Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 1
ESSERE UN HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informazioni sulla licenza d'uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo "non-commerciale" verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo "doposcuola".

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L'erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all'indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Hanno contribuito

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino - ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

1.0 Introduzione

Benvenuto al programma Hacker Highschool ! Questo programma è progettato per incoraggiarti ad aggiornarti e a trovare da te stesso le risorse necessarie. Il tema principale dell'istruzione è sfruttare la curiosità dell'hacker che c'è in te, per guidarti progressivamente attraverso la tua educazione hacker, a crescere in un ruolo responsabile, capace di determinare i problemi di sicurezza e di privacy e di assumere autonomamente le decisioni in materia di sicurezza.

L'hacking può essere emozionante, in parte, per la natura illegale dell'accesso ai computer: vogliamo dimostrarti come possa essere più emozionante avvisare gli altri dei problemi di sicurezza e renderli pubblici, senza la preoccupazione di finire in carcere per averlo fatto.

Come cittadino, in molti paesi non è solamente un tuo diritto, ma una tua responsabilità avvisare le autorità competenti di eventuali falle di sicurezza e di privacy.

In questo modo potrai aiutare coloro che non sono in grado di affrontare i problemi di sicurezza e privacy. Questo è ciò che fanno i cosiddetti "gruppi di cani da guardia" (Watchdog groups, N.d.T), questo è quello che apprenderai.

1.1 Risorse

Questa lezione tratta il modo di apprendere – una capacità critica per un hacker ma molto importante. L'hacking, in realtà, è un processo creativo basato su esperienze maturate in molti campi. Non possiamo insegnarti direttamente tutto ciò che ti necessita, possiamo però aiutarti a riconoscere cosa ti occorre imparare. Questo concetto è molto importante nel campo dei computer, considerati i costanti progressi ed innovazioni. Ciò che insegnamo oggi domani può già essere meno importante. E' più importante introdurti in ambienti di apprendimento hacker, che sono la parte più vitale dell'hacking e che ti differenzieranno da uno script kiddie (una persona che utilizza strumenti di hacking senza conoscerne il funzionamento).

Le parole e i concetti che non comprendi in questo manuale potranno richiedere ricerche sul Web o presso una biblioteca.

Se non comprendi una parola o un concetto, è essenziale che attivi la ricerca; ignorare ti renderà più difficile, se non impossibile, comprendere concetti che si trovano nelle altre lezioni del programma HHS.

Gli altri manuali potranno chiederti di approfondire alcuni argomenti sul web e si aspetteranno che utilizzi le informazioni trovate per completare gli esercizi proposti.

Questo manuale ti insegna a ricercare le informazioni che ti necessitano, questo è l'unico in cui ti forniremo informazioni dettagliate su come cercare; per questo motivo ti invitiamo a dedicare a questa lezione tutto il tempo necessario ad apprendere come investigare utilizzando tutte le risorse a te disponibili.

Non limitarti a computer, hacking, Internet. I grandi hacker sono creativi, molti di loro sono pittori, scrittori, disegnatori. Le abilità dell'hacker possono anche essere applicate in altri campi come le scienze politiche (vedi p. es. Il Principe di Macchiavelli).

A parte interessarti di altri campi, dovresti anche interessarti su come funzionano le cose. Leggere libri di tutto, dalla psicologia alla scienza narrativa ti renderà un hacker molto più versatile e funzionale. Ricorda, hacking significa occuparsi di come funzionano le cose senza preoccuparsi di come furono progettate. Questo è il modo in cui potrai identificare i problemi di sicurezza e le vulnerabilità.

1.1.1 Libri

I libri sono un buon modo per apprendere i fondamenti di tutte le scienze che desideri esplorare.

