



# Strumenti per la sicurezza delle reti

Luigi Catuogno  
luicat@dia.unisa.it  
Baronissi 26 marzo 2002

## Scopo della presentazione



- Panoramica di alcuni tra i principali "punti di insicurezza" in una rete.
- Breve rassegna degli strumenti software per la gestione della sicurezza.

## SOMMARIO



- Sicurezza dei servizi di rete
- Sicurezza del sistema
- Riservatezza dei dati
- Supporto allo sviluppo di applicazioni sicure

## Sicurezza dei servizi di rete



## Servizi di rete



- Connettività (shell, ftp)
- Condivisione di dischi e stampanti
- Database
- Web
- Posta elettronica

## Servizi di rete/2



Accede a questi servizi chi:

- E' autorizzato
- Segue le politiche di erogazione del servizio

## Sevizi di rete/3



In modo che non si pregiudichi:

- La riservatezza e l'integrità dei dati.
- La funzionalità e l'affidabilità del servizio
- La funzionalità e l'affidabilità della macchina

## Tuttavia...



Molti software per la gestione dei servizi di rete possono attuare, in alcune circostanze, comportamenti anomali tali da consentire, a terze parti, un accesso od un utilizzo illecito alle risorse della macchina.

## Un intruso potrebbe:



- Utilizzare il servizio come "porta" per accedere alla macchina, e persino ottenerne il controllo.
- Bloccare il servizio, o la macchina, per impedirne l'utilizzo.
- Utilizzare illecitamente il servizio "fingendosi" un utente autorizzato.

## Nei server su reti TCP/IP



- I servizi (ed i corrispondenti server) sono associati ad un numero di porta.
- L'associazione è stabilita dagli standard dei protocolli dei servizi

Ad esempio: il server di posta elettronica è di norma associato alla porta numero 25.

## Un client quindi..



- Si connette alla macchina server indicando il numero di porta del servizio a cui è interessato.
- Dialoga con il server attraverso un protocollo stabilito.

## Un client fraudolento però..



- Si connette come un normale client
- Invia messaggi "strani" che possono indurre il server a:
  - Bloccarsi
  - Eseguire codice "pericoloso"

## Come difendersi?



- Consultare periodicamente la documentazione del produttore del software, per avere segnalazione di nuovi BUG.
- Verificare periodicamente lo stato di efficienza dei servizi attivi attraverso appositi software di probing.
- Controllare periodicamente i file di log dei server per scoprire eventuali attività sospette.

## BOOKMARKS/1



- <http://www.sendmail.org>: è il sito dei produttori di sendmail: il più celebre (ed attaccato) server di posta elettronica. Il report dei Bug e degli Exploit per ogni versione del programma è accurato e praticamente continuo.

## Il probing



- L'amministratore può spesso verificare la robustezza delle macchine e dei servizi effettuando attacchi con le tecniche più diffuse e documentate.
- Una diffusa tecnica di probing e' detta PORT-SCANNING

## Un port scanner e'..



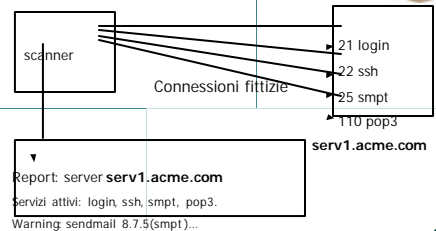
- Un programma che simula connessioni ad i servizi di rete, scandendo esaustivamente le porte per appurare quali servizi sono attivi.
- Richiede a ciascun servizio informazioni di tipo diagnostico o di aiuto per identificare il tipo di server e determinarne il grado di vulnerabilità.

## Ci sono port-scanner...



- Stupidi: che effettuano un controllo esaustivo di tutti i numeri di porta.
- Super accessoriati: in grado di:
  - gestire sessioni di probing anche periodiche, su singole macchine o su intere reti.
  - Estendibili e modulari

## Scanning di un server



## Alcuni port-scanner



- **PortScan**: il primo e più semplice
- **SATAN**: sicuramente il più famoso, ha un interfaccia basata su WEB, la più recente evoluzione si chiama **SAINT**.

## Alcuni port-scanner/2



- **NESSUS**: simile a SAINT, realizza un sistema di probing distribuito, ha un server che effettua le sessioni di scanning su richiesta di diversi client anche remoti.
- **Retina**: sofisticatissimo scanner, gestisce database di report e di exploit. Commerciale.

