Aprendendo Pentest sem dinheiro!

@an4kein

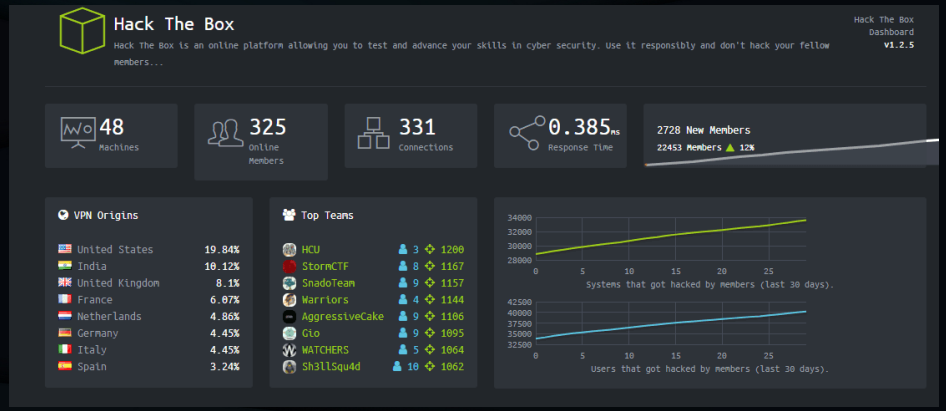
- LinkedIn (https://www.linkedin.com/in/an4kein/)
- GitHub (https://github.com/an4kein)
- Youtube (https://www.youtube.com/c/an4kein)
- Twitter @an4kein

Overview/Penetration Testing Labs

- Hack The Box
- VulnHub
- Pentestit
- Hack With GitHub

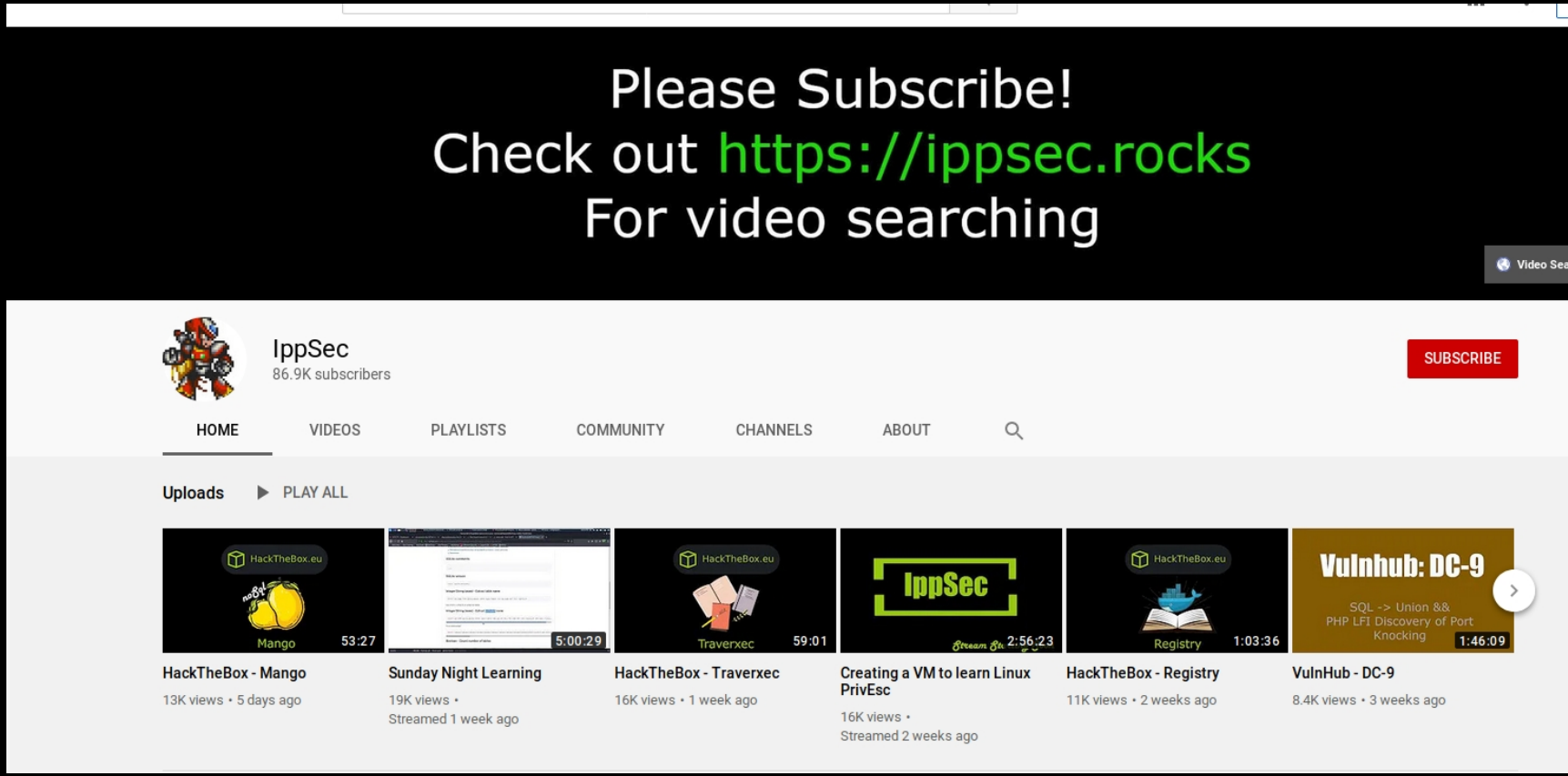
Hack The Box


Hack The Box
PEN-TESTING LABS
start@hacking:~#
INDIVIDUALS
COMPANIES & UNIVERSITIES

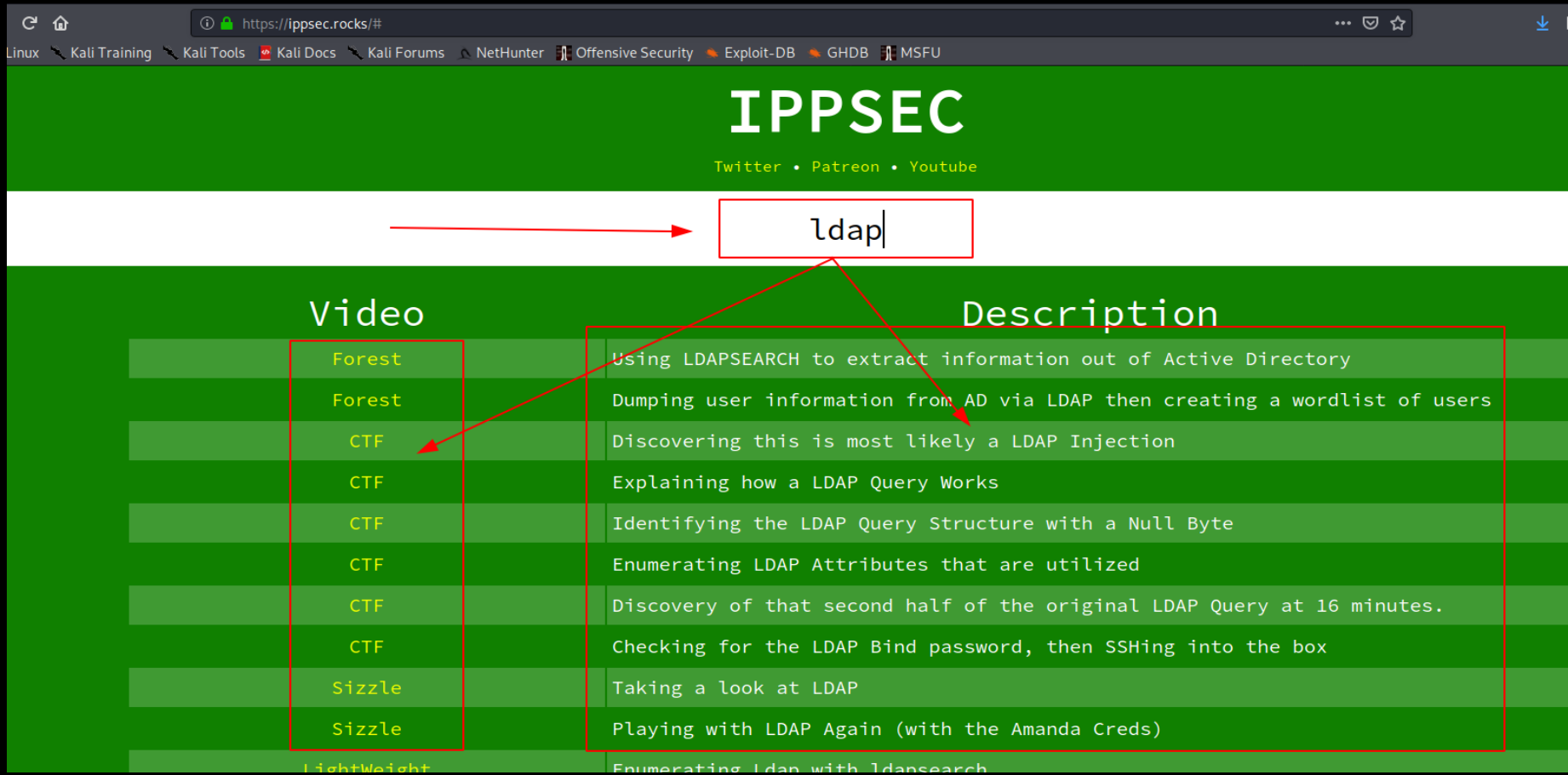

Hack The Box
Hack The Box is an online platform allowing you to test and advance your skills in cyber security. Use it responsibly and don't hack your fellow members...
Hack The Box Dashboard
v1.2.5
48
Machines
325
Online Members
331
Connections
0.385ms
Response Time
2728 New Members
22453 Members ▲ 12%
VPN Origins
United States 19.84%
India 10.12%
United Kingdom 8.1%
France 6.07%
Netherlands 4.86%
Germany 4.45%
Italy 4.45%
Spain 3.24%
Top Teams
HCU 3 1200
StormCTF 8 1167
SnadoTeam 9 1157
Warriors 4 1144
AggressiveCake 9 1106
Gio 9 1095
WATCHERS 5 1064
Sh3llSqu4d 10 1062
Systems that got hacked by members (last 30 days).
Users that got hacked by members (last 30 days).

