

Tipologie di attacchi

Introduzione agli attacchi

Tipologie di attacchi

Attacchi DoS/DDoS - Panoramica

- Incidono sulla disponibilità dell'infrastruttura e/o dei servizi
- Reca danni reputazionali alla vittima
- Se il target è un servizio essenziale (ospedali, energia, ecc...) è tra gli attacchi più efficaci e temuti

Tipologie di attacchi

Attacchi DoS/DDoS - Differenze

L'attacco **DoS** (Denial of Service) è un tipo di attacco che colpisce computer o reti e riduce, restringe o previene l'accesso alle risorse da parte degli utenti legittimi.

Un **DDoS** (Distributed Denial of Service) è un attacco DoS coordinato che coinvolge un numero elevato di computer zombie (sistemi compromessi in precedenza, botnet) per attaccare un singolo target.

Tipologie di attacchi

Attacchi DoS/DDoS - Tipologie

VOLUMETRIC ATTACK: Consuma la banda del target riducendone le performance o non facendo più funzionare il servizio. Può attaccare la rete del target o il servizio esposto.

PROTOCOL ATTACK: Utilizza risorse come le connection state table presenti negli apparati di rete. Include SYN Flood e Fragmented Packet Attack. Questo attacco è misurato in *packets per second* (Pps).

APPLICATION LAYER ATTACK: Consuma le risorse dell'applicazione (o del servizio) in modo da renderlo non funzionante agli utenti legittimi.

Tipologie di attacchi

Attacchi DoS/DDoS - Tipologie

UDP Flood: Pacchetti UDP con indirizzo IP spoofato (IP sorgente non reale ma in riferimento).

SYN Flood: Richieste SYN al target con **IP sorgente fittizio**, il target risponderà con SYN+ACK attendendo per l'ACK finale. Il target non riceverà risposta in quanto l'IP sorgente è falso; un three-way handshake incompleto può rimanere in attesa fino a 75 secondi.

Fragmentation Attack: Il target, inondato di pacchetti TCP/UDP frammentati, cercherà di riassemblarli. I pacchetti frammentati solitamente passano attraverso i sistemi di difesa network inosservati.

Multi-Vector Attack: Combinazione di attacchi volumetrici, di protocollo e application layer. Possono essere lanciati un vettore alla volta o in parallelo per confondere gli analisti.

Tipologie di attacchi

Attacchi DoS/DDoS - Detection e mitigazione

Le **tecniche di detection** sono basate sull'identificazione e la discriminazione del traffico malevolo (aumenti di traffico costanti o spike) e eventi circostanziati di aumento non previsto di pacchetti legittimi. Tutte le tecniche di detection definiscono un attacco come una **deviazione anormale e notevole dalle soglie prefissate** durante il normale traffico di rete.

Assorbire l'attacco: Utilizzare ulteriori risorse (banda, risorse di sistema).

Degradare i servizi: Spegnerne i servizi non critici e non necessari.

Spegnerne i servizi: Spegnerne tutti i servizi finché l'attacco non è finito.

Tipologie di attacchi

Session Hijacking - Concetti e tipologie

Il **Session Hijacking** è una metodologia di attacco nella quale l'attaccante cerca di inserirsi in una comunicazione TCP tra due computer. L'attaccante, sniffando il traffico, può compromettere la vittima con frodi, furti di identità e/o di credenziali.

NETWORK LEVEL HIJACKING: Intercettazione (sniff) di pacchetti durante una trasmissione TCP/UDP tra client e server.

APPLICATION LEVEL HIJACKING: Ottenimento della User Session applicativa (ad es. HTTP) tramite session ID.

