



Il protocollo SMTP e lo Sniffer SPYD

Sommario

Il protocollo SMTP

Introduzione
Breve storia della posta elettronica
Uso del protocollo
Limiti protocollo SMTP: Esempi
I comandi del protocollo
Una sessione SMTP

Lo sniffer SPYD

Descrizione dello sniffer SPYD
Un esempio di sniffing con SPYD
Come utilizzare SPYD
Come proteggere le proprie email da SPYD e da altri sniffer
I codici sorgente di SPYD

Il protocollo SMTP

Introduzione + Breve storia della posta elettronica

La Posta Elettronica (breve storia ...)

- Nel 1969 nasce ARPANET, la prima rete sperimentale.
- Due anni dopo, nel 1971, Ray Tomlinson della BBN inventa un programma "email" per inviare messaggi attraverso una rete distribuita.
- In quel periodo ci sono appena 23 host.

come funziona?

- Quando si spedisce un messaggio di posta elettronica è necessario specificare il destinatario.
- Si scrive il messaggio utilizzando un "Client".
- Il messaggio raccolto dal proprio server viene consegnato al server del destinatario.

Indirizzi E – Mail

- Un indirizzo e-mail è composto da 2 parti: il nome dell'utente ed un nome di dominio.
- Queste due parti sono separate dal simbolo '@' (che si scrive: 'at' e si pronuncia 'et').

ex. mario@posta1.acme.it
- Inviemo il messaggio al 'nostro' server SMTP (Simple Mail Transfer Protocol - semplice protocollo per il trasferimento della posta).

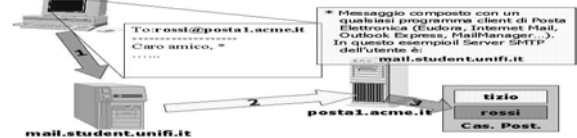
Indirizzi E – Mail (cont.)

- Quando il server SMTP viene a conoscenza dell' indirizzo IP, spedisce il messaggio al server SMTP del destinatario.
- Il messaggio raggiunge il server SMTP del destinatario, il quale tiene conto della prima parte dell' indirizzo e-mail (il nome dell' utente).
- Spedisce il messaggio in un' area del filesystem riservata esclusivamente a quell' utente.

Invio di Posta Elettronica

(Protocollo SMTP)

Schema Generale



- 1) Al momento dell'invio del messaggio, il Client di Posta Elettronica, contatta il Server SMTP di Posta Elettronica (mail.student.unifi.it).
- 2) Il Server SMTP, fungendo da tramite, provvede all'inoltrato del messaggio ai Server di Posta Elettronica di destinazione.
- 3) Il Server di destinazione provvede alla collocazione del messaggio nella casella del destinatario.

Uso del protocollo SMTP

Uso del protocollo SMTP

- Simple Mail Transfer Protocol (SMTP) è il protocollo utilizzato per trasmettere messaggi di posta elettronica tra due host.
- Il Protocollo SMTP non può essere usato per il trasferimento 'finale', poiché la macchina destinataria è di solito off-line (cioè disconnessa), ed è connessa solo per brevi periodi.
- Perciò il server SMTP trasferisce la posta al server POP (Post Office Protocol), dove viene accodato.
- Il destinatario per recuperare l' e-mail usa il protocollo POP.

Uso del protocollo SMTP

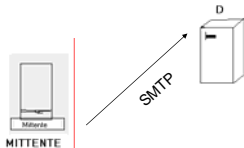
- SMTP utilizza il protocollo di trasporto TCP.
- Un server SMTP rimane costantemente in ascolto sulla porta 25.

Uso del protocollo SMTP

- Normalmente l'invio del messaggio avviene in due passi:
- 1) Il programma di posta elettronica usato dall'utente invia il messaggio al proprio server usando il protocollo SMTP.
 - 2) Il server trasferisce il messaggio al server del destinatario utilizzando lo stesso protocollo.

