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.

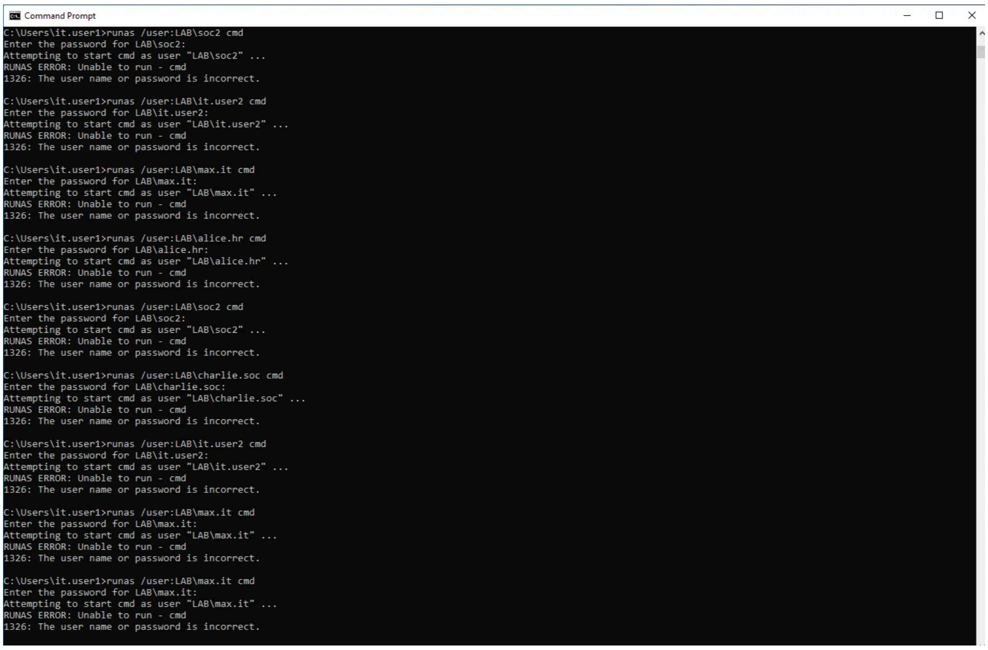
The attack was identified through analysis of **Kerberos and logon failure events** and did not result in successful authentication.

