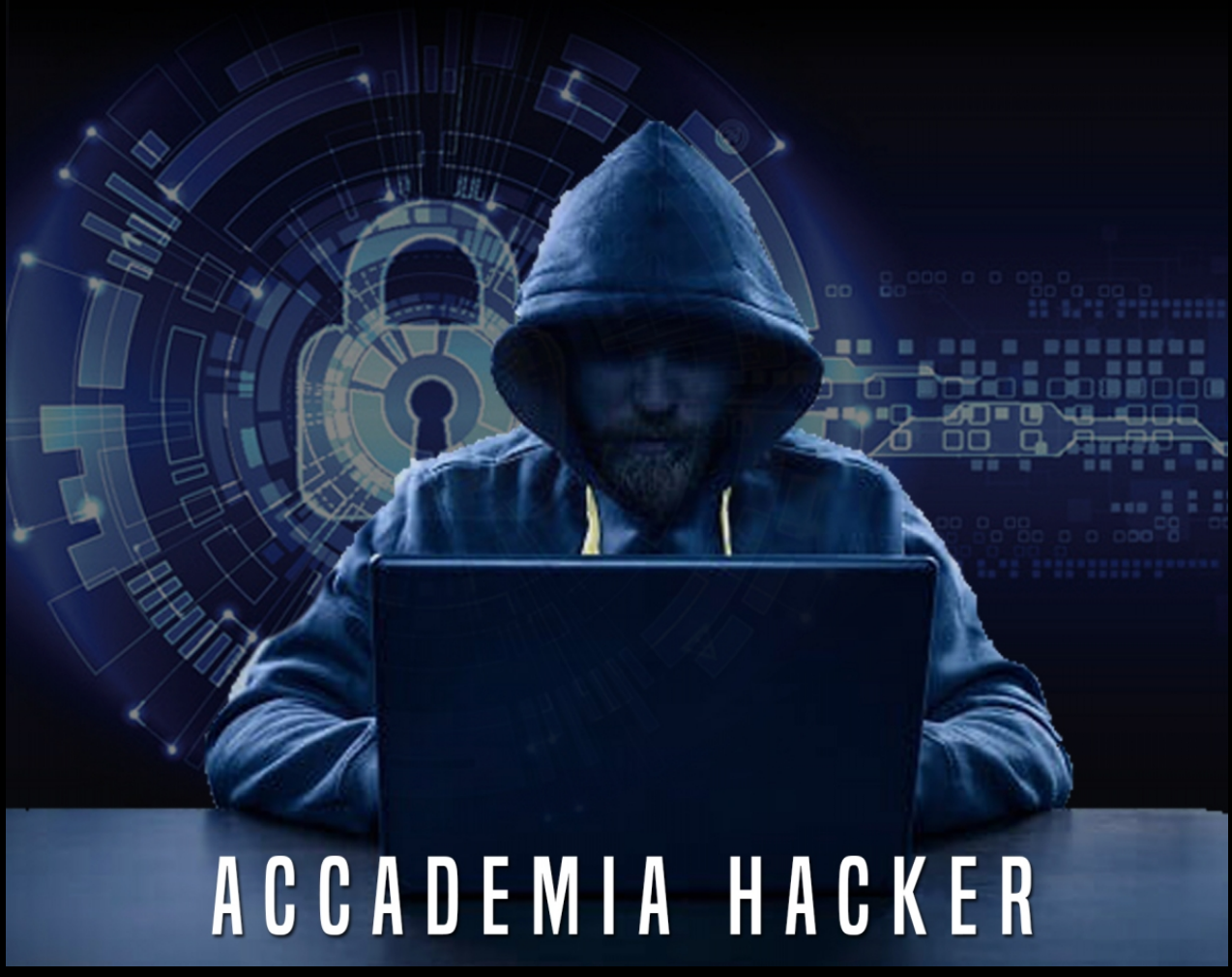
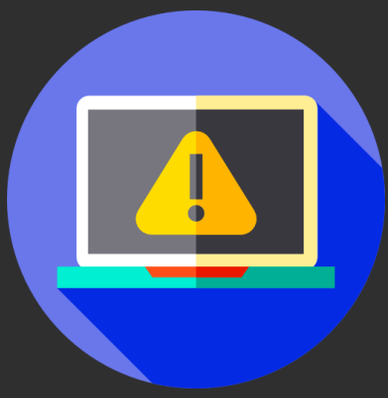
100 SEGRETI PER DIVENTARE UN HACKER

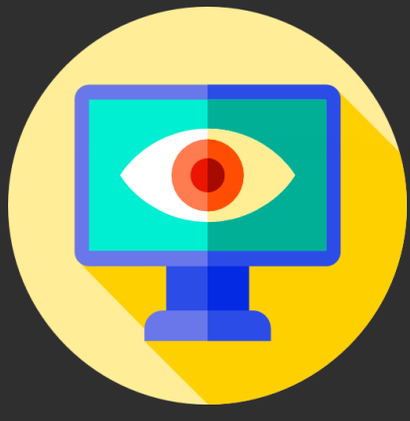
CONSIGLI, SUGGERIMENTI E RISORSE PER ETHICAL HACKER



ACCADEMIA HACKER



LA FORMAZIONE



ACCADEMIA HACKER

SEGRETO N° 1

Questa guida NON ti farà diventare un HACKER; è giusto tu lo sappia fin da subito. Il perchè non sto nemmeno a spiegartelo, è evidente e credo tu possa capirlo senza aggiungere altro.

Tuttavia se prenderai spunti da questi consigli e cercherai di applicarne alcuni, avrai delle OTTIME possibilità di poter iniziare a familiarizzare con la materia e quindi crescere professionalmente.

SEGRETO N°2

L'HACKING è il punto di arrivo di un percorso che comprende molti AMBITI e ABILITA' che è necessario possedere.

Brevemente possiamo affermare che l'HACKING o l'ETHICAL HACKING (dipende dal punto di vista in cui ci troviamo, ma per il resto non cambia assolutamente niente) è la risultante di un VIAGGIO FORMATIVO che si suddivide in:

1) RETI
2) SICUREZZA DIFENSIVA
3) SICUREZZA OFFENSIVA

L'ordine non è INVERTIBILE!

SEGRETO N°3

STUDIO DELLE RETI

Tutto parte da qui! Mi dispiace non c'è niente da fare: dovrai studiare le RETI INFORMATICHE. D'altronde come puoi pensare di PROTEGGERE/ATTACCARE una rete se non sai nemmeno cos'è un RETE. Ti pare?! Tranquillo...nel corso di questa guida ti fornirò degli ottimi suggerimenti!

SEGRETO N°4

Di seguito alcuni concetti fondamentali di RETE che dovrai conoscere BENE...

VLANs

DNS

INDIRIZZI IP PUBBLICI E PRIVATI

SUBNETTING

NAT

DHCP

SWITCH

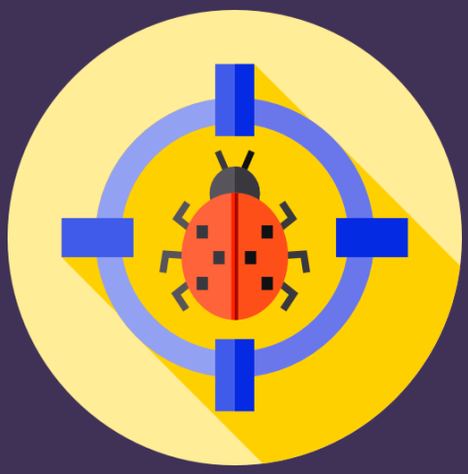
ROUTER

MODELLO ISO/OSI

INDIRIZZI MAC

ARP

TCP/IP



SEGRETO N°5

La conoscenza di un linguaggio di...

programmazione è fondamentale.
Sarebbe perfetto conoscerne uno a basso livello come il C e uno adatto alla scrittura di script come PYTHON.

Non è necessario leggersi manuali di migliaia di pagine: ci sono ottimi corsi online che ti daranno le basi per poter creare i tuoi primi script.

Ti suggerisco di dare un occhio alla piattaforma UDEMY.COM
https://www.udemy.com.
Troverai decine di corsi, anche in ITALIANO, a basso costo.

SEGRETO N° 6

Un vero HACKER non passa il tempo su sistemi operativi Windows.

Dovrai ASSOLUTAMENTE familiarizzare con un sistema operativo di tipo LINUX.

La distribuzione UBUNTU (https://www.ubuntu-it.org/download) per iniziare va benissimo: potrai sperimentare ed esercitarti senza alcun problema.

Nel corso della guida, vedremo poi le distribuzioni più adatte per un HACKER!

SEGRETO N°7

Ricorda sempre: MAI SPERIMENTARE tecniche HACKER in contesti reali.
Per questo motivo dovrai simulare tutti i tuoi attacchi in laboratorio.
Qui ci viene incontro una tecnologia informatica che risolve tantissimi problemi: LA VIRTUALIZZAZIONE.

Dai un occhio a questi due strumenti, sono entrambi ottimi...sperimenta!

