Zabezpieczanie serwerów usług aplikacyjnych na przykładzie WWW (uwięzienie w piaskownicy)

1. Wprowadzenie

Zabezpieczanie serwerów usług aplikacyjnych polega głównie na ograniczeniu jego środowiska oraz ograniczenie dostępu do zasobów systemu operacyjnego i plików w systemie. Wiele z metod służących do ograniczanie aplikacji zostało już omówiona we wcześniejszych materiałach, poprzez mechanizm PAM i limity. W tym laboratorium należy zaznajomić się z możliwością ograniczenia systemu plików i dostępu do jego zasobów aplikacji serwerowej.

Uwięzienie w piaskownicy jest jedną z metod ograniczania dostępu do systemu plików systemu operacyjnego. Ponieważ jest to jedyne zadanie tego mechanizmu nie wpływa on na zwiększenie bezpieczeństwa samej aplikacji serwerowej, a jedynie zwiększa bezpieczeństwo systemu operacyjnego.

Celem ćwiczenia jest uruchomienie serwera apache w środowisku uwięzionym w piaskownicy.

2. Uwięzienie w piaskownicy

Mechanizm ten bardzo często nazywany jest więzieniem, jednak nie jest on aż tak bezpieczny, dlatego nie powinno używać tej nazwy.

Mechanizm ten może być wykorzystywany przez każdą dowolną aplikację, jak również przez aplikacje przystosowane do wykorzystywania tego mechanizmu. Oczywiście występują duże różnice między tymi podejściami.

Aplikacje posiadające wsparcie dla tego mechanizmu same mogą uwięzić się w piaskownicy, jednak zanim uwięzią się wczytują wszystkie potrzebne biblioteki systemowe i pliki konfiguracyjne, w piaskownicy nie będą miały już do nich dostępu. Piaskownica ogranicza się wtedy do plików, które muszą być stale dostępne aplikacji (w przypadku serwera www będą to strony www).

Natomiast aplikacje nie posiadające wsparcie dla mechanizmu mogą z niego korzystać w sposób niezauważalny dla nich. Jest to możliwe pod warunkiem, że aplikacja w piaskownicy będzie posiadała dostęp do wszystkich bibliotek i plików, które są wymagane przy starcie aplikacji.

Piaskownica jest strukturą katalogową, do której będzie miała dostęp aplikacja, zazwyczaj jest to struktura wymagana przez aplikacje wraz ze wszystkimi plikami.

Podsumowanie mechanizmu piaskownicy

Mechanizm uwięzienie w piaskownicy jest stosowany jeśli chcemy ograniczyć dostęp do plików serwerom aplikacyjnym, dzięki temu możemy ograniczyć szkody, jeśli komuś uda się przełamać zabezpieczenia danej aplikacji serwerowej, jednak wtedy uzyskuje jedynie dostęp do ograniczonego środowiska piaskownicy..

3. Umieszczenie serwera Apache w środowisku uwięzienia w piaskownicy.

Po pierwsze należy stworzyć strukturę katalogową piaskownicy w jakimś katalogu systemu operacyjnego. Przykładowo stworzymy katalog /chroot/apache/. W katalogu tym musimy

stworzyć następujące katalogi:

- etc/apache2
- srv/www/htdocs
- srv/www/icons
- srv/www/cgi-bin
- lib (lub lib64)
- usr/lib (lub usr/lib64)
- usr/sbin
- var/log/apache2 (należy umożliwić zapis użytkownikowi *wwwrun*)
- var/run
- dev

Następnie należy przegrać z głównego środowiska do piaskownicy całe katalogi:

- /etc/apache2 do /chroot/apache/etc/apache2
- /srv/www/htdocs do /chroot/apache/srv/www/htdocs
- /srv/www/icons do /chroot/apache/srv/www/icons
- /srv/www/cgi-bin do /chroot/apache/srv/www/cgi-bin
- /usr/lib[64]/apache2* do /chroot/apache/usr/lib[64]/

Następnie należy przegrać kilka plików apache2 oraz podstawowych plików konfiguracyjnych systemu operacyjnego:

- /usr/sbin/apache* do /chroot/apache/usr/sbin/
- /dev/null do /chroot/apache/dev/
- /dev/random do /chroot/apache/dev/
- /dev/urandom do /chroot/apache/dev/
- /etc/mime.types do /chroot/apache/etc/
- /etc/resolv.conf do /chroot/apache/etc/
- /etc/passwd do /chroot/apache/etc/
- /etc/group do /chroot/apache/etc/
- /usr/sbin/apache2* do /chroot/usr/sbin/

Dodatkowo pliki passwd i group należy tak zmodyfikować, aby zostały tam jedynie informacje na temat użytkownika *wwwrun* i grupy *www*.

Jedynie brakuje jeszcze bibliotek, których wymaga serwer apache, listę tych bibliotek otrzymamy wykonując następujące polecenie *ldd /usr/sbin/httpd2-prefork*. Następnie wszystkie

wypisane biblioteki wraz z linkami symbolicznymi do nich należy skopiować do odpowiednich katalogów w piaskownicy.

Po ustawieniu wszystkich powyższych czynności możemy przystąpić do uruchomienia aplikacji Apache wywołując ją w następujący sposób *chroot /chroot/apache /usr/sbin/httpd2-prefork*

Przedstawione powyżej rozwiązanie nie oferuje przygotowania do obsługi skryptów PHP, jest to jedynie uwięzienie w piaskownicy samego serwera apache

4. Zadania

Wykorzystać zaprezentowane powyżej mechanizm uwięzienia aplikacji w piaskownicy w celu przygotowania aplikacji Apache do działania w uwięzionym środowisku i zweryfikowania poprawności działania serwera WWW.

5. Problemy do dyskusji

- Czy uwięzienia w piaskownicy jest dobrym mechanizmem obrony przed atakami?
- Czy mechanizm ten w ogóle służy do zabezpieczania serwera aplikacyjnego, czy raczej do zabezpieczania systemu operacyjnego?
- Czy możliwe jest obejście mechanizmu piaskownicy w podstawowej wersji wykorzystywanej w systemie Linux?
- Czy istnieją inne lepsze rozwiązania uwięzienia aplikacji w ograniczonym środowisku, jeśli tak to jakie?

6. Bibliografia

[CHROOT] apache – chroot http://www.linux.com/article.pl?sid=04/05/24/1450203

[CHROOT2] http://penguin.triumf.ca/chroot.html

[CHROOT3] http://www.faqs.org/docs/securing/chap29sec254.html

[MOD_SEC] MOD_SECURITY http://www.modsecurity.org/