Brute Force Attack

I. Introduction

A **brute force attack** is a trial-and-error method where attacker tries series of different combination of series of username and password to gain unauthorized access to systems, networks, or online accounts by systematically attempting various combinations of usernames and passwords or cryptographic keys until the correct one is found.

The attack relies on computational power and persistence, leveraging automation tools to try a large number of guesses in rapid succession.

II. Tools used by attackers to perform Brute Force attack:

Attackers use a wide variety of tools to perform brute force attacks. These tools are designed to automate the process of systematically guessing passwords, credentials, or keys. Below are some commonly used tools, along with their descriptions and typical use cases:

- Hydra
- John the Ripper
- Aircrack-ng
- Burp Suite (Intruder)
- THC-SSL-DOS
- Medusa
- Ncrack
- WFuzz
- Hashcat
- SQLmap
- Sentry MBA
- Patator
- FireForce (Burp Extension)
- RainbowCrack

Attackers have a broad arsenal of tools designed to perform brute force attacks on various systems, including web applications, network services, databases, and Wi-Fi networks. Understanding these tools allows security professionals to anticipate and mitigate potential threats by implementing appropriate defenses such as strong passwords, rate limiting, multi-factor authentication, and log monitoring.

III. Types of Brute Force Attacks

1. **Simple Brute Force Attack:**
    - Tries every possible combination of characters.
    - Effective when the password is short and lacks complexity.

   - **Example:** Testing every combination for a 4-character password like abcd.

2. **Dictionary Attack:**
   - Uses a list of commonly used passwords (e.g., password123, admin, qwerty).
   - Faster than simple brute force as it skips unlikely combinations.
   - **Example:** Trying passwords from a precompiled list like rockyou.txt.
3. **Hybrid Brute Force Attack:**
   - Combines dictionary attacks with additional permutations, such as adding numbers or symbols to common passwords.
   - **Example:** Trying password1, password!, or password1234.
4. **Credential Stuffing:**
   - Uses stolen usernames and passwords from previous data breaches to attempt logins on different systems.
   - **Example:** Testing john.doe@gmail.com with passwords leaked from a previous breach.
5. **Reverse Brute Force Attack:**
   - Starts with a common password and attempts to find matching usernames.
   - **Example:** Testing the password 123456 across multiple accounts.
6. **Password Spraying:**
   - Tries a few commonly used passwords across many accounts to avoid account lockouts.
   - **Example:** Testing Summer2024 on hundreds of usernames.

IV. Real-Life Examples of Brute Force Attacks

1. Attack on SSH Services:

- Attackers use automated tools to brute-force SSH (Secure Shell) login credentials.
- **Example:**
  - Target: An exposed SSH server.
  - Tool: Hydra or John the Ripper.
  - Result: Gain shell access to perform privilege escalation or deploy malware.

2. Credential Stuffing on Retail Websites:

- Attackers use leaked credentials to access user accounts on e-commerce sites.
- **Example:**

  - Target: An online store.
  - Method: Using a database of leaked email-password pairs from a breach.
  - Result: Unauthorized purchases using stored payment information.

3. Office 365 Email Account Compromise:

- Attackers attempt brute force against corporate email systems to access sensitive communications.
- **Example:**
  - Target: Office 365.
  - Tool: Sentry MBA or custom scripts.
  - Result: Compromise of business emails (BEC), phishing campaigns, or data theft.

4. RDP (Remote Desktop Protocol) Brute Force:

- Attackers exploit weak RDP passwords to gain access to Windows servers.
- **Example:**
  - Target: A public-facing RDP service.
  - Result: Deployment of ransomware like Conti or LockBit after access is achieved.

5. IoT Device Attack:

- Weak or default passwords on IoT devices (e.g., cameras or smart thermostats) are targeted.
- **Example:**
  - Target: A smart home camera.
  - Attack: Using default passwords like admin/admin.
  - Result: Unauthorized surveillance or device hijacking.

V. How Brute Force Attacks Work

1. **Target Identification:** The attacker identifies a target system, account, or application.
2. **Automation:** The attacker uses tools or scripts to generate and test combinations of passwords or keys.
3. **Systematic Guessing:**
   - Dictionary Attack: Using a predefined list of common passwords.
   - Simple Brute Force: Trying all possible combinations of characters.
4. **Access Gained (if successful):** Once the correct credentials are found, the attacker can log in and exploit the system.

