



Penetration Testing & Ethical Hacking

Fondamenti di Ethical Hacking

Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Chi è un Hacker?



Chi è un Hacker?

Un hacker è comunemente visto come una persona strana e maliziosa, il cui obiettivo è quello di violare sistemi, tipicamente di notte



Tale definizione non sempre rispecchia la realtà

Chi è un Hacker?

Un hacker è comunemente visto come una persona strana e maliziosa, il cui obiettivo è quello di violare sistemi, tipicamente di notte



Tale definizione non rispecchia assolutamente gli obiettivi del corso

Chi è un Hacker?

- Persona fortemente interessata al funzionamento delle cose, che sviluppa abilità come conseguenza della sua curiosità



- Un hacker
 - Persegue la conoscenza, non solo nel campo informatico, ma in qualsiasi altro settore
 - Cerca di pensare e di risolvere problemi in maniera non convenzionale

Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking

Storia dell'Hacking

1870

1870: Bell Telephone Company (oggi *American Telephone & Telegraph Company - AT&T*) assunse alcuni ragazzi per lavorare come operatori nei propri centralini telefonici



Storia dell'Hacking

1870

- Questi ragazzi cominciarono a studiare il funzionamento degli apparecchi telefonici da loro usati, al fine di
 - Dirottare intenzionalmente le telefonate
 - Disconnettere le telefonate
 - Ascoltare le conversazioni
 - Fare altri tipi di scherzi



Storia dell'Hacking

1870

- Non fu utilizzato il termine «hacking», ma questa vicenda rappresenta storicamente il primo episodio noto di «abuso» della tecnologia
- Si crede che questo sia stato uno dei motivi per cui l'azienda decise di assumere come operatori telefonici solo lavoratrici



Storia dell'Hacking

Anni '50

- **Anni 50:** Parola «Hack» usata per la prima volta
 - Scorcatoia o tecnica per utilizzare in maniera non convenzionale un sistema
- Termine coniato da appassionati di modellismo ferroviario del **MIT (Massachusetts Institute of Technology)**, appartenenti all'organizzazione **Tech Model Railroad Club (TMRC)**



Storia dell'Hacking

Anni '50

- I membri del TMRC
 - Ricevettero in donazione vecchie apparecchiature telefoniche
 - Utilizzate, in maniera non convenzionale, per creare un complesso sistema di controllo per i modellini dei treni
 - Progettarono un modo per controllare il percorso dei modellini componendo numeri sul telefono



Storia dell'Hacking

Anni '50

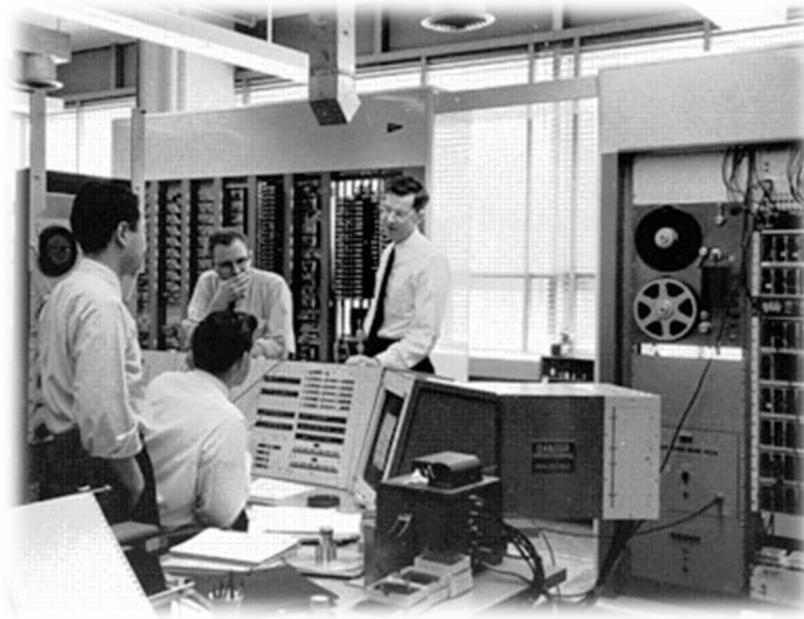
- I membri del TMRC furono i primi ad essere considerati **hacker**
- Presero le apparecchiature che avevano a disposizione e ne fecero un uso del tutto innovativo e non convenzionale



