

Laboratorium 1

Karol Słomczyński 272223

19.03.2024

Spis treści

1	Wprowadzenie	2
2	Zadanie 1	2
2.1	Podpunkt 1	2
2.1.1	Wyniki	2
2.2	Podpunkt 2	2
2.2.1	Wyniki	2
2.3	Podpunkt 3	3
2.3.1	Wyniki	3
2.4	Podpunkt 4	3
2.4.1	Wyniki	4
2.4.2	Wnioski	4
2.5	Podpunkt 5	4
2.5.1	Wyniki	4
2.5.2	Wnioski	4
3	Zadanie 2	4
3.1	Podpunkt 1	4
3.1.1	Wyniki	4
3.2	Podpunkt 2	5
3.2.1	Wyniki	5
3.3	Podpunkt 3	5
3.3.1	Wyniki	6
3.4	Podpunkt 4	6
3.4.1	Wyniki	6
3.5	Podpunkt 5	6
3.5.1	Wyniki	6
3.5.2	Wnioski	7
3.6	Podpunkt 6	7
3.6.1	Wyniki	7
3.6.2	Wnioski	8

1 Wprowadzenie

Celem laboratorium jest przeprowadzenie analizy logów dla serwisu ssh oraz serwisu SMTP. Użyłem podstawowych komend do obsługi plików tekstowych takich jak: grep, awk, sort, uniq, cut, head, tail, xargs. Utworzyłem skrypt w folderze /pliki pod nazwą script.bash który zawiera wszystkie komendy które użyłem do analizy logów.

2 Zadanie 1

Zadanie pierwsze polegało na przeprowadzeniu analizy logów serwisu ssh. Zadanie zawierało 2 pliki 'secure' oraz 'secure.1'.

2.1 Podpunkt 1

W celu zliczenia ilości prób logowania do serwisu ssh z niepoprawnymi danymi użyłem polecenia:

```
1 grep "Failed" -c secure
2 grep "Failed" -c secure.1
```

2.1.1 Wyniki

Wyniki jakie otrzymałem to dla pliku secure: 16794, dla pliku secure.1: 50570

2.2 Podpunkt 2

W celu wyświetlenia listy adresów ip z których próbowano się zalogować użyłem polecenia:

```
1 grep "Failed" secure | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq
  -c | sort -nr | uniq | head -n 30
2 grep "Failed" secure.1 | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' |
  -c | sort -nr | uniq | head -n 30
```

2.2.1 Wyniki

	secure	secure.1
1		
2	40 194.87.151.204	18 5.49.163.128
3	33 218.92.0.210	16 5.49.163.128
4	28 2.189.59.146	14 218.92.0.193
5	27 152.89.251.3	14 218.92.0.188
6	15 61.177.173.52	14 218.92.0.153
7	15 61.177.173.47	14 218.92.0.151
8	15 61.177.173.37	12 58.242.82.7
9	15 61.177.172.104	12 27.114.131.74
10	14 194.87.151.204	12 218.92.0.193
11	13 61.177.172.104	12 218.92.0.179
12	13 194.87.151.204	12 218.92.0.151
13	12 61.177.173.52	12 178.140.223.140
14	12 61.177.173.47	12 173.249.14.238
15	12 61.177.173.46	11 218.92.0.151
16	12 61.177.173.37	11 188.92.77.235
17	12 61.177.172.98	10 5.49.163.128
18	12 61.177.172.90	10 218.92.0.152
19	12 61.177.172.124	10 218.92.0.151
20	12 61.177.172.114	9 218.92.0.172
21	12 61.177.172.104	9 218.92.0.153
22	12 194.87.151.204	9 218.92.0.152
23	11 61.177.173.52	9 218.92.0.151
24	11 61.177.173.47	8 77.37.165.158
25	11 61.177.172.98	8 218.92.0.188

```

26      11 124.79.242.86      8 218.92.0.153
27      10 61.177.173.47     8 218.92.0.145
28      10 61.177.173.46     8 178.140.30.185
29      10 61.177.172.114    8 102.152.6.176
30      10 124.79.242.86     7 69.60.21.172
31      9 62.193.68.91       7 68.183.22.90

```

Jak możemy zauważyć w w pliku `secure.1` próby ataku są bardziej rozproszone niż w pliku `secure`. Co pokazuje nam że osoba przeprowadzająca atak posiada botnet lub proxy lub VPN.

