Prof. Stefano Bistarelli

A cura di:Stefano Macellari

Spoofing

INTRODUZIONE

- Cosa è lo spoofing

- Tipi di spoofing
  Parleremo di:
  - WEB spoofing
  - MAIL spoofing
  - SMS spoofing
  - ARP spoofing
  - DNS spoofing
  - IP spoofing

CHE COSA E' LO SPOOFING?

Dal Dizionario Informatico:
Spoof (ingl.) truffa
Atto di introdursi in un sistema
Informativo senza averne le
Autorizzazioni.L'intruso cambia
Il proprio IP non valido, in
Uno idoneo per l'accesso
Al sistema...

Parliamo del:

WEB spoofing

MAIL spoofing

SMS spoofing

ARP spoofing

DNS spoofing

IP spoofing

Cos'è?

Il Web Spoofing consiste nel far credere ad un utente di visitare il sito web desiderato, con la pagina richiesta, mentre nella realtà ne sta visitando un altro inconsapevolmente...

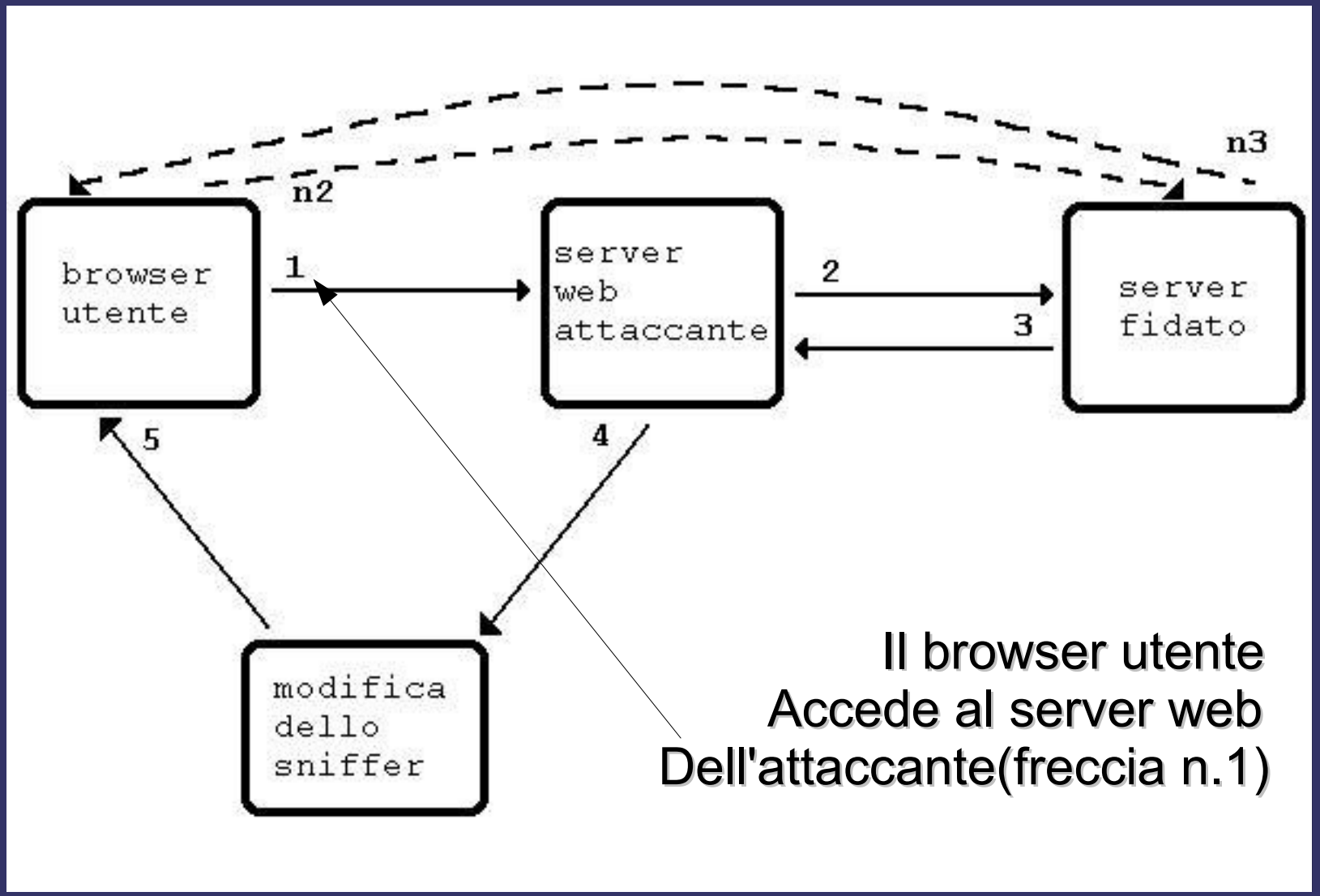
Questa tecnica fa un uso notevole di Javascript

