Attacchi Informatici

Leone Matteo Pio V L

30 novembre 2023

Indice

1 Introduzione agli attacchi informatici

Che cosa sono gli attacchi informatici?

Gli attacchi informatici sono azioni malevole o tentativi deliberati di compromettere la sicurezza dei sistemi informatici, dei dati o delle reti. Questi attacchi possono essere eseguiti da singoli hacker, gruppi organizzati o addirittura da governi, e mirano a ottenere accesso non autorizzato, danneggiare sistemi, rubare informazioni sensibili o interrompere il normale funzionamento di servizi o reti.

Cosa sono gli hacker?

Gli hacker sono individui o gruppi di persone che utilizzano le proprie abilità tecniche e conoscenze informatiche per accedere a sistemi informatici, reti, dispositivi o dati in modo non autorizzato e possono avere diversi obiettivi:

- **Violazione della sicurezza**: Ottenere accesso non autorizzato a sistemi o dati sensibili.
- **Furti o frodi**: Rubare informazioni personali, dati finanziari o proprietà intellettuale.
- **Danno**: Compromettere o danneggiare sistemi, dati o reti.

Il termine "hacker" può avere diverse sfumature a seconda del contesto:

- **Hacker Etici (White Hat)**: Sono esperti di sicurezza informatica che utilizzano le loro competenze per identificare e risolvere vulnerabilità nei sistemi, spesso su richiesta o con il consenso del proprietario del sistema.
- **Hacker Cracker (Black Hat)**: Questi hacker eseguono attività illegali. Sfruttano le loro competenze informatiche per accedere a sistemi o dati senza autorizzazione, commettendo frodi.
- **Hacker Neofiti (Script Kiddies)**: Individui che, senza avere conoscenze approfondite, utilizzano strumenti e script predefiniti per eseguire attacchi informatici di base.

2 Principali attacchi informatici

Quali sono i principali attacchi informatici?

Esistono diverse tipologie di attacchi informatici, ognuna con obiettivi e modalità d'azione specifiche:

- **Malware**: Software dannoso progettato per infiltrarsi nei sistemi e causare danni, come virus, worm, trojan, ransomware, spyware, etc..
- **Phishing**: Utilizzo di messaggi falsi (e-mail, messaggi istantanei, chiamate telefoniche) che sembrano provenire da fonti attendibili al fine di ottenere informazioni sensibili come password, dati finanziari o informazioni personali.
- **Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)**: Tentativi di rendere inutilizzabile un servizio, un sito web o un'applicazione sovraccaricandolo con traffico eccessivo (DoS) o proveniente da numerose fonti (DDoS).
- **Attacchi di Ingegneria Sociale**: Manipolazione psicologica degli utenti per ottenere informazioni riservate o per eseguire azioni non autorizzate.
- **Attacchi Zero-Day**: Sfruttano falle di sicurezza sconosciute o appena scoperte nei software prima che venga creata una soluzione per proteggere i sistemi.
- **Brute Force**: entativi di accesso non autorizzato ai sistemi provando molteplici combinazioni di password finché non viene individuata quella corretta.
- **Sniffing e Spoofing**: L'intercettazione di dati in transito attraverso una rete (sniffing) o la falsificazione dell'identità o degli indirizzi IP per mascherare la vera identità del mittente (spoofing).
- **Attacchi ai dispositivi IoT**: Sfruttamento delle vulnerabilità dei dispositivi connessi a Internet, come telecamere, termostati, ecc., che spesso hanno protezioni di sicurezza più deboli.

Questi sono solo alcuni esempi di attacchi informatici, ma esistono molte altre tecniche utilizzate dagli hacker per compromettere la sicurezza informatica.

3 Principali metodi difensivi

Le difese contro gli attacchi informatici sono fondamentali per proteggere sistemi, reti e dati sensibili. Ecco alcune misure difensive comuni:

- **Firewall**: Questo strumento aiuta a monitorare e controllare il traffico di rete in ingresso e in uscita, bloccando potenziali minacce.
- **Software Antivirus**: Programmi progettati per rilevare, bloccare e rimuovere virus, malware e altre minacce informatiche dai dispositivi.
- **Accesso con privilegi minimi**: Limitare l'accesso e i privilegi degli utenti solo a ciò di cui hanno bisogno per svolgere il loro lavoro può ridurre la superficie di attacco.
- **Autenticazione a più fattori (MFA)**: L'autenticazione a più fattori richiede più di una forma di verifica (come password e un codice inviato al telefono) per accedere ai sistemi, migliorando la sicurezza.
- **Sicurezza fisica**: Proteggere l'accesso fisico ai server e ai dispositivi è altrettanto importante quanto la sicurezza informatica per impedire l'accesso non autorizzato.
- **Crittaggio dei dati**: Utilizzare algoritmi crittografici per proteggere i dati sensibili, in modo che siano illeggibili per chiunque non autorizzato a visualizzarli.
- **Monitoraggio e rilevamento delle minacce**: Utilizzare sistemi e strumenti di monitoraggio per rilevare attività sospette o intrusioni nei sistemi in tempo reale.

