
22/SSH 53/DNS 80/HTTP 137/NETBIOS 139/SMB
443/HTTP 445/SMB 3389/RDP 9000/HTTP 9443/HTTP
32401/UNKNOWN

188.62.198.134

Synology Dsm SWISSCOM Swisscom Switzerland Ltd (3303) Zug, Switzerland

remote-access | vue.js | bootstrap | jquery | angularjs

22/SSH 80/HTTP 443/HTTP 5000/HTTP 5001/HTTP
5006/HTTP 8000/HTTP 8080/HTTP 8081/HTTP 8082/HTTP



216.238.99.75

Regular View | Raw Data | Timeline | Whois

// TAGS: cloud database honeypot vpn

General Information

Hostnames	216.238.99.75.**vultrusercontent.com**
Domains	vultrusercontent.com
Cloud Provider	**Vultr**
Cloud Region	**BR-SP**
Country	**Brazil**
City	**Osasco**
Organization	**Vultr Holdings, LLC**
ISP	**The Constant Company, LLC**
ASN	**AS20473**

Web Technologies

CI

Web Frameworks

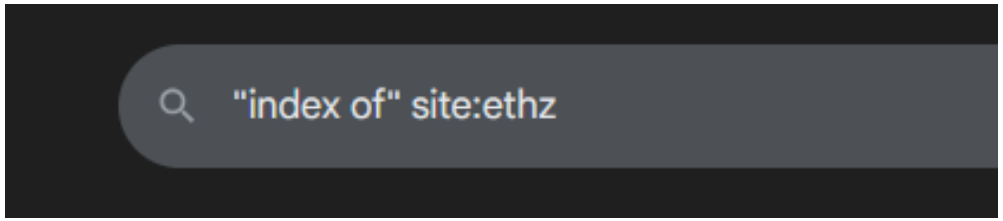
Open Ports

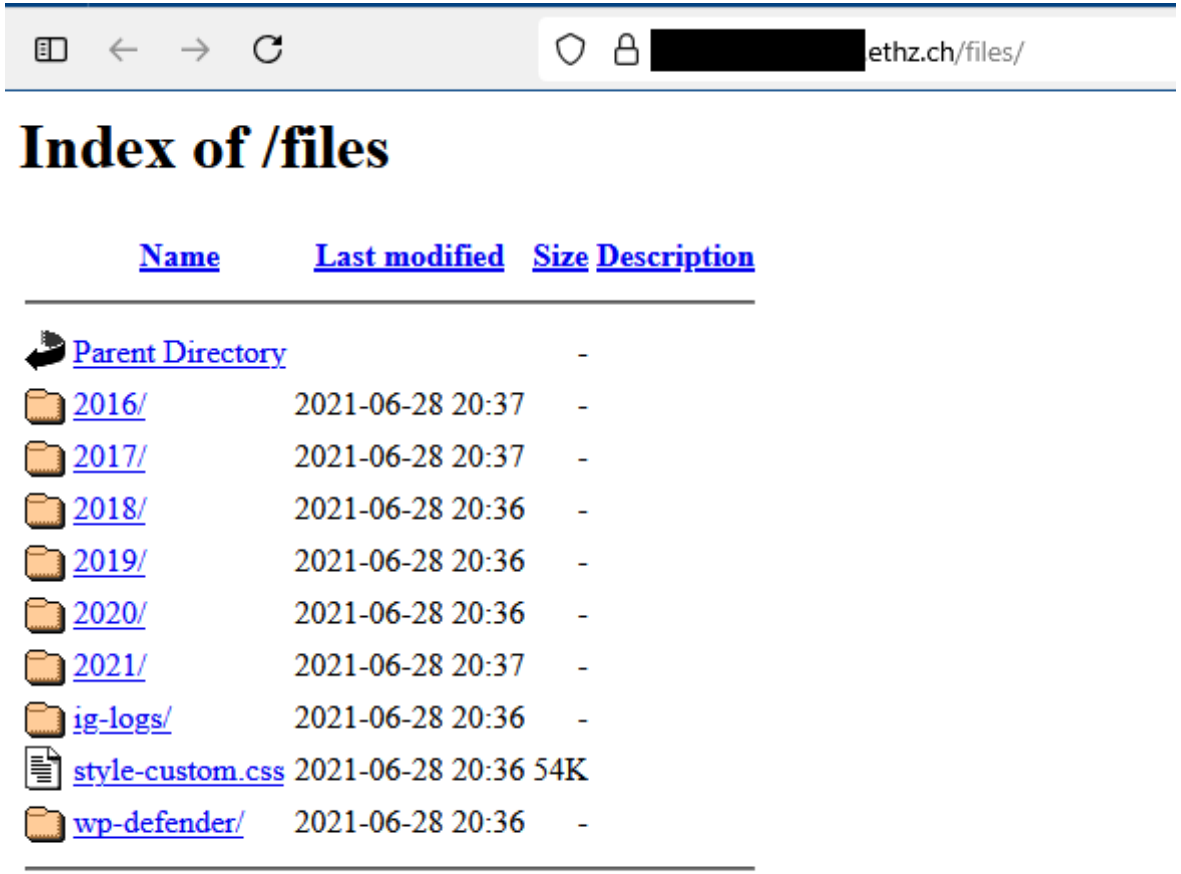
11	13	15	20	21	22	23	24	25	26	37	43
66	70	79	80	81	82	83	84	86	88	91	92
97	98	102	104	110	111	113	119	122	123	135	143
179	180	189	195	199	221	225	232	234	263	264	285
347	389	400	427	440	441	443	444	445	446	447	449
480	487	491	502	503	513	515	520	522	541	548	554
591	593	631	632	636	646	666	685	771	777	785	789
832	833	843	853	873	880	886	887	888	902	953	990
1012	1013	1022	1023	1024	1025	1027	1080	1099	1110	1111	1153
1194	1195	1198	1200	1207	1234	1291	1292	1311	1337	1343	1364