Storia dell'Hacking

Anni '50-60

- **Qualche anno dopo:** Alcuni hacker del TMRC cominciarono ad interessarsi ai nuovi sistemi informatici introdotti nel loro campus



Storia dell'Hacking

Anni '50-60

- **Nuova generazione di hacker:** appassionati di programmazione che volevano modificare i programmi esistenti per
 - Renderli migliori
 - Personalizzarli, così da poterli utilizzare per i propri fini
 - Divertirsi



Storia dell'Hacking

Anni '50-60

- Venivano prodotte versioni modificate e migliorate dei programmi originali

- Gli hacker avevano come **obiettivo**
 - Scrivere programmi per risolvere problemi
 - Scrivere programmi per risolvere problemi nel miglior modo possibile



Storia dell'Hacking

Anni '70

- **Anni 70:** Nacque una figura diversa di hacker, il cui obiettivo era lo sfruttamento del sistema telefonico
 - **Phreaker**
- **Obiettivo dei Phreaker:** capire il funzionamento del sistema di commutazione elettronica per poter effettuare gratuitamente chiamate telefoniche interurbane



Storia dell'Hacking

Anni '70

- Il Phreaking può essere visto come uno dei primi movimenti «anti-establishment», che in seguito avrebbe dato vita ai moderni hacker



Storia dell'Hacking

Anni '80

- **Anni 80:** I primi Personal Computer (PC) cominciano ad essere disponibili
- Gli hacker utilizzano la nuova tecnologia per espandere il loro campo di azione



Storia dell'Hacking

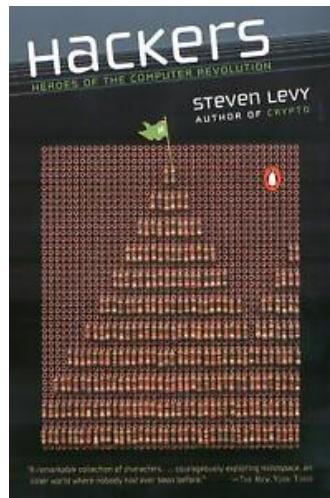
Anni '80 – Hacker Ethic

«The desire to dissect, understand, and better appreciate computer programming
in order to gain more knowledge»



Storia dell'Hacking

Anni '80 – Hacker Ethic



**«Ci dovrebbe essere un accesso illimitato e totale ai computer
per capire come funziona il mondo»**

Hackers : Heroes of the
Computer Revolution.
Steven Levy. 1984

Storia dell'Hacking

Anni '80-90

- **Fine Anni 80 – Inizio Anni 90:** Esplorare i sistemi per motivi etici (ad es., sete di conoscenza, etc) non è più «sufficiente»
- Gli hacker operano per profitto personale, impegnandosi in attività criminali
 - Vendita di videogiochi e software «pirata», distribuzione di software malevolo per attaccare sistemi (ad es., virus), etc
- **Cyber-gang alla ricerca di dati sensibili in grandi istituzioni e governi**



Storia dell'Hacking

Anni '90-00

- Ciò ha portato all'intervento delle forze dell'ordine ed all'introduzione di varie leggi per contrastare il fenomeno dell'hacking
- Molti dei membri delle cyber-gang sono stati arrestati e processati



Storia dell'Hacking

Anni '00

- **Primi Anni 2000:** crescente utilizzo delle reti Wi-Fi
 - Whacking (wireless hacking)
 - Violazione di Wireless Access Point (WAPs) non adeguatamente protetti
 - Wardriving



Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking

Tipologie di Hacker

- Gli hacker, in base al loro comportamento, tipicamente possono appartenere a tre macro-categorie
 - Black Hat Hacker (**«Cattivi»**)
 - White Hat Hacker (**«Buoni»**)
 - Grey Hat Hacker (**«Borderline»**)



Tipologie di Hacker

Black Hat Hacker

- Rappresentano, sfortunatamente, l'immagine più nota e diffusa del termine «hacker»
- Sono coinvolti in attività illegali con intenzioni malevole normalmente orientate al denaro



