

Linux Desktop Security

Giuseppe Augiero



Organizzazione

- **Location:** La Limonaia.
- **Date:** 13/20/27 giugno 2012.
- **Corso:** 3 lezioni da 2 ore (21.00-23.00).
- E' necessario portare il proprio computer portatile.

Programma

- **Prima lezione:** Concetti di base relativi alla sicurezza.
- **Seconda lezione:** La rete e il firewall.
- **Terza lezione:** Laboratorio.

Comunicazioni

- Mail list Gulp.
- Mail list del corso.

Sicurezza

Sicurezza informatica

- Cos'è per voi la sicurezza informatica?

Sicurezza IT

- Alcune definizioni grossolane di sicurezza sono:
 - Evitare che succeda qualcosa di “non buono”.
 - Avere i servizi critici sempre disponibili.
 - Rilascio indesiderato di informazioni private.
 - Evitare il danneggiamento o sostituzione di informazioni importanti.
 - Elusione dei sistemi di protezione per scopi illegali.

Affidabilità e fisicità

- Alcune volte con la parola “sicurezza del computer” si pensa all’aspetto fisico del problema.
 - Dischi in raid, backup, alimentatori doppi...
 - Estintori, accesso controllato, grate ...

Sicurezza: Quando?

- Nel caso di un software:
 - Prima dell'esecuzione.
 - Durante l'esecuzione.
 - Dopo l'esecuzione.

Sicurezza dell'informazione

- In ambito informatico con la parola “Sicurezza” si intende la sicurezza dell'informazione.
- La sicurezza informatica definisce:
 - **“Le regole per il controllo dell'accesso all'informazione e alle risorse.”**

Principi di base

- La sicurezza deve garantire:
 - **Confidenzialità.** Solo chi è autorizzato conosce l'informazione.
 - **Integrità.** L'informazione non può essere manomessa da chi non è autorizzato.
 - **Disponibilità.** L'informazione è disponibile solo per chi ha l'autorizzazione ad usarla.
 - **Non ripudiabilità.** Il mittente di un messaggio non può disconoscere la paternità del messaggio.

Confidenzialità

- Garantisce protezione dell'informazione o delle risorse sensibili.
- La necessità di mantenere l'informazione segreta nasce dall'uso dei calcolatori in campi sensibili come governo o industria.
- Principio del Need-to-know.
- La crittografia è un buon meccanismo per garantire la confidenzialità.

Integrità

- L'informazione non deve essere danneggiata o modificata dalla computazione.
- Un primo semplice approccio è quello di dare accesso in scrittura solo a chi è autorizzato.
- Occorre garantire:
 - Integrità dei dati.
 - Integrità della sorgente.
- Un meccanismo di integrità è l'uso di xor o hash.

Differenze

- La confidenzialità garantisce la non compromissione del dato.
- L'integrità garantisce correttezza ed affidabilità del dato.

Disponibilità

- La disponibilità garantisce la possibilità di utilizzo delle informazioni e delle risorse desiderate.
- Una risorsa non disponibile non è più utile di una risorsa inesistente.
- Un Denial of Service (DoS) è un tipico attacco per rendere indisponibile una risorsa.

Add-on?

- Pensare che la sicurezza informatica sia un add-on da applicare sopra al lavoro già svolto è un grave errore.
- Le soluzioni vanno pensate in modo che siano sicure già in fase di progettazione.



La sicurezza non ha uno sviluppo statico ma
è un processo iterativo.



La sicurezza
è una questione di punti di vista.

Il valore della sicurezza

- Quando si parla di sicurezza spesso **non si comprende il valore dei dati da proteggere.**
- Esiste un conflitto tra sicurezza e facilità di utilizzo di un computer.
- **La sicurezza è considerata un costo e non un beneficio.**
- Quanto costa non adottare la sicurezza?
- I benefici della sicurezza non sono sempre quantificabili.

