New Search

```
1  index=botsv2 sourcetype=wineventlog:security EventCode=4625 earliest=0
2  | eval user=coalesce(TargetUserName, Account_Name, AccountName, SubjectUserName, user, User)
3  | eval src_ip=coalesce(IpAddress, SourceNetworkAddress, Source_Network_Address, src_ip, src,
       clientip)
4  | eval user=if(isnull(user) OR user="" OR user="-", "unknown_user", user)
5  | eval src_ip=if(isnull(src_ip) OR src_ip="" OR src_ip="-", "unknown_ip", src_ip)
6  | stats count as fails by user, src_ip
7  | sort - fails
8  | head 20
```

Time range: All time

✓ **3,340 events** (before 12/26/25 8:13:10.000 AM) No Event Sampling

Statistics (9)

user	src_ip	fails
unknown_user	10.0.1.100	3162
Administrator	10.0.1.220	109
MERCURY$	10.0.1.220	109
Guest	unknown_ip	53
administrator	unknown_ip	53
unknown_user	172.16.0.1	14
VENUS$	127.0.0.1	1
administrator	127.0.0.1	1
unknown_user	unknown_ip	1