Spoofing

Corso di Sistemi di Elaborazione:
Sicurezza su Reti

A.A. 2001/2002

Prof. A. De Santis

A cura di:
Angelo Celentano matr. 53/11544
Raffaele Pisapia matr. 53/10991
Mariangela Verrecchia matr. 56/001119

Introduzione

- Cosa è lo spoofing
- Tipi di spoofing
- Parleremo di
  - web spoofing
  - mail spoofing
  - sms spoofing
  - ARP spoofing
  - DNS spoofing

.. ed in particolare di IP spoofing

Cosa è lo spoofing

Dal Dizionario informatico:

Spoofing (ingl.), imbroglio.

1) Atto di introdursi in un sistema informativo senza averne l'autorizzazione. L'intruso cambia il proprio numero IP, non valido per l'accesso al sistema, in uno autorizzato.

2) Tecnica che permette di rendere le linee di comunicazione sgombre, tramite router, da pacchetti inviati per il controllo della connessione.

Cosa è lo spoofing

Dal Dizionario informatico:

Spoofing (ingl.), imbroglio.

1) Atto di introdursi in un sistema informativo senza averne l'autorizzazione. L'intruso cambia il proprio numero IP, non valido per l'accesso al sistema, in uno autorizzato.

2) Tecnica che permette di rendere le linee di comunicazione sgombre, tramite router, da pacchetti inviati per il controllo della connessione.

Spoofing conosciuti

Esistono diversi tipi di spoofing, i più noti ed utilizzati sono:

- web spoofing
- mail spoofing
- sms spoofing
- ARP spoofing
- DNS spoofing
- IP spoofing

In ogni caso si tratta di far credere alla vittima che si è "qualcosa" di diverso, un hostname, un indirizzo ethernet o altro ancora…

Analizziamo questi tipi di spoofing…

Argomenti

Gli argomenti che tratteremo:

- **web spoofing**
- mail spoofing
- sms spoofing
- ARP spoofing
- DNS spoofing
- IP spoofing

Web spoofing

Cos'è?

Il web spoofing consiste nel far credere ad un utente che sta visitando il sito web desiderato, con la pagina richiesta, mentre ne guarda una modificata.

Questa tecnica fa uso massiccio di Javascript

Web spoofing

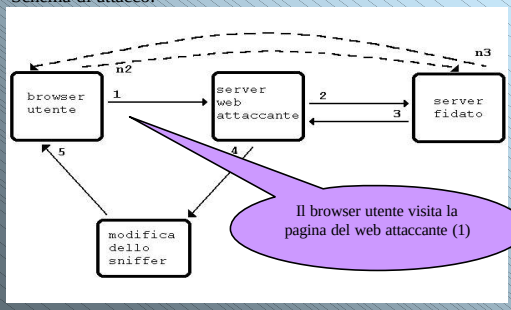
Supponiamo di visitare `www.pippo.net`

La pagina principale di `www.pippo.net` si frappone tra il nostro client e le pagine richieste successivamente: si comporterà come un proxy non voluto e non visto.

Così potrà vedere tutto ciò che vede il client: siti, form e password!

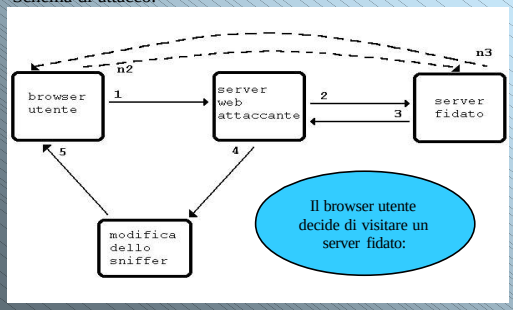
Web spoofing

Schema di attacco:



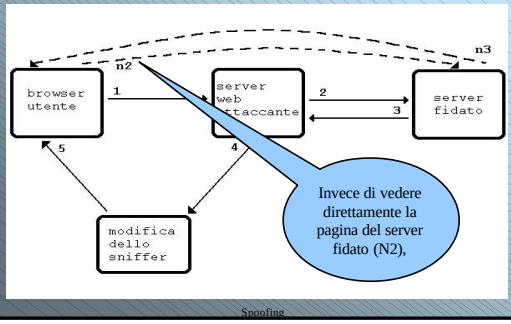
Web spoofing

Schema di attacco:



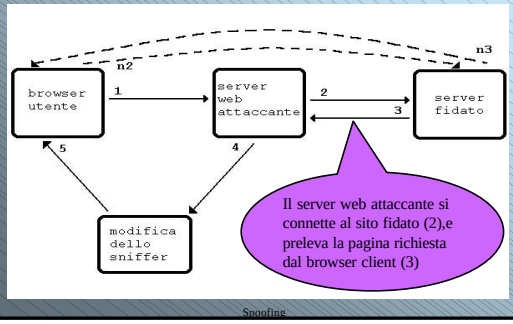
Web spoofing

Schema di attacco:



