# Bezpieczeństwo w sieci. Lab 05

Marcin Fabrykowski

20 czerwca 2012

# 1 Integralność pliku

## 1.1 MD5

```
[wto 12/06/19 23:44 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4193  (git)-[bezpieczenstwo_05]-% echo ‘‘To jest test’’ >test1.txt
[wto 12/06/19 23:44 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4193  (git)-[bezpieczenstwo_05]-% echo ‘‘To jest test’’ >test2.txt
[wto 12/06/19 23:54 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4212  (git)-[bezpieczenstwo_05]-% md5sum test1.txt >md5sums
[wto 12/06/19 23:54 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4213  (git)-[bezpieczenstwo_05]-% md5sum test2.txt >>md5sums
[wto 12/06/19 23:54 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4214  (git)-[bezpieczenstwo_05]-% cat md5sums
14d446376556dc52d16b7da9d01ef4bb  test1.txt
14d446376556dc52d16b7da9d01ef4bb  test2.txt
```

Zmiana pliku test1.txt

```
[wto 12/06/19 23:57 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4216  (git)-[bezpieczenstwo_05]-% md5sum -c md5sums
test1.txt: NIEPOWODZENIE
test2.txt: DOBRZE
md5sum: UWAGA: 1 policzona suma się NIE zgadza
zsh: exit 1     md5sum -c md5sums
```

gdczyt binarny

```
[wto 12/06/19 23:59 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4219  (git)-[bezpieczenstwo_05]-% md5sum -b test1.txt > md5bimsums
[wto 12/06/19 23:59 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4220  (git)-[bezpieczenstwo_05]-% md5sum -b test2.txt >> md5bimsums
[wto 12/06/19 23:59 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4222  (git)-[bezpieczenstwo_05]-% cat md5bimsums
dfcf2f421e3617fa8b32b1c1de977f75 *test1.txt
14d446376556dc52d16b7da9d01ef4bb *test2.txt
```

```
[śro 12/06/20 00:00 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4223  (git)-[bezpieczenstwo_05]-% md5sum -c md5bimsums
test1.txt: NIEPOWODZENIE
test2.txt: DOBRZE
md5sum: UWAGA: 1 policzona suma się NIE zgadza
zsh: exit 1     md5sum -c md5bimsums
```

Generowanie z lini poleceń

```
[śro 12/06/20 00:03 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4237  (git)-[bezpieczenstwo_05]-% echo -n ‘‘Marcin’’|md5sum
e67ce5b53efe91db1801de5b791e450e  -
```

## 1.2 SHA1

```
[śro 12/06/20 00:44 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4250 [1]  (git)-[bezpieczenstwo_05]-% echo ‘‘to jest test’’ > test3.txt
[śro 12/06/20 00:44 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4251  (git)-[bezpieczenstwo_05]-% echo ‘‘to jest test’’ > test4.txt
[śro 12/06/20 00:44 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4252  (git)-[bezpieczenstwo_05]-% sha1sum test3.txt >> sha1.txt
[śro 12/06/20 00:45 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4253  (git)-[bezpieczenstwo_05]-% sha1sum test4.txt >> sha1.txt
[śro 12/06/20 00:45 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4254  (git)-[bezpieczenstwo_05]-% cat sha1.txt
5a27078a792479814d35cffad61d6bc054b874f0  test3.txt
5a27078a792479814d35cffad61d6bc054b874f0  test4.txt
```

Po zmianie pliku test3.txt

```
[śro 12/06/20 00:51 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4257  (git)-[bezpieczenstwo_05]-% sha1sum -c sha1.txt
test3.txt: NIEPOWODZENIE
test4.txt: DOBRZE
sha1sum: UWAGA: 1 policzona suma się NIE zgadza
zsh: exit 1     sha1sum -c sha1.txt
```

Generowanie z lini polecen

```
[śro 12/06/20 01:48 CEST][pts/38][x86_64/linux-gnu/3.3.0-gentoo][4.3.15]
<torgiren@redraptor:~/szkola/semestr_6/bezpieczenstwo/05>
zsh/4 4259 [1]  (git)-[bezpieczenstwo_05]-% echo -n ‘‘Marcin’’ |sha1sum
1cf52227958603e9cfb4ae0794790e148035ce40  -
```

# 2 AIDE

Po wygenerowaniu bazy. Sprawdzenie zmienionych plików

```
redraptor torgiren # time aide --check -V
AIDE found differences between database and filesystem!!
Start timestamp: 2012-06-20 02:38:01

Summary:
  Total number of files:        110667
  Added files:                  2
  Removed files:                1
  Changed files:                5


---------------------------------------------------
Added files:
---------------------------------------------------

added: /dev/shm/pulse-shm-3360205652
added: /dev/shm/pulse-shm-3565753424

---------------------------------------------------
Removed files:
---------------------------------------------------

removed: /dev/shm/pulse-shm-2924314195

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /dev/shm
changed: /dev/shm/pulse-shm-787119478
changed: /dev/shm/pulse-shm-1590601964
changed: /dev/shm/pulse-shm-3414622995
```

```
changed: /dev/shm/pulse-shm-2604650014

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


Directory: /dev/shm
  Size     : 140                              , 160
  Ctime    : 2012-06-20 02:09:57              , 2012-06-20 02:44:30

File: /dev/shm/pulse-shm-787119478
  Bcount   : 808                              , 131080

File: /dev/shm/pulse-shm-1590601964
  Bcount   : 6672                             , 131080
  Ctime    : 2012-06-20 02:09:55              , 2012-06-20 02:44:24
  MD5      : PEQBU/aJTtd9qkTxONBn+w==         , poLf0e6GdDDFsCZVSuhxNQ==
  SHA1     : 3iATnvQJvmhLMD2VsxL3glPc0+w=     , Hz2KEStxj81TU8dORKmxWyK4USE=

File: /dev/shm/pulse-shm-3414622995
  Bcount   : 8                                , 131080

File: /dev/shm/pulse-shm-2604650014
  Bcount   : 496                              , 131080

real    7m2.515s
user    5m0.411s
sys     0m7.491s
```

# 3 Tripwire

Po przeprowadzeniu szyfrowania pliku konfiguracyjnego, nie udało mi się bazy danych. Nie możność znalezienia pliku tw.pol