Windows Server Brute Force Attempts (Elastic SIEM Lab Report)

Summary

An internet-exposed Windows server was monitored using the Elastic Stack (ELK) with endpoint log collection enabled. During the last 30 days, the server generated a high volume of failed authentication events consistent with brute-force and username-spraying activity. The attacks primarily targeted common administrative usernames (e.g., Administrator/admin) and originated from multiple external IP addresses across different countries.

Successful authentication events were minimal and attributable to known/expected access (analyst activity). No evidence of successful attacker authentication was identified within the reviewed time window based on available logs.

Lab Environment

Purpose: SOC-style detection and analysis of brute-force authentication attempts against a Windows server exposed to the internet.

Components:

- **Windows Server:** Internet-exposed test host (logged as agent.name = Windows-Server)
- **Elastic Stack:** Elasticsearch + Kibana (Security Solution)
- **Data Sources:** Windows Security Event Logs collected into Elastic

Time Range Analyzed: Last 30 days (as configured in Kibana)

Data Sources and Log Coverage

This investigation relied on Windows Security logs, primarily:

- **Event ID 4625** — Failed logon
- **Event ID 4624** — Successful logon

Logon type was used to help interpret authentication context:

- **LogonType 3** — Network logon (commonly SMB / network authentication)
- **LogonType 7 — Unlock** (user unlocks an existing local/interactive session; not a new remote login)
- **LogonType 10** — RemoteInteractive (commonly RDP)

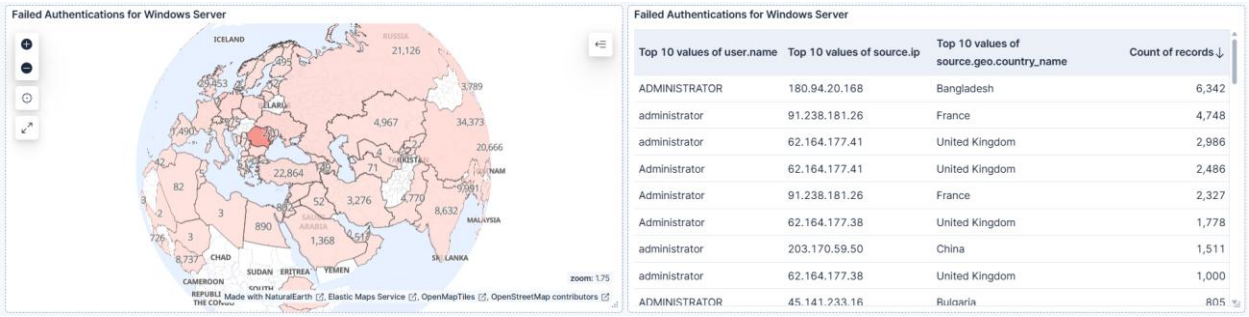
Findings

1. High Volume of Failed Logons Indicates Brute Force / Username Spraying

The Windows server recorded **50,169 failed logon events (Event ID 4625)** over the last 30 days. The volume and distribution across many external source IP addresses is consistent with automated brute-force and username-spraying activity.

Query:

event.code : "4625" and agent.name :"Windows-Server"



Top 10 values of user.name	Top 10 values of source.ip	Top 10 values of source.geo.country_name	Count of records ↓
ADMINISTRATOR	180.94.20.168	Bangladesh	6,342
administrator	91.238.181.26	France	4,748
administrator	62.164.177.41	United Kingdom	2,986
Administrator	62.164.177.41	United Kingdom	2,486
Administrator	91.238.181.26	France	2,327
Administrator	62.164.177.38	United Kingdom	1,778
administrator	203.170.59.50	China	1,511
administrator	62.164.177.38	United Kingdom	1,000
ADMINISTRATOR	45.141.233.16	Bulgaria	805

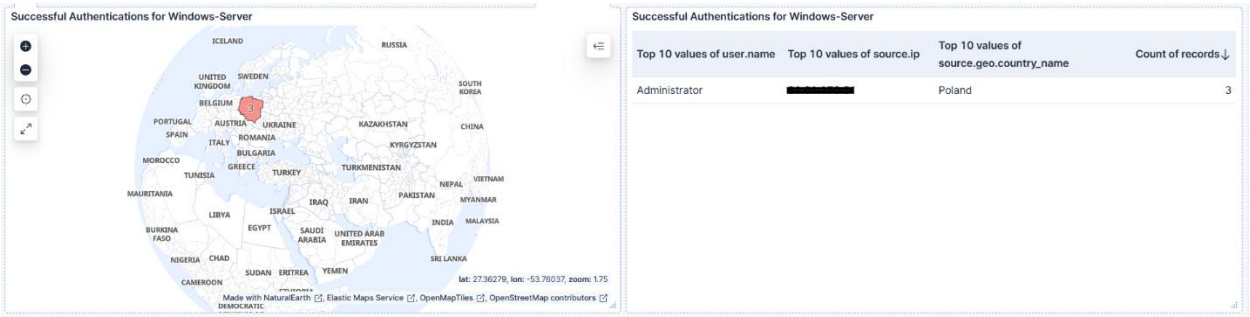
Figure 1 - Failed authentication activity (4625): geo distribution and top sources/targets (Last 30 days).