Tipologie di Hacker

Black Hat Hacker

- Criminali informatici, che tipicamente svolgono varie attività illecite, tra le quali
 - Furto di informazioni
 - Furto di denaro
 - Furto e vendita di dati da carte di credito
 - Denial of Service (DoS)
 - Frode
 - Etc



Tipologie di Hacker

Black Hat Hacker

- Ottengono benefici dalle vulnerabilità rilevate invece di contribuire a risolverle
- **Operano in maniera non etica**



Tipologie di Hacker

White Hat Hacker

- **Operano sempre nel rispetto delle regole (leggi, accordi, etc), assumendo comportamenti etici**

- Violano dispositivi e sistemi per trovare potenziali vulnerabilità, fornendo eventualmente anche soluzioni su come risolverle e prevenirle



Tipologie di Hacker

White Hat Hacker

- Garantiscono il rilascio pubblico di aggiornamenti per correggere le vulnerabilità rilevate
- Sono costantemente alla ricerca di nuove vulnerabilità in sistemi e dispositivi per renderli più efficienti e sicuri
- Sono strutturati in comunità per condividere in maniera più efficace le loro conoscenze



Tipologie di Hacker

Ethical Hacker

- Spesso sinonimo di White Hat Hacker

- **Obiettivi e Modus Operandi**
 - Rilevare e correggere le vulnerabilità in aziende o organizzazioni
 - Contribuire a migliorare il livello di sicurezza
 - Agire sempre secondo le *regole di ingaggio*, i regolamenti, le leggi, etc



Tipologie di Hacker

Grey Hat Hacker

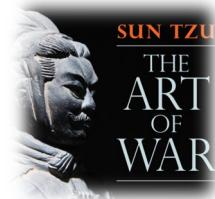
- Oltre a cercare vulnerabilità per renderle note e correggerle, talvolta svolgono anche alcune attività illecite o «immorali»
- Sono spinti da interessi economici oltre che etici
- Tendono ad usare sia mezzi leciti che illeciti per violare un sistema

- Ad es., accedono al sistema di un'organizzazione, informano della vulnerabilità che hanno trovato e forniscono suggerimenti su come risolverla
 - **Ma talvolta chiedendo qualcosa in cambio...**



Conoscere gli Hacker

- Per proteggersi dagli hacker bisogna pensare ed agire come loro
 - Acquisendo le adeguate conoscenze
 - Comprendendo
 - Le metodologie e gli strumenti che possono essere utilizzati per attaccare
 - Le motivazioni alla base di un attacco
- Questo sarà il primo passo per capire come difendersi ed eventualmente come contrattaccare

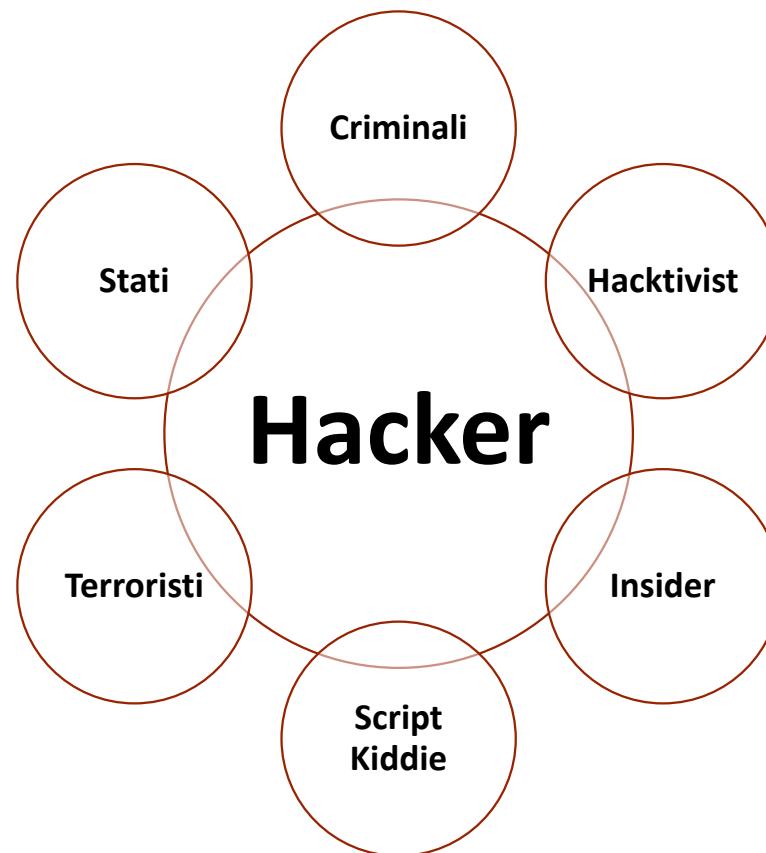


«Se conosci il nemico e te stesso la tua vittoria è sicura»
Sun Tzu, L'arte della guerra
VI - V secolo a.C.

