UNIVERSITA' DEGLI STUDI DI PERUGIA
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Magistrale in Informatica

Seminario Sicurezza Informatica

VoIP Attack

Studenti
Alfredo Parisi
Saverio Di Zeo

Docente
Prof. Stefano Bistarelli

Anno Accademico 2010 – 2011

Indice

Introduzione

Grazie alla diffusione dell'ADSL avvenuta negli ultimi anni, sono stati sviluppati algoritmi più efficienti di compressione dell'audio e del video, protocolli per velocizzare le trasmissioni di contenuti multimediali con tempi di risposta più brevi.

Questa evoluzione ci consente, proprio attraverso tecnologie nate per il trasporto di dati, una comunicazione multimediale in tempo reale.

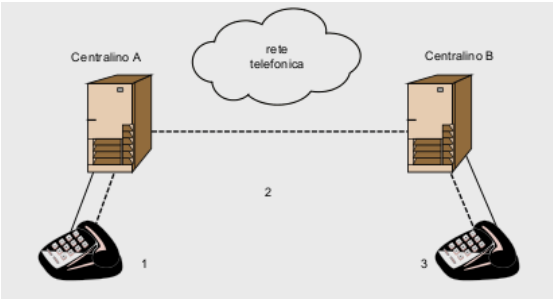
In questo contesto nasce VoIP (*Voice Over IP*), una tecnologia che consente la comunicazione telefonica attraverso internet; usando la propria connessione, un PC dotato di casse e microfono oppure un particolare telefono, si possono effettuare vere e proprie telefonate in tutto il mondo, in maniera gratis o con una spesa irrisoria.

Nato nel 1995 per consentire le chiamate da PC a PC, il VoIP si è rapidamente evoluto suscitando il forte interesse presso privati, aziende ed operatori, grazie all'introduzione di un notevole risparmio, sopratutto nelle chiamate a lunga distanza.

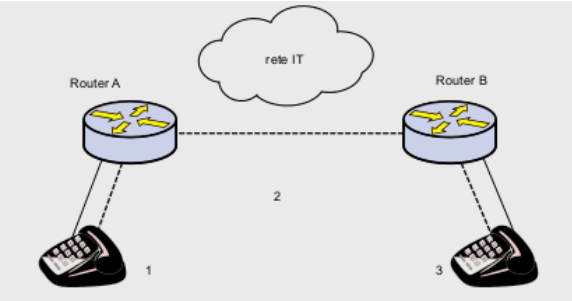
La tecnologia VoIP permette di trasformare un segnale audio (la voce) in formato digitale e di trasmetterlo sotto forma di "pacchetti dati" attraverso Internet (*VoIP = Voce su Protocollo Internet*).

Per gli utenti la convenienza è legata alla possibilità di abbattere drasticamente i costi delle bollette telefoniche o di azzerarle del tutto, effettuando chiamate da computer a computer oppure da telefono verso utenti con lo stesso abbonamento VoIP.

E' naturale chiedersi perché la tecnologia VoIP, basata sulla commutazione di pacchetto, consenta di ottenere simili risparmi rispetto alla tecnologia a commutazione di circuito, ovvero la rete telefonica tradizionale.



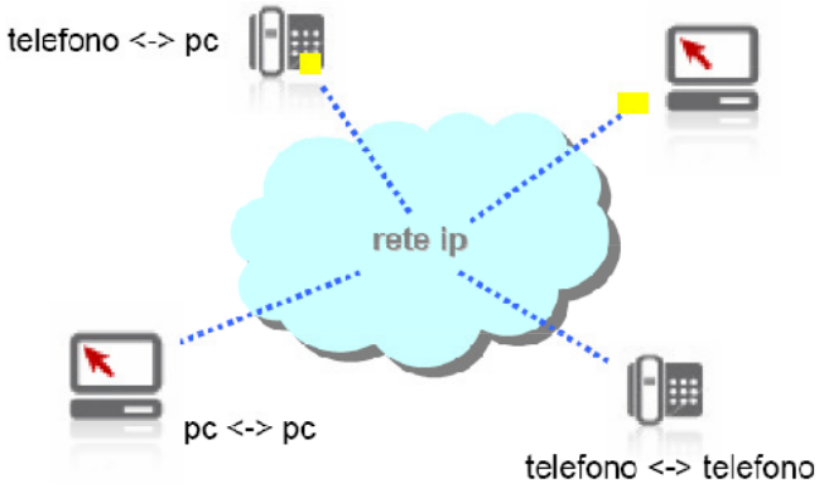
Rete telefonica tradizionale



Rete a pacchetto

Le ragioni sono principalmente le seguenti:

1. *ridotti costi di chiamata*, specialmente per quelle a lunga distanza: la chiamata telefonica fatta con il VoIP è uguale al costo di una chiamata locale per collegarsi al proprio provider Internet;
2. *riduzione dei costi di infrastruttura*: basta un unico tipo di cavo per PC e telefoni;
3. *portabilità del numero a prefisso geografico*: il numero non è legato fisicamente a uno specifico apparecchio; è possibile, anche quando si è in vacanza o si è fuori sede, essere raggiungibili sullo stesso numero di telefono di casa;
4. *implementazioni future* non richiedono nessun cambiamento dell'hardware.



Oggi moltissimi software, scaricabili in maniera gratuita da Internet, consentono a qualunque persona dotata di un PC collegato ad Internet di chiamare e videochiamare gratuitamente un'altra persona in tutto il mondo.

Tra i software più diffusi si possono ricordare *Skype*, *Google Talk* e *Msn Messenger*.

In particolare molti programmi, nati in origine solo per consentire la chat testuale, software di Instant Messaging come ad esempio Msn Messenger, sono stati successivamente arricchiti per consentire di effettuare chiamate vocali e videochiamate.

Alcuni di questi programmi, ad esempio Skype, consentono oggi di effettuare chiamate dal proprio PC verso i numeri telefonici tradizionali di rete fissa e mobile, pagando soltanto il costo di interconnessione con l'operatore telefonico e consentendo enormi risparmi.

Architettura di un sistema VoIP

L'architettura VoIP è costituita da:

I. centralino IP (IP PBX);

II. rete LAN;

III. terminali IP (PC, telefono VoIP e telefono tradizionale con adattatore ATA);

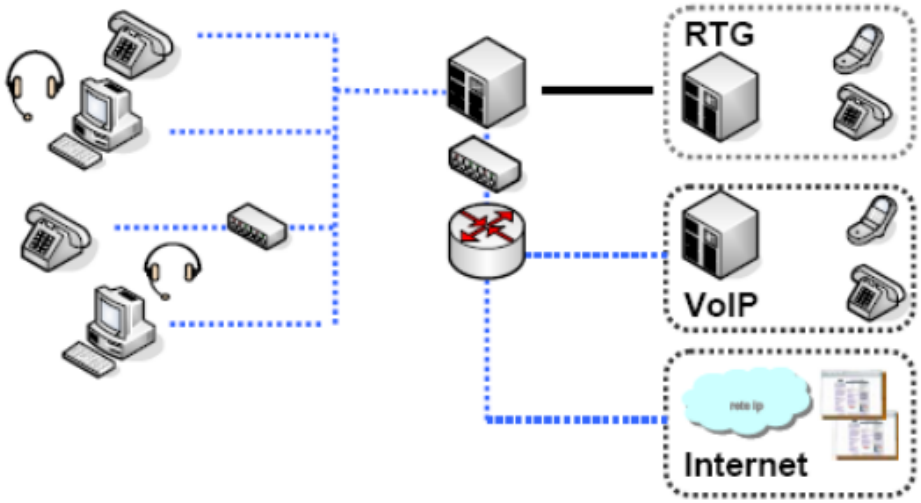
IV. gateway VoIP.

Un *centralino PBX* (*Private Branch eXchange*) è una centrale telefonica che gestisce l'instaurazione e il mantenimento della connessione fra gli apparati dei due utenti. E' in grado di gestire linee analogiche, linee digitali (ISDN) e VoIP contemporaneamente.

La *rete LAN* è l'infrastruttura di trasporto e può essere una semplice LAN switched, un collegamento WAN o una rete IP complessa.

I *terminali IP* sono i dispositivi utilizzati dagli utenti per comunicare e possono essere telefoni fisici o software eseguiti da PC. E' possibile trasformare un normale telefono tradizionale in telefono VoIP, tramite l'uso di un adattatore ATA.

Il *gateway VoIP* è un apparato di rete che permette di interfacciare la rete tradizionale con quella VoIP.



Costruzione di una chiamata VoIP

Come detto in precedenza, il VoIP si basa su protocolli che fanno riferimento all'Internet Protocol e quindi ne eredita i rischi.

E' impossibile parlare in modo univoco di VoIP in quanto esistono differenti soluzioni; alcuni sono di tipo *proprietario*, come Skype, e altri basati sul protocollo *SIP* (*Session Initiation Protocol*).

Prima di analizzare la parte inerente gli attacchi, è necessario definire le caratteristiche di una conversazione fra due apparecchi, in modo da capire dove si annidano i rischi di un eventuale attacco.

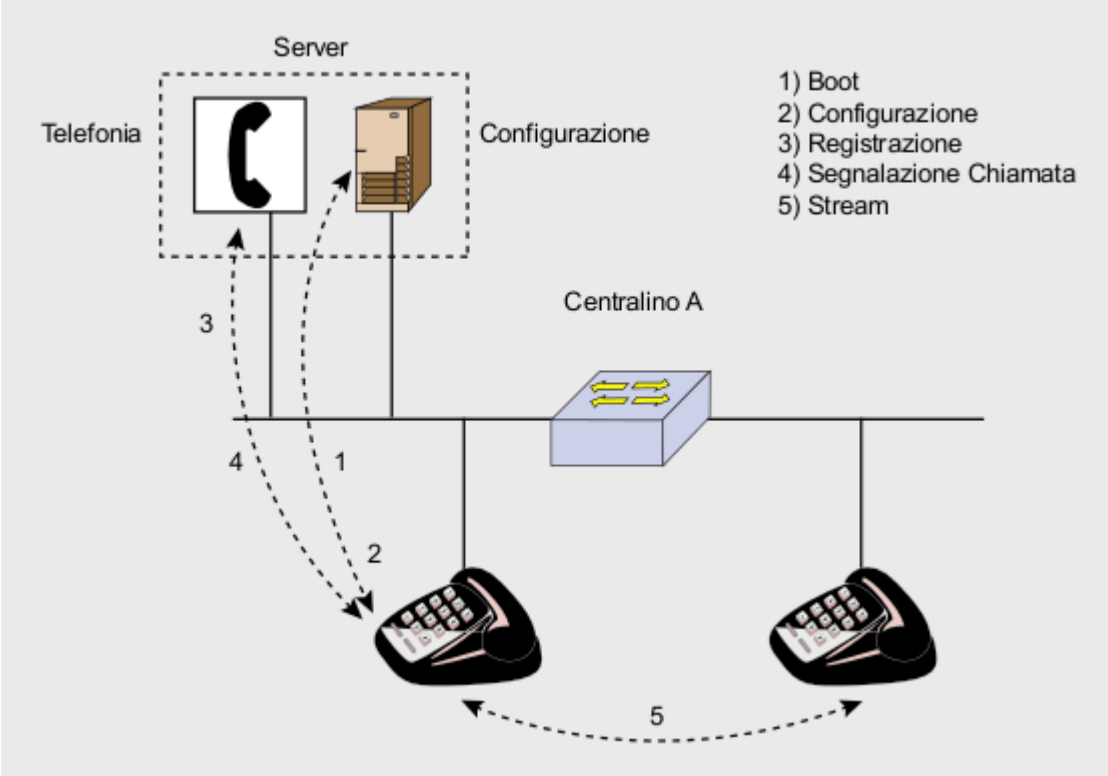
Nel momento in cui un telefono viene acceso si è nella fase di *booting* e si invia un *broadcast* sulla rete che serve ad individuare il server DHCP (*Dynamic Host Configuration Protocol*), ovvero il server che fornisce in modo automatico l'indirizzo IP a tutti i device di quella rete.

Alla fine del processo DHCP, il telefono avrà un indirizzo IP, subnet mask, default gateway e l'IP del server a cui richiede la configurazione. Successivamente il telefono si rivolge al server di configurazione (configuration server) utilizzando il protocollo TFTP (*Trivial File Transfer Protocol*) per richiedere la propria configurazione. La comunicazione con il TFTP avviene esclusivamente in UDP (*User Datagram Protocol*), quindi senza alcun meccanismo di affidabilità.

Dopo l'invio del file di configurazione, telefono e server si scambieranno tutte le informazioni necessarie alla gestione delle chiamate (ID chiamante, ID chiamato, eventuali deviazioni, trasferimenti, fine conversazione): questo flusso prende il nome di

signaling.

Terminata la fase di signaling, si instaura la conversazione vera e propria fra i due telefoni che si scambiano dati, più precisamente la voce campionata viene scambiata con il protocollo RTP (Real-time Transport Protocol). Questa comunicazione avviene su porte UDP dinamicamente stabilite.



Tipologie di attacchi

La voce su IP eredita i rischi di una rete IP in quanto tutti i servizi VoIP la utilizzano come trasporto. Una buona protezione sulla rete garantirà un buon livello di protezione anche sui livelli voce.

La tipologia degli attacchi può essere raggruppata in tre categorie:

1) attacchi mirati alla *confidenzialità* dei dati;
2) attacchi mirati all'*integrità* dei dati;
3) attacchi mirati alla *disponibilità* dei servizi.

Attacchi sugli accessi fisici

La prima tipologia di attacchi riguarda l'accesso fisico ai terminali (telefoni); bisogna consentire l'utilizzo degli apparecchi solo al personale autorizzato, in modo da evitare attacchi di tipo *spoofing* come ad esempio: leggere il nome del possessore del telefono, vedere le chiamate perse, ascoltare la casella vocale ed evitare che siano effettuate chiamate non autorizzate o illegali.

Per evitare che l'attaccante riesca ad utilizzare il telefono e le sue applicazioni senza le dovute autorizzazioni, si possono usare delle regole di autenticazione sia del dispositivo che dell'utente, utilizzando una username e password o delle chiavi di cifratura.

Il livello di protezione fisica di un telefono dipende da due fattori: *diritto del telefono e autorizzazione degli utenti,*

Per quanto riguarda il primo, un telefono che si trova in un'area di passaggio, essendo alla portata di tutti, avrà delle regole diverse rispetto ad un altro situato all'interno degli uffici.

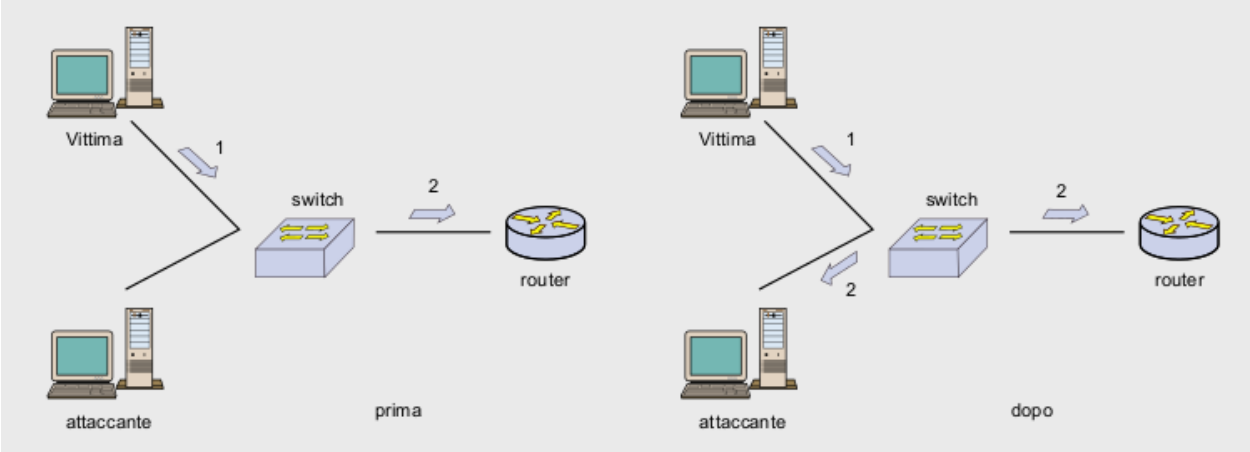
Il secondo, invece, riguarda i privilegi legati agli utenti che forniranno username e password per l'autenticazione solo all'interno degli uffici e non saranno soggetti a farlo in zone comuni.

Attacchi sull'infrastruttura di rete

Uno degli attacchi sull'infrastruttura di rete è rappresentato dal *Media Access Control* (MAC) *flooding* che tenta di "inondare" la memoria interna degli switch con un grande numero di indirizzi MAC falsificati, i quali andranno a saturare la memoria dello switch fino a farlo smettere di funzionare.

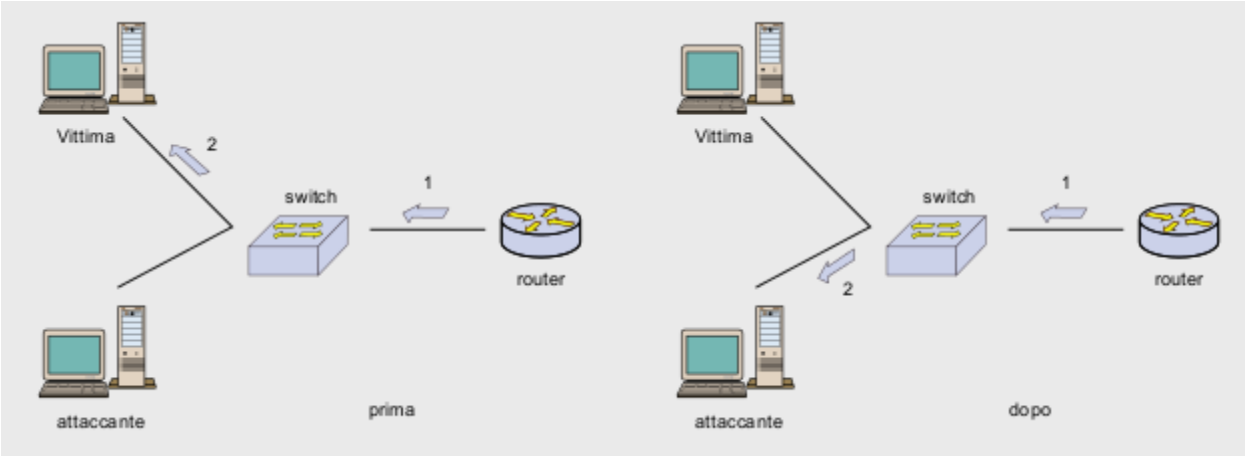
La *Content Addressable Memory* (CAM) table è una risorsa di memoria, di grandezza finita, che contiene tutti i MAC address dei terminali conosciuti.

La vulnerabilità è dovuta al riempimento (*CAM Table Overflow*) dello spazio disponibile in memoria, costringendo lo switch ad entrare in una condizione detta di *fail open* che lo fa comportare come un hub, inviando così gli stessi dati a tutti gli apparati ad esso collegati, compreso quello di un eventuale attaccante che può dunque sniffare tutto il traffico in transito nella rete.



MAC flooding

Un altro possibile attacco è rappresentato dal *Media Access Control* (MAC) *spoofing,* tramite il quale si tenta di falsificare un indirizzo MAC conosciuto o autenticato, per tentare di ottenere maggiori privilegi di accesso alla rete.



MAC spoofing

Causare una condizione di *fail open* in uno switch è il primo passo da parte di un attaccante per raggiungere altri fini, tipicamente effettuare *sniffing* o un *man in the middle* (l'attaccante è in grado di leggere, inserire e modificare messaggi tra due parti, senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce sia stato effettivamente compromesso da una terza parte).
Una contromisura a questo tipo di attacco può essere apportato configurando la *port security,* in modo che ogni porta accetti un numero finito di MAC address.

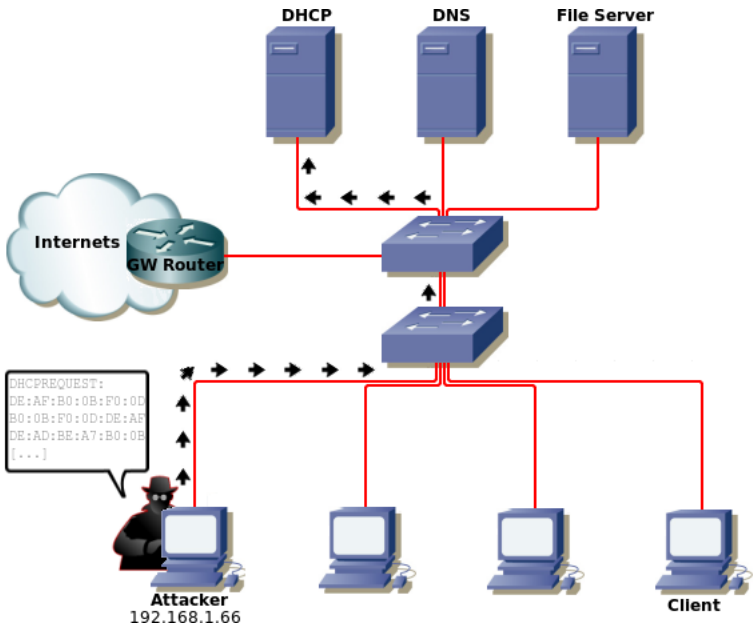
Di seguito alcuni tools per lo sniffing di pacchetti VoIP:

- Cain & Abel: tool multiuso che ha la possibilità di ricostruire gli RTP (pacchetti voce);
- AuthTool: determina la password dell'utente analizzando il traffico;
- Oreka: registra e recupera il dispositivo audio e gli stream voce VoIP;

- VoiPong: utility che rileva le chiamate VoIP sul percorso, scarica le conversazioni e separa i file .wav;
- Wireshark: è il più famoso analizzatore di traffico della rete; funziona su Windows, Linux, UNIX e su altre piattaforme.

L'*IP spoofing* è uno degli attacchi più comuni, e consiste nel falsificare l'indirizzo IP di un host (A) in modo da farlo sembrare un altro (B), superando la difesa basata sull'IP sorgente.
Si può evitare l'attacco tramite l'utilizzo di tabelle di routing oppure impedendo che da un'interfaccia (di un router/firewall) vengano inviati pacchetti in cui l'IP sorgente non è quello che ci si aspetta.

L'attacco *DHCP Starvation* può essere generato da richieste DHCP con indirizzo MAC address falso, in modo da acquisire tutti gli indirizzi IP ancora non assegnati agli host. In questo modo l'attaccante potrebbe fingersi DHCP server ed inviare agli host dei parametri contraffatti, come ad esempio IP address, default gateway o DNS.
Una contromisura utile può essere l'utilizzo di sistemi di *Network Intrusion Detection/Protection*, indirizzi IP statici o limitare il numero di MAC address sulle porte dello switch.



Attacchi sui sistemi ed applicazioni

I sistemi operativi e le applicazioni possono essere soggetti ad attacchi da parte di codice pericoloso, comunemente conosciuto come *Malware*.

Esistono vari tipi di Malware tra cui i *Virus*, ovvero delle parti di codice infetto con la caratteristica di replicarsi, *Worm* in grado di modificare il sistema operativo e di replicarsi in rete saturandone le risorse, ed i *Trojan,* parti di codice dannoso che vengono eseguite in modo non visibile all'utente, spesso mascherato all'interno di un software apparentemente innocuo.

Per quanto riguarda le contromisure da adottare per questa tipologia di attacchi, oltre al frequente aggiornamento delle versioni software per impedire che l'attaccante sfrutti eventuali difetti di programmazione, è opportuna la disabilitazione dei servizi non utilizzati, l'impiego di chiavi di accesso ai servizi (username/password, autenticazione forte, chiavi digitali) e degli strumenti di monitoraggio e prevenzione (Intrusion Detection/Protection).

Conclusioni

Le tecnologie VoIP destinate alle aziende sono una flessibile soluzione di telefonia che permette di contenere la spesa del tradizionale traffico telefonico. Adottando le opportune politiche di sicurezza, si potranno ottenere ottimi risultati.
In base all'infrastruttura si dovranno avere determinate attenzioni rivolte alla sicurezza come:

1. esporre in internet il minor numero possibile di servizi in chiaro con autenticazione debole;

2. non esporre in internet telefoni e interfacce di gestione;

3. utilizzare password sicure per la gestione dei terminali;

4. separare il traffico dati da quello VoIP, utilizzando canali cifrati per quest'ultimo;

5. gestire la qualità del servizio QoS;

6. limitare l'accesso alle proprie risorse in internet;

7. utilizzare firewall;

8. utilizzo di Intrusion Prevention System.

Bibliografia

A. Pennasilico, M. Misitano, E. Bortolani. VoIP (in)security: strumenti Open Source per il Security Assessment, 2006, pp. 1-7.

http://it.wikipedia.org/wiki/Voip

http://www.hackerscorner.org/

http://hakin9.org/

http://hakipedia.com/index.php/DHCP_Starvation

http://www.miniotto.name