ORACLE VIRTUALBOX:
(https://www.virtualbox.org/)

VMWARE PLAYER:
(https://my.vmware.com/web/vmware/free)

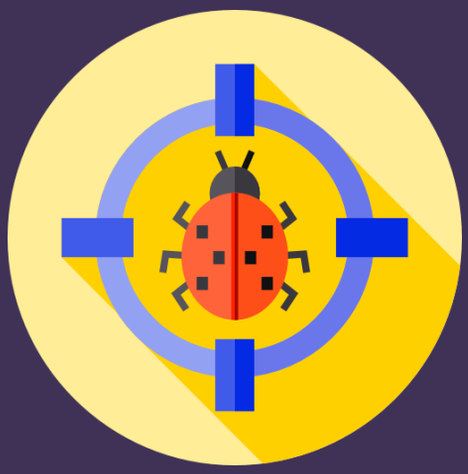
SEGRETO N°8

STUDIO DEI DATABASE

La maggior parte delle applicazioni web hanno necessità di memorizzare i dati da qualche parte.

I database sono lo strumento per la memorizzazione dei dati più diffuso. Ne esistono di vari tipi, tra cui quelli relazionali e quelli NON relazionali.

Inizia ad approfondire il linguaggio SQL: sarà un ottimo punto di partenza.



SEGRETO N°9

La conoscenza del protocollo HTTP...

e di quello HTTPS sono FONDAMENTALI.

Un hacker si trova spesso in contesti dove è necessario capire ed esaminare nel dettaglio il funzionamento di una WEB APPLICATION.

Ci sono molti strumenti che ti possono aiutare, tuttavia la prima cosa da fare è capire come funziona il protocollo HTTP e successivamente la versione sicura di quest'ultimo: HTTPS.

Su internet trovi moltissime guide e video che ti spiegano tutto nel dettaglio!

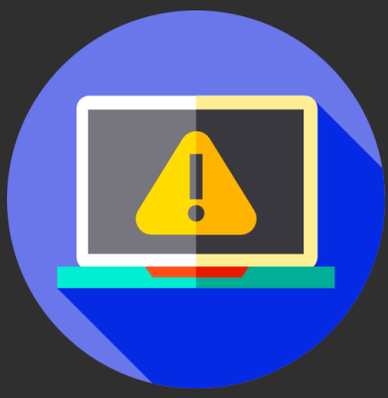
SEGRETO N° 10

Ci sono poi altre abilità meno tecniche che dovrai acquisire...

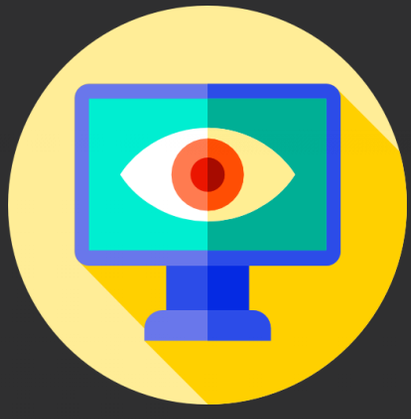
Dovrai sviluppare un'ottima capacità di PROBLEM SOLVING ovvero riuscire a trovare strade alternative quando un ostacolo si interpone tra te e il tuo obiettivo.

Dovrai poi abituarti a pensare in maniera "creativa" e cercare di percorrere strade non battute e soprattutto non visibili.

Infine dovrai essere PERSISTENTE ovvero non arrenderti al primo ostacolo che troverai lungo il tuo cammino.



LE CERTIFICAZIONI



ACCADEMIA HACKER

SEGRETO N° 11

Adesso che abbiamo introdotto alcuni aspetti legati alla formazione di un hacker, passiamo alle CERTIFICAZIONI.

Innanzitutto una premessa doverosa: le certificazioni possono dare un notevole valore aggiunto al tuo curriculum; tuttavia non possono sostituire l'esperienza acquisita in campo.

Le certificazioni utili per un aspirante hacker sono molteplici e te lo dico fin da subito: sono tutte in lingua INGLESE!

SEGRETO N°12

Innanzitutto ti consiglio di valutare l'ottenimento di una certificazione legata alle RETI INFORMATICHE: è un ottimo punto di partenza e ti fornisce delle solide basi.
In particolare te ne consiglio due:

1) Cisco CCNA Routing and Switching

(https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html#~stickynav=2)

2) CompTIA Network+

(https://certification.comptia.org/certifications/network)

La prima è orientata al vendor CISCO.
La seconda è invece NEUTRAL VENDOR cioè non legata ad un vendor specifico.

SEGRETO N°13

CERTIFICAZIONE CCNA

Per quanto riguarda questa certificazione ti consiglio di esercitarti molto oltre che studiare la teoria. Questi che ti suggerisco sono tre ottimi TOOL per simulare delle complesse architetture di rete:

1) Cisco Packet Tracer

(https://www.netacad.com/courses/packet-tracer)

2) GNS3

(https://www.gns3.com/)

3) BOSON

(https://www.boson.com/)

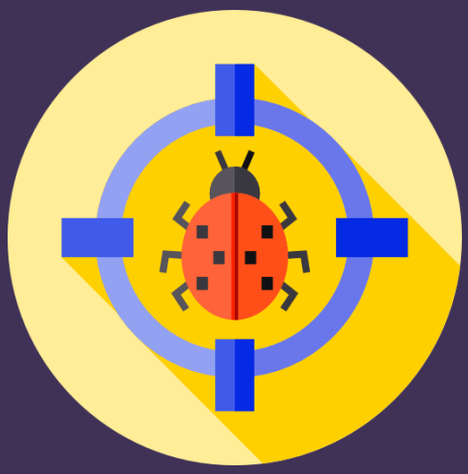
L'ultimo è a pagamento ma se non hai problemi di budget acquistalo...è davvero ottimo!

SEGRETO N°14

Adesso che hai arricchito il tuo curriculum con una certificazione sulle reti, passiamo alla SICUREZZA DIFENSIVA

Relativamente alle certificazioni in ambito SICUREZZA DIFENSIVA, abbiamo due opzioni. La prima è ottenere una certificazione legata ad un VENDOR SPECIFICO (Checkpoint, Sophos, McAfee, ecc) o ad una specifica tecnologia; la seconda è ottenere una certificazione generica come quelle rilasciate, ad esempio, dalla CompTia.
Sono entrambe valide soluzioni, dipende tutto dai nostri obiettivi professionali.





SEGRETO N°15

Le certificazioni generiche...

in ambito SICUREZZA DIFENSIVA sono molteplici e sono quasi tutte rivolte al ruolo di CYBERSECURITY ANALYST.

Ti consiglio di prendere in considerazione questi due percorsi di certificazione:

1) CompTIA (CySA+) Cybersecurity Analyst+
(https://certification.comptia.org/certifications/cybersecurity-analyst)

2) Cisco CCNA Cyber Ops
(https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-cyber-ops.html)

Se parti proprio da zero invece:

3) CompTIA Security+
(https://certification.comptia.org/certifications/security)

SEGRETO N° 16

Le certificazioni, sempre relative alla SICUREZZA DIFENSIVA, dipendono molto dallo specifico ambito in cui andremo ad operare.

Ogni vendor ha i suoi prodotti e quindi i suoi PERCORSI SPECIFICI DI CERTIFICAZIONE.

Se, ad esempio, andremo a lavorare con i FIREWALL di tipo CHECKPOINT, allora valuteremo di prendere la CERTIFICAZIONE CHECKPOINT legata a quello specifico prodotto.
Spesso sarà l'azienda stessa in cui lavoreremo a farcela conseguire.

SEGRETO N°17

E adesso passiamo alle certificazioni in ambito SICUREZZA OFFENSIVA.

Come già anticipato, ti consiglio prima di formarti bene nelle RETI e nella SICUREZZA DIFENSIVA.
Possiamo dividere queste certificazioni in due gruppi:

1) Quelle più teoriche, legate alla parte normativa, procedurale e manageriale.

2) Quelle più pratiche, legate soprattutto all'attività di PENETRATION TESTING e alla metodologia connessa.

SEGRETO N°18

CERTIFICAZIONE CEH

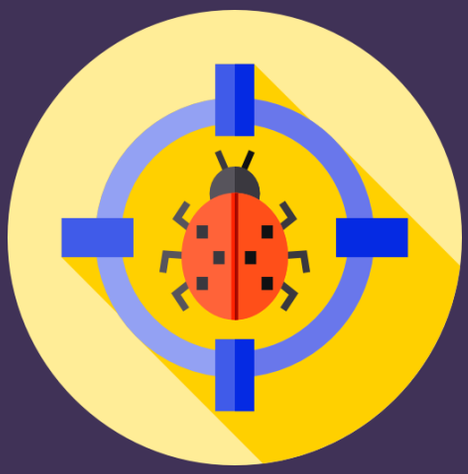
La Certified Ethical Hacker (CEH) è una delle certificazioni più conosciute in ambito internazionale.

E' teorica e l'esame consiste in delle domande a scelta multipla.

E' necessario avere una conoscenza orizzontale e teorica della SICUREZZA OFFENSIVA.

E' un buon punto di partenza anche se non si sofferma troppo negli aspetti più tecnici.

Questo il sito per avere informazioni: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/



SEGRETO N°19

La certificazione CISSP

Quest'ultima (Certified Information Systems Security Professional) è una certificazione avanzata e molto teorica, adatta soprattutto a chi vuole intraprendere una carriera nella sicurezza informatica; carriera maggiormente rivolta agli aspetti più manageriali e meno tecnici o pratici.

