



Penetration Testing & Ethical Hacking

Fondamenti di Ethical Hacking

Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

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

Outline

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

Cosa si Intende per Sicurezza?

- **Sicurezza Completa:** combinazione sinergica di sicurezza Fisica, Digitale ed Umana



Cosa si Intende per Sicurezza?



Sicurezza Fisica

- Analisi di sicurezza perimetrale
- Identificazione di accessi alternativi
- Controlli basati su RFID/NFC
- Controlli tramite dispositivi biometrici
- Illuminazione
- Analisi delle abitudini delle guardie
- Controllo remoto tramite CCTV
- ...



Sicurezza Digitale

- Analisi di sistemi perimetrali
- Analisi di server pubblici
- Controllo di domini interni
- Controllo di sistemi industriali
- ...



Sicurezza Umana

- Controlli su Phishing di massa
- Controlli su Phishing mirati
- Controlli su Vishing
- Controlli su Malware
- Controlli su USB Bait
- Controlli su Impersonificazione
- ...

**Per garantire la sicurezza nelle diverse dimensioni (Fisica, Digitale ed Umana)
vengono svolte diverse azioni**

Cosa si Intende per Sicurezza?

- I tre tipi di sicurezza sono strettamente correlati
 - Dispositivi digitali sono spesso utilizzati per garantire l'accesso in determinate aree fisiche
 - Senza proteggere adeguatamente una determinata area fisica, tutti i dispositivi digitali potrebbero essere compromessi localmente



Violazione Sicurezza Fisica

Esempi

- Analisi delle protezioni perimetrali per raccogliere informazioni sulle misure di sicurezza fisica messe in atto
 - Dopo l'intrusione si potrebbe collegare un dispositivo alla rete, estendendo la violazione della sicurezza fisica alla dimensione digitale



Violazione Sicurezza Fisica

Esempi

- Alcune porte possono essere aperte dall'interno grazie ad un sensore di movimento
- Le porte non sono perfettamente sovrapposte e possono essere aperte anche dall'esterno usando uno spray



<https://www.youtube.com/watch?v=xcA7iXSNmZE>

Violazione Sicurezza Fisica

Esempi

- Sfruttamento delle schede RFID/NFC
 - Diffuse in molti ambiti pubblici e privati
 - Utilizzano spesso configurazioni predefinite che consentono una facile duplicazione o clonazione



Violazione Sicurezza Fisica

Esempi

- Violazione di sistemi biometrici, guasti all'illuminazione, recinzioni facili da saltare, telecamere a circuito chiuso mal posizionate, etc



Violazione Sicurezza Digitale

- Tipicamente segue uno specifico pattern di attacco
 1. Utilizzo di tecniche per l'anonimia in rete (protocolli di tunneling, VPN, proxy, proxy chain, reti anonime, etc)
 2. Scelta del sistema (o dei sistemi) da attaccare
 3. Raccolta di informazioni sul sistema da attaccare
 4. Analisi delle vulnerabilità del sistema
 5. Realizzazione (o utilizzo) di strumenti per lo sfruttamento delle vulnerabilità rilevate (*exploit*)
 - Utilizzo di questi strumenti per accedere al sistema
 6. Realizzazione (o utilizzo) di strumenti per mantenere il controllo del sistema (*backdoor*) ed elevazione dei privilegi all'interno di esso

Durante il corso ci occuperemo prevalentemente di questi aspetti



Violazione Sicurezza Umana

Esempi

- Sviluppo di campagne di phishing
- Sviluppo di malware ad hoc
- Diffusione di pendrive USB infette (**USB bait**)
 - Una volta collegate ad un sistema da parte di utenti che hanno lecito accesso al sistema stesso, eseguiranno software dannoso



Tipi di Attacchi

- I sistemi sono sempre più complessi e vulnerabili
 - Il numero sempre crescente di dispositivi e tecnologie utilizzate aumenta la superficie di attacco
 - Più complesso è un sistema e più difficile risulta controllarlo
- In generale gli attacchi appartengono a tre categorie principali
 - Attacchi Fisici
 - Attacchi Sintattici
 - Attacchi Semantici

