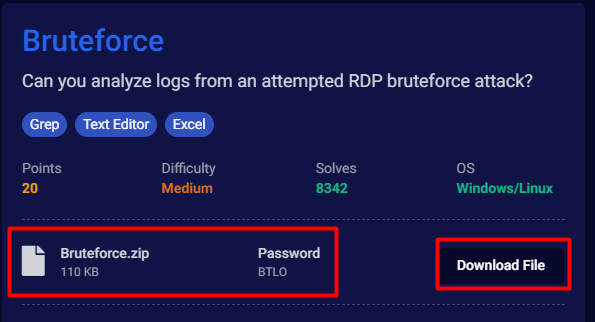
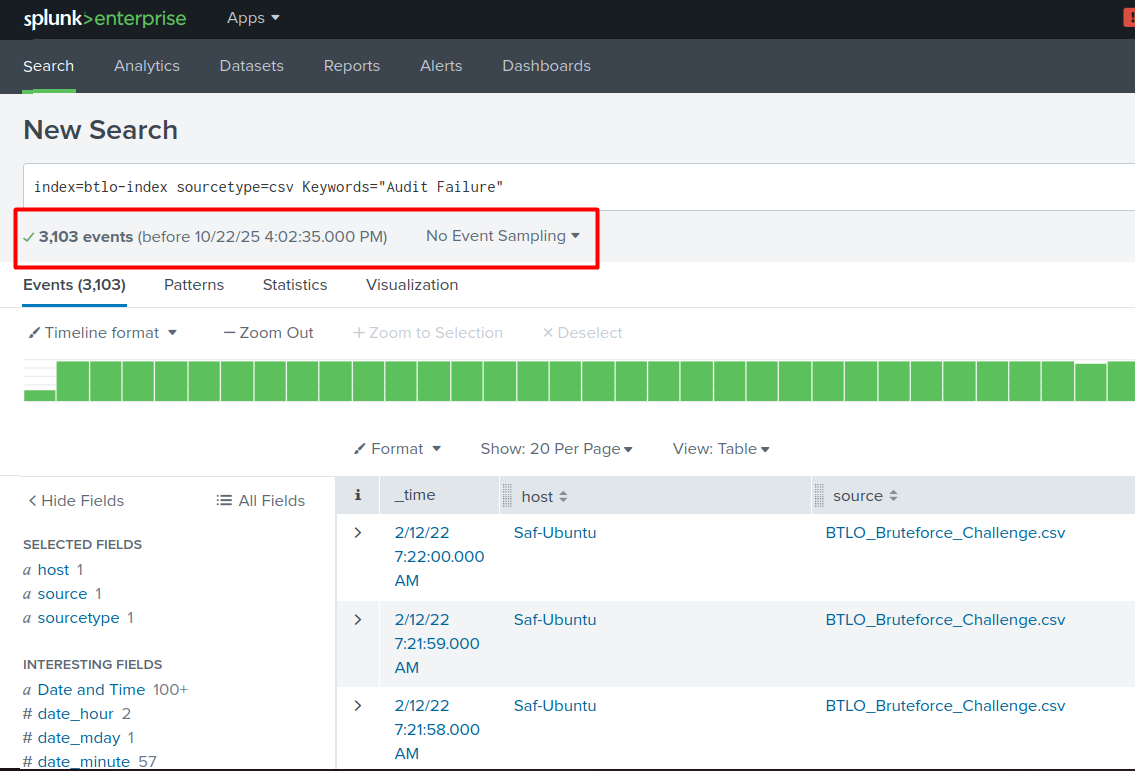
**Challenge URL:** <https://blueteamlabs.online/home/challenge/bruteforce-16629bf9a2>

