

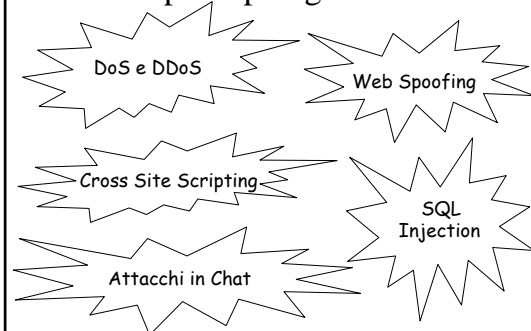


Prof. Alfredo De Santis

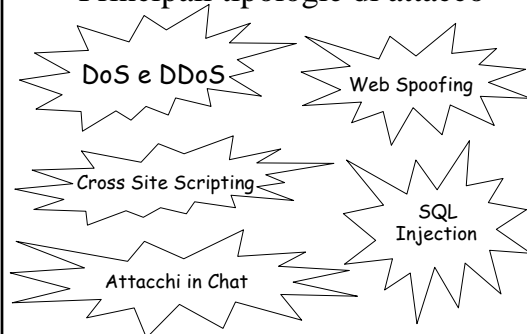
Attacchi a siti web

Cilio Giuseppe & Mea Raimondo Rosario

Principali tipologie di attacco



Principali tipologie di attacco



Denial of Service (DoS)

SCOPO: Negare a tutti gli utenti un servizio offerto da un sistema

COME?

Bandwidth Consumption (consumo della larghezza di banda)

Resource Starvation (esaurimento delle risorse)

Software Bugs (errori di programmazione)

Routing & DNS

DoS

Bandwidth Consumption: esaurisce tutta la banda a disposizione di un host inviandogli una grande quantità di traffico, superando la capacità del canale

Resource Starvation: consuma alcune risorse di tipo hardware della macchina come, ad esempio, il tempo CPU, la memoria e lo spazio su disco

Software Bugs: sfrutta i difetti di programmazione noti presenti nei software di rete dell'host

Routing & DNS: modifica la tabella d'instradamento dei router o la cache dei server DNS (Domain Naming System), allo scopo di indirizzare tutto il loro traffico verso un determinato host

DoS

Alcuni attacchi tra i più noti

SMURF/PING BROADCAST

FRAGGLE ATTACK

SYN FLOODING



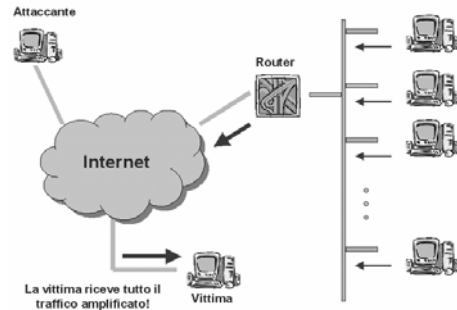
DoS- SMURF/PING BROADCAST

Strumenti: messaggi ECHO: servono a verificare se un host è attivo
indirizzi di broadcast: redirigono a tutta la sottorete i messaggi ricevuti

Idea base: viene inviato un messaggio ECHO (con protocollo ICMP) all'indirizzo di broadcast di una rete, inserendo nel campo del mittente l'indirizzo della vittima (spoofing)

Iterando: si spedisce una grande quantità di messaggi ECHO
=> la vittima viene sommersa di messaggi di risposta

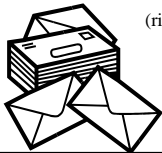
DoS



DoS- FRAGGLE ATTACK

Idea base: il meccanismo che viene attivato è identico allo Smurf/Ping, solo che sfrutta il protocollo UDP

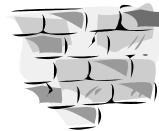
Iterando: la vittima viene sommersa di messaggi di risposta di tipo ECHO REPLY o UNREACHABLE (risposta affermativa o "irraggiungibile")



DoS- Difendersi da Smurf e Fraggle

Prevenzione:

- disattivare la funzione di risposta alle richieste ECHO
- limitare il traffico ICMP e UDP ai servizi che ne necessitano realmente
- Implementare filtri in uscita contro l'invio di pacchetti con IP "spoofati", per evitare il lancio di un attacco dalla propria rete



