Taller de Administración de Servidores Linux

CC5308

Clase 5: 18 de marzo de 2011

Control de Acceso

Luis León Cárdenas Graide
lcardena [at] dcc . uchile . cl

Copyright © 2011
Creative Commons 3.0-cl by-nc-sa

Login Shell

- login(1)
- chsh: /etc/passwd
- bash { -l | --login } || "$0" = '-'
  - /etc/profile
    - /etc/profile.d/*.sh
    - ¿Interactiva? bash [-i | -c]
      - /etc/bash.bashrc: chroot, sudo, command-not-found
  - ~/.bash_profile, ~/.bash_login || ~/.profile
  - --noprofile
  - --norc: /etc/bash.bashrc, ~/.bashrc
  - man bash: INVOCATION, FILES

Acceso Default

- Usuario:Password "admin:admin"
  - Dispositivos: Routers, Webcams, Impresoras, Teléfonos
  - Servicios: Web, Base Datos, Correo, Proxy, Aplicación
  - Aplicaciones
- Configuración default: insegura
- Documentarse, conocer, ajustar, asegurar
- Hardening (mismo curso, mismo canal)

Gestión de Usuarios

- Linux: Familia useradd (ya visto)
  - Usuarios personales vs de sistema
    - Servicios no root
- VPN (cliente): openvpn
  - Simula red local cifrando a través de red pública
  - Servidor VPN: host y puerto
  - Interfaz virtual + IP "local" + rutas
    - ¿Soporte Router/Gateway?
  - Identificación y autentificación
    - Password, certificados, passphrase
  - DNS institucional vs ISP

Login nulo

- chsh -s /bin/false
  - /etc/shells
  - /etc/login.defs
- chfn
- PAM: Pluggable Authentication Modules for Linux
  - /etc/pam.conf, /etc/pam.d/*
  - Múltiples formas de autenticación
  - Cascada de subsistemas
  - Obligatorio, Opcional, Requisito, Suficiencia
  - Acción en base a éxito/fracaso

SSH: Secure Shell (client)

- Telnet puerto 22
- Password
- ssh-keygen
- ~/.ssh (permisos)
  - id_rsa, id_rsa.pub
  - authorized_keys
  - config
- ssh-agent, ssh-add
- /etc/ssh/ssh_config
- ssh -X -C -2 -o ...

SSHd: Secure Shell Daemon

- /etc/ssh/ssh{d_config,_host_[dr]sa_key{,.pub}}
  - Port, ListenAddress, Protocol, HostKey, UsePrivilegeSeparation
  - SyslogFacility, LogLevel, LoginGraceTime
  - PermitRootLogin, StrictModes, {Deny,Allow} {Users,Groups}
  - RSAAuthentication, PubkeyAuthentication, AuthorizedKeysFile
  - PermitEmptyPasswords, {ChallengeResponse, Password}Authentication
  - X11Forwarding, PrintLastLog, TCPKeepAlive, UseLogin
  - Subsystem, UsePAM, UseDNS

Restricted* Shell

- * Restringido != Seguro
- rbash, bash { -r | --restricted }
  - man bash: RESTRICTED SHELL
- rssh: Restricted Login shell sobre SSH
  - Restringida a subsistemas
  - scp, sftp, cvs, svn, rsync, rdist, svnserve
  - chroot

LDAPv3

- Lightweight Directory Access **Protocol**
- Múltiples métodos de autenticación
- Single Sign On
  - Cookie: Autenticación ante varios sistemas
- Directorio = Árbol
  - Jerarquía: Usuarios / Roles, Geografía, Políticos
  - Directorio := Entradas*
  - Entrada := {Attributos}
  - Atributo := Nombre [= Valor] (Esquema)
- URL: ldap://host:port/DN?attributes?scope?filter?extensions

Actividad Personal

- Configurar SSHd con llaves
  - Crear llaves
  - Configurar Agente SSH en startup de X
  - Usar con authorized_keys en otras máquinas
  - Backup de llaves
  - Cerrar password
- Dar acceso rssh a nuevo usuario
  - Cambiar a login nulo
- Conectarse a VPN de facultad "a mano"
  - Tiempo Libre: ver n2n (VPN P2P)