Attacchi Fisici

- Utilizzo di metodi tradizionali per «distruggere» i dati
 - Fiamme, Esplosivi, etc
- Possono anche riguardare l'intrusione in edifici ed il furto di apparecchiature
 - Anche rovistando tra la spazzatura è possibile trovare informazioni preziose (ad es., password, diagrammi di rete, note, etc)



Attacchi Sintattici

- Sfruttano vulnerabilità tecniche o errori nel codice di un sistema informatico per comprometterne il funzionamento, ottenere accesso non autorizzato o causare danni
- Utilizzo di malware o di altre tipologie di software malevolo per violare o «disturbare» il normale funzionamento di un sistema
- Esempi di attacchi sintattici
 - Iniezione di codice (es. SQL Injection, XSS)
 - Exploit di bug software
 - Denial of Service (DoS/DDoS)
 - Malware (virus, worm, trojan)



Attacchi Semantici

- Non sfruttano direttamente vulnerabilità tecniche, ma piuttosto errori umani, inganni o tecniche psicologiche per ottenere accesso o influenzare il comportamento
- Esempi di attacchi semantici
 - Phishing
 - Social Engineering
 - Fake News & Disinformazione
 - Typosquatting
- Quindi gli attacchi sintattici colpiscono il codice ed i sistemi informatici, mentre quelli semanticci mirano a ingannare le persone e manipolare le informazioni



Obiettivo degli Attacchi

- Tutti gli attacchi sono di solito classificati come
 - Mirati
 - Non Mirati (o Generici)



Attacchi Mirati

Pattern di Attacco

➤ L'attaccante

1. Raccoglie tutte le informazioni disponibili sull'asset
2. Analizza tali informazioni, per trovare un metodo di accesso all'asset (**vettore**)
3. Si garantisce la persistenza nell'asset, installando meccanismi di accesso non rilevabili (*backdoor*)
4. Ottiene il controllo di altri sistemi nell'asset, fino a raggiungere l'obiettivo finale (Tipicamente l'Accesso ai Dati 5.)
6. Esce dall'asset

Attacchi Mirati

Svantaggi

- Richiedono tempo, motivazioni, denaro, competenze, esperienza, etc
- Non tutti sono in grado di condurre/supportare tali attività



Attacchi Non Mirati (o Generici)

- Utilizzano malware o mezzi automatizzati, come campagne di phishing o di «massive exploitation»
 - Esempio: data una vulnerabilità per una specifica versione di WordPress, si potrebbe eseguire un exploit per violare tutti i server che hanno installato tale versione di WordPress
- Attacchi più economici e meno complessi, che possono causare danni molto gravi
 - Ad es., Ransomware

Attacchi

Come Rilevarli

- Alcuni «indizi» permettono di rilevare un attacco
 - Livello insolitamente alto del traffico di rete in uscita quando non si stanno effettuando download/upload
 - Livelli elevati di attività del disco
 - Comparsa di file o directory «sospette»
 - Servizi o processi «sospetti»
 - Grande quantità di dati in ingresso (ma eventualmente anche in uscita) «bloccata» dal firewall
 - Trojan e backdoor rilevati dall'Antivirus (AV)
 - Etc



Attacchi

Come Proteggersi

- Non esiste una «regola generale», ma alcune linee guida possono essere di grande aiuto
- Aggiornare costantemente i sistemi che si utilizzano
 - Sistema operativo, applicativi, etc
- Utilizzare ed aggiornare costantemente gli strumenti di sicurezza
 - Antivirus, Firewall, IDS/IPS, etc
- Disabilitare tutti i servizi di rete non necessari
- Gestire l'accounting degli utenti secondo il *Principio del Privilegio Minimo*



