Percorso 5:
- Log/Troubleshoooting

Bartolomeo Montrucchio
bartolomeo.montrucchio@polito.it

Giovanni Squillero
giovanni.squillero@polito.it

Logging

- I file di log sono utilizzabili per cercare informazioni
  - sicurezza
  - configurazione
  - correzione errori/troubleshooting
- head, tail –f
- grep può essere usato per cercare nei file
- /bin/dmesg
- /var/log è la directory più importante

dmesg

- /var/log/dmesg
  - Cataloga tutti i messaggi provenienti dal kernel
  - Si può usare il comando dmesg per vederli
  - In questo file sono visibili numerose informazioni di basso livello sull'hardware

boot, kern, cron

- boot.log contiene dati relativi alla fase di boot
- kern.log è utile per verificare la configurazione del kernel
- Eventuali job basati su cron producono output su syslog

Logging degli account

- last
  - /var/log/wtmp
- lastlog
  - /var/log/lastlog
- faillog
  - /var/log/faillog
- who
  - /var/log/wtmp

Logging

- last -f /var/log/btmp per gli ultimi login falliti
  - /var/log/btmp
  - Solo per root
- /var/log/mail.log
  - Per il mail server
- /var/log/alternatives.log
  - Per le installazioni
- /var/log/cups
  - Per la gestione delle stampanti

X11

- /var/log/Xorg.0.log contiene informazioni per la grafica (disgiunta sotto Unix dal resto)
- /etc/X11/org.conf
- Normalmente non serve in quanto il riconoscimento della scheda grafica è automatico
- Il comando X -configure produce un file di configurazione
- Potrebbe ancora servire per monitor particolari (a tubo catodico o con frequenze particolari)

rsyslogd

- /var/log/syslog
  - messages è stato sostituito da syslog
  - si noti che ad esempio in OpenBSD è differente
- Viene utilizzato rsyslogd
- service rsyslog start
- /etc/rsyslog.conf

Rotazione dei log

- logrotate
- /etc/logrotate.conf
- Cron
  - crontab -e
- Esempio di configurazione di cron

Esercizio

- Analizzare i principali file di log
  - In fase di reboot
- Cosa succede a livello di log inserendo una chiavetta?
- Cosa succede a livello di macchina virtuale?

Installazione programmi da sorgente

- Leggere il README file e/o altri file di supporto
- **xmkmf -a**, oppure gli script INSTALL o ./configure
- Verificare che il Makefile sia corretto.
- Se necessario, lanciare **make clean**, **make Makefiles**, **make includes** e **make depend**.
- **make** (ad es. make –j 4 usa 4 thread, utile per il kernel)
- Controllare i permessi dei file generati.
- Se necessario, lanciare **make install**
- effettuare shutdown/reboot non è richiesto

Esercizio

- Scaricare nmap in formato sorgente
- Seguendo le istruzioni, compilarlo in locale (non come root)
- Infine installarlo come root
- Risolvere eventuali problemi

Bibliografia

- https://wiki.ubuntu.com/
- http://www.x.org/wiki/