VI. Indicators of a Brute Force Attack

1. **Unusual Failed Login Attempts:**
    - A spike in failed login attempts over a short period.
    - Multiple login attempts from a single IP address.
2. **Logon Attempts from Unusual Locations:**
    - Users logging in from unfamiliar geographical regions.
3. **Account Lockouts:**
    - Frequent account lockouts due to repeated failed login attempts.
4. **Increased System Resource Usage:**
    - High CPU or memory utilization caused by repeated login attempts.
5. **Unsuccessful Access to Multiple Accounts:**
    - Failed login attempts across various accounts, often with similar patterns.

VII. Investigating Brute Force Attack incident in Microsoft Sentinel

Step:1 Prerequisites:

To effectively investigate a brute force attack in Microsoft Sentinel, certain prerequisites need to be in place to ensure you have the required visibility, tools, and configurations. Below is a detailed list of the prerequisites:

1. Data Source Integration

Ensure all relevant log sources are integrated with Microsoft Sentinel to capture the necessary data for detecting and investigating brute force attacks:

- **Azure AD Logs**:
    - Integrate **Azure Active Directory Sign-In Logs** for authentication events.
    - Required for cloud-based sign-ins and conditional access policies.
- **Windows Security Event Logs**:
    - Collect logs from on-premises Active Directory via agents to capture login events (Event ID 4625 for failed logins and 4624 for successful logins).
- **Firewall and VPN Logs**:
    - Integrate firewall or VPN logs to track external access attempts.
    - Logs from **Palo Alto**, **Cisco ASA**, or **Fortinet** are particularly useful.
- **Threat Intelligence Feeds**:
    - Connect threat intelligence sources to identify known malicious IP addresses.

- **Cloud Security Logs**:
    - For hybrid/cloud environments, integrate logs from **Microsoft Defender for Cloud**, **AWS**, or **GCP** to detect access attempts across platforms.

2. Access to Sentinel Tools

Ensure access to the features and tools in Microsoft Sentinel for analyzing and responding to the attack:

- **Log Analytics Workspace**: Sentinel relies on Log Analytics; ensure your Sentinel instance is connected to an active workspace.
- **KQL Query Access**: Familiarity with **Kusto Query Language (KQL)** is essential for running advanced queries to investigate logs.
- **Workbooks**: Set up **pre-configured workbooks** for user sign-in activity or brute-force detection, such as "Sign-in Analysis Workbook."

3. Analytics Rules and Detection

Pre-configure analytics rules to trigger alerts for brute-force patterns:

- **Failed Login Attempt Threshold**: Create a rule to detect repeated failed login attempts (e.g., >10 failed attempts in 5 minutes).
- **Brute-Force Detection Templates**: Use built-in templates like:
        - "Unusual Number of Failed Logon Attempts."
        - "Multiple Failed Sign-ins from Same IP Address."
- **Custom Detection Rules**: Write custom KQL-based rules to flag suspicious patterns based on your organization's specific environment.

4. Role-Based Access Control (RBAC)

Ensure you have the appropriate permissions:

- **Microsoft Sentinel Contributor**: To access incidents, run queries, and manage resources.
- **Global Reader/Global Admin**: For Azure AD data access.

5. Threat Intelligence

Enable and configure threat intelligence to enrich investigation:

- Use **Microsoft Threat Intelligence** or third-party feeds to flag suspicious IPs or actors.
- Ensure that threat intelligence indicators are linked to Sentinel.

6. Baseline Data

Establish baselines for user behaviour:

- **Normal Sign-In Patterns**: Understand typical sign-in locations, devices, and time zones.

- **Failed Login Thresholds**: Define what constitutes “unusual” login behaviour (e.g., rapid failed attempts).

7. Integration with Identity Protection

- **Azure AD Identity Protection**: Use Identity Protection to monitor risky sign-ins and compromised accounts and also ensure Conditional Access policies are in place to mitigate brute force attacks automatically.

8. Knowledge of Key Indicators of Compromise (IoCs)

Prepare to look for the following IoCs during investigation:

- Repeated failed login attempts from the same IP.
- Sudden login success after multiple failures.
- Logins from unusual geographical locations (impossible travel).
- Use of suspicious user agents (indicative of automated tools like Hydra or Metasploit).

