Kontrola dostępu do serwera – podstawowe zabezpieczenie dla serwera Internetowego – w dwóch wydaniach *tcpwrapper* i *tcpserver*.

W. Venema kontra D. Bernstein?

(1) Piotr Kasztelowicz <Piotr.Kasztelowicz@am.torun.pl>,(2) Marek Czubenko <Marek.Czubenko@uck.uni.torun.pl>,(3) Iwona Zięba <Iwona.Zięba@uck.uni.torun.pl>
(1)Oddział Gruźlicy i Chorób Płuc, Wojewódzki Szpital im. L. Rydygiera w Toruniu (2) Uniwersyteckie Centrum Komputeryzacji, Uniwersytet Mikołaja Kopernika w Toruniu

Działania hackerów spowodowały, że początkowo chroniony jedynie hasłem dostęp do usług internetowych musiał zostać ograniczony do takiego stopnia, jaki jest potrzebny do sprawnych realizacji zadań serwera przy ograniczonym dostępie do serwera spoza lokalnej sieci do osób, dla których dostęp do tych usług z racji pełnienia określonych zadań jest niezbędny. Szereg nowoczesnych aplikacji sieciowych – między innymi *Apache, SSH,* nowoczesne wersje oprogramowania sieciowego *(Sendmail 8.9.3 i wyższe wersje, Qmail 1.03, Postfix Snapshot 20001005)* posiadają już własne systemy kontroli dostępu – w przypadku programów pocztowych jest to ograniczanie możliwości przesyłania poczty za pomocą smtp tylko dla wybranych hostów jak również blokowania otrzymywania poczty od hostów, które przesyłają permanentnie spamy (*blacklist, badmailfrom).* Część programów jednak, szczególnie tych „filogenetycznie najstarszych", uruchamianych za pomocą demona *inetd* systemowo nie posiada żadnych możliwości kontroli dostępu.

W chwili obecnej uważa się, że kontrola dostępu należy do standardowych obowiązków administratora sieci, co więcej warto dodać i pokazała to praktyka, że hosty niezabezpieczone stają się prędzej czy później ofiarą ataków hackerów, co przydarzyło się już niejednokrotnie. Cele wyeliminowania opisanej luki w bezpieczeństwie oprogramowania uruchamianego poprzez demona *inetd* w chwili obecnej są do dyspozycji dwa podstawowe i jak pisze Wietse Venema – autor jednego z nich – konkurujące, lecz nie zwalczające się ze sobą pakiety oprogramowania.

Tcpwrapper

Pierwszym systemem kontroli dostępu, powszechniej stosowanym jest *tcpwrapper*, który standardowo instalowany jest w większości instalacji *Linux'a* przez co w przypadku podjęcia decyzji i jego wykorzystaniu zadaniem administratora jest właściwa konfiguracja plików */etc/hosts.allow* i */etc/hosts.deny*. Aktualnie najnowsza wersja *tcpwrapper 7.6* może być także przystosowana do standardu *IPv6* adresów IP. Oprogramowanie to:

- Pozwala na zabezpieczanie programów uruchamianych za pomocą demona *inetd* i współpracuje z tym demonem (nie pozwala na zabezpieczanie programów uruchamianych inaczej niż poprzez demona *inetd*)
- Uruchamia się w przypadku przesłania żądania dla demona *inetd* i przejmuje dalszą kontrolę nad zabezpieczanym procesem
- Zapisuje informacje o hostach i użytkownikach (jeśli serwer otrzyma informacje o użytkownika za pośrednictwem programu *identd*) w logach

Szczegółowe informacje na temat instalacji i konfiguracji dostępne są na stronie poświęconej oprogramowaniu Wietse Venema[1] (autora tego programu) pod adresem *ftp://ftp.porcupine.org/pub/security/index.html*. Po zainstalowaniu oprogramowania należy wykonać dwie istotne czynności[2] aby zabezpieczenia działały poprawnie. Wprowadzić niezbędne zmiany w pliku */etc/inetd.conf*. Zmiany te powinny prowadzić:

- Do całkowitego zablokowania wszystkich tych usług (dla użytkowników z zewnątrz), które dla użytku zdalnego w ogóle nie są potrzebne.
- Wprowadzenia zmian w zapisie w pliku */etc/inetd.conf*, które nakazują przejęcie kontroli dostępu nad pozostałymi usługami przez demona *tcpd,* który jest podstawowym składnikiem pakietu *tcpwrapper*.

