**Splunk Queries**

1. **Total Failed SSH Login Attempts**

source="secure.log" "Failed password"

1. **Top Attacking IP Addresses**

source="secure.log" "Failed password" | top src

1. **All Targeted Failed Usernames**

source="secure.log" "Failed password" | top user

1. **Geographic Location of Attackers**

source="secure.log" "Failed password" | iplocation src | top Country

1. **Successful SSH Logins by User and IP**

source="secure.log" "Accepted password" | stats count by user, src

1. **Failed Login Attempts Over 48 Hours**

source="secure.log" "Failed password" | timechart span=2d count

1. **Geolocation of All Incoming Requests**

source="secure.log" | iplocation src | top Country

1. **Login Attempts by Hour of Day**

source="secure.log" | eval hour=strftime(\_time,"%H") | stats count by hour

1. **IPs Targeting Multiple Usernames**

source="secure.log" "Failed password" | stats dc(user) as unique\_users by src

1. **Users with Both Failed and Successful Logins**

source="secure.log" ("Failed password" OR "Accepted password") | stats count by user