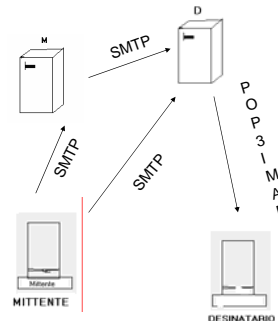
Uso del protocollo SMTP

- Lo scambio avviene fra un mittente ed un server destinatario (D) attraverso una connessione di rete.



Procedura per il trasferimento del messaggio

- Il Mittente può collegarsi ad un server M di invio di posta (caso 1) o direttamente al server D del destinatario (caso 2)
- Nel primo caso M, sulla base dell'indirizzo e-mail del destinatario, identifica il server D ed apre una connessione.
- In entrambi i casi, D identifica il nodo di rete da cui proviene la connessione (cioè il suo indirizzo IP) ed accetta la connessione
- M (caso 1) o il mittente (caso 2) comunica lo username del destinatario. D verifica la validità dell'indirizzo ed autorizza la trasmissione del messaggio.
- M (caso 1) o il mittente (caso 2) invia il messaggio e chiude la trasmissione.
- D memorizza il messaggio in attesa che il reale destinatario si colleghi e ritiri il messaggio utilizzando un apposito protocollo (solitamente POP3 o IMAP).



Analogia con la posta ordinaria

Posta ordinaria	Posta elettronica
Timbro dell'Ufficio Postale	Dati di identificazione di M (indirizzo IP)
Indirizzo del destinatario	Lo username comunicato da M a D come parte del protocollo di comunicazione (punto 3).
Indirizzo del mittente	Campo From:
Intestazione della lettera	Campo To:
Data	Campo Date:

Limiti del protocollo SMTP

Esempi

Esempi sui limiti del Protocollo SMTP

Esempio 1

- Supponiamo che il programma M giri sul nodo 192.168.0.3.
- seguendo la procedura prevista dal protocollo SMTP, può collegarsi ad hercules.arcetri.astro.it, chiedere di inviare un messaggio all'utente lfini ed inviare il seguente messaggio:

Esempio 1

From: president@whitehouse.gov
 To: berlusconi@gov.it
 Cc: lfini@arcetri.astro.it

- L'utente lfini che riceve il messaggio può avere l'impressione, del tutto falsa, di partecipare ad una comunicazione fra capi di stato.

Esempio 2

- Il programma M dal nodo 212.123.84.82 si collega a kremlino.ru e richiede di inviare all'utente vputin il seguente messaggio, contenente un virus in attachment:

From: berlusconi@gov.it

To: vputin@kremlino.it

Parts/Attachments:

1 Shown 6 lines Text 2 OK 8 KB Application

- Il mail server a kremlino.ru è dotato di segnalatore di virus.
- Neutralizza il virus contenuto nell'attachment.
- Avverte il presunto mittente (cioè berlusconi@gov.it)
L'utente che corrisponde all'indirizzo berlusconi@gov.it riceve quindi una segnalazione di virus pur essendo totalmente ignaro e non responsabile.

I comandi del protocollo SMTP

I comandi del protocollo SMTP

- **I principali comandi SMTP:**
- **HELO:** Identifica il client SMTP al server SMTP
- **HELO:** E' possibile usare anche questo comando per identificarsi, se il server supporta le SMTP Service Extensions risponderà in modo positivo altrimenti con un errore di tipo 500 (Syntax Error)
- **MAIL FROM:** <indirizzo mittente>: Indicata la mailbox del mittente del messaggio
- **RCPT TO:** <indirizzo destinatario>: Indica la mailbox del destinatario (Recipient). E' possibile specificare attraverso molteplici RCPT TO diversi destinatari

I comandi del protocollo SMTP

- **DATA:** Indica al server che quanto digitato successivamente saranno i dati del messaggio di posta
- **RESET:** Annulla i comandi (Reset) precedentemente inviati nella sessione SMTP corrente
- **VERFY <stringa>:** Chiede al server se la stringa di testo immessa rappresenta un nome utente presente ed in tal caso visualizza l'intero indirizzo
- **HELP:** Visualizza i comandi disponibili sul server
- **NOOP:** Non esegue nessuna operazione restituisce solo un messaggio 250 (Ok) se il server risponde
- **QUIT:** Termina la sessione SMTP corrente