## Sicurezza del sistema



## Sicurezza del sistema



Un sistema può essere soggetto ad attacchi provenienti "dall'interno", ossia mossi da utenti abilitati all'accesso sulla macchina, o da intrusi che vi hanno acceduto fraudolentemente dalla rete.

## Lo scopo degli attacchi potrebbe essere:



- Accedere a dati contenuti nel sistema, ad esempio:
  - Dati riservati.
  - Password o credenziali degli utenti.
- "Colonizzare" la macchina per utilizzarla in ulteriori attacchi.

## Le password



- Sono brevi stringhe di caratteri (in genere 8) segrete, che un utente fornisce a richiesta per comprovare la sua identità.
- Devono essere generalmente ricordate dal titolare.
- Sono oggetto di numerose tecniche di attacco.

## La verifica delle password



- Al momento in cui un utente viene abilitato su un sistema, la password che sceglie viene cifrata con una funzione non invertibile
- La password cifrata viene custodita in un file noto (`/etc/passwd` nei sistemi UNIX)

## La verifica delle password/2



- Quando l'utente desidera connettersi al sistema, fornisce la password.
- La password fornita viene cifrata nello stesso modo della prima volta.
- Le due stringhe vengono confrontate, se risultano uguali, la password fornita è accettata.

## Vulnerabilità delle password



- Poiché si tratta in genere di stringhe mnemoniche, un intruso può tentare di "indovinarle".
- Se il sistema è già stato "colonizzato", l'intruso potrebbe sostituire il programma preposto alla richiesta ed alla verifica delle password, con un suo programma che gli consenta di tenerne traccia.

## Vulnerabilità/2



- Durante le connessioni remote la cifratura della password è effettuata solo sulla macchina destinazione, pertanto, questa viaggia in chiaro attraverso la rete.

## Come difendersi



- Gli utenti dovrebbero aver cura di scegliere password difficilmente prevedibili, possibilmente non di senso compiuto.
- L'amministratore di sistema potrebbe verificare preventivamente che la password scelta da un nuovo utente non sia contenuta in un dato dizionario.
- L'amministratore di sistema potrebbe periodicamente verificare la bontà delle password dei suoi utenti mediante un attacco simulato.

## Smart Card



- Una tessera di plastica, dalle forme e dimensioni di una carta di credito, in cui è incastonato un microchip



- Inventate da **Roland Moreno** nel 1974

## Alcuni impieghi:



- Telefonia GSM
- Satellite Television
- Sistemi di pagamento
- Gestione informazioni personali

*Il numero di smart card in circolazione si stima in centinaia di milioni di unità*

## Memory card:



- Il chip non è programmabile ma è solo in grado di memorizzare dati
  - Limitate misure di sicurezza
  - Fornisce un elementare file system
  - Costo contenuto

## Chip Card:



- Il chip è un vero e proprio mini computer con memoria, I/O e sistema operativo a bordo.
  - Memorizza dati e software
  - Accede autonomamente ai dati
  - Sistemi di sicurezza più sofisticati
  - Più costosa

## Chip Card: architettura



- Micro Processor Unit (MPU)
  - Capacità: da 8 a 32 bit RISC
  - Velocità di clock anche fino a 32 Mhz
- I/O controller
  - Gestisce la comunicazione col Card Acceptance Device (CAD)

## Chip Card: architettura/2



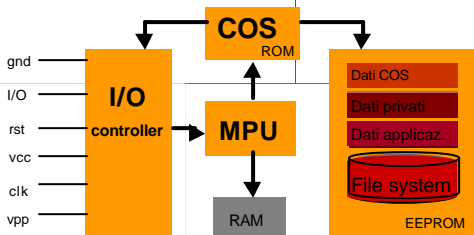
- Program Memory (ROM)
  - Contiene codice inserito dal costruttore (à la BIOS)
- Working Memory (RAM)
  - Dati prodotti dall'elaborazione
- Application Memory (EEPROM)
  - Contiene dati permanenti
  - Non volatile (durata almeno 10 anni)

## Chip Card: architettura/3



- Card Operating System (COS)
  - Istruzioni memorizzate nella ROM ad uso delle applicazioni
  - Può essere *general purpose* o *dedicated*

## Chip Card: architettura/4



## Smart Card: Comandi

- L'application Processing Data Unit (APDU) è un record contenente:
  - la rappresentazione del comando,
  - gli argomenti
  - i dati
- Per impartire un comando occorre comporre l'apposita APDU (bit per bit!)

