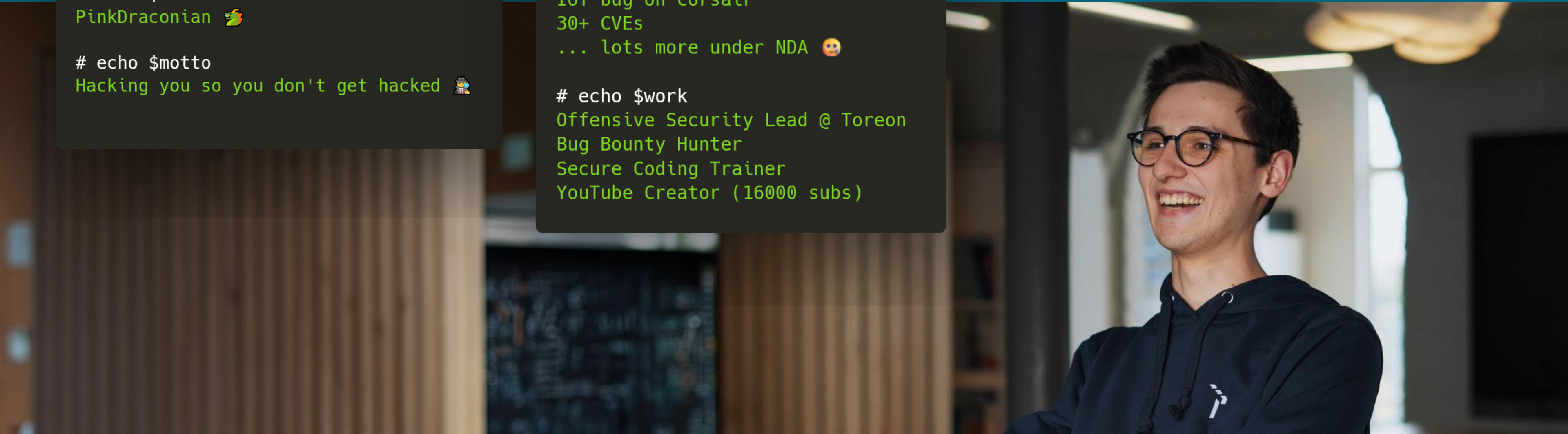
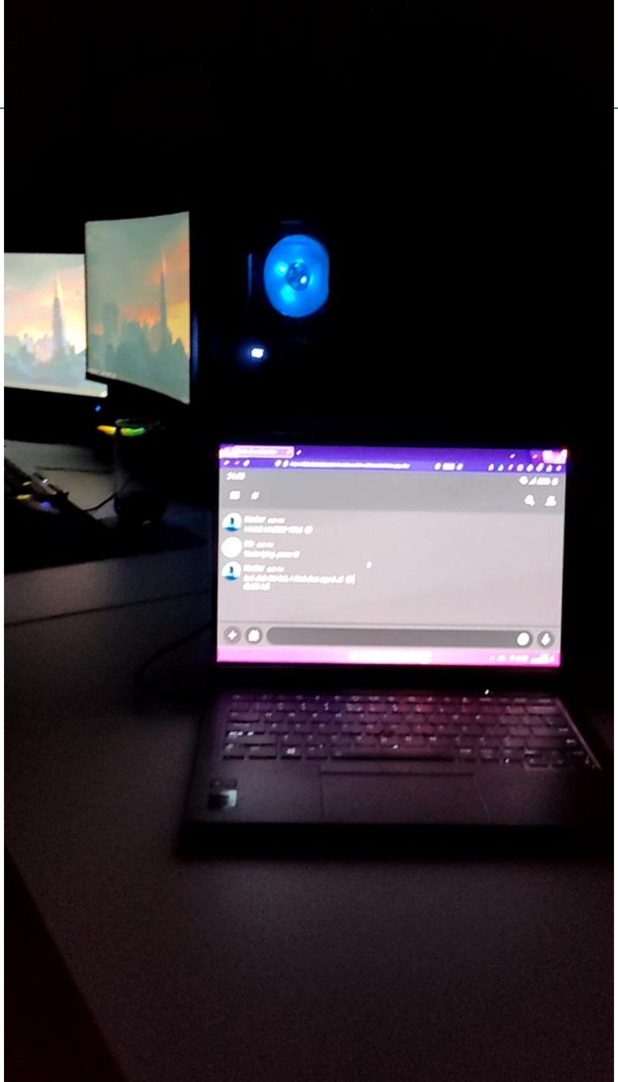
TOREON

The hacker mindset

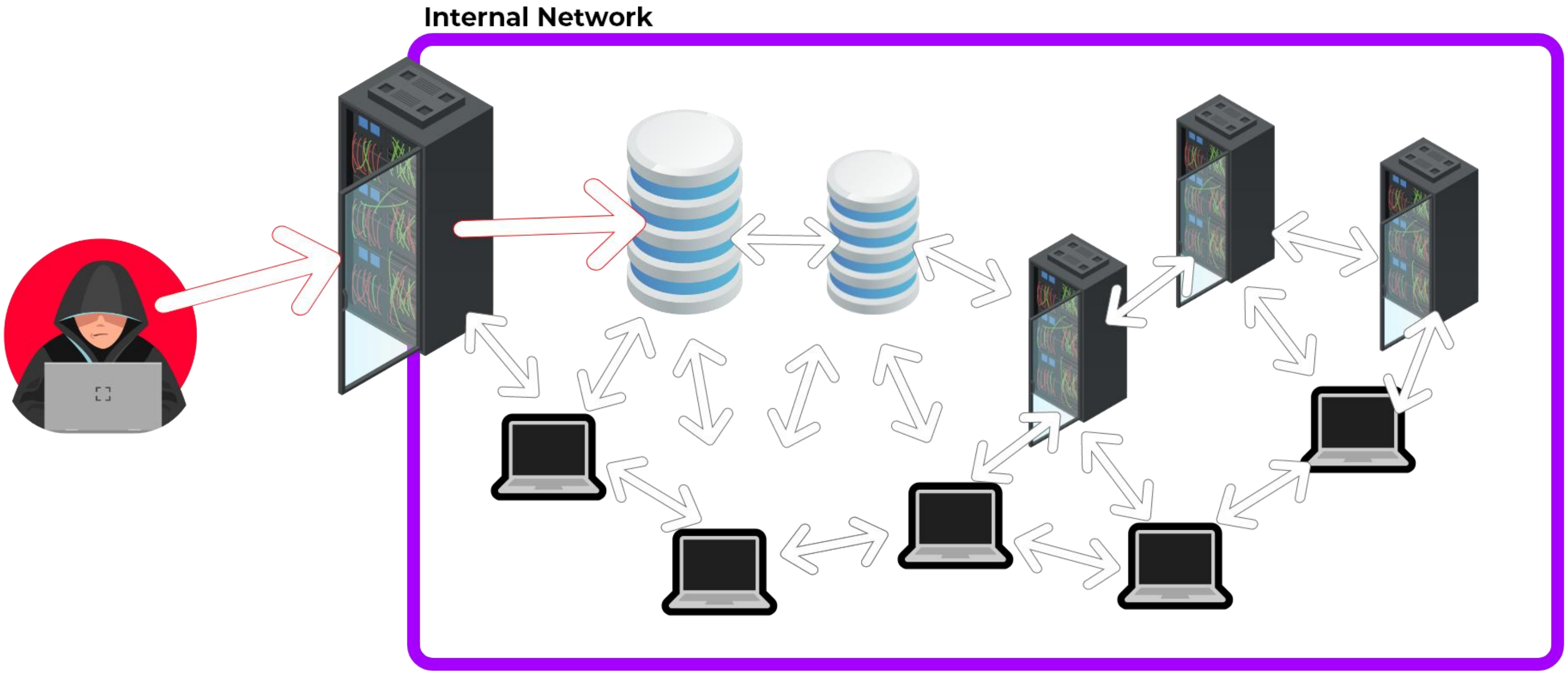
```
# whoami
Robbe Van Roey 🧑‍💻

# echo $nick
PinkDraconian 🐉

# echo $motto
Hacking you so you don't get hacked 🕵️
```