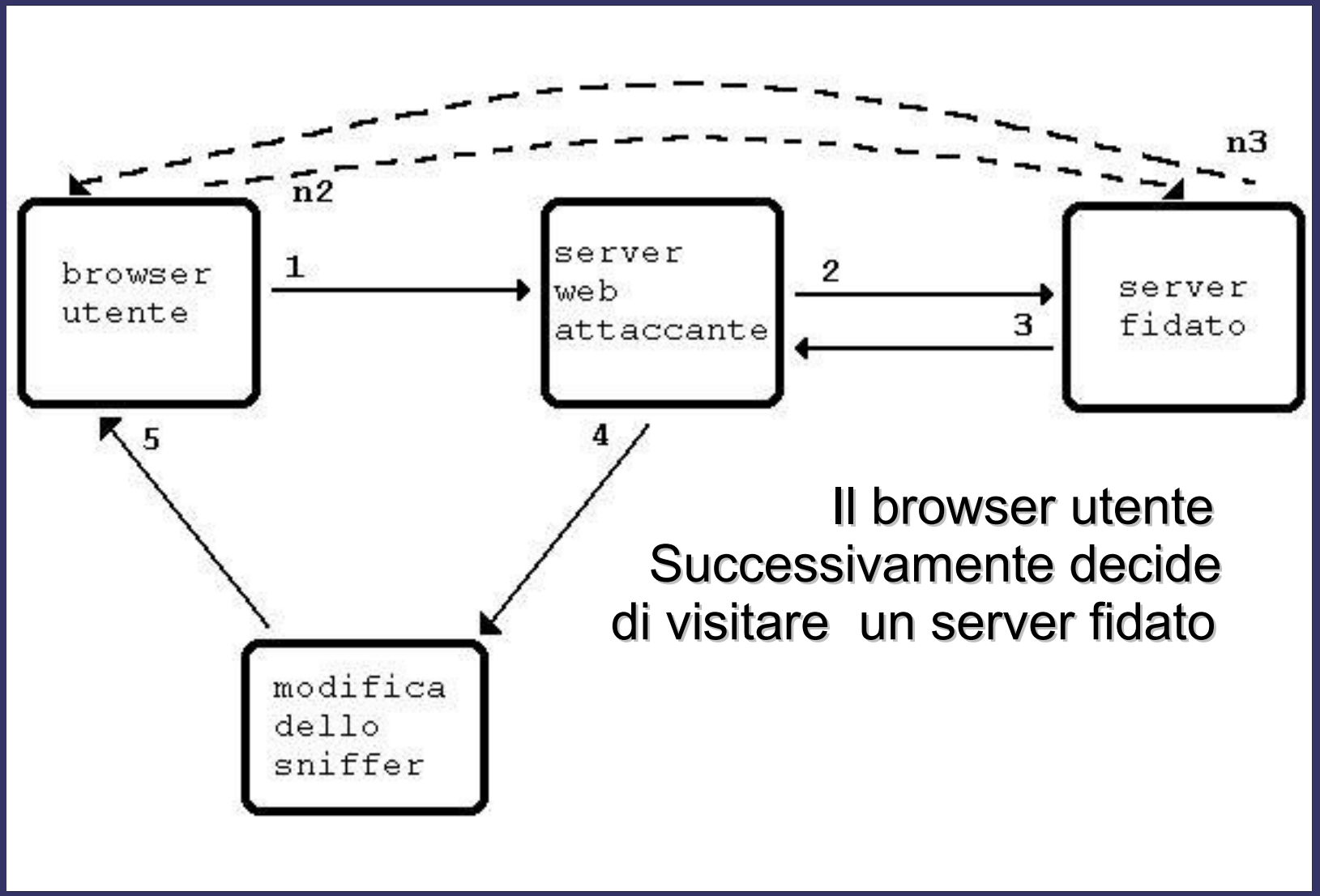
- Supponiamo di visitare il sito *www.pippo.net*
  la pagina principale di tale sito si frappone tra il client e le pagine successive richieste, generando un PROXY server non voluto....

- In questo modo al malcapitato si potrà vedere tutto!!! : siti, form e password...

