Администрирование Linux
Лекция 8
Аутентификация LDAP

Иртегов Д.В.

Новосибирский гос. Университет

2014

Зачем нужен LDAP

- Много пользователей
- Много серверов
- Заводить каждого пользователя на каждом сервере - безумие
  - Корпоративные сети
  - Терминальные классы
  - Кластеры
  - Разделяемый хостинг

Подробнее про БД учетных записей Linux

- PAM и NSS
- PAM – Pluggable Authentication Module
  - Набор библиотек для аутентификации пользователей
- Name Service Switch
  - Обеспечивает сопоставление имен и номеров
    - Пользователей и групп
    - Сервисов (портов TCP и UDP)
    - Хостов и IP адресов
    - И т.д.

Источники информации для PAM и NSS

- Files
  - passwd, shadow, group – Пользователи
  - hosts – Хосты, IP адреса
  - services – порты TCP и UDP
- NIS/NIS+ - изучать не будем
- Winbindd – аутентификация в домене Windows – тоже изучать не будем
- LDAP
- sssd (RHeL/Centos 6)

LDAP

- Lightweight Directory Access Protocol
- Разработан на основе OSI/ISO x500 (ITU-T DAP)
- Иерархическая база данных
  - Контейнеры
  - Объекты
  - Атрибуты
- Схема LDAP
  - Список типов объектов и атрибутов

Основные применения LDAP

- БД учетных записей Unix
- БД учетных записей Samba
- Аутентификация http
- Аутентификация
  - 801.1x (WPA Enterprise),
  - PPP/PPPoE,
  - RADIUS
- Почтовые адресные книги
- Справочные системы

Реализации серверов LDAP

- Microsoft Active Directory
- OpenLDAP (slapd)
- Novell eDirectory (NDS)
- Lotus Domino
- Apache Directory Server
- …

Демонстрация

- Дамп базы 389ds в формате LDIF
- Иерархия объектов в базе 389ds при помощи 389-console

Использование LDAP для аутентификации Unix

- Необходимые типы объектов
  - Пользователь
  - Группа
- Атрибуты пользователя
  - Uid
  - Хэш пароля
  - Gid
  - Username
  - Shell
  - Homedir
- OpenLDAP: NIS scheme
- MS AD: Microsoft Services for Unix

Терминология LDAP

- Bind – привязка (логин)
  - Необходимо указать имя объекта (пользователя)
  - Аутентификация SASL
- Relative Distinguished Name – относительное имя
  - Атрибут=значение
  - cn=Dmitry Irtegov
  - dc=nsu
  - o=Novosibirsk State University
- Distinguished Name (DN) – иерархическое имя
  - Аналог путевого имени файла
  - Уникально идентифицирует объект
  - cn=Dmitry Irtegov,dc=swsoft,dc=nsu,dc=ru

Демонстрация

- Настройка аутентификации LDAP средствами authconfig и sssd
- Необходима настройка TLS

Введение в TLS и PKI

- Transport Level Security
  - Стандартизованная версия Netscape SSL
  - Наиболее известен в виде протокола https
  - Надстройка над TCP, обеспечивающая аутентификацию и шифрование произвольных данных
  - IMAP/TLS, SMTP/TLS, LDAP/TLS, да тыщи их
- Опирается на Public Key Infrastructure
  - Ключи и сертификаты x509

Аутентификация публичным ключом

- Алиса имеет Kpub+Kpriv, публикует Kpub
- Боб генерирует sc, отправляет Алисе.
- Алиса
  - генерирует cr,
  - вычисляет r=S(sc+cr, Kpriv)
  - отправляет r+cr Бобу
- Боб вычисляет S(sc+cr, Kpub)
- Если сошлось, Боб может быть уверен, что Алиса имеет Kpriv