DoS- Difendersi da Smurf e Fraggle

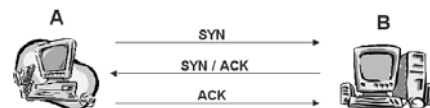
Cura: Collaborare con il proprio ISP e con la società proprietaria della rete di amplificazione per risalire all'aggressore:

- Individuare l'interfaccia che ha ricevuto il pacchetto contraffatto
- Risalire al router precedente
- Percorrere al contrario gli hop del pacchetto inviato dall'aggressore fino a giungere alla rete originaria

DoS- SYN FLOODING

Uno dei primi attacchi DoS

Sfrutta le debolezze dell'handshake di TCP, che avviene così:



DoS- SYN FLOODING

Debolezze: •la comunicazione attivata sulla macchina B non ha termine fino a che non vi è una risposta dalla macchina A o allo scadere del timeout sulla connessione

•B deve mantenere in memoria (coda) le informazioni sulla connessione

La coda ha dimensione limitata

DoS- SYN FLOODING

Idea: Se si riesce a mantenere attivi nella memoria della macchina B un gran numero di pacchetti, il servizio per sovraccarico:

•non risponde

•si blocca

•blocca l'intera macchina sulla quale è ospitato



DoS- SYN FLOODING

Come? Nella prima chiamata di connessione l'attaccante sostituisce l'indirizzo di A (di ritorno) del pacchetto, con un indirizzo inesistente o difficile da raggiungere

=> B non riesce a contattare il finto chiamante e si blocca o risponde in tempi inaccettabili



DoS- SYN FLOODING PRECURSORE DI UN'INTRUSIONE

IP HIJACKING: Approfitando di una relazione di fiducia tra due host, l'attaccante ne mette fuori uso uno, impersonandolo in seguito per accedere con i suoi privilegi all'altro host.



DoS- Difendersi dal Syn Flooding

•Ridurre l'intervallo di tempo dedicato alla realizzazione delle connessioni (non è una soluzione definitiva)

•Utilizzare Syn Cookies che, con un protocollo di autenticazione crittografica, riescono a distinguere le connessioni legittime da quelle provenienti da un attacco, respingendo automaticamente quest'ultime

•Usare software specializzati che controllano costantemente l'attività della rete, individuano un attacco e inviano pacchetti TCP adeguati che terminano le connessioni incomplete

DoS- Syn Cookies

Il secondo syn nell'handshake di TCP/IP è normalmente un numero casuale difficile da indovinare

Dopo aver inviato quest'ultimo, il sistema deve rimanere in attesa dell'ack dell'altro host

Syn Cookies: si prende un numero non casuale da inviare che contenga le informazioni (o parte di quelle informazioni) che verrebbero memorizzate nella coda

Una volta che la coda è piena le informazioni che dovrebbero essere memorizzate vengono inviate nel syn ack di risposta

DoS- Syn Cookies

Se l'handshake viene completato correttamente dal client inviando l'ack finale, le informazioni vengono estratte dal pacchetto ricevuto

L'ack di risposta viene sempre calcolato a partire dal syn, ed è quindi possibile, partendo da un ack, ricalcolare il syn originale

Principali tipologie di attacco



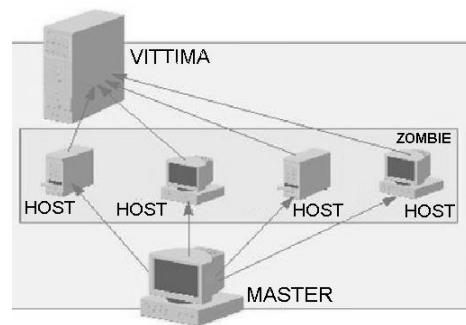
Distributed DoS (DDoS)

Stesso approccio del DoS ma utilizza più punti di ingresso contemporaneamente

Non necessita di una banda passante elevata perché l'attacco non parte dagli host dell'hacker ma da sistemi di aziende ignare e strutture pubbliche

Su queste macchine viene installato e lanciato un programma per attivare un processo zombie che resta in attesa di un comando di attivazione

DDoS



DDoS

Una volta ricevuto il comando di attivazione, i processi zombie si attivano e iniziano a bombardare di traffico la vittima designata

È una tecnica che viene preparata per tempo, attrezzandosi con un pool di macchine compromesse da poter scagliare contro il sistema vittima.