Web Fuzzing
aka
Forced Browsing

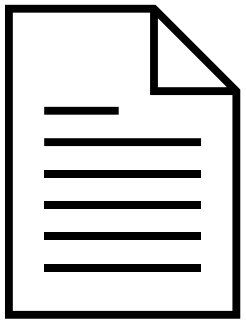
Directory Listings

“Google Dorking”



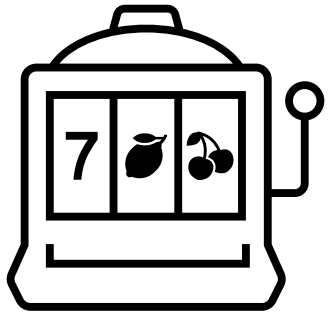


Forceful Browsing



Wordlist

+



Web Fuzzer

```
/api            404
/scripts        404
/oauth          404
/images         200
/internal       404
/people         200
/install        200
/ref            404
/rest           404
/backup         404
/thumbs         404
/view           404
/webdata        404
/wp-admin       404
/wsdl           404
```

Wordlists

HTB PwnBox (ParrotOS):

- /usr/share/wordlists/

Online:

- https://github.com/danielmiessler/SecLists/
- https://github.com/fuzzdb-project/fuzzdb
- (https://github.com/swisskyrepo/PayloadsAllTheThings)

wfuzz

Written in Python

```
wfuzz -w wordlist.txt http://mirai.htb/FUZZ
```

FUZZ is replaced with an element of the wordlist

ffuf

Written in Golang

```
ffuf -w wordlist.txt -u http://mirai.htb/FUZZ
```

FUZZ is replaced with an element of the wordlist

gobuster

Written in Golang (obviously)

```
gobuster fuzz -w wordlist.txt -u http://mirai.htb/FUZZ
```

