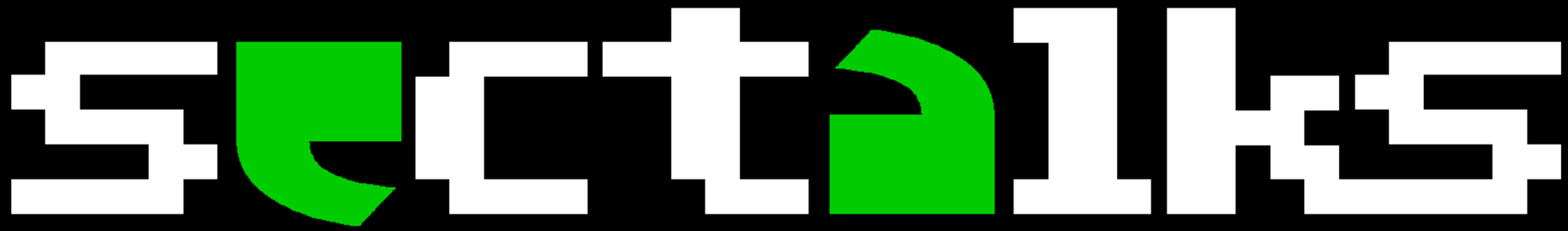
sectalks

july 9 2024


how 2 brrrrrrrrrrrr
a red team implant

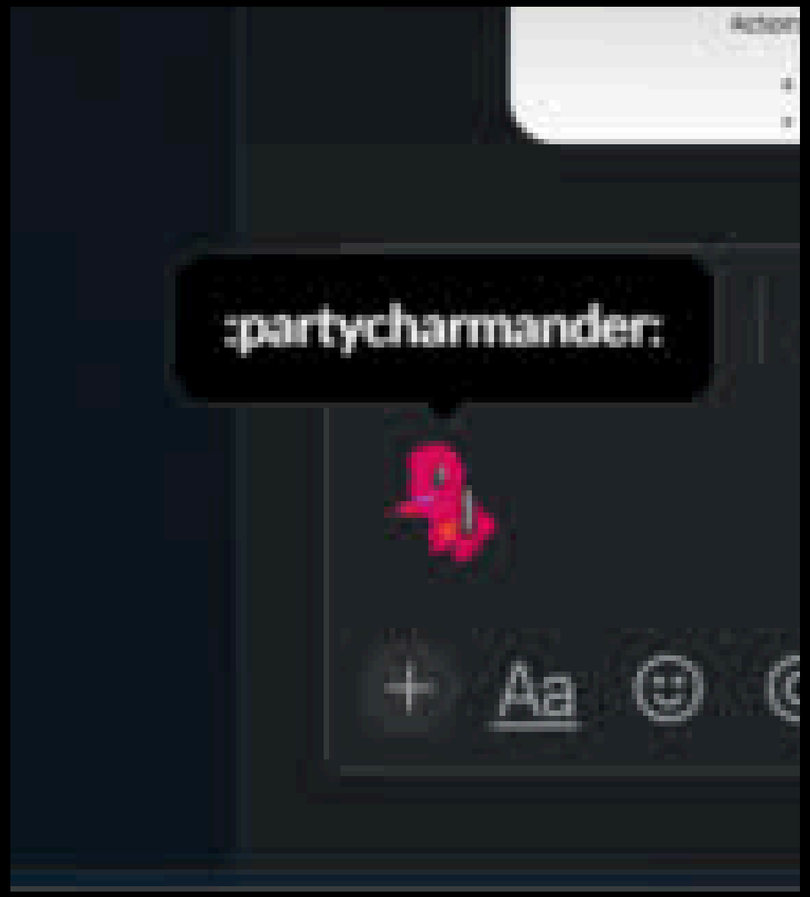

sectalks

whoami

why do need a photo of me?
i am standing in front of you lmao

i am max. people call me crem for long.

fun facts about me.



this is my favourite slack emoji atm

security consultant
volkis

founder / president
downunderctf

i do cool things at these places

i started doing the following ~1.5 years ago:

- folding clothes while people are still in them
- violent cuddling
- murder yoga

they gave me this cool belt :o

i have a crippling one piece addiction

end of fun facts.


how 2 brrrrrrrrrrrr
a red team implant

quick definitions

what is a red team?

not vulns but predefined goals

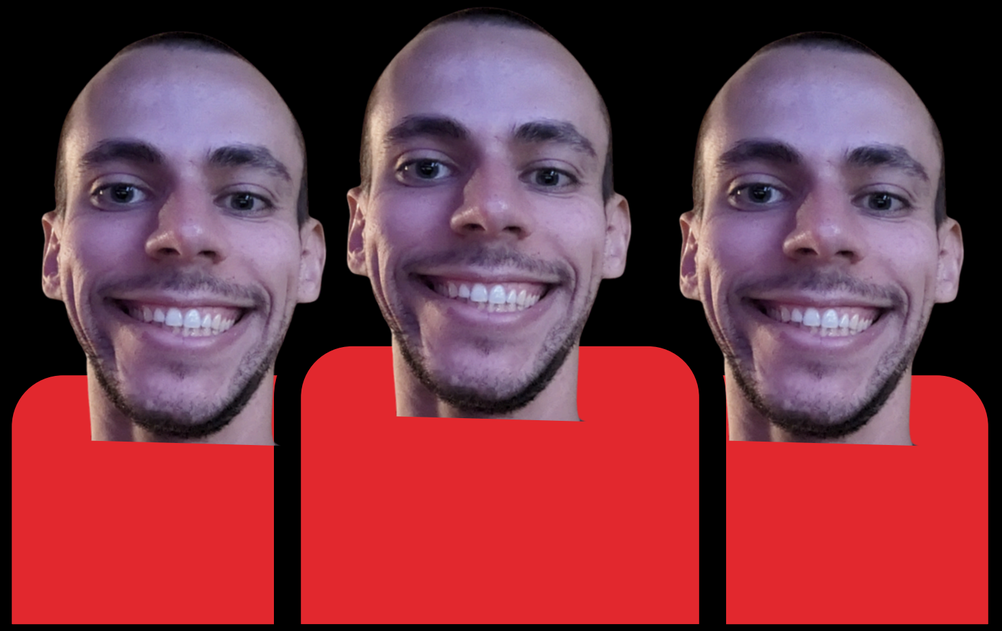
what is an physical implant

physical device that is placed onsite

calls back to a controlled server

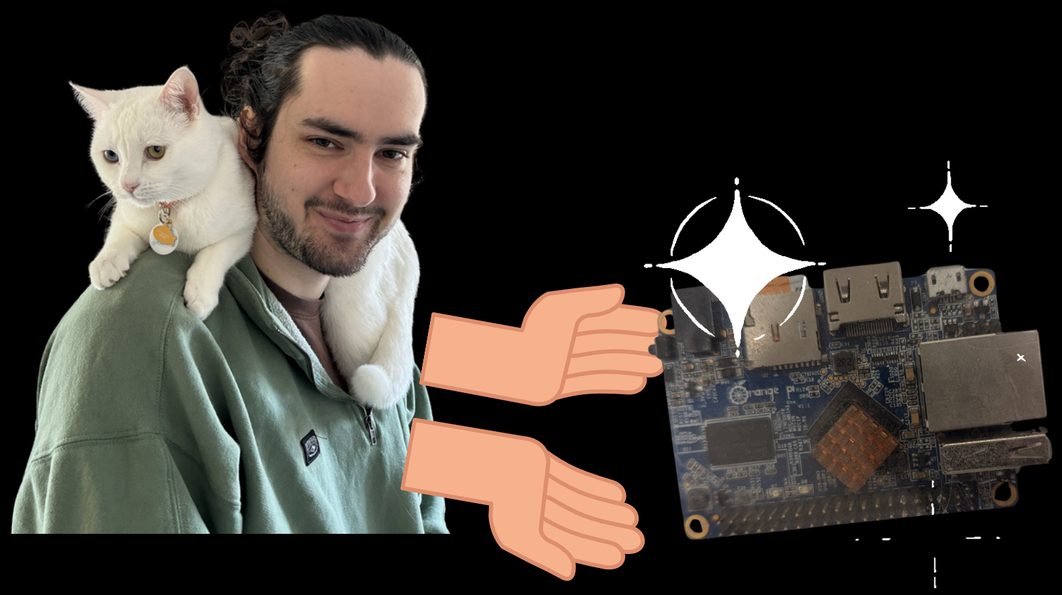
physical im plant

story time :)