Hack The Box

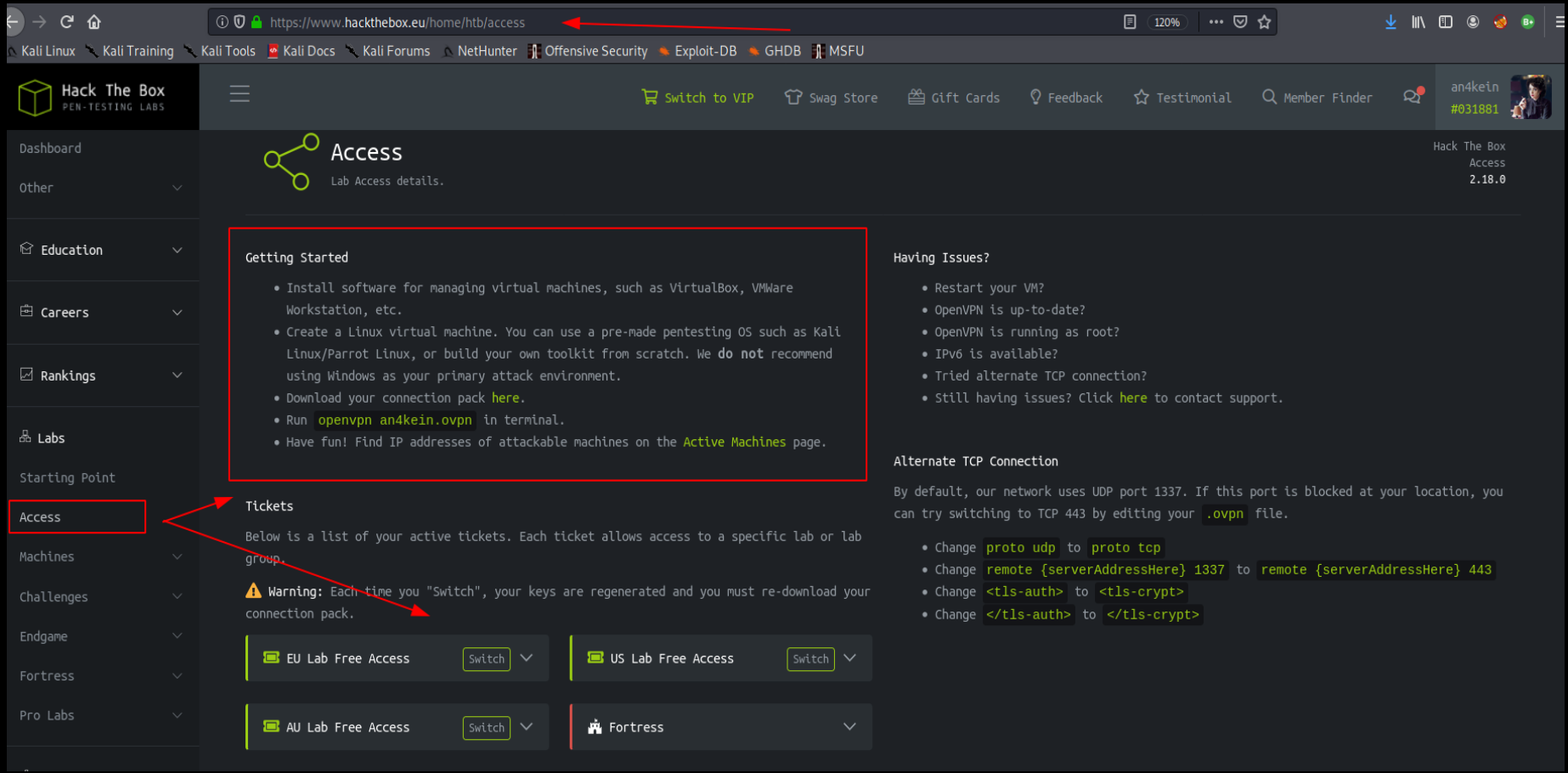
Please Subscribe!
Check out https://ippsec.rocks
For video searching



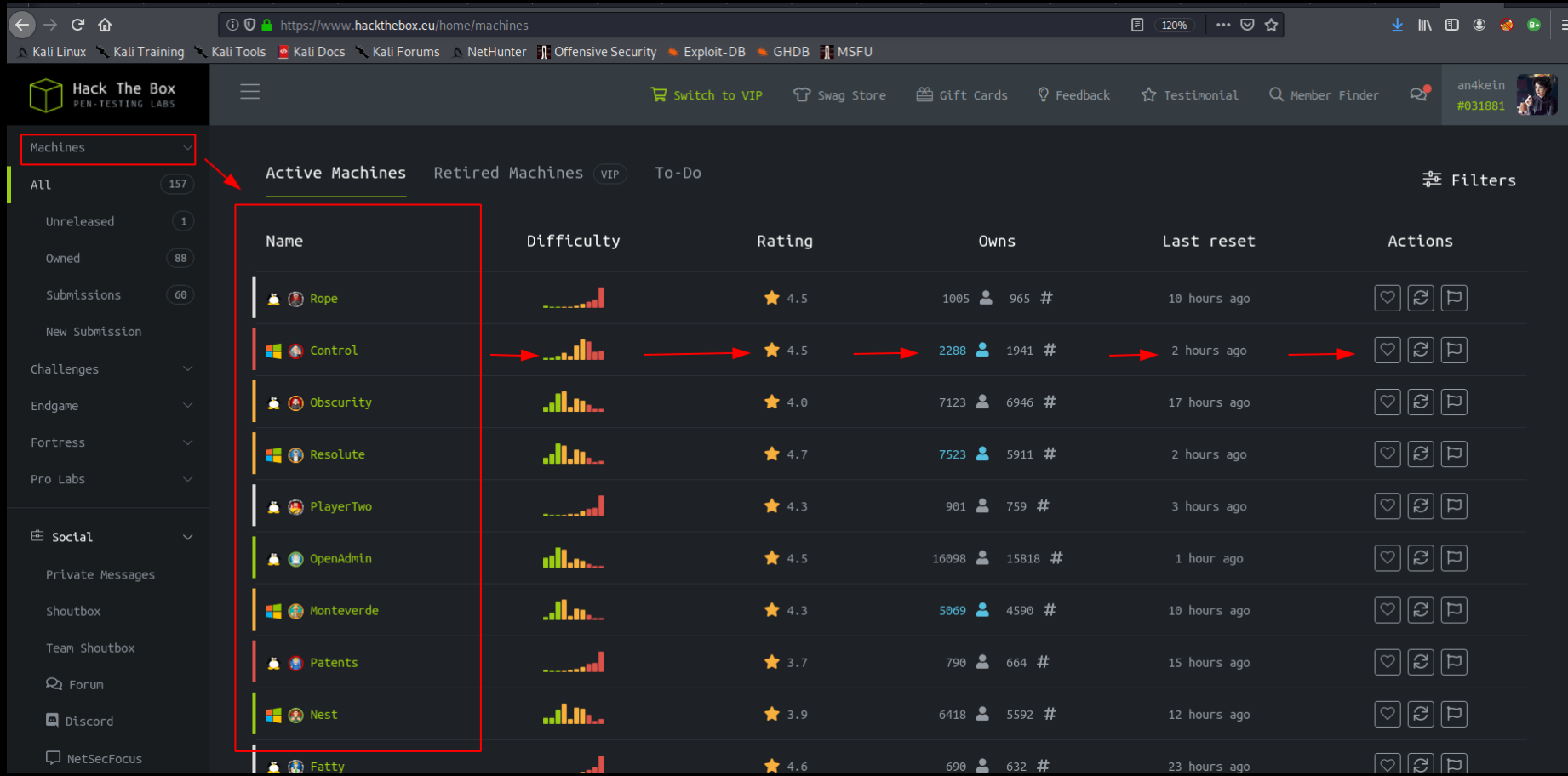
Hack The Box


https://ippsec.rocks/#
Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
IPPSEC
Twitter • Patreon • Youtube
ldap
Video
Description
Forest
Using LDAPSEARCH to extract information out of Active Directory
Forest
Dumping user information from AD via LDAP then creating a wordlist of users
CTF
Discovering this is most likely a LDAP Injection
CTF
Explaining how a LDAP Query Works
CTF
Identifying the LDAP Query Structure with a Null Byte
CTF
Enumerating LDAP Attributes that are utilized
CTF
Discovery of that second half of the original LDAP Query at 16 minutes.
CTF
Checking for the LDAP Bind password, then SSHing into the box
Sizzle
Taking a look at LDAP
Sizzle
Playing with LDAP Again (with the Amanda Creds)