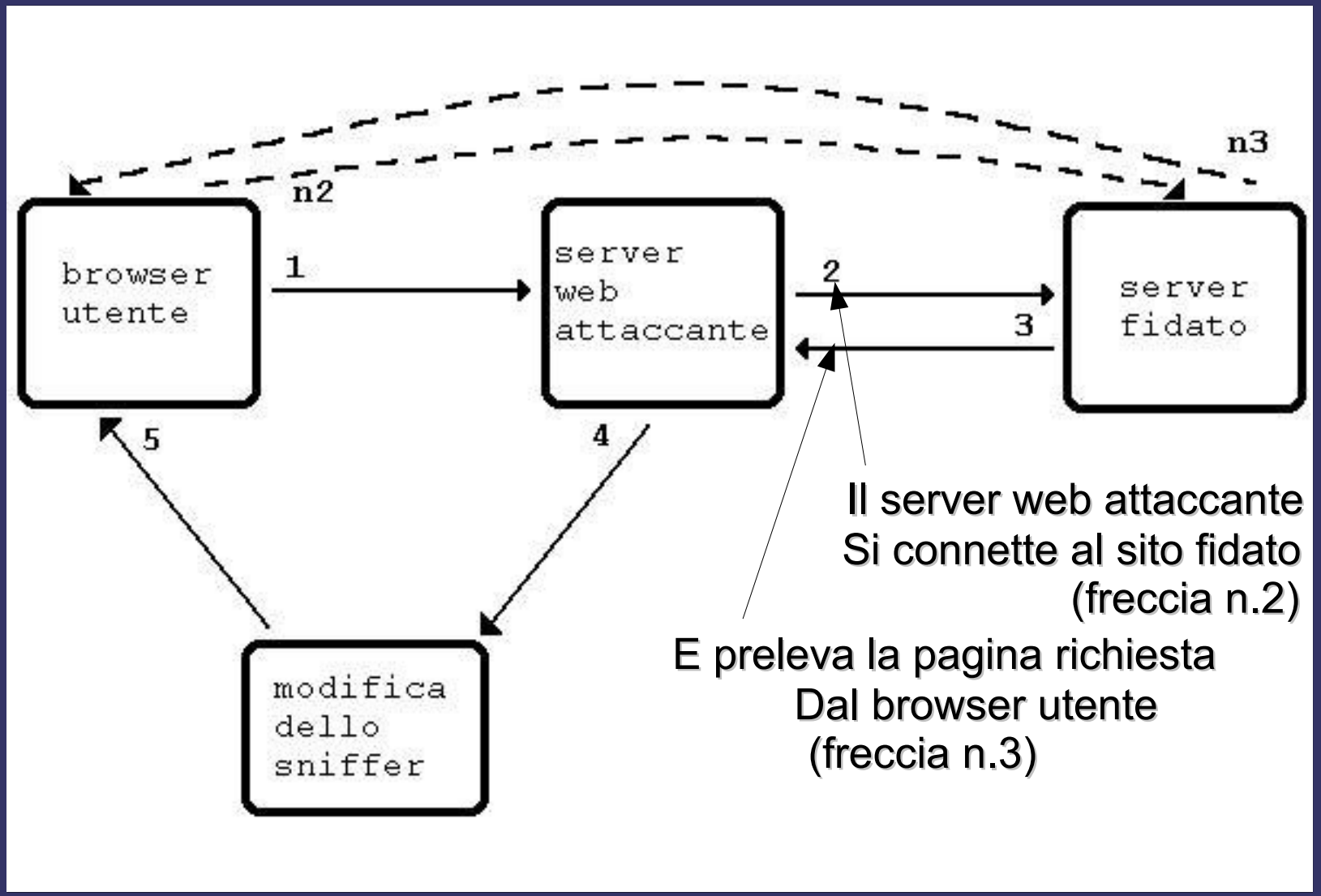
ATTACCO:


WWW
World Wide Web


n3
n2
browser utente
1
server web attaccante
2
3
server fidato
5
4
modifica dello sniffer
Il browser utente
Accede al server web
Dell'attaccante(freccia n.1)