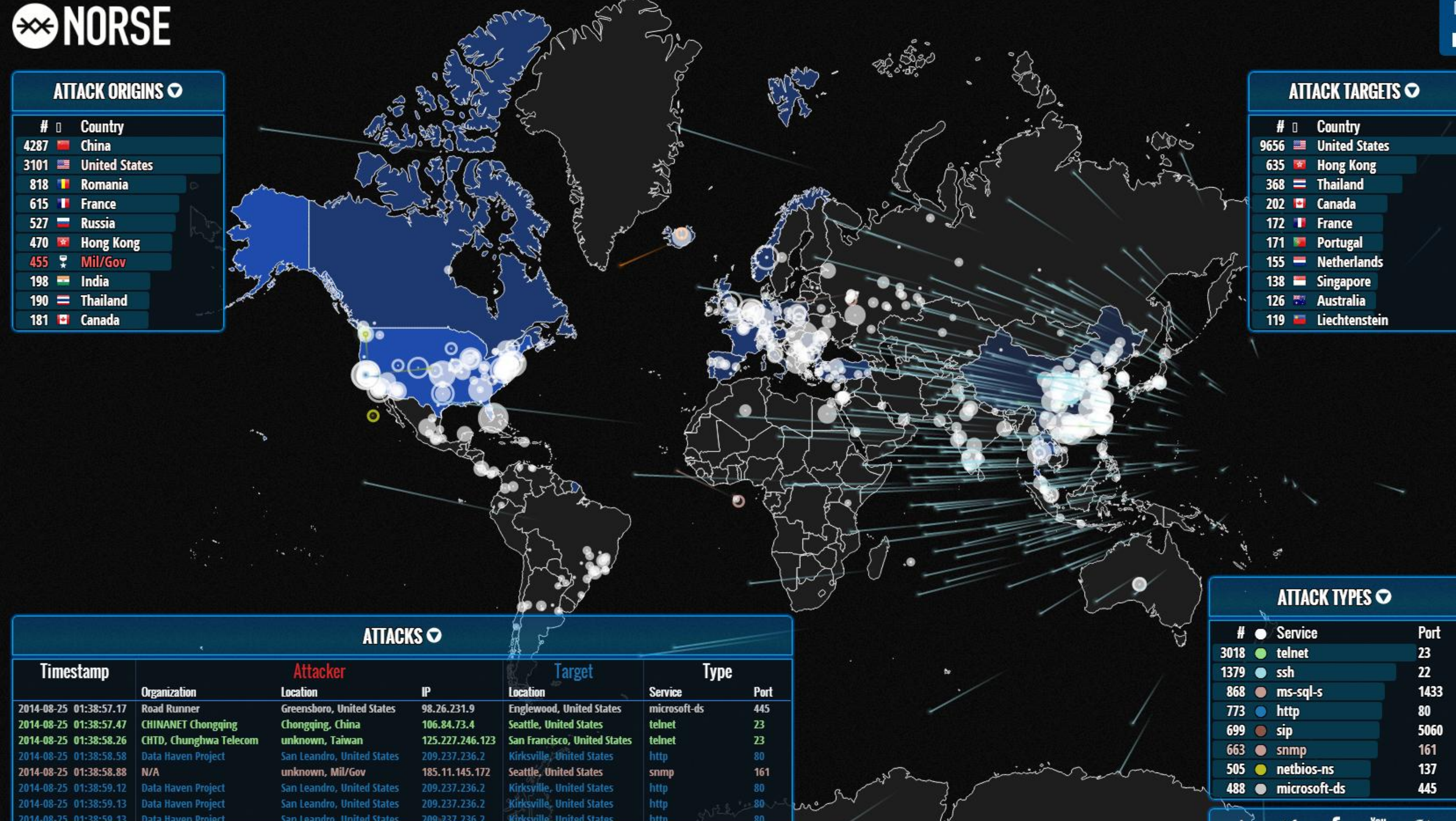
```
# echo $hacks
Critical vulnerability on NVIDIA
High-severity bug on AWS (Amazon)
IoT bug on Corsair
30+ CVEs
... lots more under NDA 🥹

# echo $work
Offensive Security Lead @ Toreon
Bug Bounty Hunter
Secure Coding Trainer
YouTube Creator (16000 subs)
```





Acme Corp





NORSE

ATTACK ORIGINS

#		Country
4287	🇨🇳	China
3101	🇺🇸	United States
818	🇷🇴	Romania
615	🇫🇷	France
527	🇷🇺	Russia
470	🇭🇰	Hong Kong
455		Mil/Gov
198	🇮🇳	India
190	🇹🇭	Thailand
181	🇨🇦	Canada

ATTACK TARGETS

#		Country
9656	🇺🇸	United States
635	🇭🇰	Hong Kong
368	🇹🇭	Thailand
202	🇨🇦	Canada
172	🇫🇷	France
171	🇵🇹	Portugal
155	🇳🇱	Netherlands
138	🇸🇬	Singapore
126	🇦🇺	Australia
119	🇱🇮	Liechtenstein

