Sicurezza telematica - tecniche di attacco
Tecniche di attacco

Il più comune attacco contro una rete o una organizzazione è basato sulle intrusioni. Attraverso le intrusioni, gli attaccanti possono utilizzare i *computer* che non appartengono loro.

Gli attaccanti hanno a disposizione diverse tecniche per penetrare all'interno di un *computer*. Tali tecniche variano da attacchi di tipo *Social Engineering* (si conosce il nome di un certo utente e si telefona all'amministratore della rete dicendo che è necessario cambiare la *password* per l'utente che si finge di impersonare) ad attacchi basati sui tentativi di indovinare *username* e *password* di un certo utente.

Denial of Service

Un attacco di tipo *Denial of Service* è un attacco che impedisce ad una organizzazione di usare i servizi della propria rete. Sebbene molti casi di sabotaggio elettronico implichino la reale distruzione dei componenti di elaborazione o lo *shutdown* dei sistemi di elaborazione, molto spesso tali attacchi possono essere ricondotti ad azioni di *flooding* ("inondazione": un attaccante spedisce ad un sistema o ad una rete una lunga sequenza di messaggi in modo da occupare interamente o quasi la CPU ed altre risorse del sistema). Negli attacchi di tipo *flooding* infatti, il sistema spende la maggior parte del tempo a rispondere ai messaggi.

Mentre il *flooding* è il modo più semplice più comune per realizzare un attacco DoS, un metodo più intelligente potrebbe disabilitare i servizi, reindirizzarli o rimpiazzarli.

In un certo senso è quasi impossibile evitare attacchi DoS. Molto spesso, il rischio di attacchi DoS è inevitabile. Gli attacchi di tipo *flooding* sono considerati poco interessanti per gli attaccanti, perché risultano troppo semplici.

Furto di informazioni

Alcuni tipi di attacchi consentono ad un attaccante di ottenere delle informazioni anche senza dover utilizzare direttamente un *computer* dell'organizzazione che intende attaccare. Solitamente tali attacchi sfruttano dei servizi Internet che sono stati configurati per fornire informazioni, inducendoli a fornire più informazioni di quelle previste oppure a fornirle alle persone sbagliate.

I furti di informazioni possono essere di tipo attivo o di tipo passivo; nel caso attivo, un attaccante può ottenere le informazioni effettuando delle *query* ad un *server*; nel caso passivo, un attaccante può ottenere le informazioni catturando il traffico che interessa un segmento di rete da lui controllato.

La cattura di informazioni può avvenire ad esempio catturando i dati di *username* e *password* che transitano su un segmento di rete al quale l'attaccante è collegato ed ha attivato un programma di *sniffing*.

Ci sono diversi tipi di protezione contro il furto di informazioni. Un *firewall* propriamente configurato può aiutare a proteggere le informazioni che si intendono fornire all'esterno.

IP spoofing 1

In un attacco di tipo *spoofing*, un attaccante spedisce pacchetti con un campo origine errato. Quando ciò accade, le risposte vengono inviate all'indirizzo di origine fittizio e non all'attaccante. Questo potrebbe sembrare un problema, ma in realtà ci sono tre casi in cui l'attaccante non si interessa di

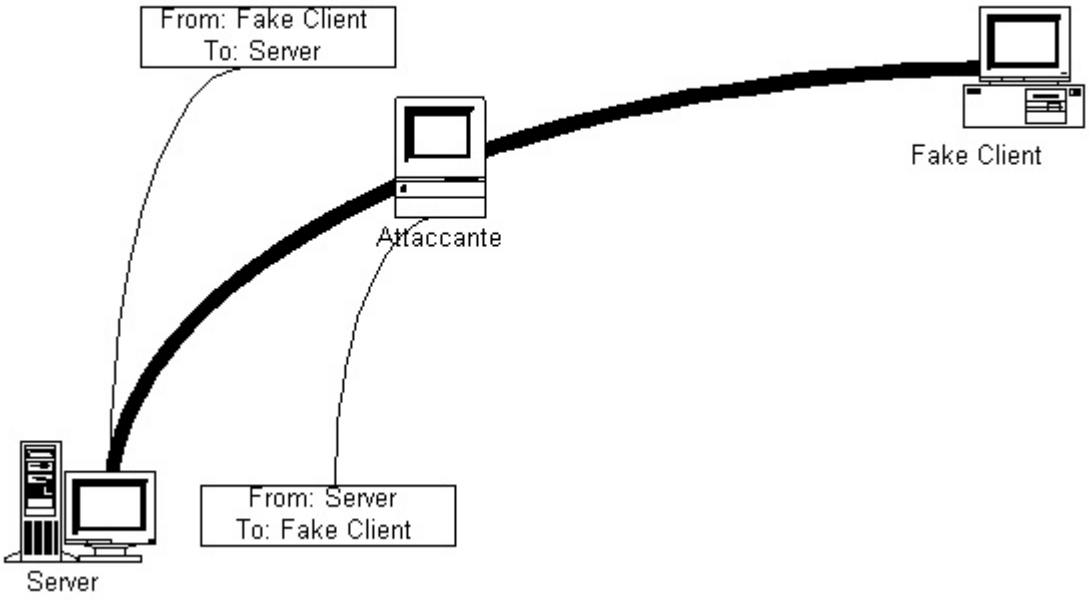
questo:

- l'attaccante può intercettare le risposte;
- l'attaccante non necessita di vedere le risposte;
- l'attaccante non è interessato alle risposte.