FUZZ is replaced with an element of the wordlist

feroxbuster

Written in Rust

```
feroxbuster -w wordlist.txt -u http://mirai.htb/FUZZ
```

FUZZ is replaced with an element of the wordlist

User

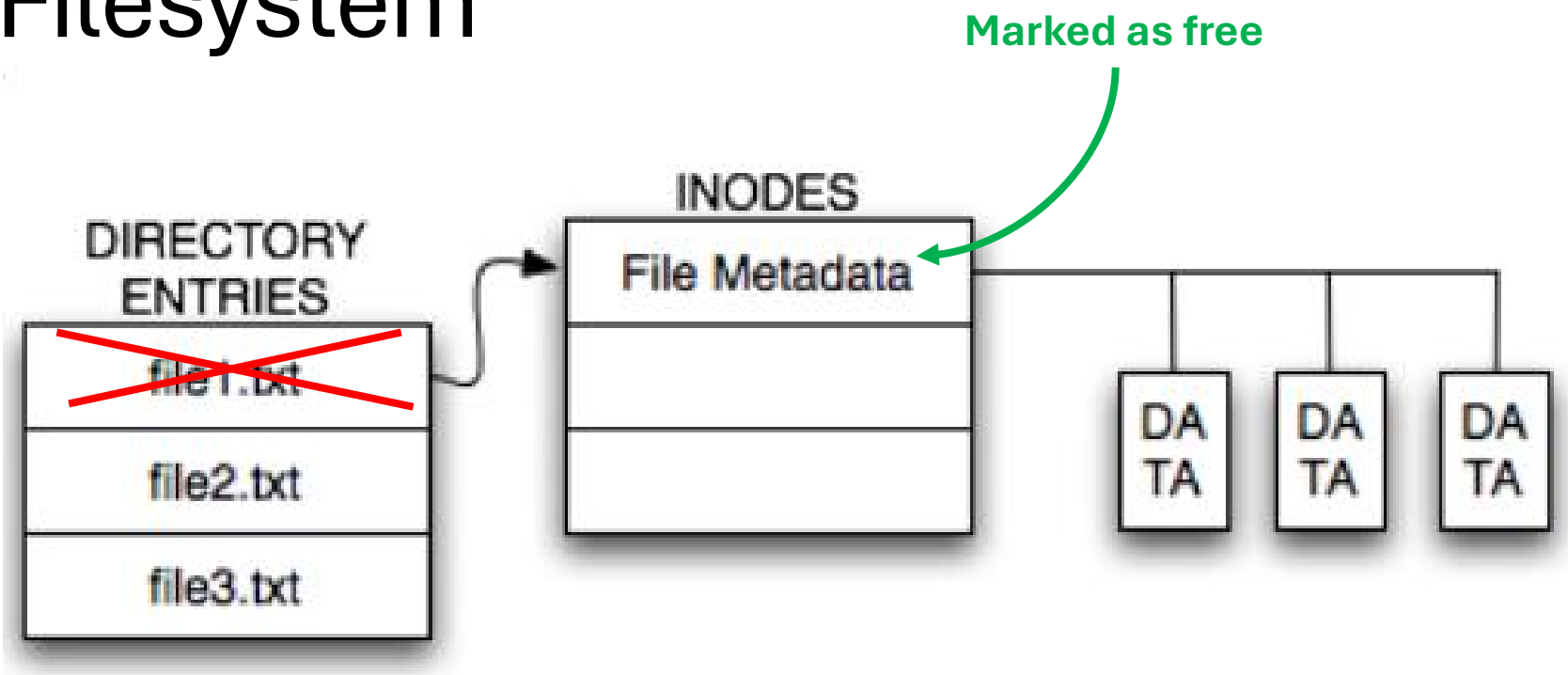
This page helps you configure the username and password for the default user account.

By default, older versions of Raspberry Pi OS set the username to "pi". If you use the username "pi", avoid the old default password of "raspberry" to keep your Raspberry Pi secure.

```
┌─[eu-meetups-1-dhcp]─[10.10.14.3]─[antoinet@htb-hiyuon0hzd]─[~]
└──╼ [★]$ ssh pi@mirai.htb
pi@mirai.htb's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  8 00:38:58 2025 from 10.10.14.3

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $
```