ATTACK TYPES

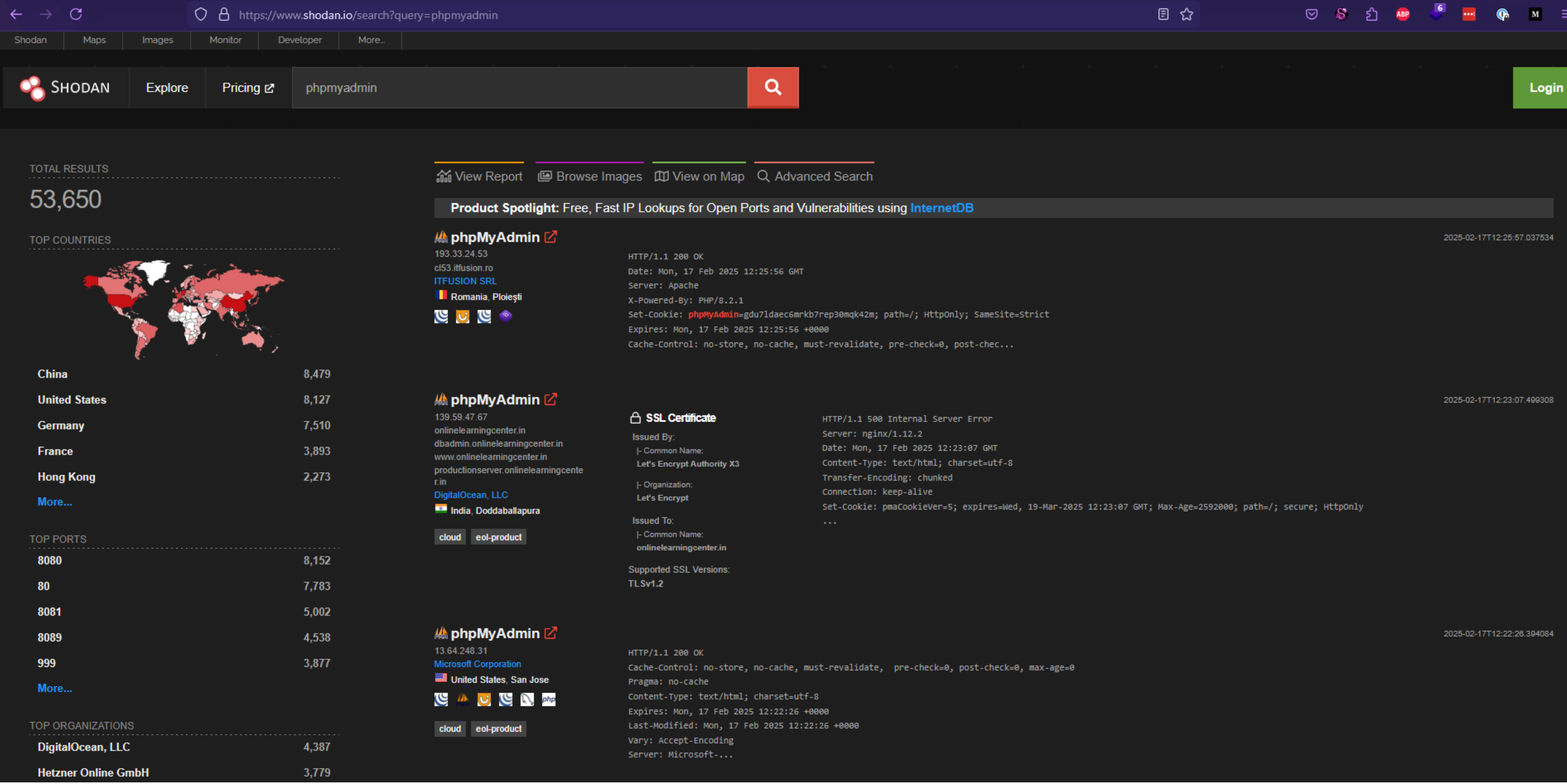
#	●	Service	Port
3018	●	telnet	23
1379	●	ssh	22
868	●	ms-sql-s	1433
773	●	http	80
699	●	sip	5060
663	●	snmp	161
505	●	netbios-ns	137
488	●	microsoft-ds	445

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-08-25 01:38:57.17	Road Runner	Greensboro, United States	98.26.231.9	Englewood, United States	microsoft-ds	445
2014-08-25 01:38:57.47	CHINANET Chongqing	Chongqing, China	106.84.73.4	Seattle, United States	telnet	23
2014-08-25 01:38:58.26	CHTD, Chunghwa Telecom	unknown, Taiwan	125.227.246.123	San Francisco, United States	telnet	23
2014-08-25 01:38:58.58	Data Haven Project	San Leandro, United States	209.237.236.2	Kirksville, United States	http	80
2014-08-25 01:38:58.88	N/A	unknown, Mil/Gov	185.11.145.172	Seattle, United States	snmp	161
2014-08-25 01:38:59.12	Data Haven Project	San Leandro, United States	209.237.236.2	Kirksville, United States	http	80
2014-08-25 01:38:59.13	Data Haven Project	San Leandro, United States	209.237.236.2	Kirksville, United States	http	80
2014-08-25 01:38:59.13	Data Haven Project	San Leandro, United States	209.237.236.2	Kirksville, United States	http	80

🧑‍💻 Demo

NMAP



TOTAL RESULTS

53,650

TOP COUNTRIES

China	8,479
United States	8,127
Germany	7,510
France	3,893
Hong Kong	2,273
More...	

TOP PORTS

8080	8,152
80	7,783
8081	5,002
8089	4,538
999	3,877
More...	

TOP ORGANIZATIONS

DigitalOcean, LLC	4,387
Hetzner Online GmbH	3,779

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

phpMyAdmin

2025-02-17T12:25:57.037534

193.33.24.53
cl53.itfusion.ro
ITFUSION SRL
Romania, Ploiești

```
HTTP/1.1 200 OK
Date: Mon, 17 Feb 2025 12:25:56 GMT
Server: Apache
X-Powered-By: PHP/8.2.1
Set-Cookie: phpMyAdmin=gdu7ldaec6mrkb7rep30mqk42m; path=/; HttpOnly; SameSite=Strict
Expires: Mon, 17 Feb 2025 12:25:56 +0000
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-chec...
```

phpMyAdmin

2025-02-17T12:23:07.499308

139.59.47.67
onlinelearningcenter.in
dbadmin.onlinelearningcenter.in
www.onlinelearningcenter.in
productionserver.onlinelearningcenter.in
DigitalOcean, LLC
India, Doddaballapura

cloud eol-product

SSL Certificate

Issued By:
|- Common Name:
Let's Encrypt Authority X3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
onlinelearningcenter.in