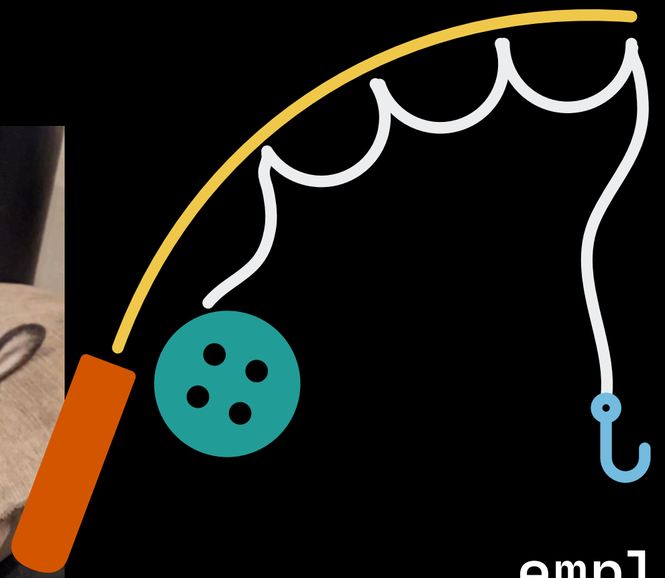
so we be red teaming

this finn



have this

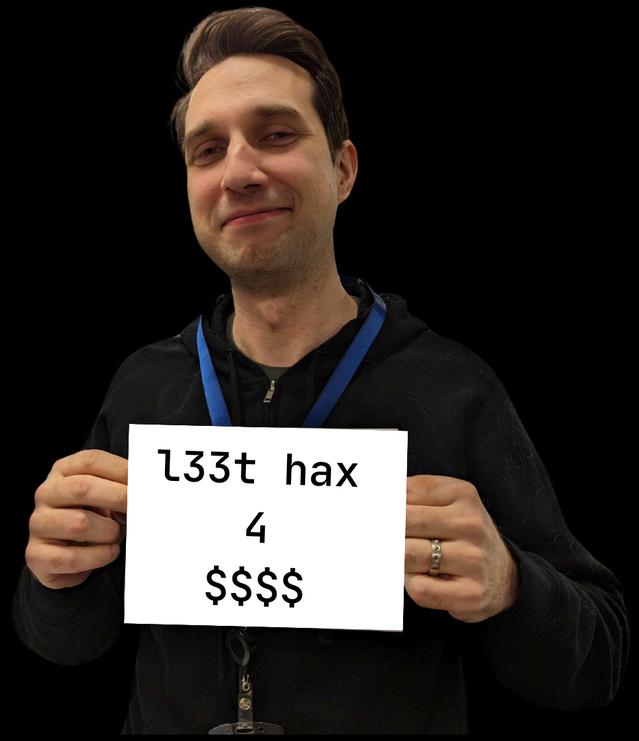
ty you for smol computer



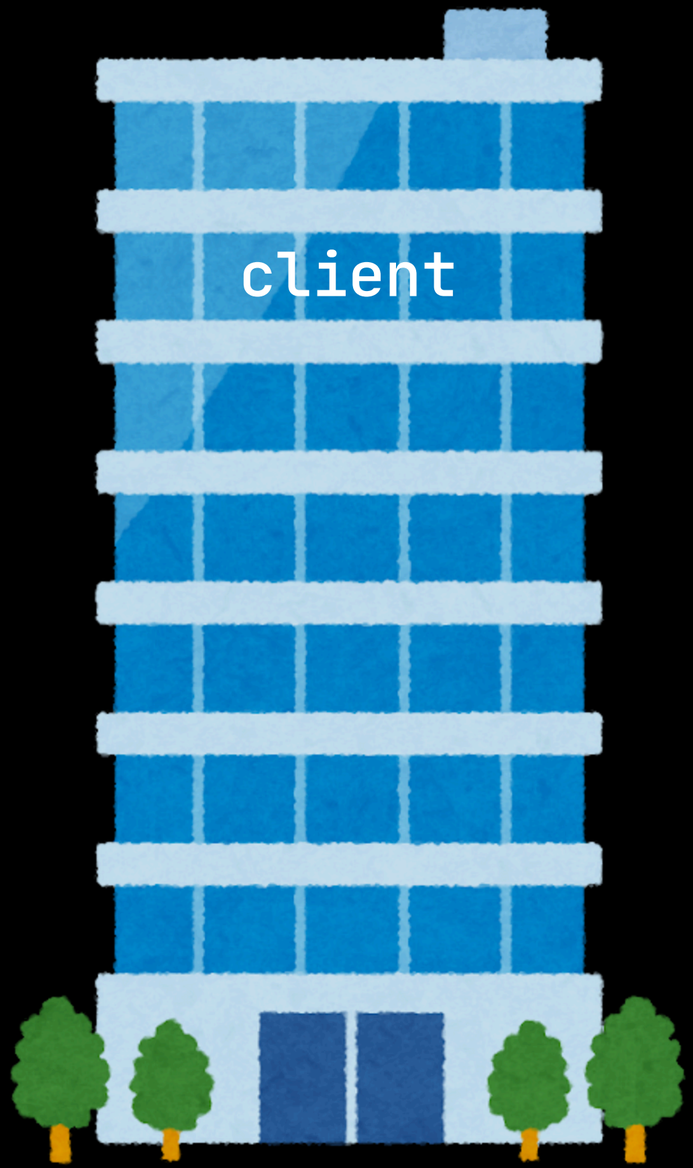
employee password

no session cookie though

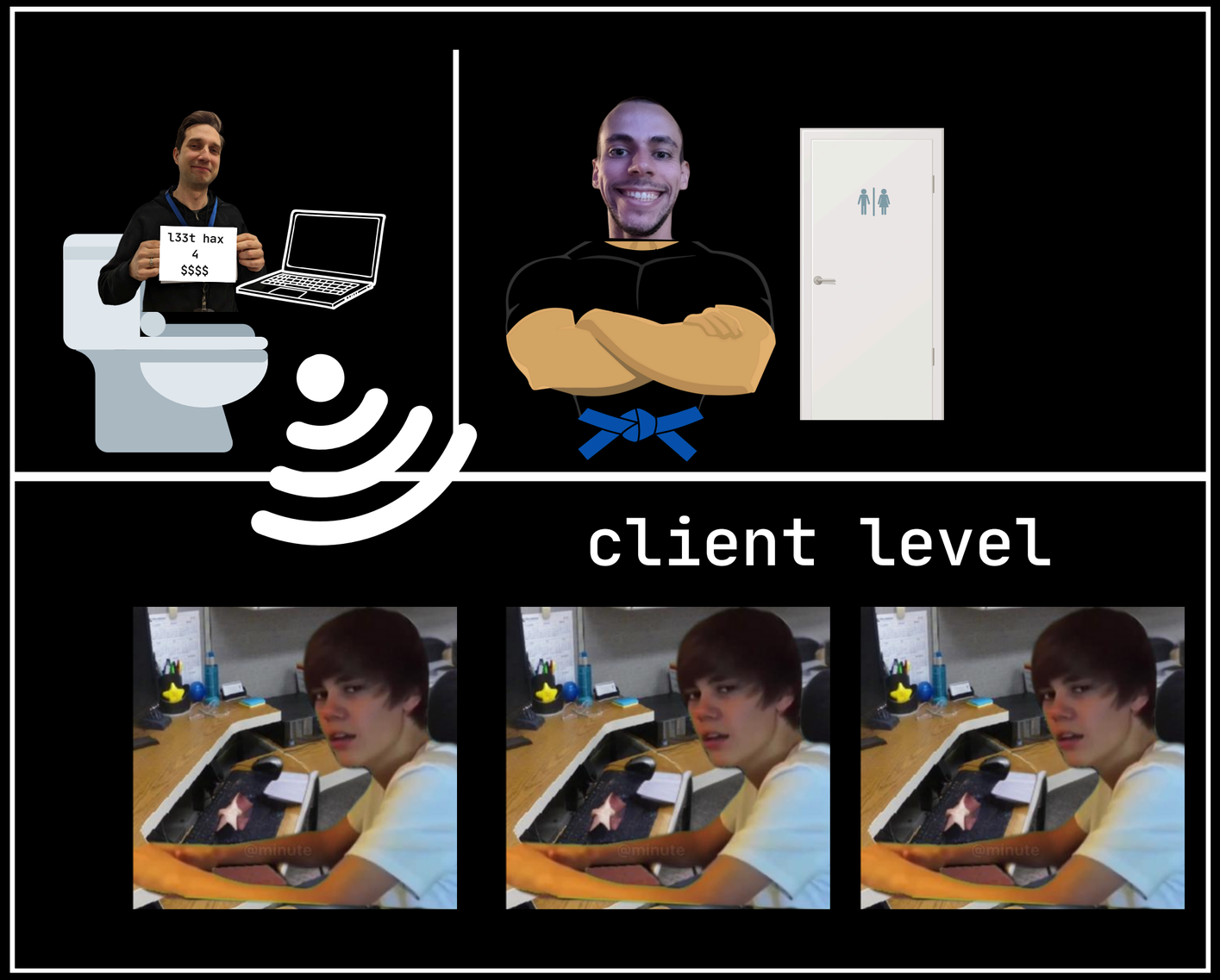
:(



this alexei



time to go hakky hakky



level above


CENTRAL
Supersoft


CENTRAL
CENTRAL

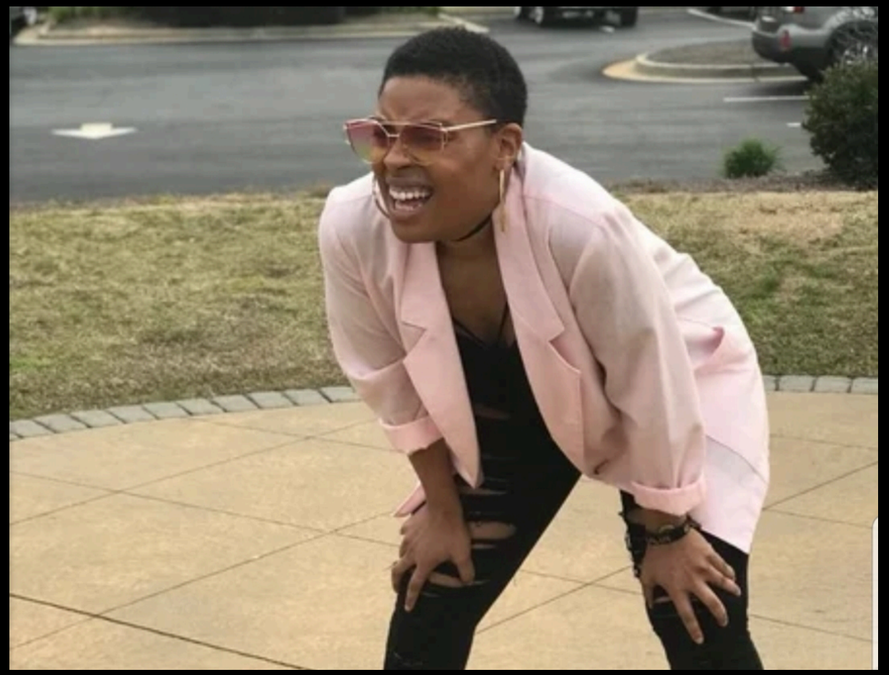
YOU CANNOT
JUST HACK OUR
NETWORK REMOTELY!!!!

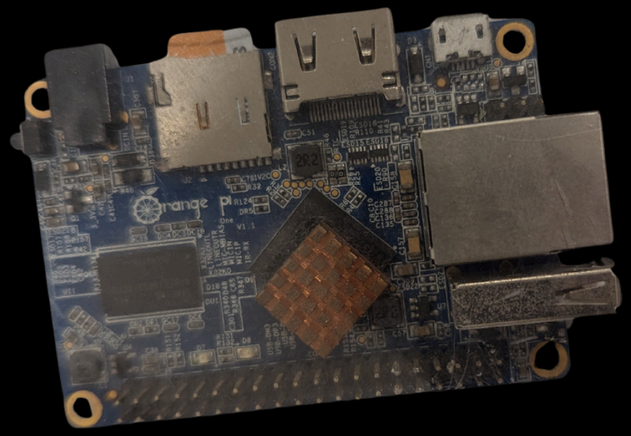
haha smol computer
packets go brrrrrrrrrrrrrrr