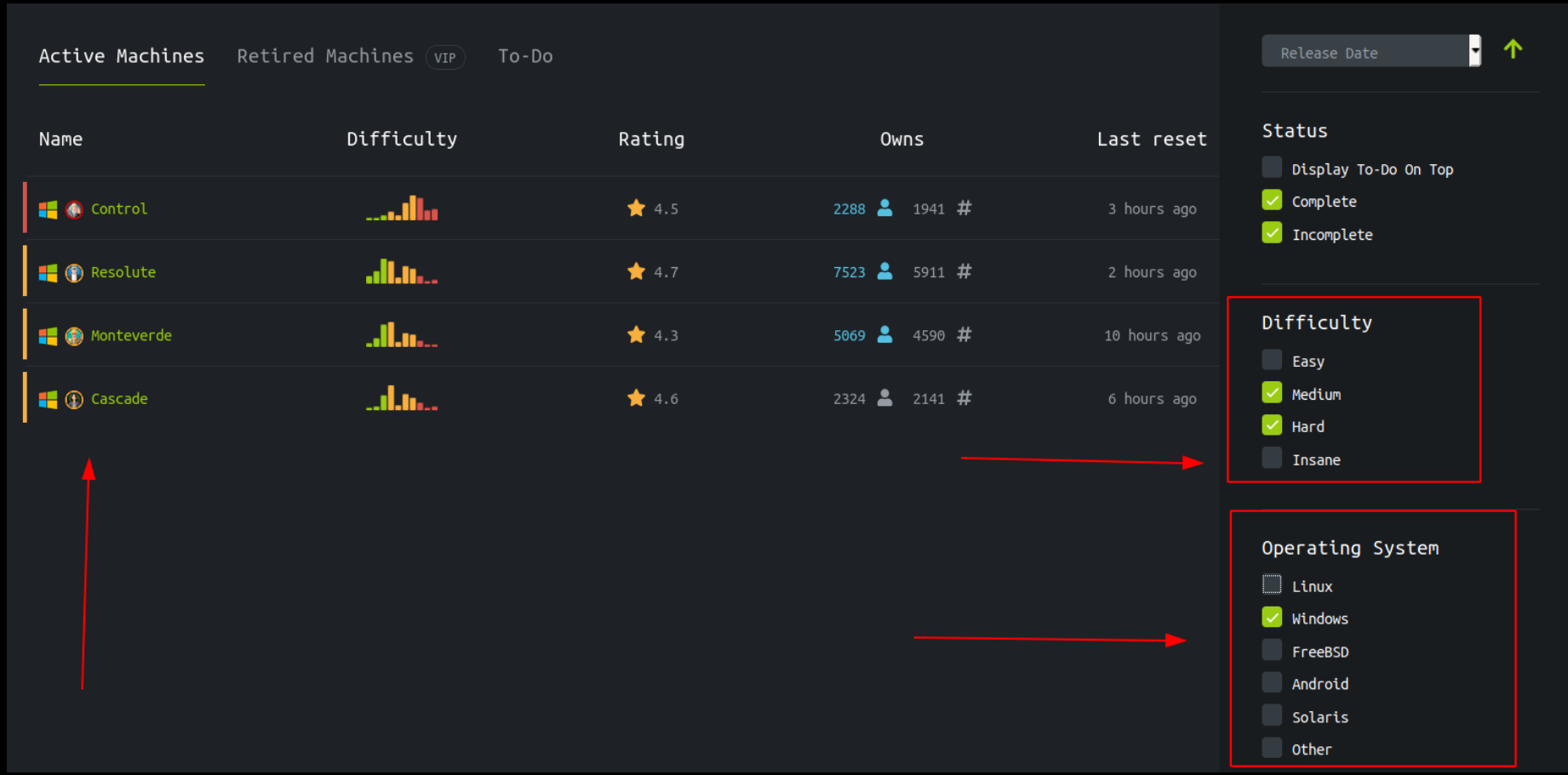
Hack The Box


https://www.hackthebox.eu/home/htb/access
120%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Hack The Box
PEN-TESTING LABS
Switch to VIP
Swag Store
Gift Cards
Feedback
Testimonial
Member Finder
an4kein
#031881
Dashboard
Other
Education
Careers
Rankings
Labs
Starting Point
Access
Machines
Challenges
Endgame
Fortress
Pro Labs
Access
Lab Access details.
Hack The Box
Access
2.18.0
Getting Started
Install software for managing virtual machines, such as VirtualBox, VMWare Workstation, etc.
Create a Linux virtual machine. You can use a pre-made pentesting OS such as Kali Linux/Parrot Linux, or build your own toolkit from scratch. We do not recommend using Windows as your primary attack environment.
Download your connection pack here.
Run openvpn an4kein.ovpn in terminal.
Have fun! Find IP addresses of attackable machines on the Active Machines page.
Having Issues?
Restart your VM?
OpenVPN is up-to-date?
OpenVPN is running as root?
IPv6 is available?
Tried alternate TCP connection?
Still having issues? Click here to contact support.
Tickets
Below is a list of your active tickets. Each ticket allows access to a specific lab or lab group.
Warning: Each time you "Switch", your keys are regenerated and you must re-download your connection pack.
EU Lab Free Access
Switch
US Lab Free Access
Switch
AU Lab Free Access
Switch
Fortress
Alternate TCP Connection
By default, our network uses UDP port 1337. If this port is blocked at your location, you can try switching to TCP 443 by editing your .ovpn file.
Change proto udp to proto tcp
Change remote {serverAddressHere} 1337 to remote {serverAddressHere} 443
Change <tls-auth> to <tls-crypt>
Change </tls-auth> to </tls-crypt>

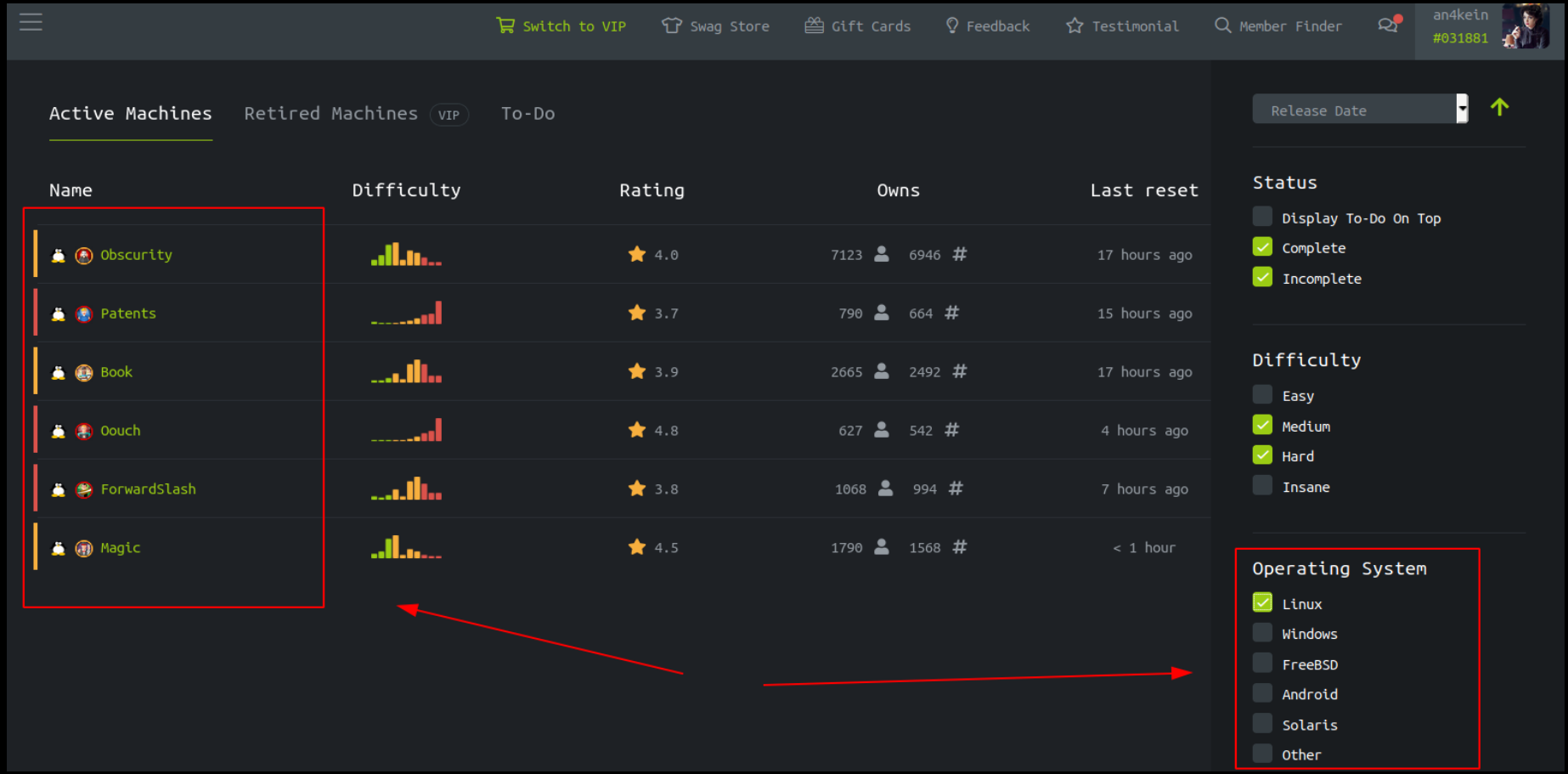
Hack The Box


https://www.hackthebox.eu/home/machines
120%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Hack The Box
PEN-TESTING LABS
Switch to VIP
Swag Store
Gift Cards
Feedback
Testimonial
Member Finder
an4kein
#031881
Machines
All 157
Unreleased 1
Owned 88
Submissions 60
New Submission
Challenges
Endgame
Fortress
Pro Labs
Social
Private Messages
Shoutbox
Team Shoutbox
Forum
Discord
NetSecFocus
Active Machines
Retired Machines VIP
To-Do
Filters
Name
Difficulty
Rating
Owns
Last reset
Actions
Rope 4.5 1005 965 # 10 hours ago
Control 4.5 2288 1941 # 2 hours ago
Obscurity 4.0 7123 6946 # 17 hours ago
Resolute 4.7 7523 5911 # 2 hours ago
PlayerTwo 4.3 901 759 # 3 hours ago
OpenAdmin 4.5 16098 15818 # 1 hour ago
Monteverde 4.3 5069 4590 # 10 hours ago
Patents 3.7 790 664 # 15 hours ago
Nest 3.9 6418 5592 # 12 hours ago
Fatty 4.6 690 632 # 23 hours ago

