CTF, Laboratori, Challenge

INTRODUZIONE:
I CTF sono strumenti utilissimi per mettersi alla prova e per imparare nuove cose, nonché per tenere il cervello allenato a pensare.
Sono in vari formati, i più comuni Boot2Root, Jeopardy e attack/defense.

Ormai internet è pieno di CTF ed io cercherò di darmi una mappa per sapervi orientare in quello che meglio si adatta alle vostre esigenze, ma tenete presente che chi non capisce un beneamato cazzo di informatica, e che a malapena sa fare click con il mouse su un sistema windows, non avrà vita facile con i CTF anzi molto probabilmente si demoralizzerà e lascerà perdere. Chi invece ha già solide basi di informatica e qualche base di Pentestet/Hacking allora troverà nei CTF un fedelissimo amico.

Meglio ancora se avete un team con cui condividere e crescere tutti assieme.

Prima di imbattersi nella lettura del resto del documento, invito caldamente a leggere questo link che secondo me racchiude la verità assoluta alle domande più frequenti che i niubbi pongono insistentemente e ciclicamente in ogni forum, gruppo, chat, riguardante la sicurezza informatica:
https://github.com/infosecita/documenti/blob/master/FAQ.md

Un altro link molto interessante è il talk del mio amico Yuntao, riguardante sempre i CTF e con una bellissima dimostrazione pratica:
https://www.youtube.com/watch?v=7i9RujKUubU

GIOCHI PER IMPARARE:
In questa lista vediamo una serie di siti nei quali sono presenti dei veri e propri giochi finalizzati ad imparare una determinata tecnologia.

- VIM Adventure è un gioco online in cui si impara ad utilizzare il mitico editor di testo da console vi o vim. Si è alle prese con un simpatico personaggio che deve muoversi nei vari schemi, ed ovviamente tutti i tasti usati per farlo muovere ed interagire sono gli stessi usati in vi.
- CommandLine Challenge è un sito che, come suggerisce il nome stesso, propone una serie di challenge base per imparare ad usare la command line di linux
- OverTheWire è un altro sito in cui ci sono micro-challenge focalizzate all'uso della console di linux e di alcuni aspetti base del sistema operativo
- UnderTheWire Allo stesso modo questo sito ha come obiettivo insegnare l'uso di powersehll in un percorso guidato
- SQL Zoo Questo sito vi guida in un step by step focalizzato ad imparare il linquaggio SQL, molto utile per l'exploitation di sql injection
- LinuxCommand.org Altro sito online per imparare l'uso della shell linux

CHALLENGE:

Vediamo ora una carrellata di siti contenenti challenge

- WebSec è un sito con varie challenge web diviso per difficoltà
- BreakThisSQLI si propone come sito di challenge orientate alle sql injection (a volte non risponde il sito, riprovare in momenti diversi)
- XSS Game come intuibile dal nome qui c'è una collezione di challenge XSS
- HackThis questo sito si compone da varie challenge divise per tipologia, in pieno stile Jeopardy
- HackThisSite altri sito in stile Jeopardy, con una sezione di challenge singole e con una serie di casi reali
- W3challs altro sito con challenge divise per categoria in stile Jeopardy
- CTFTime principale sito che raccoglie le CTF online. Queste CTF in stile Jeopardy sono online solo per il periodo della durata della CTF, si partecipa solitamente in team e c'è un sistema di ranking. Qui partecipano i team più grossi italiani e non specializzati in Jeopardy (vedi i vari team universitari ma non solo)
- RootMe altro sito con challenge di tipo Jeopardy ma contiene anche una sezione per aprire delle stanze virtuali nelle quali caricare delle Boot2Root a scelta tra quelle presenti nell'elenco
- Cryptopals come intuibile, challenge di crypto
- OwnedLab altro sito con challenge in stile Jeopardy e con macchine Boot2Root
- HackMe servizio di challenge gratuito fornito alla community da eLearnSecurity che raccoglie un'infinità di challenge principalmente orientate al WEB

