



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

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

The image shows a YouTube channel page for 'IppSec' with 86.9K subscribers. The channel's profile picture is a red and yellow robot. The main navigation bar includes links for HOME, VIDEOS, PLAYLISTS, COMMUNITY, CHANNELS, ABOUT, and a search icon. A prominent red 'SUBSCRIBE' button is located on the right side. Below the navigation, there is a section titled 'Uploads' with a 'PLAY ALL' link. Six video thumbnails are displayed, each with a title, duration, and view count:

- HackTheBox - Mango** | 53:27 | 13K views • 5 days ago
- Sunday Night Learning** | 5:00:29 | 19K views • Streamed 1 week ago
- HackTheBox - Travervsec** | 59:01 | 16K views • 1 week ago
- Creating a VM to learn Linux PrivEsc** | 2:56:23 | 16K views • Streamed 2 weeks ago
- HackTheBox - Registry** | 1:03:36 | 11K views • 2 weeks ago
- VulnHub: DC-9** | 1:46:09 | 8.4K views • 3 weeks ago

Hack The Box

The screenshot shows a web browser window with the URL <https://ippsec.rocks/#>. The page title is "IPPSEC". A search bar at the top contains the query "ldap". Below the search bar, there are two columns: "Video" on the left and "Description" on the right. The "Video" column lists several video thumbnails, some of which are highlighted with red boxes and arrows pointing to specific descriptions in the "Description" column. The "Description" column contains detailed text descriptions for each video thumbnail.

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

The screenshot shows the 'Access' page of the Hack The Box website. A red arrow points from the URL bar at the top to the 'Access' link in the top navigation bar. Another red arrow points from the 'Access' link in the left sidebar to the 'Getting Started' section. A third red arrow points from the 'Warning' text in the 'Tickets' section to the 'Warning' icon.

<https://www.hackthebox.eu/home/htb/access>

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

[Switch to VIP](#) [Swag Store](#) [Gift Cards](#) [Feedback](#) [Testimonial](#) [Member Finder](#) [an4kein #031881](#)

Dashboard Other Education Careers Rankings Labs Starting Point **Access**

Access

Lab Access details.

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.

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 [Switch](#)

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.

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

Screenshot of the Hack The Box website showing the Active Machines list.

The URL in the browser is <https://www.hackthebox.eu/home/machines>.

The sidebar on the left shows navigation links for Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, MSFU, and various challenges like Unreleased, Owned, Submissions, New Submission, Challenges, Endgame, Fortress, Pro Labs, Social (Private Messages, Shoutbox, Team Shoutbox), Forum, Discord, and NetSecFocus.

The main content area displays the "Active Machines" list with the following data:

Name	Difficulty	Rating	Owns	Last reset	Actions
Rope	Low	★ 4.5	1005 🚧 965 #	10 hours ago	
Control	Medium	★ 4.5	2288 🚧 1941 #	2 hours ago	
Obscurity	Medium	★ 4.0	7123 🚧 6946 #	17 hours ago	
Resolute	Medium	★ 4.7	7523 🚧 5911 #	2 hours ago	
PlayerTwo	Low	★ 4.3	901 🚧 759 #	3 hours ago	
OpenAdmin	Medium	★ 4.5	16098 🚧 15818 #	1 hour ago	
Monteverde	Medium	★ 4.3	5069 🚧 4590 #	10 hours ago	
Patents	Low	★ 3.7	790 🚧 664 #	15 hours ago	
Nest	Medium	★ 3.9	6418 🚧 5592 #	12 hours ago	
Fatty	Low	★ 4.6	690 🚧 632 #	23 hours ago	

Hack The Box

Active Machines Retired Machines VIP To-Do

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

Release Date ↑

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 To-Do

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
Ouch		★ 4.8	627 🚧 542 #	4 hours ago
ForwardSlash		★ 3.8	1068 🚧 994 #	7 hours ago
Magic		★ 4.5	1790 🚧 1568 #	< 1 hour

Release Date ↑

Status

- Display To-Do On Top
- Complete
- Incomplete

Difficulty

- Easy
- Medium
- Hard
- Insane

Operating System

- Linux
- Windows
- FreeBSD
- Android
- Solaris
- Other

← →

Hack The Box

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

Screenshot of the Hack The Box website showing the "Owned Machines" section.

The page title is "Owned Machines". A sub-header says: "A list of all the machines and users you have owned. Click at the cup (Trophy) to view the trophy of the machine."

The "Owned" tab is selected in the sidebar, indicated by a red border.

The main content area displays a grid of 24 machine cards, each with a thumbnail, name, IP address, points (0), and a trophy icon.