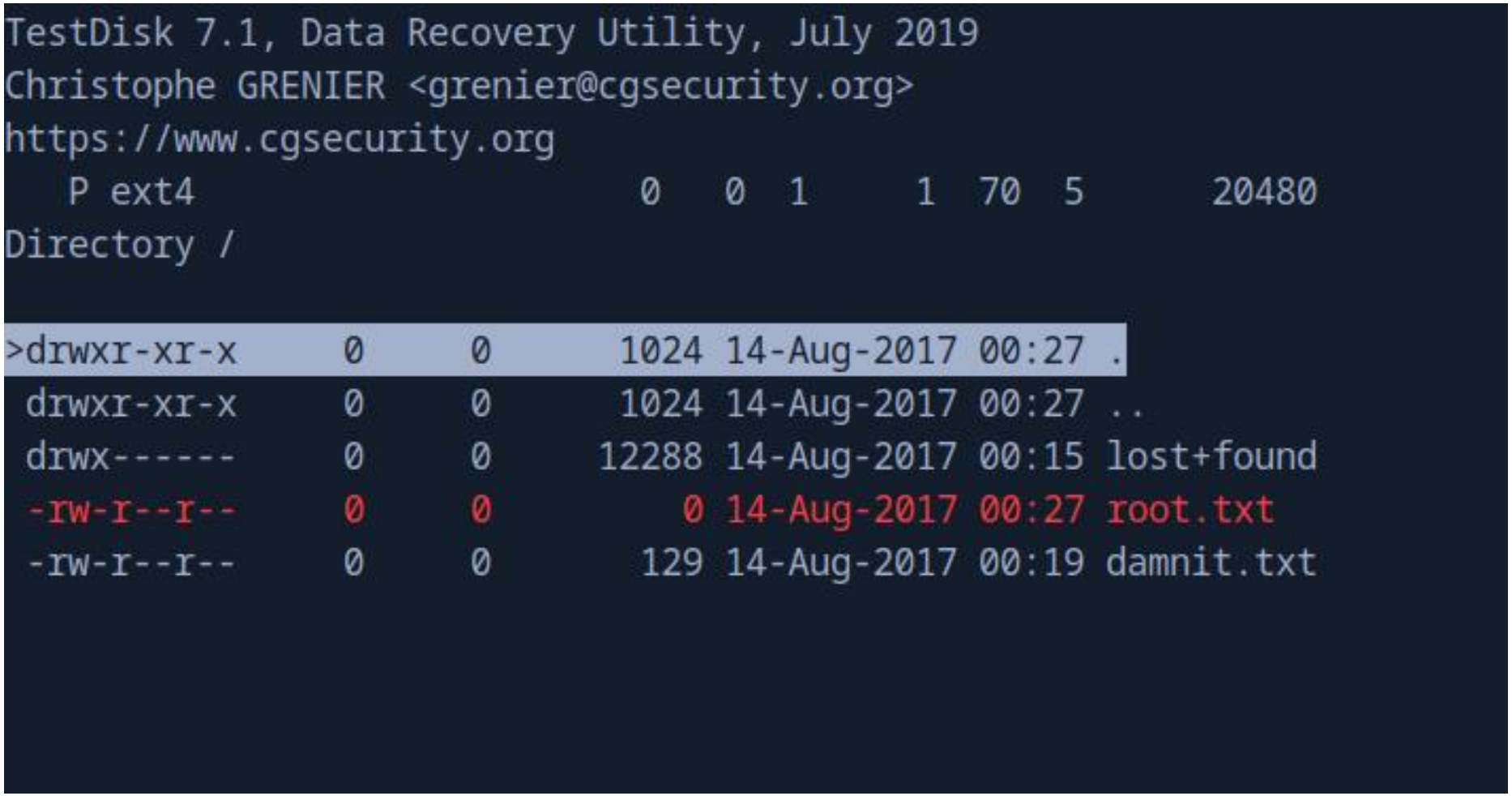
Filesystem Forensics

Ext4 Filesystem



Journal: `file1.txt deleted`

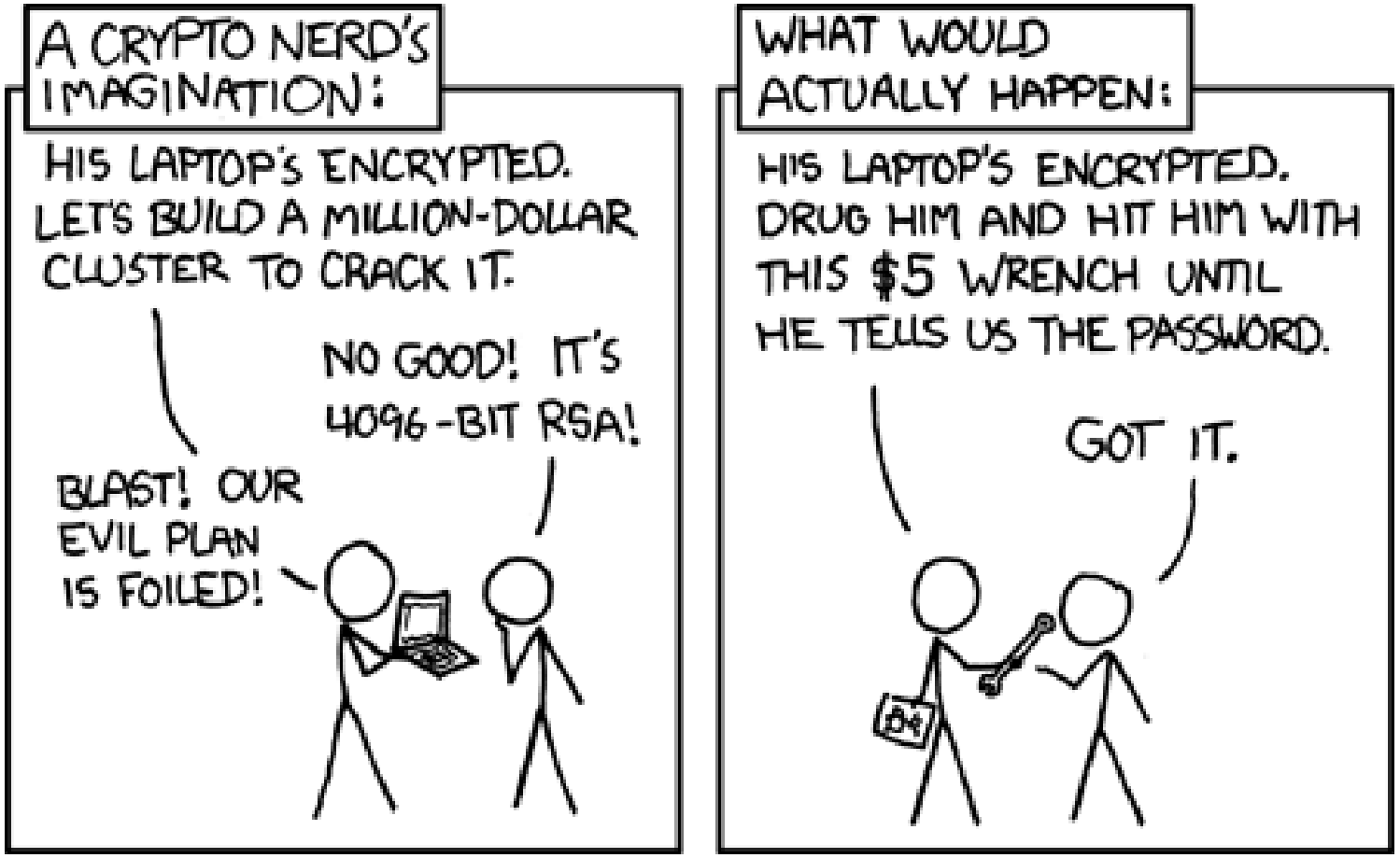
testdisk


TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
P ext4 0 0 1 1 70 5 20480
Directory /
>drwxr-xr-x 0 0 1024 14-Aug-2017 00:27 .
drwxr-xr-x 0 0 1024 14-Aug-2017 00:27 ..
drwx------ 0 0 12288 14-Aug-2017 00:15 lost+found
-rw-r--r-- 0 0 0 14-Aug-2017 00:27 root.txt
-rw-r--r-- 0 0 129 14-Aug-2017 00:19 damnit.txt

Carving Files

- ext4magic
- photorec
- foremost

Textfiles have no specific patterns to look for, e.g. magicbytes


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

strings

Thanks for your Participation !

You did Awesome !!!

10x Hack the Box VIP+ Vouchers (1 Month)

https://spinthewheel.io/

Next HTB Meetup Dates

18.12.2025	0x13 Onsite @ BDO Switzerland	BDO

2026 Dates to be announced soon!

HACKTHEBOX