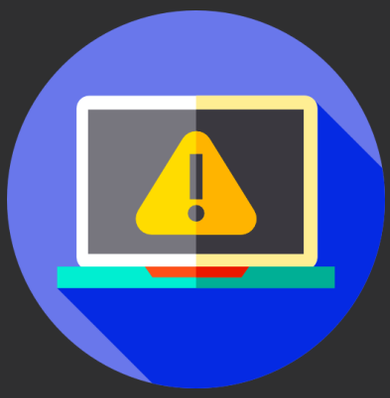
Viene data molta importanza a tutte le normative e alle procedure relativamente a svariati contesti di sicurezza.
Tuttavia non la consiglio come prima certificazione.
Questo il sito a cui fare **riferimento:** https://www.isc2.org/Certifications/CISSP.

SEGRETO N°20

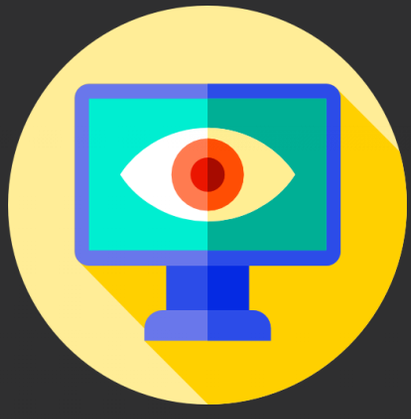
Terminiamo con una certificazione invece molto tecnica e pratica...

Se sei interessato ad applicare nella pratica le tecniche di ATTACCO di una rete o ad eseguire un PENETRATION TESTING, allora ti suggerisco caldamente di considerare la certificazione OSCP (Offensive Security Certified Professional).
E' una certificazione esclusivamente pratica e l'esame, che dura 24 ore, consiste in un laboratorio dove lo scopo è effettuare un PENETRATION TEST completo.
Preparati a studiare moltissimo e a passare notti in bianco!





MANUALI E/O GUIDE



ACCADEMIA HACKER

SEGRETO N° 21

Esistono moltissime risorse di vario genere in Internet, tuttavia la completezza che può dare un libro è spesso difficile da trovare altrove.

Per cui, di seguito, alcuni dei libri a mio avviso migliori per iniziare ad intraprendere una carriera nel mondo delle RETI e della SICUREZZA INFORMATICA.

Alcuni di questi non sono aggiornatissimi, tuttavia considera che i concetti di base sono esattamente gli stessi.

SEGRETO N°22

Il primo libro che ti voglio suggerire è legato alle RETI. Come sempre preferisco partire da quest'ultime e poi andare verso la sicurezza e l'ethical hacking.

Il libro si intitola "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference".

E' stato pubblicato nel 2004, tuttavia i concetti di rete sono espressi in modo chiaro ed esaustivo.

Ti consiglio di valutare l'acquisto. Puoi trovarlo usato anche sul sito https://www.abebooks.it/.

SEGRETO N°23

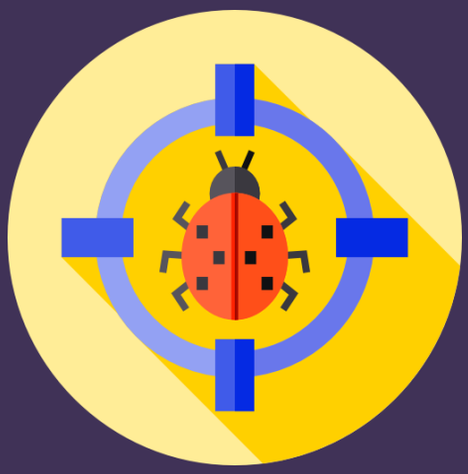
HOW TO MASTER CCNA

Questo manuale è legato nello specifico all'ottenimento della certificazione CCNA, tuttavia sono illustrati i principali concetti delle reti in modo SEMPLICE ed IMMEDIATO.

La prima pubblicazione risale al 2013.

Il titolo esatto è: "How to Master CCNA" di René Molenaar.

E' ovviamente in lingua inglese, come tutti i libri che ti suggerirò: purtroppo in lingua italiana, al momento, non è presente niente di valido o efficace.



SEGRETO N°24

Non ti basta conoscere le reti...

...nella teoria ma è ovviamente necessario avere consapevolezza di come FISICAMENTE i pacchetti si muovono all'interno di una rete.

Per questo motivo sarà necessario prendere confidenza con uno SNIFFER DI RETE; il più noto è senza dubbio WIRESHARK (https://www.wireshark.org/).

Al seguente link puoi trovare una serie di libri, tutti ottimi e completi, dedicati a questo strumento: https://www.wiresharkbook.com/

SEGRETO N°25

Adesso che hai ottenuto un'ottima conoscenza delle reti grazie ai libri che ti ho suggerito, passiamo alla SECURITY!

Sono presenti moltissimi volumi legati alla SICUREZZA DIFENSIVA, tuttavia molti di questi sono orientati alle normative e agli aspetti più teorici, soprattutto legati al mercato americano.

Un buon compromesso è il libro "Network Security Assessment: Know Your Network" di Chris McNab.

E' molto pratico e ti mostra come eseguire un SECURITY ASSESSMENT di una RETE.



SEGRETO N° 26

Passiamo adesso ai libri orientati alla SICUREZZA OFFENSIVA e al PENETRATION TESTING.

Il primo che ti consiglio è: "Penetration Testing: A Hands-On Introduction to Hacking" di Weidman Georgia.

E' un volume che ti consiglio ASSOLUTAMENTE di leggere.

Analizza ogni aspetto del penetration testing fornendone una buona infarinatura di base.

Per iniziare è ottimo!

SEGRETO N°27

Altro manuale, sempre molto pratico che ti consiglio è "The Hacker Playbook" di Peter Kim.

Sono tre volumi e ti consiglio di leggerli tutti.

Viene data molta importanza all'analisi delle WEB APPLICATION e viene mostrato l'utilizzo dei TOOL in modo molto approfondito.

Se preferisci puoi leggerli anche in versione digitale, in formato .pdf.

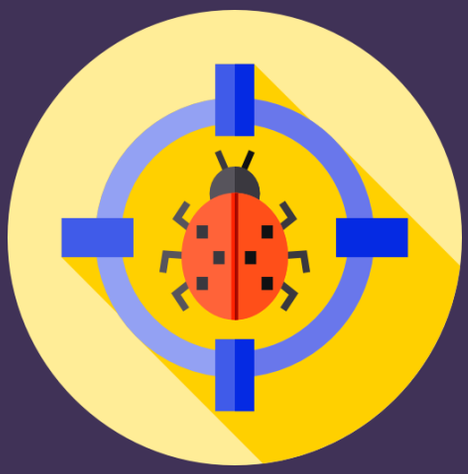
SEGRETO N°28

NMAP NETWORK SCANNING

L'anno di pubblicazione di questo libro è il 2009, tuttavia è un punto di riferimento per quanto riguarda l'utilizzo di NMAP, il famoso tool di scansione di una rete.

Il titolo è "NMap Network Scanning: Official NMap Project Guide to Network Discovery and Security Scanning" di Gordon Lyon.

Si sofferma nel dettaglio spiegando molteplici tecniche di scansione della rete utilizzando appunto NMAP.



SEGRETO N°29

Se vogliamo addentrarci nel...

...mondo delle WEB APPLICATION e di come si effettua un TEST DI SICUREZZA su quest'ultime, allora è indispensabile la lettura di questi due manuali:

1) The Web Application Hacker's Handbook di Dafydd Stuttard.

2) The Browser Hacker's Handbook di Wade Alcorn.

Non è una lettura facile o scorrevole, ma se riuscirai ad arrivare in fondo, la tua conoscenza delle WEB APPLICATION sarà invidiabile!

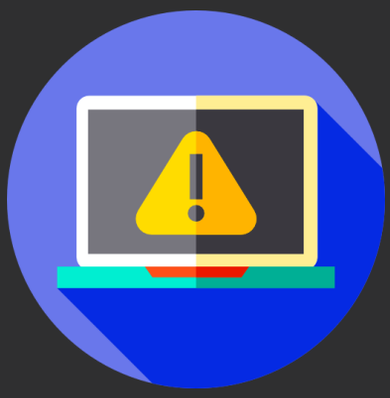
SEGRETO N°30

Terminiamo adesso questa parte legata ai libri e manuali

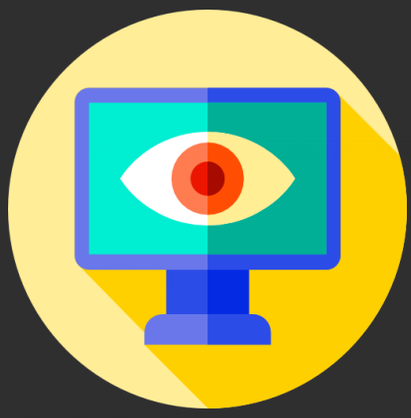
Questi che ti ho suggerito, sono solo alcuni dei volumi che si possono trovare, l'elenco non è assolutamente esaustivo, per cui ti suggerisco di cercare per conto tuo altri libri o manuali.

Nota che soprattutto su Amazon si trovano moltissimi volumi scritti da semplici appassionati, magari sconosciuti ai più.
Ti consiglio di dare un occhio anche a quelli, spesso contengono informazioni davvero utili!





CANALI YOUTUBE E/O VIDEO



ACCADEMIA HACKER

SEGRETO N° 31

Partiamo con il canale Youtube "Hak5".

LINK: https://www.youtube.com/user/Hak5Darren/videos

Questo canale è nato nel 2005 ed è formato da un gruppo di esperti in sicurezza e gamers.