Conoscere gli Hacker

- Le motivazioni alla base di un attacco possono essere varie
 - Otttenere l'accesso legale ed autorizzato ad un sistema per testarne la sicurezza, rilevando e correggendo eventuali vulnerabilità
 - Otttenere l'accesso illegale ad un sistema per pura curiosità o orgoglio
 - Otttenere l'accesso non autorizzato ad informazioni per distruggerle o manometterle
 - Accedere ad un sistema informatico in modo da carpire dati ed eventualmente venderli a terze parti
 - Etc

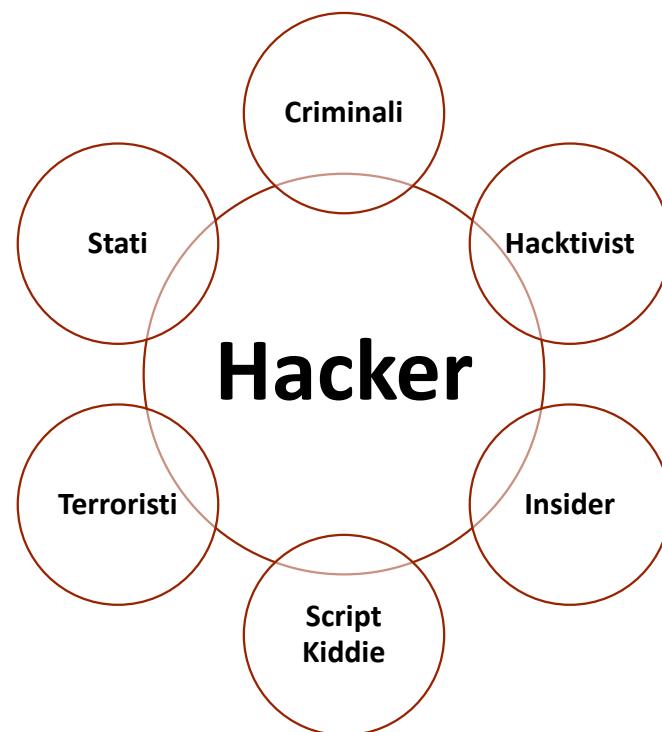
Caratterizzazione degli Hacker



Gli hacker possono essere caratterizzati a seconda delle motivazioni alla base delle loro azioni

Caratterizzazione degli Hacker

- Motivazioni, capacità, competenze, budget ed opportunità sono molto diversi per ciascuna categoria di hacker



Caratterizzazione degli Hacker

- Gli attacchi condotti da **Terroristi** e **Stati** sono di solito considerati come mirati
 - I **Terroristi** perseguono obiettivi politici o religiosi che tipicamente danneggiano strutture o servizi critici
 - Gli **Stati** (o governi) intendono acquisire quante più informazioni possibili sui loro nemici e talvolta sui loro alleati
- Non tutti i **Terroristi** e non tutti gli **Stati** conducono solo attacchi mirati

