Brute Force → Successful Login

---

1. Incident Metadata

Field	Details
Incident Title	Brute Force Login Success — Account Takeover
Impacted User	arun.patil@vasanthcorp.com
Host	HR-LAPTOP-09.vasanthcorp.com
Alert Source	Microsoft Defender for Cloud Apps
Severity	High
Incident ID	VSC-SOC-2025-001
Detection Time	19 Nov 2025 — 10:43 UTC
SOC Analyst	VR
MITRE Technique	**T1110 – Brute Force Attack**
Incident Status	Resolved / Closed

---

2. Incident Description & Why It's Critical

A threat actor attempted **57 consecutive login attempts** to the corporate Azure tenant using a weak password and successfully authenticated from a malicious foreign IP address.

This resulted in:
✓ Unauthorized account access
✓ High probability of **sensitive data exposure**
✓ Potential lateral movement risk

Since the user denied login — **True Compromise**.

---

3. Attack Analysis and Threat Behavior Summary

Attack Phase	Details
Initial Attempt	Automated brute-force login attempts targeting Azure
Exploitation	Valid password guessed
Execution	Successful login from Russia via web browser

Attack Phase	Details
Persistence	Nothing observed yet — early detection
Objectives	Account takeover for internal access

Attacker likely goal:

- Access emails (phishing internal users)
- Move laterally to privileged accounts
- Exfiltrate sensitive HR data

4.Timeline of Events

Time (UTC)	Event
10:39:12	First failed login attempt logged
10:39—10:42	57 failed login attempts detected
10:43:05	Successful login from Moscow, Russia
10:43:50	Defender generates Risky User Alert
10:44:12	SOC takes ownership → begins IR
10:45:10	User contacted → confirms NOT him
10:47:00	Password reset + Forced logout issued
10:49:26	Malicious IP blocked on firewall
10:52:40	Incident marked **True Positive**

---

5. Log Analysis & Evidence

5.1 Azure AD Sign-in Logs (Sample Logs)

Event: 4625 - Failed Login

User: arun.patil@vasanthcorp.com

Source IP: 185.231.205.222

Reason: Invalid Password

Event: 4624 - Successful Login

Login Type: Interactive Login via Browser

Country: Russia

User Agent: Mozilla/5.0 Windows NT 10.0

Risk Level: High

5.2 Threat Intel

Attribute	Result
Source IP	185.231.205.222
Reputation	Malicious
Threat History	Brute forcing, credential phishing campaigns
IOC Score	8.5/10 (High Risk)

5.3 Geo-Anomaly Analysis

- **Normal user login geography:** Bangalore, India
- **Anomalous login geography:** Moscow, Russia
- Impossible travel: 6100 km in < 5 min

✓ Confirmed account takeover

6.Root Cause Analysis

- User had **weak password**
- **No MFA configured**
- Attacker brute-forced successfully

Core Issue: Lack of multi-factor authentication increases credential attack success dramatically.

7.Remediation Actions

Action	Purpose	Status
Forced password reset	Remove attacker access	✓ Done
Block malicious IP	Prevent future attempts	✓ Done
Enable MFA for user	Strengthen auth security	✓ Done
Fed logs into TI feeds	Preempt future campaign	✓ Done
Reviewed lateral movement	Ensure no internal spread	✓ Clean

---

8. Post-Incident Recommendations

Recommendation	SOC Value
Enforce MFA across all accounts	Stops 99% of brute-force attacks
Enable smart lockout policies	Slow down password guessing
Use conditional access policies	Block risky sign-ins
Password rotation & complexity	Better credential hygiene
User training on account security	Prevent future compromises

---

9. MITRE ATT&CK Mapping

Tactic	Technique
Credential Access	**T1110 Brute Force**
Initial Access	Valid Accounts via stolen credentials
Defense Evasion	Login anomaly with no alerts triggered initially

---

10.Final Classification

Verdict	Threat Level
True Positive	High Risk – Account Takeover

Incident fully contained with **no lateral movement** detected.

❖ **IR Conclusion**

This incident demonstrates:
✓ Effective real-time alert response
✓ Proper use of Defender & Azure logs
✓ Security control weaknesses → addressed
✓ Business impact avoided due to quick IR