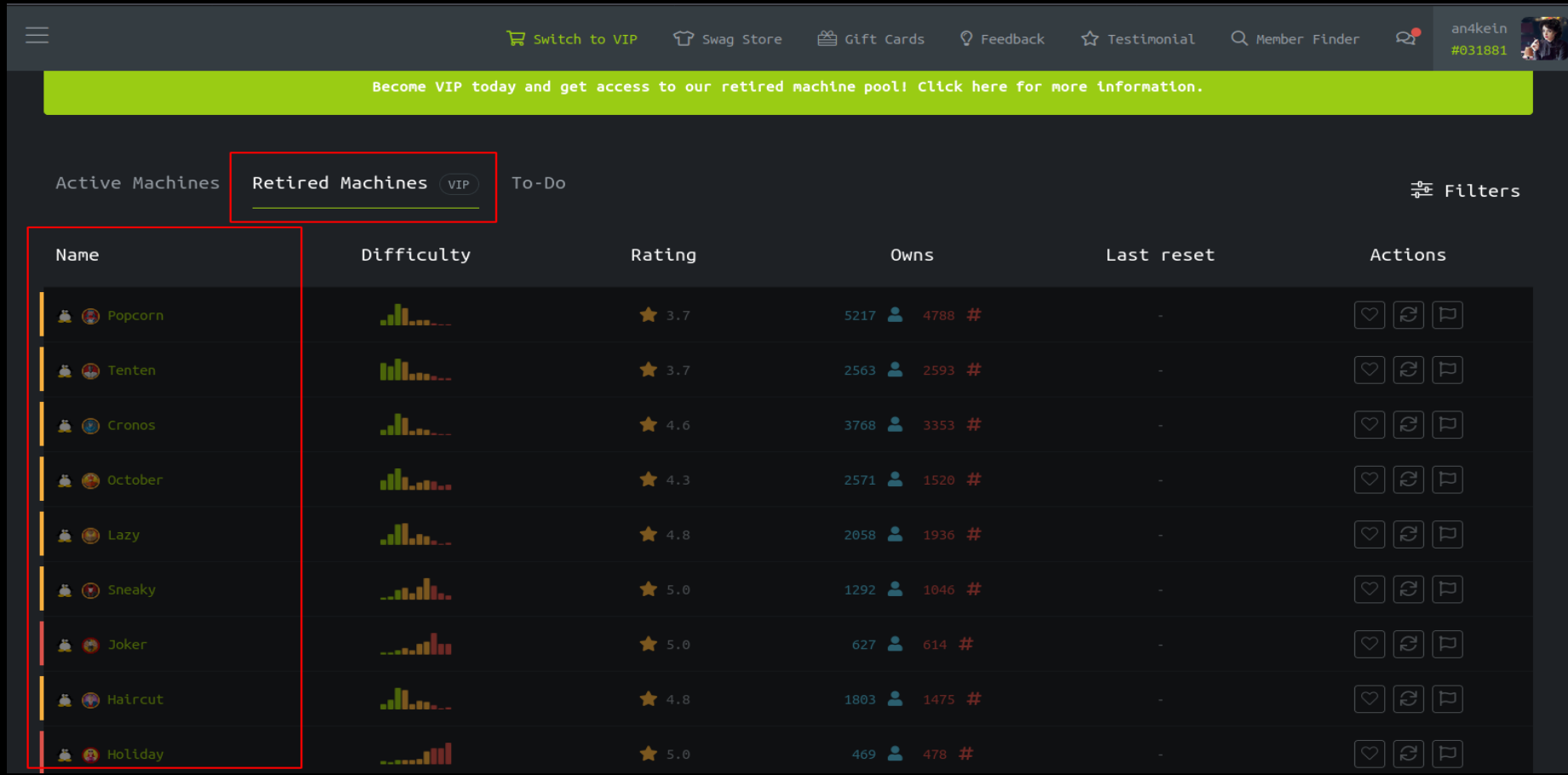
Hack The Box


Active Machines
Retired Machines
VIP
To-Do
Release Date
Name
Difficulty
Rating
Owns
Last reset
Control
4.5
2288
1941
3 hours ago
Resolute
4.7
7523
5911
2 hours ago
Monteverde
4.3
5069
4590
10 hours ago
Cascade
4.6
2324
2141
6 hours ago
Status
Display To-Do On Top
Complete
Incomplete
Difficulty
Easy
Medium
Hard
Insane
Operating System
Linux
Windows
FreeBSD
Android
Solaris
Other

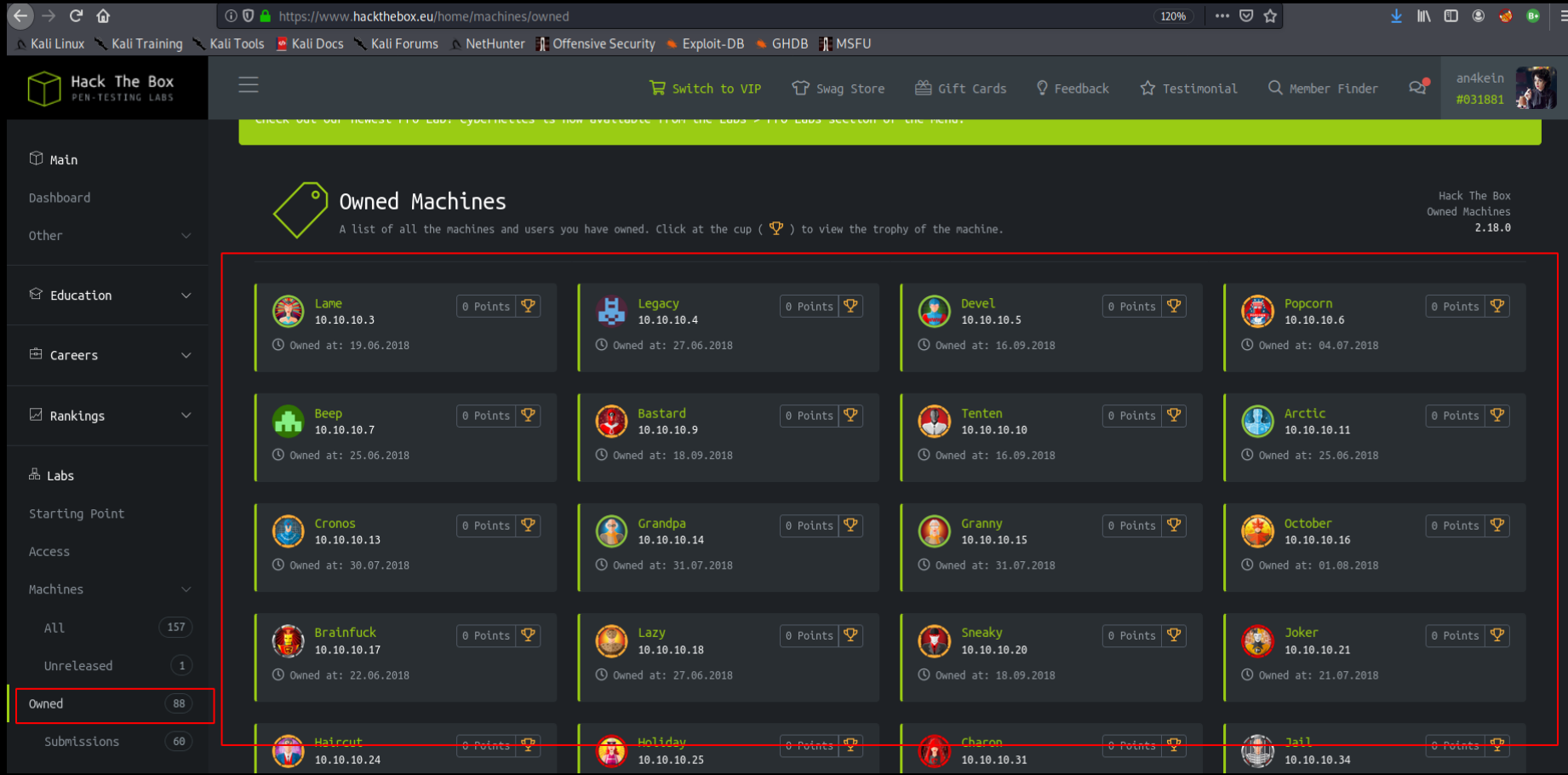
Hack The Box


Switch to VIP
Swag Store
Gift Cards
Feedback
Testimonial
Member Finder
an4kein
#031881
Active Machines
Retired Machines
VIP
To-Do
Release Date
Name
Difficulty
Rating
Owns
Last reset
Obscurity
4.0
7123
6946
17 hours ago
Patents
3.7
790
664
15 hours ago
Book
3.9
2665
2492
17 hours ago
Oouch
4.8
627
542
4 hours ago
ForwardSlash
3.8
1068
994
7 hours ago
Magic
4.5
1790
1568
< 1 hour
Status
Display To-Do On Top
Complete
Incomplete
Difficulty
Easy
Medium
Hard
Insane
Operating System
Linux
Windows
FreeBSD
Android
Solaris
Other