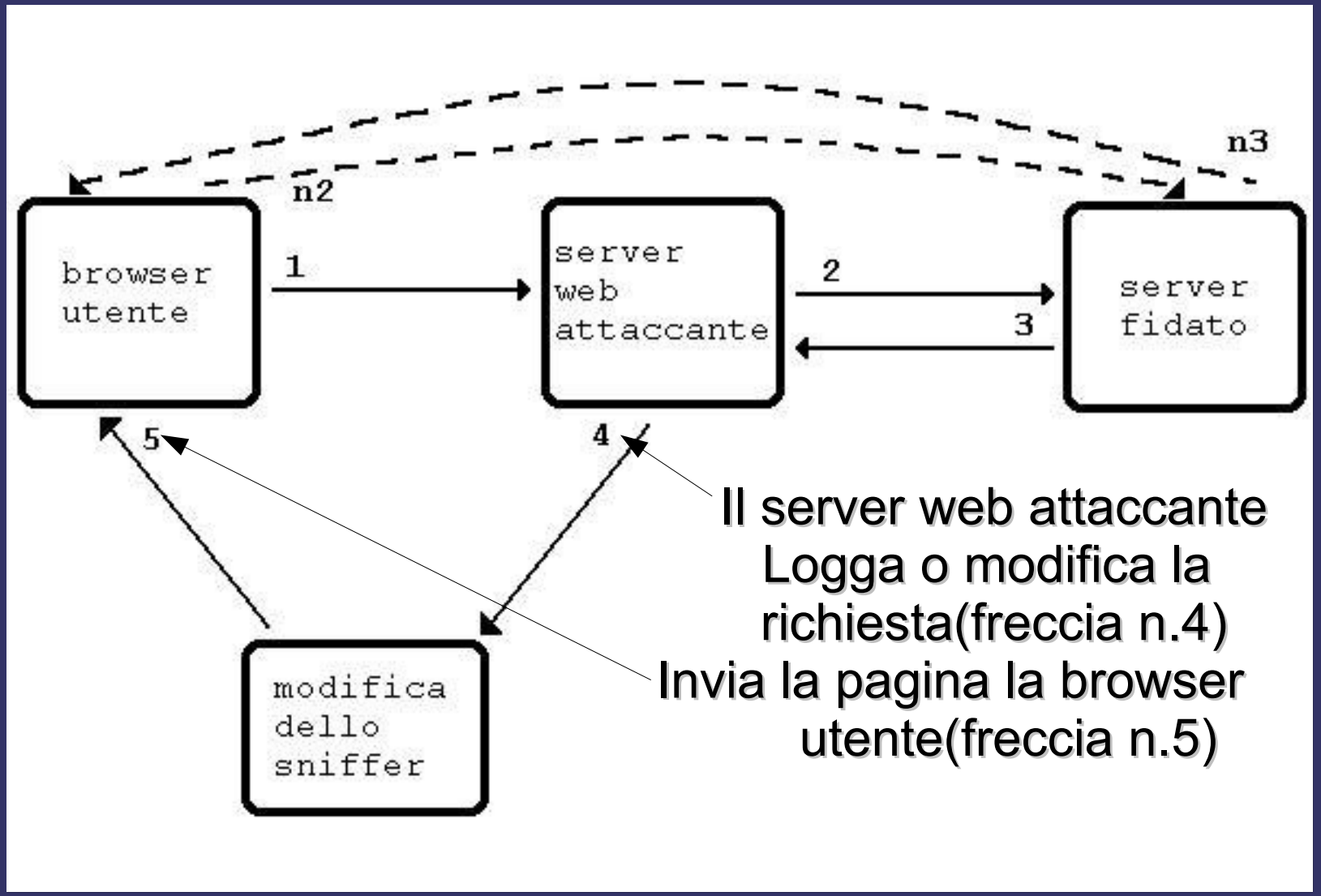


Il browser utente
Successivamente decide
di visitare un server fidato



Il server web attaccante
Si connette al sito fidato
(freccia n.2)

E preleva la pagina richiesta
Dal browser utente
(freccia n.3)



Il server web attaccante Logga o modifica la richiesta(freccia n.4)

Invia la pagina la browser utente(freccia n.5)

Con javascript il “nemico”reindirizza la connessione:

- Modifica lo status bar del browser:
  noi crediamo di avere le informazioni giuste
- Disabilita alcune funzioni dei menù del browser:
  ci impedisce la visualizzazione del codice

La Soluzione ?

- Disabilitare javascript dal nostro browser.....una soluzione drastica ma efficace.

  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 cadere in web spoofing

Passiamo ora:

WEB spoofing

MAIL spoofing

SMS spoofing

ARP spoofing

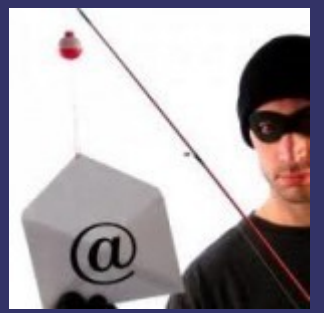
DNS spoofing

IP spoofing

SPOOFING

- Con tale tipo di attacco si fa apparire un allegato di una mail come se fosse di un tipo diverso da quello che è realmente

- Il mail spoofing si basa su una vulnerabilità dei MIME TYPE, usati per inviare mail.



È una tecnica semplice, i cui effetti possono essere disastrosi:
basta modificare opportunamente il nome degli allegati....

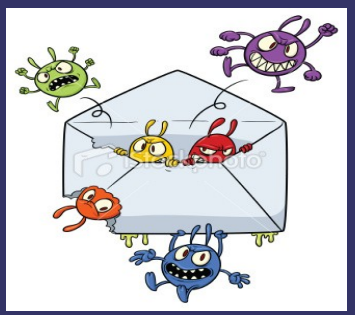
es.

cambiamo il nome di pippo.exe con pippo.jpg----------.exe

ci sono 255 spazi vuoti

Quando l'email arriva al destinatario tale leggerà il nome dell'allegato come pippo.jpg e cliccandoci sopra con l'intento di vedere l'immagine, in realtà aprirà un programma ad HOC che porterà o alla perdita di dati o all'apertura di una back door sulla macchina del client.

Pippo.exe eseguirà ad es. un FORMAT C:



La Soluzione ?

L'unica difesa da questo tipo di attacco consiste nel non aprire mail e-mail di persone che non si conoscono.

Passiamo ora:

WEB spoofing

MAIL spoofing

SMS spoofing

ARP spoofing

DNS spoofing

IP spoofing

Sms spoofing consiste nell'invio di un sms il cui mittente è falso, inesistente

Gli operatori di telefonia mobile offrono il sevizio di SMS tramite appositi Gateway raggiungibili via modem

E' possibile collegarsi via telefono all'SMS-Gateway ed ottenere il servizio di invio SMS con un apposito protocollo

Due sono i protocolli usati:

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

analizziamo UCP perchè è quello che è usato per effettuare lo spoofing.