La possibilità teorica degli attacchi DDoS è nota dal 1997, ma solo nella seconda metà del 1999 hanno iniziato a circolare nel mondo degli hacker le prime applicazioni capaci di implementare un'aggressione di questo tipo

DDoS- Difendersi dal DDoS

Prevenzione: **•Network filtering:** in una Lan connessa a Internet tramite router, si configura il dispositivo in modo da filtrare i pacchetti: sia quelli in ingresso che contengono informazioni alterate sulla loro provenienza sia quelli falsificati provenienti dalla sottorete interna



•Limit Network Traffic: limitare la quantità di banda usata da un particolare servizio (per esempio fornire più banda ai servizi web a discapito di ftp) Può essere usato anche in maniera reattiva per fermare un DDoS

DDoS- Difendersi dal DDoS

Analisi: **Intrusion Detection Systems e Host Auditing Tools:** strumenti con cui identificare malintenzionati mentre cercano di comunicare con i loro sistemi *slave, master o agent*. Ciò consente di sapere se alcune macchine della propria rete sono utilizzate per lanciare un attacco conosciuto (ma non nuove varianti o prodotti nuovi)



Network Auditing Tools: consentono l'analisi di una intera rete aziendale per verificare la presenza di agenti per DDoS

DDoS- Difendersi dal DDoS

Cura:

- Non ci sono misure che possano riportare rapidamente la situazione sotto controllo
- È molto importante riuscire a determinare la provenienza reale (indirizzi Ip) dei pacchetti usati per l'attacco, per arginare il traffico generato da chi li sta inviando
- Non basta controllare il mittente indicato nei pacchetti (l'indirizzo potrebbe essere falsificato)
- Si deve accedere ai router per ricostruire l'effettiva provenienza dei dati



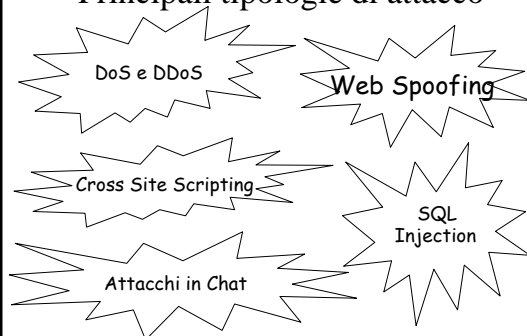
DDoS- Difendersi dal DDoS

Cura:

- In collaborazione con il proprio Isp contattare il fornitore di connessione Internet del mittente in modo che anche lui implementi dei filtri per bloccare il traffico indesiderato in entrata



Principali tipologie di attacco



Web Spoofing

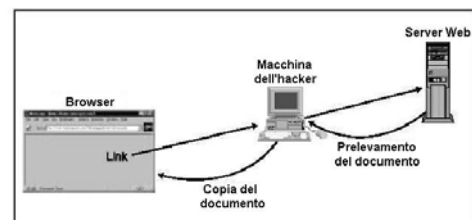
Idea: Creare una copia convincente ma falsa di un intero sito Web

Il finto sito ha tutto l'aspetto di quello vero (contiene le stesse pagine e gli stessi link), ma è completamente sotto il controllo dell'hacker

Tutto il traffico di rete fra il browser della vittima e il sito Web passa attraverso l'hacker

L'hacker può osservare o modificare tutti i dati che vanno dalla vittima al server del sito Web e controllare tutto il traffico di ritorno dal server Web alla sua vittima

Web Spoofing



Web Spoofing

Una volta attuato l'imbroglione, l'hacker può comportarsi in modi diversi e dare il via ad altre procedure

Le due più comuni sono **sorveglianza** (sniffing) e **manipolazione** (spoofing)

•**SORVEGLIANZA**: l'attaccante osserva passivamente il traffico della rete

•**MANIPOLAZIONE**: l'attaccante convince un host di essere un altro computer fidato e pertanto si prepara a ricevere informazioni



Web Spoofing

Con la manipolazione, l'hacker registra il contenuto delle pagine Web visitate dalla vittima