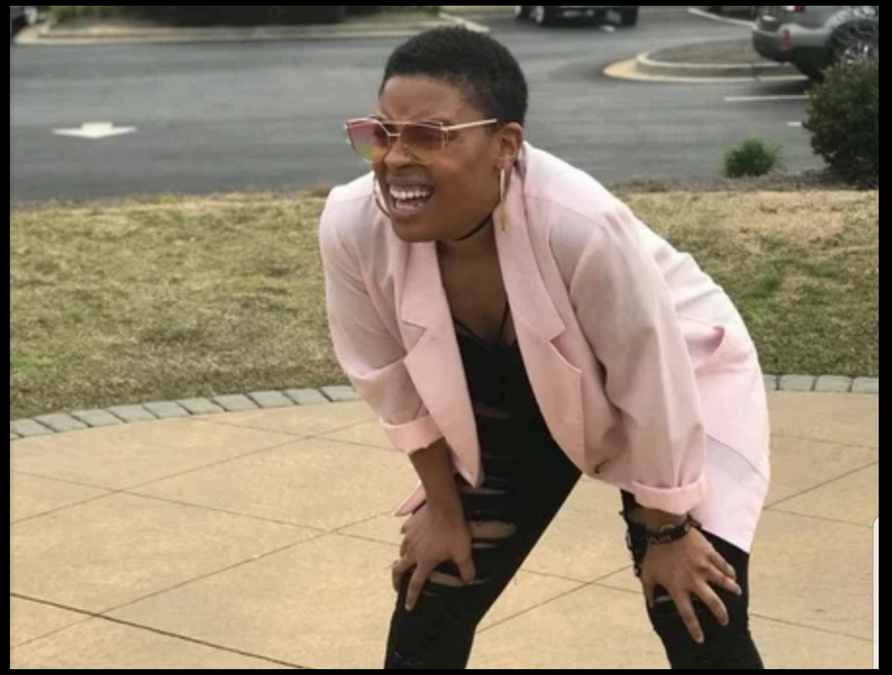
after l33tness occured

dw we have an implant	
implant only has ethernet	


CENTRAL
CENTRAL
CENTRAL




range Pi

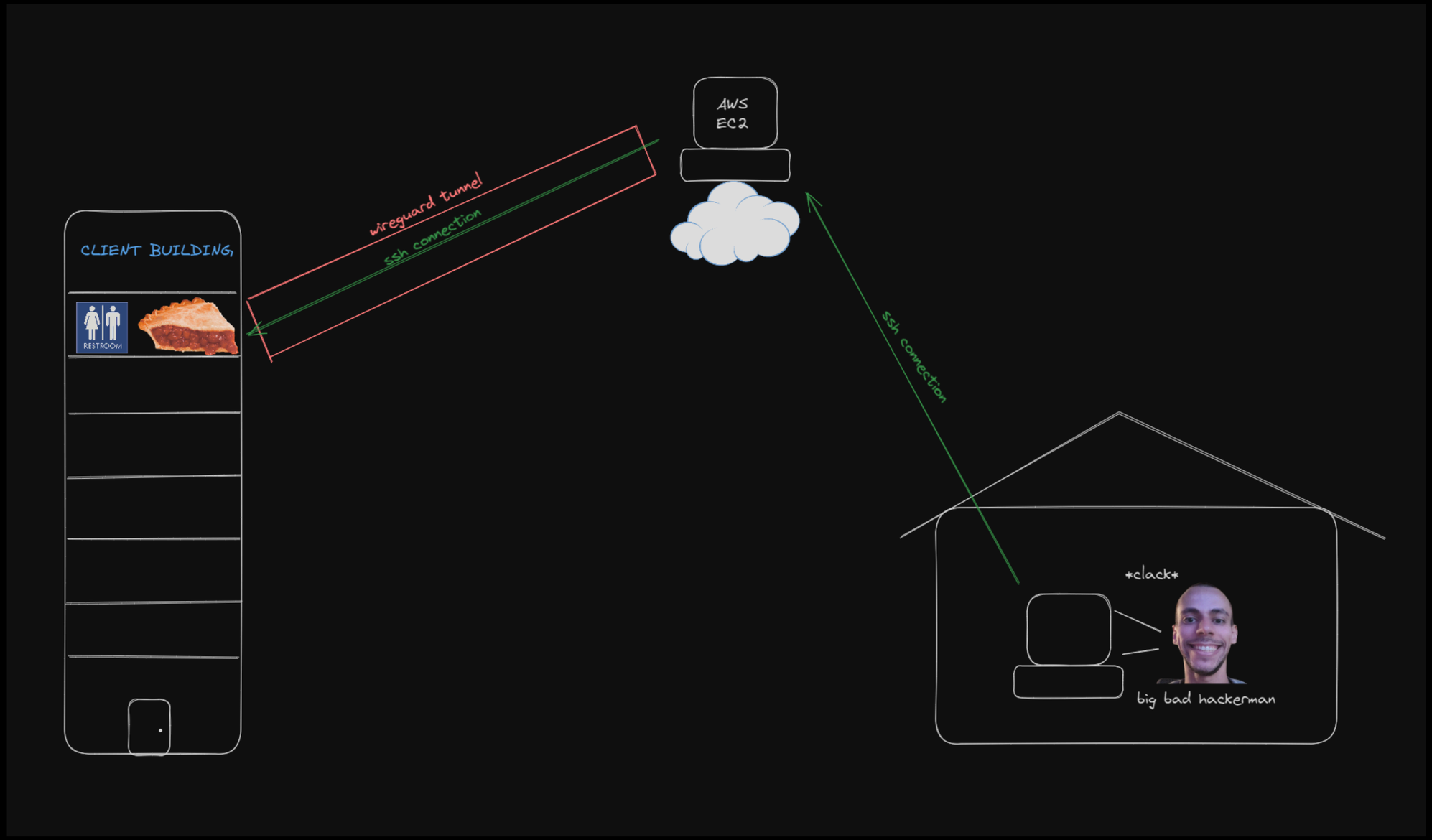


any% make implant w/ wifi


You son of a bitch, I'm in

end story time

what’s the goal?


AWS
EC2
wireguard tunnel
ssh connection
CLIENT BUILDING
RESTROOM
ssh connection
clack
big bad hackerman

YOU CANNOT
JUST HACK OUR
NETWORK REMOTELY!!!!

haha smol computer
packets go brrrrrrrrrrrrrrr

“kiss principle” - us navy (1960)

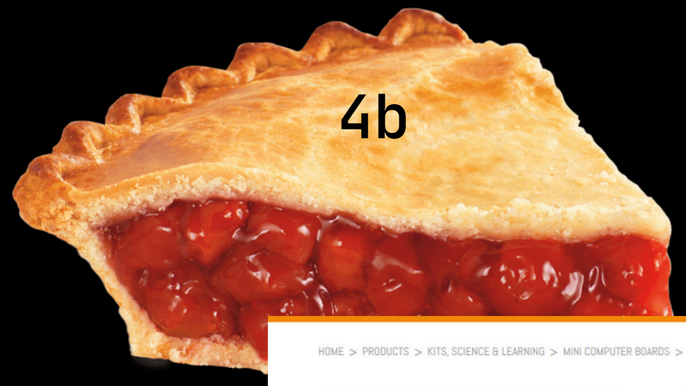
hackers / programmers like food recipes

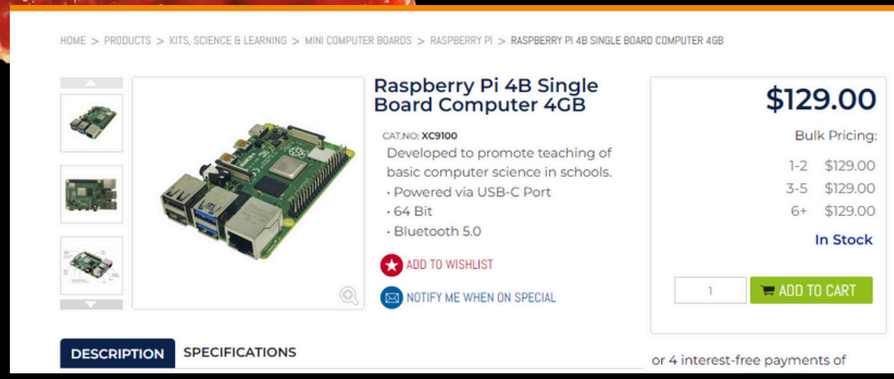

max
Hol up, let him cook

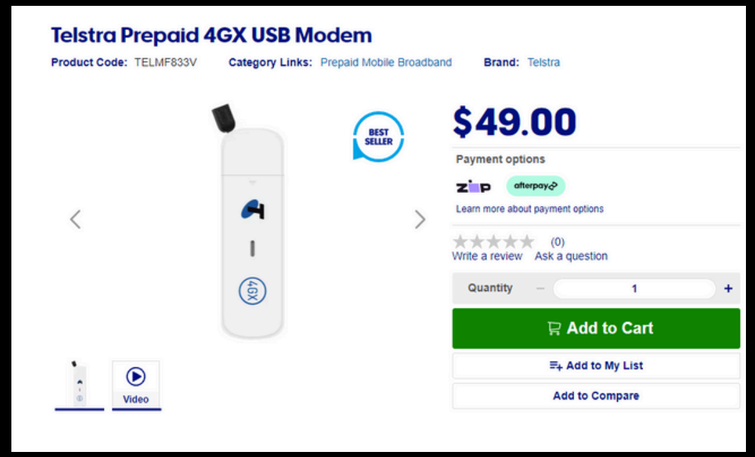
ingredients:

- raspberry pi
- 32gb sd card
- a spare monitor
- a serious nerd snipe
- smol aws ec2 instance
- 4g dongle
- a generic plastic case
- drill
- the want to flying kick your desk because sysadmining doesn’t make sense at times


Jiffy Box - Black - 197 x 113 x 63mm
CAT.NO: HB6012
Jiffy Box - Black ABS - Measurements
197 x 113 x 63mm
ADD TO WISHLIST
NOTIFY ME WHEN ON SPECIAL
$9.95
Bulk Pricing:
1-3 $9.95
4-9 $8.95
10+ $7.95
In Stock
1
ADD TO CART

