Laboratorium 1

Karol Słomczynski 272223

2024-03-19

1 Zadanie 1

1.1 Podpunkt 1

```bash
#!/bin/bash
echo "Z1.1"
grep "Failed" -c secure
grep "Failed" -c secure.1
echo "Z1.2"
grep "Failed" secure | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq -c | sort -nr | uniq | head -n 30
grep "Failed" secure.1 | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq -c | sort -nr | uniq | head -n 30
echo "Z1.3"
grep "Failed" secure | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq | xargs -I{} geoiplookup {} | sort | uniq -c | sort -nr | head -n 10
grep "Failed" secure.1 | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | uniq | xargs -I{} geoiplookup {} | sort | uniq -c | sort -nr | head -n 10
echo "Z1.4"
grep 'Failed' secure | awk '{print $9,$11}' | awk '{if ($1 == "invalid") {print $2} else if (match($1, /^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/)) {print $1}}' | sort | uniq -c | sort -nr | head -n 20
grep 'Failed' secure.1 | awk '{print $9,$11}' | awk '{if ($1 == "invalid") {print $2} else if (match($1, /^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/)) {print $1}}' | sort | uniq -c | sort -nr | head -n 20
echo "Z1.5"
```

```
    grep 'Accepted' secure | awk '{print $9}' | sort | uniq -c
    grep 'Accepted' secure.1 | awk '{print $9}' | sort | uniq -c

    echo "Z2.1"
    grep "login authenticator failed" final.log -c
    echo "Z2.2"
    grep "login authenticator failed" final.log | grep -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' -o | sort | uniq -c | sort -nr
    echo "Z2.3"
    grep "login authenticator failed" final.log | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | xargs -I{} geoiplookup {} | sort | uniq -c | sort -nr | head -n 10
    echo "Z2.4"
    grep "R=localuser" final.log | cut -d ' ' -f 5 | cut -d "@" -f 1 | sort | uniq | sort -t "-" -k 2 -n
    echo "Z2.5"
    grep "login authenticator failed" final.log | grep -v "@" | awk '{print $NF}' | cut -d '=' -f 2 | cut -d ')' -f 1 | sort | uniq -c | sort -nr | head -n 20
    echo "Z2.6"
    grep "no host name found for IP address" final.log
    grep "rejected RCPT" final.log
    grep "rejected unknown sender" final.log
    grep "message too big for system" final.log
    grep "max connection rate exceeded" final.log
    grep "authentication failed" final.log

```