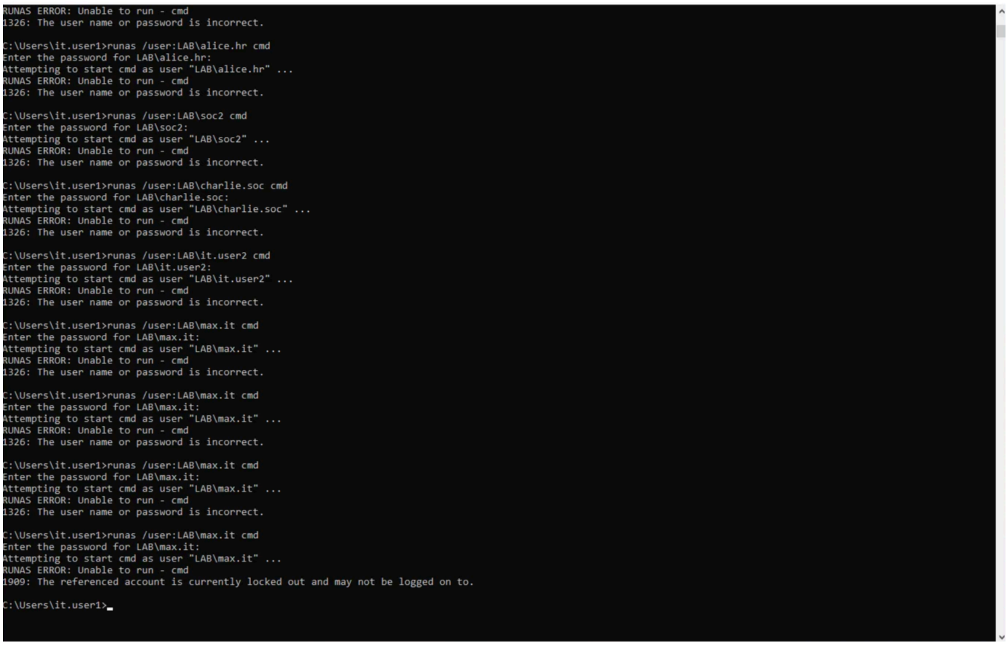
Attack Description

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
```





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

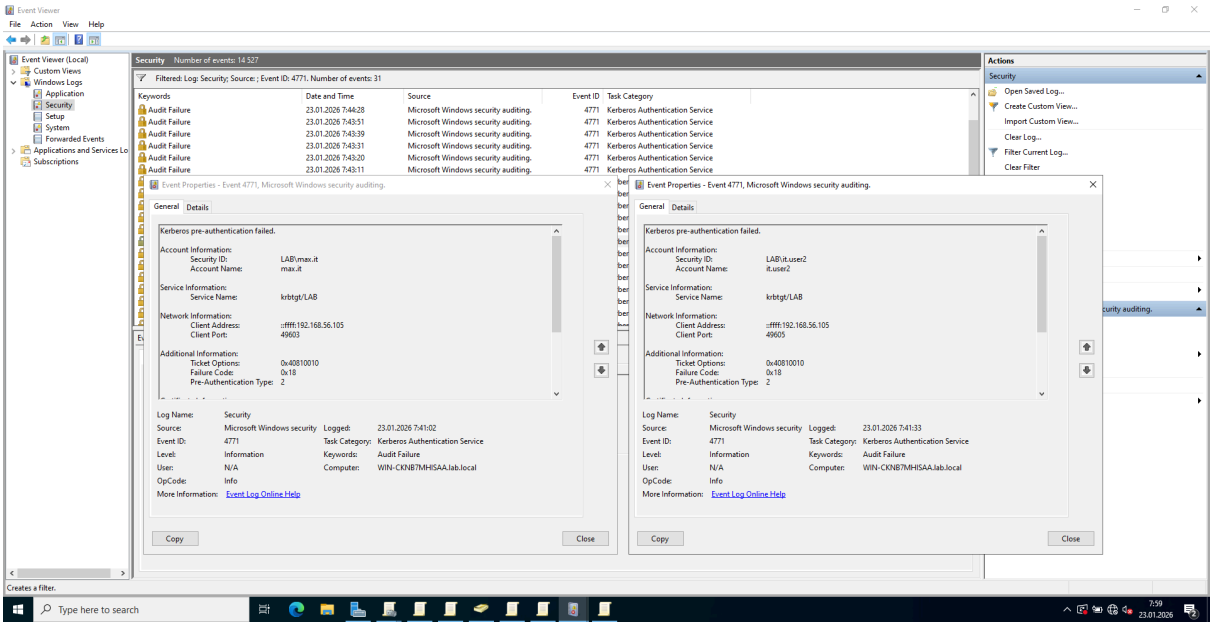
Failure Code: `0x18` (Bad password)

