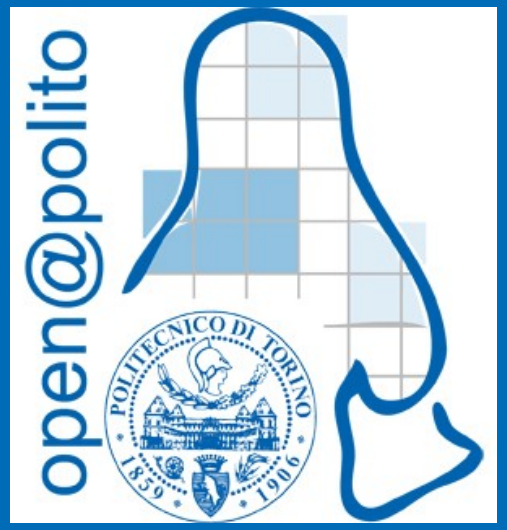
CYBERSECURITY

Di Christian Piazzolla

Con il supporto di:



Cosa intendiamo per cybersecurity?

Spoiler: NON è essere inattaccabili a livello informatico.

Il rischio 0 non esiste: la sicurezza informatica non predispone ad un sistema perfetto, bensì ad alzare il **costo d'attacco**, rendendolo così sconveniente.

L’approccio moderno alla sicurezza informatica

L'approccio moderno non è più costruire un muro altissimo attorno al sistema sperando che nessuno entri. L'approccio moderno è: *qualcuno è già entrato*. Come limitiamo i danni?

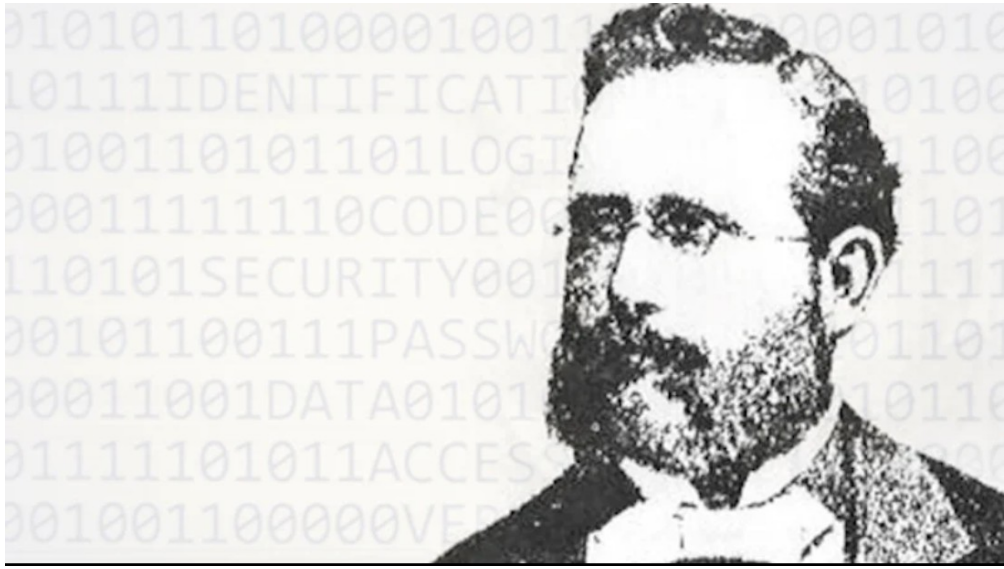
Questa pratica prende il nome di: **Assume Breach**

Fonte:
https://cyberdivision.net/2020/09/21/attacchi-informatici/

Un sistema Open Source è più o meno sicuro?

Principio di Kerckhoffs:

Nel 19° secolo, Auguste Kerckhoffs teorizzò che un sistema crittografico deve rimanere sicuro anche se tutto il suo funzionamento è di dominio pubblico, tranne la chiave.



Differenze tra Open Source e Closed Source

Closed Source

- Security by Obscurity: nascondere il codice sorgente rende più difficile trovare vulnerabilità.
- Gli hacker usano strumenti di *reverse engineering, sniffing, fuzzing...*
- Modello di fiducia centralizzato: L'utente si fida del vendor.

Open Source

- Security by Design: il codice è pubblico e verificabile da chiunque.
- La legge di Linus: Dato un numero sufficiente di occhi, tutti i bug verranno rivelati.
- Modello di fiducia: L'utente può verificare in prima persona o fidarsi di audit di sicurezza pubblici esterni.
- Storicamente patch di vulnerabilità molto più veloci ed efficienti.

La realtà dei fatti, però, è molto più complessa!

Sicurezza in Linux

Cos'è il MAC (Mandatory Access Control)?

SELinux

- Lega le regole agli inode del filesystem, assegnando un'etichetta ad ogni singolo file.
- Granularità estrema, difesa molto elevata anche quando il file viene rinominato, spostato o linkato.
- Filosofia: sicurezza totale (Default Deny)

Apparmor

- Lega le regole di sicurezza ai percorsi del filesystem (es. /usr/bin/nginx).
- Profili in testo, semplici da leggere, scrivere e gestire.
- Filosofia: protezione "Good enough", ottimo equilibrio tra sicurezza ed usabilità del sistema.

ATTENZIONE: La complessità è nemica della sicurezza!

PRATICHIAMO

L’illusione delle password

Il Vettore d'Attacco: Accesso fisico al dispositivo non cifrato.

- **La Tecnica:** Manipolazione dei parametri del kernel (init=/bin/bash).
- **Il Risultato:** Bypass totale del sistema di init (systemd) e acquisizione immediata di una shell root.

Le Difese (Defense in Depth):

- Blocco del Bootloader (Password su GRUB).
- Cifratura dei dati a riposo (LUKS / Full Disk Encryption).

PRATICHIAMO

Isolamento dei processi: Sandboxing e firejail

- **Il Limite del Modello DAC (Permessi standard):** Se l'utente esegue un malware, il malware ha i permessi dell'utente.
- **Il Paradigma "Assume Breach":** Limitare i danni assumendo che l'applicazione sia già compromessa.
- **La Soluzione (Namespaces):** Creare ambienti isolati e temporanei per singole applicazioni.

Q&A