# Mini Runbook - Failed Logons (Windows EventID 4625) - Remote Only (Logon Type 3)

Version: 1.0 | Date: 2026-01-26 | Owner: SOC Analyst

| | |
|---|---|
| **Alert name** | SOC - Failed Logons (4625) - Remote Only (Logon Type 3) |
| **Objective** | Detect remote network logon failures that may indicate brute force, password spraying, or account enumeration. |
| **Primary signal** | Windows Security EventID 4625 with LogonType=3 and a non-local IP address. |
| **Recommended severity** | Medium (elevate to High based on context/trends) |

## 1. Data Source and Dependencies

This alert relies on Windows Security logs (EventID 4625) ingested into Splunk with sourcetype XmlWinEventLog:Security. Ensure that the Security log is enabled on target endpoints and that the Splunk Universal Forwarder (or equivalent) is collecting and forwarding the Security channel.

Key fields used: EventCode/EventID, LogonType, TargetUserName, IpAddress, Status, SubStatus, host, _time.

Scope: Remote network logon failures (LogonType=3). Excludes loopback and link-local IPv6 addresses.

## 2. Detection Logic (SPL)

Current correlation search (as implemented):

```
index=lab sourcetype="XmlWinEventLog:Security" earliest=-15m latest=now
"<EventID>4625</EventID>"
| rex field=_raw "<Data Name='TargetUserName'>(?<TargetUserName>[^<]+)</Data>"
| rex field=_raw "<Data Name='IpAddress'>(?<IpAddress>[^<]+)</Data>"
| rex field=_raw "<Data Name='LogonType'>(?<LogonType>\d+)</Data>"
| rex field=_raw "<Data Name='Status'>(?<Status>0x[0-9A-Fa-f]+)</Data>"
| rex field=_raw "<Data Name='SubStatus'>(?<SubStatus>0x[0-9A-Fa-f]+)</Data>"
| eval IpAddress=coalesce(IpAddress,"")
| where LogonType="3"
AND IpAddress!=""
AND IpAddress!="-"
AND IpAddress!="127.0.0.1"
AND IpAddress!="::1"
AND NOT like(IpAddress,"fe80:%")
| stats count as fails values(Status) as Status values(SubStatus) as SubStatus by
```

```
TargetUserName IpAddress host LogonType
| sort - fails
```

Scheduling: Run every 5 minutes, searching the last 15 minutes.

Trigger condition: Trigger when number of results is greater than 0.

Trigger frequency: Once per run (recommended).

## 3. Severity Rationale

Default severity is Medium because EventID 4625 is common and can include benign causes (mistyped passwords, stale services, misconfigured applications). However, remote LogonType=3 failures from non-local IP addresses are a meaningful precursor to brute force, password spraying, and account enumeration.

### Escalate to High when any of the following are true:

- High volume (e.g., >50 failures per IP or per account within 15 minutes), or a rapid increase across runs.
- Multiple targeted users from a single external IP (spray), or a single privileged user targeted from many IPs.
- Source IP is external/untrusted, on threat intel, or geolocation inconsistent with the user/environment.
- Correlated success follows (4624 LogonType=3) shortly after failures, especially for a privileged account.

### Downgrade to Low when:

- Clear benign pattern (known scanner, approved vulnerability scan window, known misconfigured service account).
- Internal IP from a managed jump host with documented user activity and no evidence of compromise.

## 4. Quick Reference: Status and SubStatus

Windows supplies a high-level failure code (Status) and a more specific cause (SubStatus). These are useful for distinguishing brute force vs. enumeration vs. disabled/locked accounts.

| Code | Meaning (common interpretation) |
|---|---|
| 0xC000006D | Logon failure (generic - often paired with SubStatus to specify cause) |
| 0xC000006A | Bad password |
| 0xC0000064 | User name does not exist (often enumeration) |
| 0xC0000234 | Account locked out |
| 0xC0000072 | Account disabled |
| 0xC0000193 | Account expired |

| | |
|---|---|
| 0xC000015B | User does not have the requested logon type at this computer |
| 0xC0000133 | Clocks out of sync (Kerberos) |

## 5. Triage Workflow

Goal: Determine whether activity is benign, suspicious, or confirmed malicious, and take appropriate action.

