

Corso formazione ReteIDRA

Savona 23/2 – 30/4 2010
corso base

Alessandro Dentella



Lezione N. 2

- Differenza interfacce grafiche/interfacce carattere: vantaggi/svantaggi
- Connessione da remoto via ssh
- Netkit & virtualbox
- Mondo microsoft:
 - Condivisioni (share)
 - Domini / domain controller
 - Winserver
 - Join



Interfacce grafiche/cli

- Quale è più comoda?
- Perché se l'interfaccia grafica è più intuitiva dovremmo sapere altro?
- I forum preferiscono dare i suggerimenti con interfaccia carattere perché sono molto più sintetici e molto più chiari
- Guardate ad esempio quanto è lunga la **spiegazione** della generazione delle chiavi per immagini e quanto sintetico: `ssh-keygen -t dsa`



strumenti

- Lo strumento principe per fare esperienza con i sistemi operativi sono i software di virtualizzazione, ovvero dei software che simulano l'hardware necessario perché un sistema operativo “creda” di essere su hardware vero. I principali sono:
 - Netkit
 - VirtualBox
 - VmWare



Reti

kit minimo di sopravvivenza



Indirizzi IP

- Gli indirizzi ip funzionalmente hanno una stretta analogia con i numeri telefonici, cambia la forma:

192.168.1.13

335/838.8383

- Avere due numemeri di telefono, rende troppo raggiungibili, problema di sovrapposizione
- Se parlassimo con una persona da un telefono e ci rispondesse da un altro (fisso/cell) avremmo seri problemi!



locale/non locale

- Le telefonate locali sono (forse erano...) quelle con identico prefisso
- Analogamente gli apparati con uguale inizio sono sulla stessa rete locale. Quanti numeri debbano essere uguali lo vedremo la volta prossima:
192.168.1.13
192.168.1.254
- 192.168.2.15??



Anche i pc!

- Analogamente anche i pc se hanno due IP (sulla stessa rete) ma su due interfacce differenti, trovano problemi:
 - Non sanno quale usare
 - Ne scelgono una che può essere differente da quella scelta da voi: blocco!

accesso

Eth0: 192.168.0.4 Eth1: 192.168.0.253 Gw: 192.168.0.254

Raggiungibile: Da ip esterno su porta ssh Password key: SI



gateway

- Cosa hanno in comune, un telefono tradizionale quando staccate il filo ed un telefono cellulare in mezzo al deserto?
- Non sanno come uscire. Gli manca il punto per uscire ed andare nel mondo
- Se non vanno nel mondo il mondo non li raggiunge
- Nelle reti quel collegamento è il gateway

accesso

```
Eth0:          192.168.0.4          Eth1:          192.168.0.253 Gw: 192.168.0.254  
Raggiungibile: Da ip esterno su porta ssh Password key: SI
```



Altro esempio: vpn

- Installiamo una vpn fra la vostra scuola ed il mio ufficio.
- Una VPN (Virtual Private Network), è una rete virtuale nel senso che la connessione non avviene nello strato fisico (ma in un livello superiore della pila di stratificazione dei protocolli... per veri geek)



Cosa serve

- La configurazione
 - La chiave
 - Vanno messe in `/etc/openvpn`
 - Va avviato il servizio
 - Va configurato il firewall
 - `tar xzvf nome_scuola.tgz`
 - `sh ovpn/installa_openvpn.sh`
- e, solo se non lo avevate già fatto:
- `add_key sandro`
 - `add_key -s simone`



Netkit

- Base per i nostri esperimenti sarà netkit, un sistema di virtualizzazione che:
 - Gira su linux (solo!)
 - Parte da una semplice console
 - E` sviluppato dalla università di Roma3
 - Permette configurazioni semplici ma molto efficaci
 - È pacchettizzato da me nel pacchetto isi-netkit
 - Nel sito [RetelSI](#) ci sono alcune pagine dedicate a netkit, a come l'ho pacchettizzato ed a come usarlo

