Laboratorium 1

Karol Słomczynski 272223

19.03.2024

Spis treści

1 Wprowadzenie

Celem labolatorium 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 foldrze /pliki pod nazwą script.bash który zawiera wszystkie komendy które użyłem do analizy logów.

2 Zadanie 1

Zadanie pierwsze polegalo 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:

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

2.1.1 Wyniki

Wyniki jake 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:

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

2.2.1 Wyniki

```
      secure                    secure.1
      698 218.92.0.210        172 218.92.0.151
      338 139.59.18.191       124 218.92.0.153
      330 61.177.173.47       102 5.49.163.128
      304 200.60.109.53        94 46.148.21.32
      301 61.177.173.37        78 58.59.2.26
      300 61.177.173.48        58 218.92.0.188
      285 61.177.173.52        52 77.104.80.41
      280 61.177.173.31        44 218.92.0.193
      276 61.177.172.114       42 58.242.82.7
      240 61.177.173.46        42 218.92.0.172
      240 61.177.172.98        37 178.128.96.131
      240 61.177.172.90        34 218.92.0.147
      236 61.177.172.104       33 51.38.51.113
      225 61.177.173.36        33 217.61.97.168
      198 61.177.173.50        31 93.32.27.160
      191 61.177.172.19        31 77.81.228.160
      175 61.177.173.35        31 14.98.4.82
      172 61.177.172.124       31 139.59.20.188
      168 61.177.173.49        30 61.221.60.191
      153 61.177.173.51        30 218.92.0.152
      152 194.87.151.204       30 188.166.8.178
      126 61.177.172.108       29 195.22.141.33
      117 124.79.242.86        29 185.244.25.167
       87 61.177.173.39        29 144.217.160.166
```

```
      66 195.226.194.142     28 206.189.8.182
      65 195.226.194.242     28 206.189.128.7
      60 82.200.161.178      28 195.84.49.20
      60 38.54.119.47        27 217.219.132.254
      60 35.224.42.65        27 198.27.67.173
      60 206.189.49.176      27 149.202.65.173
```

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 krajow z których było najwięcej prób logowania użyłem polecenia:

```
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
grep "Failed" secure.1 | 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
```

2.3.1 Wyniki

```
                secure
   2788 GeoIP Country Edition: US, United States
   2137 GeoIP Country Edition: CN, China
   742 GeoIP Country Edition: IN, India
   664 GeoIP Country Edition: SG, Singapore
   602 GeoIP Country Edition: DE, Germany
   536 GeoIP Country Edition: JP, Japan
   391 GeoIP Country Edition: RU, Russian Federation
   388 GeoIP Country Edition: KR, Korea
   352 GeoIP Country Edition: GB, United Kingdom
   347 GeoIP Country Edition: VN, Vietnam

                secure.1
  10691 GeoIP Country Edition: CN, China
   7028 GeoIP Country Edition: US, United States
   4876 GeoIP Country Edition: FR, France
   2127 GeoIP Country Edition: IN, India
   1822 GeoIP Country Edition: DE, Germany
   1721 GeoIP Country Edition: BR, Brazil
   1610 GeoIP Country Edition: KR, Korea, Republic of
   1562 GeoIP Country Edition: SG, Singapore
   1336 GeoIP Country Edition: CA, Canada
   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:

```
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
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

```
      secure                    secure.1
    9254 root                 8273 root
    391 admin                 1314 admin
    239 test                  1120 test
    219 ubuntu                 752 user
    157 user                   739 ubuntu
    121 wang                   613 ftpuser
     85 oracle                 492 postgres
     84 postgres               481 oracle
     79 zhang                  309 nagios
     70 ftpuser                242 guest
     51 testuser               227 git
     39 chen                   223 support
     36 ali                    220 mysql
     34 test1                  212 teamspeak
     34 administrator          208 deploy
     33 yang                   205 hadoop
     33 steam                  197 minecraft
     32 pi                     179 testuser
     30 user1                  153 zabbix
     30 tomcat                 153 www
     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 miało słabe hasło.

2.5 Podpunkt 5

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

```
grep 'Accepted' secure | awk '{print $9}' | sort | uniq -c
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 wyświelnia liczby niudanych prób logowania do serwisu SMTP użyłem polecenia:

```
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:

```
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

```
69 127.0.0.1
30 142.11.199.241
27 185.180.222.147
20 185.222.209.202
18 10.0.0.142
12 185.222.209.78
10 94.102.49.198
 9 128.106.1.6
 8 91.212.150.81
 8 185.222.209.201
 7 93.157.63.30
 7 64.235.38.22
 5 185.211.245.195
 4 93.157.63.9
 4 93.157.63.8
 4 93.157.63.7
 4 93.157.63.6
 4 92.246.76.92
 4 80.85.153.204
 4 80.82.65.187
 4 62.50.131.54
 4 185.231.245.46
 4 185.231.245.44
 4 185.231.245.43
 4 185.231.245.41
 4 185.144.29.219
 4 185.144.28.111
 3 80.85.153.211
 3 80.85.153.206
 3 193.233.74.17
 3 185.231.245.49
 3 185.231.245.48
 3 185.231.245.40
 3 185.144.30.39
 3 185.144.29.30
 3 185.144.29.178
 2 37.120.146.84
 2 185.231.245.50
 2 185.144.28.241
 1 92.61.148.10
 [...]
 1 103.57.195.147
```

3.3 Podpunkt 3

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

```
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

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

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

3.4 Podpunkt 4

W celu wyświetlenia listy lokalnych użytkowników użyłem polecenia:

```
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 lokalych na których było najwięcej prób ataku użyłem polecenia:

```
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

```
72 user-81
 11 user-25-jg
 10 user-25
  5 vermont
  4 arthur
  2 user-54
  2 user-5
  2 user-25-wb
  2 user-25-lg
  2 user-10
  1 yangxiong
```

```
      1 via.postal
      1 user-9
      1 user-76
      1 user-74
      1 user-72
      1 user-71
      1 user-56
      1 toiawase
      1 tim_osborn1
```

3.5.2 Wnioski

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

3.6 Podpunkt 6

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

```
grep "no host name found for IP address" final.log
grep "rejected RCPT" final.log
grep "rejected unknown sender" final.log
grep "message too big for system" final.log
grep "max connection rate exceeded" final.log
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‘:

```
2019-03-08 04:06:06 no host name found for IP address 185.222.209.78
2019-03-08 04:06:08 no host name found for IP address 185.222.209.78
2019-03-08 04:06:40 no host name found for IP address 185.222.209.78
2019-03-08 04:06:42 no host name found for IP address 185.222.209.78
2019-03-08 04:08:24 no host name found for IP address 185.222.209.78
[...]
2019-03-18 18:32:08 no host name found for IP address 10.0.0.92
2019-03-18 18:37:42 no host name found for IP address 10.0.0.92
2019-03-18 21:20:01 no host name found for IP address 185.222.209.202
2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
2019-03-19 00:47:53 no host name found for IP address 185.231.245.41
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‘:

```
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
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
```

```
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
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
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
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
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
[...]
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
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
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
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
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
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
2019-03-19 03:43:42 H=infinity16p.cf16.pl [94.177.240.244]
  F=<foreign-user-1768@financial-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 prawopodobnie jest wykorzystywany jako "open relay". Jednakże aby mieć pewność należałoby przeprowadzić analizę logów sieciowych na portach 25 i 587.