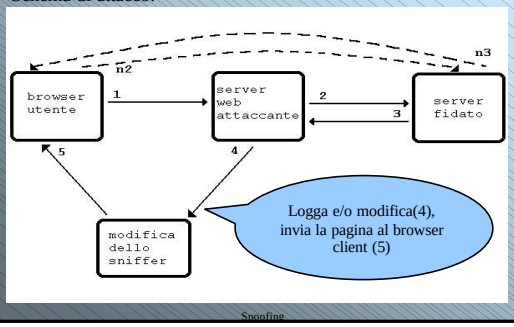
Web spoofing

Schema di attacco:



Web spoofing

Schema di attacco:



Web spoofing

Con Javascript l'host nemico reindirizza la connessione.

- modifica la status bar del browser
  - ⇒ crediamo di avere le informazioni corrette
- disabilita alcune funzioni dei menù del browser
  - ⇒ impedisce la visualizzazione del codice

Web spoofing

Soluzione :

Disabilitare Javascript dal nostro browser

Anche se drastica, questa è l'unica soluzione possibile.

Web spoofing

Importante :

Questa tecnica di attacco si basa sul fatto che la pagina web maliziosa sia contattata da un browser!

Visitando solo siti fidati è difficile subire web spoofing.

Argomenti

Gli argomenti che tratteremo:

- web spoofing
- **mail spoofing** ⇐
- sms spoofing
- ARP spoofing
- DNS spoofing
- IP spoofing

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.

Mail spoofing

E' una tecnica semplice,i cui effetti possono essere disastrosi: basta modificare in maniera opportuna il nome dell'allegato da inviare.

Esempio pratico:

Nome allegato: `pippo.exe`

Cambiamo il nome da `pippo.exe` a `pippo.jpg` `.exe`

255 spazi vuoti!

Mail spoofing

Quando la 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 involontariamente eseguirà `pippo.exe`

L'esecuzione di un programma creato *ad hoc* può portare alla perdita di dati oppure all'apertura di *back-door* sulla macchina vittima.

`pippo.exe` in realtà esegue `format c:`!!!

Mail spoofing

Soluzioni?

L'unica soluzione e difesa a questo tipo di attacco consiste nel non aprire mai gli allegati inviati da persone di cui non ci fidiamo.

Argomenti

Gli argomenti che tratteremo:

- web spoofing
- mail spoofing
- **sms spoofing**
- ARP spoofing
- DNS spoofing
- IP spoofing

SMS spoofing

Lo spoofing SMS consiste nell'invio di SMS (short message service) il cui mittente è falso o inesistente.

Gli operatori di telefonia mobile offrono il servizio di invio SMS tramite appositi SMS-gateway raggiungibili via modem.

E' possibile collegarsi via telefono agli SMS-gateway ed ottenere il servizio di invio SMS attraverso un protocollo di comunicazione.

SMS spoofing

Due sono i protocolli di comunicazione con gli SMS-gateway:

- TAP (Telematic Application Program)
- UCP (Universal Computer Protocol)

Analizziamo UCP, perché è il protocollo usato per effettuare lo spoofing.

SMS spoofing

UCP

Il pacchetto UCP:

<STX>HEADER/DATA/CRC<EXT>

<STX> è l'inizio del messaggio
<EXT> è la fine del messaggio

SMS spoofing

I campi dell'header del messaggio, separati da "/", sono:

- ✓TNR [numeric char]: intero tra 0 e 99, è il numero di transazione casuale
- ✓LNG [5 numeric char]: il numero di char tra <STX> e <ETX>
- ✓O\R [1 char]: O è richiesta di servizio
  R è la risposta alla richiesta di servizio
- ✓OPN [2 numeric char]: codice del servizio richiesto.

SMS spoofing

La lista completa dei servizi è elencata nel documento Ufficiale di UCP, "ETS 133-3", redatto da ETSI (European Technology Standard Institute)

I servizi soggetti a SMS spoofing sono:
01: invio di sms singolo
02: invio di sms multiplo

SMS spoofing

Il campo DATA cambia da servizio a servizio.

Per il servizio 01 (invio di sms singolo) in DATA avremo:

- AdC [string of numeric char] destinatario
- OAdC [string of numeric char] numero sorgente del messaggio
- OAC [string of char] codice di autentificazione del mittente
- MT [1 numeric char] tipo di sms inviato
- AMsg [string of char] il messaggio vero e proprio

Non è possibile inserire il carattere "+"

3 indica alfanumerico

vuoto

SMS spoofing

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.

