

# Password Spraying Incident Report

## Summary

During monitoring of Windows Security logs in an Active Directory lab environment, multiple failed authentication attempts were detected against different domain user accounts originating from the same source system within a short time window.

The activity pattern is consistent with a **password spraying attack**, where a single password is tested across many accounts to avoid account lockout thresholds.

The attack was identified through analysis of **Kerberos and logon failure events** and did not result in successful authentication.

---

## Attack Description

Password spraying is an authentication attack technique in which an attacker attempts to authenticate to multiple accounts using the same password, rather than trying many passwords for one account.

In this lab scenario, authentication attempts were generated using the built-in Windows command:

```
runas /user:LAB\user1 cmd  
runas /user:LAB\user2 cmd  
runas /user:LAB\user3 cmd
```

```
C:\> Command Prompt  
C:\>Users\slit\runas /user:LAB\soc2 cmd  
Enter the password for LAB\soc2:  
Attempting to start cmd as user "LAB\soc2" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\runas /user:LAB\it.user2 cmd  
Enter the password for LAB\it.user2:  
Attempting to start cmd as user "LAB\it.user2" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\alice.hr cmd  
Enter the password for LAB\alice.hr:  
Attempting to start cmd as user "LAB\alice.hr" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\soc cmd  
Enter the password for LAB\soc:  
Attempting to start cmd as user "LAB\soc" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\charlie.soc cmd  
Enter the password for LAB\charlie.soc:  
Attempting to start cmd as user "LAB\charlie.soc" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\it.user2 cmd  
Enter the password for LAB\it.user2:  
Attempting to start cmd as user "LAB\it.user2" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\>Users\slit\user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.
```

```
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\alice.hr cmd  
Enter the password for LAB\alice.hr:  
Attempting to start cmd as user "LAB\alice.hr" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\soc2 cmd  
Enter the password for LAB\soc2:  
Attempting to start cmd as user "LAB\soc2" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\charlie.soc cmd  
Enter the password for LAB\charlie.soc:  
Attempting to start cmd as user "LAB\charlie.soc" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\it.user2 cmd  
Enter the password for LAB\it.user2:  
Attempting to start cmd as user "LAB\it.user2" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1326: The user name or password is incorrect.  
  
C:\Users\lit.user1\runas /user:LAB\max.it cmd  
Enter the password for LAB\max.it:  
Attempting to start cmd as user "LAB\max.it" ...  
RUNAS ERROR: Unable to run - cmd  
1999: The referenced account is currently locked out and may not be logged on to.  
  
C:\Users\lit.user1>
```

This resulted in repeated failed logon attempts across multiple domain accounts within a short time window.

# Detection & Evidence

## Kerberos Authentication Failures

Event ID: 4771

**Description:** Kerberos pre-authentication failed

**Failure Code:** 0x18 (Bad password)

## Observed pattern:

- Multiple **different domain users**
- Same authentication source
- Short time interval between attempts

This behavior strongly indicates password spraying rather than brute-force against a single account.

Detection was based primarily on correlated Event ID 4771 logs, which provide sufficient visibility into Kerberos authentication failures across multiple domain accounts.

The screenshot shows the Windows Event Viewer interface. The left pane displays the event log structure under 'Event Viewer (Local) > Windows Logs > Security'. A search filter for 'Event ID: 4771' is applied. The right pane lists 31 events matching this filter. Two specific events are highlighted in a details view on the right.

Event ID	Task Category
4771	Kerberos Authentication Service

**Event Properties - Event 4771, Microsoft Windows security auditing.**

**General | Details**

**Kerberos pre-authentication failed.**

**Account Information:**  
Security ID: LAB\max.it  
Account Name: max.it

**Service Information:**  
Service Name: krbtgt/LAB

**Network Information:**  
Client Address: ::ffff:192.168.56.105  
Client Port: 49605

**Additional Information:**  
Ticket Options: 0x40810010  
Failure Code: 0x18  
Pre-Authentication Type: 2

**Log Name: Security**  
**Source: Microsoft Windows security** Logged: 23.01.2026 7:41:02  
**Event ID: 4771** Task Category: Kerberos Authentication Service  
**Level: Information** Keywords: Audit Failure  
**User: N/A** Computer: WIN-CKNBTMHISAA.lab.local  
**OpCode: Info**

**More Information:** [Event Log Online Help](#)

**Event Properties - Event 4771, Microsoft Windows security auditing.**

**General | Details**

**Kerberos pre-authentication failed.**

**Account Information:**  
Security ID: LAB\user2  
Account Name: it.user2

**Service Information:**  
Service Name: krbtgt/LAB

**Network Information:**  
Client Address: ::ffff:192.168.56.105  
Client Port: 49605

**Additional Information:**  
Ticket Options: 0x40810010  
Failure Code: 0x18  
Pre-Authentication Type: 2

**Log Name: Security**  
**Source: Microsoft Windows security** Logged: 23.01.2026 7:41:33  
**Event ID: 4771** Task Category: Kerberos Authentication Service  
**Level: Information** Keywords: Audit Failure  
**User: N/A** Computer: WIN-CKNBTMHISAA.lab.local  
**OpCode: Info**

**More Information:** [Event Log Online Help](#)

The screenshot shows the Windows Event Viewer interface. The left pane displays the event log structure under 'Event Viewer (Local) > Windows Logs > Security'. A search filter for 'Event ID: 4771' is applied. The right pane lists 31 events matching this filter. Two specific events are highlighted in a details view on the right.