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.12.2
Date: Mon, 17 Feb 2025 12:23:07 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: pmaCookieVer=5; expires=Wed, 19-Mar-2025 12:23:07 GMT; Max-Age=2592000; path=/; secure; HttpOnly
...
```

phpMyAdmin

2025-02-17T12:22:26.394084

13.64.248.31
Microsoft Corporation
United States, San Jose

cloud eol-product

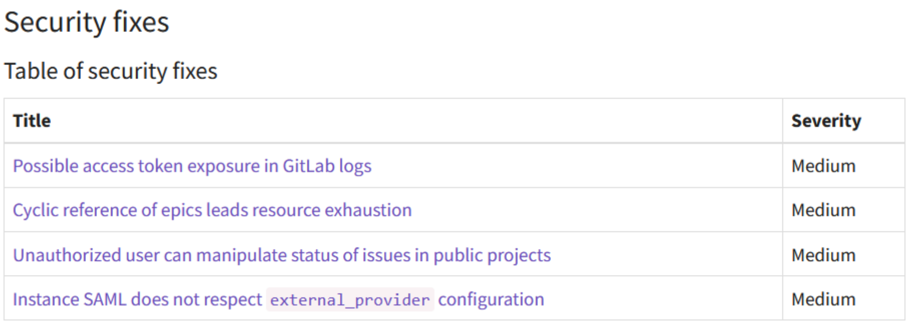
```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate,  pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: Mon, 17 Feb 2025 12:22:26 +0000
Last-Modified: Mon, 17 Feb 2025 12:22:26 +0000
Vary: Accept-Encoding
Server: Microsoft-...
```

🧑‍💻 Demo

Searchsploit

Why are these exploits public?

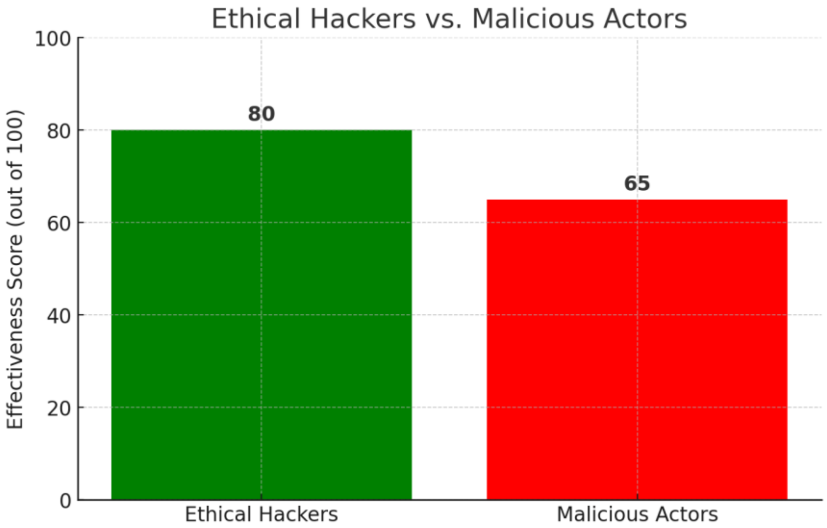
- Public disclosure pressures vendors to create patches
- Attackers already exploit vulnerabilities
  - Hiding them only benefits attackers
- Fuels innovation



Security fixes

Table of security fixes

Title	Severity
Possible access token exposure in GitLab logs	Medium
