**Threat Hunting Project Report: Brute Force Attack Analysis on Exposed Virtual Machine**

**Date:** May 23, 2025

**Prepared By:** Venkata Bharath Devulapalli

**1. Executive Summary**

This report documents a simulated threat hunting exercise conducted to identify, analyze, and respond to potential brute-force login attempts targeting a critical virtual machine (VM), windows-target-1. This VM was inadvertently exposed to the public internet due to a configuration oversight. Leveraging Microsoft Defender for Endpoint (MDE) advanced hunting capabilities, the investigation sought to confirm brute-force activity, characterize attacker methodologies, and ascertain any indicators of successful compromise.

Our analysis conclusively identified a high volume of sustained brute-force login attempts against windows-target-1, originating from a diverse range of external IP addresses. These attacks primarily targeted common administrative accounts, notably "administrator," indicative of automated credential-guessing campaigns. Despite the intensity of these attempts, no successful unauthorized logins from the identified malicious IP addresses were detected within the available log data. All successful login events were confirmed to originate from authorized internal IP ranges, affirming the integrity of legitimate user access.

Based on these findings, immediate and strategic recommendations are provided to enhance the VM's security posture. These include the implementation of stringent Network Security Group (NSG) access controls, activation of robust account lockout policies, and the establishment of advanced logging and real-time alerting mechanisms to effectively counter future adversarial activities.

**2. Introduction and Project Objective**

The objective of this project was to execute a simulated, yet realistic, threat hunting exercise using Microsoft Defender for Endpoint (MDE) advanced hunting capabilities. The scope of this exercise was a specific virtual machine, windows-target-1, which was identified as being inadvertently exposed to the public internet. The core aims were threefold:

* **Detection and Analysis:** Identify and thoroughly analyze any brute-force login attempts directed at the exposed VM.
* **Attacker Behavior Characterization:** Evaluate the patterns and methodologies employed by potential attackers.
* **Compromise Assessment:** Determine if any of the observed brute-force attempts resulted in successful unauthorized access to the VM.

This exercise serves as a proactive measure to identify vulnerabilities and enhance incident response capabilities within the environment.

**3. Preparation Phase**

**3.1. Scenario Overview** During routine security posture assessments, it was discovered that windows-target-1, a VM integral to shared services (e.g., DNS, domain services), had been inadvertently exposed to the internet without adequate protective measures. This critical misconfiguration immediately prompted a threat hunting investigation to assess the potential impact of this exposure.

**3.2. Hypothesis** Given the internet exposure and the absence of explicit account lockout configurations, it was hypothesized that:

* External adversaries would attempt brute-force login attacks against windows-target-1.
* These attempts might exploit common or default account names.
* There was a possibility of successful unauthorized access if a weak password was present or if account lockout was not enforced.

**4. Data Collection and Environment Inspection**

**4.1. Step 1: Verification of DeviceInfo Table Attributes** To ensure the integrity and completeness of the dataset for analysis, the availability of recent logs within the DeviceInfo and DeviceLogonEvents tables was confirmed.

* **Activity:** A schema review of the DeviceInfo table was performed to identify critical attributes for filtering and analysis.
* **Query (Kusto Query Language - KQL):**

Code snippet

DeviceInfo

| getschema

* **Relevance:** Key attributes such as Timestamp, DeviceId, DeviceName, PublicIP, and IsInternetFacing were identified as essential for accurately pinpointing the target VM and its internet-facing status.

**4.2. Step 2: Identification of Internet-Facing VMs** This step was crucial for definitively confirming windows-target-1's exposure to the public internet.

* **Query (KQL):**

Code snippet

DeviceInfo

| where DeviceName == "windows-target-1"

| where IsInternetFacing == true

| order by Timestamp desc

* **Result:** The query confirmed that windows-target-1 was indeed publicly exposed, reporting a visible public IP address of 172.210.179.171. This finding validated the initial premise of the threat hunt.
* **Screenshot Reference:** (Insert Image 1: MDE Query Result - DeviceInfo confirming windows-target-1 exposure)

**4.3. Step 3: Identification of DeviceLogonEvents Table Attributes** Prior to analyzing login attempts, a thorough understanding of the DeviceLogonEvents schema was necessary to extract relevant fields.