Principio funzionamento netkit

- Netkit viene visto dal kernel come un programma
- Netkit usa un file di configurazione minimale e per farlo partire basta '**lstart**'

```
fw[eth0]=tap,172.16.0.11,172.16.0.254  
fw[model-fs]=idra2.img  
fw[mem]=64
```



```
sandro@bluff: /home/sandro/Archivio/corsi-linux/alcatel/openvpn/netkit-lab
File Modifica Visualizza Terminale Schede Aiuto
sandro@bluff:openvpn $ lstart fw

===== Starting lab =====
Lab directory: /home/sandro/Archivio/corsi-linux/alcatel/openvpn/netkit-labs/openvpn
Version: 1.0
Author: Sandro Dentella
Email: sandro@e-den.it
Web: http://docs.argolinux.org
Description:
openvpn test setup

Starting "fw" with options "-q --eth1 -m lenny --mem=48 --no-log --hostlab=/home/sandro/Archivio/corsi-linux/alcatel/openvpn/netkit-labs/openvpn --hostwd=/home/sandro/Archivio/corsi-linux/alcatel/openvpn/netkit-labs/openvpn"...
Core dump limits :
    soft - 0
    hard - NONE
Checking that ptrace can change system
Checking syscall emulation patch for pt
Checking advanced syscall emulation patch
Checking for tmpfs mount on /dev/shm...
Checking PROT_EXEC mmap in /dev/shm/...
Checking for the skas3 patch in the host
- /proc/mm...not found: No such file
- PTRACE_FAULTINFO...not found
- PTRACE_LDT...not found
UML running in SKAS0 mode

The lab has been started.

sandro@bluff:openvpn $

fw
File Modifica Visualizza Terminale Schede Aiuto
Lab directory (host): /home/sandro/Archivio/corsi-linux/alcatel/openvpn
Version: 1.0
Author: Sandro Dentella
Email: sandro@e-den.it
Web: http://docs.argolinux.org/
Description:
openvpn test setup

#####

--- Netkit phase 2 initialization terminated ---

fw login: root (automatic login)
Linux fw 2.6.22.5-netkit-K2.5 #1 Thu Jan 10 13:16:36 CET 2010

The programs included with the Debian GNU/Linux system are
distributed under various free software licenses; their
the exact distribution terms for each program are described
in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
extent permitted by applicable law.
fw:~#
```