Una sessione SMTP

Una Sessione SMTP

- Il client **SMTP** contatta il server sulla porta TCP 25.
- Se questo è in ascolto e la connessione è accettata risponde con un messaggio 220 (Ready)
- Il client chiede di stabilire la sessione SMTP inviando il comando **HELO** seguito dal **FQDN** (Fully Qualified Domain Name).
- Se il server accetta risponde con un messaggio 250 (Ok)
- Il client indica il proprio indirizzo tramite il comando **MAIL FROM:** <indirizzo mittente>.
- Il server risponde con 250 (Ok) per ogni destinatario accettato

Una Sessione SMTP

- Successivamente il client indica al server i destinatari del messaggio tramite RCPT TO: <indirizzo destinatario> ed il server risponde per ogni destinatario accettato un codice 250 (Ok) *RCPT TO:* <indirizzo destinatario> ed il server risponde per ogni destinatario accettato un codice 250 (Ok).
- Il client comunica al server l'intenzione di scrivere il corpo del messaggio con *DATA*.
- Il server risponde con un codice 354 e indica come marcare il termine del messaggio.
- A questo punto è possibile scrivere un nuovo messaggio oppure inviare il comando *QUIT*, dopo il quale il server invia i messaggi e risponde con un codice 221 (Closing) e la connessione TCP viene terminata.

Lo Sniffer SPYD

Descrizione

Descrizione dello sniffer

- In una rete con tecnologia Ethernet tutti gli host sono in grado di "leggere" le informazioni che uno di questi ha trasmesso.
- In genere, le informazioni che una "scheda disonesta", o per meglio dire, un utente malintenzionato che opera sul pc della scheda Ethernet, appartengono ai pacchetti del protocollo che si trova più all'interno nell'insieme dei pacchetti annidati;
- Nel nostro caso sono, del protocollo SMTP.

Descrizione dello sniffer

- Un utente malintenzionato può ascoltare illegalmente, o sniffare una sessione di posta in uscita tra un utente ed il suo server di posta utilizzando proprio la caratteristica di tali schede con tecnologia Ethernet.

SPYD

SPYD

Il Demone SPYD



- Il programma demone SPYD ha il compito di dimostrare quanto insicura possa essere una rete con tecnologia Ethernet.
- Il nome, SPYD, sta per "The Spy Daemon", ovvero il demone spia.
- E' definito demone perché così vengono etichettati i programmi che in sistemi Unix-like (linux, FreeBSD, BSD 4.1, etc.) girano in background.

Fasi dello Sniffer SPYD

- 1) Girando su di un host X cattura ogni singolo pacchetto Ethernet.
- 2) Analizza e raggruppa i pacchetti per sessioni. SPYD ricostruisce tutti i pacchetti IP al fine di assemblare un pacchetto TCP.
- 3) Ricostruisce il pacchetto TCP estrae direttamente la sessione SMTP. Alla fine, isola la sessione, SPYD la scrive in un file di testo nel filesystem e l'utente malintenzionato può comodamente andarla a leggere (spiando dunque la posta in uscita di chiunque) senza sforzo alcuno.

Utilizzo dello Sniffer SPYD

- SPYD è stato realizzato per essere compilato ed eseguito su sistemi Linux.
- Il demone, una volta in memoria, cattura tutte le email in entrata e in uscita che passano per quella rete e memorizza ciascuna email in un file diverso.
- Ai file contenenti le lettere verrà assegnato un nome corrispondente alla data all'ora della cattura delle email relative.
- Avranno come estensione la parola .spied come ad esempio il file:

Wed_Nov_10_05:14:48_2004.spied

Un esempio di sniffing con SPYD

Un esempio di sniffing con SPYD

- Lo scenario è quello di una normale rete LAN con tecnologia Ethernet in cui un utente malintenzionato vuol leggere tutte le email che passano per quella rete.
- Il malintenzionato ha privilegi di superutente (root) su un computer con sistema Linux collegato alla LAN.

