Esercitazioni pratiche di Sicurezza informatica

Laboratorio del corso "Sicurezza dei sistemi informatici" (01GSD)
Politecnico di Torino – AA 2010/11
Prof. Antonio Lioy

preparata da:
Cataldo Basile (cataldo.basile@polito.it)
Andrea Atzeni (shocked@polito.it)

v. 0.8 (13/12/2010)

1 L'ambiente di lavoro

L'esercitazione si svolge usando la distribuzione Linux live GRML versione 2010.04 (codename: Grmlmonster). Potete scaricare l'immagine ISO:

1. dal sito ufficiale `http://grml.org/`
2. dal sito del corso `security.polito.it/~lioy/01gsd/`

Al boot di GRML vi apparirà una schermata simile a quella in Figura 1.

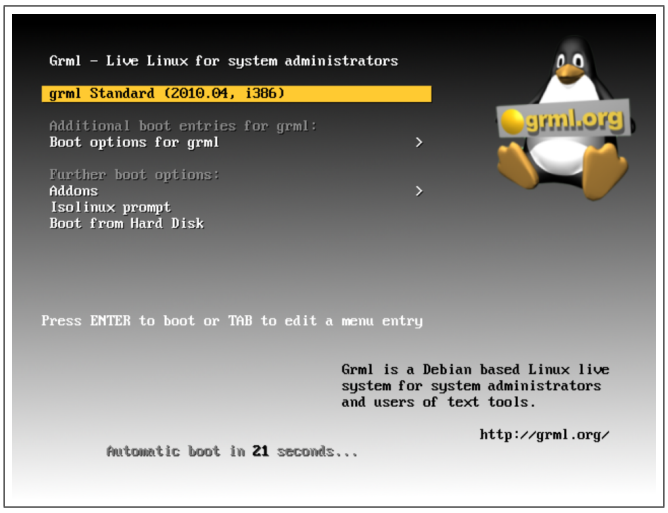

Figura 1: Schermata iniziale di GRML 2010.04 (Grmlmonster)

Scegliete "grml Standard (2010, 04 i386)" per avviare il sistema operativo. Se usate GRML da macchine fisiche (con CDROM fisico), potete caricare l'intera immagine in RAM. Scegliete "Boot options for grml" o successivamente "grml - Load to RAM". Questo eviterà gli snervanti ritardi dovuti al tempo di accesso del CDROM fisico e vi permetterà di rimuovere il CDROM dal drive (ad esempio per condividerlo con altri in laboratorio). Ma attenzione, servirà molta RAM (690 MB in più).

Per configurare la tastiera italiana potete usare i comandi:

- `loadkeys it` (in console);
- `setxkbmap it` (in modalità grafica).

In alternativa potete scegliere al boot l'opzione Isolinux prompt e digitare

```
grml grml-lang = it
```

(il trattino - sulla tastiera italiana corrisponde all'apostrofo ' e l'uguale = corrisponde alla ì).

Al termine della fase di boot, GRML 2010.04 presenterà un menù che permette di svolgere rapidamente le operazioni comuni, ad esempio, configurare la rete e far partire l'ambiente grafico.

Per configurare la rete in laboratorio, digitate il tasto `e`. Vi apparirà una finestra testuale (`netcardconfig`), scegliete "Use DHCP broadcast" e scegliete "No" quando verrà chiesto di abilitarlo in automatico agli avvii successivi.

Per avviare rapidamente il server grafico X digitate prima il tasto `x`, poi `f`, per selezionare il gestore di finestre FluxBox. In alternativa, da console, potete avviare il server X con:

```
grml-x -mode 1024x768 fluxbox
```

Per riavviare il menu testuale usate il comando "`grml-quickconfig`".

L'ambiente di lavoro apparirà come in Figura 2.

Figura 2: Ambiente di lavoro GRML

Si ricorda di seguito la sintassi di alcuni comandi utili durante lo svolgimento delle esercitazioni (nota: le parentesi quadre racchiudono qualcosa di opzionale, le parentesi graffe racchiudono una scelta, le parole in italico sono un segnaposto da sostituire con un dato appropriato).