Pacchetto UCP

<STX>

inizio messaggio

/HEADER/

TNR->intero transazione casuale
LNG->numero di caratteri del messaggio
O->richiesta servizio/R->risposta alla richiesta
OPN->codice del servizio

/DATA/

varia a seconda del servizio:invio singolo o multiplo
ADC->nome destinatario
OADC->numero del sorgente del messaggio
OAC->codice di autentificazione mittente
MT->tipo di sms
AMSG->il messaggio

/CRC<ETX> /

fine messaggio

***AMSG** è il messagio da inviare*

i caratteri che compongo il messaggio non sono trasmessi in chiaro ma vengono codificati in stringhe

IA5

↓

Trasformazione del carattere nel corrispettivo ASCII

Per mandare un messaggio al numero 338-8711150 dal numero 42 il messaggio "linux rules" ecco cosa deve comnunicare al gateway:

<STX>04/00046/O/01//00393388711150/42//3/4C696E75782052756C6573/F6<ETX>

se la query è stata accettata il gateway risponde:

<STX>01/00035/R/01/A/00393388711150:090800114008/A0<ETX>

poi occorre attendere lo smistamento del gateway.

Come si comunica con il server sms?

In rete ci sono molti programmi il più semplice è sms_client

La Soluzione ?

Fortunatamente i gateway che smistano e instradano i messaggi sono ormai immuni a questo tipo di attacco.

Passiamo ora:

WEB spoofing

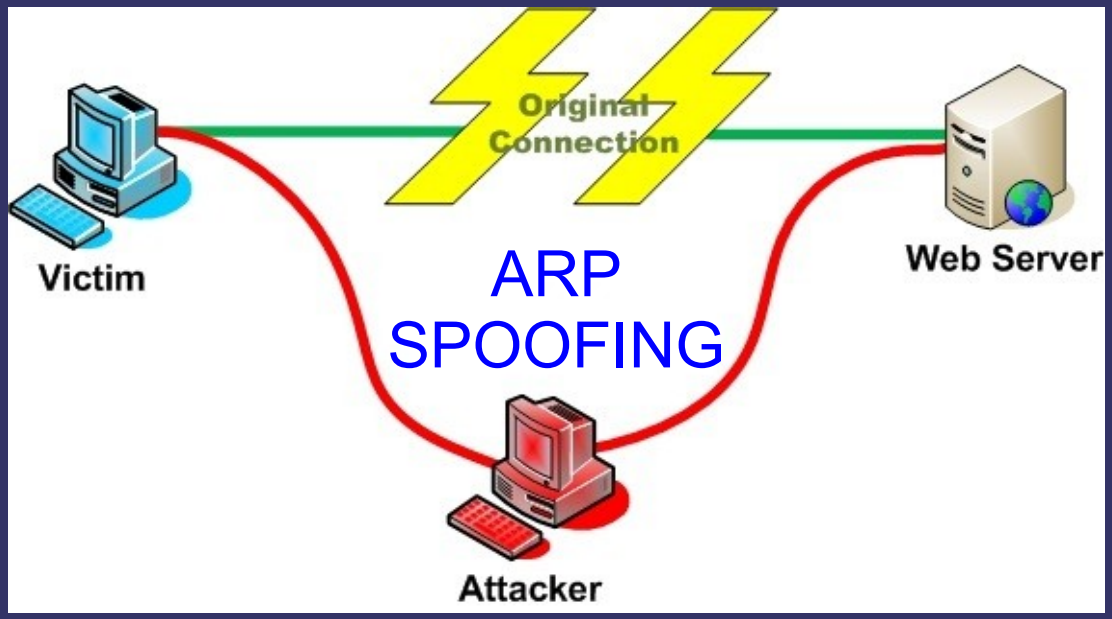
MAIL spoofing

SMS spoofing

ARP spoofing

DNS spoofing

IP spoofing



Una LAN può essere attaccata dall'interno solo se ci sono utenze maliziose...

E' un attacco applicabile su LAN Ethernet

↓

Viene sfruttata la configurazione promiscua delle schede Ethernet

↓

E' in grado di vedere tutto il traffico IP

Come funziona?

ARP ***(Address Resolution Protocol)***

è quel protocollo che provvede a far conoscere e diffondere il MAC address in una rete LAN

Dov'è D?

Chi è D?

Aggiornamento
Della ARP table

Il mio MACaddress

Sono qui

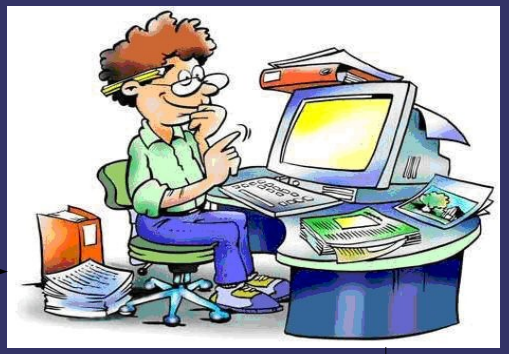
ARP SPOOFINGa

ATTACCO:

Il “cattivo”

Sono BOB

Andrea



ARP
Reply falso

Andrea invia i suoi dati a BOB

ARP SPOOFINGa

LAN con HUB

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.