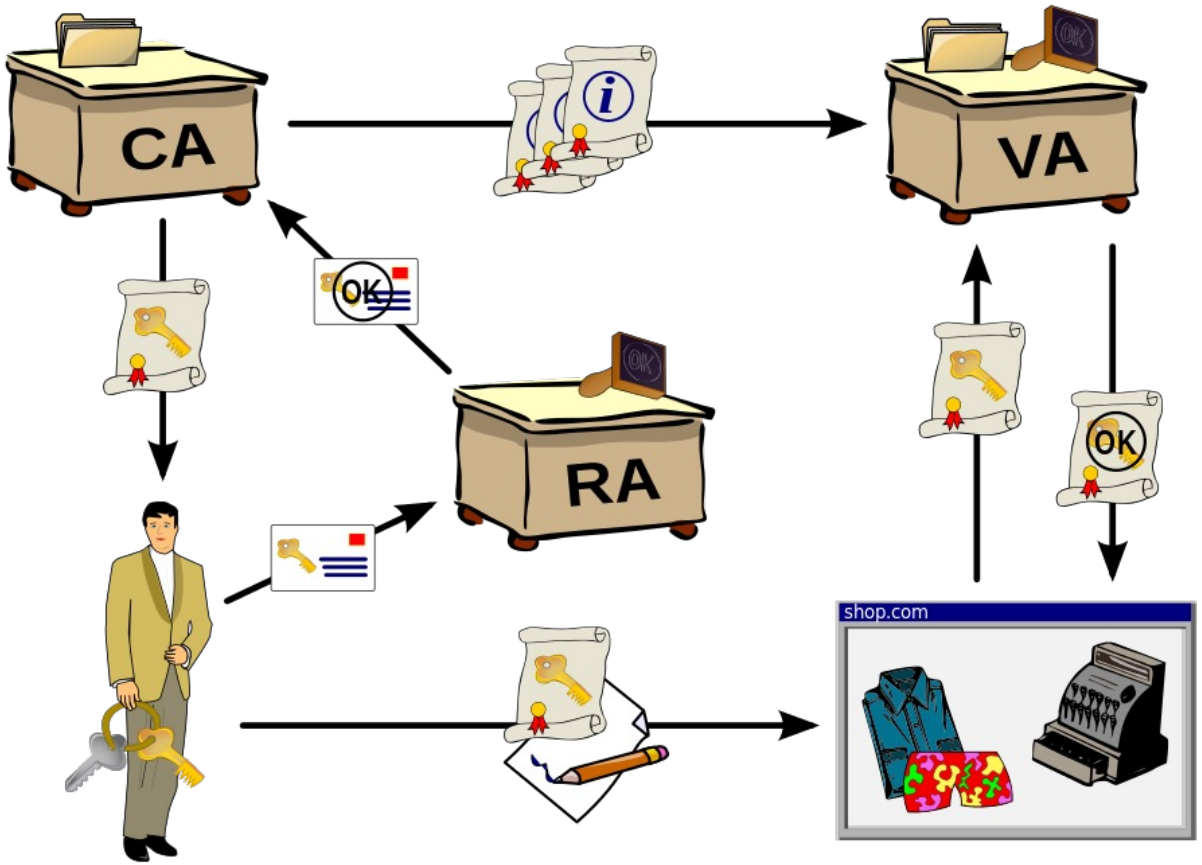
Атака «человек в середине»

- Труди имеет $Kpriv_t$+$Kpub_t$
- Подменяет $Kpub_a$ на $Kpub_t$ (например DNS спуфингом)
- Может выдать себя за Алису

Подписанные публичные ключи

- Алиса и Боб знают Kpub(CA)
- CA заверяет ключ Алисы: вычисляет S(«Алиса»+Kpub(A),Kpub(CA))
- Боб может проверить эту подпись и убедиться, что ключ
  - действительно принадлежит Алисе
  - был заверен CA
- На практике, кроме имени и Kpub(A) в подпись включают дату, время действия и флаги (список операций, для которых пригоден ключ)

PKI



Иерархические CA

- Корневой CA (Verisign) — Kpub(Verisign)
- Подчиненный CA (Thawte)
- Kbub(Thawte)+S(«Thawte»+Kpub(Thawte), Kpub(Verisign))
- Аутентификация Алисы Бобом возможна, если существует такой $CA_а$, которому доверяет Боб и которым (по цепочке) подписан ключ Алисы
- $CA_а$ и $CA_б$ могут быть разными
- Теоретически, возможна сеть доверия вместо иерархии CA