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

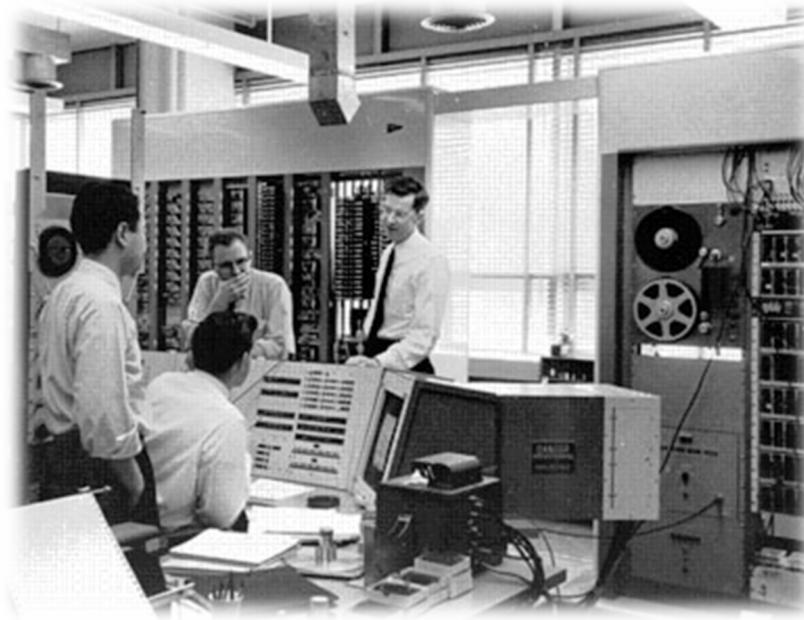
- I membri del TMRC furono i primi ad essere considerati hacker
- Presero le apparecchiature che avevano a disposizione e ne fecero un uso del tutto innovativo e non convenzionale



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 telefonica 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

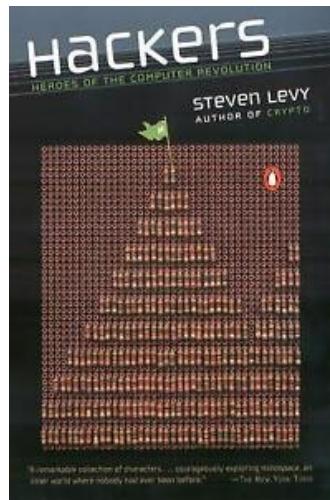
Anni '80 – Hacker Ethic

«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 vulnerabilità e potenziali minacce, fornendo eventualmente anche soluzioni su come risolverle, mitigare o prevenirle



Tipologie di Hacker

White Hat Hacker

- Garantiscono tipicamente il rilascio pubblico di aggiornamenti per correggere le vulnerabilità rilevate
- Sono costantemente alla ricerca di nuove vulnerabilità in sistemi e dispositivi per renderli più sicuri
- Sono tipicamente 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
 - Maggiori dettagli in seguito...



Tipologie di Hacker

Grey Hat Hacker

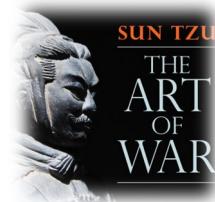
- Oltre a cercare vulnerabilità per renderle note e correggerle, talvolta svolgono anche alcune attività illecite o «immorali»
- Sono spinti da interessi economici oltre che etici
- Tendono ad usare sia mezzi leciti che illeciti per violare un sistema