## Smart Card: standard

- ISO 7816 (9 sezioni... *in aumento*)
  - Specifiche costruttive
  - Comunicazione tra carta e lettore
- EMV
  - Smart Card per servizi finanziari.
  - Voluta da Europay, Mastercard e Visa
  - Riprende ISO7816 con alcune estensioni "*business-oriented*"

## Il mondo esterno...

- Non esiste una interfaccia standard per il lettore
  - Ogni produttore fornisce driver ed API per il proprio device

## CT-API

- È uno strato software che fornisce un'interfaccia API per il CAD device driver
- Realizzata da un gruppo di aziende tra cui Deutsche Telekom
- L'interfaccia è decisamente spartana
  - Lo sviluppatore costruisce le APDU bit per bit

## PC/SC

- Framework per la realizzazione di applicazioni card-aware indipendenti dal device
- Fornisce API leggermente più evolute
- Esiste una versione per Linux (PCSC lite)
- Recentemente adottato da Microsoft per integrare il supporto di smart card in Win32

## Open Card



- Framework per applicazioni Java:
  - Tentativo di standardizzare l'interfaccia tra applicazione, sistema operativo e CAD
  - Fornisce una serie di classi per interagire con la carta.
  - La comunicazione avviene attraverso il passaggio di APDU costruite "a mano" oppure da appositi metodi
  - Gestione ad eventi

## PAM



- Un set di librerie per l'implementazione modulare delle politiche di sicurezza

## PAM/2



- Fornisce alle applicazioni una serie di API "astratte" per:
  - Autenticazione
  - Accounting
  - Sessione
  - Verifica del profilo utente
  - Modifica del profilo utente

## PAM/3



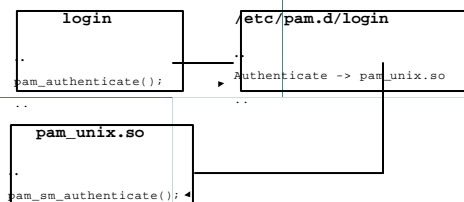
- Fornisce agli sviluppatori di sistemi di sicurezza delle API "standard" per renderli compatibili con le applicazioni *PAM-aware*
  - Tali servizi sono così implementati come moduli intercambiabili

## PAM/4



- Fornisce agli amministratori una infrastruttura per la modifica delle politiche di sicurezza
  - Mediante semplici file di configurazione
  - Senza intervenire sulle applicazioni

## PAM: architettura



## PAM: un esempio



- In un dato momento, una macchina Unix, autentica gli utenti, durante la fase di login, attraverso il classico schema a password
- Il comandi che utilizzano tale schema sono, tra gli altri:
  - Login, telnet, su, passwd, ftp, xdm, etc.

## PAM: un esempio/2



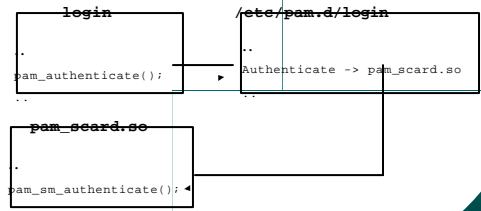
- L'amministratore di sistema decide di passare ad una procedura di autenticazione basata su smart card
- Deve necessariamente:
  - Installare il software di gestione delle carte
  - Reperire, o modificare in proprio tutti i programmi interessati a questo cambiamento

## PAM: un esempio/3



- Se però le applicazioni sono PAMaware, dovrà soltanto:
  - Installare il software di gestione delle carte
  - Installare il modulo PAM per l'erogazione dei servizi
  - Configurare i singoli comandi affinché facciano riferimento al nuovo modulo

## PAM: un esempio/4



## Codice "malizioso"



- Dopo una violazione del sistema, un intruso potrebbe installarvi dei programmi da utilizzare per sottrarre dati riservati, o per muovere attacchi verso altre macchine.
- Tale codice può anche sostituire comandi o applicazioni di sistema.