Сертификаты x509

- Содержат
  - публичный ключ
  - имя объекта (для TLS – имя хоста)
  - имя организации
  - срок действия (обычно несколько лет)
  - набор подписей (возможно, иерархических) различными CA

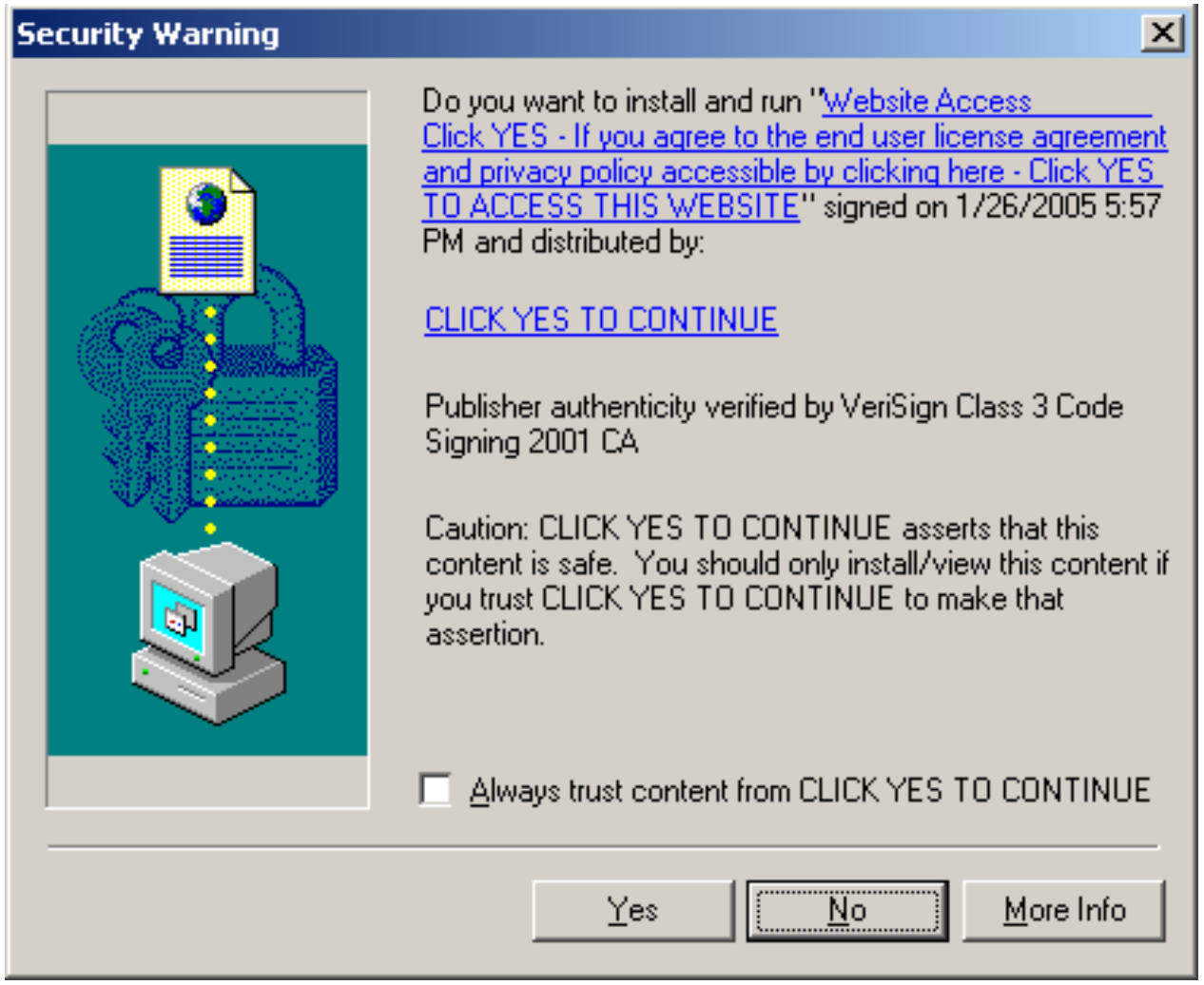
Официальные и самоподписанные CA

- Официальные CA
  - Публичные ключи зашиты в программные продукты (например, в браузер)
  - Проверяют реквизиты организации
  - Выдают ключи только зарегистрированным юрлицам
  - Организация может завести свой CA, подчиненный официальному
- Самоподписанные CA
  - Публичный ключ надо прописывать явным образом
  - Браузеры ругаются и предлагают «создать исключение безопасности»
  - Удобны для тестирования или корпоративных сетей

