SPOOFING

Sicurezza delle reti
Non bisogna essere sorpresi dal fatto che le reti di computer siano l'obbiettivo preferito, sia oggi sia in futuro, da parte di aggressori. Visto che un attacco su larga scala può mettere a rischio migliaia di sistemi informatici, con potenziali perdite del valore di milioni di euro, gli attacchi di rete sono materia di grande interesse. Esistono diversi tipi di minacce alla rete, ma tuttavia il senso generale è lo stesso: esse mirano infatti a compromettere la riservatezza, l'integrità o la disponibilità dei dati, del software e dell'hardware.
Le motivazione che spingono un aggressore a sferrare un attacco sono sostanzialmente quattro: la sfida, la fama, il denaro e l'ideologia.....

Spoofing: cos'è e come avviene
Indovinando o riuscendo ad ottenere le credenziali di autenticazione di rete di un qualsiasi utente o comunque una qualsiasi entità, un aggressore può creare una comunicazione completa sotto l'identità dell'utente. Strettamente correlato è lo spoofing: per sfoofing si intende infatti “l'arte della contraffazione dei pacchetti, intendendo per pacchetto una qualsiasi sequenza di dati distinta trasmessa su di una rete”.
In una rete di computer con il termine “spoofing” s'intende il sistema che permette di creare un pacchetto IP, ad hoc, nel quale viene falsificato l'indirizzo IP del mittente.
Durante lo spoofing, infatti, l'attaccante autentica la propria macchina nelle rete bersaglio usando i pacchetti che provengono da un host “fidato”.
Le tecniche di spoofing sono diverse, le più note e adoperate sono:
• Spoofing dell'IP
• Spoofing del DSN
• Spoofing dell'ARP
• Web Spoofing
• SMS Spoofing
• Mail Spoofing

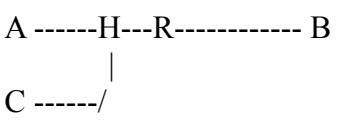
IP Spoofing
L'Ip spoofing è l'attacco più diffuso dal momento che è il più facile da eseguire. Tale attacco è reso possibile dal fatto che la maggior parte dei router all'interno, per esempio, delle reti aziendali controllano durante la richiesta di accesso ai servizi, solo l'indirizzi IP di destinazione e non quello di provenienza. Nell'intestazione di un pacchetto IP si trova, come detto in precedenza, il Source Address dove si trova l'indirizzi IP del mittente. Se chi attacca, modifica questo campo può far credere, al sistema bersaglio, che un pacchetto IP sia stato trasmesso da una macchina differente ricevendo le risposte direttamente sul falso IP.
Gli attacchi di IP Spoofing possono essere divisi in tre categorie:
• IP Spoofing non cieco: è attuabile in una rete LAN; quando chi attacca cerca di farsi passare per un host che è nella sua stessa sottorete .
• IP Spoofing cieco : quando l'attaccante cerca di farsi passare per un host di una qualsiasi sottorete.
• Attacchi DoS: l'attaccante cerca di bloccare un host per impedire a quest'ultimo di svolgere la normale attività oppure per prenderne il controllo .

Spoofing non Cieco
Solitamente i vari host (PC) di una sottorete sono collegati da apparecchi (HUB) che, per far arrivare un pacchetto ad un determinato host, lo trasmettono in broadcast (Contemporanenamente) a tutti i computer della sottorete.
Quando il pacchetto arriva ad un determinato host, quest'ultimo esamina l'indirizzo di destinazione

contenuto nel pacchetto. Se questo indirizzo coincide con quello dell'host stesso, il pacchetto viene processato, altrimenti viene scartato in quanto era destinato ad un altro host. Tuttavia esiste una modalità particolare in cui è possibile impostare la scheda di rete: la modalità promiscua. Quando la scheda di rete si trova in questa modalità, permette di processare tutti i pacchetti che arrivano. Come già accennato sopra, nel caso dello Spoofing non cieco l'attaccante sta cercando di farsi passare per un host che fa parte della sua sottorete; quindi, impostando la scheda di rete in modo promiscuo, egli riesce a leggere tutti i pacchetti indirizzati all'host che intende impersonare e può così scoprire Sequence number e Acknowledgement number della connessione in corso e cercare di inserirvisi. Alcuni tipi di attacchi che possono essere messi a segno con questa tecnica sono la chiusura di una connessione esistente e l'Hijacking.