Checklist Summary for Readiness:

Category	**Details**
Data Sources	Azure AD, Windows Event Logs, Firewalls, Threat Feeds.
Tools and Access	Sentinel Console, Log Analytics, KQL knowledge.
Detection Rules	Pre-built and custom analytics rules.
Response Mechanisms	Playbooks for automated mitigation
Baseline Behavior	Normal sign-in and login thresholds.
Threat Intelligence	Enrich investigation with IP reputation feeds.
RBAC Permissions	Sentinel Contributor, Global Reader/Admin.

Having these prerequisites in place ensures you’re fully equipped to detect, investigate, and mitigate brute force attacks using Microsoft Sentinel.

Step:2 Indicators of a Brute Force Attack

1. **Unusual Failed Login Attempts:** A spike in failed login attempts over a short period and Multiple logins attempts from a single IP address.
2. **Logon Attempts from Unusual Locations**: Users logging in from unfamiliar geographical regions.
3. **Account Lockouts:** Frequent account lockouts due to repeated failed login attempts.
4. **Increased System Resource Usage:** High CPU or memory utilization caused by repeated login attempts.

5. **Unsuccessful Access to Multiple Accounts:** Failed login attempts across various accounts, often with similar patterns.

Step:3 Security Incident Report Template:

Type of security incident: Brute Force **Severity:** High

Sentinel Security Incident: Multi-stage incident involving Initial access & Credential access involving one user.

Sentinel Incident ID: 22124 **MITRE Attack Technique:** Brute Force T1110

Date: The event started on March 16th at 03:34 **Attack duration:** 35 minutes

Identification of all the people involved: User Account

Geographical locations involved: Moscow, London, San Francisco, Washington, New York.

How the incident came about: An account with admin privilege without MFA enforced

Cyberattack kill-chain

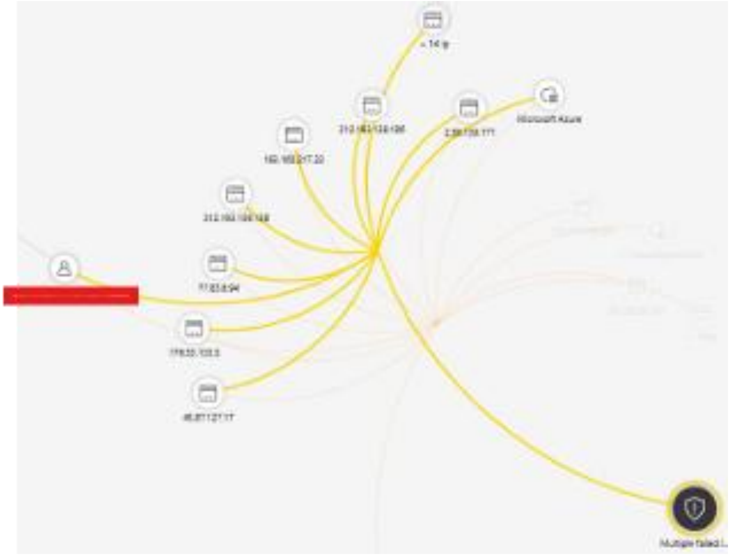
Reconnaissance -> Credential compromised -> Lateral Movement

Description of the incident: The brute force attack was completed successfully by compromising a credential with administrative privileges and performing lateral movement. It took the attacker just 35 minutes to compromise the credential after more 195 access attempts using brute-force attack techniques. With the successful attack, alerts were generated for access to Microsoft Azure related to Impossible travel, access outside the United Kingdom and finally constant access from Russia.

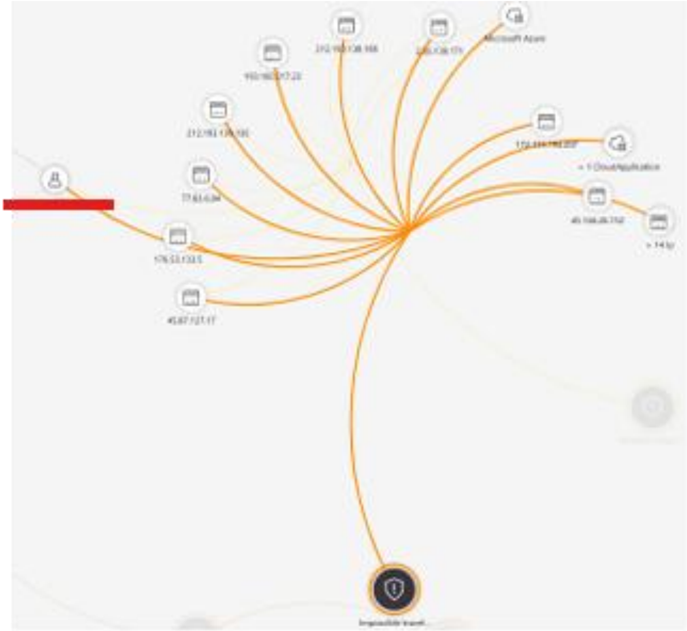
Actions and decisions taken and by whom: Actions were taken to block the account with the compromised credential.

