

30 days of Practice PenTest? #2

#30DAYSOFPENTEST

Organize as you wish, it has no focus, no deadline, 30 days does not necessarily mean 30 consecutive days.

1) Incident Responder Path

<https://app.letsdefend.io/path/incident-responder-path>

2) Cyber Kill Chain

<https://app.letsdefend.io/training/lessons/cyber-kill-chain>

3) Mitre Att&ck

<https://app.letsdefend.io/training/lessons/mitre-attck-framework>

4) GTFOBins

<https://app.letsdefend.io/training/lessons/gtfobins>

5) Hacked Web Server Analysis

<https://app.letsdefend.io/training/lessons/hacked-web-server-analysis>

6) Matrix-Breakout 2: Morpheus

<https://www.vulnhub.com/entry/matrix-breakout-2-morpheus,757/>

7) DigitalWorld.Local: Electrical

<https://www.vulnhub.com/entry/digitalworldlocal-electrical,747/>

8) Gemini Inc 2

<https://www.vulnhub.com/entry/gemini-inc-2,234/>

9) Pilgrimage

<https://app.hackthebox.com/machines/Pilgrimage>

10)Topology

<https://app.hackthebox.com/machines/Topology>

11)PC

<https://app.hackthebox.com/machines/PC>

12)Busqueda

<https://app.hackthebox.com/machines/Busqueda>

13)Routing-Based SSRF

<https://portswigger.net/web-security/host-header/exploiting/lab-host-header-routing-based-ssrf>

14) Blind SSRF with Shellshock exploitation

<https://portswigger.net/web-security/ssrf/blind/lab-shellshock-exploitation>

15) SQL injection vulnerability allowing login bypass

<https://portswigger.net/web-security/sql-injection/lab-login-bypass>

16) Blind SQL injection with conditional responses

<https://portswigger.net/web-security/sql-injection/blind/lab-conditional-responses>

17)OWASP WrongSecrets

<https://github.com/OWASP/wrongsecrets>

18)Security CTF AWS 101

<https://r00tz-ctf.awssecworkshops.com/>

19) Attacking and Defending AWS

<https://resources.tryhackme.com/attacking-and-defending-aws>

20) PenTesting Cloud Learning

<https://pentesting.cloud/>

21) Cerberus

<https://app.hackthebox.com/machines/Cerberus>

22) Coder

<https://app.hackthebox.com/machines/Coder>

23) Free Web Hacking Course

<https://davidbombal.com/free-web-hacking-course/>

24) JWT Hacking Challenges

<https://github.com/onsecru/jwt-hacking-challenges>

<https://systemweakness.com/hacking-jwt-3324cba98210>

25) JWT Security

<https://portswigger.net/web-security/jwt>

26) Threat and Vulnerability Management

<https://tryhackme.com/module/threat-and-vulnerability-management>

27) Derailed

<https://app.hackthebox.com/machines/Derailed>

28) API PenTest

<https://www.apisecuniversity.com/courses/api-penetration-testing>

29) Active Directory PenTesting

<https://dev.to/adamkatora/building-an-active-directory-pentesting-home-lab-in-virtualbox-53dc>

30) GOAD (Game of Active Directory)

<https://github.com/Orange-Cyberdefense/GOAD>

My LinkedIn: <https://www.linkedin.com/in/joas-antonio-dos-santos/>