Tipologie di attacchi

Session Hijacking - Session Management

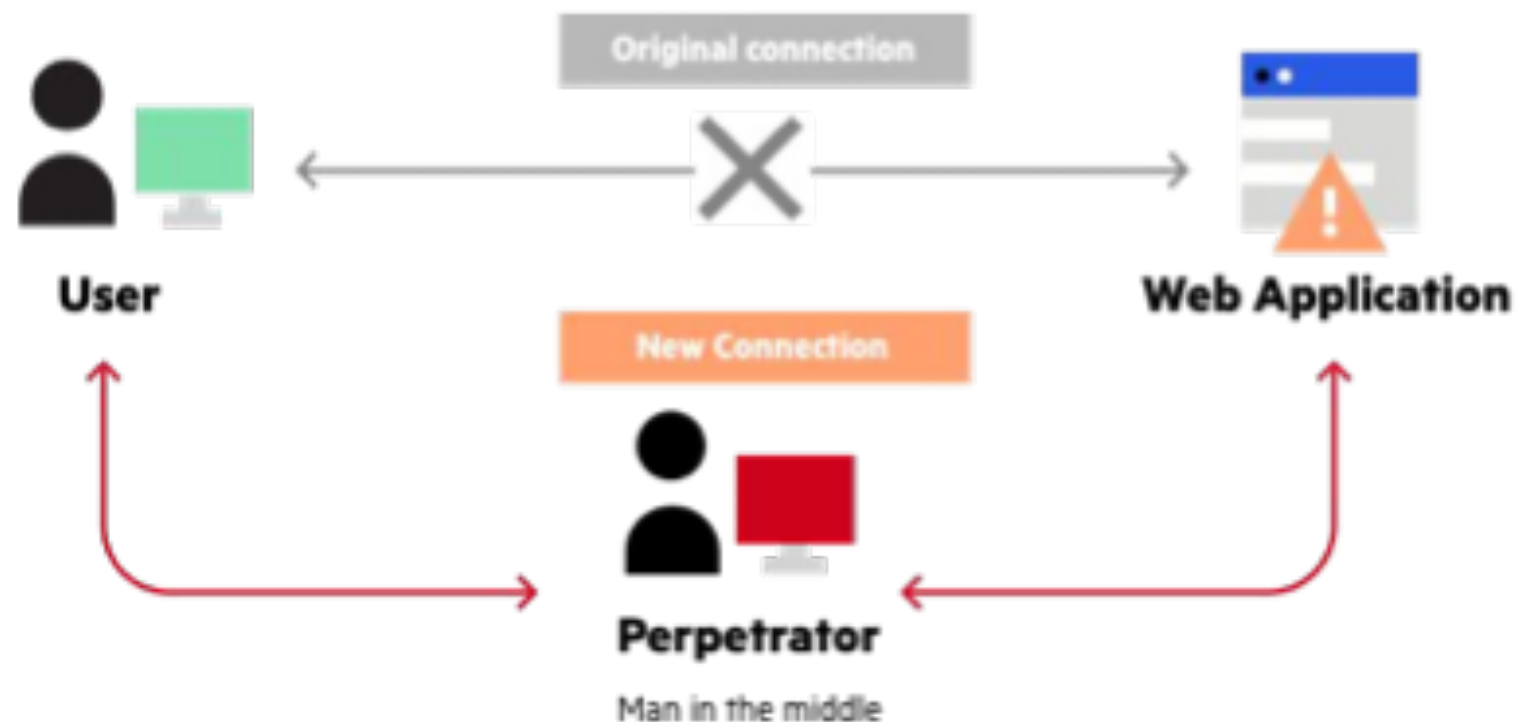
Uno dei componenti fondamentali di qualsiasi applicazione basata sul web o API stateful è il meccanismo con cui controlla e mantiene lo stato di un utente o dispositivo che interagisce con essa.

La gestione della sessione cambia un protocollo stateless (come HTTP) in stateful, che è fondamentale per differenziare diversi utenti o dispositivi.

Tipologie di attacchi

MITM - Man-in-the-middle

Un **man-in-the-middle** (MITM) è un attacco informatico in cui qualcuno si interpone nella comunicazione tra due parti.



Tipologie di attacchi

MITM - Man-in-the-middle

Un attaccante che si interpone nella comunicazione tra client e server ne può sniffare i pacchetti. Se la comunicazione non è cifrata, ad esempio come nel protocollo HTTP, l'attaccante sarà in grado di copiarne il contenuto (dati, credenziali) o addirittura manipolarle.

HTTPS invece è cifrato (HTTP all'interno di un tunnel TLS) e evita molti MITM di basso livello (MITM può accadere anche in connessioni cifrate).