- 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

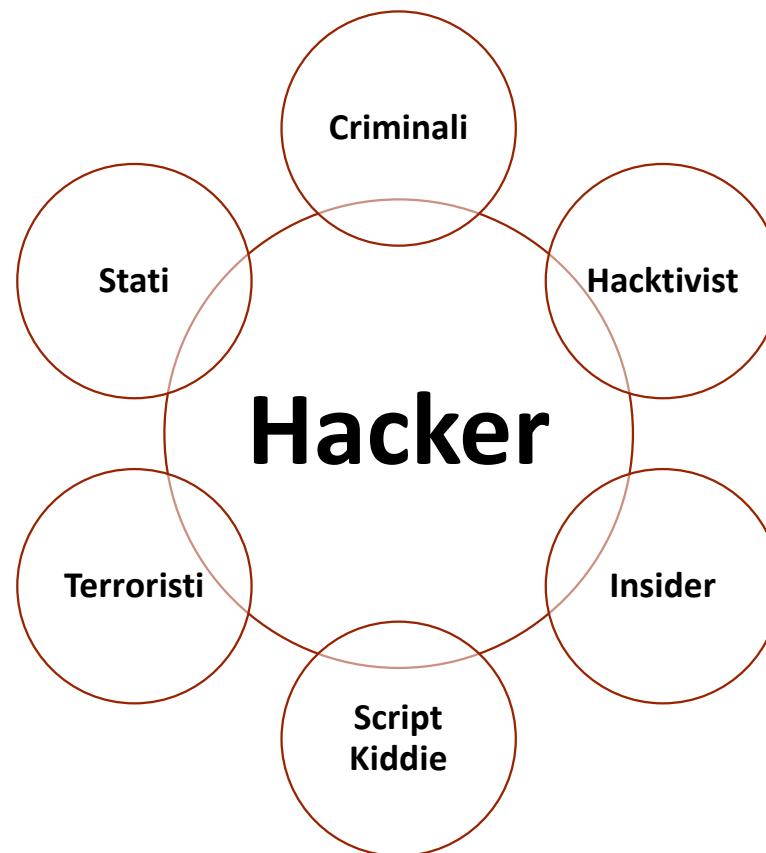


«Se conosci il nemico e te stesso la tua vittoria è sicura»
Sun Tzu, L'arte della guerra
VI - V secolo a.C.

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

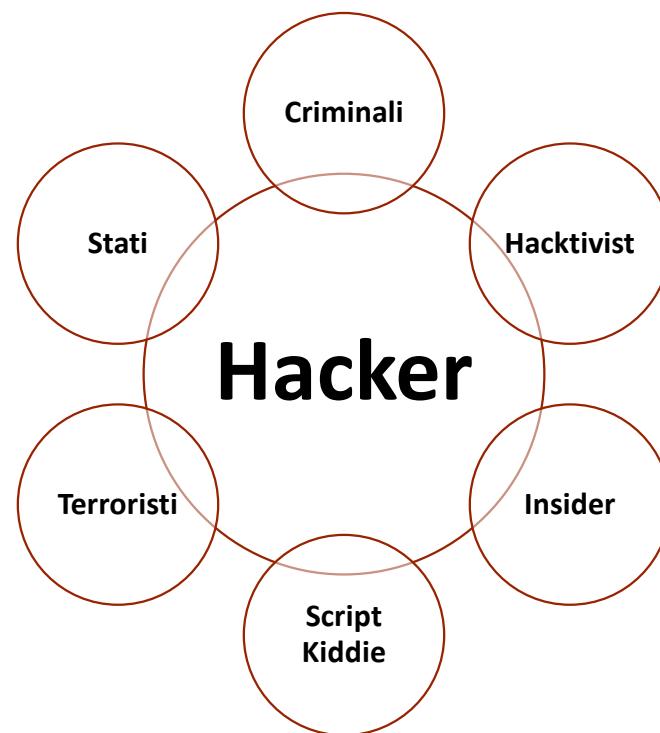
Caratterizzazione degli Hacker



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

Caratterizzazione degli Hacker

- Motivazioni, capacità, competenze, budget e tipi di attacchi condotti 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** persegono 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