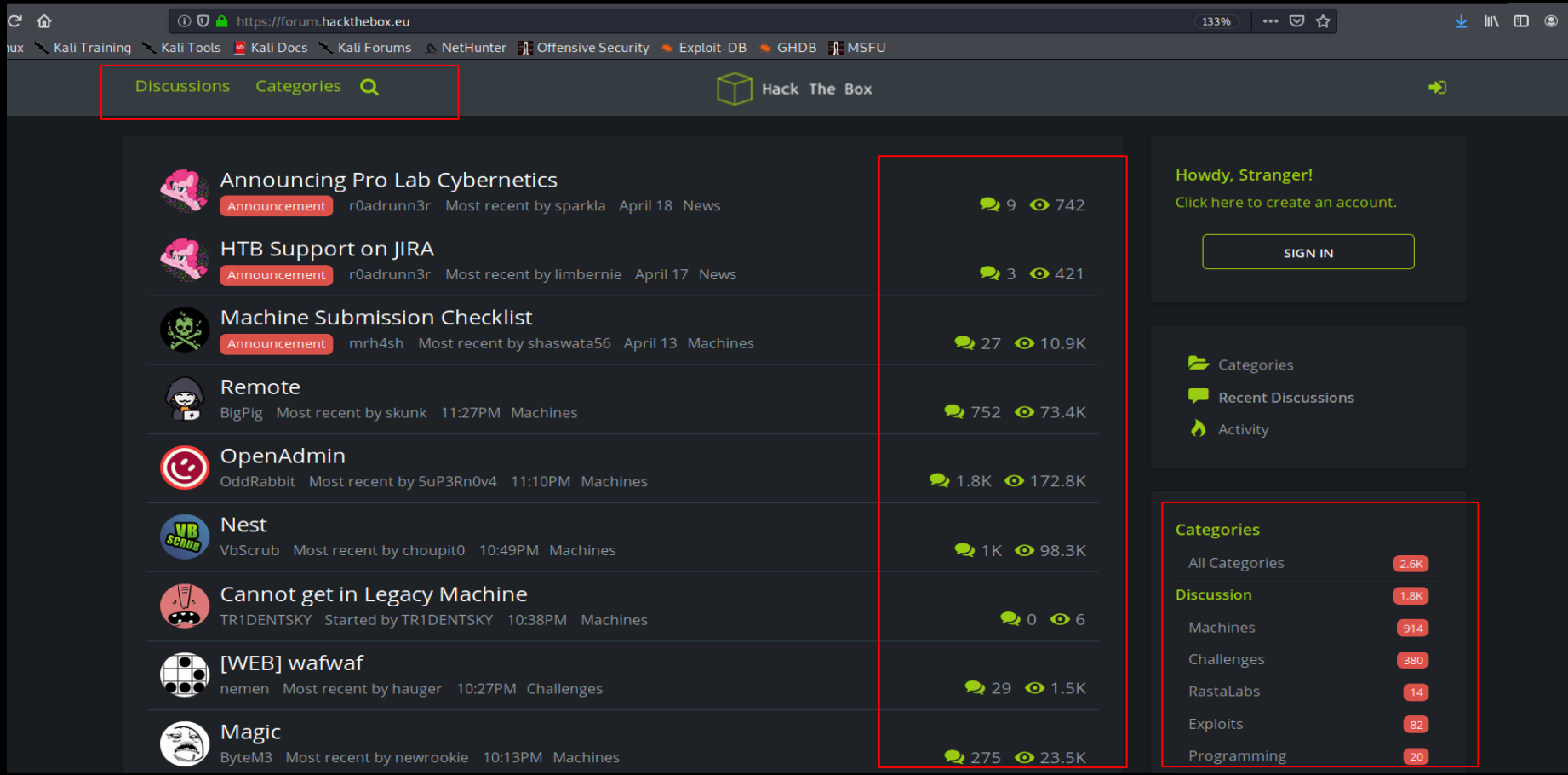
Hack The Box


Switch to VIP
Swag Store
Gift Cards
Feedback
Testimonial
Member Finder
an4kein
#031881
Become VIP today and get access to our retired machine pool! Click here for more information.
Active Machines
Retired Machines
VIP
To-Do
Filters
Name
Difficulty
Rating
Owns
Last reset
Actions
Popcorn 3.7 5217 4788 #
Tenten 3.7 2563 2593 #
Cronos 4.6 3768 3353 #
October 4.3 2571 1520 #
Lazy 4.8 2058 1936 #
Sneaky 5.0 1292 1046 #
Joker 5.0 627 614 #
Haircut 4.8 1803 1475 #
Holiday 5.0 469 478 #

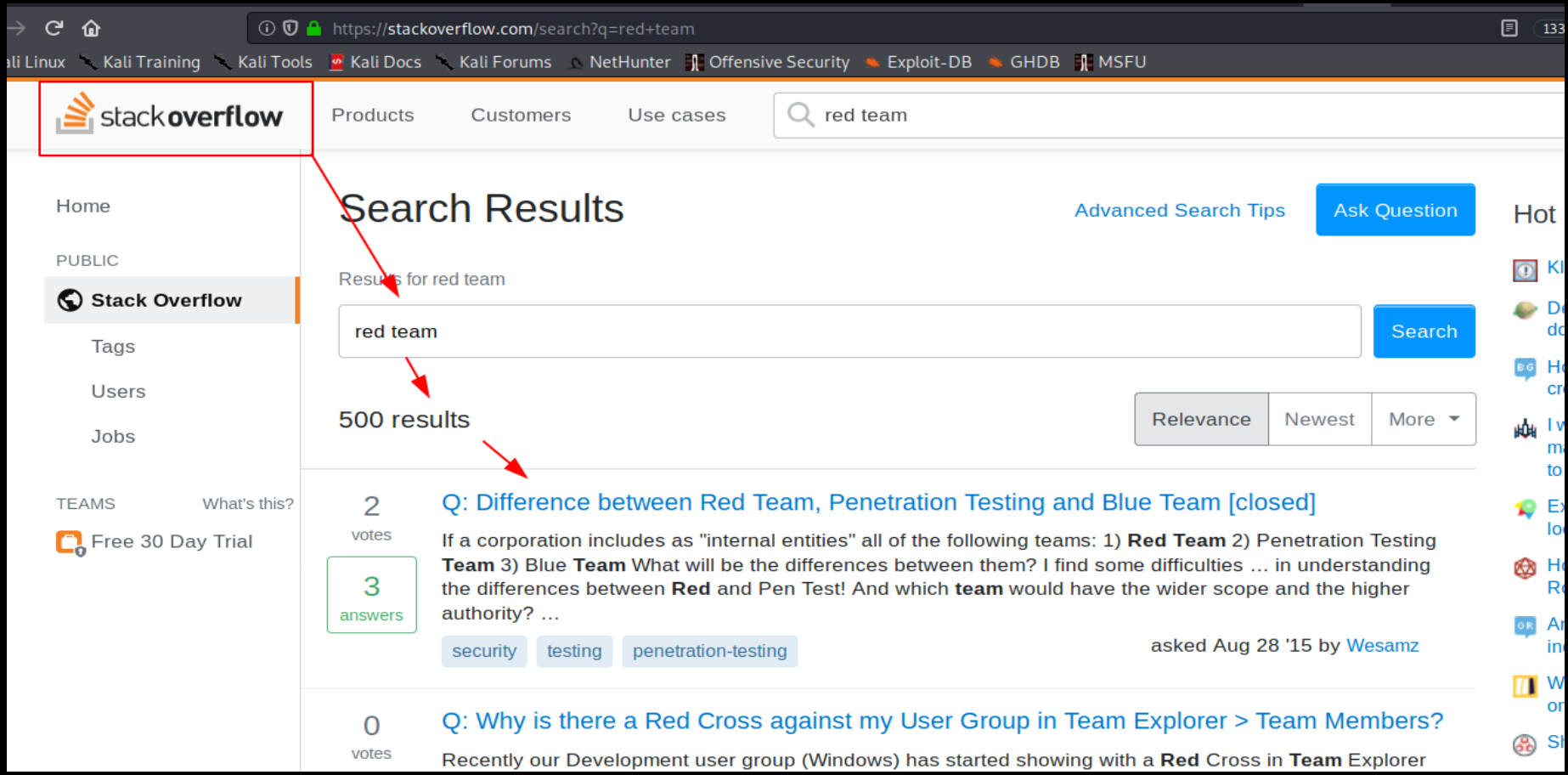
Hack The Box


https://www.hackthebox.eu/home/machines/owned
120%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Hack The Box
PEN-TESTING LABS
Switch to VIP
Swag Store
Gift Cards
Feedback
Testimonial
Member Finder
an4kein
#031881
Main
Dashboard
Other
Education
Careers
Rankings
Labs
Starting Point
Access
Machines
All 157
Unreleased 1
Owned 88
Submissions 60
Owned Machines
A list of all the machines and users you have owned. Click at the cup (🏆) to view the trophy of the machine.
Hack The Box
Owned Machines
2.18.0
Lame 10.10.10.3 0 Points Owned at: 19.06.2018
Legacy 10.10.10.4 0 Points Owned at: 27.06.2018
Devel 10.10.10.5 0 Points Owned at: 16.09.2018
Popcorn 10.10.10.6 0 Points Owned at: 04.07.2018
Beep 10.10.10.7 0 Points Owned at: 25.06.2018
Bastard 10.10.10.9 0 Points Owned at: 18.09.2018
Tenten 10.10.10.10 0 Points Owned at: 16.09.2018
Arctic 10.10.10.11 0 Points Owned at: 25.06.2018
Cronos 10.10.10.13 0 Points Owned at: 30.07.2018
Grandpa 10.10.10.14 0 Points Owned at: 31.07.2018
Granny 10.10.10.15 0 Points Owned at: 31.07.2018
October 10.10.10.16 0 Points Owned at: 01.08.2018
Brainfuck 10.10.10.17 0 Points Owned at: 22.06.2018
Lazy 10.10.10.18 0 Points Owned at: 27.06.2018
Sneaky 10.10.10.20 0 Points Owned at: 18.09.2018
Joker 10.10.10.21 0 Points Owned at: 21.07.2018
Haircut 10.10.10.24 0 Points
Holiday 10.10.10.25 0 Points
Charon 10.10.10.31 0 Points
Jail 10.10.10.34 0 Points

Hack The Box


https://forum.hackthebox.eu
133%
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Discussions
Categories
Hack The Box
Announcing Pro Lab Cybernetics
Announcement r0adrunn3r Most recent by sparkla April 18 News
9 742
HTB Support on JIRA
Announcement r0adrunn3r Most recent by limbernie April 17 News
3 421
Machine Submission Checklist
Announcement mrh4sh Most recent by shaswata56 April 13 Machines
27 10.9K
Remote
BigPig Most recent by skunk 11:27PM Machines
752 73.4K
OpenAdmin
OddRabbit Most recent by 5uP3Rn0v4 11:10PM Machines
1.8K 172.8K
Nest
VbScrub Most recent by choupit0 10:49PM Machines
1K 98.3K
Cannot get in Legacy Machine
TR1DENTSKY Started by TR1DENTSKY 10:38PM Machines
0 6
[WEB] wafwaf
nemen Most recent by hauger 10:27PM Challenges
29 1.5K
Magic
ByteM3 Most recent by newrookie 10:13PM Machines
275 23.5K
Howdy, Stranger!
Click here to create an account.
SIGN IN
Categories
Recent Discussions
Activity
Categories
All Categories 2.6K
Discussion 1.8K
Machines 914
Challenges 380
RastaLabs 14
Exploits 82
Programming 20