Un esempio di sniffing con SPYD

- L'utente jB è utente dello stesso sistema Linux del malfattore ma potrebbe tranquillamente essere un qualunque utente di qualsiasi altro computer della rete LAN;
- jB sta per ricevere un'email da Internet...



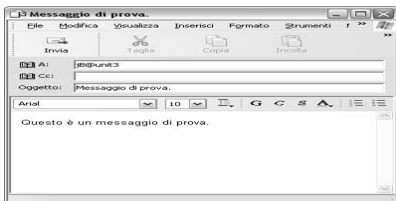
Un esempio di sniffing con SPYD (1/10)

- **Screenshot 1:** Il malintenzionato con privilegi di superutente (root) carica il programma spia spyd.

```
unit3.mirai.net - SecureCRT
root@unit3:~/home/jB/SR# ./s
Makefile  spyd  spyd.c  spyd.h
root@unit3:~/home/jB/SR# ./spyd
root@unit3:~/home/jB/SR#
```

Un esempio di sniffing con SPYD (2/10)

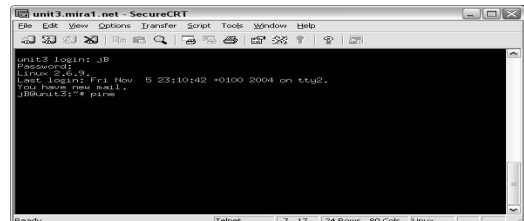
- **Screenshot 2:** Un utente da internet manda una lettera a jB che opera sullo stesso computer dove root ha lanciato una spia (ma, ripetiamo, può stare benissimo su un'altra macchina della stessa rete LAN con tecnologia Ethernet).



Un esempio di sniffing con SPYD (3/10)

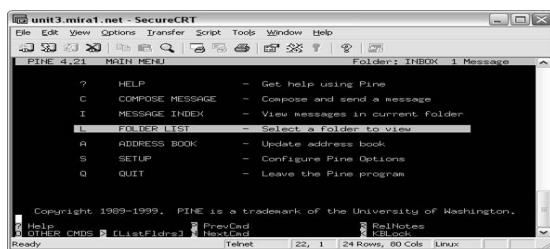
- **Screenshots 3, 4, 5, 6, 7:** L'utente jB utilizza un client di posta, pine, per leggere la sua posta normalmente, e vi legge la lettera che gli è stata inviata.

Screenshot 3



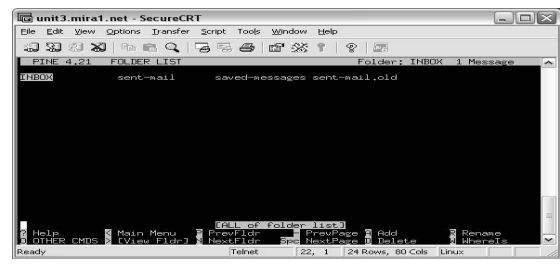
Un esempio di sniffing con SPYD (4/10)

Screenshot 4



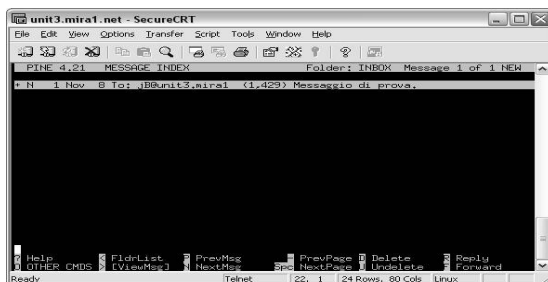
Un esempio di sniffing con SPYD (5/10)