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:

1- Ping modificato
2- TCP SYN modificato
3- Analisi del traffico verso il DNS

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

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.

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.

LAN con HUB

Prevenzione:

- Protocolli per cifrare il traffico che viaggia sulla LAN
- Installare uno SWITCH che instrada il traffico sulla LAN.

Ma lo SWITCH ci protegge?

ARP SPOOFINGa

LAN con SWITCH

Uno SWITCH su una LAN smista i pacchetti informativi...

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 SPOOFINGa

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 SPOOFINGa

Sono B

Sono A

ARP reply falso

ARP reply falso

Che bello!!!

Dati

Dati

E' per B

E' per A

LAN con SWITCH

Soluzione:

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

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.

Passiamo ora:

WEB spoofing

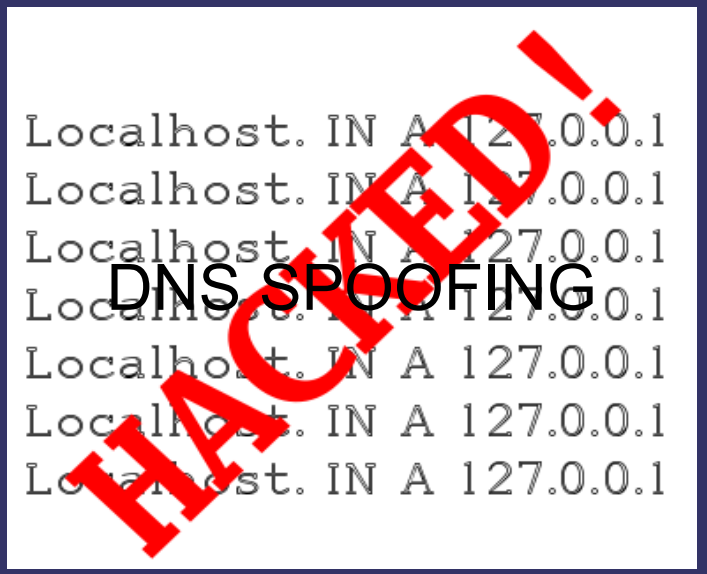
MAIL spoofing

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

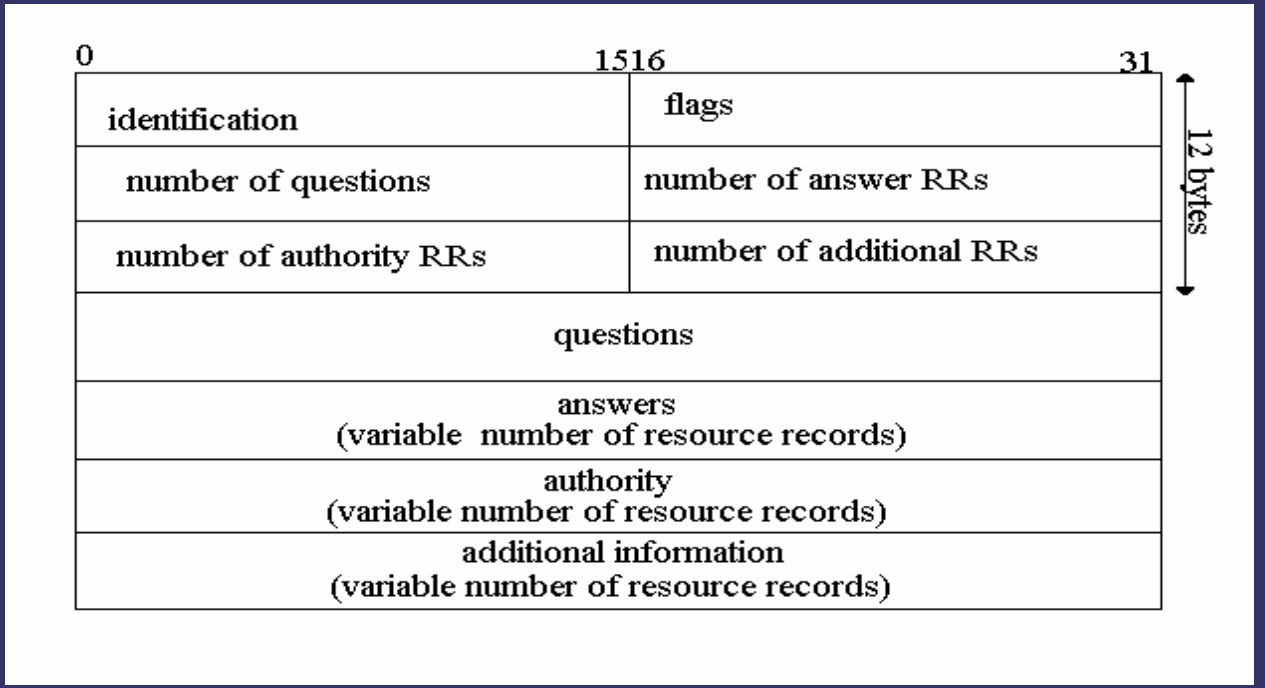
DNS : una breve introduzione

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.