SMS spoofing

Per mandare un sms al numero `3471234567` dal numero `42` il messaggio "`Linux Rules`" ecco cosa si deve comunicare al gateway:

```
<STX>04/00046/O/01//00393471234567/42//3/4C696E75782052756C6573/F6<ETX>
```

Se la query è stata accettata, il gateway risponderà con:

```
<STX>01/00035/R/01/A/00393471234567:090800114008/A0<ETX>
```

Poi occorre solo attendere lo smistamento da parte del gateway...

SMS spoofing

Invio di sms multipli: codice 02

Inviando al gateway più messaggi con un'unica chiamata, il gateway non si accorge che la destinazione dei messaggi è sempre uguale!

SMS spoofing

Come comunicare con il server sms?

In rete esistono diversi programmi, tutti facilmente reperibili. Il più semplice è `sms_client`, prelevabile da `http://www.styx.demon.co.uk`

SMS spoofing

Soluzioni?

Fortunatamente i gateway che provvedono allo smistamento e all'instradamento degli sms sono ormai immuni a questo tipo di attacco.

Argomenti

Gli argomenti che tratteremo:

- web spoofing
- mail spoofing
- sms spoofing
- **ARP spoofing**
- DNS spoofing
- IP spoofing

ARP spoofing

Una LAN può essere attaccata dall'interno se vi sono utenti maliziosi.

Questo attacco è applicabile solo su LAN ethernet.

Viene sfruttata una modalità promiscua delle schede ethernet

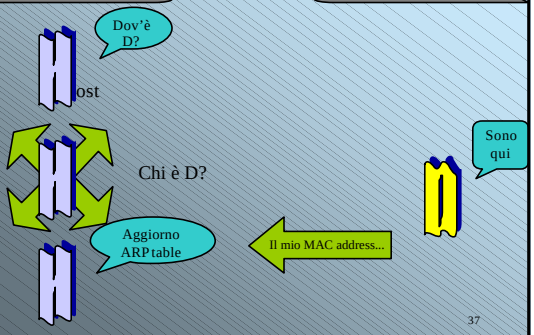
Una scheda ethernet in modalità promiscua è in grado vedere tutto il traffico della LAN.

ARP spoofing

Ricordiamo come funziona ARP (address resolution protocol)

ARP è il protocollo che provvede a far conoscere e diffondere il MAC address di una scheda su una LAN.

ARP spoofing



ARP spoofing

Esempio di attacco:

Alice invia al Nemico i dati destinati a Bob.

ARP spoofing

Distinguiamo due casi:

- LAN con HUB
- LAN con SWITCH

ARP spoofing

LAN con HUB

Un HUB lavora sul layer 1 del modello ISO/OSI.
Quando riceve dati su una porta, rimanda questi dati a tutti i dispositivi ad esso collegato.

Se è presente una scheda ethernet in modalità promiscua essa sarà in grado di analizzare e registrare tutto ciò che passa sulla rete locale.

Anche dati importanti!

Usando un programma di analisi del traffico (sniffer) si è in grado di catturare i pacchetti visti dalla nostra scheda ethernet.

ARP spoofing

LAN con HUB

E' difficile capire se sulla LAN è presente una scheda ethernet in modalità promiscua.

Esistono tuttavia degli accorgimenti che possono rivelare la presenza di una siffatta scheda.

- Ping modificato
- TCP SYN modificato
- Analisi del traffico verso il DNS

ARP spoofing

LAN con HUB

Ping modificato:

Una scheda di rete in modalità promiscua non utilizza il filtro basato sul MAC address: inviamo un pacchetto ICMP ECHO REQUEST (ping) con un MAC address inesistente.

Le macchine che rispondono hanno la scheda in modalità promiscua

ARP spoofing

LAN con HUB

Uso del flag TCP SYN:

Inviamo un pacchetto TCP SYN su una porta non standard.
Si possono ricevere due tipi di risposte:
TCP SYN/ACK la porta è in listening
TCP RST la porta è chiusa

Se la macchina è pulita, invierà un pacchetto RST.

ARP spoofing

LAN con HUB

Elevato traffico interno verso un DNS:

Molti sniffer consultano spesso il DNS per risolvere l'indirizzo IP dei pacchetti che hanno intercettato.

Se il DNS viene consultato più del solito, potrebbe esserci una scheda ethernet in modalità promiscua sulla nostra LAN.

ARP spoofing

LAN con HUB

Prevenzione:

- Protocolli per cifrare il traffico che viaggia sulla LAN
- Installare uno SWITCH che instrada il traffico sulla LAN, agendo al layer 2 del modello ISO/OSI.

Ma uno SWITCH ci protegge?

ARP spoofing

LAN con SWITCH

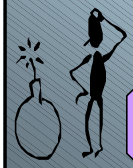
Uno SWITCH su una LAN smista i pacchetti a layer 2

Nonostante la presenza dello SWITCH è possibile effettuare un attacco Man in the Middle, senza la necessità di settare la scheda Ethernet in modalità promiscua.