Chiusura di una connessione esistente
Avendo a disposizione Sequence number e Acknowledgement number di una connessione l'attaccante può spedire in un momento preciso un pacchetto con l'intento di far cadere la connessione.
Per raggiungere questo obiettivo può usare uno dei due flag RST o FIN compresi nell'header dei pacchetti TCP.
Chiusura di una connessione esistente usando il flag RST
Per procedere al reset di una connessione esistente l'attaccante procede secondo alcuni passi.
Immaginiamo esista una situazione di questo tipo:

A e C = Host della stessa sottorete
B = Host di una rete diversa da A e C
H = HUB
R = Router che delimita la sottorete



Supponiamo che tra gli host A e B esista una connessione e che l'attaccante
si trovi nella postazione C. Per cercare di resettare la connessione esistente, come prima cosa l'attaccante aspetterà di ricevere un pacchetto proveniente dalla connessione A-B. Supponendo che riceva un pacchetto proveniente da B verso A,
egli prima calcolerà il Sequence number a partire dall'Acknowledgement number del pacchetto ricevuto, poi costruirà e spedirà un pacchetto con le seguenti impostazioni:
Campi del pacchetto IP:
IP sorgente = A (IP Spoofato).
IP destinazione = B .
Campi del Pacchetto TCP:
Porta Sorgente = Porta usata dall'host A .
Porta Destinazione = Porta usata dall'host B .
Sequence number contenente il valore appena calcolato .
Flag RST impostato .
Il risultato sarà il reset della connessione.
Ci sono però dei problemi tecnici:
questo metodo, infatti, funziona solo se il pacchetto dell'attaccante arriva prima
della reale risposta dell'host A. L'host B riceverà due pacchetti con lo stesso
Sequence number (uno mandato dall'attaccante, e l'altro mandato dall'host A),
quindi prenderà per buono il primo arrivato e scarterà il secondo credendolo un duplicato.

Chiusura di una connessione esistente usando il flag FIN

Per procedere alla chiusura di una connessione esistente usando il flag FIN
l'attaccante ha la possibilità di controllare se la connessione è stata chiusa in quanto l'host che riceverà il pacchetto di FIN risponderà con un pacchetto di Acknowledgement.
Riprendiamo la situazione precedente:

A ------H---R---------- B
|
C ------/

Supponiamo che tra gli host A e B esista una connessione e che l'attaccante
si trovi nella postazione C. Per cercare di resettare la connessione esistente, come prima cosa l'attaccante aspetterà di ricevere un pacchetto proveniente dalla connessione A-B. Supponendo che riceva un pacchetto proveniente da B verso A,
egli prima calcolerà il Sequence number a partire dall'Acknowledgement number del pacchetto ricevuto, poi costruirà e spedirà un pacchetto con le seguenti impostazioni:
Campi del pacchetto IP:
IP sorgente = A (IP Spoofato).
IP destinazione = B.
Campi del Pacchetto TCP:
Porta Sorgente = Porta usata dall'host A.
Porta Destinazione = Porta usata dall'host B.
Sequence number contenente il valore appena calcolato.
Acknowledgement number contenente il valore appena calcolato.
Flag FIN impostato.
A questo punto resterà in ascolto in attesa di un pacchetto di Acknowledgement da parte di B. Se lo riceve é sicuro che da questo momento B risponderà a tutti i pacchetti ricevuti da A con un pacchetto di reset credendo siano bugs facendo, tra l'altro, cadere anche l'altro senso di connessione.

L'Hijacking
L'Hijacking è una tecnica molto raffinata che permette di intromettersi in una connessione esistente e prenderne il controllo. Il fenomeno dell'Hijacking viene trascurato in quanto trovandosi già nella sottorete dell'host che si vuole impersonare basterebbe usare uno sniffer per catturare username e password per poi collegarsi "legalmente". Tuttavia è possibile trovarsi in situazioni in cui, ad esempio, vengono usate password "usa e getta" e quindi, anche se l'attaccante riuscisse a sniffarne qualcuna, quando andrà ad usarle queste saranno già scadute.
Prima di proseguire con la spiegazione sul funzionamento dell'Hijacking è necessario chiarire cosa si intende per stato di **desincronizzazione di una connessione**.
Per semplicità indicheremo con:
SVR SEQ il Sequence number del prossimo byte che il server spedirà
SVR ACK il prossimo byte che il server si aspetta di ricevere
SRV WND la grandezza della finestra di ricezione del server
CLT SEQ il Sequence number del prossimo byte che il client spedirà
CLT ACK il prossimo byte che il client si aspetta di ricevere
CLT WND la grandezza della finestra di ricezione del client