Ovviamente un attacco di questo tipo è possibile anche con altri protocolli.

Tipologie di attacchi

Buffer Overflow

I buffer overflow **stack-based** sono più comuni e sfruttano la memoria dello stack che esiste solo durante il tempo di esecuzione di una funzione.

I buffer overflow **heap-based** invece sono più difficili da eseguire e comportano l'inondazione dello spazio di memoria allocato per un programma oltre la memoria utilizzata per le operazioni correnti di esecuzione.

Buffer overflow example

Buffer (8 bytes)								Overflow	
U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Tipologie di attacchi

SQL Injection

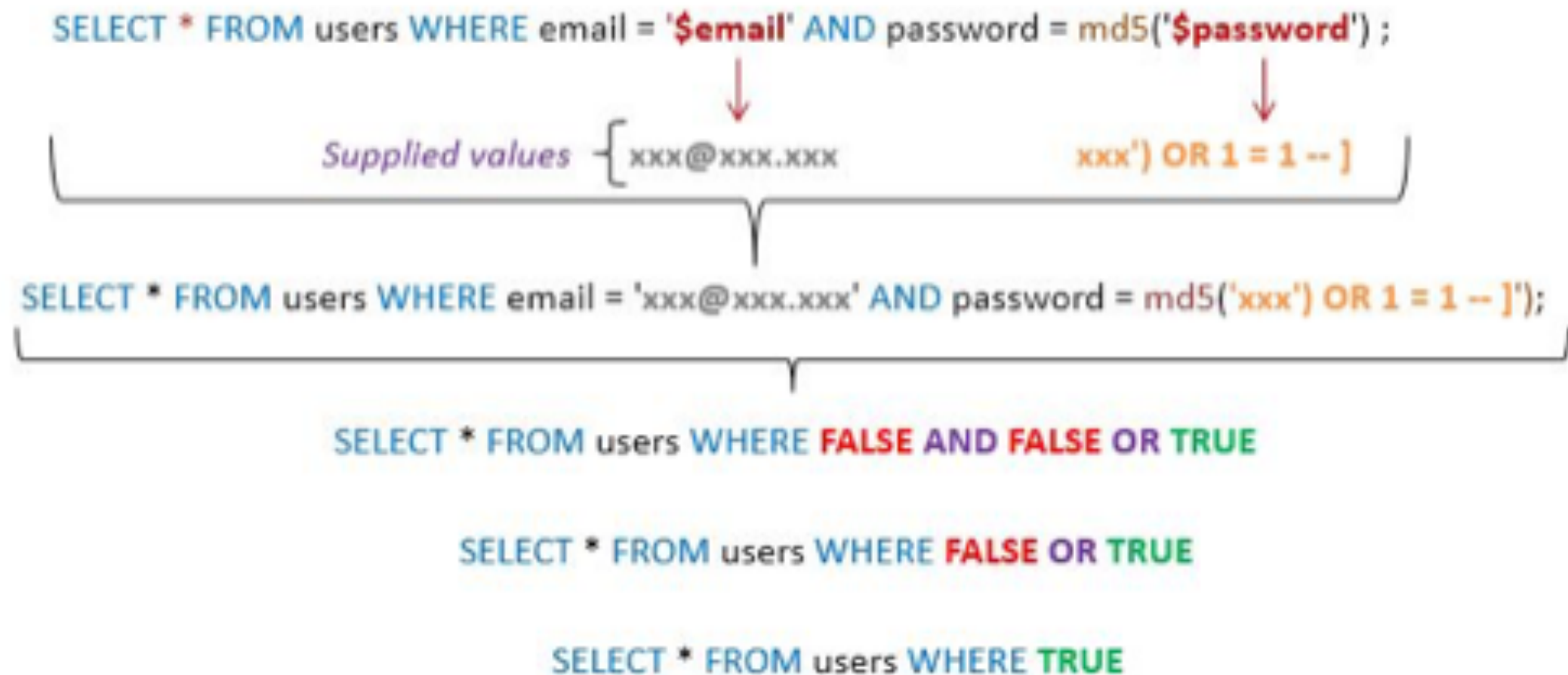
La SQL Injection è una tipologia di attacco che permette di iniettare codice in applicazioni che gestiscono dati attraverso database relazionali.