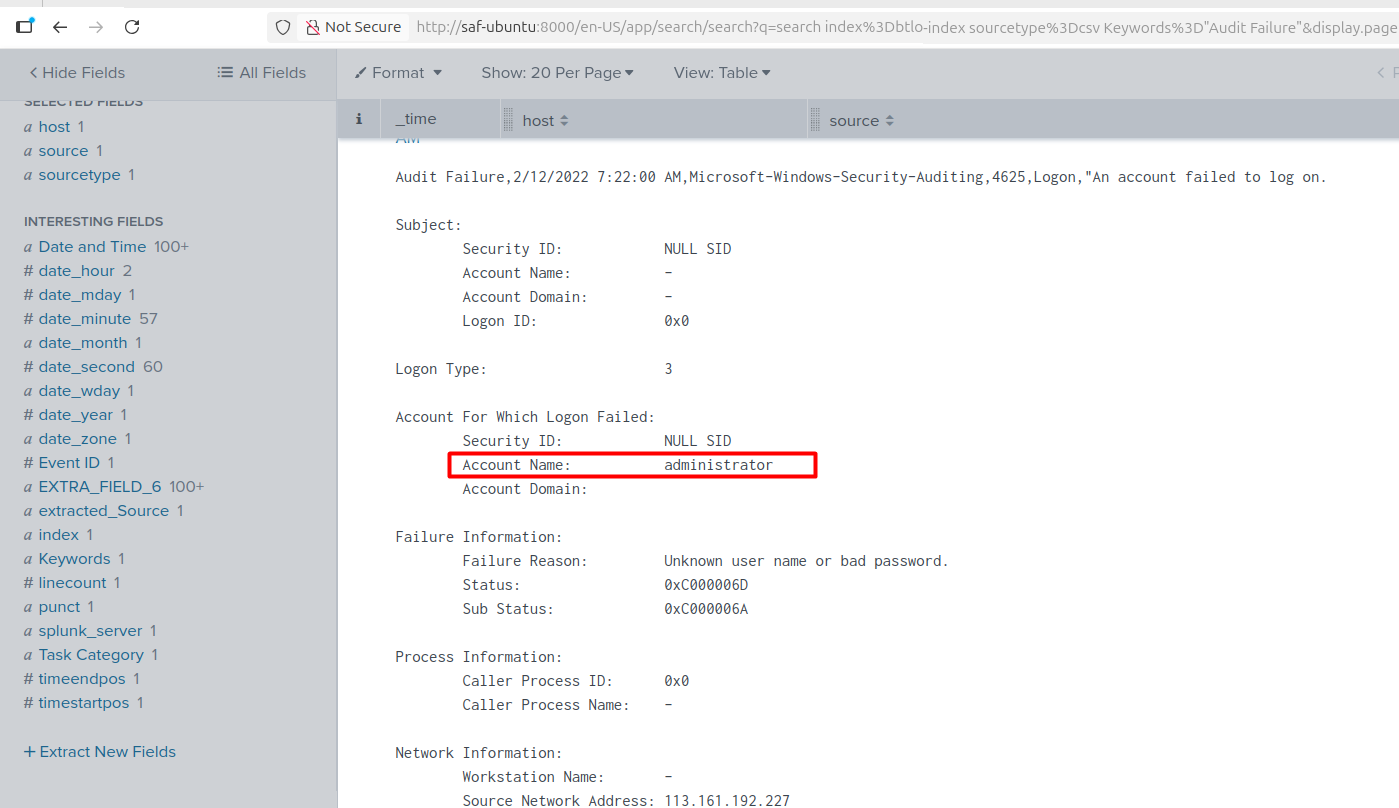


**Download the zip file to analyze the log file.**