- per cambiare utente, in particolare per diventare `root`:

  `su [- `*`username`*` ]`

  dove se non specificate *username* si assume `root`

- per ottenere informazioni sull'uso di un comando/programma:

  `man `*`program_name`*

- per avviare/fermare/riavviare servizi:

  `/etc/init.d/`*`servicename`*` { start | stop | restart }`

- per conoscere la configurazione di rete della vostra macchina (indirizzo IP, netmask, ...):

  `ifconfig`

2 Riprodurre l'ambiente di laboratorio a casa ...

Gli esercizi che vi proporremo richiedono al massimo l'uso di tre PC contemporaneamente e nelle prossime sezioni descriveremo come riprodurre a casa un ambiente molto simile a quello di laboratorio.

2.1 ...con macchine fisiche

Se avete a disposizione tre PC, potete collegarli in rete fra loro con uno switch, come mostrato in Figura 3. La connessione ad Internet non è necessaria per gli esercizi, ma può essere utile per reperire il materiale necessario e documentazione di approfondimento.

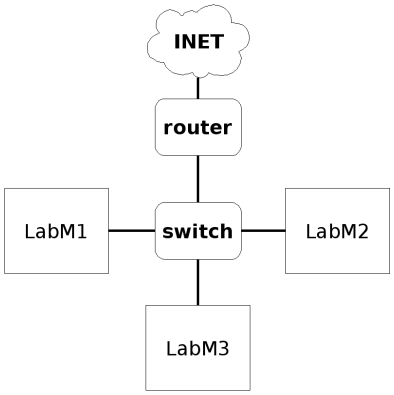

Figura 3: Topologia di rete domestica

Nel caso non abbiate un server DHCP che assegna automaticamente gli indirizzi IP alle macchine, dovrete specificare la configurazione manualmente (riferitevi alla pagina di manuale di `ifconfig` per maggiori dettagli).

Potete anche realizzare una rete WiFi (il router ADSL fa sia da switch che da router), ma prestate attenzione perché alcuni driver di schede di rete wireless hanno delle limitazioni (per cattura e inserimento di pacchetti) che potrebbero compromettere l'esito di alcuni specifici esercizi (i problemi noti sono segnalati nel testo dell'esercizio). Queste limitazioni sono tipicamente risolvibili usando una diversa versione del driver o configurandolo opportunamente.

2.2 ...con la virtualizzazione

Potete usare la virtualizzazione come strumento per avere a disposizione una o più copie di GRML funzionanti contemporaneamente su un'unica macchina fisica. La soluzione che adottiamo richiede di usare l'immagine ISO di GRML come CD-ROM virtuale per le macchine che andremo a creare: dovete quindi avere una copia locale del file `grml2010.04.iso`.

Ma attenzione, come per le reti WiFi, anche la virtualizzazione, che emula in software il comportamento di dispositivi di rete, potrebbe compromettere l'esito di alcuni esercizi (anche in questo caso, i rarissimi problemi sono segnalati nel testo dell'esercizio).

2.2.1 VMware Server Server

Nel seguito descriviamo come utilizzare VMware Server, un prodotto di virtualizzazione gratuito disponibile per piattaforma Linux e Windows. La versione a cui facciamo riferimento in questo documento è la 2.0.2. Potete scaricarla alla URL `https://www.vmware.com/products/server/`. Prima di procedere con l'installazione, dovete registrarvi per ottenere un numero di serie.

Fate riferimento alla documentazione presente in rete "VMware Server User's Guide – VMware Server 2.0" disponibile al seguente link `http://www.vmware.com/support/pubs/server_pubs.html`, per informazioni sull'installazione guardate il Capitolo 2 della guida, "Installing VMware Server".