Viene usata una tecnica chiamata *arp poisoning*

ARP spoofing

LAN con SWITCH



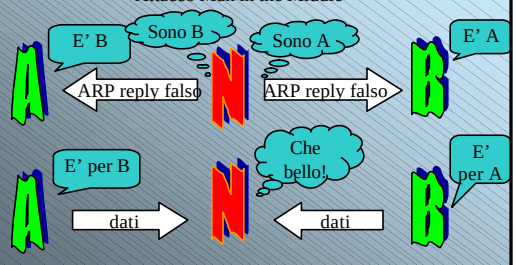
L'arp poisoning è l'attività di contraffazione della ARP table di una macchina.

Se il nemico spedisce ad una macchina un ARP reply con il proprio MAC address e con l'indirizzo IP della macchina obiettivo, tutto il traffico indirizzato a quest'ultima verrà instradato al nemico.

Facendo questo per due diverse macchine obiettivo, avremo l'attacco Man in the Middle.

ARP spoofing

Attacco Man in the Middle



ARP spoofing

LAN con SWITCH

Soluzione:

Si configura lo SWITCH in maniera tale che il traffico in uscita da una porta possa cambiare MAC address.

ARP spoofing

Soluzioni software:

- Tabelle statiche di ARP

  Mediante il comando `arp –s hostname hardware_address` è possibile creare delle tabelle statiche di ARP: queste tabelle non possono essere modificate dall'esterno. E' oneroso per grandi LAN.

- Uso di ARPwatch

  E' un utility che controlla i cambiamenti della ARP table; se vengono notati cambiamenti ARPwatch avvisa tramite email e aggiorna i log.

Argomenti

Gli argomenti che tratteremo:

- web spoofing
- mail spoofing
- sms spoofing
- ARP spoofing
- **DNS spoofing**
- IP spoofing

DNS spoofing

Cos'è?

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.

DNS spoofing

DNS spoofing può essere attuato in tre modi:

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

DNS spoofing

DNS : una breve introduzione

Il DNS (Domain Name Server) è il sistema utilizzato per effettuare la conversione:

Indirizzo IP ⟷ Nome di host

E' un database di grandi dimensioni distribuito tra più host in internet.

DNS spoofing

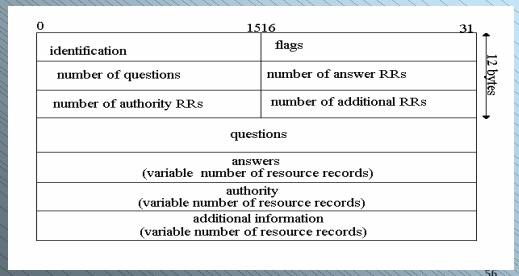
I dati richiesti e/o inviati da un DNS viaggiano sulla rete utilizzando il protocollo UDP

Le garanzie di sicurezza vengono affidate al protocollo DNS stesso

Il protocollo ha delle vulnerabilità

DNS spoofing

Header di un pacchetto DNS:



DNS spoofing

- Id [16 bit] viene generato ogni volta che si deve fare una query. La risposta ad una query, contiene lo stesso ID

Il campo interessato allo Spoofing è il campo QUESTIONS: ogni domanda ha un type, ed ogni risposta ha un type

A type è l'obiettivo del nemico:

A type è la corrispondenza [IP address – canonical name]

DNS spoofing

Simulazione delle risposte del DNS

Dato il formato dell'header di un pacchetto DNS, si ha che l'autenticità delle risposte è fondamentale!

Garanzie offerte:

- controllo del campo IDENTIFICATION
- risposta coerente con la domanda effettuata
- risposta inviata alla porta UDP scelta dal richiedente

DNS spoofing

Simulazione delle risposte del DNS

Un attacco basato sulla simulazione delle risposte deve essere in grado di considerare le tre variabili… (id, risposta, porta)

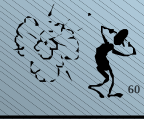
Supponiamo sia impossibile intercettare la query verso il DNS…

Si opera un attacco blind!

DNS spoofing

Simulazione delle risposte del DNS

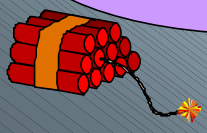
- ID: un ID a 16bit è piccolo e facile da predire (anche per come viene generato all'interno di bind!)
- Poiché ci sono servizi che interrogano DNS di continuo, con delay fisso tra le richieste, è possibile predire anche il momento in cui viene fatta una query al DNS.
- Porta UDP: solitamente BIND si affida al numero di porta progressivo fornito dal kernel.



DNS spoofing

Simulazione delle risposte del DNS

Utilizzare un resolver che genera un ID truly random e che sceglie un numero di porta truly random aumenta in maniera sostanziale la sicurezza di DNS.



DNS spoofing

Cache poisoning

Con questo tipo di attacco, dati creati *ad hoc* vengono inseriti nella cache del name server.

