Activity III: Log Analysis

By Saenyakorn Siangsanoh 6232035721

Table of Contents

Part I Can you find people trying to break into the servers?

Q1

How many hackers are trying to get access to our servers? And how many attempts are there? Explain/define how you count distinct hackers.

Answer

Service	Distinct IP	Attempt count
All	182	33,069
mailsv	175	8,111
www1	177	8,746
www2	176	7,992

Service	Distinct IP	Attempt count
www3	173	8,220

จากตารางข้างต้นสามารถหาได้จาก การหาจากไฟล์ `tutorialdata.zip:./*/secure.log` ทั้งหมดแล้ว filter ด้วยคำว่า `Failed` จากนั้นพยายามนับ Distinct IP ทั้งหมด

นอกจากนี้ ผู้เขียนยังสงสัยว่าจะมี IP ไหนที่เป็น user จริง ๆ หรือเปล่า จึงได้ลองหาดูด้วยกระบวนการคล้าย ๆ กัน คือ filter ด้วยคำว่า `Accepted` เพื่อหาว่ามี IP ไหน login สำเร็จบ้างซึ่งมีทั้งหมด 3 IP ดังนี้

1. `10.1.10.172` - `myuan`
2. `10.2.10.163` - `nsharpe`
3. `10.3.10.46` - `djohnson`

ซึ่งพบว่าแม้ว่าทั้ง 3 IP จะใส่ password ผิดเยอะมาก แต่ทั้ง 3 IP ก็สามารถเข้า Account ของตัวเองได้สำเร็จเยอะเช่นกัน และเข้าเพียงแค่ 1 Account เท่านั้น ดังนั้นจึงสรุปว่า IP ทั้ง 3 เป็นผู้ใช้จริง ๆ

Q2

What time do hackers appear to try to hack our servers?

Answer

พบว่า Service ทั้งหมดมีร่องรอยของ Hacker ในการพยายามจะ login เข้า server ทั้งหมด 8 วัน ตั้งแต่วันที่ 22 - 29 สิงหาคม 2022 ในเวลาเดียวกันของทุกวัน เป็นระยะเวลาหนึ่ง

- 12:15:02 AM
- 12:15:03 AM
- 12:15:05 AM
- 12:15:06 AM

Q3

Which server (mailsv, www1, www2, www3) sees the most attempts?

Answer

Service	Distinct IP	Attempt count
All	182	33,069
mailsv	175	8,111
www1	177	8,746
www2	176	7,992
www3	173	8,220

จากตารางข้างต้น พบว่า แต่ละ service ก็โดนโจมตีด้วยจำนวนครั้งที่ไม่ต่างกันมาก แต่ `www1` จะโดนเยอะมากที่สุด

Q4

What is the most popular account that hackers use to try to break in?

Answer

User	Attempt count
root	1493
mail	753
games	601
daemon	520
sync	487
nagios	462
nobody	442
squid	403
apache	336
jira	315
news	312
ncsd	294
backup	282
bin	259
ftp	218
jboss	215
gopher	202
djohnson	121
sneezy	84
ftpuser	83
cher	81
doc	81
madonna	81
sleepy	79
happy	76
queasy	76
beyonce	72

User	Attempt count
dopey	71
edgy	71
peevish	70
britany	69
remorseful	69
bashful	68
dizzy	68
grumpy	68
prince	68
hammer	66
surly	63
nsharpe	47
myuan	16

ตารางข้างต้นแสดงถึงจำนวนครั้งที่ Hacker พยายามจะ login ไปยัง user นั้น ซึ่งจะนับเฉพาะ user ที่มีในระบบเท่านั้น ดังนั้น user ที่มีการพยายามเข้าถึงมากที่สุดคือ root

Part II Sensitive Files on Web Servers

Q5

Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?

Answer

พบว่า Sensitive information มีดังนี้

- `/hidden/anna_nicole.html`
- `/passwords.pdf`

Path	Attempt count
/hidden/anna_nicole.html	73
/passwords.pdf	68

แต่ทั้งนี้ทั้งนั้น hacker ไม่ได้รับข้อมูลอะไรกลับไป เพราะ web server ได้ทำการ response HTTP code 404 NOT FOUND กลับไปให้

Q6

What resource/file are hackers looking for?

Answer

ข้อมูลความลับของ Anna Nicole Smith จาก path `/hidden/anna_nicole.html`

และข้อมูล passwords ของระบบจาก `/passwords.pdf`

Part III Are there bots crawling our websites?

Q7

Can you find any bots crawling our websites?

Answer

พบว่ามีการ crawler bot ที่มีชื่อว่า `Googlebot/2.1` ของ Google

Q8

What are they doing on the site? (Hint: Look for User-Agent in the web `access.logs`.)

Answer

`Googlebot/2.1` จะทำการ discover และ scan website ตามลิงก์ที่แปะอยู่ในเว็บ เพื่อให้เว็บไซต์ของเราขึ้นบน Google Search