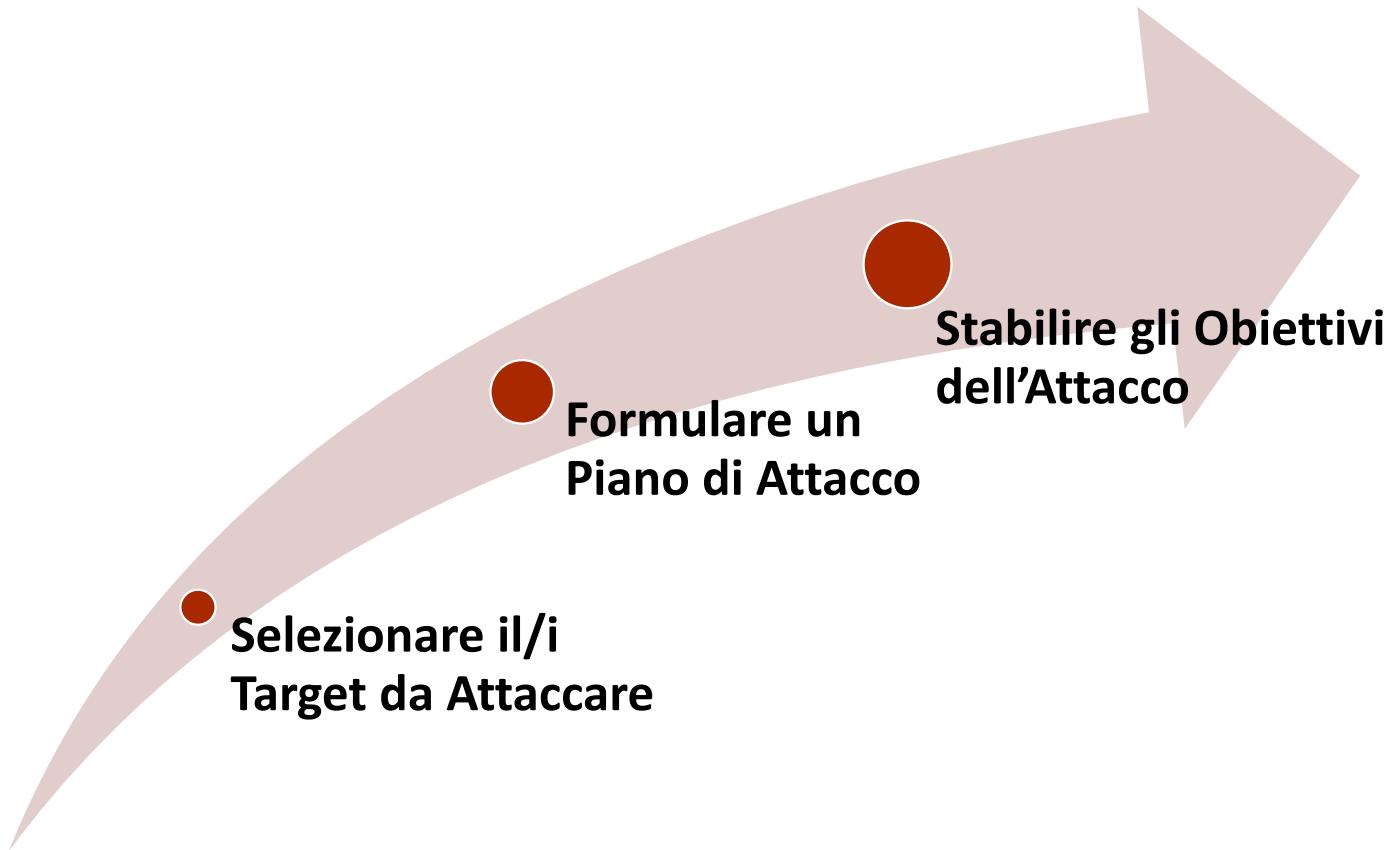
Caratterizzazione degli Hacker

- **Script Kiddie** e **Criminali** sono normalmente più legati ad attacchi non mirati
 - Gli **Script Kiddie** usano di solito strumenti automatici
 - I **Criminali** preferiscono monetizzare i loro sforzi attaccando la massa, ma potrebbero anche attaccare in modo mirato
- Gli **Insider** sono focalizzati su un singolo obiettivo, che è l'azienda (o l'organizzazione) di cui fanno parte
- Gli **Hacktivist** operano per fini sociali o politici e possono attaccare sia in modo non mirato che mirato

Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking

Ethical Hacking Plan



Ethical Hacking Plan

Selezionare il Target da Attaccare

- Il target da attaccare va scelto con estrema cura e non bisogna attaccare il primo bersaglio che capita

- È necessaria una ricerca strategica del potenziale target, eventualmente analizzando le sue abitudini e scegliendo le migliori tecniche (e strumenti) per condurre l'attacco