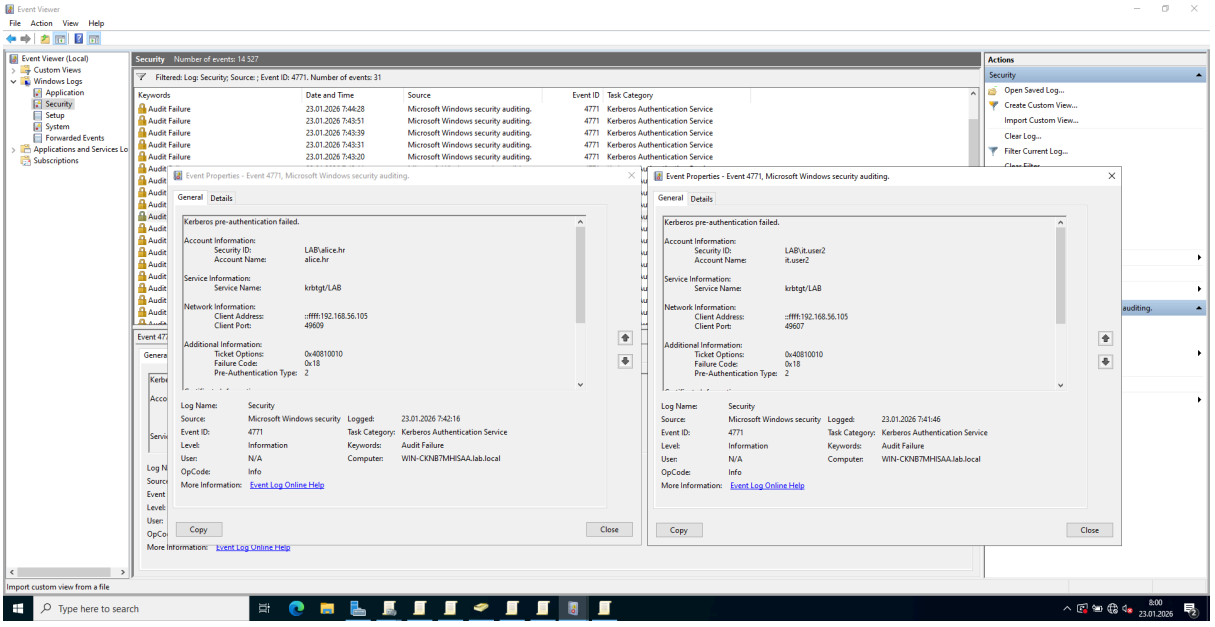
Observed pattern:

- 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.

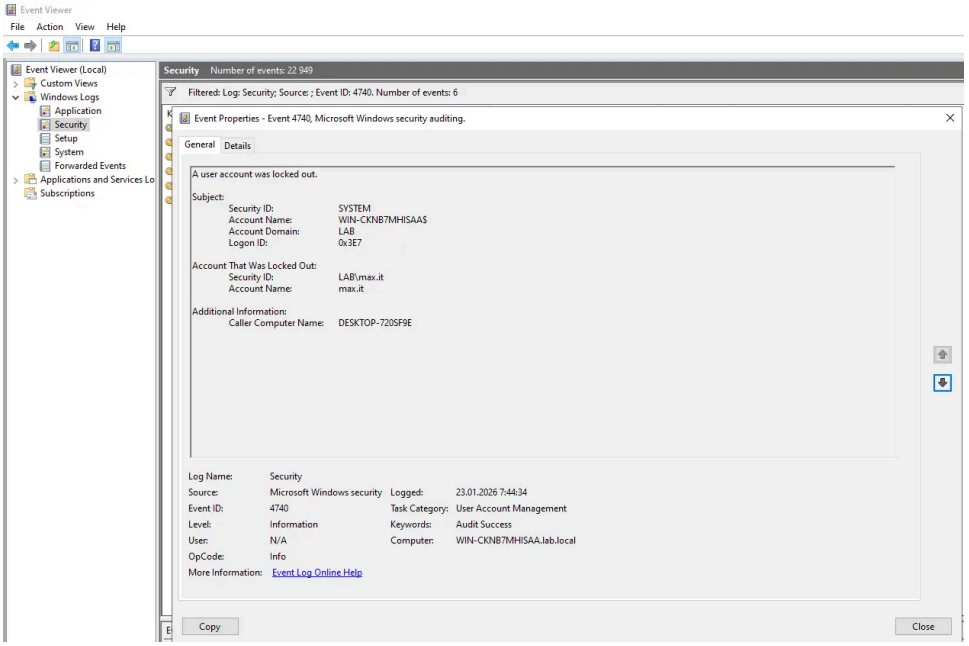




Locked Out

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)