4 Analisi dei princiapli attacchi

Sniffing

Lo "sniffing" è una pratica informatica attraverso la quale un hacker intercetta e monitora il traffico di rete al fine di raccogliere informazioni sensibili come username, password, dati finanziari o qualsiasi altra informazione confidenziale che venga trasmessa in chiaro attraverso la rete, eseguito da software chiamati "packet sniffer", come Wireshark. Per proteggere i dati sensibili dal "sniffing" e da altri tipi di intercettazioni, è fondamentale utilizzare connessioni sicure e criptate, come ad esempio HTTPS anziché HTTP per navigare su Internet, utilizzare reti Wi-Fi sicure e affidabili, e implementare protocolli di sicurezza come VPN.

Spoofing

Lo "spoofing" è una tecnica informatica in cui un individuo o un programma modifica o falsifica deliberatamente le informazioni di identità o origine per mascherare la propria vera identità o per far sembrare che l'origine dei dati sia diversa da quella reale. può essere utilizzato per scopi malevoli, come l'inganno, l'ingegneria sociale o per eseguire attacchi informatici. Le misure di difesa contro lo spoofing includono l'uso di protocolli di sicurezza, l'implementazione di autenticazione a più fattori (MFA).

Denial-of-Service (DoS)

Il "Denial-of-Service" (DoS) è un tipo di attacco informatico progettato per rendere un servizio, una risorsa o un'applicazione inaccessibile agli utenti legittimi, sovraccaricandolo con un'eccessiva quantità di traffico, richieste o dati dannosi. L'obiettivo principale di un attacco DoS è quello di sopraffare la capacità di risposta del sistema target, facendo in modo che non possa più gestire le richieste legittime. Le difese contro gli attacchi DoS includono l'utilizzo di firewall, filtri di rete, sistemi di rilevamento delle intrusioni, la gestione del traffico, e la capacità di scalare o distribuire il carico su più server per poter sopportare un maggior volume di traffico.

Malware

Il termine "malware" è l'abbreviazione di "software dannoso" (malicious software). Si riferisce a qualsiasi tipo di software progettato specificamente per danneggiare, accedere in modo non autorizzato o compromettere un sistema informatico, una rete o un dispositivo. Le tecniche per diffondere il malware possono includere allegati di e-mail, link dannosi, download da fonti non affidabili o sfruttare vulnerabilità nei sistemi operativi o nelle applicazioni.

Spamming

Lo "spamming" è la pratica di inviare grandi quantità di messaggi indesiderati e non richiesti, spesso via e-mail, ma anche attraverso SMS, messaggi instantanei, commenti sui social media o altre forme di comunicazione digitale. Lo scopo principale dello spamming è la diffusione di contenuti pubblicitari, promozionali o fraudolenti a un vasto pubblico. Le misure di difesa contro lo spam includono l'uso di filtri antispam offerti da servizi di posta elettronica, l'educazione degli utenti sul riconoscimento di e-mail o messaggi sospetti, l'evitare di condividere l'indirizzo e-mail in modo non selettivo online e l'utilizzo di strumenti di sicurezza come firewall e software antimalware per proteggere dai potenziali rischi associati allo spamming.

Nuking

Il "Nuking" è un tipo di attacco informatico che mira a distruggere o rendere inutilizzabile un sistema, una rete o un dispositivo. Questo tipo di attacco poteva essere eseguito inviando pacchetti di dati dannosi che causavano il crash o il blocco del sistema target, impedendo così il suo funzionamento normale. La protezione contro questo genere di attacchi coinvolge l'implementazione di misure di sicurezza adeguate, l'uso di software aggiornato e affidabile

Backdoor

Una "backdoor" è una vulnerabilità nascosta in un software, un sistema operativo o un dispositivo che consente l'accesso non autorizzato o privilegiato. Le backdoor possono essere introdotte deliberatamente per scopi legittimi, come facilitare l'accesso per scopi di manutenzione da parte degli sviluppatori ma, tuttavia, possono anche essere create malevolmente da individui per ottenere un accesso non autorizzato a un sistema. Le difese contro le backdoor includono l'uso di software e sistemi da fonti attendibili, l'installazione regolare di patch e aggiornamenti di sicurezza.

Steganografia

La "steganografia" è la pratica di nascondere un messaggio, un file, o qualsiasi tipo di informazione all'interno di un'altra informazione in modo che non sia evidente o riconoscibile a prima vista. La steganografia può essere utilizzata per vari scopi, inclusi il nascondere messaggi segreti, la trasmissione di informazioni in modo discreto, la protezione delle informazioni sensibili e la contraffazione o la contraffazione di dati. Tuttavia, è anche possibile che la steganografia venga sfruttata per attività illegali, come la comunicazione di terroristi o criminali. Le difese contro la steganografia possono includere l'uso di strumenti di analisi specializzati che possono rilevare cambiamenti nei file multimediali o nelle strutture dati.