E' un canale legato alla sicurezza informatica e all'ethical hacking; lo stile è molto divulgativo e divertente, i video sono tutti compresi tra 10 e 20 minuti.

SEGRETO N°32

Sempre sullo stesso stile, abbiamo il canale Youtube "JackkTutorials".

LINK: https://www.youtube.com/user/JackkTutorials/videos

Aperto nel 2011, è orientato all'intrattenimento piuttosto che al rigore accademico.

Gli argomenti spaziano dalla programmazione alle CTF (Capture The Flag) fino ad arrivare all'hardware hacking.

Ti consiglio di farci un giro!

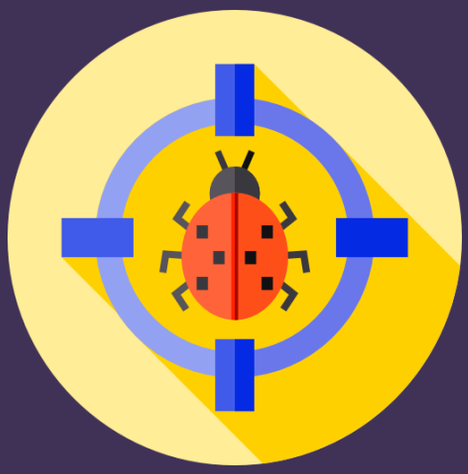
SEGRETO N°33

PENETRATION TESTING

Questo canale Youtube, dal nome "Penetration Testing" fornisce dei tutorial molto tecnici e specifici sull'utilizzo dei TOOL che ci permettono di effettuare un penetration testing.

LINK: https://www.youtube.com/channel/UCEIOXb213JZK61VNZnJ_RyA/featured

E' un canale molto più tecnico e specializzato rispetto ai precedenti.



SEGRETO N°34

Questo è un canale differente...

...dagli altri, infatti qui vengono mostrate tutte quelle tecniche MALEVOLE che un ETHICAL HACKER non dovrebbe MAI attuare.

Tuttavia per completezza e a solo scopo educativo ve lo segnalo.

Il nome del canale è: "Mr Unethical".
Il link è il seguente: https://www.youtube.com/channel/UCjT2SQBfqtPMdX99mf4ZsMg/videos

SEGRETO N°35

Adesso passiamo a qualche canale Youtube italiano...in effetti non sono molti!

Il canale che ti propongo si chiama "rev3rse security".

LINK: https://www.youtube.com/channel/UCzvJStjySZVvOBsPI-Vgj0g

E' un canale relativamente giovane, ma tuttavia si possono già trovare moltissimi video tutorial legati al penetration testing e a sfide di tipo CTF.
Ottimo soprattutto perchè è in lingua ITALIANA.



SEGRETO N° 36

Ti segnalo adesso, sempre su Youtube, questo corso completo sull'ETHICAL HACKING e PENETRATION TESTING.

E' una compilation di 106 video IN INGLESE e vengono percorse tutte le fasi di un PENETRATION TESTING.

LINK: https://www.youtube.com/playlist?list=PLBf0hzazHTGOEuhPQSnq-Ej8jRyXxfYvl

Il nome del canale è: "HackerSploit".

SEGRETO N°37

Ti suggerisco adesso un intero corso, sempre in INGLESE, della durata di 10 ore caricato su Youtube da Jerry Banfield sul suo canale Youtube: https://www.youtube.com/watch?v=OcVE6rQ9_FU.

Considera che è un solo UNICO video della durata di 10 ore!

Si parte dall'installazione di KALI LINUX fino ad eseguire un test di sicurezza su una WEB APPLICATION.

SEGRETO N°38

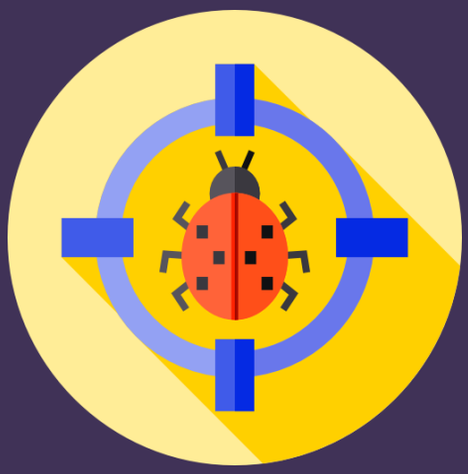
CANALE YOUTUBE INFORGE.NET

Questo è un canale Youtube italiano abbastanza variegato nei contenuti.

Tuttavia ci sono delle playlist di video legate all'hacking e nello specifico all'anonimato.

Dal momento che è in italiano potrebbe essere piacevole anche per chi conosce meno la lingua inglese.

Il nome è "inforge.net" e il link: https://www.youtube.com/user/InforgeTV/videos



SEGRETO N°39

Un sito assolutamente utile è...

...SECURITY TUBE che contiene decine di video legati alla SICUREZZA INFORMATICA e all'ETHICAL HACKING.

Si tratta di un sito web specifico e non di una canale Youtube.

Il link è il seguente: http://www.securitytube.net/

Tuittavia abbiamo la possibilità di accedere ai video passando dal canale Youtube "Pentester Academy TV": https://www.youtube.com/channel/UChjC1q6Ami7W0E71TzPZELA

SEGRETO N°40

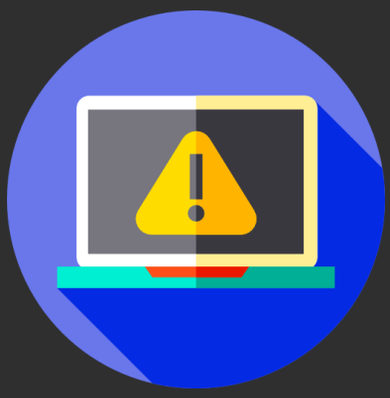
Terminiamo adesso questa parte legata alle risorse video

Questi che ti ho presentato sono a mio avviso i canale Youtube più utili.

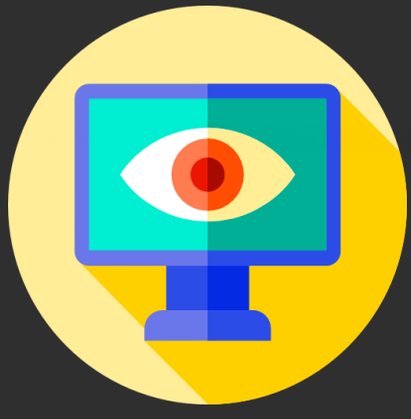
Tuttavia considera che ogni giorno ne nascono di nuovi, per cui è molto difficile stare dietro a tutti e restare sempre aggiornati.

Oltre al fatto che spesso conviene ricercare, all'interno di Youtube, direttamente l'argomento d'interesse senza passare prima da un canale specifico.





SECURITY/HACKING BLOG



ACCADEMIA HACKER

SEGRETO N° 41

Che tu sia un ethical hacker oppure un esperto in sicurezza, è assolutamente necessario restare AGGIORNATI sulle ultime notizie di questo settore, vista soprattutto la frequenza e rapidità con cui gli eventi si susseguono.

Per questo motivo, adesso ti propongo una lista di BLOG che ti consiglio di salvare nei tuoi preferiti, così da poterli consultare giornalmente o meglio ancora più volte al giorno.

SEGRETO N°42

Partiamo con il sito "https://latesthackingnews.com/".

Quest'ultimo fornisce, quasi GIORNALMENTE, aggiornamenti legati al mondo della sicurezza informatica e dell'ethical hacking.

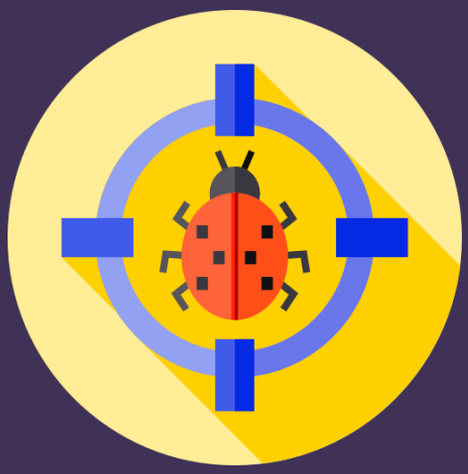
Gli autori sono un team di esperti in sicurezza, ognuno specializzato nel proprio settore.

Gli articoli hanno un taglio molto breve e divulgativo.
Si leggono quindi con facilità.

SEGRETO N°43

WELIVE SECURITY

Questo sito (https://www.welivesecurity.com/) è curato dalla "ESET SECURITY COMMUNITY".
Quest'ultima è formata da un team di altissimo livello di ricercatori ed esperti in sicurezza.
E' adatto a semplici appassionati ma anche, e forse soprattutto, agli addetti ai lavori.
Ogni settimana viene inserito un editoriale approfondito e di ottimo valore tecnico.



SEGRETO N°44

Altro blog aggiornato e completo...

Il nome è HackerOne (https://www.hackerone.com/blog).

Sono articoli principalmente divulgativi e non si perdono dietro a troppi tecnicismi.

Il blog è aggiornato con regolarità e gli articoli sono aggiunti di frequente.

Viene data molta importanza al tema della privacy, della sicurezza e protezione dei dati.
Uno dei loro obiettivi è rendere Internet un ambiente più sicuro.