## Un esempio:



- Un intruso sostituisce il server di posta elettronica in uscita (sendmail) con una sua versione che tiene traccia in un file, dei messaggi inviati da un certo utente o destinati ad un certo indirizzo.
- L'intruso sostituisce il comando ls con una sua versione che non visualizza quel suo file di messaggi.

## Codice "malizioso"/2



Simili attacchi :

- Hanno spesso lo scopo di assumere il controllo della macchina.
- Non sono facilmente individuabili una volta posti in essere.
- Talvolta l'installazione di software "modificati" può essere molto invasiva.

## Rootkits



- Raccolta di applicazioni di sistema modificate e già "pronte per l'uso".
- Una volta installato un rootkit, falsa la percezione dello stato del sistema e nasconde le tracce dell'attività dell'intruso.
- L'intruso ha il controllo della macchina ed accesso completo ai dati presenti su di essa.

## Tripwire



- E' una utility che consente di individuare programmi "contraffatti" eventualmente installati sul sistema.

## Tripwire/2



- Tripwire inizializza il suo database, raccogliendo le informazioni necessarie ai confronti sui file da "sorvegliare"
- Periodicamente calcola le stesse informazioni e le confronta con quelle ottenute durante l'inizializzazione.

## Tripwire/3



- Se le due impronte non coincidono, il file ad esse associato ha subito modifiche dall'ultimo confronto (o dall'inizializzazione del database).
- Il file in questione potrebbe essere stato modificato/sostituito.

## BOOKMARKS/2



- <http://www.tripwiresecurity.com> : è il sito della Tripwire Security Systems , dove sono distribuiti i sorgenti del pacchetto, e la relativa documentazione. Sono inoltre disponibili interessanti informazioni su eventi, prodotti e tecnologie nel campo della sicurezza.

## Codice "malizioso"/3



- Un altro metodo per l'installazione o esecuzione di software malizioso su una macchina in rete consiste nell'indurre un utente/amministratore di questa a scaricarlo dalla rete ed eseguirlo (anche inconsapevolmente).
- Un'applicazione tipica di questo approccio sono i Virus.

## Soggetti a rischio...



- Plug-in
- Applicazioni distribuite in formato binario
- Applet Java
- ActiveX
- Attachment

## Macrovirus



- Virus scritti come "macro" di applicazioni utente:
  - MS Word, Excel, Access, etc.
- Possono essere eseguiti all'atto dell'apertura di un documento
- Possono accedere virtualmente a tutte le funzioni del sistema operativo

## Macrovirus/2



- Melissa e I Love You
  - Scritti in VB
  - Si trasmettono via E-Mail
  - Accedono e modificano il file registro di Windows

## Worms



- Votati principalmente alla diffusione
  - Danneggiamento o sottrazione di dati
  - Rallentano fino a bloccare il computer ospite
  - Possono intasare una rete locale con le loro "spore"
- Possono utilizzare differenti metodi di "contagio"

## Worms/2



- Nimda
- RedAlert

## Come difendersi



- Utilizzare/installare software solo se di provenienza fidata.
- Microsoft e Sun hanno proposto alcuni sistemi per la certificazione (mediante firma digitale) dell'affidabilità di ActiveX ed Applet.
- Molti Programmi Anti Virus possono verificare la presenza di file infetti anche quando questi sono giunti sul sistema come allegati di posta elettronica.

## Sicurezza dei dati



## Sicurezza dei dati



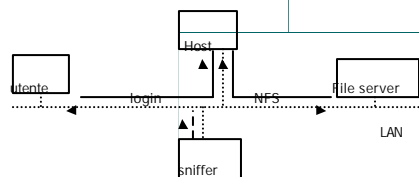
In ambienti distribuiti:

- Le risorse sono dislocate in punti diversi di una rete.
- Spesso più macchine condividono delle risorse.
- I dati transitano ripetutamente attraverso la rete ed alcuni suoi nodi.

## Un intruso può...



Accedere a dati riservati semplicemente mettendosi in ascolto sulla rete



## TCPDUMP



- E' uno sniffer estremamente semplice e versatile
- Consente di interpretare le informazioni legate ai principali protocolli di comunicazione su reti locali TCP/IP.
- Dispone di un ricco insieme di operatori che consentono di filtrare agevolmente il traffico che interessa.
- Può essere un ottimo strumento di diagnostica.