L'attacco
Riprendiamo la situazione precedente:

A e C = Host della stessa sottorete
B = Host di una rete diversa da A e C
H = HUB

R = Router che delimita la sottorete

A ------H---R---------- B
|
C ------/

Supponiamo che esista una connessione telnet da A verso B e che l'attaccante si trovi nella postazione C. Cosa succederebbe se quest'ultimo in un periodo di "calma" della connessione tra A e B mandasse un pacchetto spoofato a B in modo da far credere che provenga da A?
Semplice, B aggiornerebbe l'Acknowledgement number di A (SVR ACK) in base al pacchetto ricevuto desincronizzandosi dal Sequence number reale di A (CLT SEQ).
A questo punto i pacchetti spediti da A verranno scartati in quanto per B hanno un Sequence number errato.
C'è da notare che nell'esempio appena descritto non c'è una desincronizzazione da entrambe le parti, infatti l'host A accetterà tutti i pacchetti spediti da B come risposta ai comandi dell'attaccante, e quindi vedrà tutto quello che questi stanno facendo.
Per evitare ciò l'attaccante deve creare una situazione di desincronizzazione anche nell'altro senso di trasmissione spedendo un pacchetto spoofato ad A come se provenisse da B.
Il funzionamento si può sintetizzare in 4 punti:
1-> L'attaccante aspetta di ricevere il pacchetto SYN/ACK, proveniente dal server e diretto verso il client.
2-> Appena lo ha identificato spedisce un pacchetto di RST (Spoofato) verso il server e immediatamente dopo uno di SYN (sempre Spoofato) con gli stessi parametri, ma con un differente Sequence number.
3-> Il server chiuderà la prima connessione grazie al pacchetto RST, e ne aprirà una uguale ma con un Sequence number diverso, spedendo il pacchetto SYN/ACK.
4. L'attaccante non appena identifica quest'ultimo, spedisce il pacchetto ACK necessario a completare l'instaurazione della connessione. A questo punto la connessione è aperta, ma è in uno stato di desincronizzazione in quanto per il client il Sequence number corretto è quello che era presente nel pacchetto SYN/ACK intercettato dall'attaccante al punto 1, mentre per il server quello corretto è quello introdotto dall'attaccante nel punto 2.

IP Spoofing Cieco

Quando si parla di IP Spoofing solitamente ci si riferisce all'IP Spoofing cieco. Con questa tecnica l'attaccante cerca di farsi passare per un host qualunque d'internet, non facente parte della sottorete in cui si trova. In questo caso si parla di Spoofing cieco in quanto l'attaccante non avrà nessuna possibilità di vedere i pacchetti mandati in risposta ai pacchetti (spoofati) che ha spedito. Questi ultimi infatti saranno indirizzati all'host che egli sta impersonando, impedendogli quindi di venire a conoscenza del Acknowledgement number e Sequence number corretti per continuare la connessione.
Molte volte alcuni server danno un accesso privilegiato a degli host fidati attraverso servizi di "rlogin" senza password o servizi simili. In un caso di questo tipo l'unico controllo è fatto sul numero IP sorgente della connessione, quindi se un attaccante riuscisse ad aprire una connessione spoofando il proprio IP potrebbe lanciare dei comandi al server facendogli credere di essere l'host fidato.
Un problema che si presenta all'attaccante ancora prima della predizione del Sequence number del secondo pacchetto è che l'host che egli cerca di impersonare, non appena riceverà il secondo pacchetto, si renderà conto che non sta cercando di aprire una connessione:
quindi avviserà il server mandandogli un pacchetto di reset rendendo nullo il lavoro dell'attaccante.
Per impedire che ciò accada, quest'ultimo o aspetta che l'host da impersonare sia spento, o può cercare di "buttarlo giù" con un attacco del tipo Denail of Service.

Generazione del Sequence Number
Come fa l'attaccante a predire un numero a 32 bit?

Generazione in base alla regola dei 64k
• Incrementa ogni secondo il contatore del Sequence Number di una costante, solitamente 128000
• Se è stata aperta una connessione incrementa il contatore del Sequence Number di un'altra costante, solitamente 64000

Generazione in base al Tempo
Per generare il Sequence Number, dopo un'inizializzazione casuale, il contatore del Sequence Number viene incrementato ogni periodo di tempo prefissato.

Generazione Random
Con questa tecnica il Sequence Number viene generato quasi casualmente, ed è pressochè impossibile predirlo.