BOOT2ROOT:
I CTF Boot2Root si differenziano dalle Jeopardy in quanto qui l'ambito non è ben definito e non ci sono divisioni per categorie. In questo tipo di sfida, ci si trova davanti ad una o più macchine connesse in rete, virtuali, dockerizzate ecc.. E l'obbiettivo solitamente è prima ottenere accesso con un utente non privilegiato e quindi catturare la flag (CTF = Capture the Flag) nella home dell'utente e poi con varie tecniche di privilege escalation elevarsi a root (in ambienti linux) e system in (ambienti windows). La flag solitamente è un file di testo con una serie di numeri e lettere, a volte potrebbero essere degli MD5 o simili.

- LAMP Security Training collezione di macchine, in formato ISO da scaricare e installare tramite vmware/virtualbox/qemu utili per capire come da un app web configurata male o vulnerabile, sia possibile poi compromettere l'intero sistema
- Gracefully vulnerable Machine esempio di boot2root creata dalla simpatica autrice del blog graceful security
- VulnHub l'archivio internet più grande di boot2root, contiene piu di 100 macchine vulnerabili da scaricare e rompere :)
- RootMe altro sito con challenge di tipo Jeopardy ma contiene anche una sezione per aprire delle stanze virtuali nelle quali caricare delle Boot2Root a scelta tra quelle presenti nell'elenco
- OwnedLab altro sito con challenge in stile Jeopardy e con macchine Boot2Root

LABORATORI ONLINE:
In questa sezione vediamo dei veri e propri laboratori online, solitamente contenenti Boot2root ma con la differenza che non c'è bisogno di scaricare nulla sul proprio PC. Basta infatti collegarsi in VPN alla rete del laboratorio online e ci si trova immersi in un infinità di sistemi pronti ad essere violati.

- HackTheBox il più grande ed attivo laboratorio online, con oltre 100k utenti iscritti. Il lab è composto ad oggi da 99 macchine, di cui le ultime 20 accessibili, mentre le altre (ritirate) accessibili solo attraverso un account vip del costo di 10$ mensili. Sebbene all'inizio le macchine erano molto semplici, oramai si è raggiunto un livello di complessità tale che le macchine di OSCP sembrano un gioco da ragazzi in confronto. Consigliatissimo quindi a chiunque voglia mettersi in gioco o che voglia prepararsi per la OSCP. A supporto delle macchine ritirate, per chi vuole imparare, ci sono i writeup ufficiale (scaricabili solo con account VIP) e i fantastici video di IPPSEC (lo trovato su Youtube).
  Infine HackTheBox offre anche dei laboratori PRO al costo di 90£ al mese, come rastalab e offshore, dove c'è un'intera infrastruttura di rete con dominio windows e tutto quello che si può trovare in una rete aziendale moderna, con sistemi patchati, sistemi di protezioni attivi, e utenti reali simulati. Insomma una meraviglia.
- WizardLabs laboratorio nuovo ma ben fatto, in pieno stile HackTheBox con, per ora, 17 macchine divise per difficoltà.
- CTF365 Questo sito si offre per mettere su una piattaforma di tipo ATTACK/DEFENSE ma onestamente non ho mai capito come funzioni
- MDSEC è il laboratorio creato da e per gli autori del bestseller "The WebApplication Hackers Habdbook". Il lab si propone di offrire una piattaforma dove mettere in pratica ogni capitolo ed argomento spiegato nel libro stesso. Ad oggi il libro viene definito comunemente la bibbia del web hacking
- SEED Project questo lab offre esercitazioni riguardanti il web, il networking e il system hacking
- Pentestit.ru laboratorio fondato da una società di pentest russa, che offre dei laboratori molto grandi(tra le 40 e le 60 macchine a lab) a pagamento con tanto di persona che ti segue h24 e ti aiuta nella risoluzione del lab stesso. Il costo è di circa 400$ con l'istruttore e 250$ senza. Inoltre, ogni anno mette a disposizione un lab molto più piccolo, circa 16 macchine, totalmente gratuito.
- VulHub da non confondere con vulnhub, è una raccolta github di docker suddivisi per singola CVE, in modo da potersi esercitare in modo molto veloce su una vulnerabilità specifica.