Quando questa compila un modulo in una pagina HTML, poiché si è interposto fra il client e il server, riesce a registrare tutti i dati immessi dal client

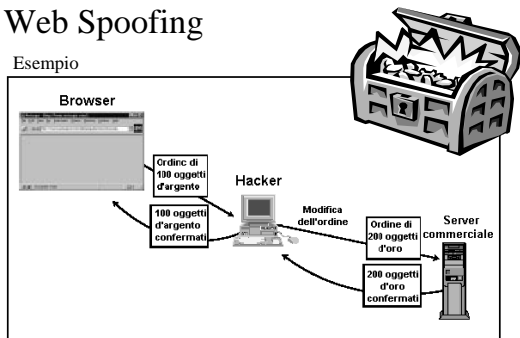
Stessa cosa per le risposte del server

La maggior parte dei servizi di commercio in Internet impiega dei moduli Web

=> l'hacker è in grado di osservare numeri di conto corrente, password e altre informazioni riservate che la vittima immette nelle schede

Web Spoofing

Esempio



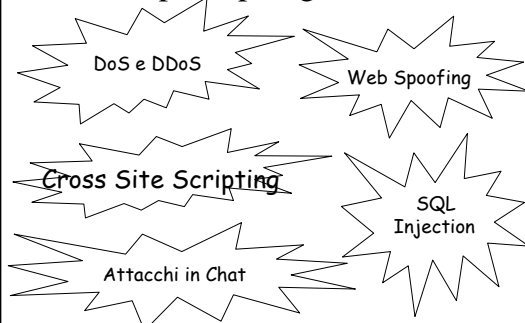
Web Spoofing- Difendersi

Questo tipo di attacco non è rilevabile, ma si può prevenire

Come?

- Disabilitare nel browser gli script JavaScript, Java e VBScript in modo che l'hacker non possa nascondere l'evidenza dell'attacco
- Assicurarsi che la riga degli indirizzi del browser sia sempre visibile
- Fare attenzione all'indirizzo URL visualizzato dal browser, assicurandosi che punti sempre al server a cui si pensa di essere connessi

Principali tipologie di attacco



Cross Site Scripting (CSS)

Idea: Inserire codice arbitrario come input di una web application, così da modificarne il comportamento

Se uno script consente questo tipo di attacco, è facile confezionare un URL ad hoc e inviarlo all'utente che diventa vittima del sotterfugio

=> gli sembra di utilizzare il normale servizio offerto dal sito web vulnerabile

Pagine web o e-mail sono i mezzi ideali per portare a termine l'attacco

CSS

Quando utilizziamo un servizio che richiede l'inserimento di username e password, questi dati vengono registrati sul nostro computer sotto forma di **Cookie** (file di testo) per non doverli digitare ogni volta

I dati contenuti nel cookie sono accessibili solo dal sito web che li ha creati

Se il sito utilizza un'applicazione vulnerabile al CSS l'aggressore può iniettare un semplice JavaScript che legge il cookie dell'utente

Il browser dell'utente permette la lettura perchè il JavaScript viene eseguito da un sito autorizzato a leggere il cookie (perchè lo ha creato)!

CSS

Risultato: l'aggressore ha accesso al cookie e, a seconda delle informazioni contenute, è in grado di leggere la nostra posta, oppure di utilizzare il nostro nickname nel forum che frequentiamo (e i nostri privilegi, se ad esempio siamo amministratori), e così via

Beffa: Il CSS richiede un intervento **attivo** da parte della vittima per poter funzionare: anche il click su un link in una pagina web o in un messaggio di posta elettronica può nascondere insidie di questo tipo

CSS

Qualsiasi tipo di applicazione web può essere a rischio, se non implementa opportuni controlli sull'input degli utenti

Si possono individuare vulnerabilità in **script casalinghi**, **applicazioni web** diffuse e **server web**



CSS

Script casalinghi: la semplicità dei moderni linguaggi lato server permette la creazione di script da utilizzare sui siti web personali. Spesso però le tecniche basilari della programmazione sicura non sono conosciute e gli script offrono molti punti vulnerabili agli attacchi di CSS