Come fa quindi l'attaccante a predire il Sequence Number per portare a termine il suo attacco?
Prima di tutto deve scoprire quale dei tre algoritmi per la generazione del Sequence Number è in uso sul server che vuole colpire. Per fare ciò manda qualche pacchetto SYN non spoofato per vedere ed analizzare le risposte del server.
Questi pacchetti di risposta gli permettono di capire con una certa facilità a quale dei tre algoritmi si trova di fronte.
-Per vedere se il server sta usando l'algoritmo che usa la regola dei 64k gli è sufficiente calcolare la differenza tra 2 pacchetti ricevuti e vedere se il numero ottenuto ` divisibile per 64000.
-Per capire se il server stà usando l'algoritmo che usa la regola in base al tempo dovrà fare dei campionamenti su una serie di pacchetti. Se i risultati di tutti i campionamenti danno un valore simile si può pensare che il server usi questo algoritmo per generare i Sequence Number.
-Se questi due test non vanno a buon fine probabilmente il server usa un algoritmo di generazione random del Sequence Number e per l'attaccante non sarà possibile continuare l'attacco. Se così non fosse il passo successivo sarà cercare di indovinare il prossimo Sequence Number che verrà generato, con le regole sopra descritte.

L'attacco
Per prima cosa l'attaccante si assicurerà che l'host che intende impersonare sia spento, sucessivamente, dopo aver capito di fronte a che tipo di algoritmo per la generazione del Sequence Number si trova, procederà secondo i seguenti passi:
1. spedirà un pacchetto SYN non spoofato

2. in base al pacchetto SYN/ACK di risposta e all'algoritmo usato calcolerà il prossimo probabile Sequence Number.

3. spedirà un pacchetto SYN spoofato con l'indirizzo sorgente dell'host fidato

4. spedirà il pacchetto ACK spoofato con l'indirizzo sorgente dell'host fidato con il Sequence Number appena calcolato.

Indovinare il numero corretto è abbastanza difficile. Certe implementazioni del protocollo TCP in alcuni sistemi facilitano il compito all'attaccante. In questi sistemi quando viene ricevuto un Sequence Number troppo alto rispetto a quello corretto viene generato un pacchetto di reset. Se invece, il Sequence Number è più basso di quello corretto non viene fatto assolutamente niente. Questo fatto viene sfruttato spedendo una serie di pacchetti ACK con Sequence Number crescenti partendo da un valore leggermente inferiore a quello predetto per arrivare ad uno un più alto.
A questo punto l'attaccante non ha la sicurezza matematica di essere riuscito ad aprire la connessione, ma ha comunque una probabilità abbastanza elevata. Poichè stava cercando di aprire una connessione con il servizio rlogin non gli sarà chiesta nessuna password per entrare.

Adesso con tutta probabilità, quindi, avrà accesso ad una shell. Il passo successivo solitamente sarà quello di inviare il comando **echo "+ +" > .rhosts** che ha l'effetto di consentire l'accesso al sistema senza password tramite servizi del tipo di rlogin a tutti i numeri IP.

Denial of Service (DoS)

Un attacco di tipo DoS ha come scopo finale escludere un determinato host dalla reta rendendolo irraggiungibile. Fondamentalmente esistono 3 categorie di DoS:

- Attacchi per l'esaurimento di banda, che si basano sull'inondare la rete dell'host bersaglio in maniera da consumare tutta la larghezza di banda a lui disponibile. Questo attacco può essere attuato in due differenti maniere: nel primo caso l'attaccante ha a disposizione una connessione più veloce della vittima e riesce dunque a saturarme la banda direttamente. Nel secondo caso, l'attaccante pur non avendo una connessione veloce, riesce a saturare la banda della vittima grazie all'utilizzo di altri host che hanno lo scopo di amplificare l'attacco (Smurf).
- Attacchi per l'esaurimento delle risorse, che hanno come scopo colpire il sistema piuttosto che la rete in cui si trova. In generale questo si traduce con il consumo di risorse come cicli di CPU, della memoria, ecc.. (SYN Flood).
- Attacchi contro difetti di programmazione che vanno a colpire bug, software o hardware. Solitamente si verificano quando vengono spediti dei dati non previsti all'elemento vulnerabile.

Molti attacchi di tipo Dos per il loro funzionamento fanno uso dell' IP Spoofing rendendo quesi impossibile capirne la provenienza.