Cyclic reference of epics leads resource exhaustion	Medium
Unauthorized user can manipulate status of issues in public projects	Medium
Instance SAML does not respect `external_provider` configuration	Medium

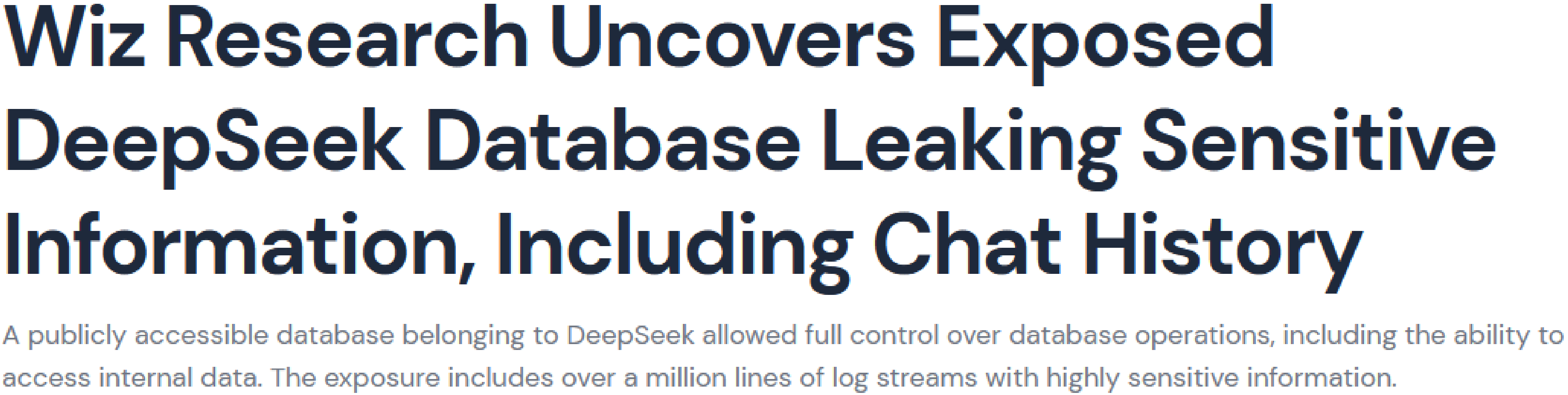


Tips & Tricks

- Make sure you know exactly what you expose to the internet
- Keep this all up to date
- => This seems easy, right?

Tips & Tricks

- Make sure you know exactly what you expose to the internet
- Keep this all up to date
- => This seems easy, right?



Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History

A publicly accessible database belonging to DeepSeek allowed full control over database operations, including the ability to access internal data. The exposure includes over a million lines of log streams with highly sensitive information.

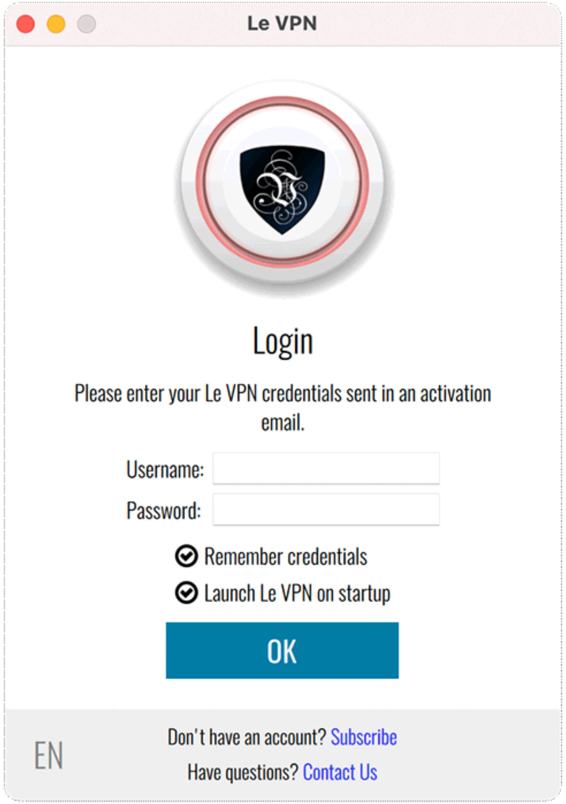
🧑‍💻 Demo

Leaked Credentials

Tips & Tricks

- Humans will use unsafe passwords
  - No matter how much you tell them not to