### Step 1 - Validate alert context

- Confirm timeframe and volume (fails).
- Identify whether the source IP is internal or external and whether it is expected for the host/user.
- Review Status/SubStatus to infer password guessing vs. enumeration vs. lockout.

### Step 2 - Check for follow-on success

Look for a successful logon (4624) from the same IpAddress/TargetUserName/host within +/- 30 minutes. A success after multiple failures materially increases risk.

### Step 3 - Assess impacted identity and asset criticality

- Is TargetUserName privileged (Domain Admin, local admin, service account)?
- Is the destination host a server, jump box, or domain controller?
- Are other security alerts present (EDR detections, unusual processes, new services, etc.)?

### Step 4 - Decide and respond

- Benign: Document reason, optionally tune exclusions, close.
- Suspicious: Escalate to IR queue, increase monitoring, consider temporary blocking of source IP, reset credentials if needed.
- Confirmed: Contain (block IP, disable account), collect evidence, follow incident response playbook.

## 6. Investigation Searches (Copy/Paste)

Use these to pivot quickly during triage.

### Baseline - failures by entity

```
index=lab sourcetype="XmlWinEventLog:Security" ("<EventID>4625</EventID>" OR
EventCode=4625)
| stats count as fails by TargetUserName IpAddress host LogonType Status SubStatus
| sort - fails
```

### Check for successful LogonType=3

```
index=lab sourcetype="XmlWinEventLog:Security" ("<EventID>4624</EventID>" OR
EventCode=4624)
| search LogonType=3
| stats count as successes by AccountName IpAddress host
| sort - successes
```

### Time series - bursts and spikes

```
index=lab sourcetype="XmlWinEventLog:Security" (EventCode=4625 OR
"<EventID>4625</EventID>")
| bucket _time span=5m
| stats count as fails by _time IpAddress TargetUserName
| sort 0 - _time
```

### Password spray heuristic - many users per IP

```
index=lab sourcetype="XmlWinEventLog:Security" (EventCode=4625 OR
"<EventID>4625</EventID>")
| stats dc(TargetUserName) as unique_users values(TargetUserName) as users count as fails
by IpAddress
| where unique_users >= 5
| sort - fails
```

## 7. False Positive Tuning

Apply tuning only after documenting evidence and getting SOC lead approval (to avoid hiding real attack activity).

### Common tuning approaches

- Whitelist known internal scanners/jump hosts: exclude specific internal IP ranges or named hosts.
- Exclude known service accounts: if a service is repeatedly failing due to stale credentials, remediate the service; only exclude once fixed and verified.
- Add thresholds: require fails >= N per IP or per user per run to reduce noise (e.g., N=5).
- Throttle: suppress repeat alerts for the same entity for a short period (e.g., 30-60 minutes) to prevent alert fatigue while investigating.

### Safe example thresholding (optional)

```
... | stats count as fails ... by TargetUserName IpAddress host LogonType
| where fails >= 5
| sort - fails
```

## 8. Operational Notes

- If you do not see new Triggered Alerts, verify the alert is Enabled, schedule is correct, and that the correlation search returns results within the configured time window.
- The list under Triggered Alerts shows each time the scheduled alert fired. Additional actions (email/webhook/notable) are optional and appear under Trigger Actions.
- Keep time range consistent: schedule every 5 minutes over last 15 minutes is standard and tolerates short ingestion delays.

## 9. Escalation and Closure Criteria

Escalate when: external IP, multiple accounts targeted, privileged account targeted, sustained activity, or any correlated success/EDR signal.
Close when: confirmed benign cause with supporting evidence and (if needed) tuning applied responsibly.