Principali attacchi informatici

Sniffing: l'attaccante intercetta e monitora il traffico di rete per catturare informazioni sensibili. Viola la riservatezza.

Spoofing: L'aggressore modifica l'indirizzo MAC del proprio dispositivo in modo che corrisponda all'indirizzo MAC di un dispositivo legittimo, consentendo all'aggressore di farlo

- Nascondi la sua identità
- Aggirare le misure di sicurezza, ad es. elenchi di controllo degli accessi o segmentazione basata su indirizzi MAC
- Ottenere l'accesso non autorizzato alla rete

L'attacco di spoofing MAC porta al furto di informazioni sensibili o allo svolgimento di altre attività dannose Viola la riservatezza- autenticità- integrità.

Dos: invia molti pacchetti alla porta della vittima per rendere indisponibile il servizio. Viola la disponibilità.

Malware: cioè "software maligni" sono una serie di software con lo scopo di danneggiare un pc. Il malware può assumere varie forme e svolgere diverse azioni dannose, tra cui:

- Trojan Horse (Cavallo di Troia): Programmi apparentemente innocui o utili che contengono un componente dannoso nascosto.
- Spyware: Programmi progettati per raccogliere informazioni da un computer senza il consenso dell'utente, spesso a fini di monitoraggio delle attività online.
- Worm: Programmi autonomi che si replicano e si diffondono attraverso reti senza bisogno di un file ospite. Si diffonde autonomamente attraverso reti e dispositivi collegati senza bisogno di un programma ospite. I worm possono sfruttare vulnerabilità di sicurezza di rete per propagarsi senza l'intervento diretto dell'utente.
- Virus: Programmi che si attaccano ad altri file eseguibili e si replicano quando tali file vengono eseguiti. Si diffonde inserendosi in altri programmi eseguibili o file di sistema. La sua diffusione dipende spesso dall'utente che condivide file infetti, ad esempio attraverso la condivisione di supporti di memorizzazione o allegati email.
- Rootkit: viene utilizzato per avere accesso ad un computer e avere i privilegi amministrativi.
- Keylogger: Software progettato per registrare le tastate dell'utente, spesso utilizzato per raccogliere informazioni sensibili come nomi utente e password. Viola la confidenzialità disponibilità integrità, autenticità
- Ransomware: Blocca i file presenti in un pc, spesso soggetto a ricatti la restituzione dei file in cambio di soldi.

Spamming: Invio massiccio di messaggi non desiderati, solitamente via e-mail, con lo scopo di diffondere messaggi pubblicitari. Viola l'autenticità

Nuking: invia un pacchetto dati per fare esplodere il sistema operativo, inviato nella porta NetBIOS la 139 si tratta di un errore di Microsoft nel protocollo TCP/IP. Viola la disponibilità.

Backdoor.: sono letteralmente "porte sul retro". Usate da utenti per entrare come amministratore all'interno dei siti web senza autorizzazione. Viola la confidenzialità.

Ddos: attaccante crea una botnet, (**insieme di computer compromessi da un malware, che permette ai malintenzionati di prendere il controllo dei pc e fargli eseguire determinate operazioni) e fa inviare a tutti i pc infettati richieste ad un determinato sito, così da metterlo fuori uso per le troppe richieste di accesso. Viola** la disponibilità.

Phishing: L'attaccante attraverso un'e-mail si spaccia per un ente reale,(magari cambiando di poco il nome di dominio) e ha lo scopo di rubare dati sensibili come credenziali di accesso, carte di credito...