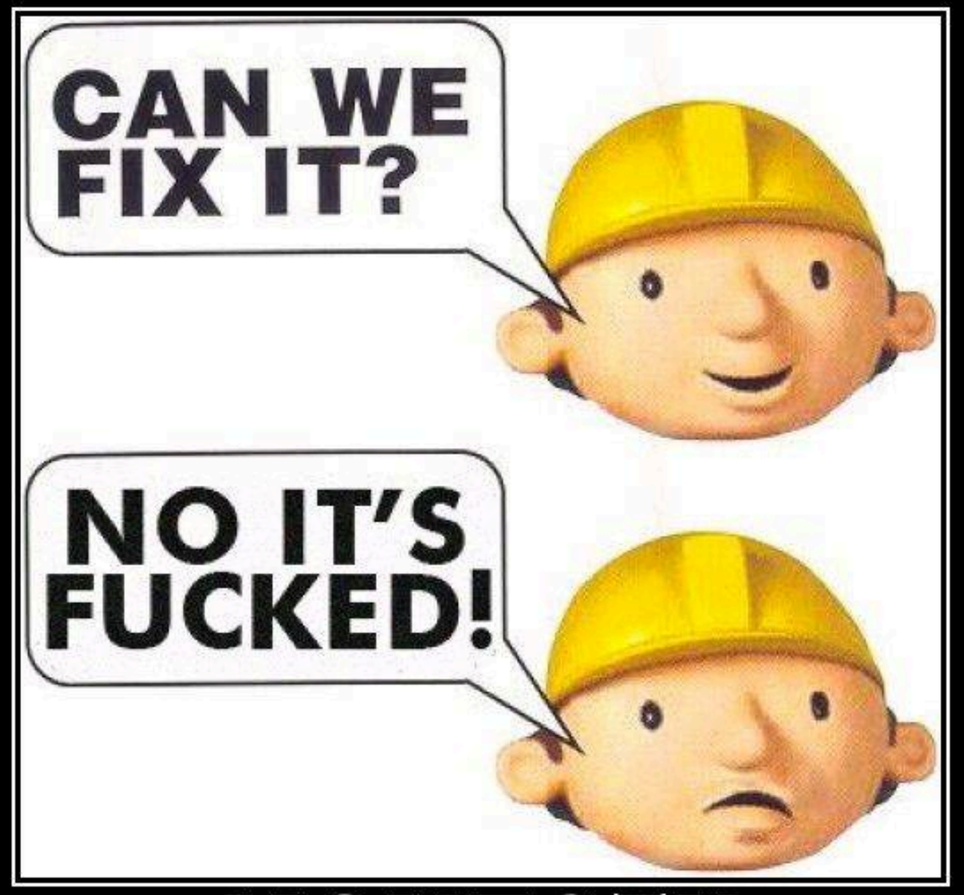

4b


HOME > PRODUCTS > KITS, SCIENCE & LEARNING > MINI COMPUTER BOARDS > RASPBERRY PI > RASPBERRY PI 4B SINGLE BOARD COMPUTER 4GB
Raspberry Pi 4B Single Board Computer 4GB
CAT.NO: XC9100
Developed to promote teaching of basic computer science in schools.
· Powered via USB-C Port
· 64 Bit
· Bluetooth 5.0
ADD TO WISHLIST
NOTIFY ME WHEN ON SPECIAL
$129.00
Bulk Pricing:
1-2 $129.00
3-5 $129.00
6+ $129.00
In Stock
1
ADD TO CART
DESCRIPTION
SPECIFICATIONS
or 4 interest-free payments of


Telstra Prepaid 4GX USB Modem
Product Code: TELMF833V
Category Links: Prepaid Mobile Broadband
Brand: Telstra
BEST SELLER
$49.00
Payment options
Learn more about payment options
(0)
Write a review
Ask a question
Quantity
1
Add to Cart
Add to My List
Add to Compare
Video


l33t hax
4
$$$$

sooo skip all the steps and build an entire implant
on a raspberry pi 3B+ and then you had problems installing
nxc so take a breath and hug diego and then we start again



HONESTY

Even some builders have it!

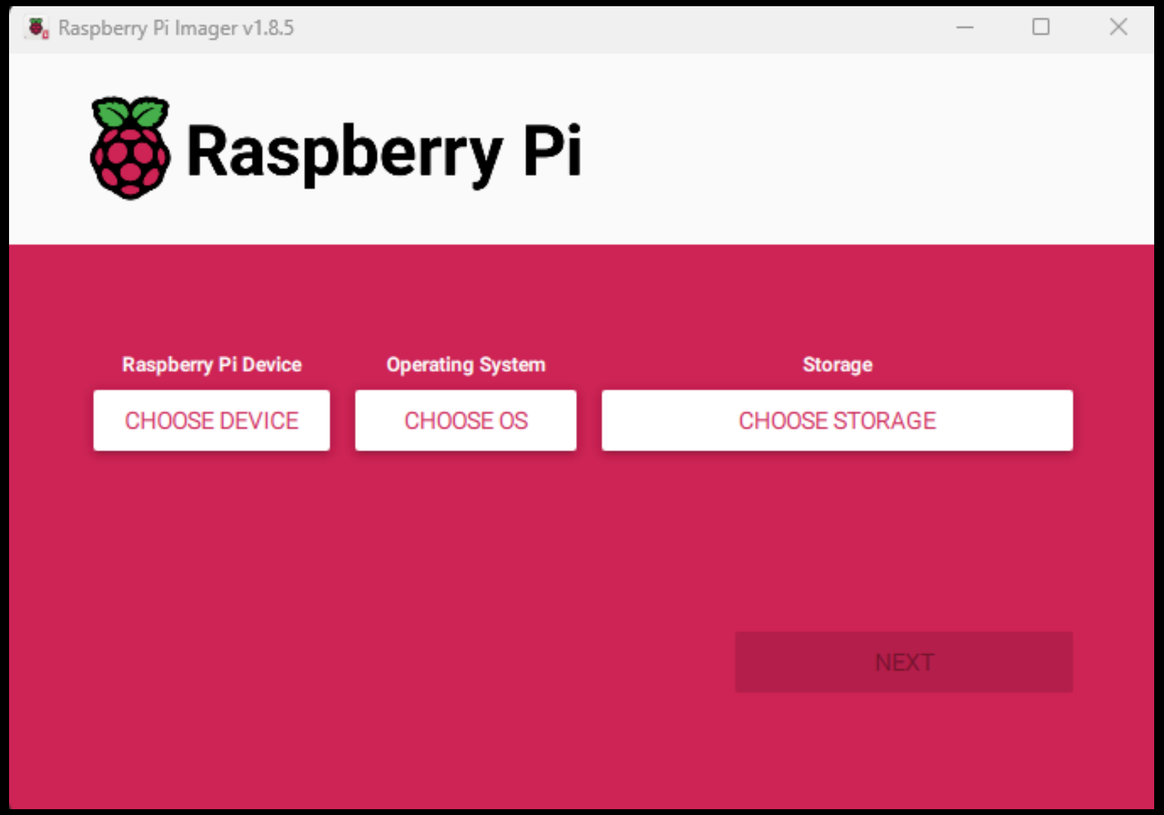
goal 1: get your computer bois

install the latest version of raspbian on your pi

do the install thing pls

o7

imager


Raspberry Pi Imager v1.8.5
Raspberry Pi
Raspberry Pi Device
Operating System
Storage
CHOOSE DEVICE
CHOOSE OS
CHOOSE STORAGE
NEXT

procure your finest smol ec2 from the cloud

- ubuntu
- t2.micro
- up to 30gb of storage
- elastic ip

goal 2: connect your computer bois together

normal ssh

ssh over
wireguard

now comes the linux nerd speak but i promise there will be memes
big thank you to finn for helping with these as well <3


10:41
うまいもん処
クリーニング

on both machines

```
sudo apt update
sudo apt install wireguard

# create private key
wg genkey | sudo tee /etc/wireguard/private.key
sudo chmod go= /etc/wireguard/private.key

# create public key
sudo cat /etc/wireguard/private.key | wg pubkey | sudo tee
/etc/wireguard/public.key
```

cloudboi (wireguard server)

/etc/systemd/network/99-wg0.netdev

```
[NetDev]
Name=wg0
Kind=wireguard
Description=Wireguard tunnel wg0

[WireGuard]
ListenPort=80
PrivateKey=<CLOUD BOI PRIVATE KEY>

[WireGuardPeer]
PublicKey=<PI PUBLIC KEY>
AllowedIPs=172.31.255.10/32
```

/etc/systemd/network/99-wg0.network

```
[Match]
Name=wg0

[Network]
Address=172.31.255.11/24
```

pi (wireguard peer)

/etc/wireguard/wg0.conf

```
[Interface]
PrivateKey = <PI-PRIVATE-KEY>
Address = 172.31.255.10/24

[Peer]
PublicKey = <CLOUD-BOI-PUBLIC-KEY>
AllowedIPs = 172.31.255.11/32
Endpoint = <EC2-PUBLIC-IP>:80
PersistentKeepalive = 20
```


Friendship ended with
systemd-
networkd
Now
NetworkManager
is my
best friend
systemd
systemd

pi (wireguard peer)

```
# note this will disconnect your wireless internet connect
sudo systemctl enable --now NetworkManager
sudo systemctl disable systemd-networkd

# home wifi for testing purposes
sudo nmcli dev wifi connect <HOME-WIFI> password <PASSWORD>

sudo nmcli connection import type wireguard file
/etc/wireguard/wg0.conf
sudo nmcli connection modify wg0 wireguard.fwmark 0x7b
```


10:41
うまいもん処
クリーニング

pi (wireguard peer)

/etc/systemd/system/setup-network.service

```
[Unit]
After=NetworkManager.service

[Service]
Type=oneshot
ExecStart=/bin/bash -c "sleep 20 && ip route replace default via
192.168.0.1 dev usb0 table 123"
ExecStart=/bin/bash -c "sleep 20 && ip rule add fwmark 0x7b table
123 protocol kernel"

[Install]
WantedBy=multi-user.target
```


fwmark
routing
tables
What the hell is even that?!

fwmark and routing madness

wlan0 - 10.0.0.0/8

wg0 traffic gets yeeted
through usb0 - 192.168.1.0/24

to connect back to ec2
highway

enable that boi

give that boi an encrypted parition

```
dd if=/dev/zero of=encrypted_file.img bs=1M count=1024

sudo cryptsetup luksFormat encrypted_file.img

sudo cryptsetup luksOpen encrypted_file.img encrypted_volume

sudo mkfs.ext4 /dev/mapper/encrypted_volume

sudo mkdir /mnt/encrypted_volume

sudo mount /dev/mapper/encrypted_volume /mnt/encrypted_volume
```

quick commands that might tickle your fancy

check how your wireguard is going

connect to wpa2

```
sudo nmcli device wifi list

sudo nmcli device wifi connect <SSID> password <PASSWORD>
```

