LAS - Appunti lezioni

Daniel

March 7, 2020

Appunti lezioni

0.1 3/3/20

Pacchi di slide viste:

- lab-virtualbox.pdf
- interfaccia di testo

Setup Macchine Virtuali La reinizializzazione dei macaddres e' indispensabile nel caso in cui le macchine virtuali debbano coesistere nello stesso segmento di rete. In caso contrario non e' strettamente necessario. Nel file /etc/udev/rules.d/70-persistent-net.rules e' possibile trovare configurazioni per la persistenza delle assegnazioni $interfaccia - rete \iff mac - addres$.
Quando si passa ad un altro utente si puo' usare il comando su, consigliato con il trattino per importare e settare tutto l'ambiente di un eventuale utente (var di ambiente, etc etc) per tornare all'utente di partenza CTRL-D (o exit) per fare clean della cli (CRTL-L) o clean CRTL-S per freezare il terminal - CRTL-Q per sbloccarlo
SUDO: quando eseguo sudo l'ambiente di esecuzione rimane invariato a quello del chiamante. perche' sudo ls -l /root ¿ /root/prova non funziona? perche' sudo agisce solo sul comando ls, quando la shell prova ad aprire in scrittura il file /root/prova ovviamente fallisce perche' las (utente da cui si e' lanciata la shell) non ha i privilegi necessari. sudo -i apre una sessione interattiva con i privilegi di root, in questa maniera l'intera gerarchia dei processi che lancio dalla shell verra' lanciata come root e quindi da utente privilegiato. (VEDERE MAN PAGE SUDO) L'utente las puo' utilizzare sudo digitando la propria passwd, questa richiesta e' un layer di sicurezza di secondo ordine - l'utente si allontana lasciando il terminale incustodito e un malintezionato prova a inserire comandi - risvegliare l'attenzione dell'utente prima di svolgere un job da root (cerca di qualcosa con privilegi elevati) Sudo inolte possiede un sistema di caching interno, una volta inserita la passwd , questa viene tenuta in cache per 5 min in modo da non doverla ridigitare continuamente. Comando visudo per modificare /etc/sudoers contenente le configurazioni di sudo e i permessi assegnati. dover inserire la passwd. (TODO:HOW?)
/etc/hosts permette di risolvere localmente richieste DNS
per disattivare un'interfaccia basta commmentare le righe relative nel file /etc/network/interfaces
CONFIGURARE /etc/netowork/interfaces per macchine client router server
esistono tool per utilizzare il mouse in cli , utile essenzialmente per fare operazioni copia incolla.

CLI interfaccia al sistema operativo. Interprete di comandi. Il linguaggio della shell si puo' pensare come un linguaggio general purpose, ha tutte le caratteristiche che servono per poter scrivere qualsiasi tipo di algoritmo. La shell offre un linguaggio che permette di automatizzare job, eseguire automaticamente set di operazioni

4 macrocategorie di comandi
BASH Manual
Codici ANSI

La shell deve distinguere sulla riga le diverse parti che successivamente all'espansione divenetaranno gli argomenti.

suffisso 'rc' = resource configuration

- comando touch

0.2 hardening e controllo dell'accesso

Sicurezza la sicurezza e' il risultato di un processo, che tiene in considerazione tutti gli aspetti non solo tencologici ma anche umani. Alcuni elementi organizzativi che possono tornare utili: - in generale la sicurezza si ottiene quando tutti gli elementi presenti posso agire in accordo alla politica dei privilegi minimi - la sicurezza e' antagonista dell'usabilita' si cercano soluzioni che pongano meno ostacoli possibili fra il servizio in oggetto e gli utenti finali che vogliono utilizzarlo

messa in sicurezza fisica la predisposizione fisica ha una sua importanza rilevante.

- collocazione hardware - allocazione delle risorse - procedura di avvio del sistema

TODO: - guardare MAN page dei tools: -adduser -addgroup -chown - concetto di entropia

1 Laboratorio