IP spoofing 2

L'attaccante può intercettare le risposte.

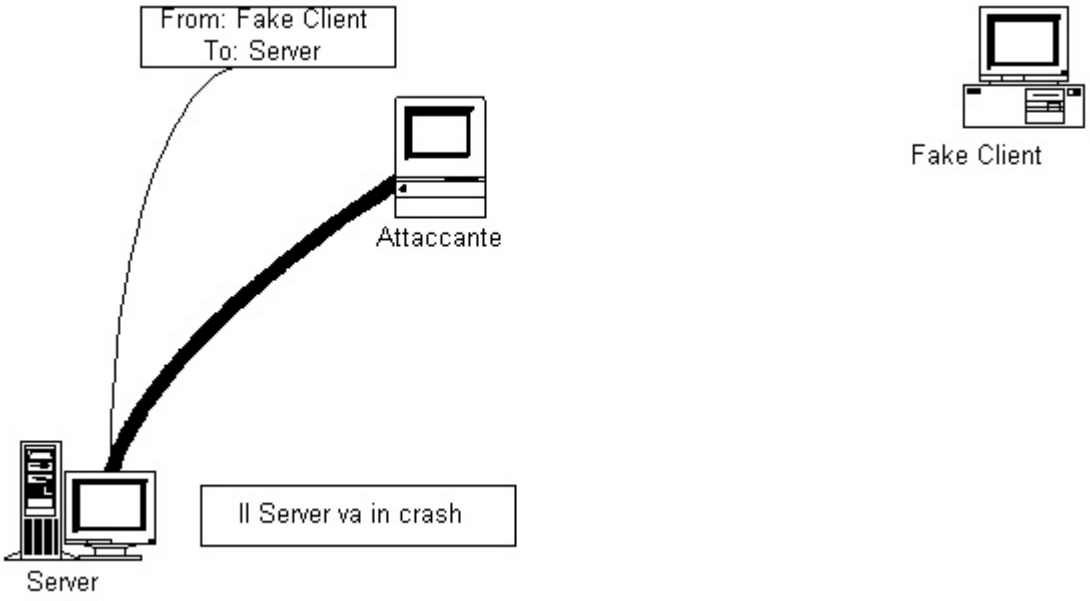
Se l'attaccante si trova in qualche punto nella rete tra la destinazione e l'origine, l'attaccante può vedere le risposte e continuare la conversazione fin quando lo ritenga necessario.



IP spoofing 3

L'attaccante non necessita di vedere le risposte.

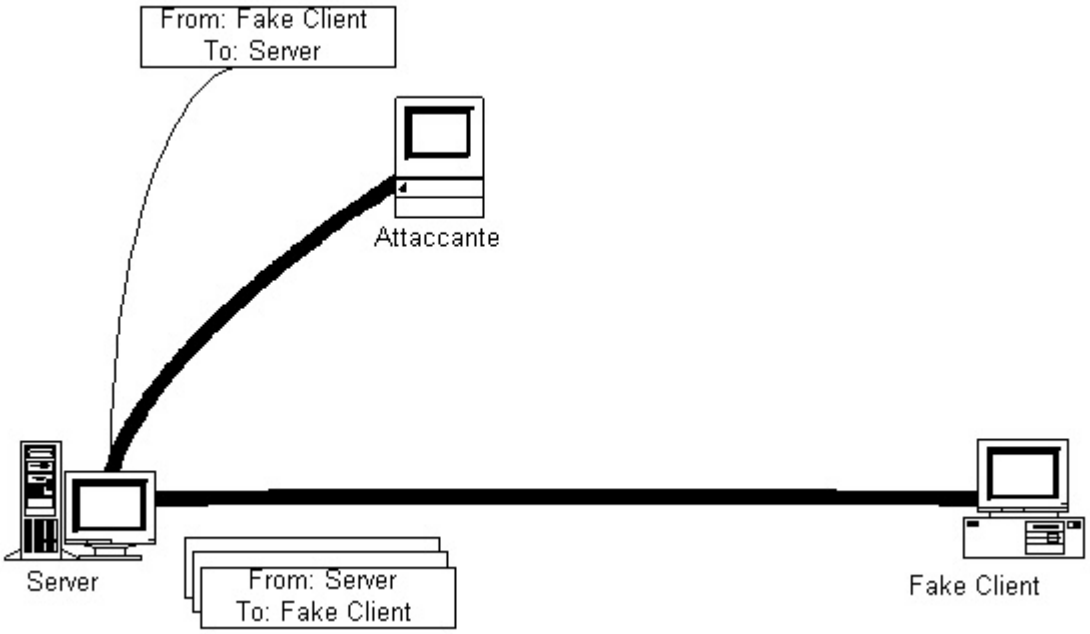
Un attaccante potrebbe condurre un attacco di tipo DoS, la macchina attaccata non sarebbe in grado di rispondere comunque.