SEGRETO N°45

Il sito che ti presento adesso è molto di più di un BLOG...

Il nome è Hakin9 (https://hakin9.org/blog/).

Infatti, oltre ad essere un BLOG, con tematiche orientate all'Ethical Hacking e al Penetration Testing, è anche una piattaforma che offre CORSI ONLINE, una RIVISTA mensile (cartacea e digitale) e uno SHOP dove poter acquistare vario MATERIALE INFORMATIVO.
Il tutto è di ottimo livello tecnico.



SEGRETO N° 46

E adesso passiamo al panorama italiano!

Innanzitutto un ottimo blog che non raccoglie solo notizie di sicurezza informatica, ma che tuttavia mi sento di consigliarti vista l'ottima qualità degli articoli.
Il nome è Zeusnews (https://www.zeusnews.it/).

Gli articoli vengono aggiunti più volte al giorno.

Le tematiche trattate riguardano l'informatica a 360 gradi.

SEGRETO N°47

Esaminiamo adesso un BLOG, sempre italiano, con un taglio nettamente più tecnico e orientato verso il CODICE.

Il suo nome è appunto CODICE INSICURO (https://codiceinsicuro.it/).

Ti consiglio ASSOLUTAMENTE la lettura di questi articoli: la notevole esperienza del suo autore non può che portarti un valore aggiunto e spunti interessanti.

Gli articoli sono aggiunti a cadenza settimanale.

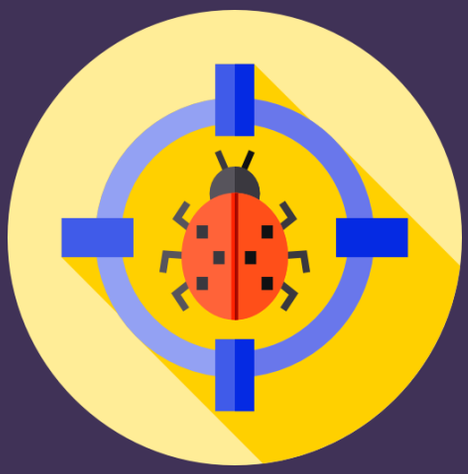
SEGRETO N°48

IL BLOG DI ANONYMOUS ITALIA

Riaperto da poco tempo, non ha bisogno di molte presentazioni.
LINK: https://anon-italy.blogspot.com/

Vengono mostrate le attività svolte dal gruppo ANONYMOUS e poi sono trattati argomenti "delicati" che richiedono attenzione ma che molto spesso non sono menzionati dagli altri media.

Per incrementare la tua cultura sul tema è importante che tu sia allineato anche su questi aspetti.



SEGRETO N°49

Altra fonte di informazioni è il forum...

...di INFORGE.NET.
(https://www.inforge.net/forum/).

Quest'ultima è una community molto attiva, composta perlopiù da semplici appassionati alla materia, molti di questi giovanissimi.

L'argomento trattato per la maggiore è l'hacking, in tutte le sue forme, dall'utilizzo dei tool alle tecniche più particolari.

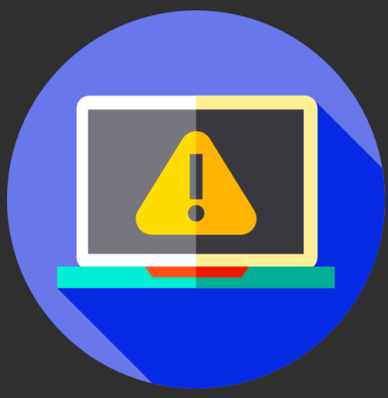
E' possibile anche scaricare del materiale, come guide e tutorial.

SEGRETO N°50

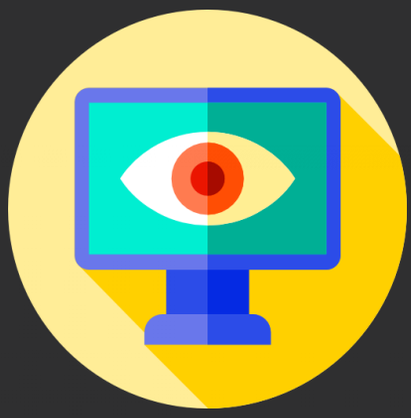
Terminiamo adesso questa presentazione dei SITI/BLOG più noti

Tieni conto che chiunque abbia intenzione di approcciarsi al mondo della sicurezza informatica, deve necessariamente rimanere aggiornato e questo non significa SOLO tecnicamente ma anche su eventi e notizie che avvengono nel panorama internazionale (e nazionale) della cybersecurity.





GLI STRUMENTI



ACCADEMIA HACKER

SEGRETO N° 51

Adesso ti mostrerò alcuni degli strumenti più utili per la tua attività di HACKING!

Partiamo con NMAP (https://nmap.org/).
Questo strumento open source ti permette di effettuare una scansione della rete completa, tra cui:

1) Identificare le porte aperte in un host.
2) Effettuare il MAPPING di una rete e la successiva ENUMERATION.
3) Identificare il SISTEMA OPERATIVO relativo ad un host.

SEGRETO N°52

WIRESHARK (https://www.wireshark.org/) è uno strumento che devi necessariamente conoscere ed utilizzare almeno nelle sue funzionalità di base.

L'analisi di un pacchetto di rete è fondamentale perchè ti permette di comprendere, nel dettaglio, il funzionamento di un'architettura di rete e di effettuare attività di troubleshooting su quest'ultima.

NOTA: il tool di simulazione GNS3 (https://www.gns3.com/) ha già Wireshark integrato!

SEGRETO N°53

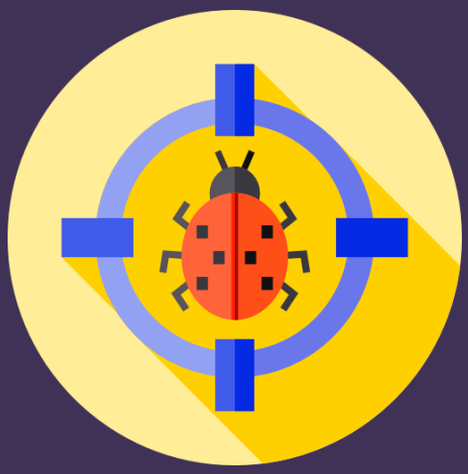
JOHN THE RIPPER

E' lo strumento più popolare per effettuare il "cracking" di password.

Permette di testare la ROBUSTEZZA di quest'ultime.

Automaticamente riesce a identificare l'ALGORITMO di cifratura utilizzato e a modificare quindi DINAMICAMENTE la metodologia di attacco da utilizzare.

LINK: https://www.openwall.com/john/



SEGRETO N°54

Introduciamo adesso METASPLOIT...

...uno degli strumenti più noti ed utilizzato dagli HACKER.
E' una piattaforma completa che offre una miriade di funzionalità e il cui obiettivo primario è di effettuare l'EXPLOITATION e la POST-EXPLOITATION di un sistema.

Sono presenti più versioni tra cui una FREE denominata COMMUNITY EDITION.

E' necessario prendersi del tempo per comprendere appieno questo strumento.
LINK: https://www.metasploit.com/

SEGRETO N°55

La ricerca delle VULNERABILITA' è un aspetto da non sottovalutare per un HACKER...

OpenVAS è appunto uno SCANNER DI VULNERABILITA' che ci permette, in automatico, di effettuare una scansione relativamente ad un certo host con lo scopo di evidenziarne tutte le possibili vulnerabilità o rischi di sicurezza.

E' open source (anche se è presente una versione commerciale) e si può utilizzare tramite un'interfaccia grafica; all'occorrenza anche da riga di comando.

LINK: http://www.openvas.org/



SEGRETO N° 56

Soffermiamoci adesso sulla parte delle WEB APPLICATION e introduciamo SQLMap (http://sqlmap.org/).

Questo strumento automatizza la ricerca di vulnerabilità di tipo SQL Injection.

Ha un motore di ricerca molto potente ed è costantemente aggiornato.
Alcuni dei database supportati sono: MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2.

SEGRETO N°57

Maltego (https://www.paterva.com/web7/downloads.php) è un tool che si occupa di raccogliere informazioni, utilizzando dati che sono pubblicamente accessibili e di raggrupparli poi in un formato grafico.

Inutile ribadire l'importanza di uno strumento simile nella fase di RACCOLTA DELLE INFORMAZIONI, relativamente all'attività di PENETRATION TESTING.

Per utilizzare lo strumento è necessario registrarsi al sito web indicato sopra.

SEGRETO N°58

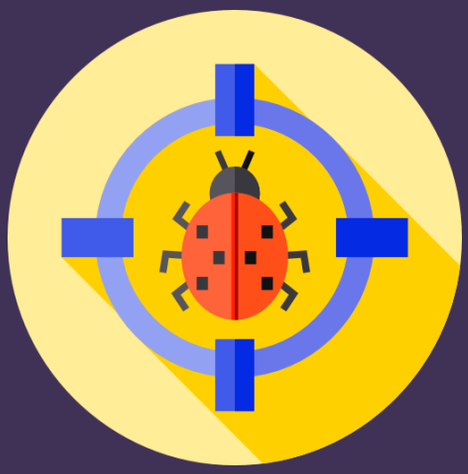
AIRCRACK-NG

Le reti WIFI rivestono attualmente una notevole importanza nell'ambito delle RETI e della SICUREZZA INFORMATICA.

