Dydaktyka Informatyki 10(2015)
ISSN 2083-3156
DOI: 10.15584/di.2015.10.20
http://www.di.univ.rzeszow.pl

Wydział
Matematyczno-Przyrodniczy UR
Laboratorium Zagadnień
Społeczeństwa Informacyjnego

Jacek WOŁOSZYN

Dr inż., Uniwersytet Technologiczno-Humanistyczny w Radomiu, Wydział Informatyki i Matematyki, Katedra Informatyki, ul. Malczewskiego 29, 26-600 Radom; jacek@delta.pl

KONTROLA INTEGRALNOŚCI KLUCZOWYCH ELEMENTÓW SYSTEMU INFORMATYCZNEGO

CHECKING THE INTEGRITY OF THE KEY ELEMENTS OF THE INFORMATICS SYSTEM

Słowa kluczowe: bezpieczeństwo systemu, integralność, suma kontrolna, Linux.
Keywords: safe system, integrity, control sum, Linux.

Streszczenie

Celem artykułu jest opisanie prostego sposobu monitorowania integralności wybranych elementów systemu z wykorzystaniem standardowych poleceń systemu operacyjnego Linux. Zapewnienie integralności kluczowych plików konfiguracyjnych systemu skutkuje jego prawidłowym i niezmiennym działaniem w procesie przetwarzania danych.

Summary

This article is to describe a simple method for monitoring the integrity of the system using standard Linux operating system command. Ensuring the integrity of key configuration files provide the correct and consistent operation in data processing.

Wprowadzenie

Usługa integralności dotyczy prawdziwości informacji; dzięki niej użytkownicy mogą być pewni, że dane są prawdziwe i nie zostały zmodyfikowane przez nieuprawnione osoby. Usługa integralności chroni przed atakami modyfikującymi i dotyczy ona informacji w formie fizycznej, elektronicznej, a także przepływającej. Obecnie prawie wszystkie systemy informatyczne nie działają samodzielnie, lecz jako elementy powiązanej ze sobą infrastruktury spełniają ściśle określoną rolę w systemie[1]. Połączenie z siecią jest niezbędnym warun-

[1] M. Rash, *Linux firewalls Attack Detection and Response with iptables, psad, and fwsnort*, No Starch Press 2007.

kiem do przetwarzania informacji w rozproszonej grupie hostów, jak i serwerów, ale jednocześnie generuje zagrożenia związane z możliwością nieautoryzowanego dostępu do elementów systemu, a co za tym idzie – istnieje możliwość naruszenia integralności systemu przez osoby nieuprawnione.

Idea przedstawionego poniżej rozwiązania polega na utworzeniu pliku z wzorcowym obrazem sum kontrolnych i cyklicznym monitorowaniu generowanych wyników z obrazem wcześniej utworzonego wzorca. W przypadku otrzymania zgodnych obrazów mamy pewność, że integralność systemu nie została naruszona. O braku zgodności z obrazem wzorcowym jesteśmy informowani odpowiednim komunikatem z nazwą pliku, którego integralność została naruszona.

1. Suma kontrolna

Istnieje zagrożenie, że pliki mogą ulec uszkodzeniu lub utracie podczas transferu danych, modyfikacji przez złośliwe aplikacje[2] zmianę zawartości zamierzoną lub niezamierzoną. Napastnik może celowo zmodyfikować istotny plik konfiguracyjny[3] systemu w celu uzyskania korzyści. W większości przypadków jest to nieuprawniony dostęp do systemu, którego celem jest uzyskanie informacji lub zmiany algorytmu przetwarzania informacji.

Suma kontrolna[4] to nic innego jak unikalny ciąg znaków wygenerowany na podstawie plików. Jest on unikalny dla każdego pliku. Jakakolwiek zmiana powoduje zmianę wyniku obliczenia sumy kontrolnej. Porównanie sum kontrolnych obrazów wzorcowych, jak i obliczonych w trakcie sprawdzania integralności informuje nas o poprawności struktury danych. Sumy kontrolne odgrywają w tym przypadku kluczową rolę informującą o poprawności struktury.