Applicazioni web: le applicazioni web create appositamente per essere diffuse e utilizzate in migliaia di siti (forum, chat, sistemi di gestione dei portali) solitamente sono sviluppate con un maggiore attenzione ai problemi della sicurezza. Ciò non esclude la scoperta periodica di nuove sviste nella programmazione che aprono le porte al Cross Site Scripting

CSS

Server web: queste applicazioni sono molto diffuse e solitamente non lasciano presagire la vulnerabilità a questo tipo di attacco. L'unico vantaggio in questo caso è la possibilità di accorgersi tempestivamente dell'attacco in corso, tramite l'analisi dei log del server

CSS- Difendersi dal CSS

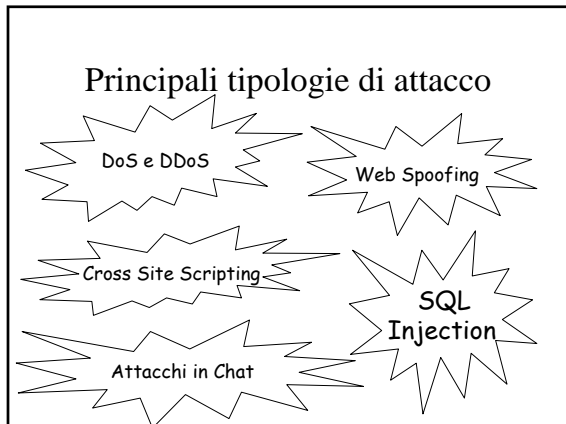
Prevenzione:

- disattivare il supporto **JavaScript**
- impostare un livello Alto di protezione

possono contrastare i codici nocivi ma creano problemi alla normale navigazione

- fare attenzione ai link da aprire e alla presenza di anomalie

Molti dei bug relativi al **CSS** possono essere risolti implementando una procedura di validazione dell'input negli script



SQL Injection

Lo **Structured Query Language (SQL)** è il linguaggio con cui vengono effettuate le interrogazioni ad alcuni database

Idea: Sfruttare le vulnerabilità specifiche di questi database attraverso stringhe create ad hoc e inviate ad un web server

Quasi tutti i portali a contenuto dinamico in internet si basano su colloqui tra web server e database SQL

SQLI

Il colloquio avviene attraverso le cosiddette query (interrogazioni), scritte codificandole attraverso degli URL generati dall'applicazione web

Le query devono rispettare un certo standard di sintassi (stringhe alfanumeriche, punteggiatura, ...)

Una query SQL dinamica generata da un'applicazione web viene codificata in Unicode

SQLI

I portali web usano molto spesso gli stessi script per effettuare le stesse operazioni di gestione

=> un hacker che sa com'è strutturato un determinato script, può inserire nella barra di indirizzi del browser un URL contenente una query SQL creata per arrecare un danno al web server e all'applicazione che risiede su di esso

Risultati:

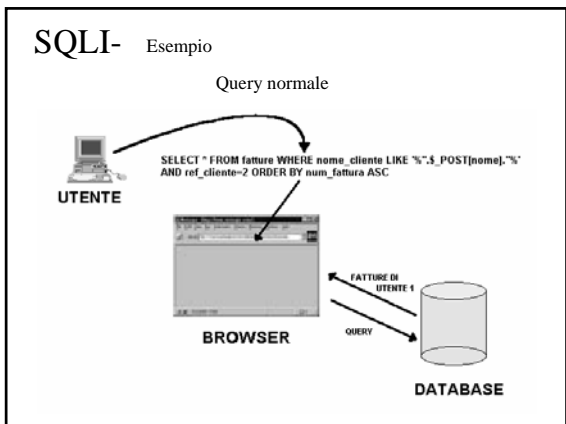
- inserire ed estrarre dati nel database a piacimento
- nei casi più gravi, poter ottenere il controllo remoto del server e di tutte le sue funzionalità