Questo strumento ci permette di testare la loro ROBUSTEZZA catturando specifici PACCHETTI ed analizzandoli di conseguenza.

Aircrack-ng contiene al suo interno tutta una serie di tool e altri strumenti necessari durante le varie fasi del testing.

LINK: https://www.aircrack-ng.org/



SEGRETO N°59

Importante l'analisi delle reti locali...

Ettercap appartiene alla categorie dei "packet sniffer" e permette di effettuare attacchi di tipo MAN_IN_THE_MIDDLE.

Interponendosi nel mezzo, riesce infatti ad analizzare i pacchetti di rete che fluiscono, identificandone eventuali DEBOLEZZE o VULNERABILITA'.

LINK: https://www.ettercap-project.org/.

SEGRETO N°60

Introduciamo adesso NESSUS, altro scanner di vulnerabilità.

Quando dobbiamo effettuare un VULNERABILITY ASSESSMENT non si può NON parlare di NESSUS. (https://www.tenable.com/downloads/nessus).

E' uno dei tool più conosciuti ed utilizzati per questo scopo.

Il livello di accuratezza raggiunto nelle scansioni è ottimo. Viene automaticamente generato un report finale.



SEGRETO N° 61

Gli attacchi di INGEGNERIA SOCIALE restano un vettore molto diffuso.

Per realizzarli ci viene in aiuto lo strumento "Social-Engineer Toolkit" (https://www.trustedsec.com/social-engineer-toolkit-set/).

Permette di simulare attacchi di vario tipo, pensa ad esempio al PHISHING.
La generazione delle MAIL o delle PAGINE WEB MALEVOLE avviene completamente in automatico.

SEGRETO N°62

W3AF è un WEB APPLICATION SCANNER. (http://w3af.org/).

Il suo scopo è di supportarci nel proteggere al meglio le WEB APPLICATION identificando le vulnerabilità e aiutandoci successivamente a porre rimedio.

Lo strumento riesce ad effettuare la ricerca di oltre 200 vulnerabilità.

Si può utilizzare sia da interfaccia grafica che da linea di comando.

SEGRETO N°63

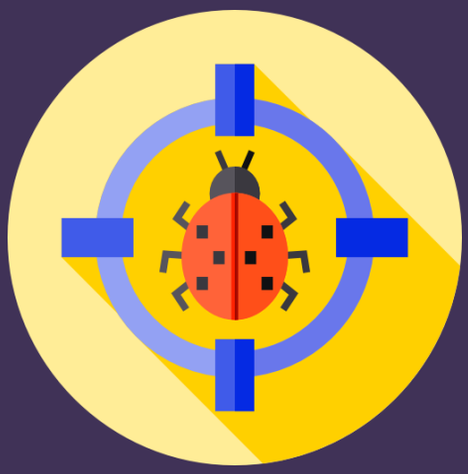
BURP SUITE

Questo è uno strumento che dovrai padroneggiare nel dettaglio se vuoi diventare un HACKER.

Si interpone nel mezzo tra CLIENT e SERVER (funzione PROXY) e ti permette quindi di analizzare il traffico HTTP/HTTPS tra quest'ultimi.

Lo scopo è di eseguire un test di sicurezza, in parte MANUALE e in parte AUTOMATICO, di una WEB APPLICATION.

LINK: https://portswigger.net/burp/communitydownload



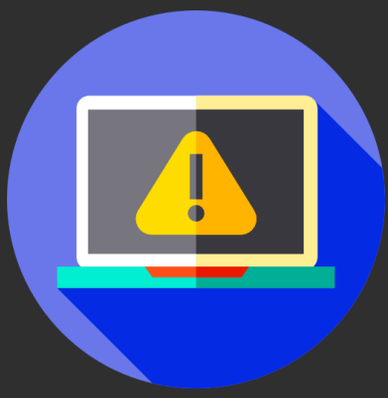
SEGRETO N°64

Angry IP Scanner...

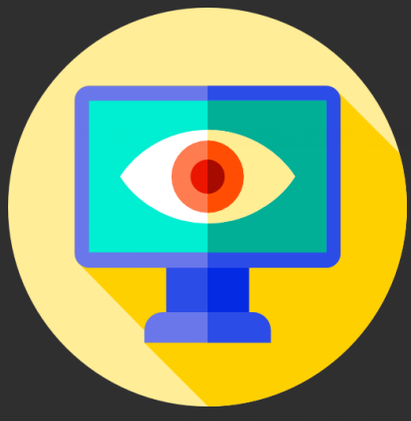
...un ottimo tool, leggero e performante, permette di effettuare la scansione di una rete allo scopo di rilevarne eventuali PORTE APERTE.

Possiamo immaginarlo come la versione più semplice ed essenziale di NMAP, tool che abbiamo già presentato.

Può effettuare la scansione delle reti LOCALI e di quelle REMOTE.
I risultati sono esportabili in più FORMATI.
LINK: https://angryip.org/download/#windows



SISTEMI OPERATIVI PER HACKER



ACCADEMIA HACKER

SEGRETO N° 66

La tipologia di SISTEMA OPERATIVO più indicata per un aspirante HACKER è senza dubbio LINUX.

Esistono svariate distribuzioni orientate alla sicurezza.

La più famosa e diffusa è senza dubbio KALI LINUX.

Basata su DEBIAN contiene oltre 500 tool per effettuare qualsiasi attività legata alla sicurezza informatica e all'hacking.

Ti suggerisco caldamente di utilizzarla!
LINK: https://www.kali.org/

SEGRETO N°67

Altra ottima distribuzione, meno diffusa rispetto a Kali Linux è PARROT SECURITY OS.
LINK: https://www.parrotsec.org/.

E' sviluppata e mantenuta da un team italiano.

I suoi punti di forza sono la PERSONALIZZAZIONE del sistema molto spinta e di ottime performance.

Oltre al fatto che è presente una community molto attiva pronta ad aiutarti in caso di difficoltà.

SEGRETO N°68

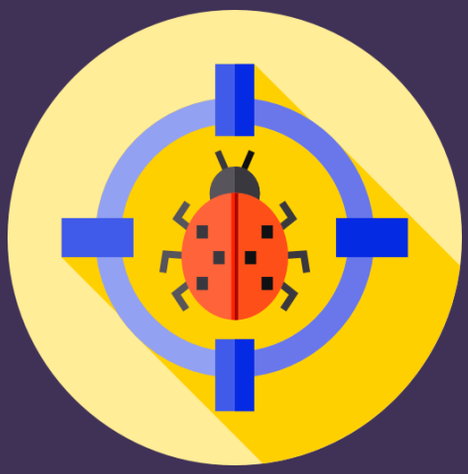
BACKBOX

Questa distribuzione è basata sulla distribuzione UBUNTU.

Contiene centinaia di tool che possono essere usati per attività di analisi sulle web application, scansioni della rete, ecc.

Comprende un ambiente DESKTOP ed è regolarmente aggiornata e mantenuta.

LINK:
https://www.backbox.org/



SEGRETO N°69

Altre distribuzioni che...

...ti invito a testare sono le seguenti:

1) Samurai Web Testing Framework - http://www.samurai-wtf.org/
2) Pentoo Linux - https://www.pentoo.ch/
3) DEFT Linux - http://www.deftlinux.net/
4) Caine - https://www.caine-live.net/
5) Network Security Toolkit (NST) - https://sourceforge.net/projects/nst/
6) BlackArch Linux - https://blackarch.org/
7) Bugtraq - http://bugtraq-team.com/

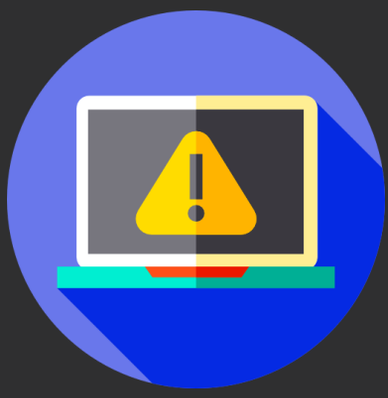
SEGRETO N°70

Crea il tuo laboratorio personale utilizzando le MACCHINE VIRTUALI.

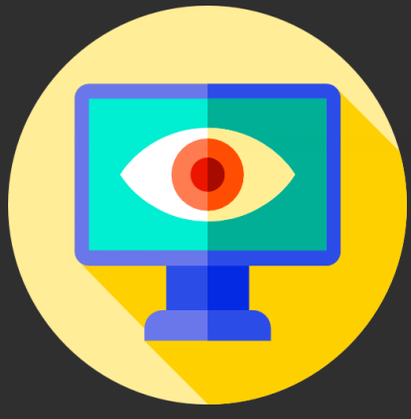
Un buon punto di partenza è installare e testare queste distribuzioni di sicurezza utilizzando la VIRTUALIZZAZIONE e le MACCHINE VIRTUALI così potrai fare test in un ambiente protetto e senza arrecare danni a nessuno.

Per iniziare potresti creare un laboratorio formato da due macchine virtuali: un ATTACCANTE (KALI LINUX ad esempio) e una VITTIMA (Windows 7 ad esempio).





WEB APPLICATION VULNERABILI



ACCADEMIA HACKER

SEGRETO N° 71

Come già anticipato è di fondamentale importanza la PRATICA: non basta conoscere i concetti TEORICI ma è necessario aver sperimentato in prima persona e lo ripeto nuovamente: SEMPRE IN LABORATORIO.