Smurf

Lo Smurf è un attacco DoS che ha lo scopo di esaurire l'intera banda dell'host vittima, sfruttando sottoreti che fungono da amplificatori. Solitamente ad ogni sottorete è associato un indirizzo IP di broadcast che ha per lo più funzioni diagnostiche. Se un pacchetto è indirizzato ad un indirizzo di broadcast significa che deve essere elaborato da tutti gli host della sottorete.

Lo smurf combina questo meccanismo di risposta multipla, con l'IP Spoofing per creare un attacco pressoché impossibile da fermare. Il funzionamento è molto semplice: l'attaccante spedisce una serie di pacchetti ICMP ECHO REQUEST con l'indirizzo dell'host della vittima a degli indirizzi di broadcast. Il risultato è che tutti gli host della sottorete elaborano il pacchetto e generano una risposta, sempre un pacchetto ICMP ECHO REPLY, indirizzato all'host vittima.

SYN Flood

Il SYN Flood è un attacco DoS che ha come scopo ultimo l'esaurire le risorse del sistema vittima. Quando un client vuole instaurare una connessione, spedisce al server una pacchetto SYN. Quando il server riceve questo pacchetto alloca una certa quantità di risorse per una futura connessione e spedisce il pacchetto SYN/ACK aspettandosi il pacchetto ACK necessario per completare la connessione.

Se il terzo e ultimo pacchetto non arriva entro un certo tempo il server libera le risorse allocate in precedenza.

Il problema sfruttato da SYN Flood è che i sever, anche se molto potenti, esauriscono velocemente le risorse usate per la realizzazione dei collegamenti, quindi, se in una certo lasso di tempo vengono ricevute molte richieste parziali di connessioni il server esaurisce le risorse. L'idea dell'attacco è spedire una serie di pacchetti SYN ogni 10 sec in modo da consumare tutte le risorse del server. I pacchetti che l'attaccante spedisce devono avere l'indirizzo sorgente Spoofato con un indirizzo di un host inesistente o spento, poichè se l'host esiste, non appena riceverà il pacchetto SYN/ACK spedito dal server, risponderà con un pacchetto di reset ed il server libererà le risorse rendendo vani gli sforzi dell'attaccante. In una situazione di questo tipo infatti il server non riuscirà mai a liberare le risorse in quanto non appena sarà passato il tempo necessario per deallocare un pò di risorse arriverà subito un pacchetto SYN che le riallocherà.

Come si può capire questo attacco è molto pericoloso in quanto si può attuare anche con una connessione lenta, inoltre spoofando gli indirizzi IP sorgenti diventa quasi impossibile risalire all'attaccante.

Spoofing del DNS

Il DNS Spoofing è un termine che viene usato quando un DNS accetta ed usa informazioni non corrette fornite da un host che non ne ha l'autorità. Tale attacco può essere attuato in tre modi:

- Cache poisoning
- Simulazione delle risposte del DNS
- Manomissine fisica del DNS

DNS (Domain Name Server) è il sistema utilizzato per effettuare la conversione tra indirizzo IP e il nome dell' host. Esso può essere considerato come un database di grandi dimensioni distribuito tra più host in internet. Il servizio permette così di utilizzare i nomi e le parole di uso comune per ricercare ad esempio un sito internet.

Le garanzie vengono affidate al protocollo del DNS stesso: tale protocollo ha però delle vulnerabilità.

Come possiamo notare dal DNS Header, l'ID, formato da 16 bit, viene generato ogni volta che si deve fare una richiesta.Il campo che interessa agli Spoofer è il campo "Questions" :
ogni domanda ha un type, ed ogni risposta ha un type (per Type si intende la corrispondenza tra IP address e canonical name).

Un attacco basato sulla simulazione delle risposte,deve essere in grado di considerare tre variabili:

- l'ID: formato, come detto in precedenza da 16bit, è piccolo e facile da prendere
- la risposta: poiché ci sono servizi che interrogano il DNS di continuo, con un delay fisso tra le richieste, è possibile predire anche il momento in cui viene fatta una richiesta al DNS
- Porta UDP: solitamente il BIND (ovvero il server DNS più usato in internet) si affida al numero di porta progressivo fornito dal kernel.

Per difendersi da un attacco che simuli le risposte del DNS, occorrerà semplicemente utilizzare un resolver che genera un "ID truly random" e che scelga un numero di porta "truly random" in modo da aumentare in maniera sostanziale la sicurezza del DNS.

