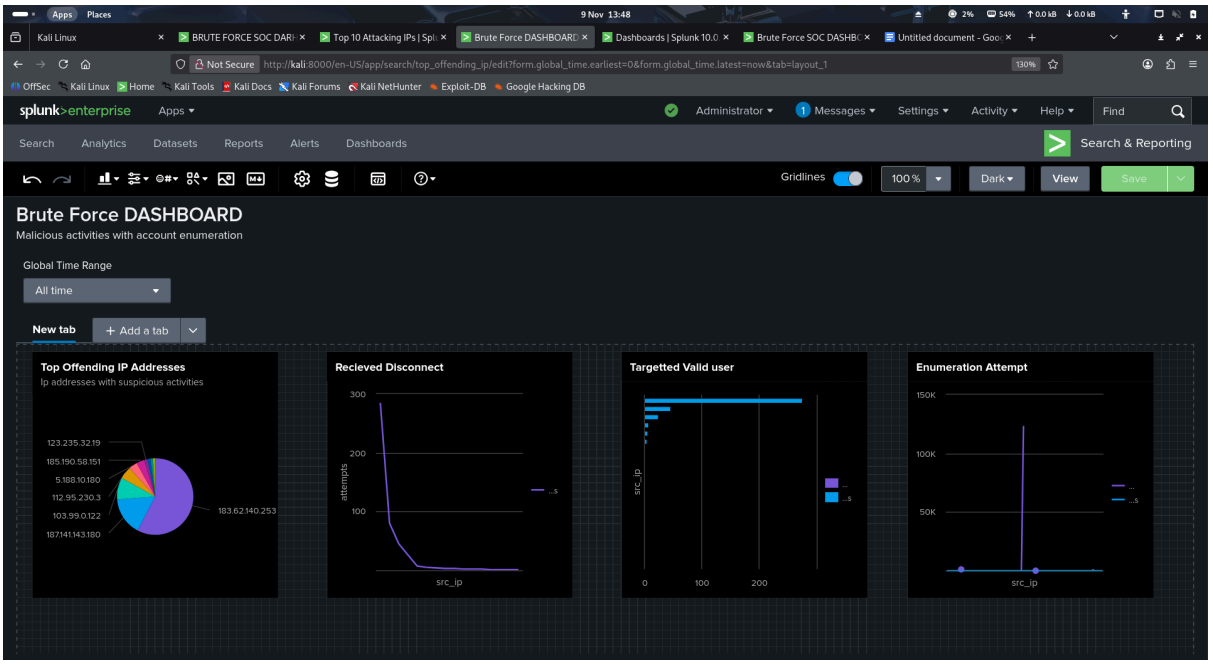
Brute-Force Detection Lab

Tool: Splunk Cloud (14-day trial)
Dataset: Simulated Windows logs (2000+ failed events)
Key Findings:
- Top attacker: 183.62.140.253 (286 failures)
- Peak: 10:00am–11:04am (286 attempts)
- Alert: Triggers on >50 fails/IP

Dashboard:


SPL Rule: source="OpenSSH.csv" index="openssh" "Failed password"
| rex field=_raw "from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3}) port"
| stats count as attempts by src_ip
| sort -attempts
| head 10
|where count > 50