Fortunatamente non è quasi più possibile trovare Name Server vulnerabili a questo tipo di attacco.

DNS spoofing

Cache poisoning

Su cosa si basa la tecnica cache poisoning?

Tutti i DNS archiviano le richieste in una memoria cache, che include un TTL (Time To Live).

Con un TTL grande e una mappatura scorretta di indirizzi IP si ottengono informazioni scorrette

DNS spoofing

Cache poisoning

Supponiamo:

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

DNS spoofing

Cache poisoning

`client.my.org` invia una query al dns per un dominio per cui `dns.my.org` non è autoritativo

`dns.my.org` accetta la query ricorsiva e risale la gerarchia dei nomi per chiedere al server autoritativo.

`dns.my.org`, ricevuta la risposta, la invia a `client.my.org`

Questa è la procedura normale che ogni richiesta dovrebbe seguire.

Vediamo come avviene l'attacco…

DNS spoofing

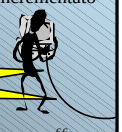
Cache poisoning

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`, `ns.pippo.net`, l'informazione richiesta.

Questa query contiene l'ID che sarà semplicemente incrementato per le prossime richieste.

Il nemico è venuto a conoscenza dell'ID!!!



DNS spoofing

Cache poisoning

Noto l'ID, il nemico chiede a `dns.my.org` l'indirizzo di `www.microsoft.com` (supponendo che l'indirizzo non sia in cache)

Immediatamente dopo si spaccia per il name server autoritativo di `microsoft.com` (grazie all'IP spoofing)…

…e spedisce una serie di risposte con l'ID che aveva ottenuto precedentemente, incrementandolo di volta in volta.

Questo perché nel frattempo `dns.my.org` può aver fatto altre query, e quindi non si ha la certezza che l'ID che la vittima si aspetta per `www.microsoft.com` sia esattamente il vecchio ID incrementato di 1

DNS spoofing

Cache poisoning

Se l'attacco riesce dns.my.org avrà in cache la corrispondenza `www.microsoft.com` con un indirizzo IP diverso da quello vero.

DNS spoofing

Cache poisoning

Un attacco di questo tipo poteva essere fatto per lungo periodo senza che ci si potesse accorgere facilmente di essere sotto attacco.

DNS spoofing

Cache poisoning

Prevenzione:

E' necessario che il server DNS stesso sia sicuro. Per minimizzare i rischi di un simile attacco ogni organizzazione e ogni responsabile per un dominio dovrebbero assicurarsi che il Name Server utilizzato non sia vulnerabile al cache poisoning.

DNS spoofing

Attacco fisico

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…

DNS spoofing

Attacco fisico

1. Assicurarsi che il NS sia autoritativo
   - Deve essere registrato presso ***interNIC***
2. Forzare le regole
   - Si applica a BIND un patch malizioso, si ricompila il tutto, e si aggiornano i file.
3. Attacco con `jizz.c`
   - Con un piccolo script bash si rende più semplice l'uso di `jizz`
4. Supponiamo di conoscere i NS della vittima…
   - Supponiamo che il NS sul quale ci si trovi sia autoritativo per i NS della vittima, allora usando `jizz` forziamo il NS ad inviare ai NS della vittima l'associazione:
     `66.35.250.165 www.microsoft.com`
     Dove 66.35.250.165 corrisponde a www.freshmeat.net

DNS spoofing

Un DNS spoof locale:

Ogni computer con sistema operativo win* ha il seguente file:
`C:\WINDOWS\hosts.sam`

In questo file sono contenute associazioni IP – host name come: `127.0.0.1 localhost`

E' possibile inserire indirizzi IP e gli host name ad essi corrispondenti

DNS spoofing

Se in coda al file `hosts.sam` si aggiunge la seguente riga:
`216.239.35.100 yahoo.com`
dove `216.239.53.100` è l'indirizzo IP di google

…ogni volta che nel browser si inserirà `yahoo.com` per visualizzare la pagina, il nostro browser invece di interrogare il name server, userà l'indirizzo riportato da `hosts.sam`

…invece di apparire la pagina di `yahoo`, apparirà `google.com`

Argomenti

Gli argomenti che tratteremo:

- web spoofing
- mail spoofing
- sms spoofing
- ARP spoofing
- DNS spoofing
- **IP spoofing**

IP spoofing

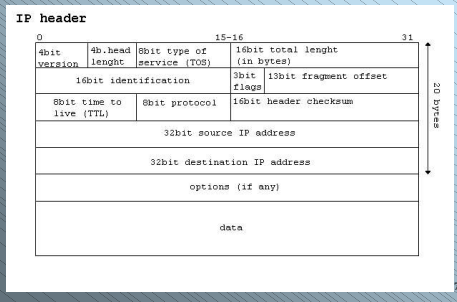
Cos'è?