Hack The Box

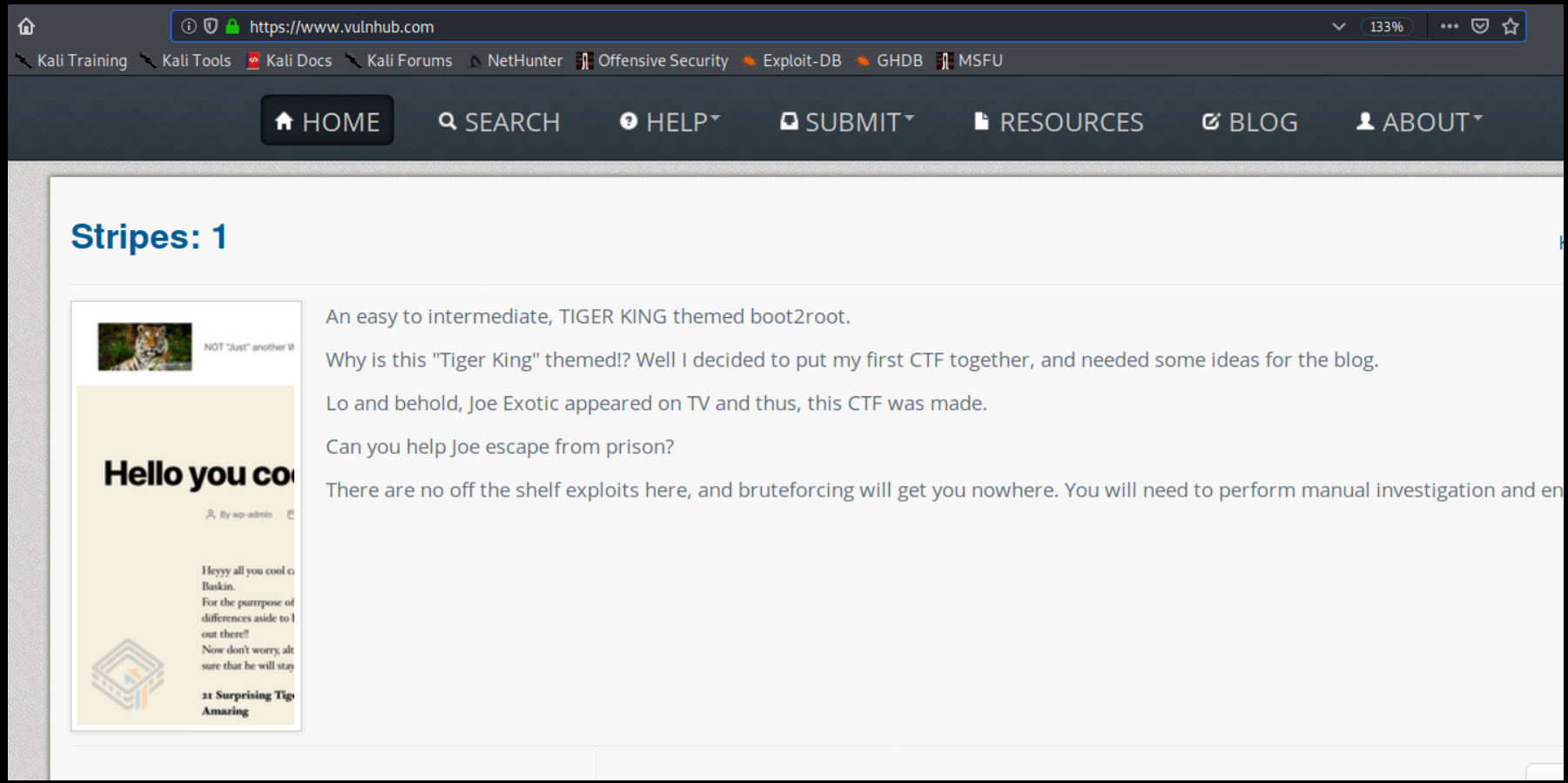

https://stackoverflow.com/search?q=red+team
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
stackoverflow
Products
Customers
Use cases
red team
Home
PUBLIC
Stack Overflow
Tags
Users
Jobs
TEAMS
What's this?
Free 30 Day Trial
Search Results
Advanced Search Tips
Ask Question
Results for red team
red team
Search
500 results
Relevance
Newest
More
2
votes
3
answers
Q: Difference between Red Team, Penetration Testing and Blue Team [closed]
If a corporation includes as "internal entities" all of the following teams: 1) Red Team 2) Penetration Testing Team 3) Blue Team What will be the differences between them? I find some difficulties … in understanding the differences between Red and Pen Test! And which team would have the wider scope and the higher authority? …
security
testing
penetration-testing
asked Aug 28 '15 by Wesamz
0
votes
Q: Why is there a Red Cross against my User Group in Team Explorer > Team Members?
Recently our Development user group (Windows) has started showing with a Red Cross in Team Explorer
Hot

VulnHub

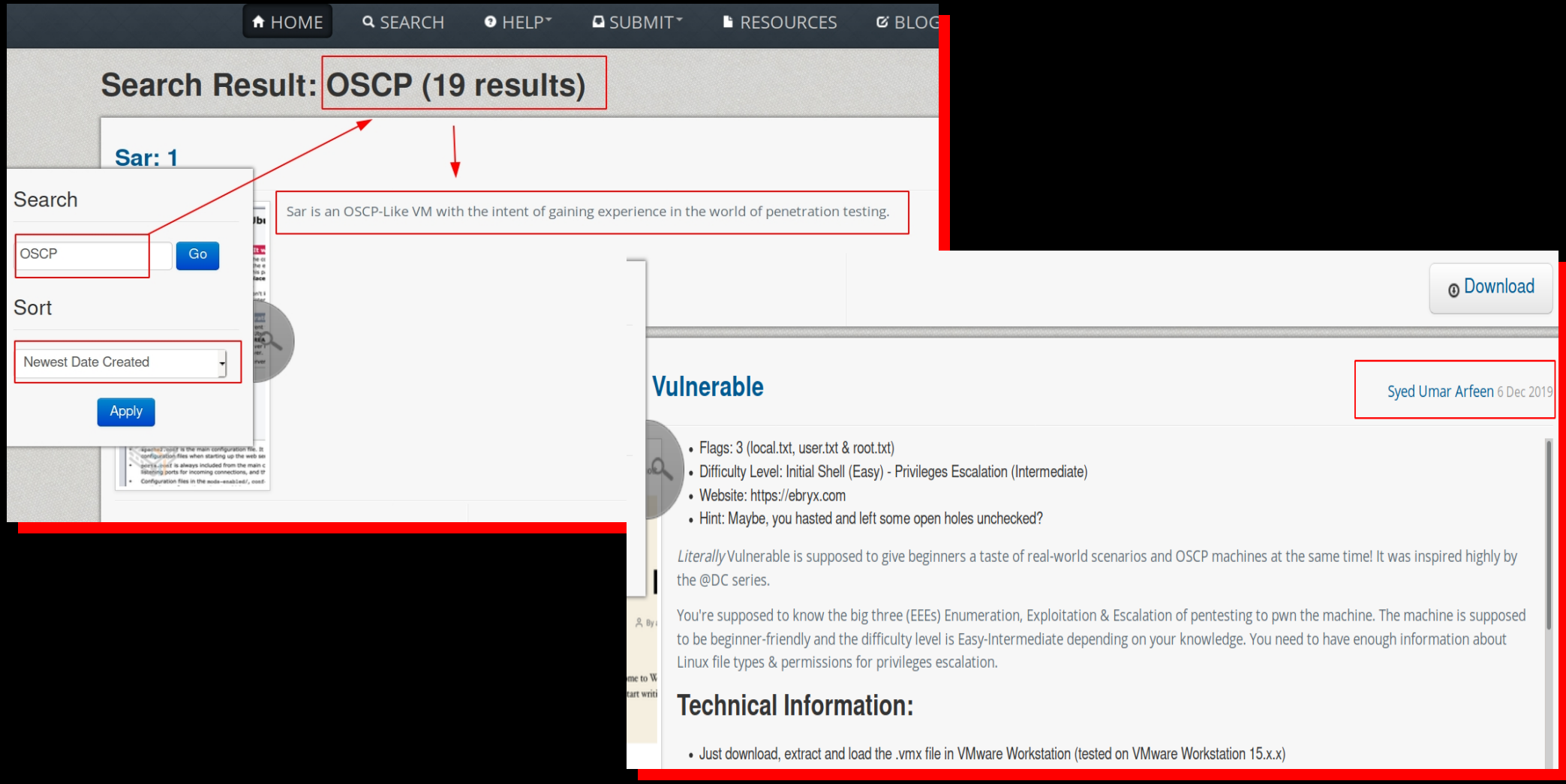

VULNHUB
VULNERABLE BY DESIGN


PWNED!
VULNHUB
VULNERABLE BY DESIGN

VulnHub

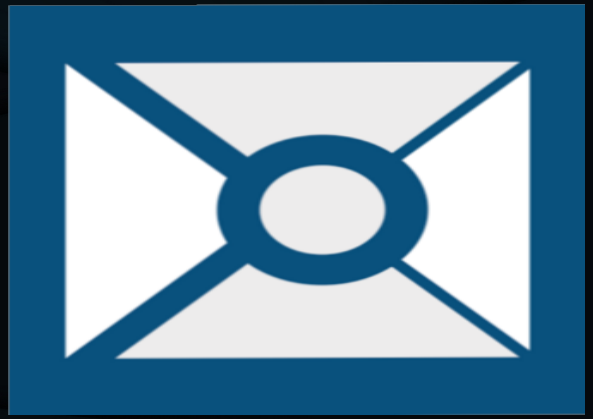

https://www.vulnhub.com
133%
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
HOME
SEARCH
HELP
SUBMIT
RESOURCES
BLOG
ABOUT
Stripes: 1
An easy to intermediate, TIGER KING themed boot2root.
Why is this "Tiger King" themed!? Well I decided to put my first CTF together, and needed some ideas for the blog.
Lo and behold, Joe Exotic appeared on TV and thus, this CTF was made.
Can you help Joe escape from prison?
There are no off the shelf exploits here, and bruteforcing will get you nowhere. You will need to perform manual investigation and en