Cache poisoning

Il DNS cache poisoning e' un attacco ad un server dns in modo che chiunque richieda un dominio venga tuttavia reindirizzato ad un altro server, senza che se ne accorga. Tale attacco si basa sul fatto che tutti i DNS archiviano le richieste in una memoria cache, che include un TTL (Time to Live, vale a dire una parte dell' IP Header che determina il numero massimo di router che possono essere attraversati da un pacchetto). Con un TTL grande e una mappatura scorretta di alcuni indirizzi IP si ottengono informazioni altrettanto scorrette.

Supponiamo che:

- dns.my.org sia un "name server" con molti clients
- dns.my.org accetta richieste ricorsive
- pippo.net sia sotto il controllo del nemico
- client.my.org sia un client che usa per server DNS dns.my.org

client.my.org invia una richiesta al DNS per un dominio per cui dns.my.org non è autoritativo. dns.my.org accetta la richiesta ricorsiva e risale la gerarchia dei nomi per chiedere al server autoritativo. dns.my.org, ricevuta la risposta, la invia a client.my.org.

Quella appena descritta è la procedura normale che ogni richiesta dovrebbe seguire. Vediamo ora come avviene l'attacco.

Chi controlla pippo.net fa una richiesta a dns.my.org per l'indirizzo IP di www.pippo.net, dns.my.org non ha il record in cache, quindi richiede al server autoritativo di pippo.net, dns.pippo.net, l'informazione richiesta; in questo modo il nemico è venuto a conoscenza dell' ID!

Noto a questo punto l'ID, il nemico chiede a dns.my.org l'indirizzo www.microsoft.com (supponendo che l'indirizzo non sia in cache), immediatamente dopo si spaccia per il "name server"

autoritativo di microsoft, grazie all'IP Spoofing e spedisce una serie di risposte con l'ID che aveva ottenuto precedentemente, incrementandolo di volta in volta. Se gli attacchi riescono, dns.my.org avrà in cache la corrispondenza www.microsoft.com con l'indirizzo IP diverso da quello vero.
Come prevenire allora tale attacco ? E' necessario che il server DNS stesso sia sicuro. Per minimizzare i rischi ogni organizzazione e ogni responsabile per un dominio dovrebbero assicurarsi che il "name server" utilizzato non sia vulnerabile al cache poisoning.

Attacco fisico
Per attuare tale attacco si altera la tabella del DNS, cambiando a mano gli indirizzi IP che interessano. Per operare questo tipo di attacco occorre avere accesso alla configurazione di un "name server" autoritativo. L'attacco si svolge in quattro semplici passi:
• assicurarsi che il name server sia autoritativo (deve essere registrato presso interNIC)
• forzare le regole: si applica al BIND un path malizioso, si ricompila il tutto e si aggiungono i file.
• attacco con jizz.c: con un piccolo script bash si rende più semplice l'uso di jizz
• supponiamo di conosce i name server della vittima: supponiamo che il name sever sul quale ci si trovi sia autoritativo, allora usando jizz forziamo il name server ad inviare ai name server della vittima l'associazione 66.35.250.165 microsoft.com
dove 65.35.250.165 corrisponde a www.freashmeat.net.

Spoofing dell'ARP
Questo tipo di Spoofing è una variante sul tema dello spoofing IP e sfrutta un punto debole molto simile.
Un computer collegato a un network basato su IP/Ethernet ha due indirizzi: uno è l'indirizzo fisico della scheda di rete ed è chiamato MAC address, mentre il secondo è l'indirizzo IP.
-L'indirizzo fisico o MAC Address è , in teoria, un indirizzo unico e non sostituibile, che è immagazzinato all'interno della scheda di rete.
-L'indirizzo IP è virtuale, cioè viene assegnato via software.Su un segmento di rete è necessario che ogni macchina abbia un indirizzo univoco, ed assegnato solo a quella macchina.
I pacchetti IP sono consegnati attraverso l'Ethernet, il quale divide i pacchetti in frames, aggiunge l'header ethernet per la consegna e spedisce i pacchetti attraverso il cavo di rete fino allo switch. Lo switch decide a quale delle sue porte deve spedire il frame, comparando l'indirizzo di destinazione del frame con gli indirizzi memorizzati nella sua tabella interna, nel quale "mappa" la porta ethernet al MAC Address della scheda a cui è collegato; è quindi necessario trovare un
modo per cui partendo da un indirizzo IP (virtuale) risalire all'indirizzo fisico (reale).
Questo meccanismo di chiama ARP, ovvero Address Resolution Protocol, tale lavora inviando verso l'esterno con un broadcast un pacchetto " ARP request ". Un pacchetto ARP request in poche parole, invia a tutti i computer della rete una domanda: " Il tuo indirizzo IP è x.x.x.x? se si inviami indietro il tuo indirizzo MAC ".
Come detto questo pacchetto viene spedito in broadcast a tutti i computer sulla rete che sia una LAN (Local Area Network) che uno "switched lan" (rete complessa) e ciascun computer esamina il pacchetto, verifica se ha assegnato in quel momento l'indirizzo IP richiesto nel pacchetto ARP, e se questa condizione è verificata, invia indietro alla macchina richiedente un pacchetto " ARP reply" contenente il proprio MAC address. A questo punto la macchina che deve inviare il frame ethernet riceve il pacchetto ARP reply, estrae l'indirizzo MAC e invia il pacchetto alla macchina destinataria attraverso la rete.
Per ridurre al minimo il numero delle richieste ARP che vengono inviate su un segmento di rete, i sistemi operativi (e con essi router e switch) immagazzinano una cache delle entry ARP che ha finora ricevuto.
Quando un computer riceve un ARP reply, questo aggiorna la propria tabella con la nuova associazione IP address / MAC address e siccome l'ARP è protocollo SENZA SESSIONE ed è un protocollo INAFFIDABILE (nel senso che il protocollo ARP invia solo la parte dati ed inoltre se il