L'IP spoofing è una tecnica di occultazione del proprio IP address: si basa sulla modifica di uno o più campi del pacchetto IP.

In pratica si falsifica l'indirizzo IP sorgente della connessione in modo da far credere di essere un altro host.

IP spoofing

Header di un datagramma IP



IP spoofing

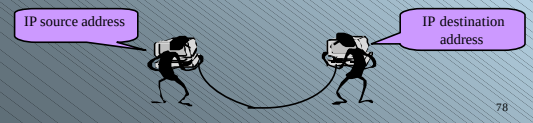
Campi interessati di un datagramma IP

- IP source address

  Indica da dove proviene la connessione in corso.

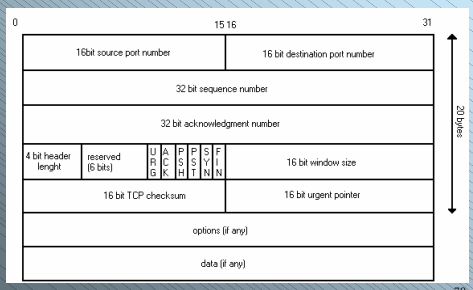
- IP destination address

  E' la destinazione, l'host a cui ci si vuol connettere



IP spoofing

Header di un pacchetto TCP



IP spoofing

Campi sfruttati in un pacchetto TCP

- source port — Porta dalla quale ha inizio la connessione
- destination port — Porta di destinazione della connessione
- Sequence Number (SN) — Numero sequenziale del pacchetto
- Acknowledge Number (AN) — Riconoscimento dei dati del pacchetto precedente
- SYN flag — Flag di sincronizzazione di una connessione
- FIN flag — Flag di fine connessione
- RST flag — Flag di terminazione immediata di una connessione

IP spoofing

TCP versus IP

IP	TCP
reliability : no	reliability: si
connectionless	connection oriented
accountability: no	accountability: si
layer 3 ISO/OSI	layer 4 ISO/OSI
manipolazione dati: si	manipolazione dati: no

relativamente allo spoofing

IP spoofing

Creazione di una connessione TCP/IP

Una connessione viene stabilita usando il “three way handshake”

client → server: SYN=1 ACK=0 SN=***X***

server → client: SYN=1 ACK=1 SN=***Y*** AN=***X+1***

client → server: SYN=0 ACK=1 SN=***X+1*** AN=***Y+1***

IP spoofing

Gestione SN e AN in una connessione

In ogni pacchetto TCP ci sono:

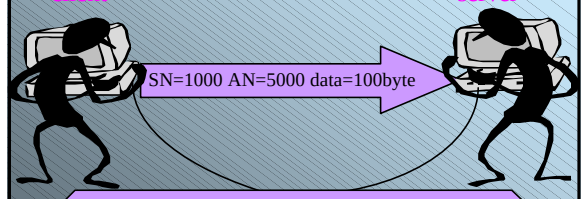
SN= numero di sequenza del primo byte contenuto

AN= numero del prossimo byte atteso; conferma la ricezione fino al byte indicato meno 1

IP spoofing

Gestione SN e AN in una connessione

client server



Il primo byte inviato ha SN 1000. Il client conferma la ricezione dei byte ricevuti in precedenza fino al 4999, e si aspetta che il prossimo byte abbia SN pari a 5000.

IP spoofing

Generazione del SN

Il sequence number è alla base di una connessione TCP: è importante per l'accountability

Poiché il nemico non è in grado di falsificare un pacchetto TCP, allora deve essere in grado di predire questo SN

Risulta importante il metodo di generazione del SN

IP spoofing

Generazione del SN

Tre sono i metodi usati per la generazione del SN:

1. Regola dei 64k
2. Generazione in base al tempo
3. Generazione random

IP spoofing

Generazione del SN

1. Regola dei 64k
   Ogni secondo il contatore del SN viene incrementato di una variabile, solitamente 128000 (128k); se una connessione è aperta allora il contatore viene incrementato di 64000 (64k)
2. Generazione in base al tempo
   L'inizializzazione del contatore è casuale al boot della macchina; in seguito il contatore viene incrementato di 1 ogni microsecondo.
3. Generazione random
   Il SN viene generato truly random (esempio di implementazione ed uso nei nuovi kernel di Linux)

IP spoofing

Chiusura di una connessione

Una connessione può essere chiusa in due modi:

Flag FIN	Flag RST
Non ci sono più dati da trasmettere, viene iniziata la procedura di chiusura (quattro passaggi richiesti)	La connessione è diventata instabile e viene chiusa immediatamente; RST può essere usato anche per rifiutare una connessione

IP spoofing

Tipi di Attacchi

Gli attacchi IP spoofing possono suddividersi in tre categorie:

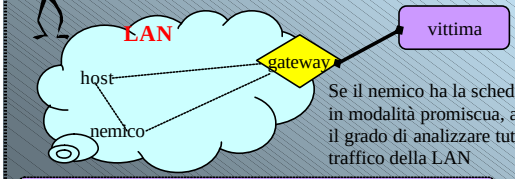
1. **IP spoofing non cieco:** attuabile in una LAN; il nemico cerca di farsi passare per un host che è nella sua stessa sottorete
2. **IP spoofing cieco:** il nemico cerca di farsi passare per un host di una qualsiasi sottorete
3. **Denial of Service(DOS):** il nemico cerca di bloccare un host per impedire a quest'ultimo di svolgere la normale attività o per prenderne il controllo (con spoof oppure hijacking)

IP spoofing

IP Spoofing non cieco

Cos'è?