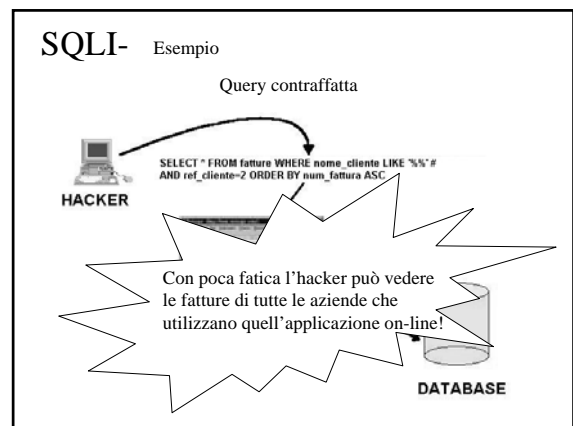
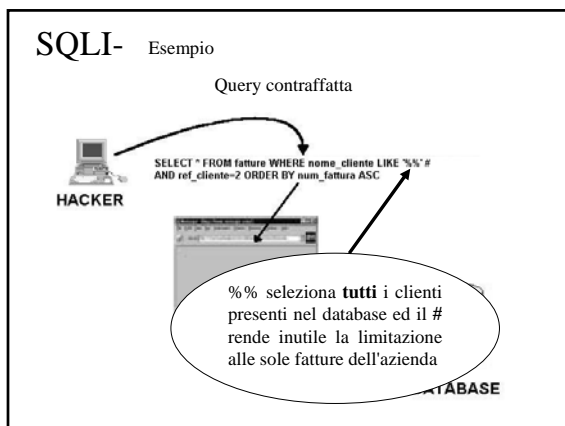
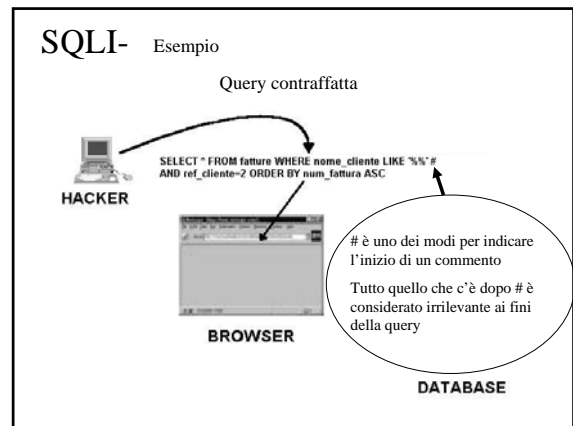
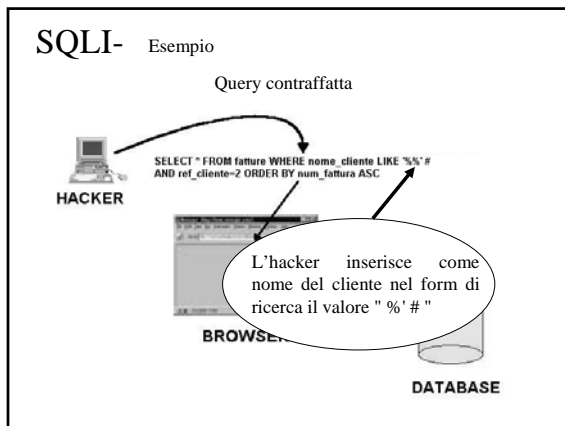
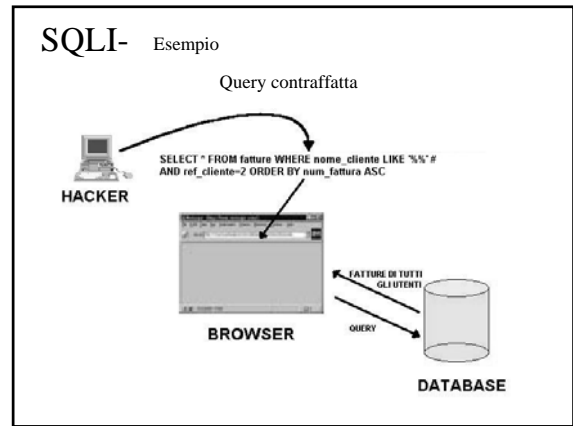
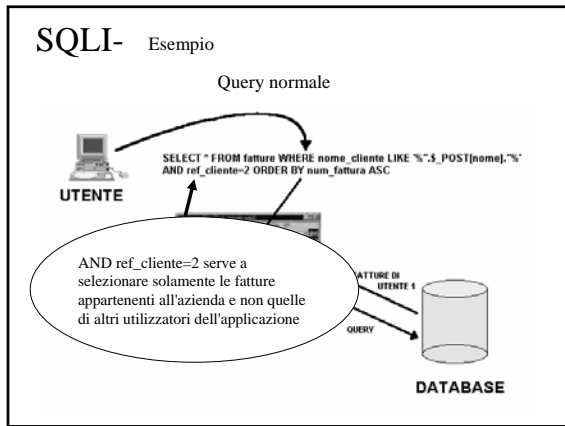
SQLI- Esempio

Gestionale che si occupa di un archivio on-line di fatture di più aziende

Motore di ricerca che permette di cercare una fattura per nome del cliente

Deve essere garantita la privacy!