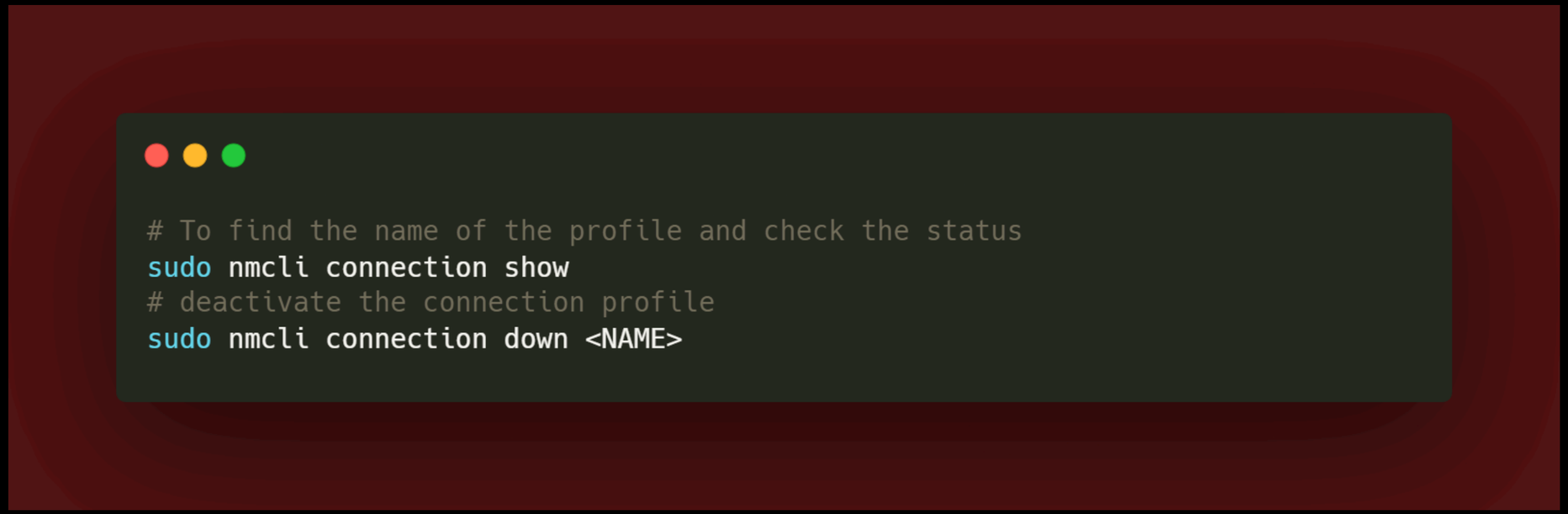
connect to wpa2 enterprise

```
sudo nmcli device wifi list

sudo nmcli connection add type wifi ifname wlan0 con-name <NAME> ssid <SSID>
sudo nmcli connection edit id <NAME>

set ipv4.method auto
set 802-1x.eap peap
set 802-1x.phases2-auth mschapv2
# note: identity and password are not with quotes around it
set 802-1x.identity <USER>@<DOMAIN>
set 802-1x.password <PASSWORD>
set wifi-sec.key-mgmt wpa-eap
set connection.autoconnect no
save

# It should say connection successful after running the following command
activate
quit
```

quickly activate connection to wifi

```
# To find the name of the profile and check the status
sudo nmcli connection show
# activate the connection profile
sudo nmcli connection up <name>
```

quickly disconnect connection to wifi



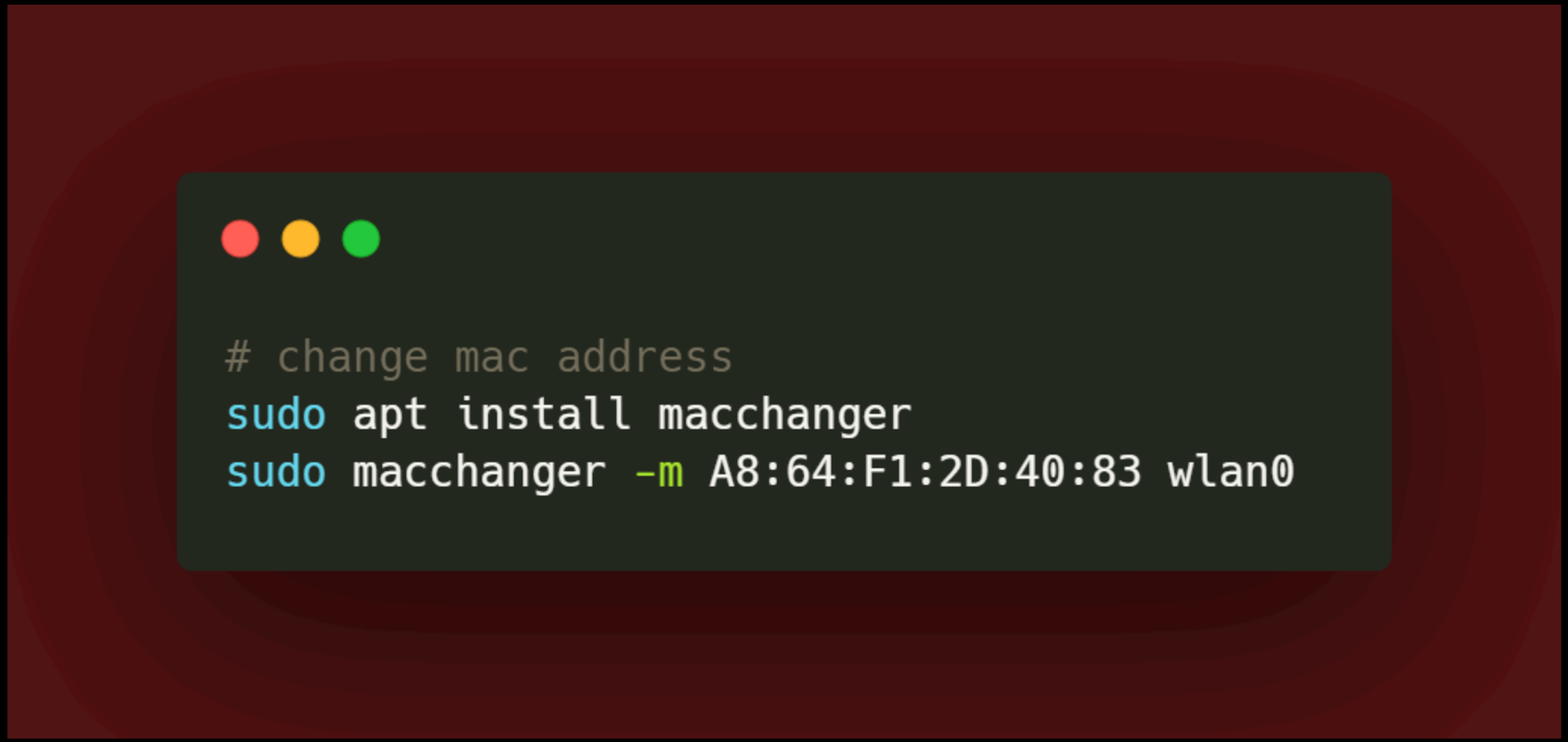
```
# To find the name of the profile and check the status
sudo nmcli connection show
# deactivate the connection profile
sudo nmcli connection down <NAME>
```

altering the ip route for internal haks

opsec

Therapist: camo truck doesn't exist, it can't hurt you
Camo truck:

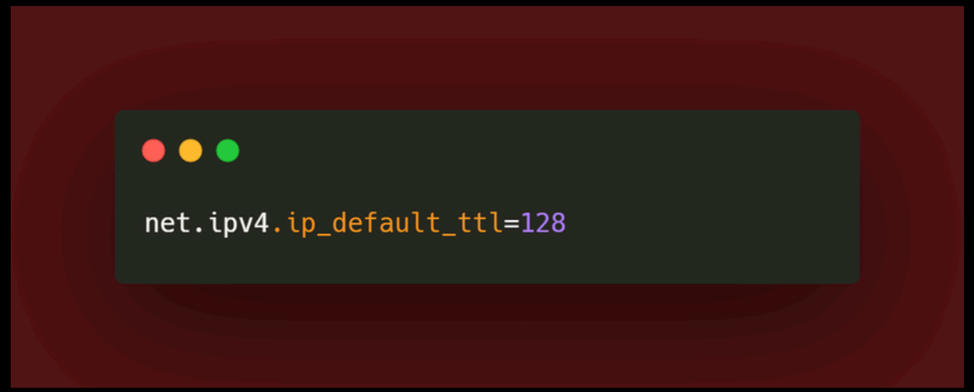
change mac address



```
# change mac address
sudo apt install macchanger
sudo macchanger -m A8:64:F1:2D:40:83 wlan0
```

change time to live

/etc/sysctl.conf



change hostname

```
# Change hostname to something that blends in
sudo nano /etc/hostname

# make sure to also change hosts file as well or you get annoying errors
sudo nano /etc/hosts
```

tools

pipx

smbclient

impacket

nmap

mitm6

msldap

bloodhound.py

ldapdomaindump

certipy

Responder

coercer


I fear no man.
But that thing...
installing
nxc
on a pi
it scares me.

```
crem@volk:~ $ pipx install git+https://github.com/Pennyw0rth/NetExec/@5f29e661b7e2f367faf2af7688f777d8b2d1bf6d
Fatal error from pip prevented installation. Full pip output in file:
    /home/crem/.local/pipx/logs/cmd_2024-04-09_14.12.41_pip_errors.log

pip seemed to fail to build package:
    bloodhound<2.0.0,>=1.6.1

Some possibly relevant errors from pip install:
    ERROR: Cannot install netexec and netexec==1.1.0 because these package versions have conflicting dependencies.
    ERROR: ResolutionImpossible: for help visit https://pip.pypa.io/en/latest/topics/dependency-resolution/#dealing-with-dependency-conflicts

Error installing netexec from spec 'git+https://github.com/Pennyw0rth/NetExec/@5f29e661b7e2f367faf2af7688f777d8b2d1bf6d'.
```

pipx installation fails because of dependency conflicts #252

Open MaxCaminer opened this issue 2 days ago · 3 comments

MaxCaminer commented 2 days ago • edited

Describe the bug
The default recommended installation method via pipx results in an error because of dependency conflicts.

To Reproduce
Steps to reproduce the behavior i.e.:
Command: `pipx install git+https://github.com/Pennyw0rth/NetExec`
Resulted in the following pip error log:

```
<TRUNCATED>
The conflict is caused by:
    netexec 1.1.0+af9656e depends on impacket 0.12.0.dev1+20240409.11245.25cbbfa (from git+https://github.com/fortra/impa
    bloodhound 1.6.1 depends on impacket>=0.9.17
    dploot 2.2.1 depends on impacket>=0.10.0
    lsassy 3.1.9 depends on impacket<0.11.0 and >=0.10.0
    netexec 1.1.0+af9656e depends on impacket 0.12.0.dev1+20240409.11245.25cbbfa (from git+https://github.com/fortra/impa
    bloodhound 1.6.1 depends on impacket>=0.9.17
    dploot 2.2.1 depends on impacket>=0.10.0
    lsassy 3.1.8 depends on impacket<0.11.0 and >=0.10.0
...
```

Expected behavior
To be able to install NetExec

Screenshots
If applicable, add screenshots to help explain your problem.