- Attack/defense laboratorio gratuito per ora, con oltre 505 esercitazioni, suddiviso in categorie stile Jeopardy. Questo lab è prodotto da PentesterAcademy, e utilizzato molto nei videocorsi offerti dal sito stesso. Veramente ben fatto e adatto a tutti i livelli
- PentesterAcademy REDTEAM Lab il più grande ed immenso laboratorio dove esercitarsi sulle tecniche di redteam, domain and AD Takeover, lateral movement ecc.. Con un costo di soli 400$ (spesso in promozione a molto meno) ci si troverà a dover affrontare 42 Challenges, 60 Flags, >200 Hours of Torture :) Basta guardare l'immagine con la mappa di rete per capire di cosa stiamo parlando. Non solo un server, non solo una rete e un dominio, ma una intera foresta, con lo scopo di exploitare anche le relazioni di trust inter foresta.
- Alpha Level e Zeta Level due lab di 24 ore ciascuno, a prezzo regalo, 15 $ ma comprando i libri dell'autore, all'interno si trovano i coupon sconto e alla fine il lab costa 10$. Nonostante i nomi dei 3 libri "hack like a pornstar, hack like a legend, hack like a god" probabilmente scelti per fare hype, i contenuti sono i più chiari ed esaustivi mai trovati (personalmente) in un libro del genere. Ogni libro costa solamente 9,99$ ed appunto contiene lo sconto per i lab, veramente istruttivi. Oltre a questi tre libri ci sono anche i libricini con i writeup per i lab, ma non comprateli, in quanto se comprate il lab, nei 15/10$ sono già compresi anche i libricini wirteup del valore di altri 9,9$. Insomma consigliatissimo.

CREA IL TUO LAB:

- https://opencyberchallenge.net/
- https://rileykidd.com/2015/05/06/how-to-add-an-xss-able-bot-to-your-ctf/
- https://github.com/Sliim/pentest-lab

CORSI UTILI GRATUITI RIGUARDANTI CTF

- https://bitvijays.github.io/content.html
- http://howto.hackallthethings.com/2016/07/learning-exploitation-with-offensive.html
- https://www.hacker101.com/
- http://www.irongeek.com/i.php?page=videos/web-application-pen-testing-tutorials-with-mutillidae

CORSI A PAGAMENTO E CERTIFICAZIONI

- https://www.pentesteracademy.com/topics
- https://www.pentesterlab.com/exercises/
- https://www.offensive-security.com/
- https://cluster9.com/
- https://www.elearnsecurity.com/
- http://hackingdojo.com/courses/

ESEMPI DI WRITEUPS

- https://jbzteam.github.io/archive/
- https://teckk2.github.io/
- https://sploitfun.wordpress.com/
- https://neverendingsecurity.wordpress.com/2015/04/07/wiki-like-ctf-write-ups-repositories-maintained-by-the-community-2013-2014-and-2015/
- https://habr.com/en/company/pentestit/blog/303700/
- https://www.chrismaddalena.com/2016/07/vulnhub-violator-1-walkthrough/
- http://fuzyll.com/2016/the-defcon-ctf-vm/
- http://security.cs.pub.ro/hexcellents/wiki/
- https://cyb3rsick.com/category/oscp-exam-writups/?order=asc

RISORSE

- https://github.com/lucyoa/ctf-wiki
- https://github.com/apsdehal/awesome-ctf
- https://github.com/Hack-with-Github/Awesome-Hacking
- https://github.com/vitalysim/Awesome-Hacking-Resources/blob/master/README.md