30 days of Practice PenTest?

#30DAYSOFPENTEST

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

Make sure you learn and absorb as much of the free as you can extract. Then I do a 30 days of vulnhub ;)

#Web #Mobile #Linux #Windows #Bufferoverflow #Activedirectory

1) Try Hack Me Room Owasp top 10
https://tryhackme.com/room/owasptop10

2) Try Hack Me Room Owasp Juice Shop
https://tryhackme.com/room/owaspjuiceshop

3) Try Hack Me Room Windows Fundamentals
https://tryhackme.com/room/windowsfundamentals1xbx
https://tryhackme.com/room/winadbasics

4) Information Disclosure Portswigger Academy
https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages

https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-version-control-history

https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-authentication-bypass

5) XSS Portswigger Academy
https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded

https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink

https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-href-attribute-sink

6) Mr r3b0t Vulnhub
https://www.vulnhub.com/entry/bizarre-adventure-mrr3b0t,561/

7) Try Hack Me Room Active Directory Attack
https://tryhackme.com/room/breachingad

8) XXE Portswigger Academy
https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files

https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf

https://portswigger.net/web-security/xxe/lab-xxe-via-file-upload

9) SSRF Portswigger Academy
https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost

https://portswigger.net/web-security/ssrf/lab-ssrf-filter-bypass-via-open-redirection

10) Rickdiculouslyeasy Vulnhub
https://www.vulnhub.com/entry/rickdiculouslyeasy-1,207/

11) Stickyfingers Vulnhub
https://www.vulnhub.com/entry/bizarre-adventure-sticky-fingers,560/

12) Kioptrix Level 1.3 Vulnhub
https://www.vulnhub.com/entry/kioptrix-level-13-4,25/

13) Bellatrix Vulnhub
https://www.vulnhub.com/entry/hogwarts-bellatrix,609/

14) Try Hack Me Room Buffer Overflow Prep
https://tryhackme.com/room/bufferoverflowprep

15) OS Command Injection Portswigger Academy
https://portswigger.net/web-security/server-side-template-injection/exploiting/lab-server-side-template-injection-basic

https://portswigger.net/web-security/os-command-injection/lab-simple

https://portswigger.net/web-security/os-command-injection/lab-blind-time-delays

16) File Upload Vulnerabilities Portswigger Academy
https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload

https://portswigger.net/web-security/file-upload/lab-file-upload-web-shell-upload-via-content-type-restriction-bypass

https://portswigger.net/web-security/file-upload/lab-file-upload-web-shell-upload-via-race-condition

17) Busqueda Hack The Box
https://app.hackthebox.com/machines/Busqueda

18) JWT Portswigger Academy
https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-unverified-signature

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature-verification

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-weak-signing-key

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-jwk-header-injection

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-jku-header-injection

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-kid-header-path-traversal

https://portswigger.net/web-security/jwt/algorithm-confusion/lab-jwt-authentication-bypass-via-algorithm-confusion

19) Cat Mobile Hack The Box
https://app.hackthebox.com/challenges/cat

20) SuperMarket Hack The Box
https://app.hackthebox.com/challenges/supermarket

21) Joker Hack The Box
https://app.hackthebox.com/challenges/joker

22) Seattle Lab Buffer Overflow
https://ys2k-iwnl.medium.com/buffer-overflow-exploiting-seattle-lab-mail-slmail-61b1f659c8dc

https://github.com/CyberSecurityUP/Buffer-Overflow-Labs

23) OnlyforYou Hack The Box
https://app.hackthebox.com/machines/OnlyForYou

24) Escape Hack The Box
https://app.hackthebox.com/machines/Escape

25) Insecure Deserialization Portswigger Academy
https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-data-types

https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-using-application-functionality-to-exploit-insecure-deserialization

https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-arbitrary-object-injection-in-php

https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-developing-a-custom-gadget-chain-for-java-deserialization

26) Djinn3 Proving Ground Lab
https://portal.offsec.com/

27) InsanityHosting Proving Ground Lab
https://portal.offsec.com/

28) Flight Hack The Box
https://app.hackthebox.com/machines/Flight

29) Absolute Hack The Box
https://app.hackthebox.com/machines/Absolute

30) Joestar Vulnhub
https://www.vulnhub.com/entry/bizarre-adventure-joestar,590/

Sometimes I draw some things or play some vouchers, sometimes it's to help, sometimes it's for me to feel good and useful with myself.

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