In una LAN, il nemico cerca di farsi passare per un host che è nella sottorete.



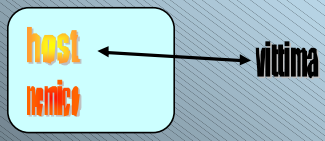
Se il nemico ha la scheda di rete in modalità promiscua, allora è il grado di analizzare tutto il traffico della LAN

Questo attacco presuppone la scheda di rete in modalità promiscua

IP spoofing

IP Spoofing non cieco

Esempio di attacco

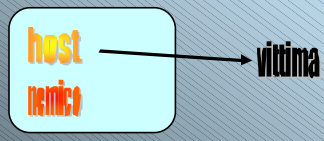


Supponiamo che l'host sia connesso con la vittima…

IP spoofing

IP Spoofing non cieco

Esempio di attacco

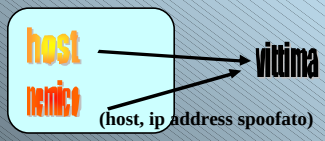


Come prima cosa il nemico fa chiudere la connessione dalla vittima verso l'host

IP spoofing

IP Spoofing non cieco

Esempio di attacco

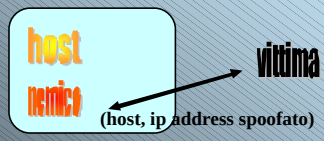


Il nemico apre una connessione con la vittima, fingendo di essere l'host.

IP spoofing

IP Spoofing non cieco

Esempio di attacco



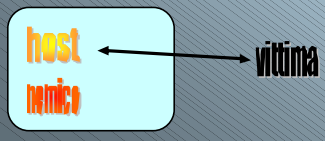
La vittima ignora ogni richiesta proveniente da host credendo che siano richieste errate, e stabilisce una connessione con il nemico, credendolo **host.**

IP spoofing

IP Spoofing non cieco: chiusura di una connessione esistente

Per poter chiudere una connessione esistente, il nemico ha a disposizione due metodi:

1. Uso del flag RST
2. Uso del flag FIN



IP spoofing

IP Spoofing non cieco: chiusura di una connessione esistente

1. Uso del flag RST
   - Il nemico attende dati dalla connessione **host-vittima**
   - … calcola il SN in base ai dati raccolti…
   - … spedisce un pacchetto con le seguenti impostazioni:
     - datagramma IP: IP source address : host
       IP destination address: vittima
     - pacchetto TCP: source port: porta usata dall'host
       destination port: porta usata dalla vittima
       SN appena calcolato
       flag RST impostato

Importante: funziona solo se arriva prima della risposta dell'host!

IP spoofing

IP Spoofing non cieco: chiusura di una connessione esistente

2 Uso del flag FIN

- Il nemico attende dati dalla connessione **host-vittima**
- … calcola SN e AN
- … spedisce un pacchetto con le seguenti impostazioni:

datagramma IP: IP source address : host
IP destination address : vittima
pacchetto TCP: source port: quella usata dall'host
destination port: quella usata dalla vittima
SN e AN calcolati
FIN impostato

La vittima risponderà con un ACK a questo messaggio, e in seguito risponderà a tutti i successivi pacchetti dell'host con messaggi di RST: in tal modo cade la connessione.

IP spoofing

IP Spoofing non cieco: hijacking

Con questa tecnica si prende il controllo della connessione.

L'hijacking si basa sulla desincronizzazione: due host che si scambiano dati non hanno SN e AN correlati tra loro.

Il nemico non fa altro che intromettersi nella connessione tra l'host e la vittima, inviando loro dati costruiti ad hoc.

IP spoofing

IP Spoofing non cieco: hijacking

L'hijacking consiste nell'intromissione nel three way handshake:

1 Il nemico attende un SYN/ACK della connessione **host-vittima**

2 … spedisce RST(spoofato) e SYN(spoofato) verso la **vittima**

3 La vittima chiude la connessione con l'host, e apre una nuova connessione inviando un pacchetto SYN/ACK

4 Il nemico intercetta la risposta e risponde con un ACK prima dell'host.

IP spoofing

IP Spoofing cieco

In questo caso il nemico cerca di farsi passare per un host qualsiasi: il nemico quindi non è in grado di osservare le risposte del server.