Ethical Hacking Plan

Formulare un Piano di Attacco

- 1. Otttenere l'approvazione e l'autorizzazione necessaria per effettuare i test di sicurezza (attività di Ethical Hacking)**
 - Contratto firmato
- 2. Accertarsi che i responsabili dell'autorizzazione siano pienamente consapevoli delle attività di Ethical Hacking che si andranno a svolgere**
- 3. Accertarsi che le attività di Ethical Hacking non coinvolgano terze parti (servizi cloud, servizi di web hosting, etc)**
 - In tal caso sarà necessaria l'autorizzazione di tutte le parti coinvolte



Ethical Hacking Plan

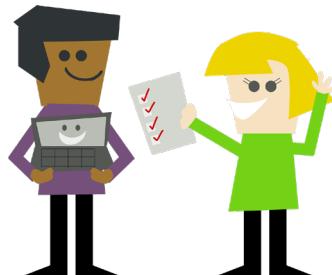
Formulare un Piano di Attacco

4. Determinare le componenti più critiche e vulnerabili, che dovranno essere valutate per prime

- Una volta valutate tali componenti si potrà procedere «a cascata» valutando via via tutte le altre

5. Valutare i rischi

- È importante avere sempre un piano di emergenza nel caso in cui l'attività di ethical hacking non vada a buon fine
- Determinare a priori in che modo le persone ed i sistemi possano essere interessati da tali eventi



Ethical Hacking Plan

Formulare un Piano di Attacco

6. Determinare il programma di test

- Un test potrebbe essere effettuato durante il normale orario di lavoro, al mattino presto o anche in tarda notte
- **N.B.** I Black Hat Hacker non si limitano a momenti specifici per effettuare un attacco
 - Il modo migliore per valutare la sicurezza di un sistema sarebbe quello di avviare qualsiasi tipo di test in qualsiasi momento della giornata
 - Le uniche eccezioni sono tipicamente gli attacchi DoS completi, la sicurezza fisica ed i test basati sull'ingegneria sociale



Ethical Hacking Plan

Formulare un Piano di Attacco

- 7. Acquisire conoscenza dell'asset che si va a testare**

- 8. Definire le azioni da intraprendere nel caso in cui vengano riscontrate vulnerabilità**

- 9. Definire come comunicare le vulnerabilità rilevate a chi ha commissionato l'analisi di sicurezza**

- 10. Definire eventualmente chi deve risolvere le vulnerabilità riscontrate**



Ethical Hacking Plan

Formulare un Piano di Attacco

11. Determinare i risultati/documenti finali attesi da chi ha commissionato l'analisi di sicurezza

- *Penetration Testing Report*, documento di replicabilità, rapporti di scansione dettagliati contenenti informazioni sulle vulnerabilità e raccomandazioni su come risolverle, presentazione digitale, etc

12. Determinare l'insieme degli strumenti necessari per condurre l'analisi di sicurezza

- Strumenti più appropriati per determinati compiti o esigenze



Ethical Hacking Plan

Stabilire gli Obiettivi dell'Attacco

- L'Ethical Hacking mira a scoprire tutte le vulnerabilità di un sistema per impedire agli hacker criminali (Black Hat Hacker) di violarlo

- Per ottenere un'analisi efficace della sicurezza è necessario adottare la stessa mentalità dei Black Hat Hacker



Ethical Hacking Plan

Stabilire gli Obiettivi dell'Attacco

➤ **Definire ed allineare gli obiettivi**

- Gli obiettivi dell'ethical hacker devono essere gli stessi di chi ha commissionato l'analisi di sicurezza
- È anche necessario accordarsi sulle metriche per la valutazione dei risultati dei test

Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- **I Dieci Comandamenti dell'Ethical Hacking**

I 10 Comandamenti dell'Ethical Hacking

1. Stabilire gli Obiettivi

- Di quali informazioni potrebbero disporre gli hacker (criminali) per attaccare un determinato asset?
- In che modo gli hacker (criminali) potrebbero sfruttare queste informazioni?
- L'utente (o l'organizzazione) è a conoscenza di passati tentativi di violazione del proprio asset?



