Costruire una password robusta

La definizione di robustezza è variata nel tempo e ad oggi non ci aspettiamo che la password sia il solo strumento di protezione da intrusioni indebite.

Una "buona" password bilancia al meglio possibile la difficoltà di indovinarla con la menmonicità.

Molti attacchi informatici sono legati alla violazione dei sistemi di autenticazione. Il riutilizzo di password su più sistemi spesso è causa di problemi. Con un minimo di social engineering è facile scoprire una password utilizzata più volte. Vedi ad esempio i **password reuse attack**.

Il **NIST** nel **2004** ha stabilito gli standard per le password sicure. Lunghezza, lowcase, uppercase, numeri e caratteri speciali come le conosciamo oggi. Ha rivisto gli standard nel **2017** consapevole della memonicità, chiedendo di utilizzare password semplici ma con un controllo sulla soglia dei possibili inserimenti.

Nonostante le linee guida sono state date ancora ad oggi tanti molti enti non sono conformi.

Firewall

Il firewall è una **difesa perimetrale** per ambiti diversi. Come le misure già discusse, non garantisce protezione a 360 gradi, sebbene se combinata ad altri strumenti e ben configurato possa garantire protezione adeguata da alcuni tipi di minacce. Un esempio di minaccia che non può contrastare è ad esempio l'**insider threats** (letteralmente una minaccia dall'interno).

Definizione di sicurezza

📝 **Domanda d'esame** - 📔 **Definizione**: Dare una definizione (per punti) di sicurezza:

- **non è un prodotto ma un processo**;
- anello più debole di una catena;
- espresso da che cosa (complemento di causa efficiente).
  Non esiste un concetto assoluto di sicurezza, ma specificato **da che cosa il sistema è al sicuro**;
- sempre soggetta ad **analisi costi/benefici** dell'attaccante
  (permette di individuare chi è l'attaccante. Coerentemente con il punto precedente, si può scegliere di essere protetti contro cosa x ma non contro cosa y);
- si realizza in pratica mediante **livelli di sicurezza**
  (il sistema è sicuro da questo tipo di attaccanti ma non da quest'altro)

La sicurezza è un processo in continua esecuzione, prevede procedure in continua evoluzione, processi continui. Prevede anche dei piani per la prevenzione e la gestione degli incidenti più disastrosi. In casi simili infatti bisogna garantire la **continuità operativa**. Ci sono inoltre degli standard per gestire gli incidenti.

Rischi base per la sicurezza

Il sistema che si vuole proteggere è sempre più complesso di quanto si possa pensare, soprattutto nel momento in cui più sistemi vengono combinati ed iniziano ad interagire tra loro (**sicurezza punto-punto** come sicurezza di molteplici sistemi, ad esempio un dispositivo che accede alla rete WIFI. In questo caso il sistema nel complesso diviene meno "sicuro" rispetto ai singoli sistemi)

Bug

Un bug è una proprietà inattesa. **Il discriminante tra bug e feature è l'intenzionalità, quindi sta nella policy.**

Proprietà emergenti

Se inventiamo sistemi nuovi abbiamo proprietà nuove da considerare. Queste possono destabilizzare il nostro sistema.

Interazione con l'essere umano

L'essere umano va visto come una vulnerabilità del sistema.

📝 **Domanda d'esame**: quali sono i **rischi base per la sicurezza**?

Rischi digitali per la sicurezza

1. **Automazione dell'offensiva**
    - microfurti
    - violazioni (quasi intracciabili)
    - privacy a rischio (esfiltrazioni di dati)
2. **Assenza della distanza**
    - in rete siamo esposti, i nostri siti sono esposti.
      Potenzialmente chiunque è contro di noi perché non ci sono limiti di distanza.
    - L'aspetto giudiziario è complesso perché mentre il web è senza limiti, le leggi sono soggette a territorialità.
      È spesso difficile ricondurre un crimine ad una precisa legislazione.
3. **Propagazione delle tecniche**
    - Le tecniche si propagano con estrema velocità
    - Diventare offensivi non implica abilità
4. **Difficoltà di reazione/risposta**
    - L'**incident response** è complicato.
      (Come faccio **route cause analysis**? Cosa faccio quando ho trovato un problema?)

📝 **Domanda d'esame**: perchè la sicurezza è un problema?
Esempio di risposta: vanno descritti sia i problemi base che questi indicati in questa sezione.

Il gioco della sicurezza

Il gioco della sicurezza è un continuo loop tra attacco e difesa. Questo è coerente con quanto detto sulla sicurezza come processo.

Metodologia di attacco:

- Studio il sistema target
- Ricerca dei punti deboli
- Disegnare o utilizzare un eseguibile già esistente per verificare i punti deboli
- Ripetere

Metodologia di difesa:

- Proteggersi come meglio si può, utilizzando gli strumenti a disposizione
- Aggiornare il sistema quando richiesto
- Monitorare il sistema
- Ripetere

Terminologia

- **Red team:** chi esegue l'attacco
- **Blue team**: chi si difende

Porte di sistema

📔 **Definizione**: **port, an addressable network location implemented inside of the operating system.**
Una locazione di rete indirizzabile, esponibile.

Port scanning: scansionare le porte, provare a collegarsi e capire quali sono aperte e quali servizi sono in funzione.
Problema del ladro: capire quale processo c'è dietro, se è vulnerabile, senza farlo capire, in modo tale che non si riesca a rispondere di conseguenza.

Esempio di analisi per l'attacco: verificare che versione di deamon del processo c'è in ascolto su una certa porta per capire quali vulnerabilità **già note** ha. Ad esempio, versione 1 di finger magari ha una certa vulnerabilità, trovandolo attivo è possibile sfruttarla.

Nmap: overview

Attraverso il tool nmao è possibile effettuare una scansione **stealtyness** (scansione invisibile ai processi attaccati).
Più la scansione è aggressiva più sarà facile rilevarla.

Si può così osservare quali servizi sono attivi (**comprensione del target**) e in base ai servizi attivi scegliere il tipo di attacco da eseguire. Questi strumenti di diagnostica sono anche i primi strumenti offensivi.

Intrusion detection system: overview

Un intrusion detection system verifica le intrusioni, è spesso configurabile. Se la configurazione è troppo aggressiva si hanno molti falsi positivi, se invece risulta essere troppo morbida potrebbe non rilevare le intrusioni. Quello della "giusta configurazione" è un problema aperto quindi e spesso bisogna trovare delle euristiche e affidarsi alla statistica.

```
# bin/bash!
# Esempio di uno script di intrusion detection
# Trova i file con il bit SUID impostato
cd // && find / -type f -perm -u=s -iname ".*" 2>/dev/null
```

Elenco di lettura

- NIST Password Guidelines
- Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques
- Incident response, cos'è e come funziona passo per passo: ecco cosa fare
- Why Light Bulbs May Be the Next Hacker Target
- MITRE ATT&CK