Bezpieczeństwo systemów informatycznych

ĆWICZENIE Kerberos i ACL

1. Mechanizm rozproszonego uwierzytelniania – Kerberos

1.1 Opis systemu

Kerberos jest rozproszonym systemem uwierzytelniania z zaufaną stroną trzecią (*third-party trust*). Stroną, której ufają wszystkie elementy systemu (użytkownicy i usługi), nazywane *principals*, jest serwer Kerberos. Wszystkie elementy principals współdzielą hasło, lub klucz z serwerem Kerberos i to pozwala im sprawdzać, czy wiadomości od serwera Kerberos są autentyczne. System używa centralnej bazy danych uwierzytelniających. Baza taka jest zaimplementowana na jednym lub wielu węzłach o wysokim poziomie bezpieczeństwa, pełniących rolę centrów dystrybucji kluczy (KDC). Podmioty funkcjonujące w systemie (użytkownicy, hosty lub programy funkcjonujące w imieniu użytkownika) otrzymują z centrum KDC „dowody osobiste" (*credentials*), zawierające bilet (*ticket*) oraz jednorazowy klucz szyfrowania (*session key*) niezbędny w dostępie do poszczególnych usług, np. zdalnego logowania, drukowania itd. Każdy host, podobnie jak każdy użytkownik funkcjonujący w domenie uwierzytelniania (*realm*) musi zostać do niej indywidualnie dołączony.

1.2 Wykorzystanie Kerberosa

1.2.1 Stworzenie serwera.

Serwer Kerberos wymaga określenia domeny realm oraz utworzenia bazy kluczy KDC. Konfigurację przechowuje plik /etc/krb5.conf, którego przykładowa zawartość wygląda następująco:

```
 1   [libdefaults]
 2      Default_realm = MY.REALM
 3      dns_lookup_kdc = false
 4      dns_lookup_realm = false
 5   [realms]
 6   MY.REALM = {
 7         kdc = nazwa_serwera_Kerberos
 8     admin_server = nazwa_serwera_Kerberos
 9   }
10   [domain_realm]
11      .my.domain = MY.REALM
12   [logging]
13      kdc = FILE:/var/log/krb5kdc.log
14      admin_server = FILE:/var/log/kadmin.log
15      default = FILE:/var/log/krb5lib.log
```

`MY.REALM` – nazwa domeny Kerberos
`kdc` – nazwa komputera, na którym należy szukać KDC.

UWAGA! Nazwa domeny realm może choć nie musi (jak powyżej) być identyczna z nazwą domeny DNS określoną dla danego komputera. Jednak nazwa komputera KDC musi odpowiadać nazwie kanonicznej (DNS) tego komputera w sieci.

Linie 3 i 4 mają za zadanie wyłączyć zapytania do DNS. Zamiast DNS można wykorzystać plik /etc/hosts. W tym celu należy dodać w nim nazwę komputera stanowiącego KDC, zarówno na nim samym, jak i na komputerach z niego korzystających, np.:

```
150.254.1.1 nazwa_hosta, nazwa_hosta.my.domain, nazwa_hosta.my.realm
```

Klucze są przechowywane w bazie danych. Do ich szyfrowania można wykorzystać klucz główny (*master key*). W celu stworzenia i zainicjowania bazy kluczy należy uruchomić program kdb5_util:

```
# kdb5_util create -r MY.REALM -s
```

Następnie należy stworzyć administratora systemu Kerberos uruchamiając program kadmin.local:

```
# kadmin.local
kadmin.local: addprinc admin/admin@MY.REALM
```

Następnie należy poleceniem `addprinc` dodać do bazy użytkownika:

```
kadmin.local: addprinc scott
kadmin.local: addprinc secoff
```

Na końcu należy stworzyć bazę danych kluczy administratora:

```
kadmin.local: ktadd -k /var/lib/kerberos/krb5kdc/kadm5.keytab
              kadmin/admin kadmin/changepw
```

Do właściwej pracy bazy danych potrzebny są także pliki konfiguracyjne kdc.conf i kadm5.acl. Należy je utworzyć w katalogu /var/lib/kerberos/krd5kdc/. W zawartości trzeba podać domenę. Przykładowa zawartość pliku kdc.conf:

```
[kdcdefaults]
        kdc_ports = 750,88

[realms]
        MY.REALM = {
                database_name = /var/lib/kerberos/krb5kdc/principal
                admin_keytab =
FILE:/var/lib/kerberos/krb5kdc/kadm5.keytab
                acl_file = /var/lib/kerberos/krb5kdc/kadm5.acl
                key_stash_file =
/var/lib/kerberos/krb5kdc/.k5.MY.REALM
                kdc_ports = 750,88
                max_life = 10h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
        }
[logging]
    kdc = FILE:/var/log/kdc.log
    admin_server = FILE:/var/log/kadmin.log
```

Przykładowa zawortość pliku kadm5.acl, opis manual kadmind(8):

```
*/admin@CS.PUT.POZNAN.PL  *
*/*@CS.PUT.POZNAN.PL i
```

