INTERESTING SSH ATTEMPTS

I have a small system I play with, nothing fancy. But even I have been noticing the increased level of ssh attempts. Previously in my backwater avenue of the internet such things rarely raised their head, but now. Now i see more and more of it. At first I thought just automated the blocking - easy enough. But as I saw more and more attempts, I found my curiosity raised. So I started tracking them. To see what I could see as the old rhyme goes. Now to put it in context, this is not a business line, I host no websites on this line and is only for this last month. And no, while these are not hordes upon hordes of attempts, they are more then i usually see. Lets see what we can see...

Lets first look for the source of these attempts. Well I use something similar to..

```
lastb -i | gawk '{ print $3 }'  | sort | uniq -c | wc -l
```

That gives me an answer of 368 uniq source ips. Damn. So, how many attempts does that equate to? I use something like..

```
lastb -i | gawk '{ print $3 }'  | wc -l
```

That gives me an answer of 368603. Alrighty then. So lets take a look at the heavy hitters, something like..

```
lastb -i | gawk '{ print $3 }'  | sort | uniq -c | sort -n
```

That gives me a long list that looks like...

```
.
.
<remove anything less then 900 attempts>
   912 207.36.196.104
    952 84.38.68.65
    968 95.174.160.147
    973 210.40.128.31
    986 117.21.248.100
   1016 61.187.64.8
   1018 200.11.190.106
   1042 64.237.103.145
   1044 196.46.252.10
   1044 72.14.182.81
   1044 80.86.201.29
   1061 121.14.144.217
   1061 62.212.66.84
   1133 128.107.79.64
   1142 219.143.251.37
   1153 219.140.253.199
   1208 221.232.131.51
   1234 85.21.206.18
   1402 195.56.77.54
   1510 211.20.38.246
   1541 61.51.18.121
   1598 83.209.13.4
   1603 58.180.45.71
   1648 158.109.64.191
   1648 202.100.108.22
   1648 95.131.89.114
   1660 218.1.73.102
   1670 141.85.254.152
   1677 67.55.73.244
   1722 61.128.110.217
   1762 202.99.122.230
   1856 159.226.208.105
   1999 200.24.4.69
   2095 221.130.180.178
   2287 114.108.128.76
   2371 203.255.251.34
   2718 202.44.47.125
   2949 118.129.166.149
   3122 193.136.39.26
   3129 203.169.48.6
   3266 61.242.253.93
   3592 61.189.16.38
   5031 67.202.25.223
   5110 212.69.111.22
   5171 222.68.194.69
   5265 67.212.92.67
   5339 196.22.230.245
   5449 64.191.12.6
   5476 61.176.218.17
   6306 121.124.127.76
   7064 207.248.163.76
   7253 122.41.175.118
   7604 64.5.39.39
   7629 221.238.193.71
   8345 117.21.246.164
   8964 61.152.169.68
   9432 125.206.243.126
  11959 60.195.250.54
  12653 94.155.49.93
  12766 206.212.240.251
  18109 83.170.92.31
  19079 122.33.194.148
  31598 77.51.250.130
  56406 61.158.205.231
```

That is quite something. Lets see if we can go a bit further, at software77.net you can enter in a group of addresses to get country listings, so lets do that..

```
94.155.49.93    # BG Bulgaria
67.212.92.67    # CA Canada
80.86.201.29    # CH Switzerland
221.238.193.71  # CN China
61.242.253.93   # CN China
61.152.169.68   # CN China
219.140.253.199 # CN China
61.158.205.231  # CN China
60.195.250.54   # CN China
117.21.246.164  # CN China
61.128.110.217  # CN China
61.187.64.8     # CN China
121.14.144.217  # CN China
202.99.122.230  # CN China
210.40.128.31   # CN China
```

```
222.68.194.69   # CN China
202.100.108.22  # CN China
61.51.18.121    # CN China
219.143.251.37  # CN China
61.189.16.38    # CN China
117.21.248.100  # CN China
221.232.131.51  # CN China
159.226.208.105 # CN China
61.176.218.17   # CN China
218.1.73.102    # CN China
221.130.180.178 # CN China
200.24.4.69     # CO Colombia
84.38.68.65     # DE Germany
196.46.252.10   # DZ Algeria
141.85.254.152  # EU European Union
158.109.64.191  # EU European Union
95.174.160.147  # FR France
83.170.92.31    # GB United Kingdom
195.56.77.54    # HU Hungary
125.206.243.126 # JP Japan
122.41.175.118  # KR Korea Republic of
203.255.251.34  # KR Korea Republic of
121.124.127.76  # KR Korea Republic of
58.180.45.71    # KR Korea Republic of
122.33.194.148  # KR Korea Republic of
114.108.128.76  # KR Korea Republic of
118.129.166.149 # KR Korea Republic of
203.169.48.6    # MN Mongolia
207.248.163.76  # MX Mexico
62.212.66.84    # NL Netherlands
193.136.39.26   # PT Portugal
77.51.250.130   # RU Russian Federation
95.131.89.114   # RU Russian Federation
85.21.206.18    # RU Russian Federation
212.69.111.22   # RU Russian Federation
83.209.13.4     # SE Sweden
202.44.47.125   # TH Thailand
211.20.38.246   # TW Taiwan; Republic of China (ROC)
64.237.103.145  # US United States
72.14.182.81    # US United States
64.5.39.39      # US United States
67.202.25.223   # US United States
206.212.240.251 # US United States
64.191.12.6     # US United States
128.107.79.64   # US United States
207.36.196.104  # US United States
67.55.73.244    # US United States
200.11.190.106  # VE Venezuela
196.22.230.245  # ZA South Africa
```

Interesting. The usual suspects appear as expected. China and neighboring areas, US, Russia. The 2 biggest source's come from Russia and China respectively. But no fear, I do not feel left out, there are many other parts of the world also having a go. Bear in mind these are just the heavy hitters. If I checked all the 'small fry' as well, I could well find others country's represented. Lastly, lets take a look at the top 20 most used accounts for these attempts, something like..

```
lastb | gawk '{ print $1 }' | sort | uniq -c | sort -n | tail -20
```

That gives me..

```
   726 web
    778 nagios
    786 backup
    796 toor
    812 testing
    816 www
    858 info
    896 webmaste
    936 temp
   1062 student
   1082 tester
   1344 administ
   1354 mysql
   2000 user
   2686 guest
   3682 a
   4406 oracle
   6463 test
   6856 admin
  54180 root
```

Boy, not shy about going for 'root' are they? But we do see that that most attempts seem to focus on system or application accounts. These accounts tend to be shared accounts, or generally viewed 'do not touch' or better yet 'someone else's problem'. So besides some fun for me, what does this show us?

1. If little old me is getting this type of traffic, imagine what bigger public companies are getting?
2. While there are definite hotbeds of scanning, it can still happen from everywhere. I mean ... Mongolia?
3. The bad guys do just scan the web. This is not a myth.
4. Check all parts of your system, all the accounts
5. Sometimes I just do not understand what they are trying... 2682 attempts on user 'a'? Is that a common user?

Final Words

I like numbers. Numbers and details help me put things into context. And context helps us make better choices. For example, just by not allowing root access you negate about 14% of the total attacks. To me, that sounds like a good investment in effort. And having these numbers also gives a baseline. If you change something -like the listening port- you can pull the numbers again and see if it made a difference. As always have fun and learn. As for me, I am going to think some more on this... what else can I do?