Attacchi

*Appunti di **Giuseppe Pitruzzella** - Corso di Internet Security @ DMI, UniCt*

Il concetto di sicurezza può essere definito come la prevenzione degli attacchi pur mantenendo usabile il sistema, ovvero la piena funzionalità del sistema.

Attacco reale: furto del dispositivo

Iniziamo a studiare la tassonomia a partire da una prima tipologia di attacco: l'**attacco fisico**. Ogni attacco di questa tipologia prevede un **attacco fondamentale**.
Immaginiamo, quindi, che un attaccante si trovi in mano un dispositivo rubato o penetretion tester che deve verificare la sicurezza di un dispositivo

Lo scenario ipotetico su cui si basano gli attacchi fisici che studiamo si basano su un attaccante
Gli attacchi che studiamo all'interno di questo paragrafo si basano su uno dei seguenti due scenari:
(i) un *penetration-tester* che deve verificare la sicurezza di un dispositivo o (ii) un *attaccante* che vuole *bypassare* la sicurezza di un dispositivo che è stato rubato, due scenari che si basano sulla stessa *cyber-kill-chain*.

> [$Approfondimento$] Una **cyber-kill-chain**, un concetto pubblicato da *Lockheed Martin*, la principale industria americana nel settore della difesa, è una procedura che descrive la struttura dei passi che genera l'intrusione/attacco. L'analisi della *kill chain* permette di capire come un avversario per raggiungere il suo obiettivo debba riuscire a progredire attraverso tutta la catena, mettendo bene in evidenza quali azioni di mitigazione sono efficaci per interrompere la *kill chain* stessa.

Una *cyber-kill-chain* semplificata che studiamo all'interno del corso è la seguente:

1. **Accedere al sistema** (*attacco fondamentale*).
   Per accedere al sistema è necessario violare l'autenticazione, unica **contromisura** rispetto questo attacco fondamentale, la quale può essere formata da autenticazione biometrica e/o password alfanumeriche.
   Purtroppo, sappiamo bene che questa contromisura è facilmente violabile a partire dai metodi studiati nei $mini - challenge$. Abbiamo visto, infatti, che esiste un modo per violare sia sistemi Linux che sistemi Windows (entrambi prevedono di ottenere una shell con i permessi di amministratore).
   1.1 **Sfruttare le funzionalità del sistema**, si pensi per esempio all'utilizzo della potenza computazionale della cpu di una macchina o all'utilizzo dello spazio del suo disco. In questo caso, parliamo di **cyber-security**.
   Una **contromisura** rispetto questa attività è l'autenticazione rispetto la specifica funzionalità (per esempio l'autenticazione al servizio o app). Purtroppo, questa contromisura spesso fallisce in scenari in cui le password vengono salvate dal browser o app.
   1.2 **Aquisizione di dati sensibili** all'interno della macchina. In questo caso, parliamo di **privacy** o *data-protection*, ovvero la *cyber-security* istanziata al dato. Una **contromisura** rispetto questa attività è la crittografia dei dati. Purtroppo, spesso vi è molta riluttanza verso la codifica o cifratura di un unità.
   [*NB*] In generale la privacy include anche degli aspetti funzionali di cui gode il proprietario del dato.

Attacco reale: pirateria digitale

Distinguiamo diversi tipi di pirateria digitale, ovvero:

- **Furto di proprietà intellettuale**, per es. rispetto un film, il quale viene scaricato illegalmente. Chiaramente questa era una attività popolare durante i primi anni duemila. Con il passare degli anni, infatti, il furto è sempre meno effettuato poichè è cambiato il modello di business legato alle proprietà intellettuali. Quest'ultimo modello è basato sull'acquisto ad prezzo inferiore di servizi che prevedono di poter visualizzare quest'ultime (vedi per es. Netflix).

  > [$Approfondimento$] Il termine **watermark**, si riferisce all'inclusione di informazioni all'interno di un file multimediale o di altro genere, che può essere successivamente rilevato o estratto per trarre informazioni sulla sua origine e provenienza. In altre parole, il watermarking dimostra la proprietà di un file multimediale e vuole essere una contromisura verso l'abuso del prodotto. Quest'ultimo potrebbe non essere visibile e non è possibile rimuoverlo. Una tecnica banale di watermarking è l'encoding nei bit meno significativi dei pixel.

- **Furto di identità**, per es. effettuare l'autenticazione come se fossimo il proprietario della macchina. Ancora una volta vale l'autenticazione come unica contromisura.
- **Furto di marchio**.

Tassonomie di attacchi

Notiamo adesso la tassonomia degli attacchi, dagli attacchi di attacchi criminali fino agli attacchi per scopi pubblicitari. Il tutto è rappresentato graficamente attraverso l'immagine sottostante.