W tym momencie można już uruchomić KDC poleceniem:

```
# rckrb5kdc start
# rckadmind start
```

Można też zainicjować użytkownika:

```
# kinit me
me@MY.REALMS's Password:
```

i wypisać swój bilet:

```
# klist
Credentials cache: /tmp/krb5cc_0
        Principal: me@MY.REALM

  Issued           Expires          Principal
Aug 25 07:25:55  Aug 25 17:25:55  krbtgt/MY.REALM@MY.REALM
```

A także wylistować wszystkie wpisy w bazie :

```
# kdb5_util dump
```

Niezbędnym składnikiem serwera jest jeszcze baza kluczy. Serwer Kerberos musi posiadać wszystkie klucze serwerów usług. Pozwala to na weryfikacje tożsamości innych hostów i ich wzajemną autentykację. Klucz taki musi być przesłany do serwera Kerberos w sposób bezpieczny, inaczej klucz prywatny stanie się kluczem publicznym, co w sposób oczywisty zagraża bezpieczeństwu. Zazwyczaj przesyła się je używając programu `kadmin`. Komenda `ank --random-key` pozwala wygenerować i dodać do bazy klucz, a komenda ktadd pozwala na przerzucenie go do pliku `keytab.`

```
# kadmin -p admin/admin@MY.REALM
kadmin> ank --random-key host/myserver
 kadmin> ktadd host/myserver
```

W komputerze dodawanym plik krb5.conf musi być zgodny z plikiem krb5.conf na serwerze Kerberos.

Polecenia `kinit` i `klist` to polecenia klienckie, wykonywane na dowolnym komputerze w domenie Kerberos.

1.2.2 Korzystanie z Kerberosa

Przed uruchomieniem aplikacji korzystających z systemu uwierzytelniania Kerberos należy uruchomić program `kinit` z przełącznikiem `–f`, aby uzyskać klucz, który będzie mógł być przesyłany dalej (*forwarded*) aż do serwera docelowego lub w obrębie grupy serwerów świadczących określone usługi. Pozwoli to na zachowanie jednokrotnego uwierzytelniania.

Aby umożliwić zdalne logowanie przy pomocy autentykacji Kerberosem należy stworzyć serwer Kerberos, dodać do niego zdalny host, przekopiować na host plik /etc/krb5.conf, a także w pliku /etc/hosts klienta dodać informację odnośnie KDC, a w KDC odnośnie hosta klienta. Następnie w pliku /etc/xinetd.d/klogin odblokować uruchamianie tej usługi i uruchomić usługę xinetd.

Każdy użytkownik powinien posiadać listę uwierzytelnienia w pliku .k5login w katalogu domowym. Każda linia w pliku musi być postaci: *principal/instance@realm*. Muszą się w nim znajdować informacje odnośnie użytkowników, którzy mają prawo się logować jako dany użytkownik. Aby uniknąć kłopotów z bezpieczeństwem właścicielem pliku .k5login musi być użytkownik. Jeśli plik nie istnieje dopuszczeni zostaną użytkownicy o nazwie w systemie kerberos zgodnej z nazwą użytkownika w systemie.

Należy następnie uruchomić ponownie demona inetd oraz zalogować się korzystając z polecenia

```
/usr/lib/mit/bin/rlogin –l nazwa_uzytkownika zdalny_host
```

Kerberos można wykorzystać także do innych usług, takich jak finger, HTTP, SSH i inne. Należy wówczas oczywiście wprowadzić odpowiednie modyfikacje w odpowiednich plikach konfiguracyjnych.

1.2.3 Uwierzytelnianie użytkowników w systemie Windows XP

W systemie Windows XP programy do skonfigurowania uwierzytelniania przy wykorzystaniu serwera Kerberos znajdują się na oficjalnej płycie instalacyjnej w tzw. „Support Tools” i są to narzędzia działające w linii poleceń.

Konfiguracja systemu Windows przebiega następująco:

```
> ksetup.exe /addkdc MY.REALM serwer_kerberos
> ksetup.exe /addkpasswd MY.REALM serwer_kerberos
> ksetup.exe /setrealm MY.REALM
```

Ustawienie hasła systemu windows:

```
> ksetup.exe /setcomputerpasswd haslo
```

Należy również na serwerze Kerberosa dodać wpis dotyczący danego systemu Windows (hasło należy podać identyczne z hasłem wpisanym dla systemu Windows:

```
kadmin> ank -e rc4-hmac:normal host/system_windows
```

Należy jeszcze zdefiniować, którzy użytkownicy będą uwierzytelniani poprzez system Kerberos:

```
> ksetup.exe /mapuser kerberos_principal local_account
> ksetup.exe /mapuser * *
```

Ostatnim krokiem jest restart systemu i próba zalogowania się z wykorzystaniem haseł zawartych w systemie Kerberos.

Zadania:

1. Zrealizować uwierzytelnianie poprzez system Kerberos dla usługi rlogin.
2. Zrealizować autoryzację użytkowników dla systemu Windows XP.
3. Wyczyścić konfigurację systemów Windows i Linux do początkowych.