* **Activity:** A schema review of the DeviceLogonEvents table was conducted.
* **Query (KQL):**

Code snippet

DeviceLogonEvents

| getschema

* **Relevance:** Critical attributes identified for subsequent analysis included Timestamp, DeviceId, DeviceName, ActionType (e.g., LogonFailed, LogonSuccess), LogonType, AccountName, RemoteIP, and FailureReason. These fields are fundamental for detecting and characterizing login anomalies.

**4.4. Step 4: Initial Review of Failed Login Attempts** This initial query aimed to retrieve all recorded failed login attempts against the target VM, providing a baseline for further analysis.

* **Query (KQL):**

Code snippet

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == "LogonFailed"

| project Timestamp, AccountName, RemoteIP, ActionType, LogonType

| order by Timestamp desc

* **Result:** The query revealed a significant volume of failed login attempts. A prominent observation was the consistent targeting of the administrator account. Multiple distinct external IP addresses were identified as sources, including 202.59.15.125 and 103.56.162.115, confirming active adversarial probing.
* **Screenshot Reference:** (Insert Image 2: MDE Query Result - Initial Failed Logins)

**5. Analyzing Failed Login Patterns**

**5.1. Step 5: GeoIP Check (Non-Functional)** An attempt was made to enrich the RemoteIP data with geographical context (country and city); however, this functionality was not available within the current MDE configuration.

* **Query (KQL):**

Code snippet

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == "LogonFailed"

| project Timestamp, AccountName, RemoteIP, RemoteIPCountry, RemoteIPCity

| order by Timestamp desc

* **Error:** The query failed with a semantic error, stating that RemoteIPCountry and RemoteIPCity columns do not exist.
* **Screenshot Reference:** (Insert Image 3: MDE Error Message - GeoIP Columns)
* **Impact Assessment:** The inability to perform GeoIP enrichment limited the immediate understanding of the geographical distribution of the attacking entities. This information is valuable for attributing attacks, identifying common threat actor origins, and informing geopolitical threat intelligence.
* **Future Enhancement:** It is highly recommended to enable NSG Flow Logs and integrate them with a traffic analytics solution that supports GeoIP enrichment to overcome this limitation.

**6. Detecting Brute-Force Behavior**

**6.1. Step 6: Summarizing Failed Attempts by IP and Account** This analysis aimed to quantify the intensity and scope of brute-force attempts by aggregating failed logins per source IP address and targeted account. This provides a clear overview of the most active attackers and their preferred targets.

* **Objective:** To identify IP addresses exhibiting high volumes of failed login attempts and to determine the specific accounts being targeted. Grouping by RemoteIP, DeviceName, and AccountName facilitated the detection of concentrated attack vectors. The inclusion of FirstSeen and LastSeen timestamps provided a temporal context, allowing for assessment of attack duration and persistence.
* **Query (KQL):**

Code snippet

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == 'LogonFailed'

| where isnotempty(RemoteIP)

| summarize

FailedAttempts = count(),

FirstSeen = min(Timestamp),

LastSeen = max(Timestamp)

by RemoteIP, DeviceName, AccountName, ActionType

| where FailedAttempts > 5 // Filtering for significant activity

| order by FailedAttempts desc

* **Result:** The results unequivocally demonstrated active brute-force campaigns. For example, 147.45.112.27 was responsible for 86 failed attempts. Other highly active source IPs included 196.251.84.131, 185.42.159.50, and 191.85.17.22, each contributing a substantial number of failed logins.
* **Key Findings:**
  + Multiple VMs (specifically windows-target-1) experienced hundreds to thousands of login attempts from consistent external IP addresses, strongly indicating automated brute-force bots.
  + The primary targets were default privileged accounts (e.g., root, administrator) and other common usernames, a typical strategy for credential guessing.
  + While some attempts were distributed over time, a significant portion exhibited concentrated bursts within short durations, further corroborating automated attack methodologies.
* **Screenshot Reference:** (Insert Image 4: MDE Query Result - Summarized Failed Attempts)

**6.2. Step 7: Focus on Bursts (Short Window Logins)** To distinguish between sporadic failed logins (e.g., user error) and deliberate, automated brute-force attacks, this step focused on identifying concentrated bursts of failed login attempts within a defined short time window (5 minutes).