2. Validation: Successful Authentication Events (Known Activity)

A separate review of successful logons (4624) showed minimal successful authentication activity. In the dashboard, successful authentications were associated with expected/known access (analyst activity). This supports the conclusion that brute-force activity was present, but no attacker-success evidence was found within the reviewed logs. The analyst source IP was anonymized for privacy.

Query:

agent.name:"Windows-Server" and event.code:"4624" and winlog.event_data.LogonType:(3 or 7 or 10)



OSINT Validation (AbuseIPDB)

To add external context, the top attacking source IPs were checked in AbuseIPDB. Multiple IPs had prior abuse reports and non-trivial abuse confidence scores, supporting that the observed activity is consistent with known suspicious infrastructure.

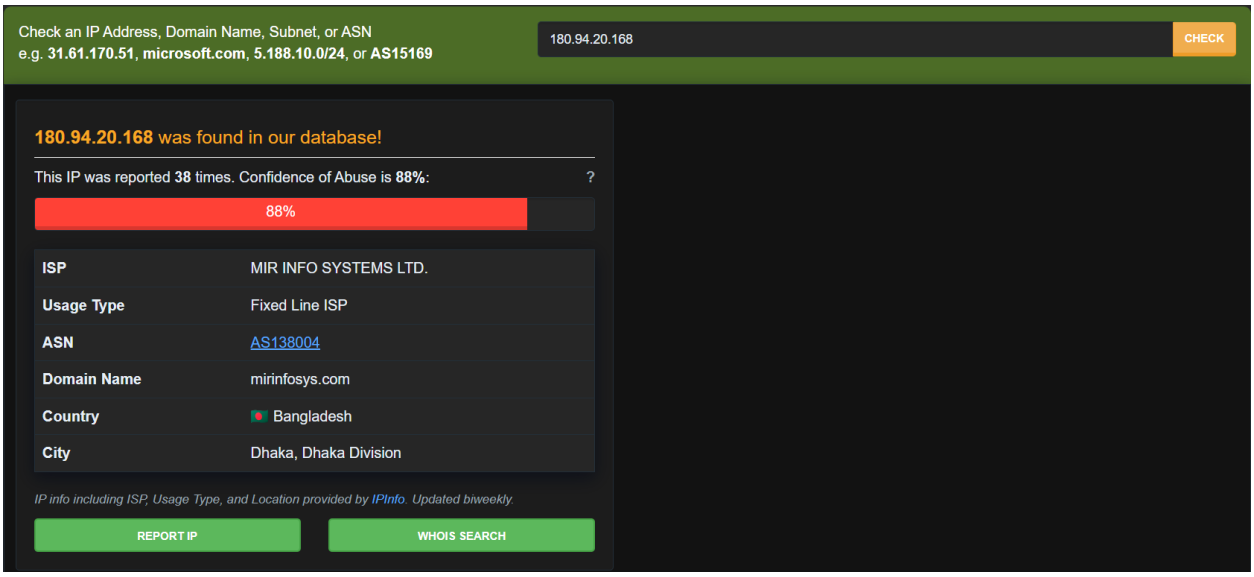


Figure 2 - AbuseIPDB result for 180.94.20.168

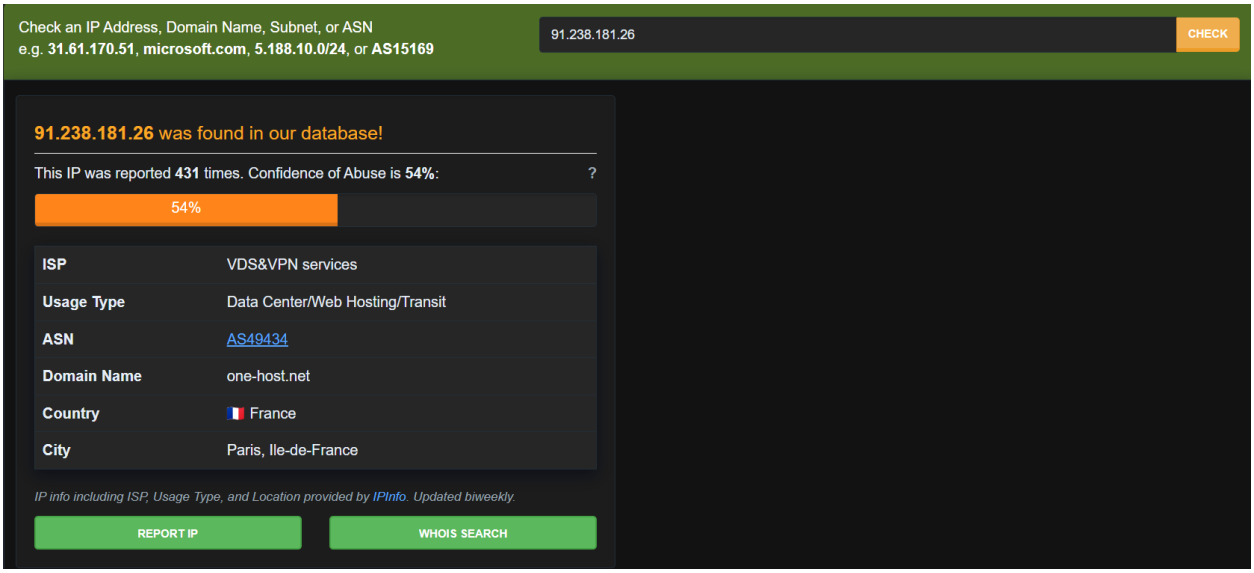


Figure 3 - AbuseIPDB result for 91.238.181.26

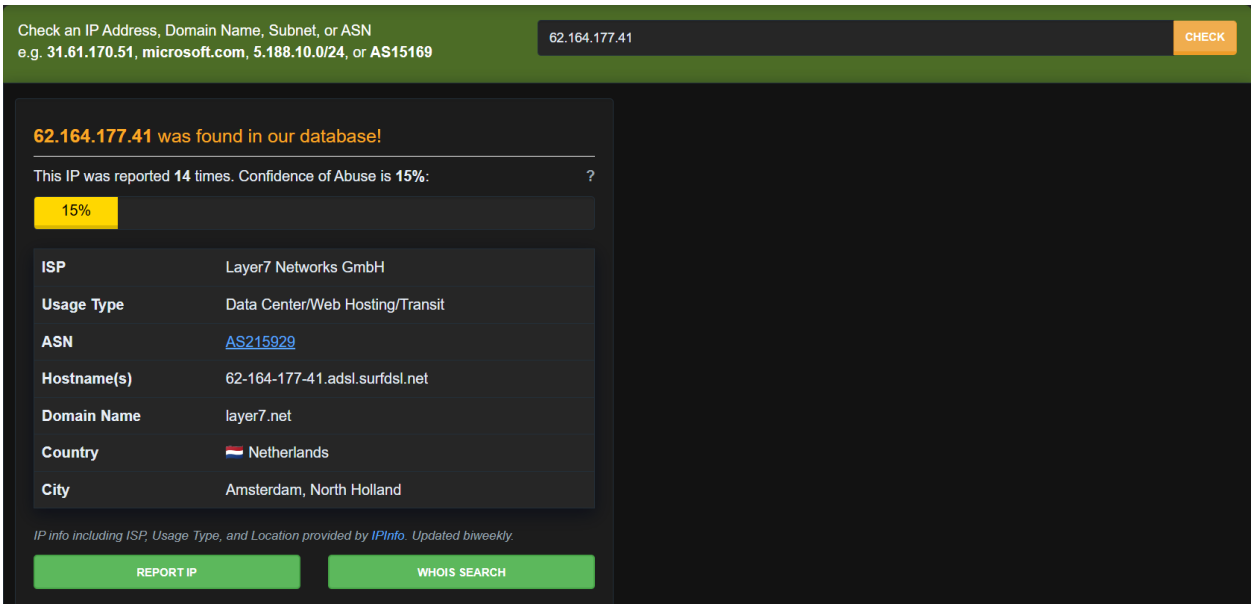


Figure 4 - AbuseIPDB result for 62.164.177.41

Conclusion

During the last 30 days, the internet-exposed Windows server generated a high volume of failed authentication events (Event ID 4625), consistent with automated brute-force and username-spraying behavior. The activity originated from multiple external source IP addresses and primarily targeted common administrative usernames (e.g., Administrator/admin), which is typical for opportunistic scanning against publicly reachable Windows systems.

All observed failed attempts in the dataset were associated with LogonType 3 (Network), indicating network-based authentication attempts (commonly SMB/network authentication) rather than interactive local logons. Review of successful authentication events (Event ID 4624) showed only limited successful activity attributable to known/expected access (analyst activity). Successful LogonType 3 events were observed but originated only from a known analyst IP address (anonymized), and no successful authentications were identified from the top external attacker IP addresses observed in the failed logon dataset.

OSINT enrichment using AbuseIPDB for selected top source IPs showed prior abuse reporting and elevated confidence-of-abuse scores for multiple addresses, supporting that the observed sources are likely associated with suspicious or previously reported infrastructure. Based on the reviewed logs and OSINT context, the observed activity is assessed as ongoing opportunistic brute-force attempts with no evidence of successful attacker authentication during the analysis window.