pacchetto ARP non giunge a destinazione non viene re-inviato ad oltranza) molti sistemi operativi e dispositivi che necessitano di fare cache delle entry ARP (router appunto) aggiornano la propria tabella solo nel caso in cui alla macchina giunge una risposta alla sua request (ovvero quando ad un ARP Request, riceve la relativa ARP Reply).
Date queste premesse iniziamo a spiegare cos'è l'ARP SPOOFING ovvero l'invio "forzato" di pacchetti ARP reply, in cui il computer che riceve questo pacchetto ARP reply viene messo in condizione tale per cui crede di spedire i frame ethernet al computer A (ovvero quello legittimo destinatario della connessione) ma che invece fisicamente lo spedisce al computer B il quale ha "spooffato" la entry ARP, creando quindi nella cache della vittima una associazione tra IP inesistente e MACaddress, (vero), del mittente, forzando l'update della macchina bersaglio" e generando quello che si chiama AVVELENAMENTO ARP.
Per difendersi da un attacco del genere si possono usare un Ipv6, un IPsec o una tabella ARP statica, in più si può adottare anche la SARP, Secure ARP ,che permette di autenticare il sender o di creare il port security forzando l'associazione della porta con un solo MAC address. La soluzione migliore è realizzare una connessione 802.1x su server RADIUS che forza l'autenticazione remota.

Web Spoofing
Il web spoofing consiste nel far credere ad un utente che sta visitando il sito web desiderato, con la pagina richiesta, mentre invece, ne guarda un'altra modificata. Questa tecnica fa un uso massiccio di script realizzati con il linguaggio JavaScript. Supponiamo di visitare il sito www.acquisti.net; al momento della connessione al sito, la falsa pagina principale, residente sul server web attaccante e creata opportunamente simile all'originale, si colloca immediatamente tra il nostro browser web e le altre pagine richieste successivamente al server fidato: la finta pagina si comporterà, quindi, come un server proxy non voluto e non visibile. Così, l'attaccante, potrà vedere tutto ciò che vede il visitatore del sito: informazioni, moduli e password. Usando JavaScript, chi attacca, è in grado di reindirizzare la connessione, modificare la barra di stato del browser, disabilitare alcune funzioni dei menu del browser e impedire la visualizzazione del codice della pagina. La soluzione al problema è drastica, bisognerebbe disattivare, dal browser web, il supporto di JavaScript, ma soprattutto visitare solo siti veramente fidati, assicurarsi che la riga degli indirizzi del browser sia sempre visibile, ed infine Fare attenzione all'indirizzo URL visualizzato dal browser, assicurandosi che punti sempre al server a cui si pensa di essere connessi.

