Mokha Lerthsuwanroj 6331339421

**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.**

A screenshot of a computer

Description automatically generated

source="tutorialdata.zip:\*\secure.log" password\_status="failed password" (ip="\*.\*.\*.\*" OR invalid\_user\_ip="\*.\*.\*.\*")

| stats count by ip

| where count > 10

**ANS:** 185 hackers with 33,179 attempts. Assume that hackers tried more than 10 times to login with any password. So, query status “Failed password” with ip count more than 10 both valid and invalid user.

**Q2. What time do hackers appear to try to hack our servers?**

**A screenshot of a computer

Description automatically generated**

source="tutorialdata.zip:\*\secure.log" password\_status="failed password" (ip="\*.\*.\*.\*" OR invalid\_user\_ip="\*.\*.\*.\*")

| stats count by time

| sort count DESC

**ANS:** Mostly attempts on “Sun Aug 16 2023 18:06:30”

**Q3. Which server (mailsv, www1, www2, www3) sees the most attempts?**

**A screenshot of a computer

Description automatically generated**

source="tutorialdata.zip:\*\secure.log" password\_status="failed password" (ip="\*.\*.\*.\*" OR invalid\_user\_ip="\*.\*.\*.\*")

| stats count by time

| sort count DESC

**ANS:** “www1” with 8780 attempts

**Q4. What is the most popular account that hackers use to try to break in?**

**A screenshot of a computer

Description automatically generated**

source="tutorialdata.zip:\*\secure.log" password\_status="failed password" (ip="\*.\*.\*.\*" OR invalid\_user\_ip="\*.\*.\*.\*") user!="invalid"

| stats count by user

| sort count DESC

**ANS:** “root” with 1493 attempts

**Q5. Can you find attempts to get access to sensitive information from our web servers? How many attempts were there?**

**A screenshot of a computer

Description automatically generated**

source="tutorialdata.zip:\*\access.log" (status="403" OR status=”404”)

| stats count by path

**ANS:** “/hidden” and “/passwords.pdf” seems to be the path to the sensitive information. Then query including error status 403 which means URL restriction or error status 404 which means URL not found, sum up within 141 attempts in total.

**Q6. What resource/file are hackers looking for?**

**ANS:** “/hidden/anna\_nicole.html” and “/passwords.pdf”

**Q7. Can you find any bots crawling our websites?**

**A black and grey striped background

Description automatically generated**

source="tutorialdata.zip:\*\access.log" useragent="\*bot\*"

| stats count by useragent

**ANS:** Yes, as we can see the “Googlebot” and “YandexBot” from the query above.

**Q8. What are they doing on the site?**

**A black and grey striped background

Description automatically generated**

source="tutorialdata.zip:\*\access.log" useragent="\*bot\*" action="action=\*"

| stats count by action

| sort count DESC

**ANS:** They mostly “addtocart” with 223 attempts