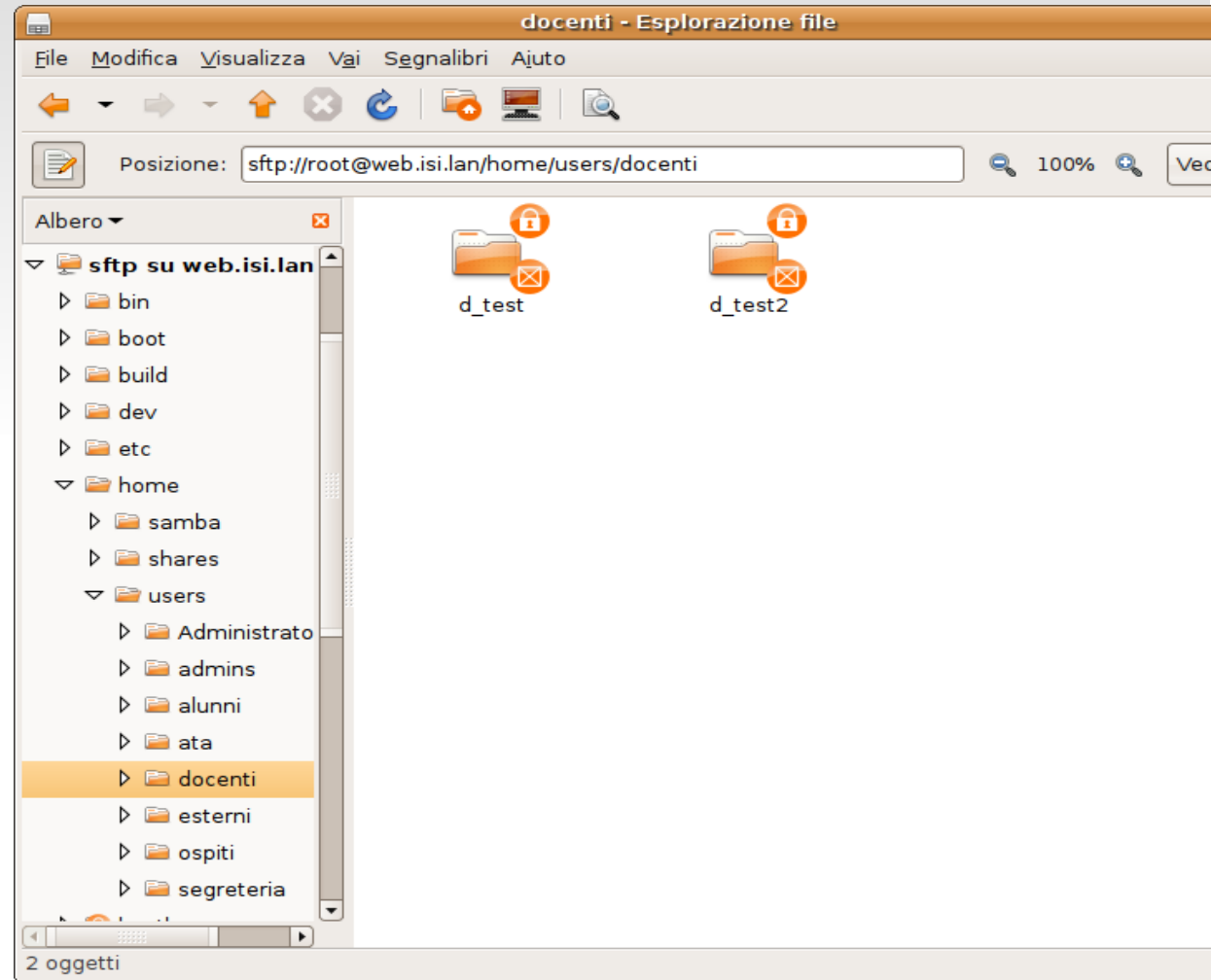


Connessione ssh

- Ci conatteremo alla macchina virtuale con ssh:
`ssh root@172.16.0.11`
- Ci viene chiesta una password, possiamo impostarla dalla console con il comando `passwd`
- A questo punto siamo l'utente **root** sul server

nautilus

- Se ci interessa solo vedere file ed eventualmente editarne qualcuno possiamo usare nautilus



modifiche

- Possiamo fare tutte le modifiche che vogliamo, aggiungere utenti, cancellare file, provare a configurare servizi. Quando abbiamo finito, possiamo uscire con
 - **halt** (sul server virtuale): ogni modifica verrà salvata in un file
 - **lcrash** (sulla macchina principale): le modifiche verranno cancellate e ripartendo avremo nuovamente una macchina “pulita”

Pro & contro

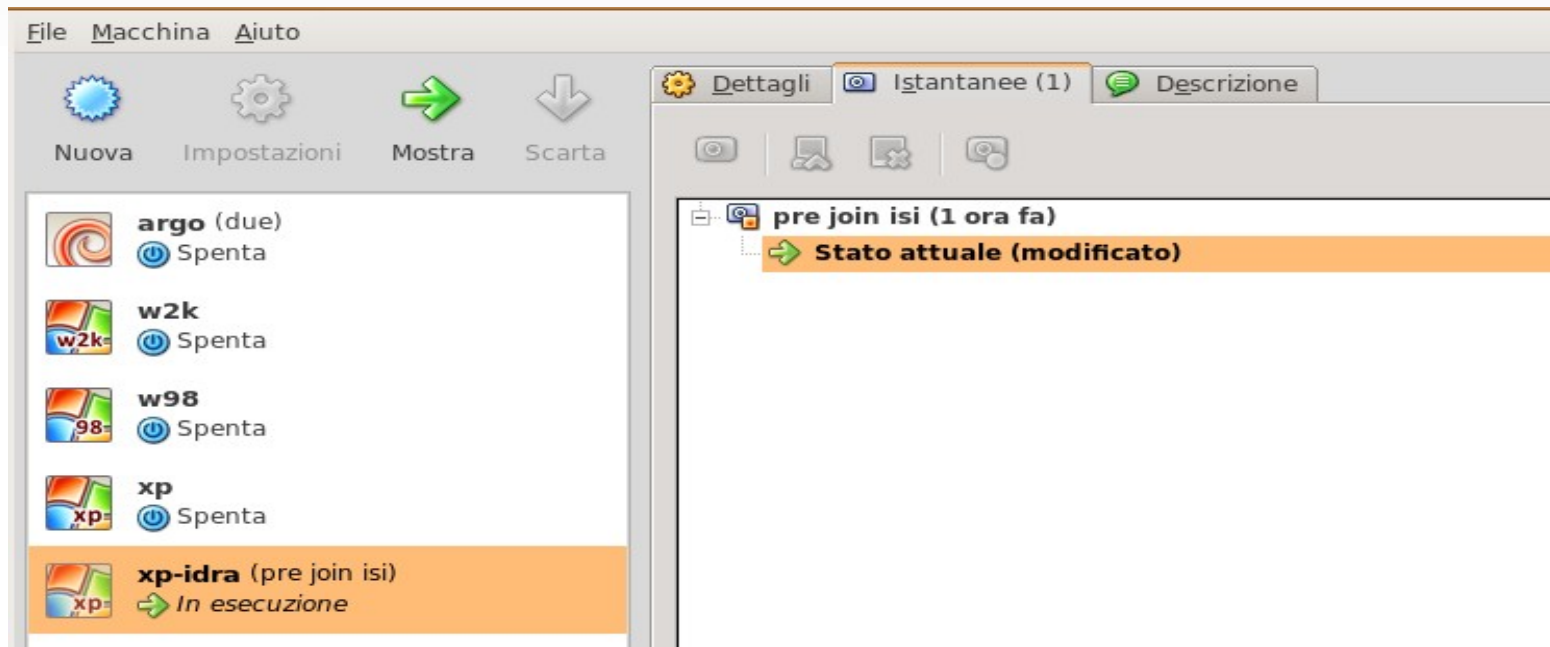
- Netkit è un **ottimo** strumento che permette cose che altri sistemi di virtualizzazione non permettono
- E` leggero
- Ripartire è particolarmente semplice
- (Le reti possono essere configurate dall'esterno)
- Una configurazione di un laboratorio è veramente piccola
- ... ma è limitato a Linux