2.3 Podpunkt 3

W celu wyświetlenia listy krajów z których było najwięcej prób logowania użyłem polecenia:

```

1  grep "Failed" secure | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq
   -- | xargs -I{} geoiplookup {} | sort | uniq -c | sort -nr | head -n 10
2  grep "Failed" secure.1 | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' |
   -- | xargs -I{} geoiplookup {} | sort | uniq -c | sort -nr | head -n 10

```

2.3.1 Wyniki

```

1      secure
2      2788 GeoIP Country Edition: US, United States
3      2137 GeoIP Country Edition: CN, China
4      742  GeoIP Country Edition: IN, India
5      664  GeoIP Country Edition: SG, Singapore
6      602  GeoIP Country Edition: DE, Germany
7      536  GeoIP Country Edition: JP, Japan
8      391  GeoIP Country Edition: RU, Russian Federation
9      388  GeoIP Country Edition: KR, Korea
10     352  GeoIP Country Edition: GB, United Kingdom
11     347  GeoIP Country Edition: VN, Vietnam
12
13     secure.1
14     10691 GeoIP Country Edition: CN, China
15     7028 GeoIP Country Edition: US, United States
16     4876 GeoIP Country Edition: FR, France
17     2127 GeoIP Country Edition: IN, India
18     1822 GeoIP Country Edition: DE, Germany
19     1721 GeoIP Country Edition: BR, Brazil
20     1610 GeoIP Country Edition: KR, Korea, Republic of
21     1562 GeoIP Country Edition: SG, Singapore
22     1336 GeoIP Country Edition: CA, Canada
23     1211 GeoIP Country Edition: GB, United Kingdom

```

2.4 Podpunkt 4

W celu wyświetlenia listy użytkowników lokalnych na których było najwięcej prób ataku użyłem polecenia:

```

1  grep 'Failed' secure | awk '{print $9,$11}' | awk '{if ($1 == "invalid") {print $2}
   -- else if (match($1, /^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/)) {print
   -- $1}}' | sort | uniq -c | sort -nr | head -n 20
2  grep 'Failed' secure.1 | awk '{print $9,$11}' | awk '{if ($1 == "invalid") {print $2}
   -- else if (match($1, /^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/)) {print
   -- $1}}' | sort | uniq -c | sort -nr | head -n 20

```

2.4.1 Wyniki

```
1      secure      secure.1
2    391 admin    1314 admin
3    239 test     1120 test
4    219 ubuntu   752 user
5    157 user     739 ubuntu
6    121 wang     613 ftpuser
7     85 oracle   492 postgres
8     84 postgres 481 oracle
9     79 zhang    309 nagios
10    70 ftpuser   242 guest
11    51 testuser  227 git
12    39 chen     223 support
13    36 ali      220 mysql
14    34 test1    212 teamspeak
15    34 administrator 208 deploy
16    33 yang     205 hadoop
17    33 steam    197 minecraft
18    32 pi       179 testuser
19    30 user1    153 zabbix
20    30 tomcat   153 www
21    30 guest    143 teamspeak3
```

2.4.2 Wnioski

Jak można zauważyć zarówno w pliku secure i secure.1 ataki są przeprowadzane na konta o nazwach domyślnych takich jak admin, test, user, ubuntu, ftpuser, postgres, oracle. Moim zdaniem atakujący liczy, że któryś z ‘domyślnych’ użytkowników będzie miał słabe hasło.

2.5 Podpunkt 5

W celu wyświetlenia listy użytkowników na które zalogowanie się powiodło użyłem polecenia:

```
1  grep 'Accepted' secure | awk '{print $9}' | sort | uniq -c
2  grep 'Accepted' secure.1 | awk '{print $9}' | sort | uniq -c
```

2.5.1 Wyniki

W przypadku obu plików wyniki są podobne w pliku secure udało się zalogować na konto root 1 raz, natomiast w pliku secure.1 udało się zalogować na konto local_user 29 razy

2.5.2 Wnioski

Ataki słownikowe nie powiodły się ponieważ wykorzystywane jest logowanie poprzez klucz prywatny-publiczny.