Name	IP Address	Points	Trophy
Lame	10.10.10.3	0 Points	
Legacy	10.10.10.4	0 Points	
Devel	10.10.10.5	0 Points	
Popcorn	10.10.10.6	0 Points	
Beep	10.10.10.7	0 Points	
Bastard	10.10.10.9	0 Points	
Tenten	10.10.10.10	0 Points	
Arctic	10.10.10.11	0 Points	
Cronos	10.10.10.13	0 Points	
Grandpa	10.10.10.14	0 Points	
Granny	10.10.10.15	0 Points	
October	10.10.10.16	0 Points	
Brainfuck	10.10.10.17	0 Points	
Lazy	10.10.10.18	0 Points	
Sneaky	10.10.10.20	0 Points	
Joker	10.10.10.21	0 Points	
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

Discussions Categories

Announcing Pro Lab Cybernetics
Announcement r0adrunn3r Most recent by sparkla April 18 News

HTB Support on JIRA
Announcement r0adrunn3r Most recent by limbernie April 17 News

Machine Submission Checklist
Announcement mrh4sh Most recent by shaswata56 April 13 Machines

Remote
BigPig Most recent by skunk 11:27PM Machines

OpenAdmin
OddRabbit Most recent by 5uP3Rn0v4 11:10PM Machines

Nest
VbScrub Most recent by choupit0 10:49PM Machines

Cannot get in Legacy Machine
TR1DENTSKY Started by TR1DENTSKY 10:38PM Machines

[WEB] wafwaf
nemen Most recent by hauger 10:27PM Challenges

Magic
ByteM3 Most recent by newrookie 10:13PM Machines

Howdy, Stranger!
Click here to create an account.

SIGN IN

Categories

Recent Discussions

Activity

Categories

Category	Count
All Categories	2.6K
Discussion	1.8K
Machines	914
Challenges	380
RastaLabs	14
Exploits	82
Programming	20

Hack The Box

A screenshot of a web browser displaying search results on Stack Overflow for the query "red team". The results page shows 500 results for the term "red team". The first result is a question titled "Q: Difference between Red Team, Penetration Testing and Blue Team [closed]". The question has 2 votes and 3 answers. It is tagged with security, testing, and penetration-testing. It was asked on August 28, 2015, by Wesamz. The second result is a question titled "Q: Why is there a Red Cross against my User Group in Team Explorer > Team Members?". The results page includes navigation buttons for Relevance, Newest, and More.

https://stackoverflow.com/search?q=red+team

Products Customers Use cases

red team

Home

PUBLIC

Stack Overflow

Tags

Users

Jobs

TEAMS

What's this?

Free 30 Day Trial

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

KI

D

BG

H

I

E

H

OR

W

S

VulnHub



VulnHub

https://www.vulnhub.com

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

NOT "Just" another V

Heyyy all you cool cats! I'm Baskin. For the purrpose of differences aside to look out there! Now don't worry, alt sure that he will stay

xx Surprising Tiger Amazing

VulnHub

[HOME](#)[SEARCH](#)[HELP](#)[SUBMIT](#)[RESOURCES](#)[BLOG](#)

Search Result: OSCP (19 results)

Sar: 1

Search

OSCP

[Go](#)

Sort

Newest Date Created

[Apply](#)

Sar is an OSCP-Like VM with the intent of gaining experience in the world of penetration testing.

[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?

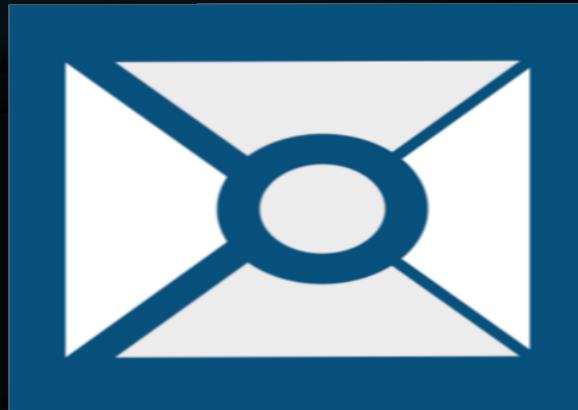
LiterallyVulnerable is supposed to give beginners a taste of real-world scenarios and OSCP machines at the same time! It was inspired highly by the @DC series.