Dla przykładu zakładając, że *tcpd* został zainstalowany w katalogu */usr/sbin* dla usługi finger wpis w pliku */etc/inetd.conf* [3]

finger stream tcp nowait root /usr/sbin/fingerd fingerd

należy zamienić na

finger stream tcp nowait root /usr/sbin/tcpd fingerd

(chociaż prawdę mówiąc finger jest usługą, którą dla użytkowników z zewnątrz należałoby zablokować w ogóle).

Drugim krokiem jest dokonanie odpowiednich wpisów w plikach gdzie przechowywana będzie lista hostów którym przyznany będzie dostęp do danych usług */etc/hosts.allow* i zabroniony dostęp */etc/hosts.deny* do zabezpieczonych przez demona *tcpd* usług. Składnia polecenia wygląda mniej więcej następująco:

Usługa : adres : ALLOW – gdy zezwalamy na dostęp

Usługa : adres : DENY - gdy zabraniamy danego dostępu

Wpisy do plików czytane są po kolei, dzięki temu możemy w pliku *etc/hosts.allow* użyć tzw. składni rozszerzonej wpisując na końcu pliku:

ALL : ALL : DENY

co oznacza, że wszelkie inne usługi, niż te, które zostały dozwolone wpisami znajdującymi się powyżej są już zabronione. Przy takim wpisie nie jest konieczne tworzenie pliku */etc/hosts.deny*.

Przykłady wpisów

ftp: .nucleus.com : ALLOW
ftp: 128.4.5. : ALLOW
telnet: pekasz@amedec.amg.gda.pl : rcf931 : ALLOW
ALL : ALL : DENY

Pierwszy (z kropką na początku) mówi, że wszystkie hosty z domeny *nucleus.com* mają zezwolenie na dostęp do uslugi *ftp* . Drugi, że wszystkie hosty z IP *128.4.5.x* gdzie x jest każdym hostem w tej domenie mają zezwolenie na dostęp do usługi *ftp*. Trzeci zapis mówi, że

identyfikator *pekasz* na serwerze *amedec.amg.gda.pl* ma dostęp do usługi *telnet* ale tylko wtedy, jeśli jego tożsamość zostanie na zdalnej maszynie sprawdzone poprzez *identd*.

Tcpserver

Jest drugim z wymienionych rozwiązaniem autorstwa Dan'a Bernsteina[4] znanym szczególnie administratorom, którzy jako oprogramowanie pocztowe instalują *Qmail*. *Tcpserver* jest częścią pakietu *Ucspi-tcp* i charakteryzuje się całkiem odmienną filozofią:

- Pozwala na zabezpieczenie dowolnej usługi zdalnej – nie tylko tych, które uruchamiane są za pośrednictwem demona *inetd*.
- Nie współpracuje z demonem *inetd* ale całkowicie go zastępuje, stąd jest programem, który sam uruchamia dane usługi *TCP* i kontroluje do nich dostęp
- Z powyższego względu wymaga całkowitego zablokowania w pliku */etc/inetd.conf* usług jakie ma uruchamiać.
- Aby usługi te były dostępne po reboocie systemu wymaga dokonania odpowiednich wpisów w plikach startowych */etc/rc2.d/*
- Do zapisywania logów używa demona systemowego *syslogd* i oprogramownia *logger* lub dodatkowo instalowanego programu *multilog* z pakietu *demontools*[5]

Informacje na temat pakietu *Ucspi-tcp* znajdują się na stronie *http://cr.yp.to/ucspi-tcp.html*.

Po instalacji oprogramowania należy całkowicie zablokować wszystkie usługi w pliku */etc/inetd.conf*. Kolejną czynnością jest sporządzenie plików kontroli dostępu, które można tworzyć osobno dla każdej z usług przechowywanych zwyczajowo w katalogu */etc/tcp*. Przykładowy plikiem kontroli dostępu dla usługi telnet – czyli */etc/tcp/tcp.telnet* wyglada w sposób następująco:

localhost:allow
ania.el.pl:allow
=.ss.pl:allow
22.5.144.33:allow
:deny

Pierwsza linia zezwala na dostęp hostowi lokalnemu, druga maszynie *ania.el.pl*, trzecia linia pozwala na dostęp wszystkim maszynom których adres kończy się na *ss.pl*, czwarta hostowi o IP *22.5.144.33*. Ostatnia linia zabrania dostępu innym zdalnym maszynom. Istotne jest, że program *tcpserver* korzysta z plików kontroli dostępu zapisanych nie w formie tekstowej – jak powyżej – tylko w formie plików bazy *cdb*. Z tego powodu po zakończeniu i każdorazowo po aktualizacji plików trzeba dokonać konwersji pliku tekstowego w plik cdb – przy użyciu dostępnego w pakiecie *Ucspi-tcp* programu *tcprules*. W przypadku telneta będąc w katalogu */etc/tcp* i po sporządzeniu pliku *tcp.telnet* należy wykonać następującą komendę[6]:

tcprules /etc/tcp/tcp.telnet.cdb /etc/tcp/tcp.telnet.tmp < /etc/tcp/tcp.telnet

gdzie pliku *tcp.telnet.tmp* nie tworzymy – jest to plik tymczasowy, który tworzy się sam i następnie jest automatycznie usuwany. Następnie musimy uruchomić program *tcpserver* z opcją –v –x tak aby uzyskiwać informacje, które będą umieszczane w logach a ocja –x

nakazuje uruchamiać program z kontrolą dostępu. Dla usługi *telnet* należy uruchomić (jako root) ją poprzez *tcpserver* w sposób następujący:

tcpserver –v –x /etc/tcp/tcp.telnet.cdb 212.51.193.152 23 /usr/sbin/telnetd &

Znaczek „&” nakazuje uruchomić proces w tle adres IP jest adresem naszego serwera a liczba 23 portem, z którego korzysta *telnet*. Gdy dokonamy stosownych testów oprogramowania powinniśmy stworzyc odpowiednie pliki startowe dla systemu. W przypadku administrowanego przeze mnie serwera utworzyłem (dla systemu operacyjnego *Solaris*) plik startowy */etc/rc2.d/S69tcpserver-sshd*

```
#!/bin/sh
#
# Piotr Kasztelowicz, skrypt uruchamiajacy tcpserver i sshd
#
#
sleep 1
#
if [ -f /usr/local/bin/tcpserver -a -f /etc/tcp/tcp.ftp.cdb  ]; then
        /usr/local/bin/tcpserver -v -x /etc/tcp/tcp.ftp.cdb 212.51.193.152 21 /usr/sbin/in.ftpd
2>&1 | /bin/logger -p local1.info -t ftp &                    echo "starting tcpserver for
ftp account"
fi
#
if [ -f /usr/local/bin/tcpserver -a -f /etc/tcp/tcp.telnet.cdb ]; then
        /usr/local/bin/tcpserver -v -x /etc/tcp/tcp.telnet.cdb 212.51.193.152 23
/usr/sbin/in.telnetd 2>&1 | /bin/logger -p local1.info -t telnet &    echo "starting tcpserver for
telnet account"
fi
#
#
sleep 1
#
if [ -f /usr/local/sbin/sshd ]; then
        /usr/local/sbin/sshd            echo "starting secure shell daemon"
fi
```

Jak widać skrypt ten uruchamia przy starcie uruchamia z kontrolą dostępu poprzez *tcpserver* usługę *telnet* i *ftp* oraz już „samodzielnie”, z własnym systemem kontroli dostępu *sshd*. Jednocześnie w przypadku usługu *telnet* i *ftp* informacje wyjściowe w postaci logów zapisywane są poprzez oprogrmowanie *logger* i demon systemowy *syslogd* do plików logów zgodnie ze wskazaniami pliku */etc/syslog.conf*. Należy pamiętać także o całkowitym zablokowaniu *telneta* i *ftp* w pliku */etc/inetd.conf* tak aby nie mogły być uruchamiane przez *ineta*.

Kontrola dostępu do serwera Internetowego stała się tak istotnym elementem zabezpieczeń, że uważa się, że powinna znajdować się na każdym serwerze. Z uwagi na duże znaczenie tego tematu przedstawiliśmy dwa sprawdzone i uznane na całym świecie choć różniące się od siebie rozwiązania. Osobiście mieliśmy okazję stosować oba rozwiązania. W każdym miesiącu nasze maszyny notują próby skanowania portów powierzonych naszej opiece serwerów, stąd można powiedzieć, że sprawnie działające oprogramowanie zabezpieczające przed niepowołanym dostępem z zewnątrz wielokrotnie uratowało naszym serwerom „życie”. Referat ten traktujemy jako zachętę do zastosowania jednego z

przedstawionych pakietów oprogramowania wszędzie tam, gdzie jeszcze takie systemy nie są stosowane. Oprogramowanie to przeznaczone jest oczywiście dla systemu UNIX (w tym *Linux*), jednak w przypadku serwerów właśnie ten system operacyjny stał się wiodący – także w przypadku serwerów medycznych.

---

[1] http://www.porcupine.org/wietse/

[2] http://andromeda.roque.ing.iac.es/docs/cfg/security/tcpwrappers/tcpwrappers.html

[3] http://www.phys.ufl.edu/docs/system/public_domain/tcpwrapper.html

[4] http://cr.yp.to/djb.html

[5] http://cr.yp.to/daemontools.html

[6] http://Web.InfoAve.Net/~dsill/lwq.html