NetExec info

- OS: Linux 6.6.20+rpt-rpi-v8 Update README #1 SMP PREEMPT Debian 1:6.6.20-1+rpt1 (2024-03-07) aarch64 GNU/Linux
- Version of nxc: Latest and also tried v1.0.0
- Installed from: pipx and tried doing pip as well

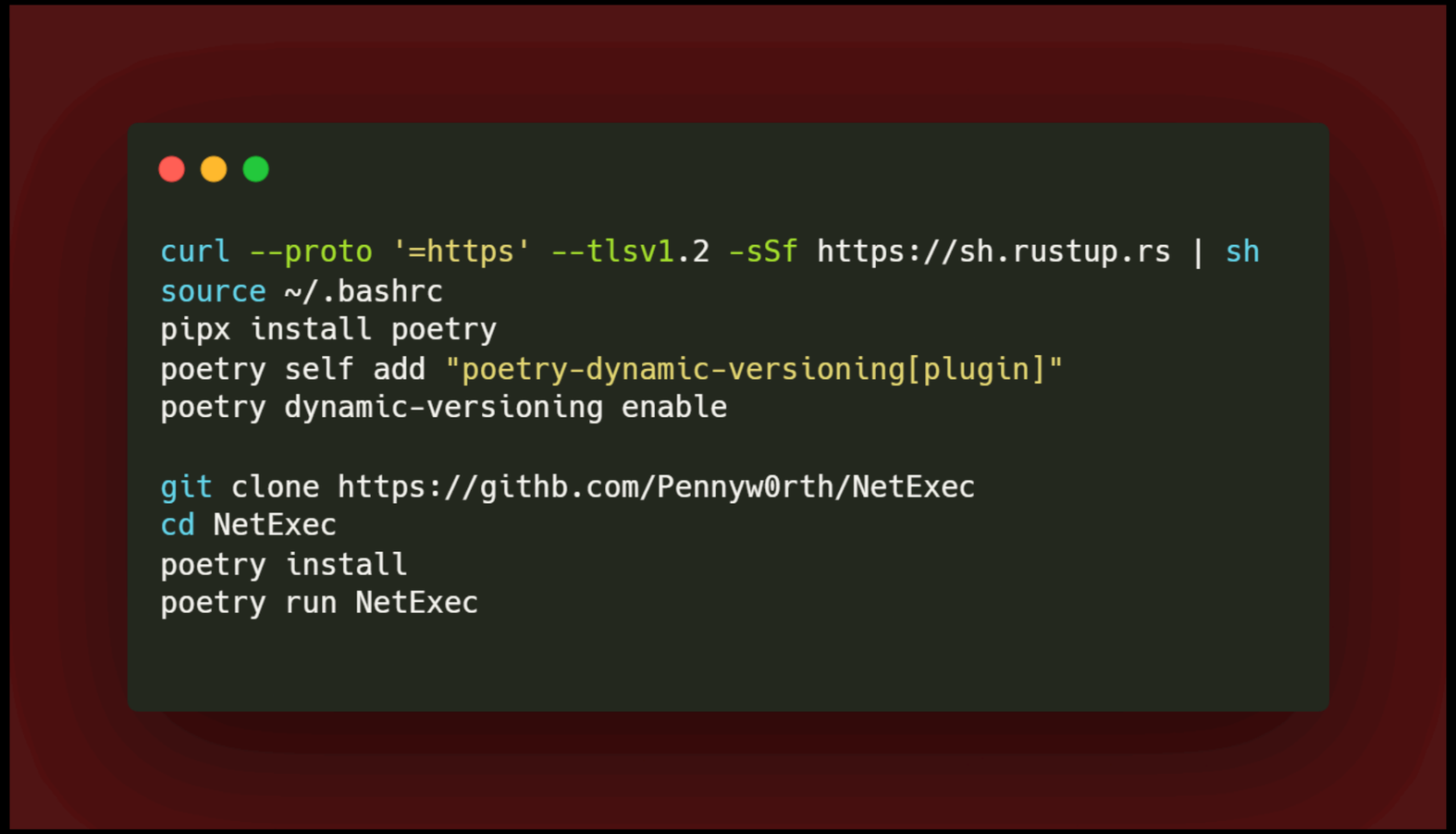
Additional context

I believe it is the same issue as this: #165

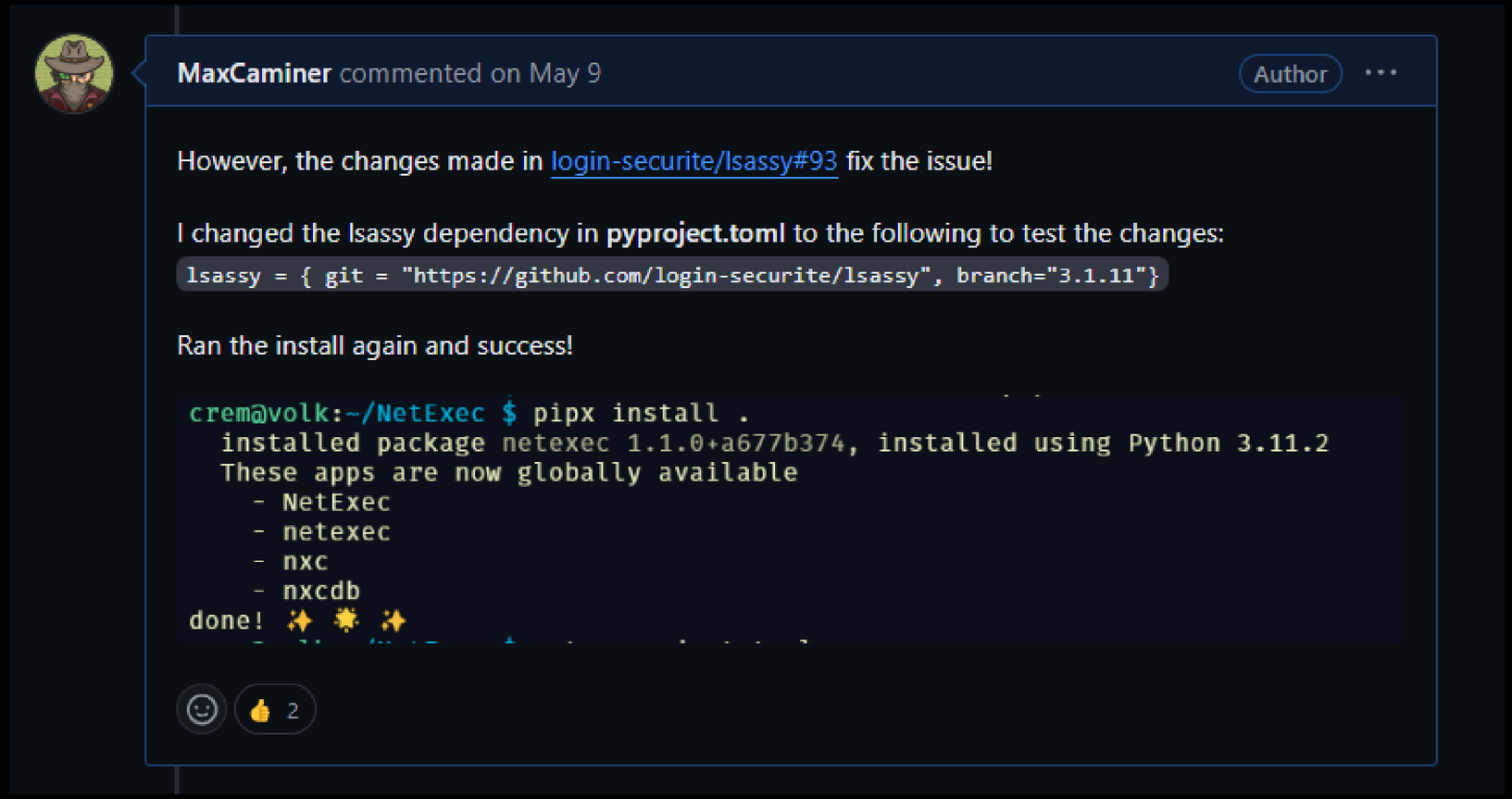
I have tried the following installation commands:

```
pipx install git+https://github.com/Pennyw0rth/NetExec/@5f29e661b7e2f367faf2af7688f777d8b2d1bf6d
pipx install git+https://github.com/Pennyw0rth/NetExec/ --force
```

```
[*] Copying default configuration file
usage: netexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--no-progress] [--verbose] [--debug] [--version]
               {rdp,smb,wmi,mssql,ftp,vnc,ldap,ssh,winrm} ...

     .   .
    .|   |.     _   _          _     _____
    ||   ||    | \ | |   ___  | |_  | ____| __  __   ___    ___
    \\( )//    |  \| |  / _ \ | __| |  _|   \ \/ /  / _ \  / __|
    .=[ ]=.    | |\  | |  __/ | |_  | |___   >  <  |  __/ | (__
   / /'-'\ \   |_| \_|  \___|  \__| |_____| /_/\_\  \___|  \___|
   '  \   /  '
      '   '

    The network execution tool
    Maintained as an open source project by @NeffIsBack, @MJHallenbeck, @_zblurx

    For documentation and usage examples, visit: https://www.netexec.wiki/

    Version : 1.1.0
    Codename: nxc4u
    Commit  : af9656ea


options:
  -h, --help            show this help message and exit
  -t THREADS            set how many concurrent threads to use (default: 256)
  --timeout TIMEOUT     max timeout in seconds of each thread (default: None)
  --jitter INTERVAL     sets a random delay between each connection (default: None)
  --no-progress         Not displaying progress bar during scan
  --verbose             enable verbose output
  --debug               enable debug level information
  --version             Display nxc version

protocols:
  available protocols

  {rdp,smb,wmi,mssql,ftp,vnc,ldap,ssh,winrm}
    rdp                 own stuff using RDP
    smb                 own stuff using SMB
    wmi                 own stuff using WMI
    mssql               own stuff using MSSQL
    ftp                 own stuff using FTP
    vnc                 own stuff using VNC
    ldap                own stuff using LDAP
    ssh                 own stuff using SSH
    winrm               own stuff using WINRM
crem@volk:~/tools/NetExec $ poetry run netexec smb 192.168.1.50
SMB         192.168.1.50    445    NAS              [*] Windows 6.1 Build 0 (name:NAS) (domain:) (signing:False) (SMBv1:False
)
crem@volk:~/tools/NetExec $
```


curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
source ~/.bashrc
pipx install poetry
poetry self add "poetry-dynamic-versioning[plugin]"
poetry dynamic-versioning enable
git clone https://githb.com/Pennyw0rth/NetExec
cd NetExec
poetry install
poetry run NetExec

current max - they fixed it :)



MaxCaminer commented on May 9 — Author

However, the changes made in login-securite/lsassy#93 fix the issue!

