Taller de Administración de Servidores Linux

CC5308

Clase 16: 14 de abril de 2011

Hardening, Arquitecturas, Réplicas

@chidalgo
chidalgo [at] nic . cl

Hardening

¿Es UNIX/Linux seguro?

Hardening

- Seguridad <> Diversión, Conveniencia
- MundoReal™
  - Ataques externos
  - Ataques internos
    - Usted confía ciegamente en sus empleados?
  - Sistemas EXTREMADAMENTE complejos
    - P(falla) = 1

Hardening

- Cómo nos atacan?
  - InJenieria Social

```
<Cthon98> hey, if you type in your pw, it will show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
```

  - Vulnerabilidades en el Software
  - Errores de Configuración

Hardening

- “Fortaleciendo” el sistema:
  - Buenos passwords
  - PAM et al
  - Proceso contínuo de software
    - Actualizaciones del sistema
    - Actualizaciones de distribución
    - Desarrollo contínuo de software
  - Usar servicios 'seguros' (SSH)

Hardening

- “Fortaleciendo” el sistema:
  - Desabilitar servicios innecesarios
    - *chkconfig –list*
    - *chkconfig <service_name> off*
    - *service –status-all*
    - *update-rc.d <service_name> remove*
  - *Desinstalar Software*
  - *Desabilitar binarios SUID / SGID*
    - *find / \(-perm -4000 -o -perm -2000 \) -print*

Hardening

- “Fortaleciendo” el sistema:
  - Establecer límites
    - *quota*(1)
      - *edquota -u <username>*
      - *edquota -g <group>*
      - Archivos *aquota.user*, *aquota.group* en raiz del filesystem
    - *chattr*(1) / *lsattr*(1)
    - SELinux, AppArmor, Grsecurity
      - OjO

Hardening

- “Fortaleciendo” el sistema:
  - limits.conf(5)
    - 'Fork Bombs' (Wikipedia)
      - :(){ :|:& };:
    - /etc/security/limits.conf
    - /etc/security/*.conf

```
*               soft    core            0
root            hard    core            100000
*               hard    rss             10000
@student        hard    nproc           20
@faculty        soft    nproc           20
@faculty        hard    nproc           50
ftp             hard    nproc           0
@student        -       maxlogins       4
```

Hardening

- “Fortaleciendo” el sistema:
  - Parámetros del kernel
    - *sysctl*(8)
    - /etc/sysctl.conf
    - Ejemplos:
      - net.ipv4.tcp_syncookies
      - net.ipv6.conf.all.forwarding
      - net.ipv4.ip_forward
      - … y muchos más!

Hardening

- Hay MUCHO que hacer y mirar para fortalecer un sistema
  - A veces, demasiado
    - Criterio
    - Automatización
  - Dónde más mirar?
    - http://wiki.debian.org/Hardening
    - Linux Hardening HOWTO
    - NSA Guide
    - Guias de CERTs

Replicación & HA

- Conceptos Genéricos
  - Master
  - Slave
  - Hot Spare/Hot Standby
  - Balanceadores de carga
  - Backups
  - HA
  - Failover
  - Watchdog

Replicación & HA

- Topologias
  - Master – Slave
  - Master – Master
  - Master – Master (Activo/Pasivo)
  - Multimaster – Slave
  - Master – Master con esclavos
  - Anillo (Masters)
  - Master + Distribuidor + Esclavos
  - Árbol

Replicación & HA

- Sharding
  - Particionamiento horizontal
    - En bases de datos, conjunto de filas en distintas particiones
  - Ventajas:
    - Reduce tamaño de índice
    - Distinto hardware
      - Redundancia, HA
    - Performance

Replicación & HA

- En el caso de motores de DB...
  - MySQL
    - Binary log
    - Reply queries
    - 5.1: row-based replication
  - PostgreSQL
    - Log shipping
    - Streaming replication
    - Procedimientos almacenados

Actividad Personal

- Hardening:
  - Revisar los límites del sistema donde estén trabajando, via quota, ulimit, revisando /etc/security/*.conf
  - Revisar servicios activos:
    - Cuáles sirven? Cuáles no? Por qué?
- Replicación:
  - Construir 2 instancias de MySQL, crear una base de datos en ella, y probar la replicación Master-Slave (Guía)