Vuoi conoscere qualcosa di un campo della scienza, come i dettagli dell'hardware del tuo personal computer ? Nulla ti aiuterà di più che leggere un buon libro che tratta questo tema. Il problema principale con i libri che riguardano i computer è che diventano datati molto in fretta; per questo motivo è consigliabile imparare a cogliere gli aspetti fondamentali evitando inutili dettagli. Per esempio MS-DOS e Microsoft Windows sono chiaramente differenti, entrambi sono però basati sugli stessi principi di logica booleana che hanno governato i computer sin dai tempi in cui Ada, Contessa di Lovelace, scrisse il primo programma per computer nel diciannovesimo secolo. Le questioni della sicurezza e della privacy possono essere cambiate negli ultimi 2500 anni, ma il libro di strategia "L'arte della guerra" di Sun Tzu descrive gli aspetti fondamentali ancora applicabili oggi.

Scoprirai che l'informazione trovata nei libri puo' non essere aggiornata, ma è più accurata nei fatti di quella proveniente da altre fonti. Uno scrittore che impiega un anno

per scrivere un libro è probabile che controlli più scrupolosamente i fatti di chi aggiorna un blog sei volte al giorno (Vedi paragrafo 1.2.3 Zines e Blog). Ricorda comunque - accurato non significa obiettivo.

Dove si possono trovare i libri ? Ovunque. Non è necessario creare una propria libreria, ricorda però che scrivere annotazioni a margine o sottolineare parti di testo sono operazioni che puoi fare con i tuoi libri.

Se cominci un libro, non lo abbandonare a metà solo per la sua dimensione e complessità. Molte volte non ti sarà necessario leggere un libro dal principio alla fine. Puoi aprire un libro e cominciare a leggere da un punto casuale; se non capisci qualcosa puoi cercare nei capitoli precedenti. Salta avanti e indietro proprio come faresti con i link di una pagina web. La lettura non lineare è molto più interessante e soddisfacente per gli hacker poichè si tratta di soddisfare la curiosità più che "leggere".

1.1.2 Riviste e Quotidiani

L'utilizzo di riviste e quotidiani è raccomandata per mantenere l'informazione concisa ed aggiornata. Tuttavia di solito le riviste offrono pochi dettagli e si focalizzano troppo sulla comunità dei lettori. Ciò può produrre informazione poco precisa, creata per la stampa sensazionalista. Ovviamente ciò trova la spiegazione nell'obiettivo di aumentare il numero di abbonamenti e/o di vendite, in quanto anche le riviste gratuite hanno bisogno di sottoscrittori per vendere la pubblicità.

Un altro aspetto da tenere presente è il tema che tratta la rivista. Per esempio una rivista di Linux potrebbe avere la tendenza a disprezzare Microsoft Windows, perchè esiste un conflitto tra i due sistemi operativi ed è ciò che presumibilmente i suoi lettori sperano di leggere.

Se leggete un fatto interessante su una rivista, non lasciatevi influenzare da un solo punto di vista, cercate invece eventuali altre conferme e confutazioni.

Esercizi:

a. Cerca nel Web tre riviste relative alla Sicurezza.
b. Come le hai trovate ?
c. Tutte e tre le riviste riguardana la sicurezza informatica ?

1.1.3 Zine e Blog

Le Zine (dall'inglese, "E-zines", N.d.T.) sono riviste che hanno una distribuzione limitata (meno di 10.000 lettori) e sono spesso prodotte da hobbisti o da giornalisti dilettanti. Alcune Zine, come la famosa 2600 Magazine o Phrack, sono scritte da volontari ed i produttori non modificano il contenuto per errori non-tecnici. Ciò significa che il linguaggio puo' essere grezzo per coloro che non sono abituati a questo tipo di letture. Le Zine trattano temi molto forti ed illustrano diverse opinioni, anche quelle contrastanti, in quanto non devono curarsi degli abbonati e della pubblicità.

I Blog rappresentano una modernizzazione delle Zine, sono aggiornati con frequenza e sono utilizzati dalle comunità per discutere temi forti. Come per le Zine, chiunque puo' criticare una storia o manifestare opinioni contrastanti. Per i Blog è importante leggere i commenti, oltre che la storia.