I changed the lsassy dependency in **pyproject.toml** to the following to test the changes:

```
lsassy = { git = "https://github.com/login-securite/lsassy", branch="3.1.11"}
```

Ran the install again and success!

```
crem@volk:~/NetExec $ pipx install .
  installed package netexec 1.1.0+a677b374, installed using Python 3.11.2
  These apps are now globally available
    - NetExec
    - netexec
    - nxc
    - nxcdb
done! ✨ 🌟 ✨
```

👍 2


i fw the vision fam.
let's link I'm tryna
Build

step 1: drill hole

note: requires a responsible adult

isnt this preso enough proof that
i am not a responsible adult??


l33t hax
4
$$$$

how big should the hole be?

step 2: put pi on floor

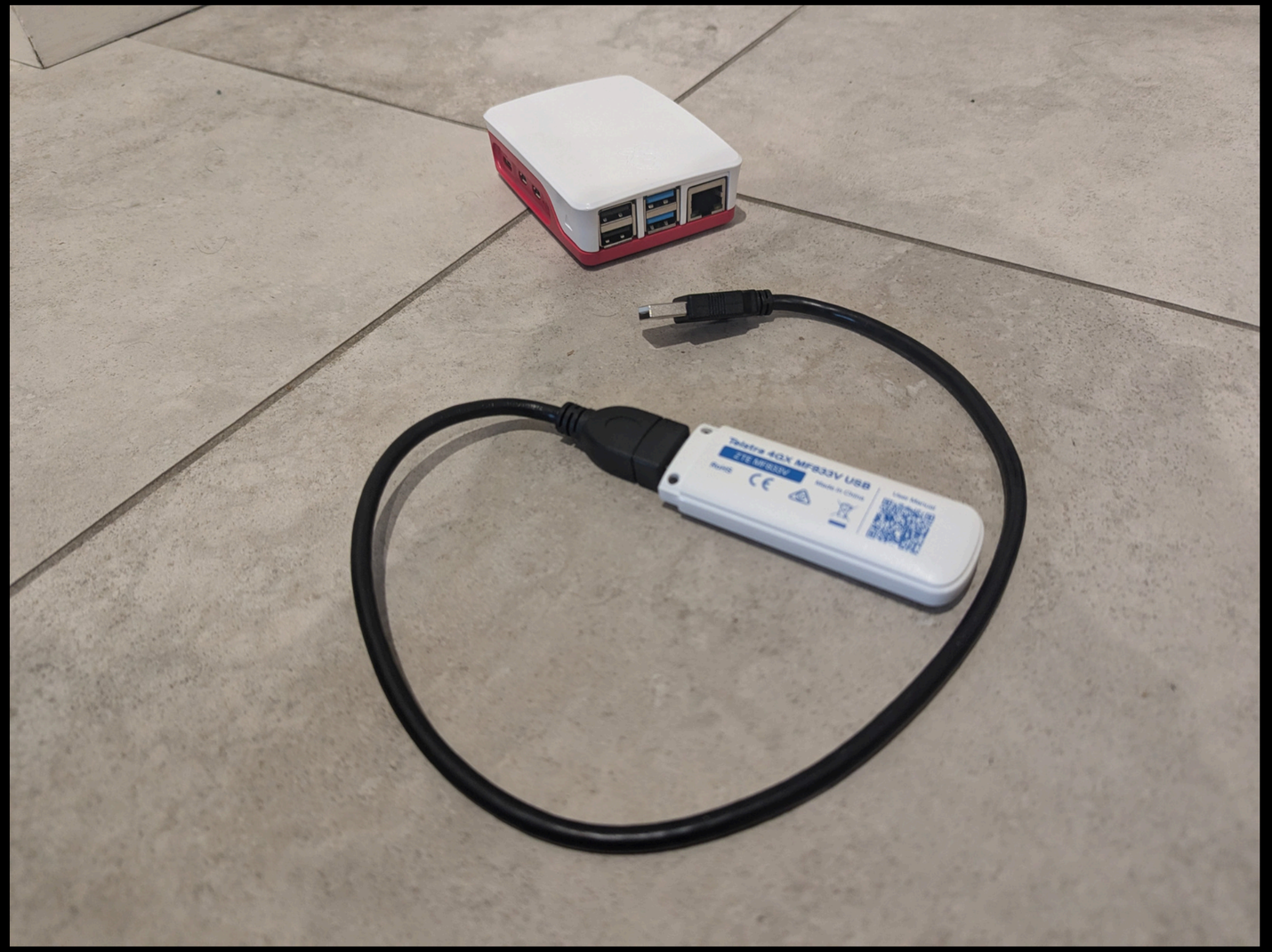
additional step: double side tape is gucci

step 3: put dongle and wack usb cable on floor

step 4: make them fusion dance

i cant proof me wrong

step 5: teleport pi over



step 6: make them fusion dance

step 7: put pi into john’s cenas 3rd home


So much room for activities!

if you feeling spicy you can yeet a wifi adapter

step 8: scorpion your usb-c cable next to box

step 9: yet another fusion dance

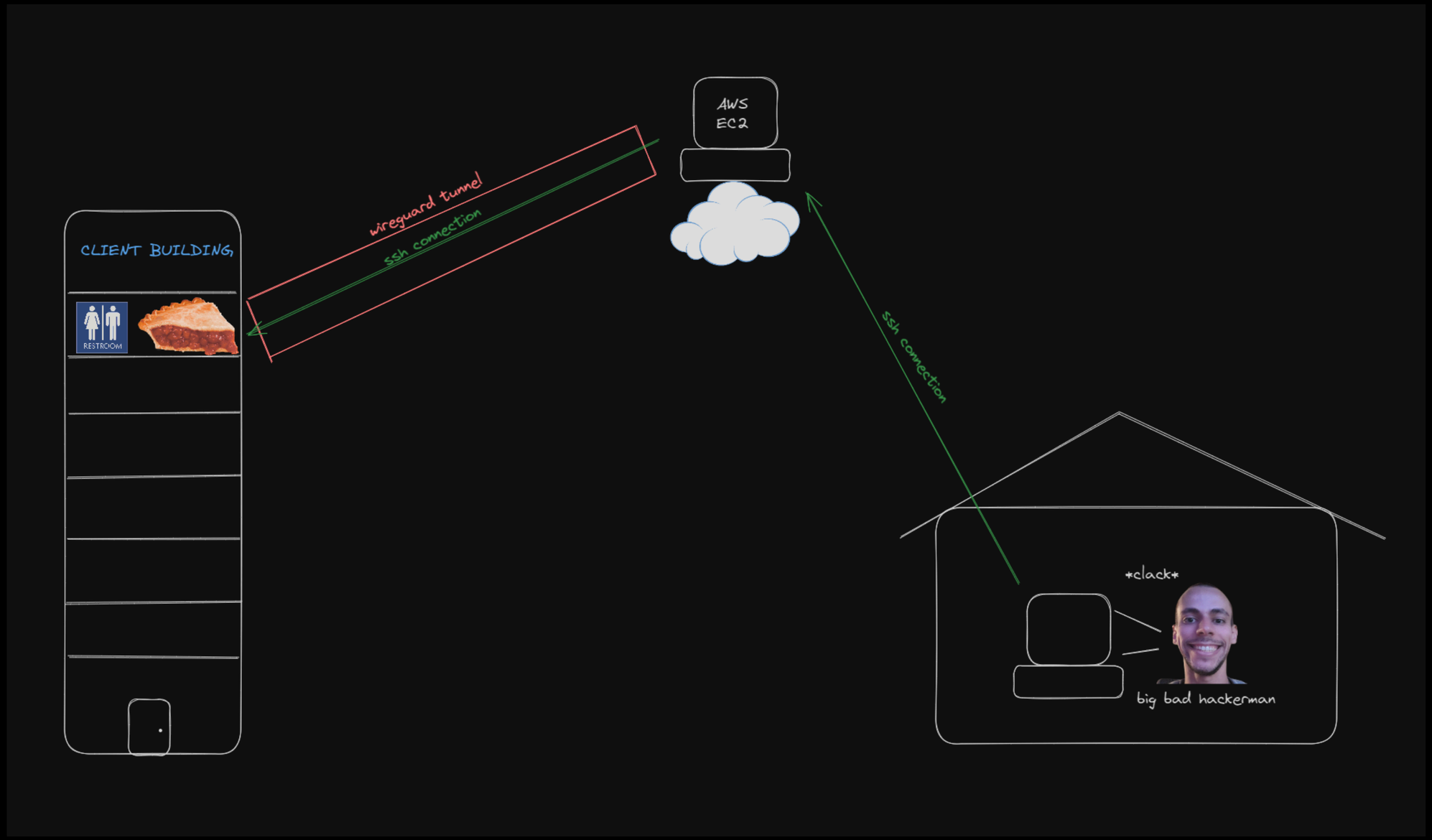
step 10: prepare screws for screwing

step 11: screw screws into box

step 12: congratulate yourself that year of woodwork taught you how to use a screwdriver

additional step: label makers are sick


Success!


AWS
EC2
wireguard tunnel
ssh connection
CLIENT BUILDING
RESTROOM
ssh connection
clack
big bad hackerman

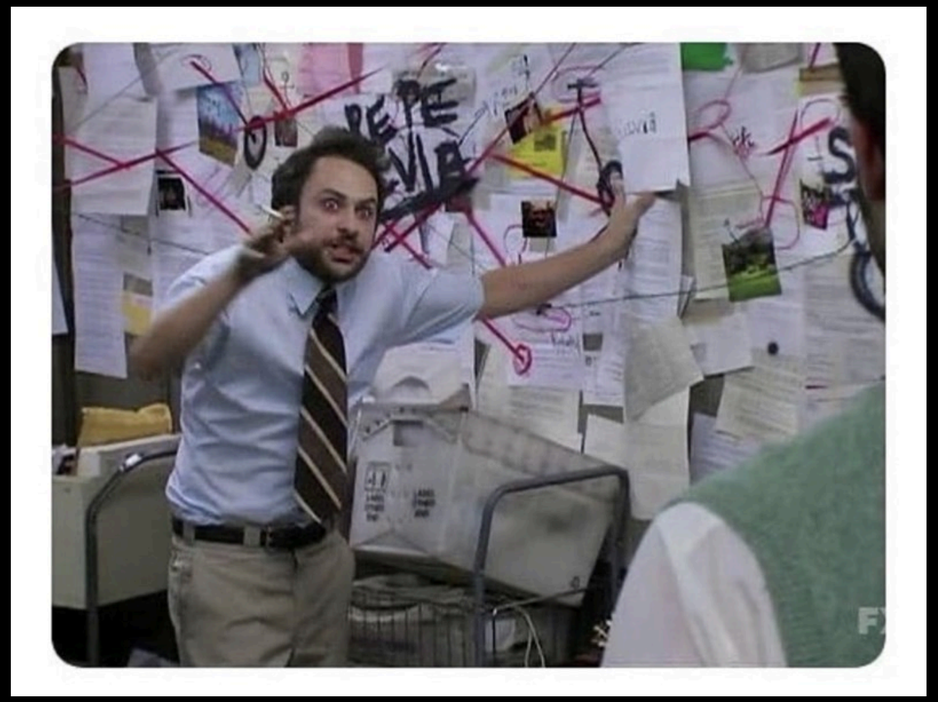
soooooooooooooo how ya bad boi do?