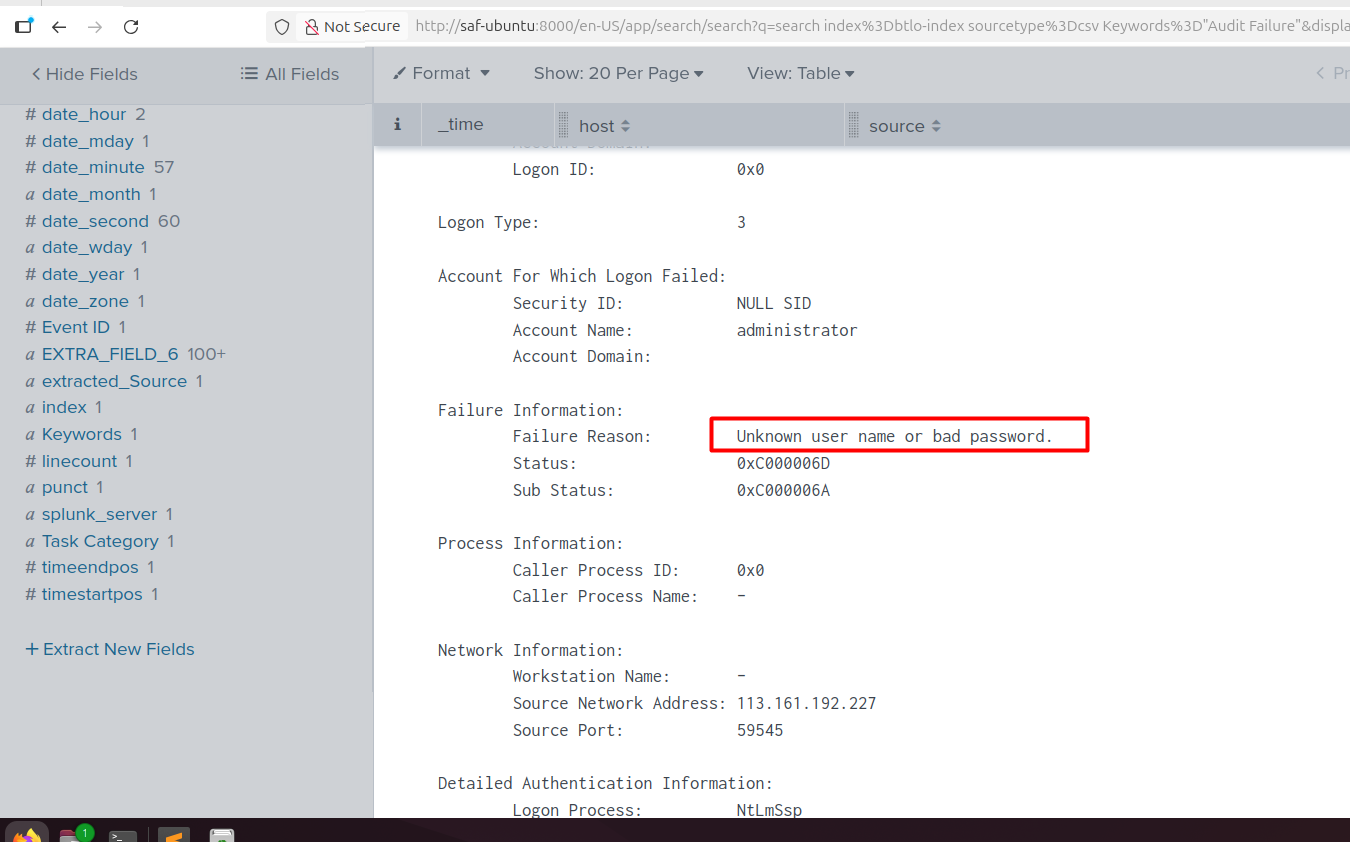
**Question 1) How many Audit Failure events are there? (Format: Count of Events)**