A tale scopo ci vengono in aiuto le cosiddette "VULNERABLE WEB APP", delle web application in cui sono state VOLUTAMENTE lasciate delle vulnerabilità o criticità legate alla sicurezza.

SEGRETO N°72

Partiamo con BWAPP (http://www.itsecgames.com/).

E' una web application che contiene al suo interno più di 100 vulnerabilità di vario tipo, come Cross Site Scripting (XSS) o SQL Injection.

BWAPP utilizza il linguaggio PHP e come database MySQL.

Può essere ospitata su web server di tipo Apache o IIS.

Tra l'altro sono presenti anche alcuni tutorial.

SEGRETO N°73

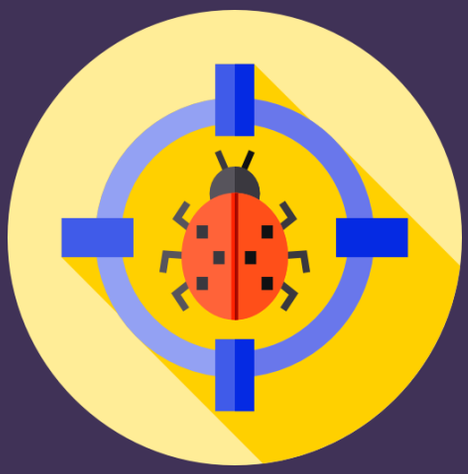
GOOGLE GRUYERE

Simpatica web application realizzata da Bruce Leban, Mugdha Bendre e Parisa Tabriz.

Oltre a permetterci di esercitarci, questa app si focalizza anche su come poter prevenire le varie vulnerabilità.

Alcuni degli attacchi presenti sono Cross Site Scripting (XSS) e Cross-Site Request Forgery (XSRF).

LINK: http://google-gruyere.appspot.com/



SEGRETO N°74

OWASP Mutillidae II

Sono presenti oltre 40 vulnerabilità tra cui quelle contenute nella OWASP Top Ten 2007, 2010, 2013 e 2017.

Può essere installata sia su Linux che Windows.
E' già preinstallata su alcune distribuzioni di sicurezza come Samurai Web Testing Framework (WTF).

Un punto a favore di quest'ultima è che viene aggiornata di frequente.
LINK: https://github.com/webpwnized/mutillidae

SEGRETO N°75

http://testphp.vulnweb.com/

Uno dei punti di forza di questa web application è la possibilità di essere raggiunta direttamente da Internet.

Non è quindi necessario effettuare alcuna installazione: possiamo effettuare tutti i test di sicurezza direttamente su quest'ultima.

La web app è messa a disposizione da ACUNETIX produttore di un famoso scanner di vulnerabilità: https://www.acunetix.com/.



SEGRETO N° 76

Peruggia è un'altra web application vulnerabile con cui puoi esercitarti.

E' realizzata in PHP e MySQL, ormai è leggermente datata vista che l'ultimo aggiornamento risale al 2009 tuttavia per alcune esercitazioni di base è ancora utile.

Questo il sito web da dove possiamo scaricarla:

https://sourceforge.net/projects/peruggia/

SEGRETO N°77

Tutte queste web app analizzate finora si possono installare singolarmente.

Un'alternativa che vi consiglio è di scaricare "OWASP Broken Web Applications".
Quest'ultima è una macchina virtuale che riunisce tutte insieme le web app presentate, oltre a moltissime altre.

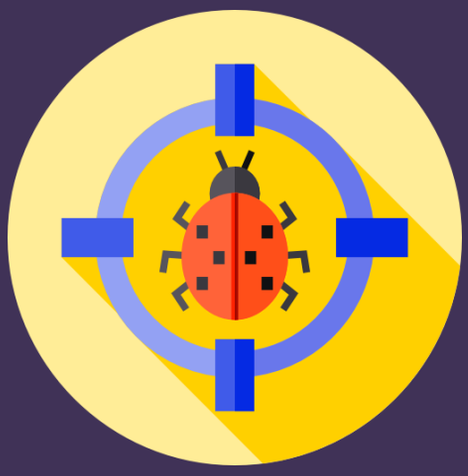
Questo il link del progetto dove possiamo scaricare la macchina virtuale:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

SEGRETO N°78

OWASP TOP 10

L'organizzazione OWASP, tra i vari compiti, si occupa di stilare una lista dettagliata delle 10 vulnerabilità più pericolose che colpiscono le web application.
Molte di queste sono simulate nelle applicazioni mostrate in precedenza.

Ti consiglio di leggere e studiare con attenzione questa classifica, oltre a tutte la varie risorse gratuite messe a disposizione sempre da OWASP.
Di seguito il link alla TOP 10 2017 che è l'ultima attualmente disponibile:
https://www.owasp.org/index.php/Top_10-2017_Top_10



SEGRETO N°79

Ecco la lista TOP 10 2017...

1) Injection
2) Broken Authentication
3) Sensitive Data Exposure
4) XML External Entities (XXE)
5) -Broken Access Control
6) Security Misconfiguration
7) -Cross-Site Scripting (XSS)
8) Insecure Deserialization
9) -Using Components with Known Vulnerabilities
10) -Insufficient Logging&Monitoring

Puoi scaricare il PDF direttamente da: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

SEGRETO N°80

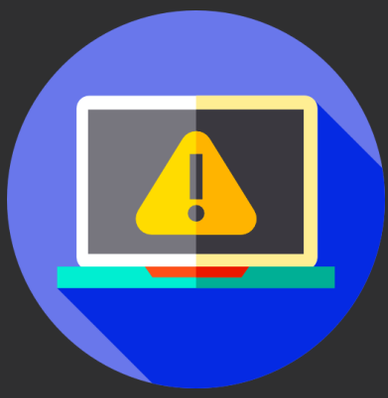
Ti consiglio di procedere come segue...

...per prima cosa installa sul tuo PC un software di VIRTUALIZZAZIONE come ad esempio Oracle Virtualbox.

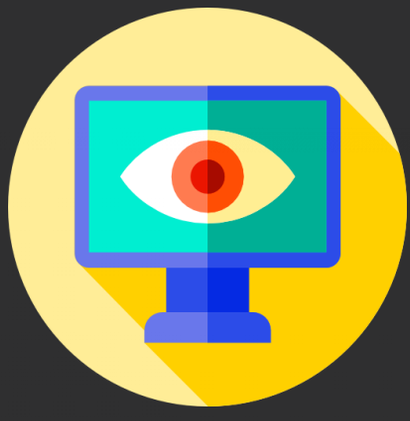
Scaricati una distribuzione Linux orientata al penetration testing, Kali Linux è ottima.
Installati una delle web application analizzate oppure la macchina virtuale OWASP che le racchiude tutte...

...ED ESERCITATI IL PIU' POSSIBILE!





RISORSE UTILI DI VARIA NATURA



ACCADEMIA HACKER

SEGRETO N° 81

Ti presento adesso il sito HACK THE BOX (https://www.hackthebox.eu/), un laboratorio online dedicato al penetration testing.

Sono presenti moltissime sfide, strutturate su livelli di competenza differenti e aggiornate costantemente.

Al momento sono presenti 92 macchine con cui esercitarti.

Come già detto se vuoi diventare un hacker devi fare PRATICA...molta pratica!

SEGRETO N°82

Vulnhub (https://www.vulnhub.com/) è un ottimo progetto a mio avviso, una delle migliori risorse per fare esercizio. Praticamente gli utenti mettono a disposizione degli altri utenti delle macchine virtuali scaricabili che contengono vulnerabilità di vario tipo, non solo legate alle web application ma anche al sistema operativo stesso.

Basta scaricarne una, seguire le istruzioni fornite dal creatore della macchina e iniziare a ricercare tutte le vulnerabilità.

Al momento ci sono decine di macchine presenti!

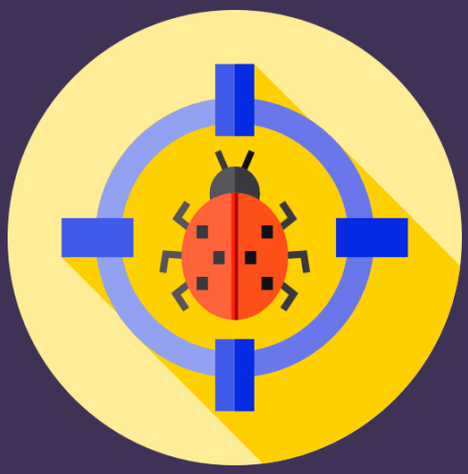
SEGRETO N°83

ROOT ME

Altro sito con cui mettersi alla prova!
Root-me(https://www.root-me.org).

Contiene attualmente più di 300 sfide, 73 ambienti virtuali e 3000 soluzioni.

Basta solo registrarsi ed iniziare la sfida!



SEGRETO N°84

Hack.me

Hack.me è una piattaforma FREE gestita da eLearnSecurity.

Anche in questo caso basta solo registrarsi e abbiamo decine di sfide pronte ad attenderci!

Al seguente link è possibile visualizzare quelle attualmente disponibili: https://hack.me/explore/.

E' possibile creare anche le proprie APPLICAZIONI VULNERABILI e caricarle sulla piattaforma.

SEGRETO N°85

https://github.com/rapid7/metasploitable3

Altro suggerimento è di utilizzare, oltre alle web application vulnerabili e ai siti già visti, una macchina virtuale denominata METASPLOITABLE che contiene svariate vulnerabilità, molte delle quali legate alla sicurezza del sistema operativo.