Costi della sicurezza

- Adottare la sicurezza significa sostenere i seguenti costi:
 - Selezionare, formare, mantenere personale qualificato.
 - Acquistare tecnologia hardware e software.
 - Tenere aggiornata la tecnologia usata.
 - Aumento della complessità operativa ed organizzativa.
 - Aumento dell'overhead e degrado delle performance.

Il beneficio della sicurezza

- I costi da sostenere sono inferiori al costo che l'organizzazione sosterrrebbe in caso di compromissione del sistema.

Da dove iniziare

- Il primo passo da effettuare per la definizione delle politiche di sicurezza è **l'analisi dei rischi.**
- L'analisi dei rischi deve individuare i punti critici del sistema IT.
- I punti critici rappresentano gli elementi di ridotta robustezza dell'infrastruttura informatica.

Robustezza informatica

- La robustezza di un componente è la capacità di **non danneggiare** il sistema in cui è inserito quando vengono violate le specifiche del comportamento stesso.
- Violazioni delle specifiche significa:
 - Input diversi da quelli specificati.
 - Risorse diverse da quelle specificate.

100% sicuri

- **E' inutile cercare di essere impenetrabili.**
- Occorre essere costosi (tempo e denaro) nell'essere attaccati.
- Per proteggere un bene dal punto di vista IT non si dovrebbe mai spendere di più del valore del bene stesso.
- La sicurezza al 100% non esiste!

Il rischio

- Il rischio è l'incertezza che eventi inaspettati possano manifestarsi producendo effetti negativi in un dato contesto.

Risk assessment (I)



- Il processo di **risk assessment** è usato per determinare l'ampiezza delle potenziali minacce ad un sistema IT ed identificare tutte le possibili contromisure per ridurre o eliminare tali voci di rischio.

Risk assessment (II)

- Vengono identificati:
 - Asset.
 - Minacce.
 - Vulnerabilità.
 - Contromisure.
- Vengono determinati:
 - Impatto prodotto dalle minacce.
 - Fattibilità delle minacce.
 - Complessivo livello di rischio.

Risk mitigation

- Nel processo di **risk mitigation** vengono analizzati le contromisure raccomandati dal team di assessment, e vengono selezionati e implementate le contromisure che presentano il miglior rapporto costi/benefici.



Catene di sicurezza

- La sicurezza di un sistema può essere paragonato a una catena.
- La misura del livello di sicurezza dell'intero sistema è determinato dalla robustezza dell'anello più debole della catena.

Sicurezza ... relativa

- La nozione di sicurezza è un qualcosa di relativo e non di assoluto.
- Non esiste un sistema sicuro in assoluto.
- La sicurezza è un concetto relativo:
 - “Il sistema A è più sicuro del sistema B?” (quesito errato)
 - “Il sistema è sufficientemente sicuro da sostenere il mio business?” (quesito corretto)

Usabilità

- **Sicurezza e usabilità sono spesso in antitesi.**
- Il sistema più usabile è quello privo di misure di sicurezza.
- Un sistema completamente sicuro è un sistema che opera solo localmente, staccato dalla rete, collocato in un bunker, senza finestre, con un plotone di guardie armate e cani ringhiosi e con un sistema di video sorveglianza.
- Chi vorrebbe lavorare in tali condizioni?

Security trade off

- **Occorre trovare il giusto equilibrio tra usabilità e produttività da un lato e sicurezza dall'altro.**

Politiche di sicurezza

- Tre sono le politiche fondamentali per la robustezza:
 - **controlli nell'accesso degli oggetti.**
 - **controlli di identificazione.**
 - **politiche di crittografia:**
 - per l'identificazione degli oggetti.
 - per la confidenzialità dei dati.

Modelli di sicurezza

- Esistono tre approcci di base per sviluppare un modello di sicurezza:
 - **Offuscamento (by obscurity).**
 - **Difesa perimetrale.**
 - **Difesa in profondità.**
- E' possibile usare una combinazione delle 3 possibilità.

Un buon approccio...