**Question 2) What is the username of the local account that is being targeted? (Format: Username)**



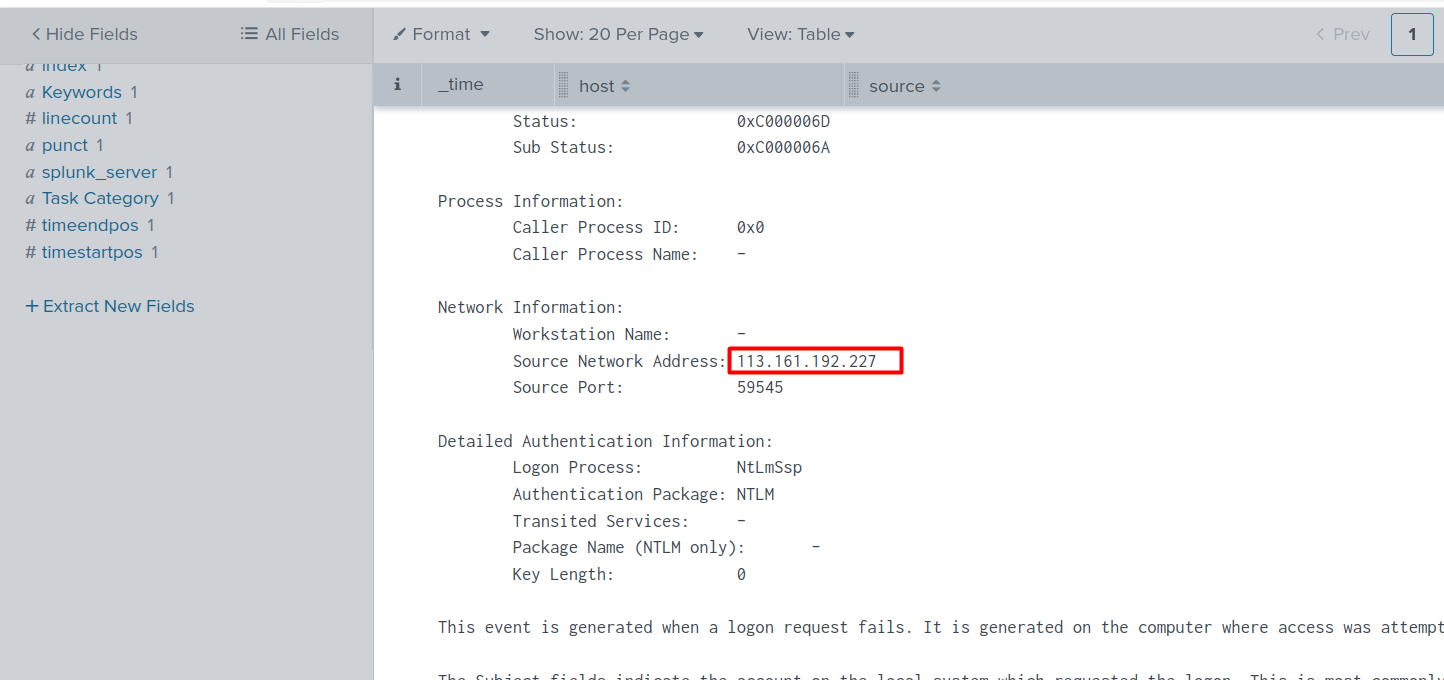
**Question 3) What is the failure reason related to the Audit Failure logs? (Format: String)**



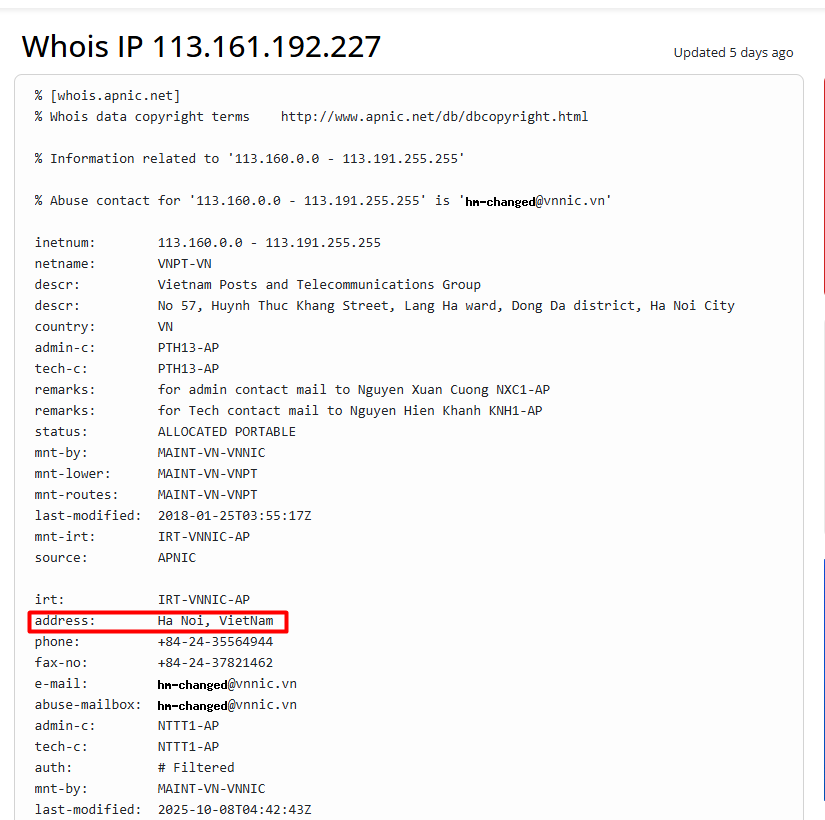
**Question 4) What is the Windows Event ID associated with these logon failures? (Format: ID)**