- Humans will keep on clicking on links
  - No matter how much you tell them not to
- => We need to assume a colleague is going to get hacked

The Uber hack



Le VPN

Login

Please enter your Le VPN credentials sent in an activation email.

Username:

Password:

✓ Remember credentials

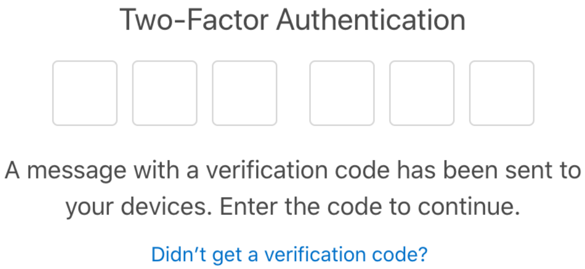
✓ Launch Le VPN on startup

OK

EN

Don't have an account? Subscribe

Have questions? Contact Us

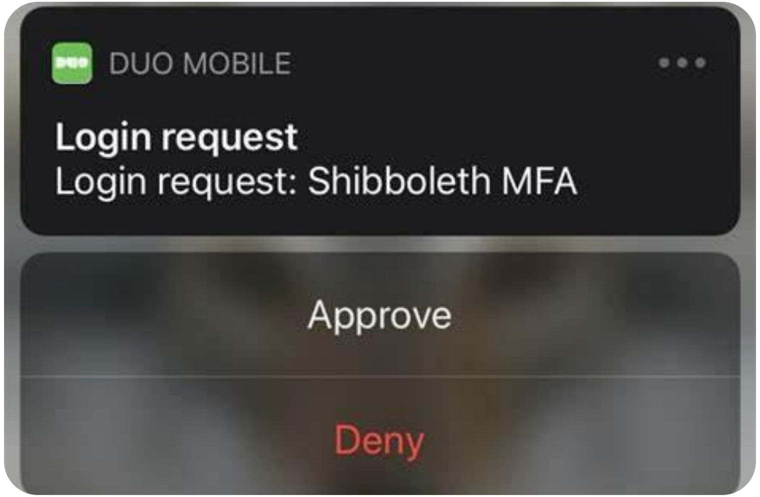


Two-Factor Authentication

□ □ □ □ □ □

A message with a verification code has been sent to your devices. Enter the code to continue.

Didn’t get a verification code?



DUO MOBILE

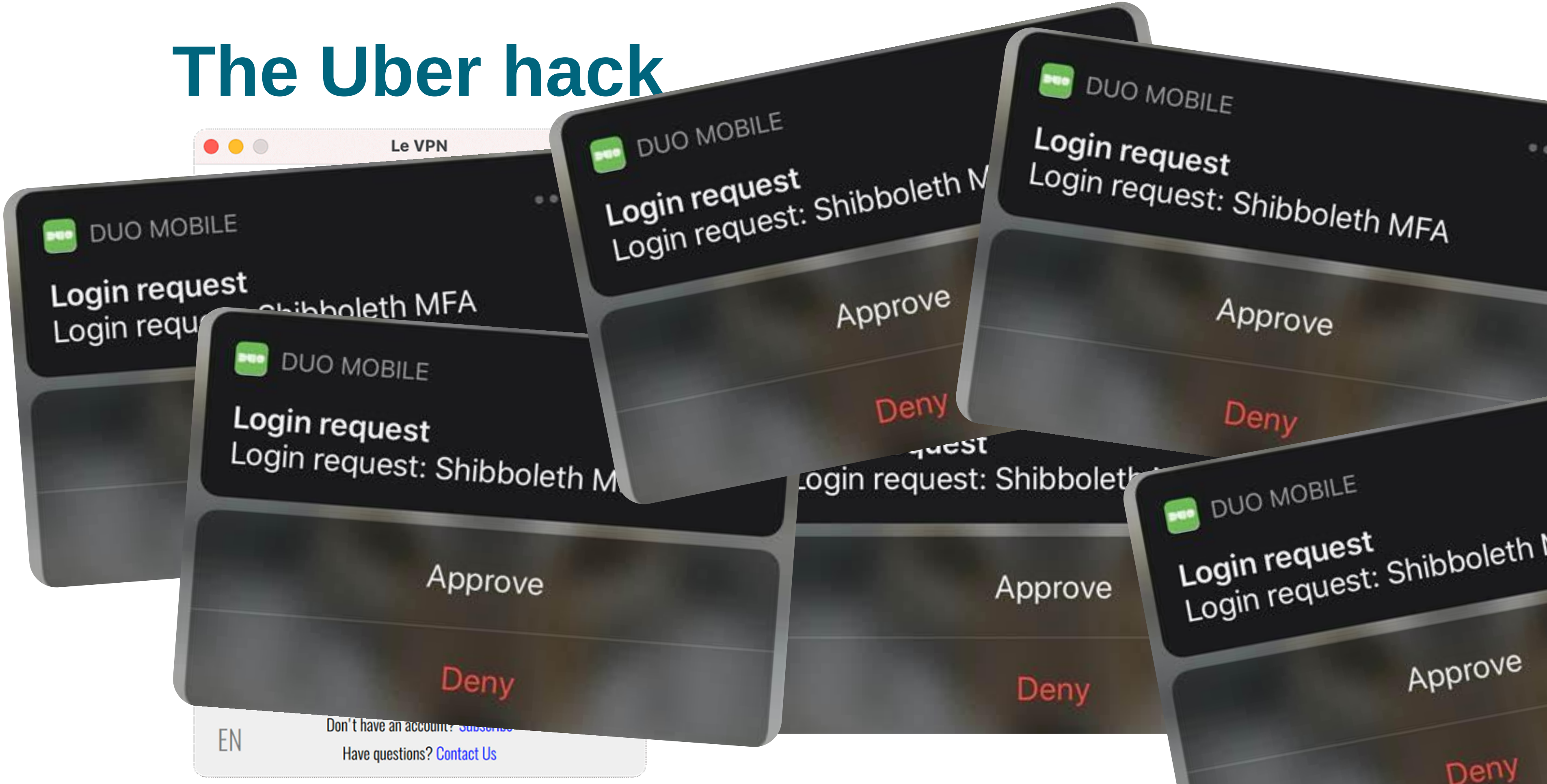
Login request

Login request: Shibboleth MFA

Approve

Deny

The Uber hack



DUO MOBILE

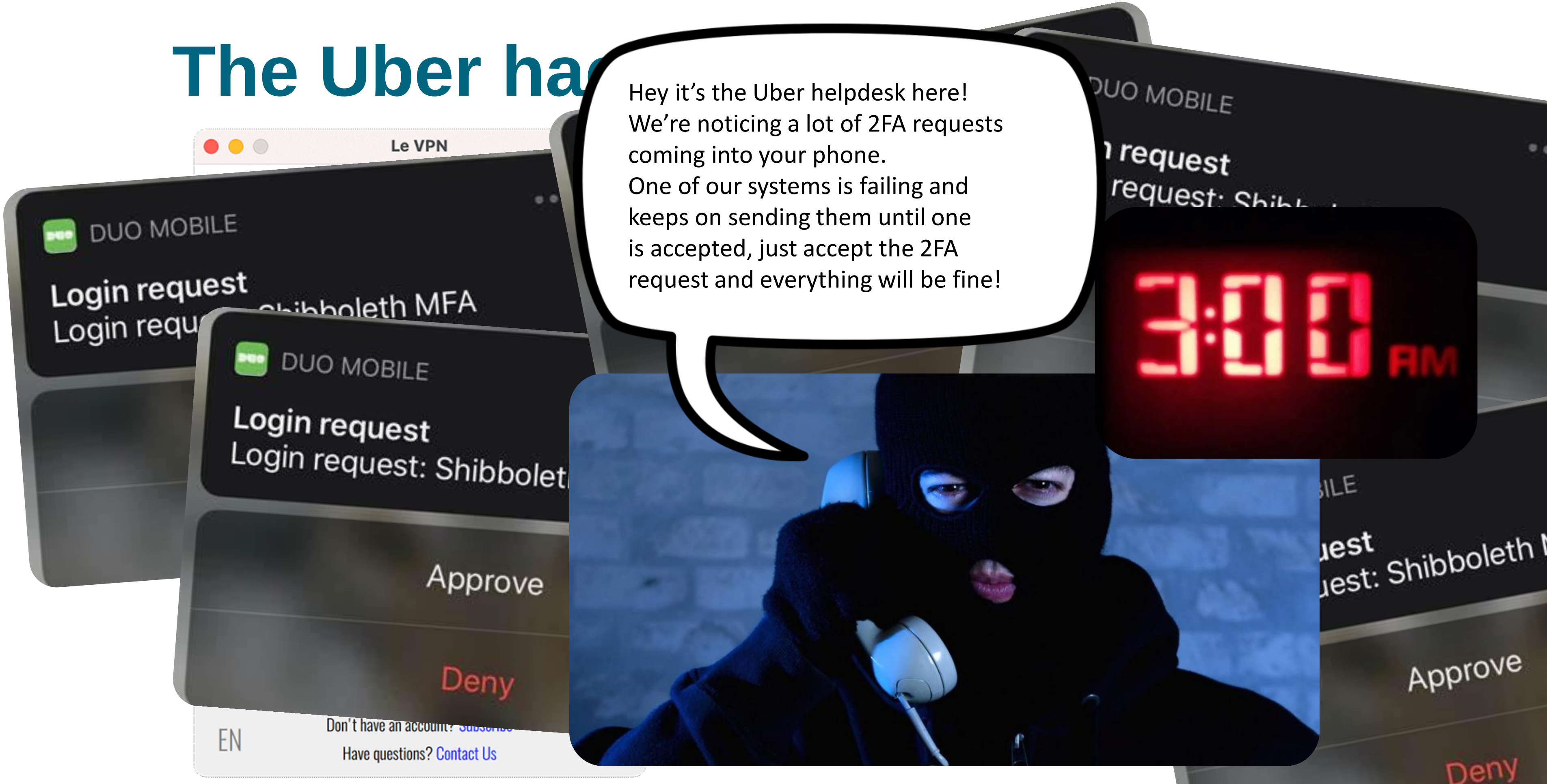
Login request

Login request: Shibboleth MFA

Don't have an account? Subscribe

Have questions? Contact Us

The Uber ha



Hey it’s the Uber helpdesk here!