3 Zadanie 2

Zadanie drugie polegało na przeprowadzeniu analizy logów serwisu SMTP. Zadanie zawierało plik final.log

3.1 Podpunkt 1

W celu wyświetlenia liczby niudanych prób logowania do serwisu SMTP użyłem polecenia:

```
1  grep "login authenticator failed" final.log -c
```

3.1.1 Wyniki

Wynik jaki otrzymałem to 234

3.2 Podpunkt 2

W celu wyświetlenia listy adresów ip z których nastąpiły błędne próby logowania użyłem polecenia:

```
1 grep "login authenticator failed" final.log | grep -E  
  _ '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' -o | sort | uniq -c | sort -nr
```

3.2.1 Wyniki

```
1 69 127.0.0.1  
2 30 142.11.199.241  
3 27 185.180.222.147  
4 20 185.222.209.202  
5 18 10.0.0.142  
6 12 185.222.209.78  
7 10 94.102.49.198  
8 9 128.106.1.6  
9 8 91.212.150.81  
10 8 185.222.209.201  
11 7 93.157.63.30  
12 7 64.235.38.22  
13 5 185.211.245.195  
14 4 93.157.63.9  
15 4 93.157.63.8  
16 4 93.157.63.7  
17 4 93.157.63.6  
18 4 92.246.76.92  
19 4 80.85.153.204  
20 4 80.82.65.187  
21 4 62.50.131.54  
22 4 185.231.245.46  
23 4 185.231.245.44  
24 4 185.231.245.43  
25 4 185.231.245.41  
26 4 185.144.29.219  
27 4 185.144.28.111  
28 3 80.85.153.211  
29 3 80.85.153.206  
30 3 193.233.74.17  
31 3 185.231.245.49  
32 3 185.231.245.48  
33 3 185.231.245.40  
34 3 185.144.30.39  
35 3 185.144.29.30  
36 3 185.144.29.178  
37 2 37.120.146.84  
38 2 185.231.245.50  
39 2 185.144.28.241  
40 1 92.61.148.10  
41 [...]  
42 1 103.57.195.147
```

3.3 Podpunkt 3

W celu wyświetlenia listy krajów z których nastąpiły błędne próby logowania użyłem polecenia:

```
1 grep "login authenticator failed" final.log | grep -Eo  
  _ '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | xargs -I{} geoiplookup {} | sort  
  _ | uniq -c | sort -nr | head -n 10
```

3.3.1 Wyniki

```
1 105 GeoIP Country Edition: RU, Russian Federation
2 88 GeoIP Country Edition: IP Address not found
3 46 GeoIP Country Edition: NL, Netherlands
4 44 GeoIP Country Edition: GB, United Kingdom
5 38 GeoIP Country Edition: US, United States
6 11 GeoIP Country Edition: VN, Vietnam
7 9 GeoIP Country Edition: SG, Singapore
8 4 GeoIP Country Edition: EG, Egypt
9 2 GeoIP Country Edition: TH, Thailand
10 2 GeoIP Country Edition: DE, Germany
```

Jak można zauważyć próby ataku przede wszystkim pochodzą z Rosji, Holandii, Wielkiej Brytanii, Stanów Zjednoczonych.

3.4 Podpunkt 4

W celu wyświetlenia listy lokalnych użytkowników użyłem polecenia:

```
1 grep "R=localuser" final.log | cut -d ' ' -f 5 | cut -d "@" -f 1 | sort | uniq | sort
  _ -t "-" -k 2 -n
```