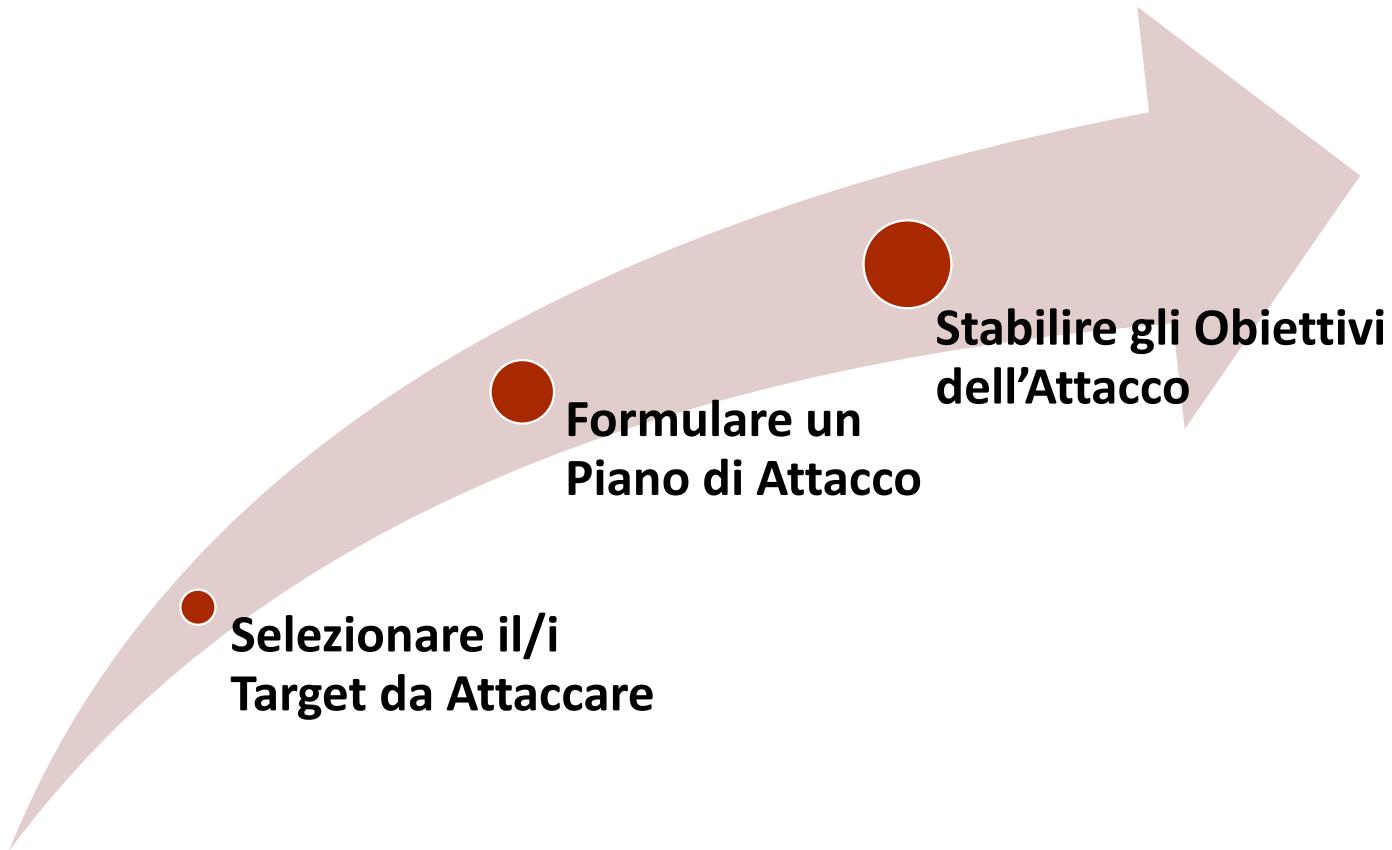
Caratterizzazione degli Hacker

- **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 accurata 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

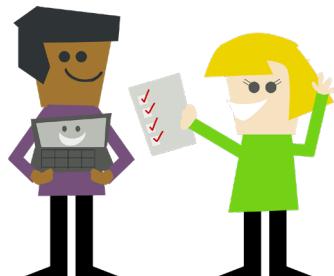
Formulare un Piano di Attacco

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