VulnHub


HOME
SEARCH
HELP
SUBMIT
RESOURCES
BLOG
Search Result: OSCP (19 results)
Sar: 1
Sar is an OSCP-Like VM with the intent of gaining experience in the world of penetration testing.
Search
OSCP
Go
Sort
Newest Date Created
Apply
Download
Vulnerable
Syed Umar Arfeen 6 Dec 2019
Flags: 3 (local.txt, user.txt & root.txt)
Difficulty Level: Initial Shell (Easy) - Privileges Escalation (Intermediate)
Website: https://ebryx.com
Hint: Maybe, you hasted and left some open holes unchecked?
Literally Vulnerable is supposed to give beginners a taste of real-world scenarios and OSCP machines at the same time! It was inspired highly by the @DC series.
You're supposed to know the big three (EEEs) Enumeration, Exploitation & Escalation of pentesting to pwn the machine. The machine is supposed to be beginner-friendly and the difficulty level is Easy-Intermediate depending on your knowledge. You need to have enough information about Linux file types & permissions for privileges escalation.
Technical Information:
Just download, extract and load the .vmx file in VMware Workstation (tested on VMware Workstation 15.x.x)

Pentestit


CYBERATTACK WORLD MAP
IP
Location
Port
119.32.44.X
Guangzhou, CN
25
97.49.39.X
LaCrosse, US
25
107.18.3.X
NewYork, US
22
23.48.2.X
Ashburn, US
22
43.31.31.X
Kurashiki, JP
25
95.45.44.X
Cork, IE
22
81.35.29.X
LosRealejos, ES
22
51.19.7.X
CityofLondon, GB
8080
47.8.15.X
Lucknow, IN
8080
70.36.12.X
Saint-Pierre, PM
8080
89.27.45.X
Vantaa, FI
8080
43.31.31.X
Kurashiki, JP
25
115.14.3.X
Jeju-si, KR
443
55.35.26.X
SierraVista, US
443
59.32.37.X
Heyuan, CN
443
CYBERATTACK ACTIVITY
80
60
40
20
0



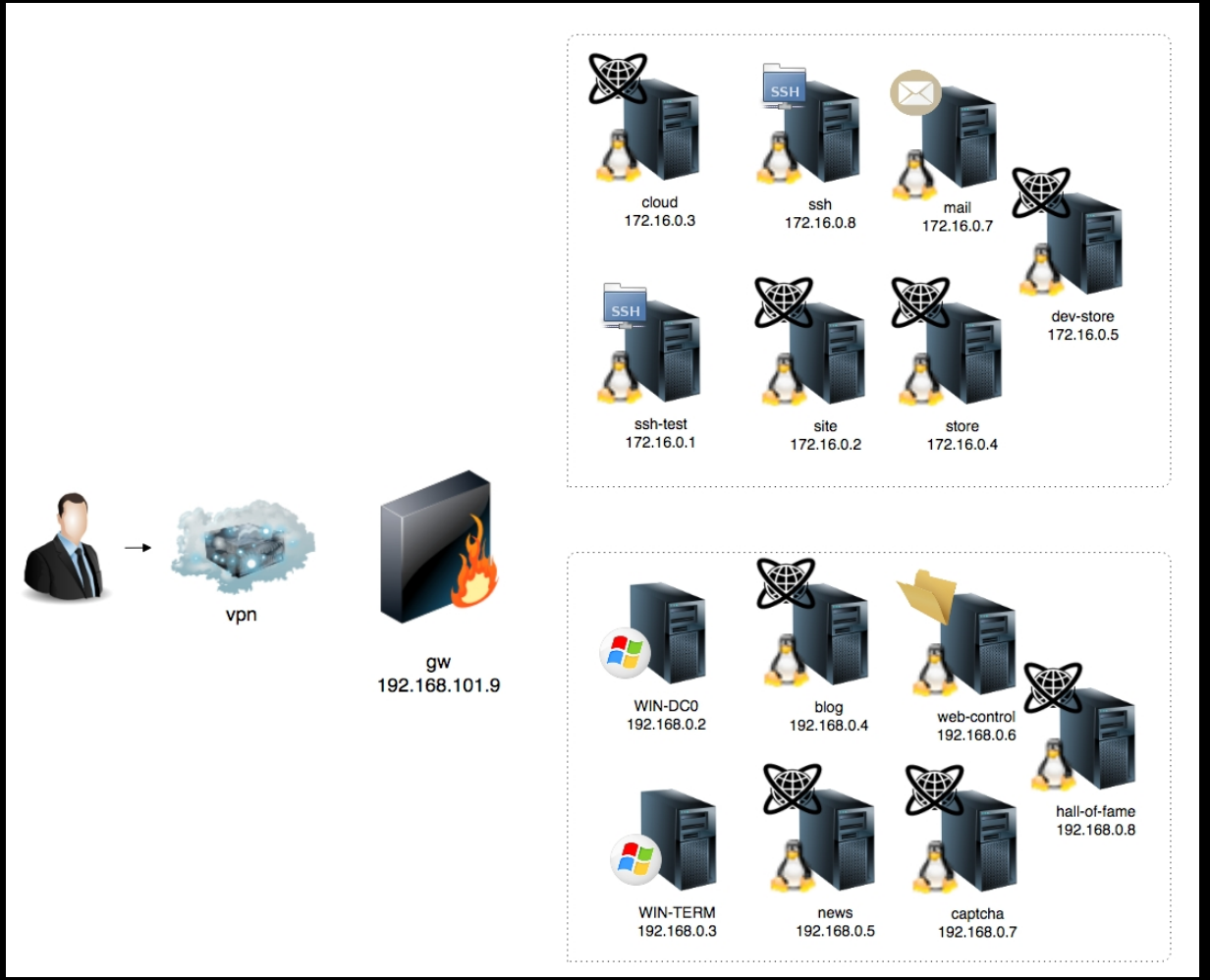
Pentestit

No laboratório são utilizados:

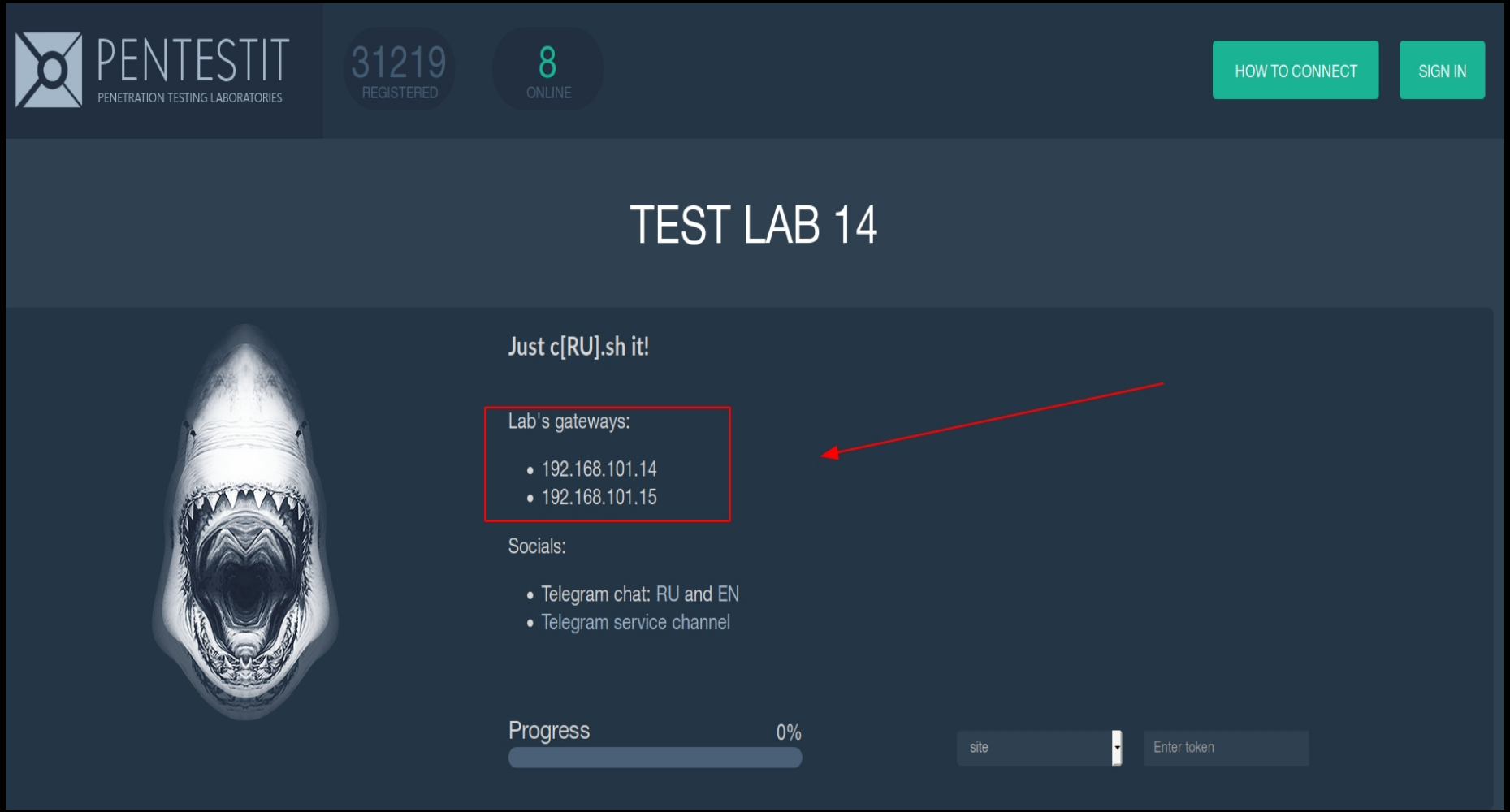
- Serviços de rede diferentes (Mail, DNS, AD, VPN, IDS, WAF, DB, etc.);
- Aplicações web, API e micros serviços (PHP, Python, Django, Java);
- Diferentes aplicativos de desktop e cliente-servidor;
- Serviços de suporte adicionais para deixar ainda mais realista.