Демонстрация

- Список публичных ключей, прописанных в Mozilla Firefox и IE
- Подключение Firefox к https серверу с самоподписанным сертификатом

Официальные CA не панацея



SSL/TLS и startTLS

- Шифрованный протокол поверх TCP
  - TLS handshake:
    - согласование версии протокола
    - обмен публичными ключами
    - аутентификация сервера (обязательно)
    - аутентификация клиента (опционально)
    - согласование алгоритма шифрования
    - согласование сессионного ключа и его времени жизни
  - Обычно, шифрованная версия работает на другом порту TCP
    - http – 80, https – 443
    - IMAP – 25, IMAP+TLS – 993
  - startTLS
    - В некоторых прикладных протоколах (SMTP, LDAP) TLS handshake может происходить не с самого начала сессии, а после выдачи клиентом определенной команды

Использование LDAP с TLS

- Настоятельно рекомендуется
  - Авторизация CHAP с использованием хэшей пароля
  - При смене пароля, хэш пароля передается по сети
  - Authconfig GUI не позволит включить LDAP без TLS
- Указать URL ldaps://

Или

- Указать URL ldap:// и включить StartTLS
- В обоих случаях, необходимо выкачать публичный ключ CA сервера
  - Authconfig GUI сам его подложит куда надо

Демонстрация

- Настроечные файлы PAM и SSSD до включения LDAP
- Включение LDAP
- Настроечные файлы PAM и SSSD после включения LDAP
- Вход пользователем LDAP
- Регистрация пользователя при помощи 389-console
- Вход вновь созданным пользователем
- Обратите внимание, что локальные пользователи никуда не делись!!!

Упражнение

- Подключить ваши виртуальные машины к серверу LDAP
  - URL ldap://ws179.swsoft.nsu.ru
  - Search DN “dc=swsoft,dc=nsu,dc=ru”
  - CA key URL http://parallels.nsu.ru/~fat/ca-cert.crt
- Войти пользователем test2, пароль linuxcourse2014

Обзор sssd

- System Security Services Daemon
- Изобретение Red Hat
- Обеспечивает аутентификацию, трансляцию имен в номера и кэширование запросов к соответствующим базам
- Реализован как модуль PAM/NSS, но имеет собственные подключаемые модули и может брать на себя функции других модулей PAM/NSS

Что умеет sssd

- Работу с локальной индексированной БД учетных записей (не путать с /etc/passwd)
- Взаимодействие с NIS, LDAP, Winbindd
- Аутентификацию LDAP, Winbindd, Kerberos
- Кэширование внешних БД, переключение серверов при отказе и работу в оффлайне
- Управление таблицами sudoers (собственная версия sudo), automount, ключами ssh
- Переключение БД учетных записей при помощи authconfig и authconfig GUI
- Унифицированное управление разными источниками БД через /etc/sssd/sssd.conf
  - в PAM/NSS каждый модуль надо настраивать по своему

Демонстрация

- Файл /etc/sssd/sssd.conf

Чего не умеет sssd

- Перечисление пользователей во внешних БД
  - getent passwd выдает только локальных пользователей
  - getent passwd username, id username работает
  - Надо поставить enumerate=true в sssd.conf
    (но у меня почему-то не получилось)
- Создание пользователей во внешних БД
- Сброс пароля другого пользователя из-под рута
  - В обоих случаях надо использовать внешнюю по отношению к sssd оснастку
  - Я привык использовать smbldap-tools
  - Требует хранить в файле пароль администратора LDAP
    файл доступен только root, но…
  - Наверное, ставить такие оснастки на все узлы кластера
    плохая идея