Assignment 07

Linux os & scripting – b keerthana

AMRUTHESH

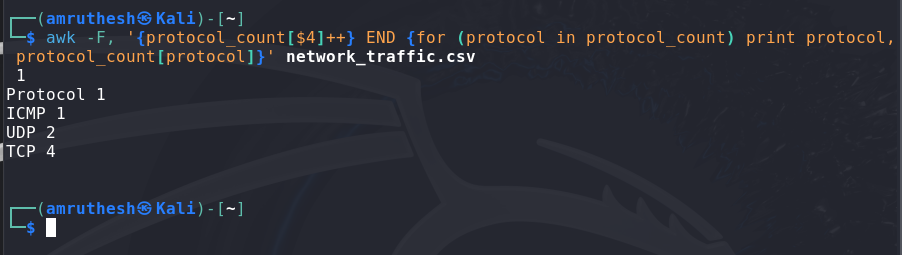
241059041

M.E – Cyber Security

MSIS, MANIPAL

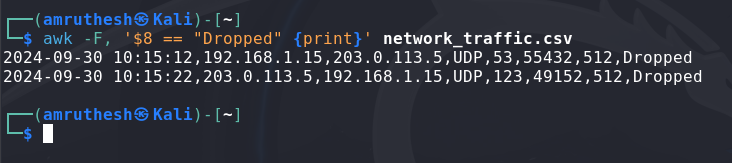
**1. Count how many packets use each protocol (TCP, UDP, ICMP)**

awk -F, '{protocol\_count[$4]++} END {for (protocol in protocol\_count) print protocol, protocol\_count[protocol]}' network\_traffic.csv



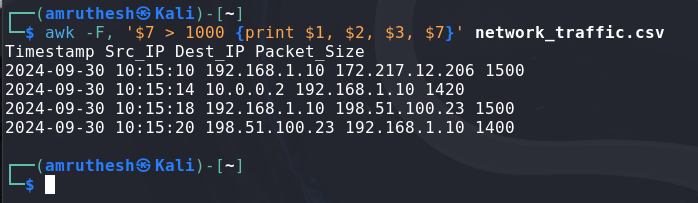
**2. Filter and print only the dropped packets.**

awk -F, '$8 == "Dropped" {print}' network\_traffic.csv



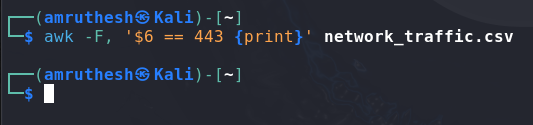
**3. Print the Timestamp, Source\_IP, Destination\_IP, and Packet\_Size for packets with** **size > 1000 bytes.**

awk -F, '$7 > 1000 {print $1, $2, $3, $7}' network\_traffic.csv



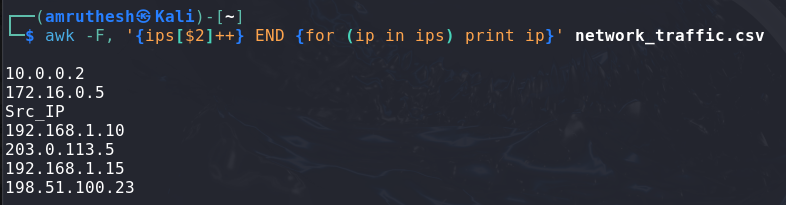
**4. Display traffic directed to destination port 443.**

awk -F, '$6 == 443 {print}' network\_traffic.csv



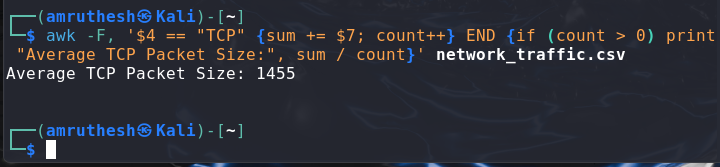
**5. Print all unique Source\_IP addresses.**

awk -F, '{ips[$2]++} END {for (ip in ips) print ip}' network\_traffic.csv



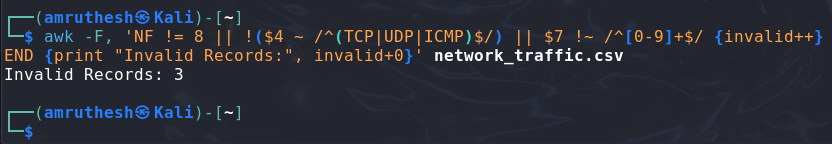
**6. Filter only TCP traffic and calculate the average packet size.**

awk -F, '$4 == "TCP" {sum += $7; count++} END {if (count > 0) print "Average TCP Packet Size:", sum / count}' network\_traffic.csv