- Fornire linee guida.
- Soluzioni implementabili.
- Accettabile da parte di tutti.
- Controllare che siano rispettate (audit)
- Responsabilizzare.
- Scegliete gli obiettivi per valutare il trade-off.
- Facilità di utilizzo.
- Valutare i costi.

I consigli della nonna

- Minimi privilegi.
- Prevedere diversi livelli.
- Prevedere diversi sistemi di sicurezza.
- Centralizzare la gestione.
- Concentrare l'attenzione sui punti deboli.
- Fail-over.
- Partecipazione di tutti gli utenti.

Audit

- In una “buona sicurezza” non può mancare il monitoring e l’audit.
- Le ragioni di analisi possono essere:
 - Controllo delle operazioni effettuate.
 - Controllo del rispetto delle politiche di sicurezza.
 - Ricerca di segni di intrusione.
- Analisi dei log non è una operazione banale.

Chi?

- Da chi dobbiamo difenderci:
 - Hackers.
 - Crackers.
 - Ricercatori di informazioni.
 - Procuratori di Denial of Service.
 - Script kiddies.

Come?

- L'attacco può essere portato a termine attraverso:
 - Exploit.
 - Zero day.
 - DoS.
 - Virus / cavalli di troia.
 - Malware.
 - Phising.

Perchè?

- Motivi di attacco o di penetrazione possono essere:
 - Furto dati.
 - Modifica delle informazioni.
 - Odio.
 - Motivazioni politiche/religiose.
 - Sfida intellettuale.

Social Engineering

- Con la parola “**Social Engineering**” si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.
- E' **l'arte di saper mentire.**
- Spesso è “poco tecnologico”.

Da cosa dobbiamo difenderci

Virus

- Un **Virus informatico** è un programma che involontariamente viene memorizzato nella memoria di massa del computer e la cui esecuzione provoca effetti indesiderati ed imprevedibili sui dati del computer e sul suo funzionamento.
- Il Virus viene attivato automaticamente con l'esecuzione di programmi applicativi o di comandi di sistema operativo.

Tipologie di virus

- **Macro:** Autoreplicanti. Distruggono o alterano i dati. Sono attivati quando vengono eseguiti i programmi a cui si sono attaccati (tipicamente file Word, Excel).
- **Worm:** entrano in funzione in modo autonomo. Distruggono e/o alterano i dati. Si autoreplicano e tramite connessioni di rete si diffondono sulla rete.
- **Trojan:** Programmi “apparentemente” utili o di intrattenimento usati per introdursi illecitamente nel computer ed inviare in rete dati ed informazioni in modo.

Phishing

- “Attività criminale che sfrutta tecniche di ingegneria sociale (pressione psicologica, fiducia irragionevole, propensione a rispondere in modo diretto ed immediato...), ed è utilizzata per ottenere l'accesso ad informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo di comunicazioni elettroniche, soprattutto email fasulle, chat, e contatti telefonici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc...” (Wikipedia).

Malware (I)

- **Spyware:** software illecito per monitorare e registrare le scelte e preferenze di un utente senza che ne sia consapevole:
- **Keylogger:** programmi che registrano tutti i tasti premuti dall'utente.
- Programmi che inviano l'audio ed il video in ingresso.

Malware (II)

- **Adware:** software che si introduce nel computer, talvolta insieme ad altro software di utilità, che visualizza messaggi pubblicitari. Può essere associato a sistemi di tracking che intercettano e trasmettono dati ed informazioni riservate.

Maleware (III)

- **Dialer:** software che riconfigura la connessione ad Internet (via modem) verso un numero di telefono a tariffazione maggiorata.
- Spesso si installano nel computer all'accesso di pagine web di siti pubblicitari o di natura erotica.
- Non hanno effetto nelle connessioni a rete locale o tramite ADSL.

Botnet

- Una **botnet** è una rete formata da computer collegati ad Internet e infettati da malware, controllata da un'unica entità, il **botmaster**.
- A causa di falle nella sicurezza o per mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, i computer vengono infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto.

Linux Desktop Security

Giuseppe Augiero