Do obliczenia sumy kontrolnej w tym przypadku można użyć polecenia md5sum[5]. Generuje ono łańcuch sumy kontrolnej poprzez zastosowanie odpowiedniego algorytmu dla zawartości pliku.

Wypisuje albo sprawdza sumy kontrolne MD5 (128-bitowe).
Możliwe opcje:
-b, --binary czytanie w trybie binarnym;

[2] J. Faircloth, *Penetration Tester's Open Source Toolkit*, Syngress 2011; J.C. Huang, *Software error detection*, Wiley 2009.

[3] R. Pinkal Pollei, *Debian 7 System Administration Best Practices*, Packt 2013; G. Stepanek, *Software Project Secrets*, Apress 2012.

[4] K.R. Fall, W.R. Stevens, *TCP/IP od środka. Protokoły*, wyd. II, Helion, Gliwice 2013; Ch. Negus, *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012; E. Nemeth, G. Snyder, R. Trent, H. Whaley, *Ben Unix and Linux system administration handbook fourth edition*, Pretence Hall 2010.

[5] K.R. Fall, W.R. Stevens, *TCP/IP od środka…*; R. Stevens, *TCP/IP Illustrated Vol. 1*, Pretence Hall 2010.

-c, --check sprawdzanie sum MD5 zapisanych w PLIKACH;
-t, --text czytanie plików w trybie tekstowym (domyślnie).

Następujące opcje są przydatne tylko przy sprawdzaniu sum kontrolnych:

--quiet bez wypisywania OK dla każdego pozytywnie zweryfikowanego pliku;
--status bez wypisywania niczego, kod wyjścia przekazuje wynik;
--w ostrzeganie o niepoprawnie sformatowanych liniach sum;
--strict z --check będzie zwracany niezerowy status wyjścia, jeżeli dane wejściowe są błędne;
--help wyświetlenie tego opisu i zakończenie;
--version wyświetlenie informacji o wersji i zakończenie.

Sumy są liczone wg opisu w dokumencie RFC 1321. Przy sprawdzaniu dane wejściowe powinny być takie jak wygenerowane przez ten program na wyjściu. Domyślny tryb to wypisanie linii z sumą kontrolną, znaku wskazującego typ (`*' binarny, ` 'tekstowy) i nazwy każdego pliku.

Obliczenie sumy kontrolnej dla pojedynczego pliku może nastąpić po wydaniu polecenia:

```
root@dlt:~# md5sum /etc/hosts.deny
92a0a19db9dc99488f00ac9e7b28eb3d  /etc/hosts.deny
```

Jak widać, została wygenerowana suma kontrolna dla pliku hosts.deny. Zapis tej sumy kontrolnej można przekierować ze standardowego wyjścia do pliku i zapisać jako suma_kontrolna.md5. Oczywiście jest to tylko zaproponowany przykład, nazwa pliku może być dowolna.

Wydanie polecenia md5sum z parametrem -c spowoduje sprawdzenie sum kontrolnych zapisanych w plikach.

```
root@dlt:~# md5sum /etc/hosts.deny > suma_kontrolna.md5
root@dlt:~# md5sum -c suma_kontrolna.md5
/etc/hosts.deny: DOBRZE
```

Uzyskana informacja DOBRZE informuje nas o tym, że sumy kontrolne zgadzają się, a tym samym nie została naruszona struktura pliku.