Header DNS-->



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 ha 3 forme

- Chache poisoning
- Simulazione delle Risposte DNS
- Manomissione fisica DNS

DNS SPOOFING

Il campo interessato allo Spoofing è il campo QUESTIONS:

ogni domanda ha un type, ed ogni risposta ha un type.
A type è la corrispondenza [IP address – canonical name]

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…
- 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

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

Cache poisoning

Supponiamo:

→ *dns.my.org* accetta query ricorsive
→ *pippo.net* sia sotto il controllo del nemico
→ *dns.my.org* sia un name server con molti clients
→ *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 in 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.

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:

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

Cache poisoning

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 autritativo 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

Cache poisoning

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.

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*

Passiamo ora:

WEB spoofing
MAIL spoofing
SMS spoofing
ARP spoofing
DNS 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.

In ogni pacchetto TCP/IP 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

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

Generazione del SN

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)

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.

Generazione random

Il SN viene generato truly random (esempio di implementazione ed uso nei nuovi kernel di Linux)

Tipi di Attacchi

Gli attacchi IP spoofing possono suddividersi in tre categorie:

IP spoofing non cieco: attuabile in una LAN; il nemico cerca di farsi passare per un host che è nella sua stessa sottorete

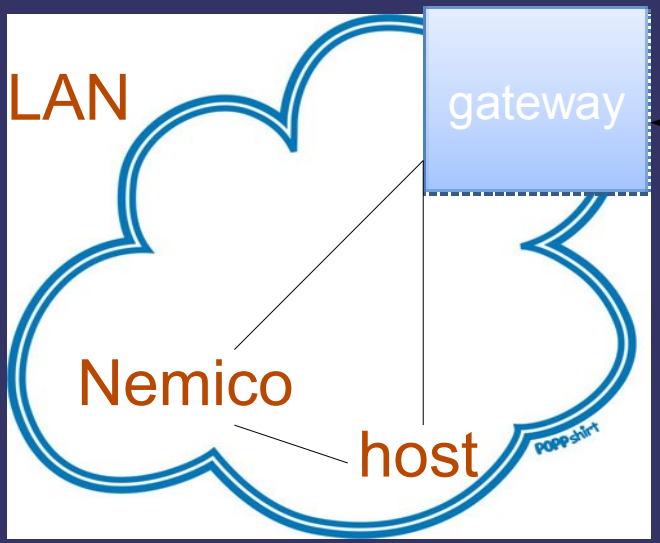
IP spoofing cieco: il nemico cerca di farsi passare per un host di una qualsiasi sottorete

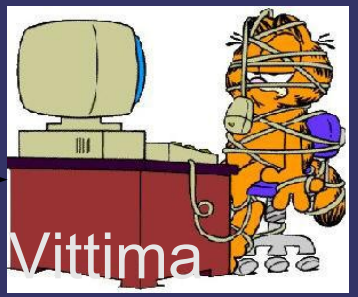
Denial of Service(DOS): il nemico cerca di bloccare un host per impedire a quest'ultimo di svolgere la normale attività o per prenderne il controllo (con spoof oppure hijacking)

IP Spoofing non cieco

Cos'è?

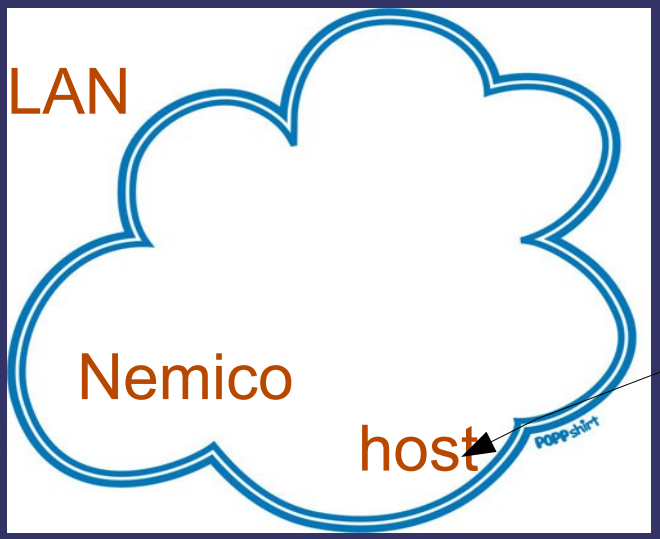
In una LAN, il nemico cerca di farsi passare per un host che è nella sottorete.





