

GLOSSARIO

TERMINOLOGIA E DEFINIZIONI FONDAMENTALI NEL CAMPO DELLA
SICUREZZA INFORMATICA

Fonti:

- *Joda - Io Hacker*
- *Treccani - Antivirus*

DEFINIZIONE

È una qualsiasi vulnerabilità di sicurezza informatica non espressamente nota allo sviluppatore o alla casa che ha prodotto un determinato sistema informatico; definisce anche il **programma** detto **exploit**, che sfrutta questa vulnerabilità informatica per consentire l'esecuzione anche parziale di azioni non normalmente permesse da chi ha progettato il sistema in questione. **Vengono chiamati 0-day proprio perché sono passati zero giorni da quando la vulnerabilità è stata conosciuta dallo sviluppatore e quindi lo sviluppatore ha avuto “zero giorni” per riparare la falla nel programma prima che qualcuno possa scrivere un exploit per essa.**

Curiosità
Project Zero

DEFINIZIONE

Applicazione informatica che svolge una **funzione di blocco, controllo ed eventualmente rimozione di altre applicazioni** progettate per attaccare e danneggiare in vario modo il software di base e applicativo di un computer. L'antivirus contiene funzionalità che ne permettono l'**aggiornamento frequente via Internet**, per garantire una tempestiva protezione anche dai più recenti attacchi.

Approfondimento

Il tuo Antivirus potrebbe spiarti

DEFINIZIONE

Termine che deriva dall'inglese “to crack” ovvero “rompere”, identifica genericamente i **criminali informatici**. Viene spesso sostituito erroneamente con il termine hacker.



Figura 1: creata con Gemini

DOXING

DEFINIZIONE

Pratica di **raccogliere e pubblicare online informazioni personali e sensibili su un individuo senza il suo consenso**, spesso con l'intento di molestare, intimidire o danneggiare quella persona. Queste informazioni possono includere indirizzi, numeri di telefono, dettagli finanziari e altro ancora.



Figura 2: creata con Gemini

DEFINIZIONE

Termine che rappresenta una comunità di **esperti informatici** molto vasta, con competenze comuni, approcci comuni alla risoluzione dei problemi, con dei tratti simili per alcuni comportamenti, ma molto diversi tra loro. Si differenziano soprattutto per le intenzioni e le modalità con cui agiscono.

- **Black Hat:** Hacker che non agisce secondo la legge, infrangendola con scopi malevoli per recare danno a persone, cose, aziende o governi. Agisce di solito per un proprio tornaconto personale (denaro, gloria, fama o ideologie estreme);

DEFINIZIONE

- **White Hat:** Hacker che agisce all'interno della legalità e quando viola i sistemi, le reti o i software, lo fa su richiesta di aziende, polizia o governi, oppure per verificare la vulnerabilità e tenuta dei sistemi e garantire una maggiore sicurezza informatica. Agisce come un Black Hat ma per motivi opposti.

Oggi si definiscono **Etical Hacker**;

Curiosità

Programma Bug bounty

- **Gray Hat:** Hacker solitamente attivista che animato da buone intenzioni infrange la legge, ad esempio per segnalare ad aziende delle vulnerabilità che in mano a Black Hat potrebbero causare gravi danni. A volte crea un dilemma etico che la legge, gli avvocati, i giudici, ma anche la gente comune, deve affrontare per giudicare le sue azioni: Quando non si tratta di Black Hat ma di Gray Hat? Qual è il confine tra etica e illegalità?

DEFINIZIONE

In italiano: “Zoppo”, viene utilizzato per indicare qualcosa o qualcuno di rozzo. Le attività dei Lamer sono grossolane, anche se riescono a fare dei danni o a violare delle reti o rubare delle password, **in genere sono persone molto poco preparate e poco propense allo studio, che usano tool inventati da altri per fare danni.**



Figura 3: creata con Gemini

DEFINIZIONE

Il **Penetration Test** viene condotto su più fasi dal punto di vista di un potenziale attaccante e **simula l'attacco informatico di un utente malintenzionato**. Il test sfrutta le **vulnerabilità conosciute** o rilevate, aiutando così a determinare se le difese del sistema sono sufficienti o se invece sono presenti altre vulnerabilità, elencando in questo caso in un report quali difese il test ha sconfitto.

Approfondimento

Esempio di azienda che offre Penetration Test

DEFINIZIONE

I **tools di rete** sono **software progettati per monitorare, analizzare e gestire le reti informatiche**. Questi strumenti aiutano gli amministratori di rete a garantire la sicurezza, l'efficienza e la funzionalità delle reti. Di seguito alcuni tools comunemente usati:

- **Shodan**: motore di ricerca per dispositivi connessi a Internet, utile per identificare vulnerabilità e configurazioni errate;
- **Wireshark**: analizzatore di protocolli di rete che consente di catturare e analizzare il traffico di rete;