Screenshot 5



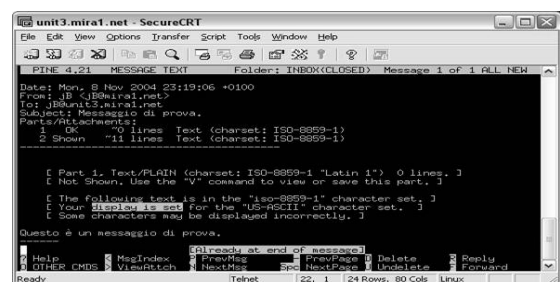
Un esempio di sniffing con SPYD (6/10)

Screenshot 6



Un esempio di sniffing con SPYD (7/10)

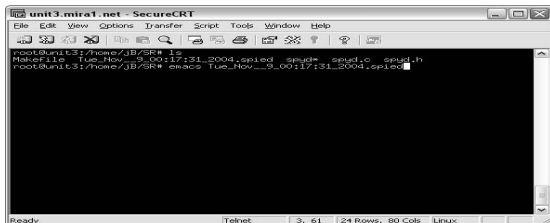
Screenshot 7



Un esempio di sniffing con SPYD (8/10)

- **Screenshots 8, 9, 10:** root raccoglie i frutti del programma spia e legge comodamente la lettera per JB che è stata intercettata e copiata.

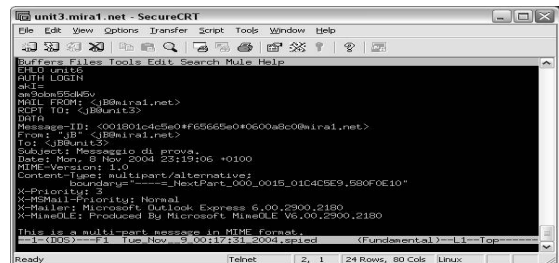
Screenshot 8



```
unit3.mira1.net - SecureCRT
File Edit View Options Transfer Script Tools Window Help
root@unit3:~/home/jb/9K# ./s
Makefile Tue Nov 9 00:17:31 2004.spied spied= spied.o spied.o
root@unit3:~/home/jb/9K# emacs Tue_Nov__9_00:17:31_2004.spied
Ready Telnet 3, 61 24 Rows, 80 Cols Linux
```

Un esempio di sniffing con SPYD (9/10)

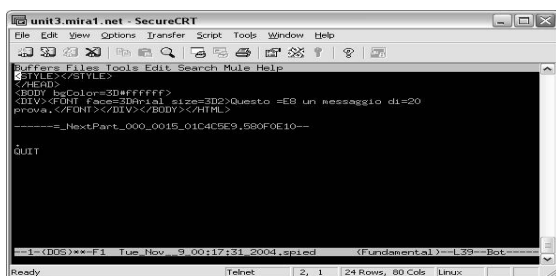
Screenshot 9



```
unit3.mira1.net - SecureCRT
File Edit View Options Transfer Script Tools Window Help
BUFFERS FILES Tools Edit Search Mute Help
RFD (v1.1):
AUTH LOGIN
ehc
am9kbm55d45v
MAIL FROM: <JB@mira1.net>
RCPT TO: <JB@unit3>
Data
Message-ID: <001801c4c5e0f65665e0*0600a3c0@mira1.net>
From: JB <JB@mira1.net>
To: JB@unit3
Subject: Messaggio di prova
Date: Mon, 8 Nov 2004 23:19:06 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
Boundary="=_NextPart_000_0015_01c4c5e9_590f0e10_"
X-Priority: 3
X-Mail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MIMELE: Produced By Microsoft MimeOLE V6.00.2900.2180
This is a multi-part message in MIME format.
--1-(DOS)--F1 Tue Nov 8 00:17:31 2004.spied (Fundamental)--L1--Top--
Ready Telnet 2, 1 24 Rows, 80 Cols Linux
```

Un esempio di sniffing con SPYD (10/10)