2. Zastosowanie sumy kontrolnej w przypadku wielu plików

Suma kontrolna działa doskonale także w przypadku wielu plików, co umożliwia zastosowanie jej do struktury katalogów[6], a tym samym sprawdzenia jego integralności. Generowanie rekurencyjne sumy kontrolnej dla katalogu

[6] Ch. Negus, *Linux. Biblia*…; R. Pinkal Pollei, *Debian 7*…

można wykonać za pomocą polecenia md5deep z parametrami -r, która włącza tryb rekurencyjny oraz -l umożliwiającą włączenie trybu ścieżki względnej. Ostatecznie użycie polecenia wygląda następująco:

```
root@dlt:~# md5deep -rl /etc > suma_katakog_etc.md5
```

Za pomocą tego polecenia utworzono plik z obrazem sum kontrolnych katalogu /etc. Zawartość utworzonego pliku wygląda następująco:

```
root@dlt:~# cat suma_katakog_etc.md5 | head
85da64f888739f193fc0fa896680030e  /etc/pam.d/sudo
ee93e13ec6aa3f3120c6939a2880a5b6  /etc/pam.d/sshd
931055740c22663fcef3e304dcf89c54  /etc/pam.d/atd
9900720564cb4ee98b7da29e2d183cb2  /etc/pam.d/chpasswd
c0914a9d5dfaf3d5b09f83045e8bee93  /etc/pam.d/cron
1454e29bfa9f2a10836563e76936cea5  /etc/pam.d/newusers
9c81c4f58a8079fbeb7524bc40d29bbd  /etc/pam.d/gdm3
9f114bd9c338ab017db2ee6fee96deaa  /etc/pam.d/common-auth
cc163be3dbe4258e639238ccd5bcdea0  /etc/pam.d/ppp
e6f9c742b53359a4371dd9bfc209880c  /etc/pam.d/login
```

Zasadniczo składa się z dwóch kolumn: jedna z sum kontrolnych, a druga z nazwy pliku wraz ze ścieżką dostępu. Plik ten będzie używany jako wzorzec do wykonywanych cyklicznie obliczeń sum kontrolnych. Należy go odpowiednio zabezpieczyć, aby nie uległ uszkodzeniu lub przypadkowej modyfikacji.

Alternatywnie można użyć polecenia find i zastosować przetwarzanie potokowe strumienia danych, aby osiągnąć podobny efekt.

```
root@dlt:~# find /etc -type f -print0 | xargs -0 md5sum > suma_katalog_etc_1.md5
```

Po częściowym wylistowaniu pliku i porównaniu go z utworzonym wcześniej plikiem można stwierdzić, że są one identyczne, czyli utworzenie go za pomocą polecenia find jest poprawne.

```
root@dlt:~# cat suma_katalog_etc_1.md5 | head
85da64f888739f193fc0fa896680030e  /etc/pam.d/sudo
ee93e13ec6aa3f3120c6939a2880a5b6  /etc/pam.d/sshd
1454e29bfa9f2a10836563e76936cea5  /etc/pam.d/newusers
9900720564cb4ee98b7da29e2d183cb2  /etc/pam.d/chpasswd
9f114bd9c338ab017db2ee6fee96deaa  /etc/pam.d/common-auth
c0914a9d5dfaf3d5b09f83045e8bee93  /etc/pam.d/cron
9c81c4f58a8079fbeb7524bc40d29bbd  /etc/pam.d/gdm3
931055740c22663fcef3e304dcf89c54  /etc/pam.d/atd
e6f9c742b53359a4371dd9bfc209880c  /etc/pam.d/login
a69b859744494a52ecf10bb604544093  /etc/pam.d/samba
```