Con questo attacco è possibile eseguire esfiltrazione di dati, creare backdoor applicative o a livello di Sistema Operativo o il danneggiare/eliminare dati.

L'obiettivo di una SQL Injection è inserire il proprio codice SQL all'interno della query originale dell'applicazione, sfruttando le vulnerabilità del linguaggio di programmazione o errori di progettazione.

Tipologie di attacchi


SQL Injection



Tipologie di attacchi

Command Injection

Il **command injection** è un attacco in cui l'obiettivo è l'esecuzione di comandi arbitrari sul Sistema Operativo host attraverso un'applicazione vulnerabile.



```
<?php
  if (isset($_GET['domain'])) {
    echo '<pre>';
    $domain = $_GET['domain'];
    $lookup = system("nslookup {$domain}");
    echo($lookup);
    echo '</pre>';
  }
?>
```

Notice how the 'domain' parameter is taken in from the GET request, and immediately interpolated into a command string.

Malware

Malware

Panoramica

Un malware è un software malevolo in grado di arrecare danni ad un sistema, disabilitare funzionalità e/o fornire il controllo remoto all'attaccante.

I malware sono suddivisi in famiglie, come i virus biologici. Un ransomware ad esempio, può essere della famiglia “Lockbit” ma avere funzionalità leggermente differenti e/o “potenziamenti”.

Malware

Composizione di un malware

- **CRYPTER:** Protegge il malware dal processo di Reverse Engineering
- **DOWNLOADER:** Trojan che scarica altri malware dalla rete
- **DROPPER:** Trojan che installa altri malware
- **EXPLOIT:** Codice malevolo che sfrutta una vulnerabilità per entrare nel sistema
- **INJECTOR:** Programma che inietta codice all'interno dei processi vulnerabili

Malware

Composizione di un malware

- **OBFUSCATOR:** Programma che permette l'offuscamento del codice e degli intenti di un malware così da rendere difficile la rilevazione e la rimozione
- **PACKER:** Programma che permette di pacchettizzare tutti i file necessari ad un malware in un singolo eseguibile, permette di bypassare i controlli di sicurezza
- **PAYLOAD:** Parte di software che permette di ottenere il controllo del sistema (dopo l'exploit)
- **MALICIOUS CODE:** Comandi che definiscono le funzionalità del malware come furto di credenziali, creazione di backdoor o altre attività malevole

Malware

Malware Analysis

È il processo di **reverse engineering** di un malware al fine di individuare l'origine, le funzionalità e il potenziale impatto sui sistemi.

STATIC ANALYSIS: È solo code analysis, senza esecuzione del codice. Serve a capire il funzionamento del malware.

DYNAMIC ANALYSIS: Nota anche come behavior analysis, esegue il codice malevolo per capire come interagisce e capire che impatti potrebbe avere.

Malware

Metodi di detection

- **SCANNING:** Calcolata la signature viene ricercata in un database, in caso di corrispondenza viene lanciato un alert
- **INTEGRITY CHECKING:** Legge l'intero disco e "registra" l'integrità dei dati (come le signature)
- **INTERCEPTION:** Le richieste al Sistema Operativo vengono messe sotto monitoraggio
- **CODE EMULATION:** L'antivirus esegue il codice malevolo all'interno di una macchina virtuale chiamata sandbox
- **HEURISTIC ANALYSIS:** Controlla potenziali funzionalità malevole, attività sospette o system call

Malware

Indicatori di compromissione

- I processi richiedono più tempo e più risorse per essere eseguiti
- Beep del computer senza nessun video
- Le etichette (label) dei drive cambiano
- Il Sistema Operativo viene caricato con errori o non viene caricato affatto
- Avvisi costanti dall'antivirus
- Il computer si blocca di frequente o restituisce errori come BSOD (Blue Screen of Death)
- Mancano file e cartelle
- L'attività dell'harddisk è sospetta
- Le finestre del browser di bloccano
- Mancanza di spazio su disco
- Popup di pubblicità inattesi