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



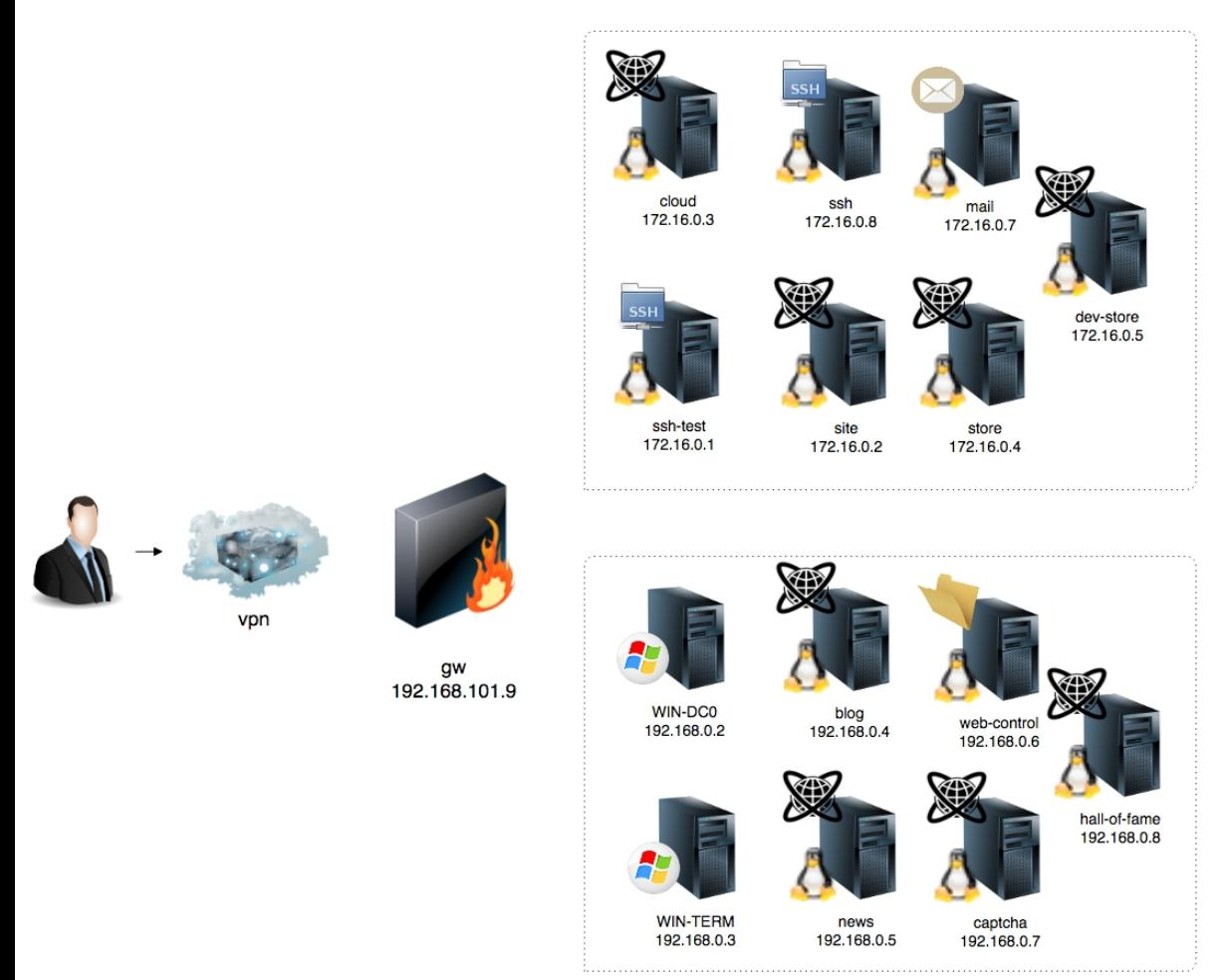
Pentestit

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

penetration-testing

Here are 670 public repositories matching this topic...

Language: All ▾ Sort: Best match ▾

[Hack-with-Github / Awesome-Hacking](#) Star 36.7k

Code Issues Pull requests

A collection of various awesome lists for hackers, pentesters and security researchers

android security awesome reverse-engineering pentesting-windows hacking penetration-testing
bug-bounty fuzzing

Hack With GitHub

The screenshot shows a GitHub search results page for the topic "penetration-testing". The URL in the address bar is https://github.com/topics/penetration-testing. The search results are displayed in a grid format.

Top Result (swisskyrepo / PayloadsAllTheThings):

- Repository Name:** swisskyrepo / **PayloadsAllTheThings**
- Star Count:** 14.1k
- Issue Count:** 2
- Description:** add section with code snippets, that protect against all listed payloads
- Comment by rubo77:** commented on Mar 24
It would be great if we add solution to each section that protects your code/server.
For example a PHP script that sanitises re [Read more](#) against all attacks
- Status:** wontfix

Bottom Result (vitalysim / Awesome-Hacking-Resources):

- Repository Name:** vitalysim / **Awesome-Hacking-Resources**
- Star Count:** 9.4k
- Description:** A collection of hacking / penetration testing resources to make you better!

Hack With GitHub

The screenshot shows a GitHub topic page for 'pentesting-windows'. The URL in the browser bar is <https://github.com/topics/pentesting-windows>. The page features a navigation bar with 'Explore', 'Topics' (which is underlined), 'Trending', 'Collections', 'Events', and 'GitHub Sponsors'. A red arrow points from the top right towards the 'Topics' bar. Below the navigation is a search bar. A red box highlights the repository title 'BloodHoundAD / SharpHound'. To the right of the title is a star icon and the number '439'. Another red arrow points from the top right towards this star/icon area. Below the title are buttons for 'Code', 'Issues', and 'Pull requests'. A red box highlights the tags 'csharp', 'pentesting-windows', 'bloodhound', and 'activedirectory'. A red arrow points from the bottom right towards this tag box. At the bottom left, it says 'Updated on Mar 21'. A green circle icon with 'C#' next to it is also present.

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=PLzxyLGmoMYGljvpYPDvZz2A87ZXifoXL>
- Hack With GitHub
 - <https://github.com/Hack-with-Github/Awesome-Hacking>
 - <https://github.com/topics/>