* **Justification:** A high volume of failed logins within a compressed timeframe is a strong indicator of an automated attack, as opposed to manual attempts or legitimate user errors. The 5-minute window was chosen as a practical threshold to identify rapid, automated activity.
* **Query (KQL):**

Code snippet

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == 'LogonFailed'

| where isnotempty(RemoteIP)

| summarize

FailedAttempts = count() by RemoteIP, DeviceName,

AccountName, ActionType, bin(Timestamp, 5m) // Binning into 5-minute intervals

| where FailedAttempts > 5 // Threshold for burst detection

| order by FailedAttempts desc

* **Result:** Analysis of burst activity revealed critical insights. For instance, 185.42.159.50 recorded 27 failed attempts within a single 5-minute window, providing compelling evidence of an active and aggressive brute-force bot.
* **Screenshot Reference:** (Insert Image 5: MDE Query Result - Burst Login Attempts)

**7. Cross-Checking for Successful Logins**

**7.1. Step 8: Query for Any Prior LogonSuccess From Brute-Force IPs** This crucial step aimed to determine if any of the identified brute-force source IP addresses had ever successfully authenticated to windows-target-1, which would indicate a compromise.

* **Query (KQL):**

Code snippet

let bruteForceIPs =

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == "LogonFailed"

| summarize FailedCount = count() by RemoteIP, bin(Timestamp, 5m)

| where FailedCount > 5

| project RemoteIP; // Collect IPs with significant failed attempts

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == "LogonSuccess"

| where RemoteIP in (bruteForceIPs) // Check if any of these IPs had successful logins

| project Timestamp, AccountName, RemoteIP

| order by Timestamp desc

* **Result:** The query returned no results, indicating that no successful logins were recorded from any of the IP addresses identified as sources of brute-force attacks. This is a critical finding, suggesting that the attacks were likely unsuccessful in gaining unauthorized access.
* **Screenshot Reference:** (Insert Image 6: MDE Query Result - No Successful Logins from Brute-Force IPs)

**7.2. Step 9: Verification of Normal LogonSuccess Activity** To provide further assurance that no unauthorized access occurred, all successful login events to windows-target-1 were reviewed to confirm that legitimate internal IP addresses were the sole sources.

* **Query (KQL):**

Code snippet

DeviceLogonEvents

| where DeviceName == "windows-target-1"

| where ActionType == "LogonSuccess"

| where isnotempty(RemoteIP)

| project Timestamp, AccountName, RemoteIP, ActionType, LogonType

| order by Timestamp desc

* **Result:** All observed successful logins originated from expected internal (private) IP addresses, such as 10.0.8.4 and 10.0.8.6, associated with legitimate internal user accounts like josh1, dwm-3, and umfd-3. An external IP 115.125.23.18 from Japan was also noted, which was determined to be a routine, legitimate user login. Crucially, none of the IP addresses implicated in the brute-force attempts were present in the successful login records.
* **Screenshot Reference:** (Insert Image 7: MDE Query Result - Normal Successful Logins)

**8. Relevant MITRE ATT&CK TTPs**

The observed adversarial activities and their potential implications align with the following MITRE ATT&CK Techniques, Tactics, and Procedures (TTPs):

* **Tactics:** Credential Access (TA0006)
* **Primary Technique Observed:**
  + **T1110 – Brute Force:** This technique involves an adversary attempting to gain access to accounts by systematically guessing or cracking passwords or keys. This was directly observed through the high volume of failed login attempts.
    - **T1110.001 – Password Guessing:** Direct attempts to guess passwords for accounts. The repeated attempts against specific accounts (e.g., administrator) are indicative of this sub-technique.
    - **T1110.003 – Password Spraying:** Attempting a small number of commonly used passwords against many accounts. While not definitively confirmed as password spraying (as opposed to targeted password guessing), the diverse targeting of multiple accounts suggests this possibility.
* **Potential Techniques if Successful (not observed in this hunt, but relevant for context):**
  + **Tactics:** Persistence (TA0003), Privilege Escalation (TA0004), Defense Evasion (TA0005), Credential Access (TA0006), Discovery (TA0007), Lateral Movement (TA0008), Collection (TA0009), Command and Control (TA0011)
  + **T1078 – Valid Accounts:** Adversaries may obtain and abuse credentials of legitimate accounts as a primary means of initial access, persistence, or lateral movement.
    - **T1078.001 – Default Accounts:** The targeting of accounts like administrator directly aligns with attempts to exploit common default credentials, which often have predictable usernames and sometimes weak default passwords.
  + **T1133 – External Remote Services:** Adversaries may leverage legitimate remote services (e.g., RDP, SSH) that are exposed to the internet to access an internal network. The exposure of windows-target-1 facilitated this potential initial access vector.