Screenshot 10



```
unit3.mira1.net - SecureCRT
File Edit View Options Transfer Script Tools Window Help
BUFFERS FILES Tools Edit Search Mute Help
RFD (v1.1):
<?HEAD>
<BODY bgcolor=#30FFFFFF>
<DIV style="font-family: serif; font-size: 10pt; color: #000000; text-align: center;">Questo è un messaggio di prova.</DIV></BODY></HTML>
-----_NextPart_000_0015_01c4c5e9_590f0e10_--
QUIT
--1-(DOS)--F1 Tue Nov 9 00:17:31 2004.spied (Fundamental)--L39--Bot--
Ready Telnet 2, 1 24 Rows, 80 Cols Linux
```

Come utilizzare SPYD

Come utilizzare SPYD

- SPYD è stato realizzato per essere compilato ed eseguito su sistemi Linux.
- Ha bisogno di parecchi privilegi e quindi è altamente consigliabile essere superutente (root) al momento del lancio del programma.

Come utilizzare SPYD

- I requisiti di sistema dunque sono alquanto minimi. Per eseguire al meglio il programma c'è bisogno di:
 - Un sistema Linux con una interfaccia (scheda di rete) alla rete Ethernet dalla quale si vuole "sniffare" il traffico di posta elettronica,
 - Un compilatore C (possibilmente gcc 2.95.3 o superiore) per compilare il demone,
 - Privilegi di superutente per eseguire lo stesso.

Come proteggere le proprie email da SPYD e da altri sniffer

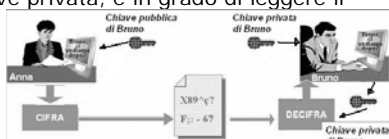
Come proteggere le proprie email da SPYD e da altri sniffer

Il modo più efficace per avere garantita la propria sicurezza durante l'invio di email non è quello di evitare l'intercettazione, bensì quello di non far capire a chiunque a chiunque utilizzi sniffer come SPYD cosa c'è scritto nelle stesse email.

Avvalendosi di programmi di crittografia (come ad esempio quelli inclusi nei più recenti client di posta elettronica) è possibile codificare il testo in chiaro di una email tramite l'utilizzo di una coppia di parole chiave. Di tale coppia una è resa pubblica e viene usata per codificare (o firmare) e l'altra per decodificare (o verificare) una firma.

Come viene cifrato un messaggio di posta elettronica

Per cifrare il contenuto di un messaggio di posta elettronica (inclusi eventuali allegati) deve essere utilizzata la chiave pubblica del destinatario del messaggio. In questo modo solo il destinatario, con la propria chiave privata, è in grado di leggere il contenuto del messaggio.



- Anna deve inviare dei dati riservati a Bruno
- Anna cifra i dati utilizzando la chiave pubblica di Bruno
- Bruno decodifica il messaggio cifrato da Anna, utilizzando la sua chiave privata (chiave segreta, unica chiave in grado di decifrare il messaggio)

Come viene cifrato un messaggio di posta elettronica

Tra le chiavi esiste una correlazione matematica, tuttavia dalla chiave pubblica è un'impresa ardua risalire alla chiave privata.

Lo schema sottostante riporta un promemoria di come devono essere utilizzate la chiave segreta (privata) e quella conosciuta (pubblica).

Azione da compiere	Chiave usata	Di chi?
Firmare un messaggio da spedire	Chiave privata	Di chi spedisce
Verificare la firma del messaggio	Chiave pubblica	Di chi spedisce
Spedire un messaggio criptato	Chiave pubblica	Del ricevente
Decifrare un messaggio criptato	Chiave privata	Del ricevente

I codici sorgenti di Spyd

I codici sorgenti di SPYD

- Il programma SPYD è stato realizzato da Giovanni Bembo, Mara Chirichiello, Iolanda Viscito, Aniello Viviano, ed è distribuito come "freeware" o "Open Source Software".
- Tale programma ha come scopo unico quello di mettere in evidenza le debolezze di una rete con tecnologia Ethernet e **DEVE** essere utilizzato esclusivamente per fini educativi.
- Gli autori si ritengono non responsabili di eventuali conseguenze di qualunque genere causate da un utilizzo improprio del software di SPYD.

- I codici sorgente di SPYD sono disponibili sul sito relativo all'indirizzo:

<http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/spyd/index.html>