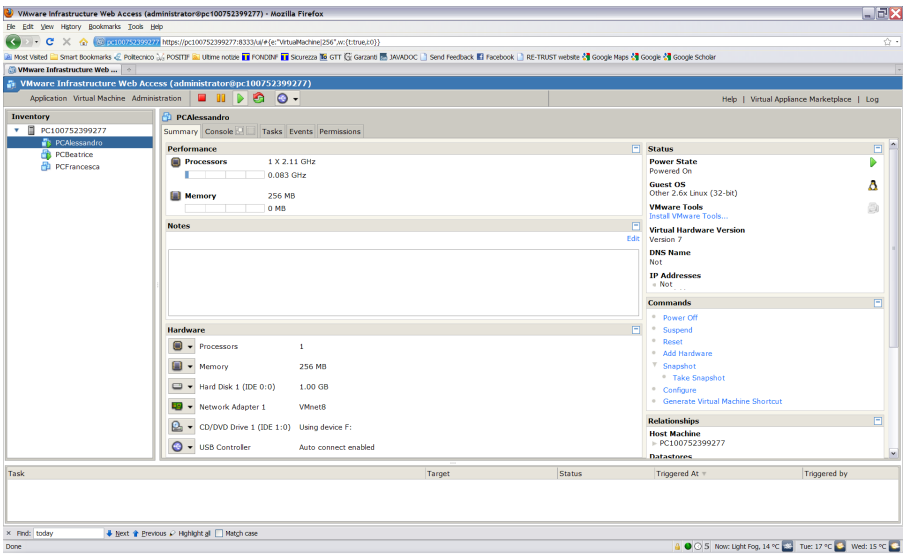

Figura 4: Pagina principale di VMware Server

Dalla versione 2.0, VMware Server non è più un programma stand alone ma un web service disponibile (tramite Apache Tomcat) sia da localhost che da remoto.

Assumiamo ora che abbiate VMware Server funzionante, è necessario creare le macchine virtuali.

Lanciate la VMware Server Home Page (per ulteriori istruzioni guardate il capitolo 3 della guida VMware Server). La finestra dovrebbe apparire come in Figura 4, selezionate dal menù:
`Virtual Machine` > `Create Virtual Machine`.

Apparirà una finestra con un wizard:

1. inserite il nome della VM, poi `Next` (nelle esericitazioni i tre partecipanti saranno chiamati Alessandro, Beatrice, Claudio, per comodità potete chiamare le VM `PCAlessandro`, `PCBeatrice`, `PCClaudio`);
2. selezionate il sistema operativo `Linux Operating`, versione `Other 2.6x (32-bit)` e procedete;
3. selezionate la RAM (256MB dovrebbero essere sufficienti) ed i processori/core da mettere a disposizione alla VM (un core è di solito più che sufficiente), poi cliccate su `Next`;
4. dovete scegliere le impostazioni relative al disco virtuale cliccando su `Create New Virtual`; visto che al termine del processo elimineremo il disco, specificate un valore basso (ad esempio 1GB), lasciate la "location" standard;
5. cliccate su `Virtual Device Mode` e selezionate un `Adapter` di tipo `IDE0` (sono occasionalmente stati rilevati dei problemi con i device SCSI usando GRML), poi cliccate su `Next`;
6. cliccate su `Add Network` per aggiungere una rete locale; nelle esercitazioni di laboratorio va sempre bene selezionare `Network Connection` di tipo `NAT` (talvolta indicata come `VMnet8`); per configurazioni più complesse fare riferimento al capitolo 11 della guida VMware Server;
7. scegliete il CD/DVD cliccando su `Use Phisycal Drive`, per evitare conflitti di accesso noi abbiamo creato dei dispositivi virtuali (es. con DAEMON Toolsdisponibile presso `http://www.daemon-tools.cc/eng/downloads`) ed abbiamo associato un drive virtuale ad ogni VM, in ogni caso associare più VM allo stesso drive non dovrebbe creare problemi;
8. cliccate su `Don't add a floppy`;
9. cliccate su `Add a USB Controller` se avete intenzione di usare una chiavetta USB (es. per passare i dati tra PC fisico e macchine virtuali, anche se noi abbiamo preferito SSH);
10. cliccando nella finestra di riepilogo su `Finish` comparirà una nuova macchina virtuale.

La configurazione di rete che abbiamo consigliato permette alle macchine di dialogare tra loro attraverso uno switch virtuale e di uscire all'esterno via Network Address Translation (NAT).