SQLI- Difendersi dall' SQL Injection

Prevenzione: Un amministratore di rete che vuole difendersi da un attacco di questo tipo deve:



- testare tutti gli script che fanno parte dell'applicativo che gestisce

- verificare che tutti siano immuni all'attacco

Principali tipologie di attacco



Attacchi in Chat

L'aggressione più nota che si può subire in Chat è il **nuke** (disconnessione del computer o blocco del sistema)

Sfrutta dei buchi nella sicurezza del sistema su cui gira il client e per difendersi occorrono delle patch

Si può diventare bersaglio anche di attacchi DoS, per tutelarsi occorre dotarsi di firewall

Nessuno di questi attacchi può danneggiare il nostro sistema, il peggio che può accadere è che sia necessario resettare la macchina

Chat- IRC

IRC (Internet Relay Chat) è un sistema di comunicazione che consente di conversare in modo interattivo con una o più persone

E' basato sull'architettura client-server, come la maggior parte dei servizi offerti su Internet

Esiste un certo numero di calcolatori sparsi per il mondo (server) il cui compito e' quello di trasmettere i messaggi degli utenti in tempo reale

Si hanno a disposizione delle aree di conversazione (**canali**) dove si può chiacchierare liberamente dell'argomento corrente

Chat- IRC

Il numero dei canali non e' prefissato, ma varia in continuazione (c'è tuttavia un certo numero di canali sempre presenti)

In IRC ognuno usa un suo nome inventato (nickname)

Tale nome deve essere univoco in tutto il mondo

Se il nick è già stato scelto da qualcun altro, al momento della connessione il server lo segnalerà e chiederà di cambiarlo (errore di **nick collision**)

Chat- Conquista dei canali

IRC prevede il ruolo di gestori dei canali (Channel Operator) che hanno la possibilità di cacciar fuori gli utenti indesiderati

Per essere operatore di un canale occorre essere il primo ad accedervi oppure farsi "**oppare**" da un altro operatore

La struttura di IRC e le sue regole hanno permesso il dilagare di vere e proprie lotte per lo status di operatore e di pericoli come il **Takeover** (appropriazioni indebite di un canale)

Chat- Conquista dei canali

IRC prevede il ruolo di gestore e gli utenti hanno la possibilità di cacciare gli operatori

OPPARE:
Concedere lo status di operatore

Per essere operatore di un canale occorre essere il primo ad accedervi oppure farsi "oppare" da un altro operatore

La struttura di IRC e le sue regole hanno permesso il dilagare di vere e proprie lotte per lo status di operatore e di pericoli come il **Takeover** (appropriazioni indebite di un canale)

Chat- Takeover (metodo 1)

Un server può (spesso) trovarsi disconnesso dalla restante rete IRC (**splittato**)

Un server splittato vede solo i propri utenti

Un utente che si collega ad un canale attraverso un server splittato non vede nessuno su quel canale, ricevendo automaticamente lo stato di operatore

Quando si risolve la situazione di split, questo nuovo utente si trova ad avere gli stessi privilegi dei legittimi operatori del canale

Chat- Takeover (metodo 2)

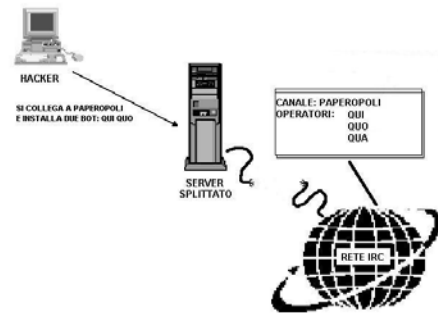
Sfrutta la **nick collision**, per metterla in pratica