3. Sprawdzanie integralności

Mając utworzone wzorcowe struktury plików z sumami kontrolnymi katalogów można przystąpić do porównania sum kontrolnych na chwilę obecną działania systemu z wartościami zapisanymi w pliku wzorcowym. Wykorzystane zostanie do tego opisane już wcześniej polecenie md5sum z parametrem -c:

```
root@dlt:~# md5sum -c suma_katakog_etc.md5 | tail
md5sum: UWAGA: 1 policzona suma się NIE zgadza
/etc/networks: DOBRZE
/etc/skel/.bash_logout: DOBRZE
/etc/skel/.profile: DOBRZE
/etc/skel/.bashrc.original: DOBRZE
/etc/skel/.bashrc: DOBRZE
/etc/ld.so.conf: DOBRZE
/etc/cupshelpers/preferreddrivers.xml: DOBRZE
/etc/host.conf: DOBRZE
/etc/libccid_Info.plist: DOBRZE
/etc/alternatives/flash-mozilla.so: DOBRZE
```

Ze względu na długość listowanego pliku, zaprezentowano tylko kilka linii uzyskanych informacji. Jak można zauważyć, prezentowany jest każdy plik podlegający kontroli i prezentowany jest jego rezultat za pomocą informacji DOBRZE lub NIE. W przypadku, gdy kontrolowaną grupę stanowi duża ilość plików, dobrze jest zastosować przetwarzanie potokowe na przykład używając polecenia grep w celu filtrowania tylko interesujących nas treści. W tym przypadku słowo 'NIE' zastosowane w tym filtrze spowoduje, że zostaną tylko wyświetlone pliki, których suma kontrolna została zmieniona i na nią należy zwrócić szczególną uwagę i przeanalizować przyczyny tej zmiany.

```
root@dlt:~# md5sum -c suma_katakog_etc.md5 | grep 'NIE'
/etc/mtab: NIEPOWODZENIE
md5sum: UWAGA: 1 policzona suma się NIE zgadza

root@dlt:~# md5sum -c suma_katalog_etc_1.md5 | head
/etc/pam.d/sudo: DOBRZE
/etc/pam.d/sshd: DOBRZE
/etc/pam.d/newusers: DOBRZE
/etc/pam.d/chpasswd: DOBRZE
/etc/pam.d/common-auth: DOBRZE
/etc/pam.d/cron: DOBRZE
/etc/pam.d/gdm3: DOBRZE
/etc/pam.d/atd: DOBRZE
/etc/pam.d/login: DOBRZE
/etc/pam.d/samba: DOBRZE
```

Wnioski

Wykorzystanie opisanego powyżej rozwiązania pozwala na bieżące kontrolowanie integralności kluczowych elementów systemu. Jednak sprawdzanie ręczne wyników z odpowiednią częstotliwością byłoby zapewne uciążliwe. Jednym z rozwiązań, które mogłoby odciążyć administratora od tej czynności jest użycie systemowego CRON-a. Odpowiedni wpis w pliku crontab automatyzowałby cały proces i w zależności od zapisanych ustawień uruchamiał proces kontroli integracji. W przypadku wystąpienia słowa 'NIE' zostałby uruchomiony skrypt wysyłający maila z informacją na konto administratora, powiadamiający go o tym fakcie. Jest to rozwiązanie proste i skuteczne, niewymagające specjalnych narzędzi i oparte wyłącznie na poleceniach systemu operacyjnego.

Bibliografia

Faircloth J., *Penetration Tester's Open Source Toolkit*, Syngress 2011.

Fall K.R., Stevens W.R., *TCP/IP od środka. Protokoły*, wyd. II, Helion, Gliwice 2013.

Huang J.C, *Software error detection*, Wiley 2009.

McNab Ch., *Network Security Assessment*, O'Reilly 2007.

Negus Ch., *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012.

Nemeth E., Snyder G., Trent R. Whaley H., *Ben Unix and Linux system administration handbook fourth edition*, Pretence Hall 2010.

Pollei Pinkal R., *Debian 7 System Administration Best Practices*, Packt 2013.

Rash M., *Linux firewalls Attack Detection and Response with iptables, psad, and fwsnort*, No Starch Press 2007.

Stepanek G., *Software Project Secrets*, Apress 2012.

Stevens R., *TCP/IP Illustrated Volume 1*, Pretence Hall 2010.