Event ID	Task Category
4771	Kerberos Authentication Service

**Event Properties - Event 4771, Microsoft Windows security auditing.**

**General | Details**

**Kerberos pre-authentication failed.**

**Account Information:**  
Security ID: LAB\alice.hr  
Account Name: alice.hr

**Service Information:**  
Service Name: krbtgt/LAB

**Network Information:**  
Client Address: ::ffff:192.168.56.105  
Client Port: 49609

**Additional Information:**  
Ticket Options: 0x40810010  
Failure Code: 0x18  
Pre-Authentication Type: 2

**Log Name: Security**  
**Source: Microsoft Windows security** Logged: 23.01.2026 7:42:16  
**Event ID: 4771** Task Category: Kerberos Authentication Service  
**Level: Information** Keywords: Audit Failure  
**User: N/A** Computer: WIN-CKNBTMHISAA.lab.local  
**OpCode: Info**

**Event Properties - Event 4771, Microsoft Windows security auditing.**

**General | Details**

**Kerberos pre-authentication failed.**

**Account Information:**  
Security ID: LAB\user2  
Account Name: it.user2

**Service Information:**  
Service Name: krbtgt/LAB

**Network Information:**  
Client Address: ::ffff:192.168.56.105  
Client Port: 49607

**Additional Information:**  
Ticket Options: 0x40810010  
Failure Code: 0x18  
Pre-Authentication Type: 2

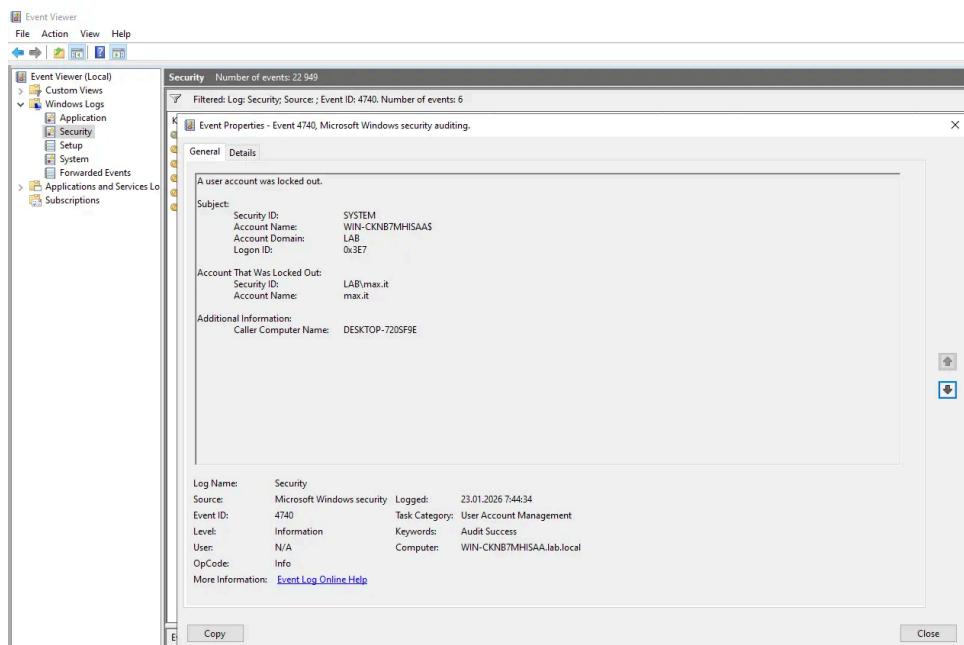
**Log Name: Security**  
**Source: Microsoft Windows security** Logged: 23.01.2026 7:41:46  
**Event ID: 4771** Task Category: Kerberos Authentication Service  
**Level: Information** Keywords: Audit Failure  
**User: N/A** Computer: WIN-CKNBTMHISAA.lab.local  
**OpCode: Info**

**More Information:** [Event Log Online Help](#)

## Locked Out

Following multiple failed Kerberos authentication attempts (Event ID 4771), one domain account was locked out as enforced by the Account Lockout Policy.

Event ID 4740 confirms that the configured Account Lockout Policy successfully mitigated the password spraying activity.



## Impact Assessment

- No successful authentication events detected
- No privilege escalation observed
- No lateral movement identified
- Domain integrity remained intact

The attack was **detected at the authentication stage** before any account compromise occurred.

## Mitigation & Recommendations

- Enforce strong and unique password policies

- Review and tune account lockout thresholds
- Monitor:
  - Event ID **4771**
  - Event ID **4625**
  - Event ID **4740**
- Implement alerting for:
  - Multiple failed logons across different users from a single source
- Educate users on password hygiene

## MITRE ATT&CK Mapping

Tactic	Technique
Credential Access	Password Spraying (T1110.003)