We’re noticing a lot of 2FA requests coming into your phone.
One of our systems is failing and keeps on sending them until one is accepted, just accept the 2FA request and everything will be fine!

🧑‍💻 Demo

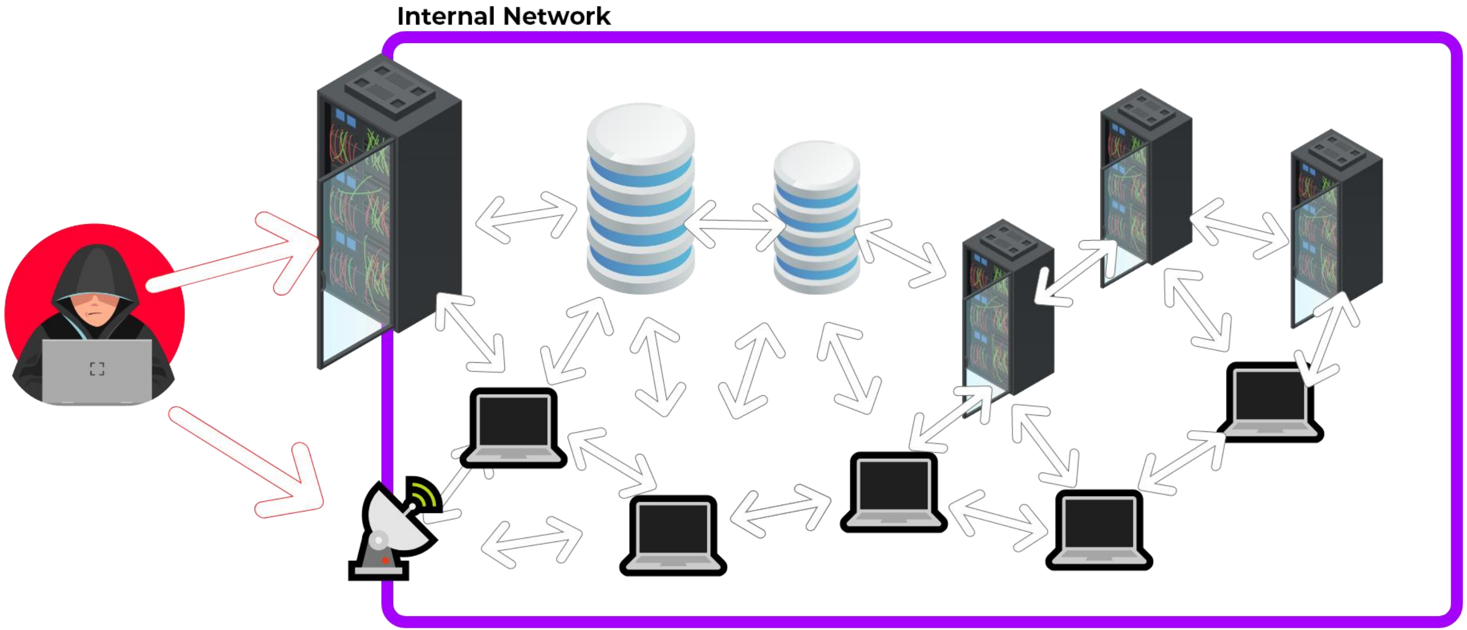
Vulnerability scanning
Vs
Pentesting

Not only external threats

- Application
  - For organizations developing software
  - Contains
    - Web applications
    - Mobile applications
    - Thick-clients
    - AI-systems
    - IoT device
    - Cloud systems
    - APIs
    - Blockchain
    - SCADA/ICS
    - Hardware hacking
    - …

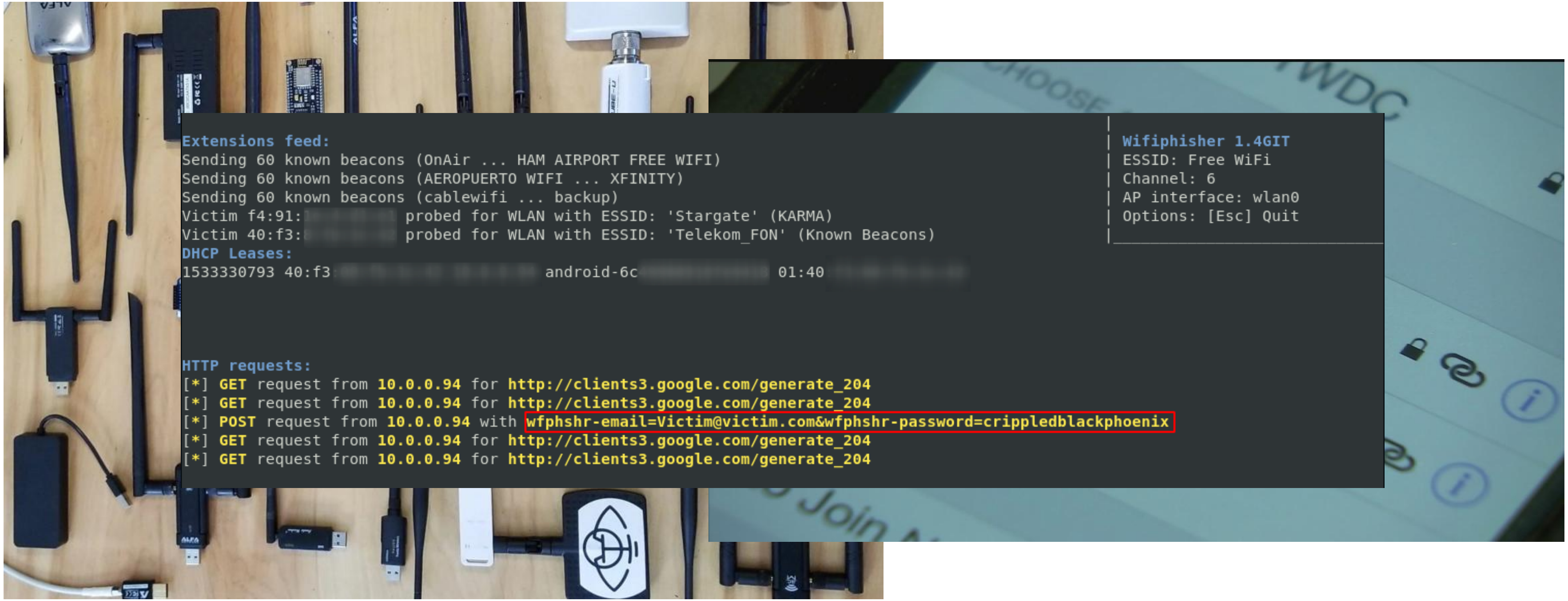
- Organization
  - For any organization
  - Contains
    - Internal Network
    - External Network
    - OSINT
    - Physical
    - WiFi
    - Active Directory
    - Social Engineering
    - Phishing
    - Badge hacking
    - …

Not only external threats



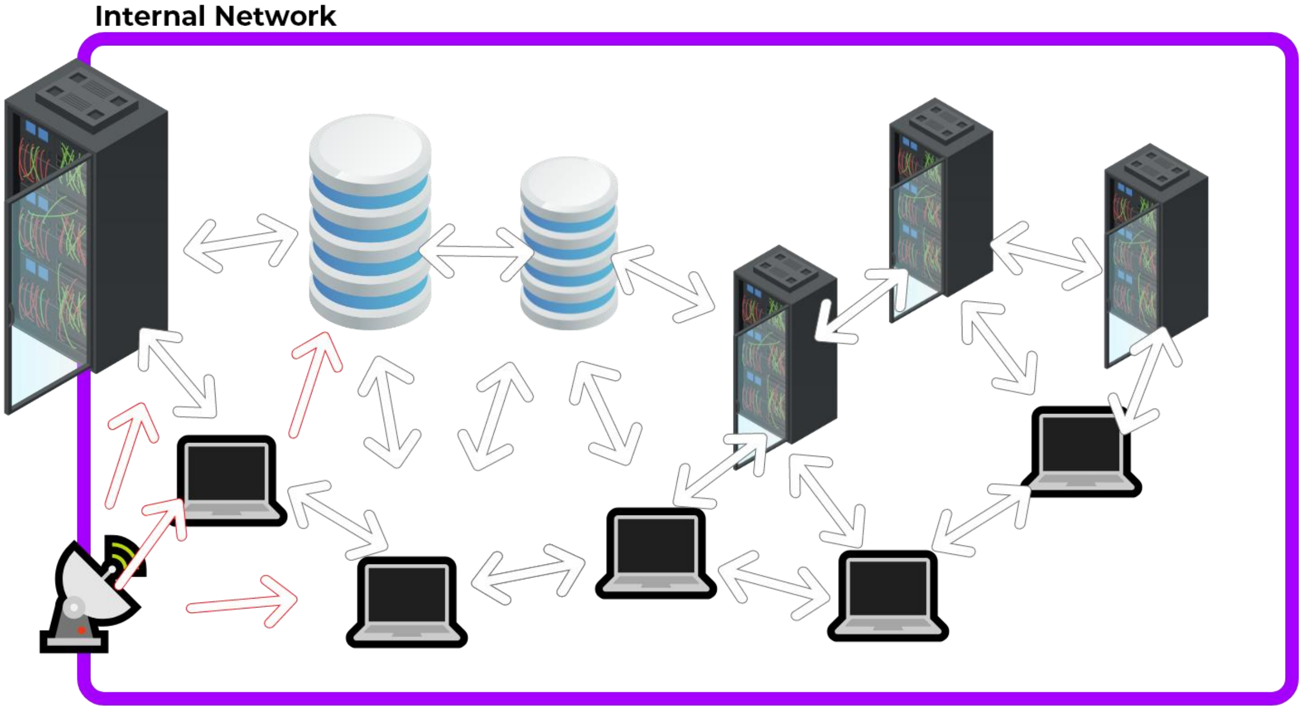
Not only external threats

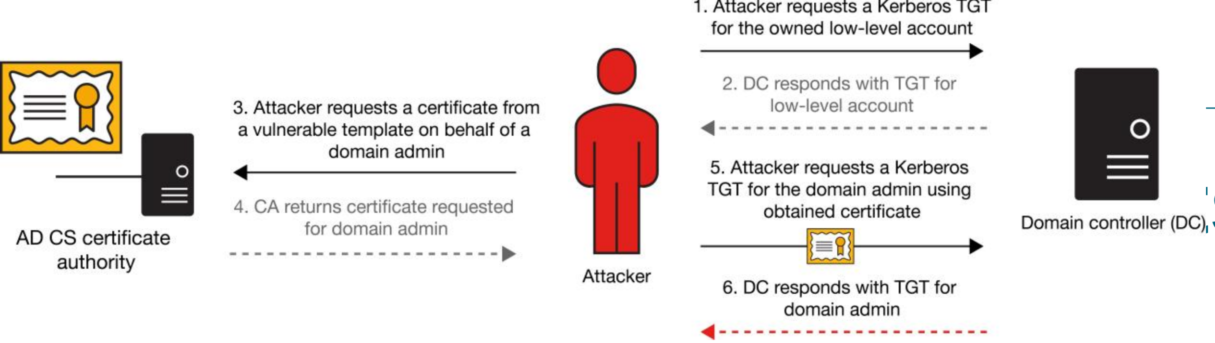
Not only external threats