Prima di avviare una macchina virtuale, ricordate di inserire nel drive CD/DVD fisico il CDROM di GRML oppure di "montare" l'immagine ISO di GRML tramite il gestore di virtual drive. Notate che, visto che l'immagine ISO di GRML viete utilizzata in read-only, potete condividerla tra tutte le macchine, senza necessità di sprecare spazio su disco (ma, come spiegato in precedenza, conviene montarla su dispositivi virtuali differenti).

La prima volta che avviate una macchina virtuale dovete cambiare la sequenza di boot per far partire GRML da CDROM:

1. nel frame `Inventory` di "VMware Infrastructure Web Access" avete la lista di tutte le macchine virtuali, cliccate su quella che volete far partire;
2. nel frame `Commands` (a destra) scegliete `Configure VM`;
3. selezionate la checkbox "Enter the BIOS setup screen the next time this virtual machine boots";

Per avviare una VM:

1. nel frame (`Inventory`) di "VMware Infrastructure Web Access" avete la lista di tutte le macchine virtuali, cliccate su quella che volete far partire;
2. cliccate e scegliete `Power` dal frame `Commands` o premete il tasto verde in alto (col simbolo "Play");
3. cliccate sul tab `Console` (la prima volta vi chiederà di scaricare un plug in);
4. cliccate su un punto qualsiasi e la VM partirà in una nuova finestra. La prima volta che avviate la VM vi apparirà il menu del BIOS, impostate come primo dispositivo nella sequenza di boot il CDROM (usando i tasti "+" e "-").

Ripetendo più volte lo stesso procedimento, potete creare repliche di GRML (l'unico limite, è a questo punto la vostra RAM).

2.2.2 Oracle VM VirtualBox

Una valida alternativa a VMware Server è VirtualBox, ha meno opzioni di configurazione e non supporta la gestione delle macchine virtuali da remoto, ma sicuramente molto più leggero dal punto di vista computazionale. Vi consigliamo anche di installare su ogni macchina virtuale le "Guest Addition", disponibili come .iso nella cartella di installazione di Virtual Box. Informazioni più dettagliate sulle "Guest Addition" sono disponibili al seguente lnk (`http://www.virtualbox.org/manual/ch04.html`).

La procedura per la creazione di una nuova macchina virtuale è analoga a quella di VMware Server.

Scegliendo il pulsante "`New`" si fa partire la procedura di creazione di una nuova Virtual Machine guidatache consiste nelle seguenti fasi (per i valori fate riferimento alla sezione 2.2):

- scelta del nome e del tipo di sistema operativo
- scelta della dimensione della RAM
- scelta dell'Hard Disk, deselezionate "`Boot Hard Disk`" e continuate (imposteremo in seguito il boot da CDROM)

Selezionando la macchina virtuale appena creata ed in seguito il pulsante "`Settings`" è possibile aggiungere un CD/DVD e creare un Hard disk virtuale:

- selezionate "`Storage`" (comparirà una finestra come quella in figura 5);
- selezionate il drive IDE "`Empty`" ed aggiungete un'immagine cliccando nel frame "`Attributes`" sul tasto "`Open Virtual Media Manager`"

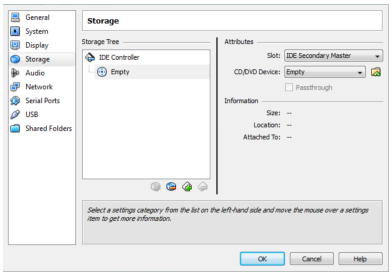

Figura 5: Topologia di rete domestica

- aggiungete una nuova immagine cliccando su "`Add`" e selezionando sul vostro Hard Disk il file iso di GRML
- cliccate con il tasto destro su "`IDE controller`", scegliete "`Add CD/DVD device`" e ripetete la stessa procedura per aggiungere la .iso delle "Guest Addition"
- cliccate sul tasto "`Add Controller`" e aggiungete un "SATA Controller"
- aggiungete un Hard Disk cliccando su add Hard Drive (tasto a destra della scritta SATA Controller) e seguite la procedura guidata per creare un nuovo Hard Disk virtuale (è consigliabile un `Dynamically expanding storage`).