2. POSIX Access Control Lists

2.1 Wprowadzenie

ACL został opracowany, aby rozszerzyć standardowe prawa, które opisują dostęp do pliku (lub katalogu) dla właściciela, grupy oraz innych użytkowników. Rozszerzenie dotyczy możliwości definiowania dodatkowych uprawnień dla innych użytkowników i/lub grup. Dodatkowe uprawnienia ograniczają się do prawa odczytu (read), zapisu (write), wykonywania/przeszukiwania (execute).

Używanie ACL jest możliwe w wielu rodzajach systemów plików w systemie operacyjnym Linux, np.: ext2, ext3, reiserfs, nfs.

2.2 Algorytm sprawdzania uprawnień dostępu

Standard POSIX ACL oferuje możliwość maskowania uprawnień poprzez pole maski. Efektywnie uprawnienia do pliku są sumą bitową uprawnień użytkownika/grupy i maski.

Kolejne kroki algorytmu sprawdzenia uprawnień dostępu:

1. jeśli użytkownik jest właścicielem pliku – dopuść,
2. jeżeli użytkownik jest na liście nazwanych użytkowników i ma odpowiednie efektywne uprawnienia – dopuść,
3. jeżeli jedna z grup użytkownika jest grupą właściciela i posiada odpowiednia efektywne prawa – dopuść,
4. jeżeli jedna z grup użytkownika występuje jako grupa nazwana i posiada odpowiednie efektywne prawa – dopuść,
5. jeżeli jedna z grup użytkownika jest grupą właściciela lub należy do grup nazwanych, ale nie posiada dostatecznych efektywnych uprawnień – dostęp jest zabroniony,
6. następnie uprawnienia innych (others) określają możliwość dostępu.

2.3 Polecenia

Dostępne są dwa polecenia, jedno służy do odczytu rozszerzonych praw, drugie do ich ustawiania:

- getfacl
- setfacl

2.3.1 Polecenie getfacl

Program wypisuje rozszerzone uprawnienia do plików i katalogów.

```
% ls -l
 -rw-r--r-- 1 user group 1000 2004-10-01 09:00 plik.txt

% getfacl plik.txt
# file: plik.txt
# owner: user
# group: group
user::rw-
group::r--
other::r--

% getfacl plik.txt –-omit-header
user::rw-
group::r--
other::r--
```

2.3.2 Polecenie setfacl

Polecenie pozwala zmienić, dodać lub usunąć uprawnienia z rozszerzonych uprawnień.

Dodanie uprawnień:

```
% setfacl -m user:kowalski:rwx plik.txt
% getfacl plik.txt –-omit-header
user::rw-
user:kowalski:rwx
group::r--
mask::rwx
other::r--
```

Zmiana uprawnień:

```
% setfacl -m u:kowalski:r plik.txt
% getfacl plik.txt –-omit-header
user::rw-
user:kowalski:r
group::r--
mask::rwx
other::r--
```

Usunięcie uprawnień:

```
% setfacl -x u:kowalski plik.txt
% getfacl plik.txt –-omit-header
user::rw-
group::r--
mask::r--
other::r--
```

Uprawnienia domyślne dotyczą tylko katalogów i umożliwiają automatyczne nadawanie rozszerzonych uprawnień do nowotworzonych plików/katalogów w katalogu, któremu nadaliśmy uprawnienia domyślne.

Dodanie uprawnień domyślnych:

```
% setfacl -d -m group:students:wx katalog
% getfacl katalog –-omit-header
user::rwx
group::r-x
other::r-x
default:user::rwx
default:group::r-x
default:group:students:-wx
default:mask::rwx
default:other::r-x
```

Modyfikacja i usuwanie domyślnych uprawnień jest analogiczne.

Możliwość ustawiania pola maski jest możliwa poprzez następujące polecenie:

```
% setfacl -m mask::rwx plik.txt
```

Istnieją jeszcze opcje pozwalające całkowicie skasować rozszerzone uprawnienia (`-b`) oraz domyślne uprawnienia (`-k`).

Zadania:

1. Stworzyć katalog z prawami 0750 i zobaczyć listę rozszerzonych praw do tego katalogu.
2. Dodać uprawnienia do zapisu i przeszukiwania do powyższego katalogu koledze siedzącemu przy sąsiednim komputerze.
3. Sprawdź czy możesz zapisać jakiś plik do katalogu kolegi. Jeśli nie – sprawdź przyczynę.
4. Wykonać chmod g-w <katalog>, następnie sprawdzić czy kolega może stworzyć plik w tym katalogu. Sprawdzić rozszerzone uprawnienia dla tego katalogu.
5. Wykonać chmod g+w <katalog> i ponownie wykonać punkt poprzedni.
6. Nadać katalogowi uprawnienia domyślne. Stworzyć w katalogu kolegi plik, katalog. Sprawdzić rozszerzone uprawniania nowo utworzonego pliku i katalogu.
7. Utworzyć nowy katalog ~/public z uprawnieniami "wx" dla grupy "students" oraz "rwx" dla grupy "staff". Dodać domyślne uprawnienia dla samego siebie.