Authentication Events

## Summary

This lab investigates the SSH log from an AWS based Linux system exposed to the internet. Both passwords and private key logins were enabled.

The system owner’s public IPv4 address was 23.244.198.127. You will see both successful and failed logins from that address for setup, testing, and monitoring. All other public addresses are considered hostile.

Your investigation should answer the following questions:

1. What user accounts were successfully accepted?
2. How long was the system up before the first attempted attack?
3. How many failed login attempts?
4. What IP address generated the most attacks?
5. What ISP generated the most attacks?
6. What country generated the most attacks?
7. What was the most popular user name to attack?
8. Who successfully logged into the system?
9. Were any attacks successful? If so, provide details.
10. Any trends or other insights seen in the log?

## Tools/Resources

Parrot

Labs assume Parrot OS running on VirtualBox.

## Walkthrough

Download from Canvas files the ssh\_events.log file. It was generated using the command “journalctl -u sshd.service > ssh\_events.log”. Then transferred to Canvas using SCP and HTTPS.

1. What user accounts were successfully accepted?

grep Accept ssh\_events.log | awk '{print $9}' | sort -g | uniq -c | sort -g

4 ec2-user

4 kmh722

1. How long was the system up before the first attempted attack?

# The first line will tell when ssh started:

head -1 ssh\_events.log | awk '{print $1, $2, $3}'

Aug 05 20:38:06

# Discard the “safe” traffic from 23.244.198.127

grep -v "23.244.198.127" ssh\_events.log | grep Failed >ssh\_attacks.log

# Discard the “invalid user” tag for consistent columns in log

sed -i 's/invalid user //g' ssh\_attacks.log

# View the first failure (this assumes no successful attacks)

grep Failed ssh\_attacks.log | head -1 | awk '{print $1, $2, $3}'

Aug 05 20:54:30

START=`date -d "Aug 05 20:38:06" +%s`

STOP=`date -d "Aug 05 20:54:30" +%s`

COUNT=$((STOP-START))

echo $COUNT

984

1. How many failed login attempts?

grep Failed ssh\_events.log | wc

389 5914 55173

1. What IP address generated the most attacks?

cat ssh\_attacks.log | awk '{print $11}' | sort -g | uniq -c | sort -g | tail -1

30 183.82.126.193

1. What ISP generated the most attacks?

grep Failed ssh\_attacks.log | awk '{print $11}' > ip\_count

awk '{print $1}' ip\_count | while read ip; do code=`curl -s ipinfo.io/$ip | jq -r ".org"`; echo "$code"; done > isp

cat isp | sort -g | uniq -c | sort -g

2 AS6167 Verizon Business

3 AS136170 PT. EXABYTES NETWORK INDONESIA

4 AS139293 UFO Network Limited

5 AS16509 Amazon.com, Inc.

6 AS137718 Beijing Volcano Engine Technology Co., Ltd.

6 AS45090 Shenzhen Tencent Computer Systems Company Limited

7 AS12874 Fastweb SpA

8 AS135377 UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED

10 AS9269 Hong Kong Broadband Network Ltd.

11 AS36947 Telecom Algeria

13 AS45117 Ishan's Network

14 AS398101 GoDaddy.com, LLC

15 AS13335 Cloudflare, Inc.

19 AS10796 Charter Communications Inc

29 AS58563 CHINANET Hubei province network

30 AS138133 Universitas Muslim Indonesia

30 AS18209 Atria Convergence Technologies pvt ltd

30 AS38283 CHINANET SiChuan Telecom Internet Data Center

30 AS4766 Korea Telecom

33 AS4134 CHINANET-BACKBONE

77 AS14061 DigitalOcean, LLC

1. What country generated the most attacks?

grep Failed ssh\_attacks.log | awk '{print $11}' > ip\_count

awk '{print $1}' ip\_count | while read ip; do code=`curl -s ipinfo.io/$ip | jq -r ".country"`; echo "$code"; done > countries

cat countries | sort -g | uniq -c | sort -g

7 IT

11 DZ

13 AU

15 TW

18 DE

18 SG

22 HK

30 KR

33 ID

43 IN

68 US

104 CN

1. What was the most popular user name to attack?

cat ssh\_attacks.log | awk '{print $9}' | sort -g | uniq -c | sort -g | tail -1

root

1. Did any attack attempt using a SSH key?

cat ssh\_attacks.log | awk '{print $7}' | sort -g | uniq -c | sort -g

382 password

1. Were any attacks successful? If so, provide details.

grep -v "23.244.198.127" ssh\_events.log | grep Accepted | awk '{print $11}' | sort -g | uniq -c | sort -g

1 172.31.32.156

1 18.116.199.236

1. Any trends or other insights seen in the log?

## Submission

Upload to Canvas a docx or pdf containing the answers to the questions.

## Additional Thoughts

Should the successful login from address 172.31.32.156 be considered an attack? It is a private address. Does that make it safe?