Esercizi:

a. Cerca nel Web tre Zine correlate alla sicurezza informatica.
b. Come hai trovato queste Zine ?
c. Perchè le classifichi come Zine ? Ricorda, il solo fatto che siano etichettati come Zine non significa necessariamente che lo siano.
d. Cerca nel web 3 Blog correlati alla sicurezza informatica.
e. A quali comunità sono associati i 3 blog ?

1.1.4 Forum e Mailing list

I Forum e le Mailing list sono media sviluppati per le comunità, simili alla registrazione di una serie di conversazioni durante una festa. La conversazione cambia frequentemente fuoco, la maggior parte di ciò che si dice sono "voci" e quando la festa è finita, nessuno è sicuro di "chi ha detto che cosa". I forum e le mailing list sono simili, perché ci sono molti modi con cui la gente può contribuire con informazioni non accurate - qualche volta intenzionalmente – e ci sono anche modi per contribuire in forma anonima. Come con i Blog, è importante leggere tutte le risposte ed i commenti - e non solamente i primi - se si desidera avere la maggior informazione possibile.

Vi sono Forum che trattano praticamente tutti gli argomenti e molte riviste e periodici online offrono forum ai lettori per ottenere il feedback dagli articoli pubblicati. In questo caso i forum sono indispensabili per avere più di una opinione dello stesso argomento, indipendentemente dal gradimento dell'articolo stesso.

Esistono molte mailing list che trattano temi molto specifici, ma sono difficili da trovare. Spesso devi cercare un'idea, prima di trovare una comunità che la supporta con una mailing list.

Per un hacker è importante sapere che molti forum e mailing list non sono esplorabili dai principali motori di ricerca. E' possibile trovare un forum o una mailing list per mezzo di una ricerca per soggetto, ma non è possibile trovare informazioni nei singoli messaggi. Queste informazioni costituiscono il "Web invisibile" in quanto sono invisibili ai più perchè richiedono ricerche molto specifiche - spesso con motori di tipo meta-search, a volte direttamente nel sito web del forum - per scoprirle.

Esercizi:

a. Cerca 3 forum di sicurezza informatica.
b. Come hai trovato questi forum ?
c. Puoi determinare il tema principale che tratta il sito web ?
d. Gli argomenti che hai trovato riflettono la tematica del sito web che li ospita ?
e. Cerca 3 mailing list sulla sicurezza informatica.
f. Chi è il "Proprietario" della lista ?
g. In quale lista ti aspetti di trovare informazioni più oggettive e meno soggettive e perchè ?

1.1.5 Gruppi di discussione

I gruppi di discussione, o newsgroup, sono attivi da molto tempo, prima ancora che esistesse il Web. Google acquistò l'intero archivio dei newsgroup e lo pose online all'indirizzo http://groups.google.com.

Vi si trovano messaggi a partire dai primi anni 90. Questo archivio è importante per trovare chi ha originato un'idea o un prodotto e per trovare le c.d. "informazioni oscure", troppo limitate per trovare spazio su una pagina web.

I gruppi di discussione di oggi si utilizzano come un tempo, prima che il web divenisse la principale fonte per condividere l'informazione; tuttavia con l'avvento del web la loro espansione si è fermata e la loro popolarità ha ceduto il passo ai blog e ai forum.

Esercizi:

a. Utilizzando i gruppi di Google trova il messaggio più antico sulla sicurezza.

b. Cerca altri modi per utilizzare i newsgroup - ci sono applicazioni che puoi usare per leggere i newsroup ?

c. Quanti gruppi di dicussione su "computer hacking" puoi trovare ?