IP spoofing 4

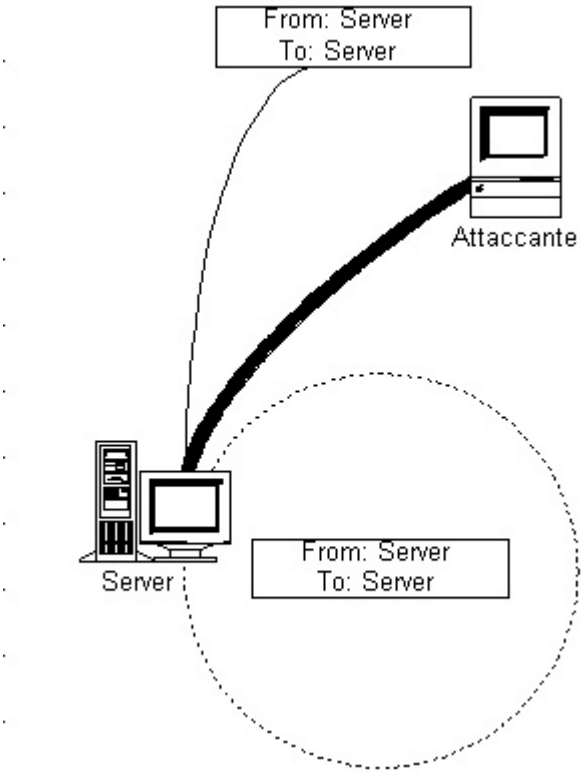
L'attaccante non è interessato alle risposte.

Alcuni attacchi sfruttano il fatto che le risposte raggiungono un altro *client* (ignaro).



L'attacco di tipo *smurf* utilizza indirizzi di origine fittizi per attaccare l'*host* che sembra l'origine; un attaccante invia ad un *server* (la vittima fittizia) un pacchetto con indirizzo di origine uguale a quello di un altro *host* (la vittima reale). A questo punto, gli amministratori della vittima reale e di quella fittizia iniziano a sospettare ciascuno dell'altro.

Un altro tipo di attacco, chiamato attacco di tipo *land*, spedisce un pacchetto con indirizzo di origine uguale a quello di destinazione; tale pacchetto molte volte provoca un *loop*.



Port scanning

Il *port scanning* è il processo con cui si cercano i *PORT* su cui un *host* è in ascolto, al fine di individuare cosa si possa attaccare. Il *port scanning* incrementale (si inviano pacchetti TCP/IP con numeri di porta crescenti) è molto semplice da individuare, e quindi gli attaccanti cercano di camuffarlo con diverse tecniche. Ad esempio, molte macchine non effettuano il *logging* delle connessioni fino a quando non sono state interamente completate, quindi un attaccante potrebbe spedire un pacchetto iniziale con SYN uguale ad 1 e ACK uguale a 0, attendere la risposta (SYN e ACK uguali ad 1 (se il PORT è attivo;, RST uguale ad 1 se il PORT è chiuso) e bloccarsi. Questa tecnica è comunemente chiamata SYN *scan* oppure *Half open scan*.

Gli attaccanti possono anche trasmettere altri tipi di pacchetti, considerando la porta chiusa se ricevono un pacchetto RST, considerandola aperta se non ottengono risposta oppure se ottengono altri messaggi di errore. A volte possono essere utilizzati tutti i *flag*; in questo caso la tecnica in cui tutti i *flag* sono impostati viene chiamata *Christmas tree* mentre quella in cui tutti i flag resettati viene chiamata *null*.

Sniffing

La tecnica che consente di leggere i pacchetti quando attraversano la rete viene comunemente chiamata *packet sniffing*. Se si inviano informazioni non cifrate in rete, lo *sniffing* è uno strumento di utilizzo immediato per la loro cattura.

Il modo più semplice per applicare lo *sniffing* è controllare una macchina che si trova in una posizione privilegiata rispetto al traffico che ci interessa, ad esempio un *router* oppure un *server* (tipicamente tali macchine sono ben protette, anche dal punto di vista fisico, per cui ci si riduce ad attaccare macchine meno sicure).