Pentestit

Pentestit Lab v10



Pentestit


PENTESTIT
PENETRATION TESTING LABORATORIES
31219
REGISTERED
8
ONLINE
HOW TO CONNECT
SIGN IN
TEST LAB 14
Just c[RU].sh it!
Lab's gateways:
192.168.101.14
192.168.101.15
Socials:
Telegram chat: RU and EN
Telegram service channel
Progress
0%
site
Enter token

Pentestit

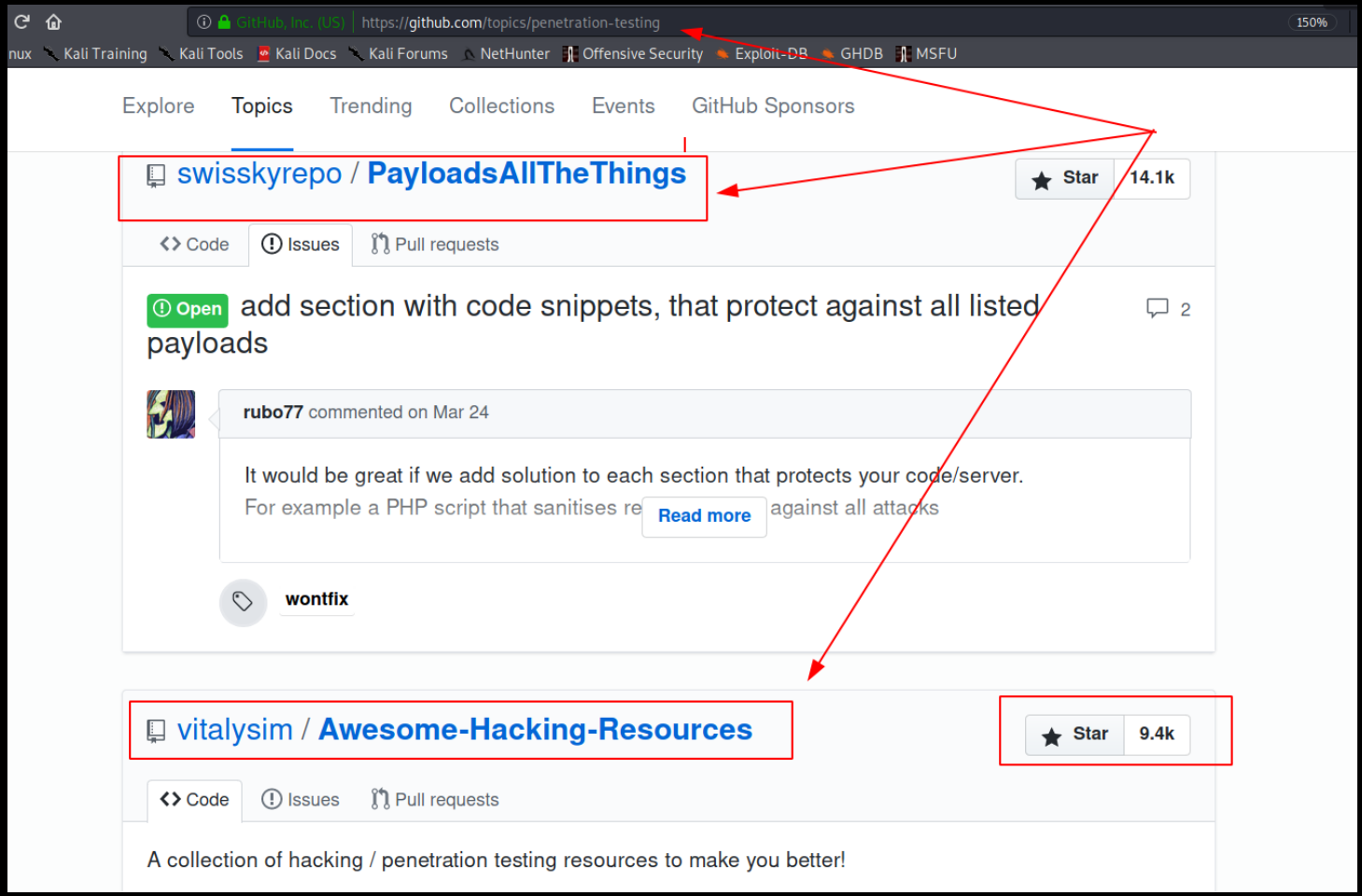
Para passar no laboratório, é necessário:

- Habilidades de trabalho com vários serviços e protocolos de rede;
- Conhecimento das melhores práticas de teste de penetração (OSINT, OWASP, etc.);
- Habilidades em trabalhar com ferramentas especializadas (Nmap, SQLmap, Burp Suite, WPScan, Nikto / DirBuster / w3af, Dig, Patator / Hydra, IDA Pro, etc.);
- Experiência em desenvolvimento e engenharia reversa (engenharia reversa);
- Experiência de pesquisa de fuzz e vulnerabilidade em serviços de rede e aplicativos da web.

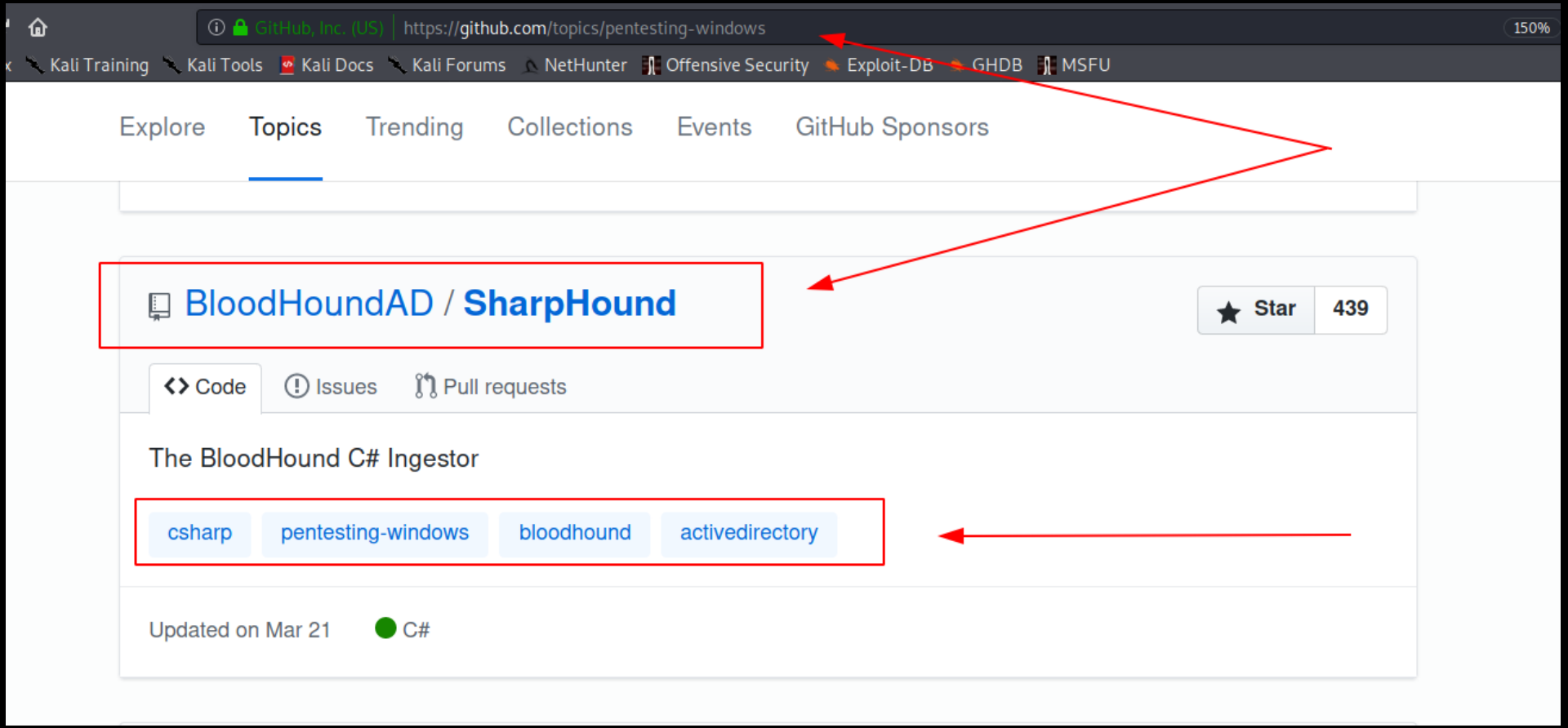
Hack With GitHub

Hack With GitHub

Hack With GitHub



Hack With GitHub



References:

- HackTheBox
  - https://www.hackthebox.eu/testimonials
  - https://www.hackthebox.eu/
  - https://stackoverflow.com/search?q=red+team
  - https://lolbas-project.github.io/#
  - https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
  - https://gtfobins.github.io/
- Pentestit
  - https://medium.com/@Pentestit_ru/just-crush-it-penetration-testing-laboratory-test-lab-14-34ee99874910
  - https://lab.pentestit.ru/pentestlabs/14

References:

- VulnHub
  - https://www.vulnhub.com/
  - https://www.youtube.com/watch?v=KzZXpwerD9E&list=PLzxlyLGmoMYGIjvpYPDvZz2A87ZXifoXL
- Hack With GitHub
  - https://github.com/Hack-with-Github/Awesome-Hacking
  - https://github.com/topics/