1.1.6 Pagine Web

Lo standard di fatto per condividere l'informazione oggi è costituito da un browser web. Anche se classifichiamo tutto come "web", il termine corretto è "servizi web" poichè non tutte le cose sul web sono siti web. Se controlli la tua posta utilizzando un browser, stai utilizzando un servizio web. Spesso i servizi web richiedono opportuni privilegi. Ciò significa che necessiti di un nome per il login e di una password per avere l'accesso al servizio. Avere l'accesso e il diritto legale di accedere è noto come avere i privilegi. Dell'hacking verso un sito web per modificare una pagina web può darti l'accesso, però poichè non possiedi il diritto legale di farlo non si tratta di un accesso privilegiato. Noi siamo solo interessati agli accessi privilegiati, a mano a mano che la tua esperienza maturerà troverai che molti siti concedono accessi ad aree privilegiate per errore. Se ne incontri qualcuno, abituati a segnalarlo al proprietario del sito.

I siti web sono esaminabili da un gran numero di motori di ricerca. Se hai tempo e spazio sull'hard disk, puoi farti un motore di ricerca. Spesso è proprio il motore di ricerca che ottiene l'accesso privilegiato e ti passa le informazioni. A volte è in forma di cache. La cache è un'area di memoria sul server del motore di ricerca in cui il motore memorizza le pagine che soddisfano il tuo criterio di ricerca. Se clicci su un link che indica "Copia cache" oppure "Cached", invece che sul link reale, vedrai una pagina che rappresenta l'istantanea della pagina web archiviata durante la scansione del web dal motore di ricerca; la cache puo' essere utilizzata per visualizzare pagine provenienti da un server molto lento, tuttavia ricorda che è possibile che il contenuto della pagina sia stato modificato. Uno dei più utili siti che offrono accesso pubblico alla cache è : http://www.archive.org

Una nota finale sui siti web: non considerare affidabile l'informazione che compare in un sito web solamente perchè compare in un motore di ricerca.

Molti virus e attacchi si diffondono solamente visitando una pagina web o scaricando e eseguendo un programma da siti web non affidabili.

Puoi proteggerti evitando di scaricare programmi da fonti non sicure e assicurandoti che il browser che utilizzi sia aggiornato con le opportune patch di sicurezza.

Esercizi:

a. Utilizzando un motore di ricerca, trova siti che offrono, accidentalmente, accesso privilegiato a tutti. Per farlo cerca listati di directory che sono accessibili senza accedere ad una pagina web definita. Per esempio vai su http://www.google.com e cerca la seguente frase:

```
allintitle:  "index of" .pdf
```

Dai risultati ottenuti, visita alcune directory, dovresti poter accedere a tutti i contenuti. Questo tipo di ricerca si chiama Google hacking.

b. Puoi trovare altri tipi di documenti utilizzando Google ? Trova 3 listati di directory che contengono archivi di tipo .xls e .avi.

c. Esistono molti motori di ricerca oltre Google. Un buon hacker sa come e quando utilizzarli tutti. Alcuni siti web si specializzano nella ricerca dei motori di ricerca, ad esempio www.searchengine.com. Esiste persino un motore di ricerca per il "Web invisibile". Trova 10 motori di ricerca che non siano di meta-informazioni.

d. Trova "security testing and ethical hacking" ed elenca le prime 3 risposte.

e. Ripeti la ricerca precedente ma ometti le virgolette. I risultati sono differenti ?

f. E' molto differente trovare una parola chiave o una frase intera. Nell'esercizio d, hai trovato una frase intera. Ora cercherai un'idea. Per farlo devi pensare a cosa e come la vuoi trovare. Per esempio, vuoi trovare risorse online relative all'hacking etico (Ethical hacking). Se indichi a un motore di ricerca "Online resource of magazine for ethical hacking", otterrai molte opinioni sull'argomento. Tuttavia ciò non è esattamente quello che cercavi: ottenere le risorse. In alternativa devi pensare "Se dovessi realizzare una tale risorsa, quale informazione dovrebbe esserci e quali parole chiave potrei estrarre da questa informazione?" Cerca le seguenti frasi e parole con un motore di ricerca e trova quale fornisce i migliori risultati per la tua ricerca:

1. my favorite list of magazines on ethical hacking
2. list of ethical hacking magazines
3. resources for ethical hackers
4. ethical hacking magazine
5. magazines ethical hacking security list resource
6. Trova il sito web più antico del browser Mozilla nell'archivio Internet. Devi cercare www.mozilla.org in http://www.archive.org.
7. Ora, per esercitare i vari aspetti evidenziati, supponiamo che vuoi scaricare la versione 1 del browser Netscape. Utilizzando un motore di ricerca e gli archivi Internet (la cache) trova e scarica il browser richiesto (però NON INSTALLARLO).

1.1.7 Chat

Le Chat, anche note come Internet Relay Chat (IRC) e come sistema di messaggeria istantanea (IM) sono modi popolari per comunicare rapidamente con gli altri in tempo reale. Come fonte di informazione le chat sono contradditorie in quanto avrai a che fare con molte persone in tempo reale; alcuni saranno gentili, altri villani. Alcuni saranno burloni innocui, altri bugiardi maliziosi. Alcuni saranno intelligenti e disposti a condividere informazioni, alcuni completamente disinformati ma non meno desiderosi di condividere. Potrà risultare molto difficile distinguere con chi avrai a che fare. Ad ogni modo una volta che ti sentirai a tuo agio con un certo gruppo di utenti potrai essere accettato nella comunità e ti sarà concesso di porre più domande e imparerai su chi fare affidamento. Eventualmente, avrai l'opportunità di apprendere le informazioni più recenti sulla sicurezza (note come zero day o giorno zero, che significa che sono appena state scoperte o rilasciate), che ti permetteranno di ampliare la tua conoscenza. Devi anche tener presente che a volte si ottengono informazioni false; è necessario acquisire sufficiente esperienza per distinguere l'informazione vera da quella che non lo è.

Esercizi:

a. Trova 3 programmi di Chat. Cosa li rende differenti? Si possono utilizzare per parlare l'un l'altro?

b. Trova che cosa è IRC e come vi si puo' connettere, entra poi nella chat room di ISECOM, come indicato nella pagina di http://www.isecom.org.

c. Come puoi conoscere quali canali esistono in un IRC System ? Trova tre canali di sicurezza informatica e 3 canali hacker. Puoi entrare in questi canali ? Ci sono persone che conversano, o sono "bots" ?

1.1.8 P2P

La rete Peer to Peer, anche conosciuta come P2P, è una rete interna a Internet. Invece di molti computer locali che comunicano attraverso un server centralizzato, i computer di una rete P2P comunicano direttamente l'un l'altro. Esistono molti client P2P che permettono di scaricare mp3 e film piratati. In generale però la rete P2P permette lo scambio di contenuti in formato digitale. Maggiori informazioni si possono trovare sul sito: http://www.infoanarchy.org. Su questo sito puoi trovare un elenco di reti P2P e di client.

Il problema del P2P è che da un lato puoi trovare informazioni su praticamente qualsiasi cosa, dall'altro che parte dell'informazione si trova sulla rete in modo illegale. Il programma Hacker Highschool condanna l'uso illegale del P2P, ovvero lo scaricamento di materiale soggetto al diritto d'autore. Le reti P2P sono di importanza vitale per la ricerca dell'informazione, non c'è nulla di illegale nell'uso del P2P, ci sono molti file che possono essere distribuiti gratuitamente sotto varie licenze: vi sono tuttavia molti file che non lo sono in quanto sottoposti alla legge sul copyright. Non temere nell'usare la rete P2P, sii però consapevole.

1.2 Ulteriori approfondimenti

Ora dovresti sperimentare per acquisire esperienza nelle tecniche di ricerca. Più lo farai, più rapidamente acquisirai informazione e imparerai. Alcuni temi correlati al programma Hacker Highschool che potranno aiutarti a guadagnare maggiore esperienza sono:

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine