“Sniffare” informazioni: problemi tecnici o etici?

È noto che le informazioni che viaggiano sulle reti, se non vengono usati accorgimenti particolari, sono “vulnerabili” e possono essere intercettate anche da chi non sarebbe autorizzato a farlo. Forse meno noto, per i non addetti alla sicurezza, è la relativa facilità con cui questo può essere fatto. L’ articolo illustra il funzionamento degli “sniffer”: programmi creati e sviluppati per monitorare le informazioni, ma che possono essere usati per accedere ad esse anche quando non si dovrebbe/potrebbe farlo.

SNIFFARE” CHE COSA?

Esistono molti modi per poter carpire le informazioni sulle attivit di una persona che usi un computer. Alcuni possono sembrare fantascientifici (come captare le onde elettromagnetiche generate dal computer per risalire alle attivit in corso, stando anche ad una distanza di alcune centinaia di metri dal computer che si vuole monitorare), altri necessitano l accesso al computer stesso (come per installare programmi che registrano le attivit della tastiera, detti keyboard sniffers).
In questo articolo ci occuperemo in particolare di come si possano sniffare le informazioni che viaggiano su di una rete, facendo uso di programmi disponibili per chiunque (e nella maggior parte dei casi gratuiti e scaricabili da Internet). L unica limitazione al loro uso che bisogna avere i permessi di amministratore o superuser sulla macchina dove si vogliono installare tali programmi. Ovviamente per poter intercettare una comunicazione necessario essere collegati ad una linea in cui tale comunicazione passi.
Per esempio possibile intercettare qualunque comunicazione che viaggi su una rete Ethernet locale.

UN PO’ DI TERMINOLOGIA

Per prima cosa definiamo alcuni termini che useremo nel corso dell articolo.
Parlando di attacco ci riferiremo ad un tentativo di violare le politiche (o i servizi) di sicurezza di un sistema. Per attacco attivo si intende il tentativo di alterare le risorse o le funzionalit del sistema, mentre per attacco passivo si intende il tentativo di carpire informazioni, ma senza alterare il sistema oggetto dell attacco [1]. In origine sniffer si riferiva ad un programma specifico (The Sniffer Network Analyzer , prodotto dalla Network Associates Inc., http://www.sniffer.com, Figura 1), e come tale protetto da trademark, ma esso oramai entrato nell uso comune e, come accennato in precedenza, con il termine sniffer si soliti identificare una classe di programmi che intercettano informazioni: in questo articolo lo useremo per indicare un programma atto

Figura 1 · il sito www.sniffer.com

a intercettare informazioni che viaggiano su una rete di calcolatori. Normalmente i protocolli per gestire la trasmissione delle informazioni su una rete, dividono tali informazioni in pacchetti. Per questo motivo si soliti indicare i programmi atti ad intercettarle come packet sniffers . Questi programmi sono alla base degli attacchi passivi che, solitamente, sono propedeutici agli attacchi attivi.
Ethernet il modello di rete locale attualmente pi diffuso, e prevede l utilizzo di un unico cavo a cui sono collegate le macchine della rete locale. Le schede di rete, installate su ogni computer collegato con tale architettura, possiedono degli indirizzi che permettono di identificarle in maniera univoca all interno della rete.Quando due computer vogliono scambiarsi dei dati devono provvedere a inserire gli indirizzi corretti nelle intestazioni dei messaggi. Tutti i computer che sono collegati alla rete ricevono il messaggio, ma lo ignorano tutti coloro che non possiedono la scheda di rete con l indirizzo interessato alla comunicazione (le schede di rete possono essere paragonate a filtri che lasciano passare solo l informazione attinente). Per esiste una modalit di funzionamento delle schede di rete, chiamata modalit promiscua , per cui la scheda di rete legge tutto il traffico che passa sul cavo, senza escludere le comunicazioni non indirizzate a lei.

COME LAVORA UNO SNIFFER

Per prima cosa necessario installare il programma, e per farlo necessario avere i permessi di amministratore o superuser sulla macchina.
Una volta installato, il programma provvede a mettere la scheda di rete in modo promiscuo. In questo modo potr ricevere tutto il traffico che viaggia sulla rete a cui la macchina connessa.
Tipicamente ogni sniffer possiede la possibilit di creare dei filtri, in modo da monitorare solo certe attivit .
L informazione considerata interessante viene memorizzata in un buffer locale. Avere a disposizione solo i dati grezzi non di molto aiuto, a meno di non conoscere bene i vari protocolli

Figura 2 · Ettercap in azione (http://ettercap.sourceforge.net/).

usati:spesso tale informazione viene anche salvata in modo decodificato , maggiormente leggibile per una persona (senza tutti i dettagli usati dal protocollo). A questo punto ci si pu chiedere se uno sniffer in grado di trovare informazioni che non passano sulla rete: supponendo per esempio di essere collegato con il mio modem a Internet attraverso un ISP, ho modo di sniffare le comunicazioni che passano sul mio ISP?
La risposta no. Potrei farlo solo riuscendo ad accedere alla macchina (o ad una delle macchine) dell ISP, installando in loco uno sniffer e poi facendomi arrivare i dati che esso legge. Questa sequenza di operazioni tipica di ogni attacco passivo.

PROGRAMMI DISPONIBILI

Esistono molti programmi sniffer, per quasi tutti i sistemi operativi.
La maggior parte di essi non richiede hardware particolari, se non adattatori di rete standard.
Per capire la facilit (relativa) di scrivere uno sniffer, seppur rudimentale, si consideri il programma presente sul sito http://stein.cshl.org/~lstein/talks/WWW6/sniffer/: esso consiste in appena 39 linee di codice Perl!
Esistono sia programmi sniffer a pagamento, sia gratuiti.
Segnaliamo: WinSniffer (http://www.winsniffer.com/ws.html) e UfaSoft Sniffer (http://www.ufasoft.com/sniffer/) per Windows, ettercap (http://ettercap.sourceforge.net/, uno screen shot del programma lo trovate in Figura 2), COLD (http://www.ipv4.it/cold/) e Sniffit (http://reptile.rug.ac.be/~coder/sniffit/sniffit.html) per Linux.
Potete trovare un elenco di altri packet sniffer alla pagina http://www.tlsecurity.net/unix/ids/sniffer/, o fare una ricerca su Internet con il vostro motore di ricerca preferito.

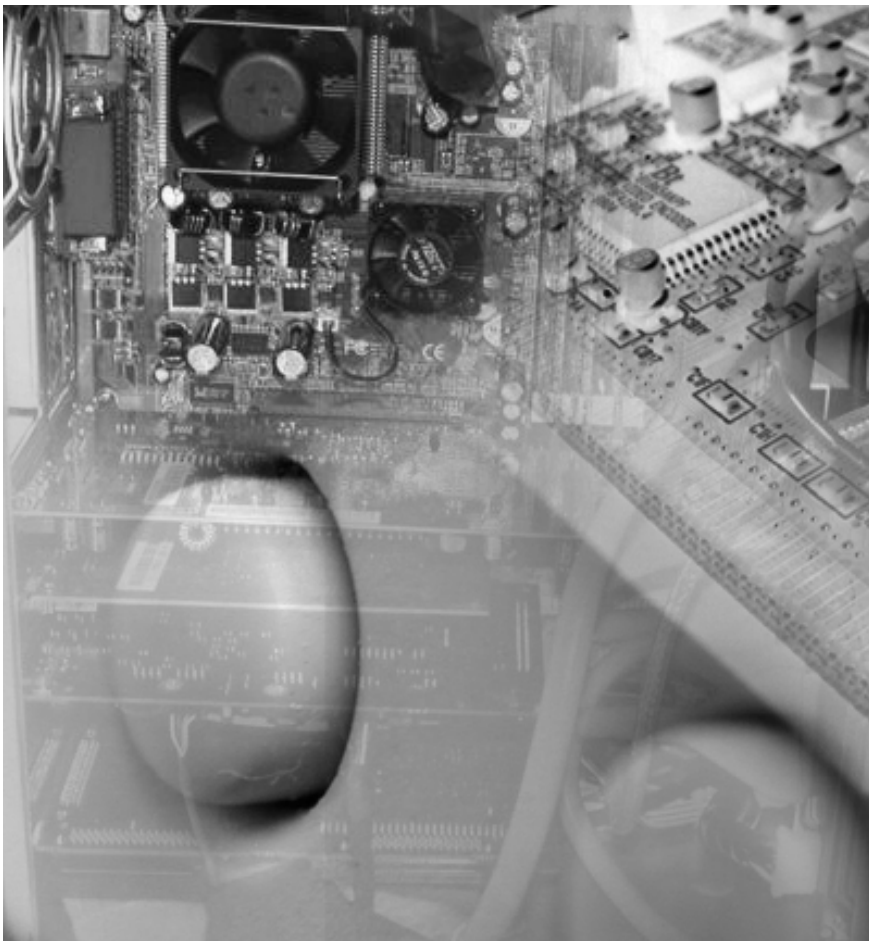
ACCORGERSI DI ESSERE "SNIFFATI"

Anche se un programma sniffer passivo, esistono dei metodi che permettono di rivelarne la presenza. La maggior parte di tali metodi consiste nel mandare richieste (o messaggi) a cui nessun computer della rete dovrebbe rispondere (o accorgersi dell avvenuto invio di tali richieste). Se qualche dispositivo lo fa, evidente che la sua scheda di rete sta lavorando in modo promiscuo, cosa che dovrebbe indurre ad indagarne i motivi.
Altre volte possibile accorgersi della presenza di sniffer dal traffico

che generano (pur essendo programmi passivi, necessitano di mandare dei messaggi per decodificare indirizzi DNS, per esempio). Un altro modo pu essere quello di simulare accessi (con un qualsiasi protocollo) usando nomi di accesso e password fittizi (e quindi non validi), e restare in attesa di tentativi di accesso con tali informazioni. Se questo avviene chiaro che qualcuno in ascolto e usa le informazioni trasmesse. Per i dettagli tecnici delle tecniche pi diffuse si faccia riferimento al documento Sniffer Detection Tools and Countermeasures presente all indirizzo http://rr.sans.org/covertchannels/sniffer.php. Esistono infine tool che permettono di rilevare in automatico la presenza di eventuali sniffer: per una lista di prodotti si veda la directory di Google alla categoria Computers > Security > Intrusion Detection Systems .

COME DIFENDERSI

Esistono modi per difendere i dati da attacchi passivi? Evitare che qualcuno si metta ascolto sulla linea pressoch impossibile (a meno di casi estremi, in cui possibile arrivare anche a questa situazione cos restrittiva). Alcuni sniffer funzionano solo se la rete viene gestita attraverso degli hub. In tal caso sufficiente installare uno switcher. Purtroppo questa soluzione non basta per altri tipi di sniffer (per esempio ettercap in grado di funzionare anche in questo caso). Alcuni protocolli (come il TCP/IP) non offrono meccanismi standard che permettano di proteggere i dati da chi non autorizzato a riceverli n offrono strumenti per la verifica del mittente e/o destinatario.
Il primo consiglio di usare tecniche per cifrare i dati (per una panoramica introduttiva sull argomento si veda [2]), sfruttando protocolli che permettano tale possibilit . Ma bisogna fare attenzione perch non tutti i protocolli che cifrano i dati sono sicuri : il gi citato ettercap riesce, per esempio, a funzionare anche nel caso si faccia uso di SSH1 e HTTPS. Per una panoramica introduttiva sulle tecniche crittografiche si veda [2]. Una strada alternativa consiste nell usare ogni volta password diverse. Tale strategia , chiamata one time password , prevede la generazione di una lista di password. Ogni accesso prevede l utilizzo della password successiva, rendendo non valide le password gi utilizzate.
In questo modo chi entra in possesso della password attuale , non la pu utilizzare, rendendo inutile la presenza di uno sniffer (all indirizzo Web http://www.nas.nasa.gov/Groups/Security/OPIE/ si possono trovare i dettagli di OPIE, OneTime Password in Everything).



REPERIRE ULTERIORI INFORMAZIONI

In quest articolo stata presentata solo una minima parte degli strumenti e delle problematiche relative agli sniffer. Per approfondire i diversi aspetti del problema si pu far riferimento alle risorse presentate in Tabella 1. La problematica del proteggere le informazioni vasta e si applica a tutte le tecnologie di trasmissione. Si pensi che esistono sniffer anche per connessioni Wireless (si veda http://www.iss.net/wireless/WLAN_FAQ.php). Altre informazioni (link a documenti sia in inglese che in italiano, link a prodotti, commerciali e free) le potete trovare all indirizzo http://ivan.0catch.com/risorse/sniffers.htm.

PROBLEMI ETICI

Esistono usi leciti di questi programmi? Sicuramente s , e vogliamo credere che essi nascono proprio per risolvere tali problematiche. Pensiamo ai problemi di configurazione o taratura della rete e dei programmi: necessario monitorare la loro attivit per rendersi conto dei possibili problemi.
L FBI usa un particolare sniffer,

Carnivore (si veda http://www.howstuffworks.com/carnivore.htm), per investigare sulle attivit di presunti criminali. Altre volte necessario monitorare le attivit in corso, per accertarsi che non stiano avvenendo attacchi (lo sniffer permette di registrare ogni attivit in corso, comprese quelle non autorizzate). Inoltre spesso necessario simulare degli attacchi per rendersi conto della sicurezza di un sistema (consulenti che fanno questo di professione vengono definiti anche Ethical Hackers , si veda a tal proposito l articolo Ethical hacking , http://www.research.ibm.com/journal/sj/403/palmer.html).
Ma, a fronte dei molti usi leciti, questi programmi permettono sia di controllare le attivit dei singoli utenti sia di carpirne eventuali informazioni riservate. Ovviamente certi utenti (amministratori dei sistemi) hanno privilegi per cui (teoricamente) possono accedere a tutte le informazioni che transitano sulla rete che amministrano o che sono memorizzate nei loro sistemi. Ø ovvio che la fiducia in tali persone deve essere assoluta. Ma che dire se ad usare gli sniffer sono i dirigenti di aziende, per controllare l attivit dei dipendenti, a loro insaputa? Ø un aspetto controverso, anche sul piano giuridico, e le leggi che regolato tali aspetti variano da paese a paese. A parte l uso improprio degli strumenti, un problema etico si pone anche a chi sviluppa programmi, offrendo funzionalit il cui scopo difficilmente giustificabile da fini leciti (si pensi al reperimento in automatico di tutte le password che transitano sulla rete). Per , chi conosce le problematiche della sicurezza, sa che non l ignoranza sui possibili buchi o usi di standard/programmi che rende una risorsa sicura . Anzi: in mancanza di comunicazione dei problemi o degli usi possibili di una risorsa, si rischia che tale conoscenza sia in possesso solo dei malintenzionati. Insomma, chi sviluppa gli sniffer non fa un uso improprio della tecnologia, ma ne mostra i limiti e contribuisce a far evolvere la tecnologia. Conoscendo i possibili limiti dei sistemi utilizzati, si permette un loro uso pi consapevole e privo di false sicurezze.

L'autore
IVAN **VENUTI**
e-mail: i_venuti@yahoo.it

Bibliografia:

[1] "Internet Security Glossary", R. Shirey, RFC 2828, http://www.isi.edu/in-notes/rfc2828.txt

[2] "Cryptography", A.Cecconi, G. Gallileo http://telemat.det.unifi.it/book/1997/cryptography/Welcome.html