## TCPDUMP/2



- Pone la scheda ethernet in modalità promiscua (ossia, in grado di ricevere anche i frame che non sono destinati a lei).
- Legge i dati provenienti dalla rete.
- Li "organizza" a seconda delle richieste dell'utente.

## BOOKMARKS/3



- <http://www.icpdump.org>: sito ufficiale del progetto TCPDUMP, vi si possono trovare i sorgenti, documentazione e link a numerosi progetti analoghi.

## Altri sniffer



TCPDUMP è per lo più uno strumento di diagnostica. Sono disponibili programmi più sofisticati che offrono servizi più "specializzati" per il tipo di dati che si intende captare (password di login, web, segmenti NetBIOS, etc.).

## Altri sniffer/2



- Dsniff: popolarissimo sniffer, tra i più semplici da usare.
- Snort: consente di "tener d'occhio" e tracciare l'attività di una rete locale. Altamente configurabile, è utilizzato come strumento di "intrusion detection".
- WebSniff: sniffer specializzato nell'intercettazione di password sul Web.

## Come difendersi



- Esistono diversi tool e tecniche che possono aiutare nel rilevare la presenza di uno sniffer sulla rete.
- Si può rendere incomprensibile il risultato dello sniffing mediante la **cifratura dei dati**.

## Difendersi dagli sniffer



- Utilizzando protocolli di comunicazioni basati sulla crittografia, un intruso in ascolto non può comprendere i dati captati.



## Cifratura dei dati



- Secure Shell (ssh)
- Secure Ftp (sftp)
- HTTP over SSL (https)
- Pretty Good Privacy (PGP)
- Transparent Cryptographic File System (TCFS)

## Secure Socket Layer



- SSL è un protocollo di comunicazione sicuro implementato al quarto livello dello stack ISO/OSI (transport layer).
- SSL consente la creazione di un canale cifrato tra i partecipanti ad una connessione.
- SSL è alla base di alcuni dei più diffusi pacchetti per la protezione dei dati su reti

## Secure Shell



- Applicazione client/server per la realizzazione di connessioni interattive attraverso un canale cifrato.

## HTTPS



- Protocollo per il trasferimento di documenti ipertestuali attraverso un canale cifrato.
- Viene utilizzato nei siti web in cui sono richiesti e trattati dati sensibili (dati personali, finanziarie, etc.)
- Si basa su SSL, e sulla tecnologia dei certificati digitali.

## HTTPS/2



Supportano HTTPS (tra gli altri)

- Apache
- Microsoft IIS
- Netscape enterprise
- IBM Web Sphere

## HTTPS/3



Supportano HTTPS (tra gli altri):

- Netscape navigator
- Microsoft Internet Explorer

## BOOKMARKS/4



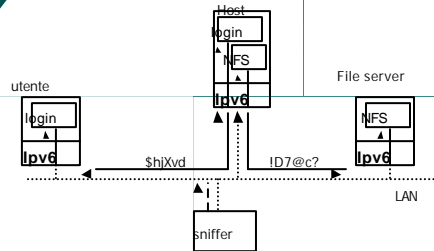
- <http://www.openssl.org>: sito ufficiale del progetto OpenSSL.
- <http://www.openssh.org>: sito ufficiale del progetto OpenSSH
- <http://www.modssl.org>: sito ufficiale dell'estensione SSL per il server web apache. Contiene una imponente documentazione per l'utilizzo del protocollo HTTPS con apache.

## IP versione 6



- E' il protocollo di rete che dovrebbe sostituire l'attuale protocollo IP (IPv4)
  - Ampliamento dello spazio degli indirizzi
  - Autenticazione dei datagram IP
  - Cifratura dei datagram IP

## IP versione 6 vs Tcpdump



## IPv6: Vantaggi



- Politiche di sicurezza omogenee per tutti i servizi di rete
- I servizi non devono implementare in proprio i servizi di cifratura

## IPv6: svantaggi....



## BOOKMARKS/5



- <http://www.ietf.org>: il sito ufficiale dell' "Internet engineering task force"
  - Coordinamento nello studio ed applicazione dei protocolli internet
  - Repository delle specifiche degli standard in vigore (le famose RFC)

## BOOKMARKS/6



- <http://www.diareti.diaedu.unisa.it> sito del "Laboratorio Reti". Vi potrete trovare tutta la documentazione riguardante il corso, il software e le modalità di utilizzo delle strutture.