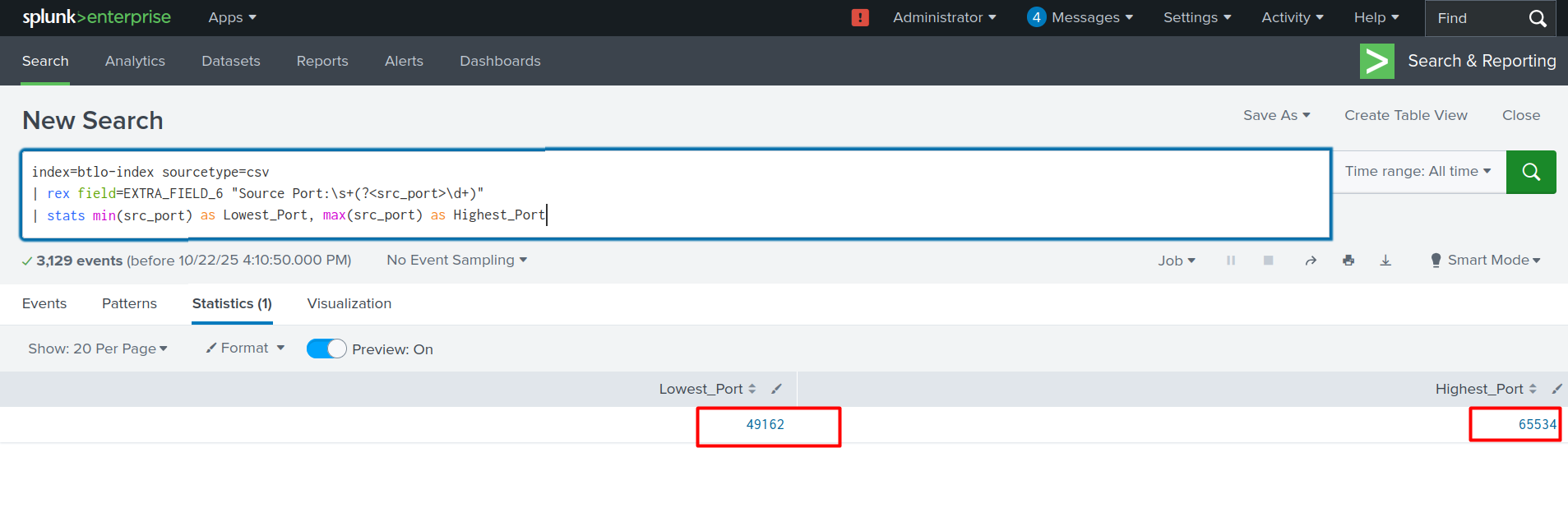
**Question 5) What is the source IP conducting this attack? (Format: X.X.X.X)**



**Question 6) What country is this IP address associated with? (Format: Country)**



**What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)**



**To see the lowest and highest port**

index=btlo-index sourcetype=csv

| rex field=EXTRA\_FIELD\_6 "Source Port:\s+(?<src\_port>\d+)"

| stats min(src\_port) as Lowest\_Port, max(src\_port) as Highest\_Port

**To see all the ports with event**

index=btlo-index sourcetype=csv

| rex field=EXTRA\_FIELD\_6 "Source Port:\s+(?<src\_port>\d+)"

| table \_time src\_port host source

**Country Extraction and visualization**

index=btlo-index sourcetype=csv

| rex field=EXTRA\_FIELD\_6 "Source Network Address:\s+(?<src\_ip>\d{1,3}(?:\.\d{1,3}){3})"

| iplocation src\_ip

| stats count by Country

| sort -count

**With Username and success failure**

index=btlo-index sourcetype=csv

| eval Status=if(match(EXTRA\_FIELD\_6, "An account failed to log on"), "Failure", "Success")

| rex field=EXTRA\_FIELD\_6 "Account Name:\s+(?<username>\S+)"

| stats count by Status, username

| sort - count