Al momento l'ultima disponibile è METASPLOITABLE 3.

Anche in questo caso basta sfruttare il laboratorio personale virtualizzato.



SEGRETO N° 86

Già anticipato nella parte FORMAZIONE, è necessario studiare almeno un linguaggio di programmazione.

Ci saranno molte occasioni in cui avrai la necessità di creare i tuoi SCRIPT o TOOL che magari ti velocizzeranno alcune operazioni o saranno più efficaci dei tool standard in determinati contesti.

Di seguito alcune RISORSE UTILI per fare pratica.

SEGRETO N°87

Il sito CODERBYTE (https://coderbyte.com/) ti permette di fare esercizio mettendoti a disposizione decine di "sfide di codice".

Quest'ultime sono suddivise per DIFFICOLTA' e per TIPOLOGIA.

E' sufficiente registrare un account.

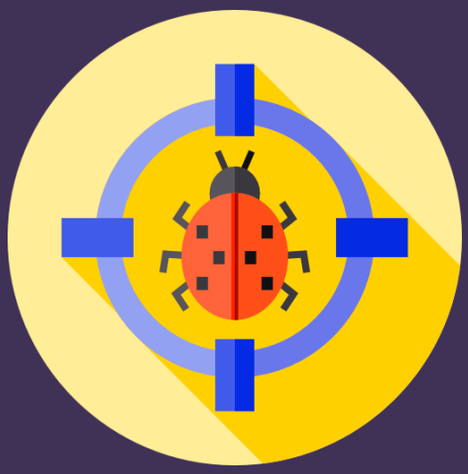
Considera inoltre che molte sfide ti porteranno via pochissimo tempo e quindi puoi fare esercizio anche nei ritagli di tempo.

SEGRETO N°88

ALTRI SITI...

Altri siti simili a quello appena presentato sono:

1) https://codesignal.com/
2) http://www.codeabbey.com/
3) http://fightcodegame.com/
4) https://www.reddit.com/r/dailyprogrammer/
5) https://www.codingame.com/start
6) https://www.hirevue.com/products/assessments
7) https://www.hackerearth.com/
8) https://www.spoj.com/
9) https://github.com/Microsoft/computerscience



SEGRETO N°89

Riepilogo...

Concludiamo adesso con il riepilogo dei suggerimenti che dovrai tenere a mente per diventare un HACKER.

TUTTAVIA CONSIDERA CHE NON C'E' MAI UN'UNICA STRADA PERCORRIBILE, LE POSSIBILITA' SONO SVARIATE E ALCUNE MENO EVIDENTI.

SEGRETO N°90

Primo suggerimento...

...anche se la voglia di sperimentare tutte le risorse che ti ho suggerito è tanta, cerca di PROCEDERE PER GRADI e soprattutto cerca di dedicare del tempo allo studio delle RETI.

Ricorda che non è una perdita di tempo o qualcosa di inutile.

Conoscere il funzionamento della RETE è il primo vero investimento professionale che puoi fare!



SEGRETO N° 91

Ti ho già mostrato le migliori risorse per studiare le RETI, tuttavia il miglior modo di procedere è, anche in questo caso, esercitandoti.

Inizia subito col scaricarti il simulatore Cisco Packet Tracer (https://www.netacad.com/courses/packet-tracer) e a fare i primi esercizi.

Su Youtube ne trovi moltissimi già svolti.

SEGRETO N°92

Parallelamente allo studio delle RETI devi approfondire un linguaggio di programmazione.

Ti consiglio PYTHON che è molto facile da apprendere e può darti moltissime soddisfazione a breve termine.

Le risorse a tua disposizione sono di ogni tipo: video, libri, corsi, articoli, ecc...

Anche in questo caso meglio non perdere troppo tempo studiando la teoria ma piuttosto fare molti esercizi pratici!

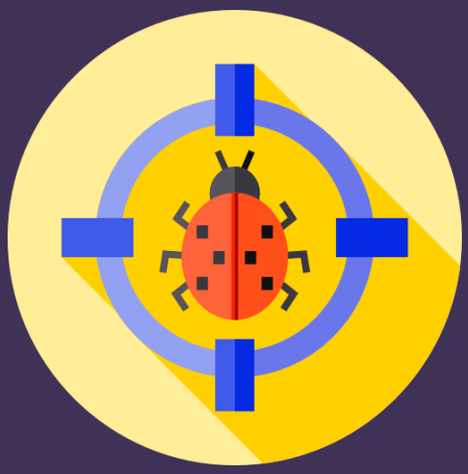
SEGRETO N°93

CERTIFICAZIONI

Per attestare la competenza nelle reti, ti invito a valutare l'idea di prendere una CERTIFICAZIONE.

Molto richiesta e di ottimo valore è la Cisco CCNA Switching & Routing.

Nella parte FORMAZIONE trovi tutti i link.



SEGRETO N°94

e la SICUREZZA...

Adesso che hai una buona conoscenza delle RETI e conosci un linguaggio di programmazione, puoi iniziare ad avvicinarti al mondo della SICUREZZA INFORMATICA.

Il suggerimento è di non perdere tempo dietro a dettagli teorici e/o normativi ma passa subito alla pratica.

Anche qui tramite laboratori virtuali, puoi simulare quasi tutti gli scenari, anche i più complessi.

SEGRETO N°95

Sicurezza Difensiva...

Puoi fare esercizio in molteplici campi della sicurezza informatica, ad esempio:

1) Configurazione di FIREWALL.
2) Analisi dei MALWARE.
3) Sicurezza in ambito CLOUD.
4) Linux/Windows hardening.
5) Protezione ENDPOINT.
6) Configurazione IDS/IPS.
7) Configurazione NAC.
8) Sicurezza in ambito MOBILE.
9) Sicurezza dispositivi IOT.



SEGRETO N° 96

A questo punto hai una conoscenza delle RETI e della SICUREZZA INFORMATICA e puoi quindi iniziare ad approcciarti all'ETHICAL HACKING.

Come vedi è un percorso: non si parte MAI direttamente dall'ethical hacking, altrimenti la tua formazione sarà incompleta e le tue competenze tecniche scarse.

SEGRETO N°97

Per quanto riguarda l'ethical hacking puoi valutare le certificazioni che ti ho suggerito, in particolare l'OSCP.

Tuttavia qui conta moltissimo la pratica: ti ho elencato decine di risorse utili per esercitarti, cerca di sfruttarle tutte!

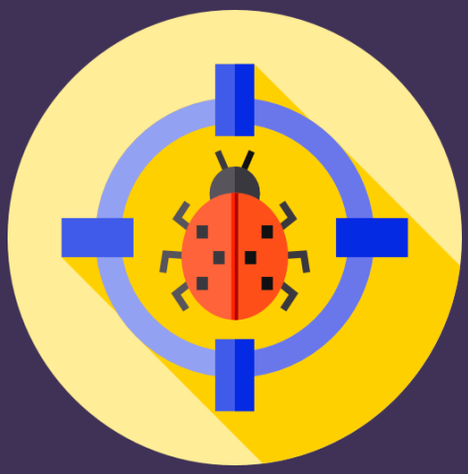
SEGRETO N°98

AZIENDE...

Quasi tutte le aziende che ti proporranno una posizione lavorativa come ETHICAL HACKER vorranno vedere nella pratica ciò che sai fare.

Avere una certificazione come l'OSCP può essere senz'altro d'aiuto ma non è sicuramente l'unico fattore di valutazione.

E ripeto: la conoscenza delle RETI e della SICUREZZA DIFENSIVA sarà un elemento FONDAMENTALE anche in questo caso.



SEGRETO N°99

VIAGGIO FORMATIVO...

Spero di averti trasmesso il fatto che la SICUREZZA INFORMATICA è una disciplina senza dubbio affascinante ma anche complessa.

Una sorta di VIAGGIO FORMATIVO che parte dalla conoscenza di una RETE, dalla sua MESSA IN PROTEZIONE e successivamente verso l'ATTACCO di quest'ultima.

RICORDA: l'ordine di queste FASI non è negoziabile!

SEGRETO N° 100

Ultimo SEGRETO...

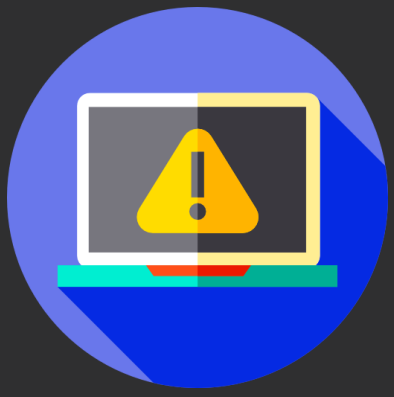
L'ultimo SEGRETO è destinato proprio a dirti che, in verità, non esistono SEGRETI per diventare un HACKER!

L'hacker non è altro che un esperto in sicurezza informatica che ha dedicato molti anni di studio alla materia.

Ogni trucco o scorciatoia ti porterà senza dubbio fuori strada.

Detto questo: BUONA FORTUNA E IN BOCCA AL LUPO PER TUTTO!





GRAZIE!
Se hai apprezzato questi consigli ricordati di lasciarmi una RECENSIONE...per noi autori è molto importante e a te costa solo qualche secondo di tempo...
GRAZIE!