**9. Conclusion & Recommendations**

**9.1. Key Findings** Based on the comprehensive threat hunting exercise, the following key findings are reported:

* **Vulnerability Confirmed:** The VM windows-target-1 was confirmed to be exposed to the public internet with open ports, representing a significant security vulnerability.
* **Active Brute-Force Attacks:** Multiple, sustained brute-force login attempts were detected, originating from a diverse set of external IP addresses. These attacks primarily targeted common administrative accounts.
* **No Confirmed Compromise:** Crucially, no successful logins from the identified malicious IP addresses were detected within the available MDE logs.
* **Legitimate Access Verified:** All observed successful logins were confirmed to originate from authorized internal (private) IP addresses, indicating normal and legitimate user behavior.

**9.2. Strategic Recommendations** To significantly enhance the security posture of windows-target-1 and similar assets, and to mitigate the risk of future brute-force attacks, the following strategic recommendations are provided:

1. **Network Access Hardening (Immediate Action):**
   * **Reconfigure NSG:** Immediately reconfigure the Network Security Group (NSG) associated with windows-target-1 to restrict all inbound access to only explicitly trusted IP ranges (e.g., internal corporate networks, authorized VPN gateways). All other inbound ports should be closed or filtered.
   * **Principle of Least Privilege for Network Access:** Ensure that only absolutely necessary ports are open, and only to the minimum required source IP addresses.
2. **Account Security Enhancement:**
   * **Implement Account Lockout Policy:** Enable and enforce a robust account lockout policy within Active Directory or local security policies. A recommended starting point is to lock accounts after 5-10 failed login attempts within a 5-minute window, with a lockout duration of at least 30 minutes or until manually reset.
   * **Strong Password Policy:** Reinforce and audit adherence to a strong password policy requiring minimum length (e.g., 14 characters), complexity (mix of uppercase, lowercase, numbers, symbols), and disallowing commonly used or breached passwords.
   * **Multi-Factor Authentication (MFA):** Implement MFA for all administrative and critical accounts, especially for any remote access. This is the most effective control against credential-based attacks.
3. **Logging, Monitoring, and Alerting:**
   * **Enable NSG Flow Logs & Traffic Analytics:** Activate NSG Flow Logs and integrate them with Azure Network Watcher's Traffic Analytics. This will provide invaluable GeoIP data, network flow visibility, and behavioral enrichment for network traffic, significantly aiding future threat hunting, anomaly detection, and incident response.
   * **Proactive Alerting:** Establish real-time alerts within MDE (or a Security Information and Event Management - SIEM system) for:
     + Any IP address attempting more than 5 failed logons within a 5-minute window.
     + Logon failures from non-standard geographic locations (once GeoIP is enabled).
     + Logon failures targeting highly privileged accounts (e.g., administrator, root).
   * **Threat Intelligence Integration:** Continuously feed high-failure IP addresses into external threat intelligence platforms (e.g., AbuseIPDB, VirusTotal) and integrate these feeds into perimeter defenses (e.g., firewalls, WAFs) for proactive blocking.
4. **Regular Security Audits:**
   * Conduct periodic security audits and vulnerability assessments to identify and remediate misconfigurations and exposures proactively.

**Disclaimer**

This report is based on a simulated threat hunting exercise utilizing available log data from Microsoft Defender for Endpoint. While the analysis aims for accuracy, it is limited by the scope of the simulation and the data accessible. Real-world threat landscapes are dynamic, and continuous monitoring and adaptation of security controls are essential.