I 10 Comandamenti dell'Ethical Hacking

2. Pianificare Sempre in Anticipo

- La valutazione della sicurezza di un sistema è tipicamente soggetta a vincoli: tempo, risorse (soldi, manodopera), etc

- Il lavoro va quindi pianificato
 - Identificare quali componenti dell'asset devono essere valutate
 - Determinare gli intervalli dei testing
 - Definire in maniera chiara la procedura di testing
 - Creare un piano di testing da condividere con le parti interessate
 - Ottenere l'approvazione del piano



I 10 Comandamenti dell'Ethical Hacking

3. Ottenere Sempre l'Autorizzazione prima valutare la sicurezza di un sistema

- **Si potrebbe incorrere in Rati Penali**
 - Assicurarsi che chi ha commissionato l'analisi di sicurezza (organizzazione, ente, singolo individuo) abbia concesso i necessari permessi tramite opportuni documenti scritti
 - I documenti dovrebbero stabilire che
 - È stata concessa l'approvazione per testare il sistema secondo un piano pre-approvato
 - Il committente supporterà l'hacker etico (pentester) in caso di eventuali spese legali



I 10 Comandamenti dell'Ethical Hacking

4. Essere Etico

- Un hacker etico è vincolato a rispettare requisiti di professionalità, riservatezza e coscienza

- È necessario
- Rispettare sempre il piano precedentemente approvato ed evitare di aggiungere nuovi dettagli in corso d'opera
- Non condividere i risultati dei test di sicurezza con persone non autorizzate
 - Sia all'interno che all'esterno dell'organizzazione che ha commissionato il test



I 10 Comandamenti dell'Ethical Hacking

5. **Tenere Traccia dell'Attività Svolta**, mediante documenti (*registri*) elettronici o cartacei per memorizzare di volta in volta le informazioni ottenute
 - Annotando tutte le attività eseguite
 - Annotando tutti i test eseguiti, comprese le date
 - Avendo sempre una copia di backup dei log
 - Memorizzando in maniera accurata i risultati ottenuti, anche se alcuni test o attività potrebbero non andare come pianificato



I 10 Comandamenti dell'Ethical Hacking

- 6. Proteggere le Informazioni Riservate:** un hacker etico durante la propria attività potrebbe trovare molte informazioni, anche potenzialmente sensibili, in tal caso, esso dovrà
- Rispettare la privacy delle persone e trattare ogni informazione con riservatezza
 - Proteggere e non usare le password ed altre informazioni sensibili trovate durante i test



I 10 Comandamenti dell'Ethical Hacking

- 7. Non Causare Danni:** spesso vengono causati danni imprevisti, è necessario quindi
- Avere sempre un piano ed attenersi ad esso
 - Evitare di causare (anche accidentalmente) interruzioni o di interferire con altre attività
 - Essere a conoscenza degli strumenti che si stanno utilizzando e delle loro implicazioni
 - Scegliere gli strumenti con consapevolezza e leggere sempre la relativa documentazione



I 10 Comandamenti dell'Ethical Hacking

8. Non Usare Strumenti a Caso

- Esistono numerosi strumenti per condurre attività di penetration testing / ethical hacking
- È facile essere tentati dal provarli tutti
 - La maggior parte di essi sono gratuiti e facilmente accessibili
- Meglio concentrarsi solo su alcuni strumenti
 - Di cui è nota l'efficacia e con cui si ha familiarità



I 10 Comandamenti dell'Ethical Hacking

9. Il Processo di Penetration Testing deve essere Sempre Strutturato

- È necessario un processo caratterizzato da
 - Obiettivi quantificabili
 - Coerenza e ripetibilità
 - Permanenza dei risultati
- Sono quindi necessarie metodologie di testing
 - Maggiori dettagli in seguito...



I 10 Comandamenti dell'Ethical Hacking

10. Segnalare e Memorizzare Tutte le Scoperte

- Se durante i test di sicurezza vengono individuate vulnerabilità o minacce nel sistema, queste devono essere immediatamente segnalate e memorizzate tramite l'opportuna documentazione

- Assicurarsi di non tralasciare alcun risultato, non importa quanto insignificante esso possa sembrare
- Tutti i risultati vanno sempre documentati
 - Non è necessario evidenziare nelle parti iniziali della documentazione (*Penetration Testing Report*) tutti i risultati ottenuti
 - È sempre necessario inserire tali risultati nelle descrizioni dettagliate presenti nella documentazione
 - *Maggiori dettagli in seguito...*



Bibliografia

- **Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security.** Gary Hall & Erin Watson. 2016
- Capitoli 1, 2, 3 e 4