SMS Spoofing
Lo spoofing SMS consiste nell'invio di SMS (Short Message Service) il cui mittente è falso oppure inesistente. Tutti gli operatori di telefonia mobile offrono il servizio di invio SMS attraverso appositi Gateway SMS raggiungibili via modem. È possibile collegarsi via telefono a questi gateway ed ottenere il servizio di invio SMS attraverso uno specifico protocollo di comunicazione.
Due sono i protocolli usati per comunicare con i gateway SMS:
TAP (Telematic Application Program)
UCP (Universal Computer Protocol)
Analizziamo l'UCP, perché è il protocollo usato per effettuare lo spoofing. Il pacchetto UCP è composto da:
<STX>HEADER/DATA/CRC<EXT>
<STX> è l'inizio del messaggio
<EXT> è la fine del messaggio
I servizi soggetti a SMS spoofing sono:
01: invio di sms singolo
02: invio di sms multiplo.
Il campo DATA cambia da servizio a servizio. Per il servizio 01 (invio di sms singolo) in DATA avremo:
AdC [string of numeric char]: indica il destinatario (non è possibile inserire il carattere "+")
OadC [string of numeric char]: indica il numero sorgente del messaggio

OAC [string of char]: indica il codice di autenticazione del mittente (vuoto)
MT [1 numeric char]: indica il tipo di sms inviato
AMsg [string of char]: indica il messaggio vero e proprio.
Come detto sopra, Amsg è il messaggio da inviare, i caratteri che compongono il messaggio non sono inviati in chiaro, ma vengono codificati in stringhe IA5: la codifica IA5 non fa altro che trasformare un carattere nel corrispondente codice ASCII. In rete esistono diversi programmi per comunicare con i server SMS, il più diffuso è SMS Client. Per fortuna ormai quasi tutti i server che provvedono allo smistamento e all'instradamento degli SMS sono immuni a questo tipo di attacco.

Mail Spoofing
Con mail spoofing si fa apparire un allegato di una mail come se fosse di un tipo diverso da quello che è realmente. Questo attacco si basa su una vulnerabilità dei MIME TYPE, usati per inviare e-mail (il MIME Type specifica il tipo di dati che vengono trasferiti attraverso il protocollo HTTP o SMTP).
Questo tipo di Spoofing è una tecnica molto semplice, i cui effetti possono essere disastrosi: basta modificare in maniera opportuna il nome dell'allegato da inviare:
esempio pratico: il nome allegato è “pippo.exe”, cambiando il nome da:
“pippo.exe” a “pippo.jpg (255 spazi vuoti) .exe”
Quando l'e-mail arriva, il client interpreterà il nome dell'allegato solo come pippo.jpg. L'ignaro utente cercherà di visualizzare il file, ma in realtà eseguirà involontariamente pippo.exe.
L'esecuzione di um programma creato ah hoc può portare alla perdita di dati oppure all'apertura di una back-door sulla macchina della vittima. L'unica soluzione di difesa a questo tipo di attacco consiste nel NON aprire mai gli allegati di persone non fidate.

Conclusioni:
Lo Spoofing è sempre intenzionale, ma di fatto, cattive configurazioni e piccole disattenzioni nella propria rete possono causare lo stesso effetto di un attacco deliberato. Gli attacchi subdoli, come lo Spoofing, sono molto più blandi di quelli manifesti. In questo senso lo spoofing ha un enorme vantaggio rispetto alle vulnerabilità vere e proprie, quindi richiede maggiore attenzione e applicazione per difendersi efficacemente: All'interno del certificato, il nome visualizzato accanto alla voce **“Rilasciato a”** deve corrispondere o quantomeno essere simile a quello del sito che state visitando. Se invece il nome è molto diverso, è possibile che sia in corso un attacco di Web spoofing. Se non siete certi dell'autenticità di un certificato, non inserite informazioni personali, evitate di eseguire qualsiasi operazione e lasciate immediatamente il sito.
È inoltre consigliabile sniffare il traffico della propria rete periodicamente ed evitare di fare clic su eventuali collegamenti sospetti in messaggi di posta elettronica o annunci pubblicitari online. In caso di dubbi, non fate clic sul collegamento, ma digitate l'indirizzo del sito nella barra degli indirizzi del browser o verificate in altro modo l'autenticità del collegamento. Ricordate: diffidate delle offerte troppo allettanti!!!!

Riferimenti
(1) http://sicurezza.html.it/articoli/leggi/2174/tecniche-lo-spoofing/
(2) http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0102/Spoofing_Slide.pdf
(3) http://www.orkspace.net/docs/IP_Spoofing_in_Scioltezza.pdf
(4) http://www.securityfocus.com/infocus/1674
(5) C. Pfleeger, S. Pfleeger: Sicurezza in informatica – Pearson 1a ed. italiana – 2004.
(6) ”A short overview of IP spoofing: PART I” reperibile in rete
(7) ”A short overview of IP spoofing: PART II” reperibile in rete
(8) ”IP-spoofing Demystified” tratto da ”Phrack Magazine Issue 48”
(9) ”A Simple Active Attack Aganinst TCP” reperibile in rete