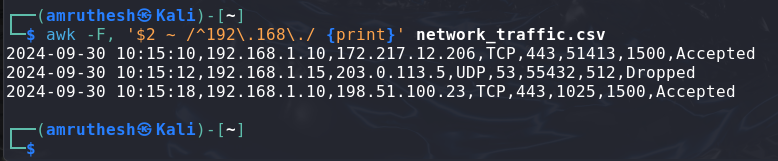
**7. Count invalid records (missing or malformed fields).**

awk -F, 'NF != 8 || !($4 ~ /^(TCP|UDP|ICMP)$/) || $7 !~ /^[0-9]+$/ {invalid++} END {print "Invalid Records:", invalid+0}' network\_traffic.csv



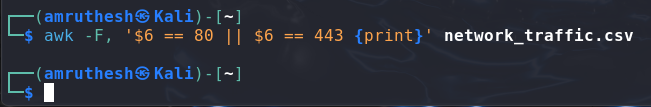
**8. Extract and print rows where Source\_IP is in the 192.168.x.x range.**

awk -F, '$2 ~ /^192\.168\./ {print}' network\_traffic.csv



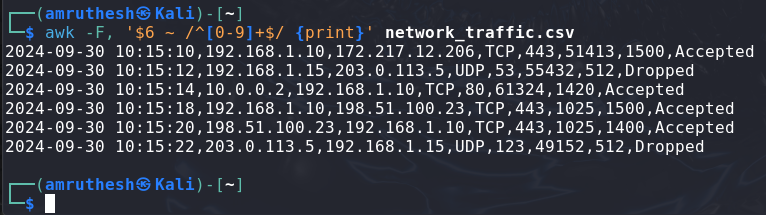
**9. Match traffic directed to either port 80 (HTTP) or port 443 (HTTPS).**

awk -F, '$6 == 80 || $6 == 443 {print}' network\_traffic.csv



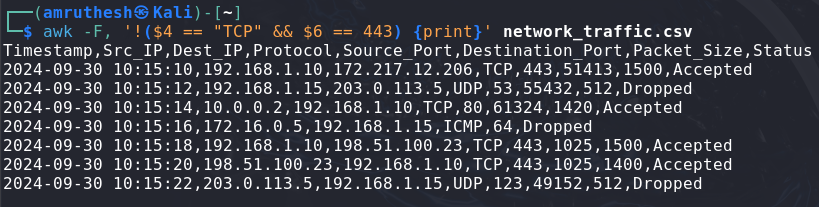
**10. Filter out rows where the Destination\_Port contains any alphanumeric characters.**

awk -F, '$6 ~ /^[0-9]+$/ {print}' network\_traffic.csv



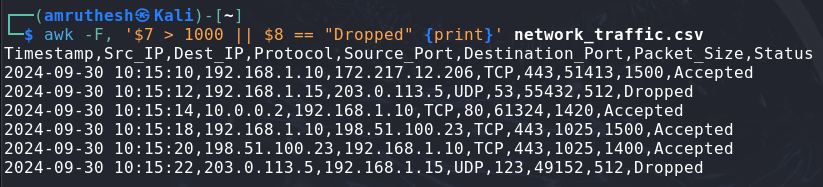
**11. Filter out traffic where the protocol is TCP AND the destination port is 443.**

awk -F, '!($4 == "TCP" && $6 == 443) {print}' network\_traffic.csv



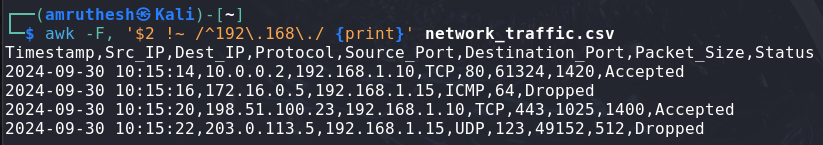
**12. Filter out and print traffic where the Packet\_Size is > 1000 OR the Status is Dropped.**

awk -F, '$7 > 1000 || $8 == "Dropped" {print}' network\_traffic.csv



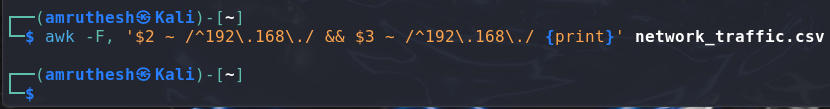
**13. Print traffic NOT originating from 192.168.x.x IP addresses.**

awk -F, '$2 !~ /^192\.168\./ {print}' network\_traffic.csv



**14. Filter rows where both Source\_IP and Destination\_IP are within the 192.168.x.x range.**

awk -F, '$2 ~ /^192\.168\./ && $3 ~ /^192\.168\./ {print}' network\_traffic.csv



**15. Filter out traffic where the destination port is 22 OR the packet size is less than 100** **bytes.**

awk -F, '!($6 == 22 || $7 < 100) {print}' network\_traffic.csv