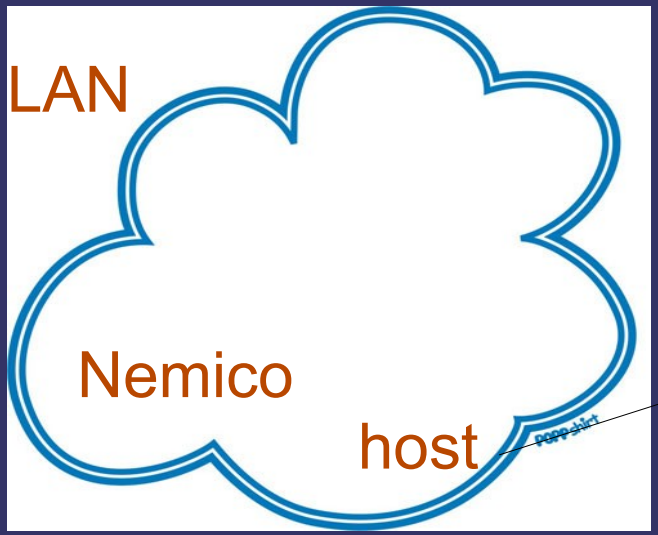
Se il nemico ha la scheda di rete in modalità promiscua, allora è il grado di analizzare tutto il traffico della vittima

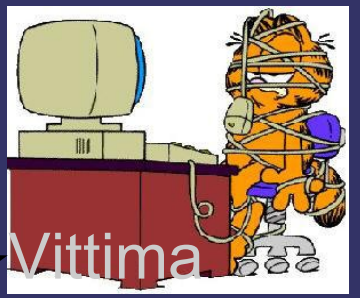
IP SPOOFING: A Hacking Technique



Supponiamo che l'host sia connesso con la vittima…

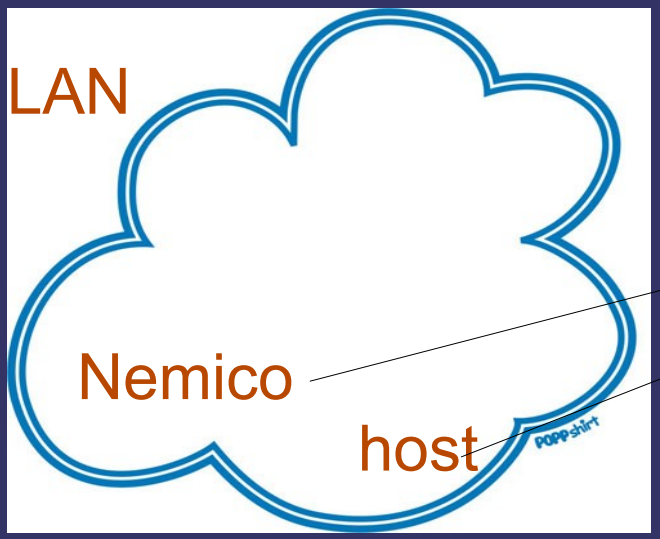
IP SPOOFING: A Hacking Technique

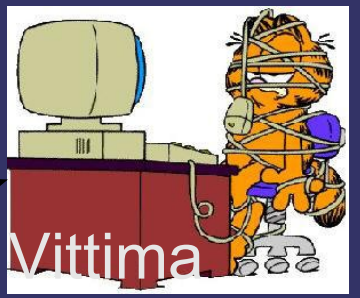




Come prima cosa il nemico fa chiudere la connessione dalla vittima verso l'host

IP SPOOFING: A Hacking Technique





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

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

IP Spoofing non cieco: chiusura di una connessione esistente

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

Uso del flag RST

Uso del flag FIN

1->Il nemico attende dati dalla connessione host-vittima
2->… calcola il SN in base ai dati raccolti…
3->… 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

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

1->Il nemico attende dati dalla connessione host-vittima
2->… calcola SN e AN
3->… 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

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 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.

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

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

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.

SN viene calcolato in base ai campionamenti fatti

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

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.

DOS

Cos'è?

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

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.

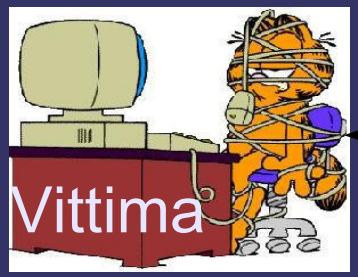
IP SPOOFING: A Hacking Technique

DOS : SMURF

L'obiettivo di questo tipo di attacco è l'esaurimento della banda a disposizione della vittima. Viene sfruttato il meccanismo di risposta multipla fornito dal broadcast address di una LAN.

nemico

ECHO REQUEST
(indirizzo spoofato della vittima)



ECHO REPLY

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!

DOS: SYN flood

Cos'è?

Questo attacco sfrutta le risposte SYN/ACK ad una richiesta di connessione.
Quando si richiede una connessione, inviando un SYN, il server risponde con SYN/ACK, allocando per questa probabile connessione delle risorse.

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.


FINE