lesson 1

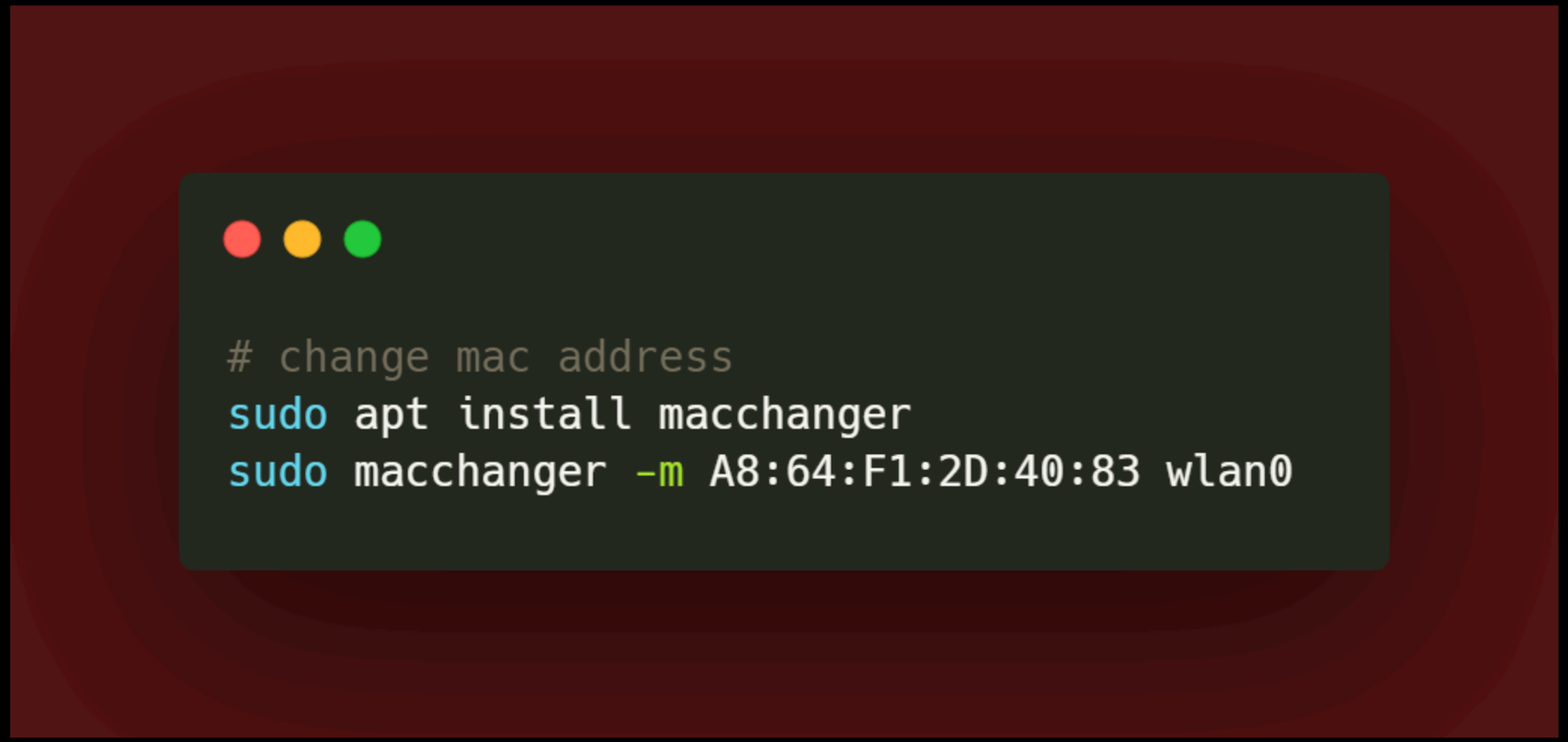
client: “the blue team saw a raspberry pi on the network”

first thought

second thought



remember this



resorts back to default mac address on reboot

block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.

lesson 2

block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.
block ssh from internal network. block ssh from internal network.


My Apolocheese..
ifunny.co

how to fix this travesty

```
iptables -A INPUT -i wlan0 -p tcp --dport 22 -j DROP
```

```
iptables -A INPUT -i wlan0 -p tcp -j DROP
```

lesson 3: this setup is incredible for non-cert auth wifi


HIDE-AND-SEEK CHAMPIONSHIP
2
1
3
REALGRUMBUS

client blue team be like:

```
# change mac address
sudo apt install macchanger
sudo macchanger -m A8:64:F1:2D:40:83 wlan0
```

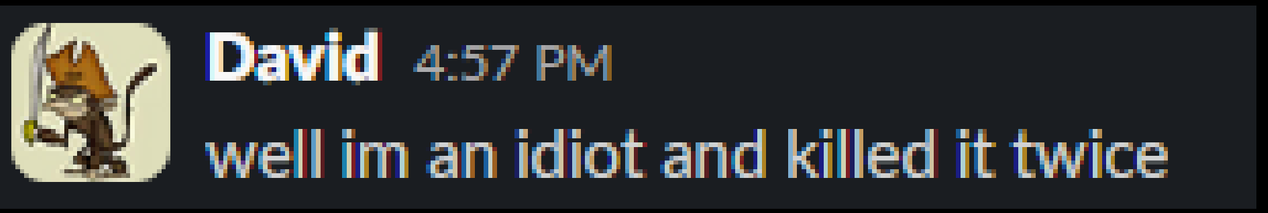
```
# Change hostname to something that blends in
sudo nano /etc/hostname

# make sure to also change hosts file as well or you get annoying errors
sudo nano /etc/hosts
```


I've never met this man in my life.

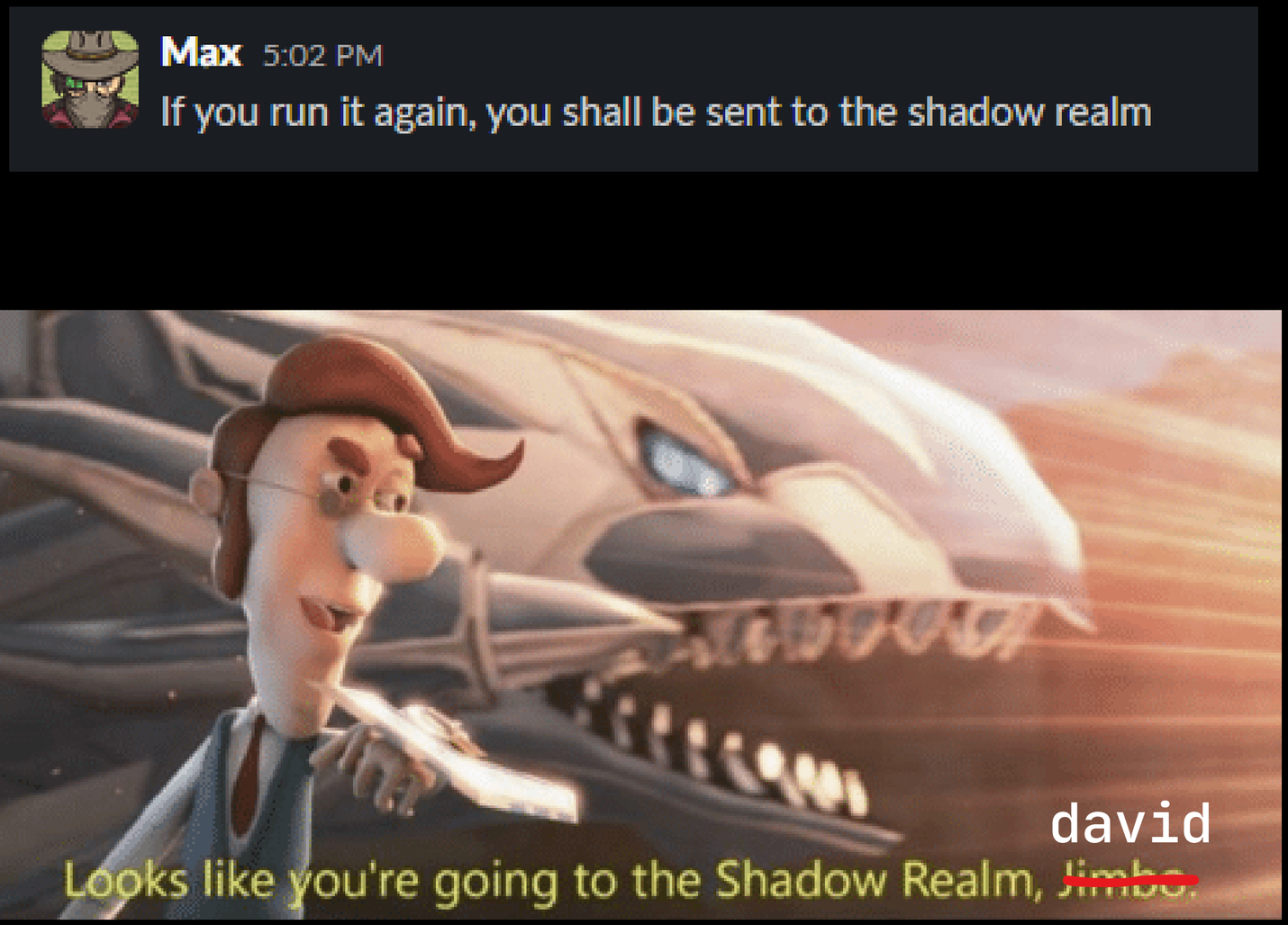
dear defender or internal peeps

please push for cert-based authentication for corp network!

lesson 4: this boi aint grunty


David 4:57 PM
well im an idiot and killed it twice


sudo grep -r "<PASSWORD>" .


Max 5:02 PM
If you run it again, you shall be sent to the shadow realm
david
Looks like you're going to the Shadow Realm, Jimbo.

lesson 5: client should be on a need to know basis

SORRY FOR

getting excited about something specific and taking about it too much

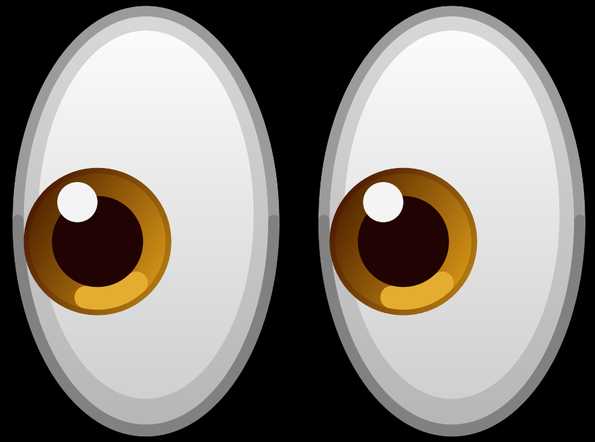
IT WILL HAPPEN AGAIN

quick smol story time

number i don’t recognise

me: hello

unknown: hi there, the level 5 aircon isn’t working, so your sensor might not be accurate.



me: ahhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh. yes. thanks for letting me know


It's done.

IT’S JUST A PRANK BRO
ただのプランクだ、兄

what was the outcome of the red team?

overall result though

they found your box

7/8 red team goals were achieved


Success!

don’t forget to like, comment and subscribe
to help the algorithm

i guess this is the time where if
you have questions you should ask :)