3.4.1 Wyniki

Konta lokalne to user-3, user-4, user-5, user-6, user-7, user-8, user-9, user-10, user-11, user-12, user-13, user-14, user-16, user-17, user-18, user-19, user-20, user-23, user-24, user-25, user-25-jg, user-25-lg, user-25-wb, user-30, user-32, user-34, user-35, user-40, user-41, user-43, user-44, user-45, user-47, user-48, user-50, user-51, user-53, user-54, user-55, user-56, user-57, user-58, user-59, user-60, user-61, user-68, user-69, user-70, user-71, user-72, user-73, user-74, user-75, user-76, user-77, user-78, user-79, user-81, user-82, user-83, user-84, user-86, user-87, user-88, user-89, user-90, user-91, user-93, user-94, user-95, user-96, user-97, user-99

3.5 Podpunkt 5

W celu wyświetlenia listy użytkowników lokalnych na których było najwięcej prób ataku użyłem polecenia:

```
1 grep "login authenticator failed" final.log | grep -v "@" | awk '{print $NF}' | cut -d
  _ '=' -f 2 | cut -d ')' -f 1 | sort | uniq -c | sort -nr | head -n 20
```

3.5.1 Wyniki

```
1 72 user-81
2 11 user-25-jg
3 10 user-25
4 5 vermont
5 4 arthur
6 2 user-54
7 2 user-5
8 2 user-25-wb
9 2 user-25-lg
10 2 user-10
11 1 yangxiong
12 1 via.postal
13 1 user-9
14 1 user-76
15 1 user-74
16 1 user-72
17 1 user-71
```

```

18 1 user-56
19 1 toiawase
20 1 tim_osborn1

```

3.5.2 Wnioski

Jak można zauważyć najwięcej prób ataku były przeprowadzane na konto 'user-81", prawdopodobnie zostało skompromitowane.

3.6 Podpunkt 6

W celu wyświetlenia prób wykorzystywania serwera jako 'open relay' użyłem kilku poleceń:

```

1 grep "no host name found for IP address" final.log
2 grep "rejected RCPT" final.log
3 grep "rejected unknown sender" final.log
4 grep "message too big for system" final.log
5 grep "max connection rate exceeded" final.log
6 grep "authentication failed" final.log

```

Jak można zauważyć użyłem 6 komend które pozwolą nam na sprawdzenie czy serwer jest wykorzystywany jako "open relay", jednakże nie jest to jednoznaczne. Komenda 1 pozwala sprawdzić czy serwer nie jest w stanie zidentyfikować adresu IP. Komenda 2 pozwala sprawdzić czy serwer odrzuca wiadomości. Komenda 3 pozwala sprawdzić czy serwer odrzuca nieznanych nadawców. Komenda 4 pozwala sprawdzić czy serwer odrzuca wiadomości które są za duże. Komenda 5 pozwala sprawdzić czy serwer odrzuca wiadomości które są wysyłane zbyt szybko. Komenda 6 pozwala sprawdzić czy serwer odrzuca próby logowania.

3.6.1 Wyniki

Nie dla wszystkich komend udało mi się uzyskać wyniki, jednakże dla komend w 1 i drugiej linijce udało mi się uzyskać wyniki.

Wyniki dla komendy 'grep "no host name found for IP address" final.log':

```

1 2019-03-08 04:06:06 no host name found for IP address 185.222.209.78
2 2019-03-08 04:06:08 no host name found for IP address 185.222.209.78
3 2019-03-08 04:06:40 no host name found for IP address 185.222.209.78
4 2019-03-08 04:06:42 no host name found for IP address 185.222.209.78
5 2019-03-08 04:08:24 no host name found for IP address 185.222.209.78
6 [...]
7 2019-03-18 18:32:08 no host name found for IP address 10.0.0.92
8 2019-03-18 18:37:42 no host name found for IP address 10.0.0.92
9 2019-03-18 21:20:01 no host name found for IP address 185.222.209.202
10 2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
11 2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
12 2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
13 2019-03-19 02:55:01 no host name found for IP address 91.212.150.81

