Splunk Use Cases with Solutions

# 1. Detection of Repeated Access from a Suspicious IP

Condition: More than 10 connections from the same external source IP within 5 minutes.  
Splunk Query:  
index=firewall\_logs "Log comp"="Firewall Rule"  
| stats count by "Src IP", span=5m  
| where count > 10

# 2. Access to Restricted Ports

Condition: Traffic to restricted or non-standard destination ports (e.g., 21, 23, 3389).  
Splunk Query:  
index=firewall\_logs "Dst port" IN (21, 23, 3389)  
| stats count by "Dst port", "Dst IP", "Src IP"

# 3. Firewall Rule Mismatch

Condition: NAT rule present but Firewall rule is missing.  
Splunk Query:  
index=firewall\_logs  
| where isnull("Firewall rule") AND isnotnull("NAT rule")

# 4. Multiple NAT Rule Hits

Condition: NAT rule hit more than 50 times in a day.  
Splunk Query:  
index=firewall\_logs  
| stats count by "NAT rule name"  
| where count > 50

# 5. Traffic from Blacklisted IP Ranges

Condition: Traffic from IPs in known blacklisted ranges (e.g., 45.147.66.0/24).  
Splunk Query:  
index=firewall\_logs  
| where like("Src IP", "45.147.66.%")

# 6. Incomplete Log Entry Detection

Condition: Missing values in critical fields like Firewall rule, Out interface.  
Splunk Query:  
index=firewall\_logs  
| where isnull("Firewall rule") OR isnull("Out interface")

# 7. Protocol Misuse Detection

Condition: Uncommon protocol usage (non-TCP/UDP).  
Splunk Query:  
index=firewall\_logs  
| where NOT protocol IN ("TCP", "UDP")

# 8. High Volume Traffic to Specific Destination

Condition: More than 100 hits to a specific destination IP within 30 minutes.  
Splunk Query:  
index=firewall\_logs  
| stats count by "Dst IP", span=30m  
| where count > 100

# 9. Unusual Internal to External Access

Condition: Internal IP accessing many new external IPs.  
Splunk Query:  
index=firewall\_logs  
| stats dc("Dst IP") as distinct\_dst by "Src IP"  
| where distinct\_dst > 10

# 10. Same Source Port Reuse Across Sessions

Condition: Same source port used for multiple destination IPs.  
Splunk Query:  
index=firewall\_logs  
| stats dc("Dst IP") as dst\_count by "Src port"  
| where dst\_count > 1