Settings that could have prevented this incident: MFA enforced

Step:4 Brute Force Attack Graph:

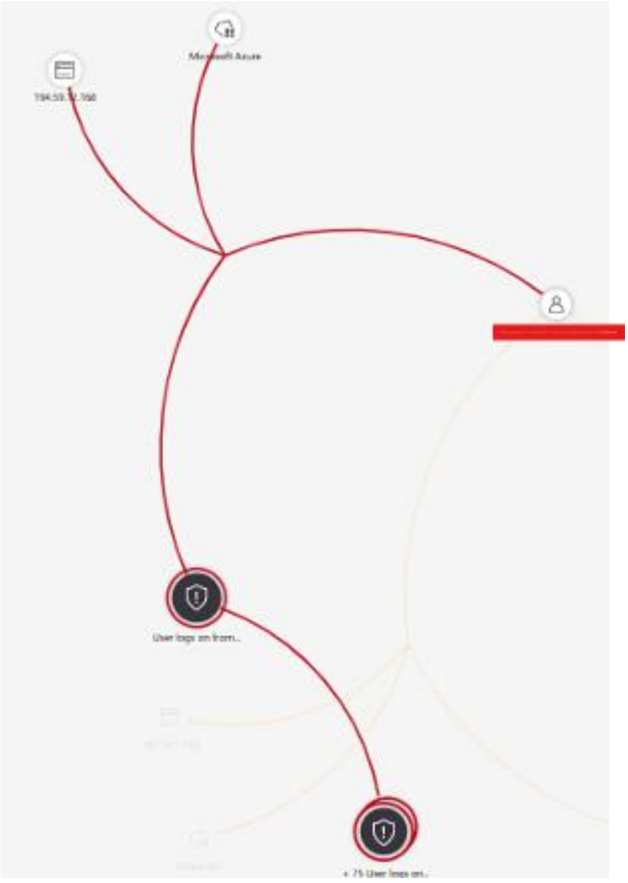

[redacted]

Step:5 Impossible Travel Graph:



[redacted]

Step:6 Logon From Russia Graph:



[redacted]

Step:7 Prevention Strategies:

1. Enforce Strong Password Policies:

- Use long, complex passwords that include upper/lowercase letters, numbers, and special characters.
- Avoid dictionary words and predictable patterns.

2. Enable Account Lockout Policies:

- Lock user accounts after a set number of failed login attempts to deter brute force attempts.

3. Implement Multi-Factor Authentication (MFA):

- Require additional authentication factors, such as OTPs or biometrics, beyond just a password.

4. Use CAPTCHA Mechanisms:

- Add CAPTCHA challenges to login pages to prevent automated attacks.

5. Employ Network Protection:

- Restrict access to login portals through firewalls and VPNs.
- Monitor and block suspicious IP addresses using tools like Azure Firewall or Conditional Access.

6. Rate Limiting:

- Limit the number of login attempts per minute to slow down brute force attacks.

7. Threat Intelligence:

- Use threat intelligence feeds to block IPs and domains known for brute force activity.

8. Log Monitoring and Alerts:

- Regularly monitor logs for failed login attempts and configure alerts for suspicious activities.

Step:8 Commonly applied policies

- Requiring multi-factor authentication for users with administrative roles.
- Requiring multi-factor authentication for Azure management tasks.
- Blocking sign-ins for users attempting to use legacy authentication protocols.
- Requiring trusted locations for Azure AD Multi-Factor Authentication registration.
- Blocking or granting access from specific locations.
- Blocking risky sign-in behaviours.
- Requiring organization-managed devices for specific applications.

Step:9 Configure Azure Identity Protection features.

- Sign in risk
- User at risk

Step:10 Configure Azure Polices

Business rules for handling non-compliant resources vary widely between organizations. Examples of how an organization wants the platform to respond to a non-compliant resource include:

- Deny the resource change
- Log the change to the resource
- Alter the resource before the change
- Alter the resource after the change
- Deploy related compliant resources
- Block actions on resources