KØBENHAVNS UNIVERSITET

ITS - Assignment 6

Anders Friis Persson, Oliver Meulengracht og Mikkel Willén

1. november 2022

Indhold

Analysis of auth.log

We were tasked with analysing a file called auth.log. This file contains log data from a ssh server, which has been under attack.
Running the command "wc"in the terminal on the file, we get the following output:

```
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ wc auth.log
  11287  135886 1134054 auth.log
```

Figur 1: Output from running "wc"command on auth.log

We can see the file contains 11287 lines, is 135886 words long, as the size of the file is 1134054 bytes. If we take a look at the responses from the server:

```
Oct 23 19:13:02 cluster1 sshd[9105]: Invalid user alice from 109.196.143.60
Oct 23 19:13:02 cluster1 sshd[9105]: input_userauth_request: invalid user alice [preauth]
Oct 23 19:13:02 cluster1 sshd[9105]: pam_unix(sshd:auth): check pass; user unknown
Oct 23 19:13:02 cluster1 sshd[9105]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eui
d=0 tty=ssh ruser= rhost=109.196.143.60
Oct 23 19:13:04 cluster1 sshd[9105]: Failed password for invalid user alice from 109.196.143.60 port
 33717 ssh2
Oct 23 19:13:04 cluster1 sshd[9105]: Connection closed by 127.0.0.1 [preauth]
```

Figur 2: Example of the response from the server to 1 instance of the attack

we can see, that the length of a response in lines are 6. This means that the attack has tried to log in:

$$\frac{11287}{6} \approx 1880$$

times. This seems to indicate, that the attack was done by a program, and not a person trying to guess passwords. Another indicater of this is, that the first login attempt was at 19:13:02 and the last was at 20:40:10, which means an attempted login once every 2 seconds roughly.
Using grep and searching for possible terms indicating a valid login we got the following output:

```
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep success auth.log
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep Success auth.log
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep " valid " auth.log
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep " Valid " auth.log
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep accept auth.log
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep Accept auth.log
Oct 23 20:31:07 cluster1 sshd[18327]: Accepted password for tom from 109.196.143.60 port 35901 ssh2
```

Figur 3: Grep showing a successful login

Running the following command, we can count the number of occurences of the IP address:

```
(base) mikkel@mikkel:~/Dokumenter/ITS/assignment6$ grep -o -i 109.196.143.60 auth.log | wc -l
6167
```

Figur 4: The number of occurences of the IP address

and we can see the IP address was in the file 6167 times, which makes it clear, that the successful login came from the attack, and not from a user trying to log in at the same time the attack was ongoing.
We can therefore conclude, that the attack was successful and, the attack has access to the SSH server.

Protecting the SSH server

Skifte passwords Lukke serveren midlertidigt

timeout, hvis man har forsøgt for mange gange sådan en "im not a robot"tingeling Begrænsninger på, hvem der kan ssh til serveren

Short questions

1.

2.

3.

4.