```

Wyniki dla komendy 'grep "rejected RCPT" final.log':

```

1 2019-03-08 04:42:04 H=smtp.dzim.zarow.pl [51.38.142.82]
   - F=<foreign-user-2641@sermn.zagan.pl> temporarily rejected RCPT
   - <user-25-wb@some-domain.pl>: Could not complete sender verify
2 2019-03-08 05:42:25 H=(maerke.nl) [31.132.218.252] F=<foreign-user-1378@maerke.nl>
   - rejected RCPT <user-25-lg@some-domain.pl>: Access denied - 31.132.218.252 listed by
   - dnsbl.sorbs.net
3 2019-03-08 05:42:25 H=(maerke.nl) [31.132.218.252] F=<foreign-user-1378@maerke.nl>
   - rejected RCPT <user-25-jg@some-domain.pl>: Access denied - 31.132.218.252 listed by
   - dnsbl.sorbs.net
4 2019-03-08 05:42:25 H=(maerke.nl) [31.132.218.252] F=<foreign-user-1378@maerke.nl>
   - rejected RCPT <user-25@some-domain.pl>: Access denied - 31.132.218.252 listed by
   - dnsbl.sorbs.net

```

```

5 2019-03-08 05:42:25 H=(maerke.nl) [31.132.218.252] F=<foreign-user-1378@maerke.nl>
   └ rejected RCPT <user-25-wb@some-domain.pl>: Access denied - 31.132.218.252 listed by
   └ dnsbl.sorbs.net
6 2019-03-08 05:52:03 H=smtp.dzim.zarow.pl [51.38.142.82]
   └ F=<foreign-user-2641@sermn.zagan.pl> temporarily rejected RCPT
   └ <user-25-wb@some-domain.pl>: Could not complete sender verify
7 2019-03-18 18:02:31 H=(125-209-69-138.multi.net.pk) [202.142.163.62]
   └ F=<foreign-user-1395@multi.net.pk> rejected RCPT <user-25-wb@some-domain.pl>:
   └ Access denied - 202.142.163.62 listed by dnsbl.sorbs.net
8 [...]
9 2019-03-19 02:34:44 H=rrcs-162-155-179-211.cenhidden_useral.biz.rr.com
   └ [162.155.179.211] F=<foreign-user-1199@rr.com> rejected RCPT
   └ <user-25@some-domain.pl>: Access denied - 162.155.179.211 listed by
   └ b.barracudacenhidden_useral.org
10 2019-03-19 02:34:45 H=rrcs-162-155-179-211.cenhidden_useral.biz.rr.com
   └ [162.155.179.211] F=<foreign-user-1199@rr.com> rejected RCPT
   └ <user-25-wb@some-domain.pl>: Access denied - 162.155.179.211 listed by
   └ b.barracudacenhidden_useral.org
11 2019-03-19 02:43:33 H=(168-195-135210.deltanetworks.net.br) [168.195.135.210]
   └ F=<foreign-user-1360@deltanetworks.net.br> rejected RCPT
   └ <user-25-lg@some-domain.pl>: Sender verify failed
12 2019-03-19 02:43:33 H=(168-195-135210.deltanetworks.net.br) [168.195.135.210]
   └ F=<foreign-user-1360@deltanetworks.net.br> rejected RCPT
   └ <user-25-jg@some-domain.pl>: Sender verify failed
13 2019-03-19 02:43:34 H=(168-195-135210.deltanetworks.net.br) [168.195.135.210]
   └ F=<foreign-user-1360@deltanetworks.net.br> rejected RCPT <user-25@some-domain.pl>:
   └ Sender verify failed
14 2019-03-19 02:43:34 H=(168-195-135210.deltanetworks.net.br) [168.195.135.210]
   └ F=<foreign-user-1360@deltanetworks.net.br> rejected RCPT
   └ <user-25-wb@some-domain.pl>: Sender verify failed
15 2019-03-19 03:43:42 H=infinity16p.cf16.pl [94.177.240.244]
   └ F=<foreign-user-1768@finacial-hidden_users.pl> rejected RCPT
   └ <user-25-lg@some-domain.pl>: Access denied - 94.177.240.244 listed by
   └ dnsbl.sorbs.net

```

3.6.2 Wnioski

Jak można zauważyć w obu przypadkach logi są długie(800+ lini) co pokazuje nam że serwer prawdopodobnie jest wykorzystywany jako "open relay". Jednakże aby mieć pewność należałoby przeprowadzić analizę logów sieciowych na portach 25 i 587.