L'attaccante deve conoscere il numero e i nomi degli operatori presenti sul canale da conquistare

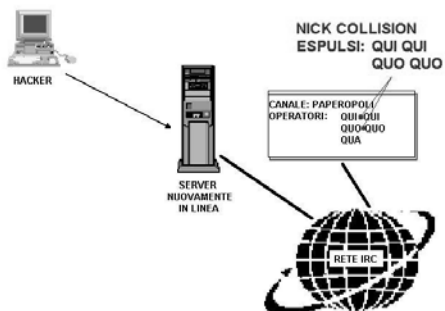
Deve usare dei **bot** (applicazioni create per simulare la presenza di un utente sul canale)

Se ad esempio sul canale sono presenti quattro operatori installa tre bot che abbiano gli stessi nomi dei tre operatori

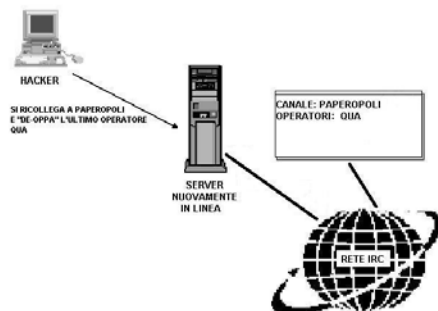
Chat- Takeover (metodo 2)



Chat- Takeover (metodo 2)



Chat- Takeover (metodo 2)



Chat- Difendersi dagli attacchi in Chat

Per difendere il proprio canale dai diversi tipi di takeover occorre:

- Gestire il canale in più persone
- Rendere il canale +i, cioè ad invito
- Settare il canale come +m cioè moderato
- Bannare e kickare (scacciare) tutti i presunti hacker usando il carattere "*" in modo da impedire che semplici cambi di nick sfuggano alla nostra azione



Chat- Difendersi dagli attacchi in Chat

Per difendere il proprio canale dai diversi tipi di takeover occorre:

- Gestire il canale in più persone
- Rendere il canale +i, cioè ad invito
- Settare il canale come +m cioè moderato
- Bannare e kickare (scacciare) tutti i presunti hacker usando il carattere "*" in modo da impedire che semplici cambi di nick sfuggano alla nostra azione

Si può accedere al canale solo se si viene "invitati" da un operatore con un comando specifico



Chat- Difendersi dagli attacchi in Chat

Per difendere il proprio canale dai diversi tipi di takeover occorre:

- Gestire il canale in più persone
- Rendere il canale +i, cioè ad invito
- Settare il canale come +m cioè moderato
- Bannare e kickare (scacciare) tutti i presunti hacker usando il carattere "*" in modo da impedire che semplici cambi di nick sfuggano alla nostra azione

Solo gli utenti in modalità +V e gli operatori possono parlare sul canale

+V può essere concesso solo dagli operatori e permette di parlare su un canale moderato



Chat- Difendersi dagli attacchi in Chat

Per difendere il proprio canale dai diversi tipi di takeover occorre:

- Gestire il canale in più persone
- Rendere il canale +i, cioè ad invito
- Settare il canale come +m cioè moderato
- Bannare e kickare (scacciare) tutti i presunti hacker usando il carattere "*" in modo da impedire che semplici cambi di nick sfuggano alla nostra azione

Un utente marchiato da un operatore con un "*" non può avere accesso al canale gestito da quell'operatore



Chat- Difendersi dagli attacchi in Chat

In caso di attacco è utile:

- Aprire nuove sessioni del client di chat in modo da poter accedere con altri nick allo stesso canale e oppare tutti gli alias
- Cambiare spesso nick, in modo da prevenire il più possibile le nick collision provocate dagli aggressori

Bibliografia

Testi:



- S. McClure, J. Scambray e G. Kurtz: "Hacking exposed: Network Security Secrets and Solutions" McGraw-Hill
- W. R. Stevens: "TCP/IP Illustrated, Volume 1 : The Protocols" Addison-Wesley

Bibliografia



Web:

- http://www.cert.org/tech_tips/denial_of_service.html
- <http://www.cert.org/homeusers/ddos.html>
- <http://www.cs.princeton.edu/sip/WebSpoofing/>
- http://www.cert.org/archive/pdf/cross_site_scripting.pdf
- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>