virtualbox

- Virtualbox è un software di virtualizzazione che offre invece la possibilità di fare girare anche altri sistemi operativi
- Ha una struttura client/server (recente acquisizione)
- Ha una interfaccia grafica per gestire le macchine
- E` un prodotto Sun Microsystem (gli stessi di Openoffice, Oracle, Mysql...) con una versione completamente libera ed una per uso personale ed una per uso commerciale

Virtualbox & fat client

- Purtroppo virtualbox non gira sui fat client che usiamo noi...
- ... facciamo comunque una prova...



Domini microsoft



Savona -2010

dominio

- Il dominio è un sistema di utenti e computer che “vivono” in un sistema di relazioni “sicure” nel senso che tutti sono stati autorizzati da un ente fidato
- Questo ente che autorizza funziona da certificatore sia degli utenti che delle macchine

join

- Certifica gli utenti creandoli e dandogli una password
- Certifica le macchine scambiando con loro delle chiavi in modo che ogni successivo contatto avvenga crittato: questa operazione si chiama “**join**”, ed è autorizzata dal dominus supremo: l'**administrator** (che può avere anche un altro nome). In realtà è solo una persona che appartiene ad un gruppo particolare.

implicazioni

- Questo significa che se portate il vostro portatile a scuola e volete guardare la **vostra** cartella, dovete sincerarvi di essere autorizzati
- Questo assicura che se uno studente porta il proprio portatile a scuola, o il proprio iphone, non avrà lo stesso privilegio di un pc della scuola

Join al PDC

- Creazione di un legame fra Client e PDC
- Una volta creato un join client e PDC si possono scambiare le password in modo che non possano essere lette da altri
- Non possibile/necessario per Windows 98
- Quindi come fanno?
... lo simulano senza crittazione e senza “fiducia”
- XP home? Non lo permette (meno che Win98)

PDC: primary domain controller

- Fornisce l'autenticazione
- Fornisce condivisioni/servizi
- Fornisce logon.bat da eseguire al logon

problemi

- Il join può fallire per vari motivi, raramente Windows vi darà suggerimenti utili. Ad esempio:
“Le credenziali sono incompatibili con altre”
Significa che siete già loggati sul server di dominio (ad esempio avete sfogliato la rete e dato una password) e windows si rifiuta di joinarsi.

Non esiste un server di dominio

- Probabilmente avete dimenticato di configurare la rete o di passare un wins server
- Per evitare questa dimenticanza è sempre meglio fare in modo che il dhcp sever passi anche il wins server

Profilo

- Il profilo è l'insieme di informazioni dell'utente che sono destinate a “seguirlo”: configurazioni di programmi (es.: posta elettronica), impostazioni web, segnalibri...
- Vengono tenute nella macchina Windows fino a che l'utente si scollega ed a quel punto copiate sul server. E` necessario che l'utente abbia i permessi adeguati
- Anche il desktop fa parte di questi
- La cartella *Documenti* no

Problemi con le dimensioni

- Proprio per il fatto che sono file che vengono spostati ogni volta è importante che il profilo venga tenuto contenuto di dimensioni:
 - MAI lasciare file sul desktop (link va bene perché sono leggeri)
 - Mai lasciare la posta nel profilo (si preferisca la posta via web o programmi come thunderbird)

Logon

- script che il server PDC passa al client al momento del LOGON
- Retelsi usa questa script per impostare il profilo dell'utente e per agganciare condivisioni al client a seconda del gruppo principale
- Informazioni come il proxy da usare vengono impostate in questo momento
- Nel logon.conf possiamo dire quali condivisioni connettere

share

- Nel logon vengono connesse le unità di rete decise in logon.conf: queste unità devono però essere già esistenti in samba
- Una share di samba ha:
 - Un nome
 - Un path (dove è situata)
 - Eventualmente delle limitazioni all'accesso

Viste differenti

- L' interfaccia web permette di definire viste differenti a seconda degli utenti