Il problema è predire il SN per l'instaurazione della connessione.

Nota storica: questo tipo di attacco fu usato per la prima volta nel 1994 da Kevin Mitnick.

IP spoofing

IP Spoofing cieco: predizione del SN

- **Regola dei 64k**: si calcola la differenza tra due pacchetti e poi si vede se tale differenza è divisibile per 64000.

Per predire il SN, il nemico spedisce un SYN alla vittima, osserva la risposta e predice il SN

- **Regola in base al tempo**: si effettuano una serie di campionamenti ed analisi per calcolare le differenze di tempo.

Il SN viene calcolato in base ai campionamenti fatti

- **Generazione random**: per il nemico è arduo predire il SN.

IP spoofing

IP Spoofing cieco: attacco

Il nemico spedisce un SYN autentico alla vittima
- riceve SYN/ACK di risposta
- … calcola il SN
- spedisce un SYN falso alla vittima
- invia un ACK spoofato con SN+1 (SN è quello calcolato)

Il risultato è l'instaurazione della connessione con la vittima, anche se il nemico non può intercettare le risposte di quest'ultima.

IP spoofing

DOS

Gli attacchi DOS hanno l'obiettivo di escludere un host dalla rete, rendendolo irraggiungibile, oppure limitandone la fruibilità dei servizi offerti.

IP spoofing

DOS

È possibile suddividere gli attacchi DOS in quattro categorie:

1. **Esaurimento banda**: l'obiettivo è saturare la banda della vittima:
   - se il nemico ha la connessione più veloce della vittima questo è banale
   - se il nemico ha una connessione lenta, usa un Distribuited DOS
2. **Esaurimento risorse**: vengono consumate le risorse della vittima (cicli di CPU, memoria, spazio su disco)
3. **Difetti di programmazione**: sono attacchi mirati a bug o difetti di un particolare programma usato dalla vittima.
4. **Generici**: focalizzano l'azione contro singoli servizi.

IP spoofing

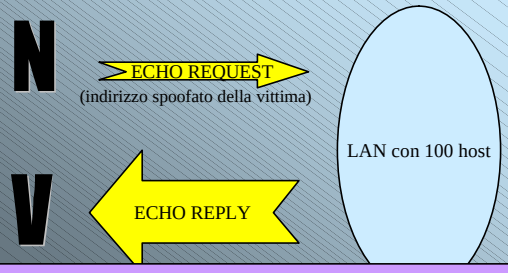
DOS : SMURF

L'obiettivo di questo tipo di attacco è l'esaurimento della banda a disposizione della vittima (rientra nella categoria 1).

Viene sfruttato il meccanismo di risposta multipla fornito dal broadcast address di una LAN.

IP spoofing

DOS: SMURF



La vittima riceverà 100 ECHO reply: l'attaccante ha generato un traffico di 500k/s provocando una risposta di 4Mbit al secondo,saturando la banda della vittima!

IP spoofing

DOS: SYN flood

Cos'è?

Questo attacco sfrutta le risposte SYN/ACK ad una richiesta di connessione (rientra nella categoria 2).

Quando si richiede una connessione, inviando un SYN, il server risponde con SYN/ACK, allocando per questa probabile connessione delle risorse.

IP spoofing

DOS: SYN flood

Il nemico invia centinaia di richieste di connessioni parziali (SYN) e non risponde (ACK) alle richieste di completamento di connessione inviate dal Server (SYN/ACK) .

Il server allocherà delle risorse per tutte le richieste ricevute; poiché il nemico non risponde, il server dovrà attendere che le richieste di connessione parziali vadano in TIME OUT, liberando successivamente le risorse..

Il nemico, una volta esaurite le richieste del server, continuerà ad inviare poche decine di richieste SYN, così da continuare a tenere sature le risorse del server, impedendo a quest'ultimo di funzionare correttamente.

Bibliografia e fonti

Siti internet:

- http://www.cert.org
- http://www.nmrc.org
- http://www.fuzztech.com

- http://www.securezone.it
- http://www.insecure.org
- http://www.s0ftpj.org

- http://golug.cc.uniud.it
- http://www.di.unipi.it/~carboni
- http://www.dei.unipd.it/~keatch
- http://www.cs.princeton.edu/sip/

- http://www.iwar.org.uk
- http://www.insecure.org
- http://www.phrack.org
- http://www.zeroack.it
- http://neworder.box.sk
- http://black.box.sk

Bibliografia e fonti

Documenti e libri specializzati:

- Linux Massima Sicurezza Anonimo
- IPCHAINS howto
- TCP/IP Illustrated vol.1 R.Stevens

Software usato

ARPwatch: http://ftp.sunet.se/pub/security/tools/audit/arpwatch