Minacce sicurezza informatica

- **Quali sono le principali minacce della sicurezza informatica?**

Tipi di attacchi informatici più comuni

Malware

Il termine malware definisce software malevoli, come spyware, ransomware, virus e worm. Il malware viola una rete sfruttando una vulnerabilità, di solito quando un utente seleziona un link pericoloso o apre un allegato ricevuto via e-mail che installa il software dannoso. Una volta all'interno del sistema, il malware può:

Bloccare l'accesso ai componenti principali della rete (ransomware)
Installare malware o altri software dannosi
Ottenere informazioni di nascosto trasmettendo dati dal disco rigido (spyware)
Interferire con alcuni componenti e rendere il sistema inutilizzabile

Phishing

Il phishing consiste nell'inviare comunicazioni fraudolente che sembrano provenire da una fonte affidabile, di solito una e-mail. L'obiettivo è quello di rubare dati sensibili come carte di credito e informazioni di accesso, o di installare un malware sul computer della vittima. Il phishing è una minaccia informatica sempre più comune.

Attacco man in the middle (MitM)

Gli attacchi man in the middle (MitM), noti anche come attacchi di intercettazione, si verificano quando gli hacker si inseriscono in una transazione fra due parti. Una volta che hanno interrotto il traffico, i criminali possono filtrare e rubare i dati. I punti di ingresso comuni per gli attacchi MitM sono:

Reti Wi-Fi pubbliche non sicure, dove gli hacker possono inserirsi tra il dispositivo di un visitatore e la rete. Senza saperlo, il visitatore passa tutte le informazioni all'hacker.
Una volta che il malware ha violato un dispositivo, un hacker può installare il software per elaborare tutti i dati della vittima.

Attacco denial-of-service

Un attacco denial-of-service invia enormi flussi di traffico a sistemi, server o reti per esaurirne le risorse e la larghezza di banda. Di conseguenza, il sistema sotto attacco non è più in grado di soddisfare le richieste legittime. Per lanciare un attacco di questo tipo, gli hacker possono anche utilizzare più dispositivi compromessi. In questo caso si parla di attacco distributed-denial-of-service (DDoS).

SQL injection

Una SQL (Structured Query Language) injection si verifica quando un hacker inserisce codice malevolo in un server che utilizza SQL e lo forza a rendere pubbliche informazioni che normalmente dovrebbero rimanere riservate. Per effettuare una SQL injection, è sufficiente aggiungere del codice malevolo nella casella di immissione di un sito web vulnerabile.

Attacchi zero-day

Un attacco zero-day colpisce non appena viene scoperta una vulnerabilità nella rete, ma prima che sia possibile implementare una patch o una soluzione. Gli hacker prendono di mira la

vulnerabilità rivelata durante questa finestra temporale. Il rilevamento delle minacce di vulnerabilità zero-day richiede una consapevolezza costante.

Tunneling DNS

Il tunneling DNS utilizza il protocollo DNS per trasmettere traffico non DNS sulla porta 53. Sfrutta il DNS per inviare traffico con il protocollo HTTP e con altri protocolli. Esistono vari motivi legittimi per utilizzare il tunneling DNS. Tuttavia, i servizi di tunneling DNS su VPN vengono usati anche per ragioni malevole. Ad esempio, possono servire a camuffare come DNS il traffico in uscita, nascondendo i dati normalmente condivisi tramite una connessione Internet. Se l'uso è malevolo, le richieste DNS vengono manipolate per esfiltrare i dati da un sistema compromesso e dirottarli verso l'infrastruttura dell'hacker. Il tunneling può essere utilizzato anche per i callback di comando e controllo dall'infrastruttura dell'hacker verso un sistema compromesso. ono di eseguire script lato client in contesti web inaffidabili. Ciò consente agli aggressori di rubare informazioni, prendere il controllo degli account degli utenti, modificare le pagine web e eseguire azioni in nome degli utenti. Le applicazioni web vulnerabili a XSS includono spesso forum, portali di commenti e altre pagine che consentono agli utenti di inserire contenuti in modo interattivo.

Cross-Site Scripting (XSS)

Il Cross-Site Scripting (XSS) è una vulnerabilità delle applicazioni web che consente agli aggressori di iniettare script malevoli in pagine web visualizzate da altri utenti. Gli attaccanti sfruttano vulnerabilità nelle applicazioni web che consentono di eseguire script lato client in contesti web inaffidabili. Ciò consente agli aggressori di rubare informazioni, prendere il controllo degli account degli utenti, modificare le pagine web e eseguire azioni in nome degli utenti. Le applicazioni web vulnerabili a XSS includono spesso forum, portali di commenti e altre pagine che consentono agli utenti di inserire contenuti in modo interattivo.

Attacchi di Forza Bruta

- Gli attacchi di forza bruta sono un metodo per decifrare password o crittografie deboli provando ripetutamente tutte le possibili combinazioni finché non si trova quella corretta. Gli hacker possono utilizzare programmi automatizzati per generare e provare una vasta gamma di possibili password o chiavi di crittografia per ottenere l'accesso non autorizzato a sistemi protetti.

Attacchi di Ingegneria Sociale

Gli attacchi di ingegneria sociale coinvolgono l'inganno e la manipolazione delle persone per ottenere informazioni riservate o l'accesso a sistemi protetti. Gli aggressori possono impersonare figure di autorità, fingere di essere colleghi o amici fidati, o utilizzare altre tattiche per ottenere l'accesso ai dati sensibili o per indurre le vittime a compiere azioni che compromettono la sicurezza.

Attacchi di Spear Phishing

Gli attacchi di spear phishing sono una variante più mirata del phishing standard. Gli aggressori mirano a un individuo o a un'organizzazione specifica, personalizzando le comunicazioni in modo da sembrare più credibili e autentiche. L'obiettivo è di ottenere informazioni riservate o di indurre la vittima a eseguire azioni dannose, come fornire credenziali di accesso o aprire allegati contenenti malware.

Attacchi di Backdoor

Gli attacchi di backdoor coinvolgono l'inserimento di porte secondarie nascoste o vulnerabilità nei sistemi, consentendo agli aggressori di accedere in modo non autorizzato in futuro. Queste porte

secondarie possono essere utilizzate per bypassare le normali procedure di autenticazione e per ottenere accesso non autorizzato o per introdurre altri tipi di malware nel sistema.

Attacchi di Ransomware

Gli attacchi di ransomware coinvolgono la crittografia o il blocco dell'accesso ai dati dell'utente da parte di un hacker. Gli aggressori richiedono quindi un pagamento, di solito in criptovaluta, in cambio della chiave per ripristinare l'accesso ai dati. Questi attacchi possono causare danni significativi alle aziende e agli individui, con potenziali perdite finanziarie e danni alla reputazione.