```
Extensions feed:                                                                   | Wifiphisher 1.4GIT
Sending 60 known beacons (OnAir ... HAM AIRPORT FREE WIFI)                         | ESSID: Free WiFi
Sending 60 known beacons (AEROPUERTO WIFI ... XFINITY)                             | Channel: 6
Sending 60 known beacons (cablewifi ... backup)                                    | AP interface: wlan0
Victim f4:91:[redacted] probed for WLAN with ESSID: 'Stargate' (KARMA)             | Options: [Esc] Quit
Victim 40:f3:[redacted] probed for WLAN with ESSID: 'Telekom_FON' (Known Beacons)  |___________________
DHCP Leases:
1533330793 40:f3[redacted] android-6c[redacted] 01:40[redacted]



HTTP requests:
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] POST request from 10.0.0.94 with wfphshr-email=Victim@victim.com&wfphshr-password=crippledblackphoenix
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
[*] GET request from 10.0.0.94 for http://clients3.google.com/generate_204
```

Not only external threats





1. Attacker requests a Kerberos TGT for the owned low-level account

2. DC responds with TGT for low-level account

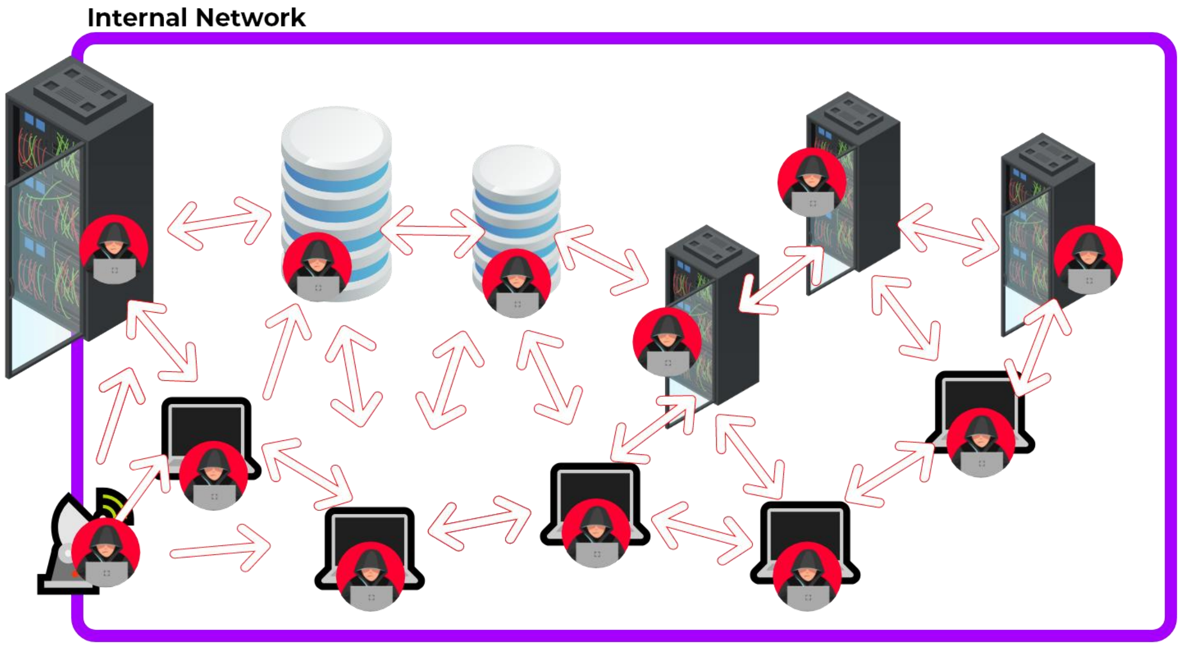
3. Attacker requests a certificate from a vulnerable template on behalf of a domain admin

4. CA returns certificate requested for domain admin

5. Attacker requests a Kerberos TGT for the domain admin using obtained certificate

6. DC responds with TGT for domain admin

S



TOREON

The hacker mindset

```
# whoami
Robbe Van Roey 🧑‍💻

# echo $nick
PinkDraconian 🐲

# echo $motto
Hacking you so you don't get hacked 🕵️
```

```
# echo $hacks
Critical vulnerability on NVIDIA
High-severity bug on AWS (Amazon)
IoT bug on Corsair
30+ CVEs
... lots more under NDA 🥹

# echo $work
Offensive Security Lead @ Toreon
Bug Bounty Hunter
Secure Coding Trainer
YouTube Creator (16000 subs)
```