### **1. Preparation**

* **Goal**: Set up the hunt by defining what you're looking for.
  + During routine maintenance, the security team is tasked with investigating any VMs in the shared services cluster (handling DNS, Domain Services, DHCP, etc.) that have mistakenly been exposed to the public internet. The goal is to identify any misconfigured VMs and check for potential brute-force login attempts/successes from external sources.
* **Activity**: Develop a hypothesis based on threat intelligence and security gaps (e.g., “Could there be lateral movement in the network?”).
  + During the time the devices were unknowingly exposed to the internet, it’s possible that someone could have actually brute-force logged into some of them since some of the older devices do not have account lockout configured for excessive failed login attempts.

### **2. Data Collection**

* **Goal**: Gather relevant data from logs, network traffic, and endpoints.
  + Consider inspecting the logs to see which devices have been exposed to the internet and have received excessive failed login attempts. Take note of the source IP addresses and number of failures, etc.
* **Activity**: Ensure data is available from all key sources for analysis.
  + Ensure the relevant tables contain recent logs:
    - DeviceInfo
    - DeviceLogonEvents

### **3. Data Analysis**

* **Goal**: Analyze data to test your hypothesis.
* **Activity**: Look for anomalies, patterns, or indicators of compromise (IOCs) using various tools and techniques.
  + Is there any evidence of brute force success (many failed logins followed by a success?) on your VM or ANY VMs in the environment?
  + If so, what else happened on that machine around the same time? Were any bad actors able to log in?

### **4. Investigation**

* **Goal**: Investigate any suspicious findings.
* **Activity**: Dig deeper into detected threats, determine their scope, and escalate if necessary. See if anything you find matches TTPs within the [MITRE ATT&CK Framework.](https://attack.mitre.org/)
  + You can use ChatGPT to figure this out by pasting/uploading the logs: [Scenario 1: TTPs](https://docs.google.com/document/d/12Bxj4nXZHzci1TH2RAEKXLBoNgeO7K-k4qL-6FoWnjg/edit)

### **5. Response**

* **Goal**: Mitigate any confirmed threats.
* **Activity**: Work with security teams to contain, remove, and recover from the threat.
  + Can anything be done?

### **6. Documentation**

* **Goal**: Record your findings and learn from them.
* **Activity**: Document what you found and use it to improve future hunts and defenses.
  + Document what you did

### **7. Improvement**

* **Goal**: Improve your security posture or refine your methods for the next hunt.
* **Activity**: Adjust strategies and tools based on what worked or didn’t.
  + Anything we could have done to prevent the thing we hunted for? Any way we could have improved our hunting process?

**Timeline Summary and Findings:**

Windows-target-1 Has been internet facing for the last several days with port 3389 RDP:

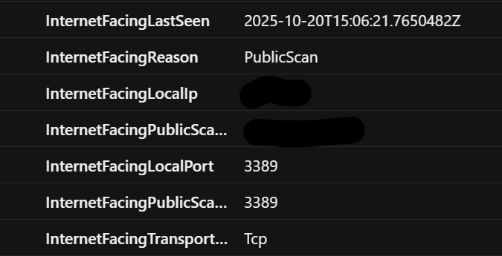
DeviceInfo

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

| where IsInternetFacing == True

| sort by Timestamp desc

Last internet facing time: **Oct 21, 2025 6:14:29 AM**

****

**— — — —**

Multiple bad actors attempting remote login to the exposed device:

DeviceLogonEvents

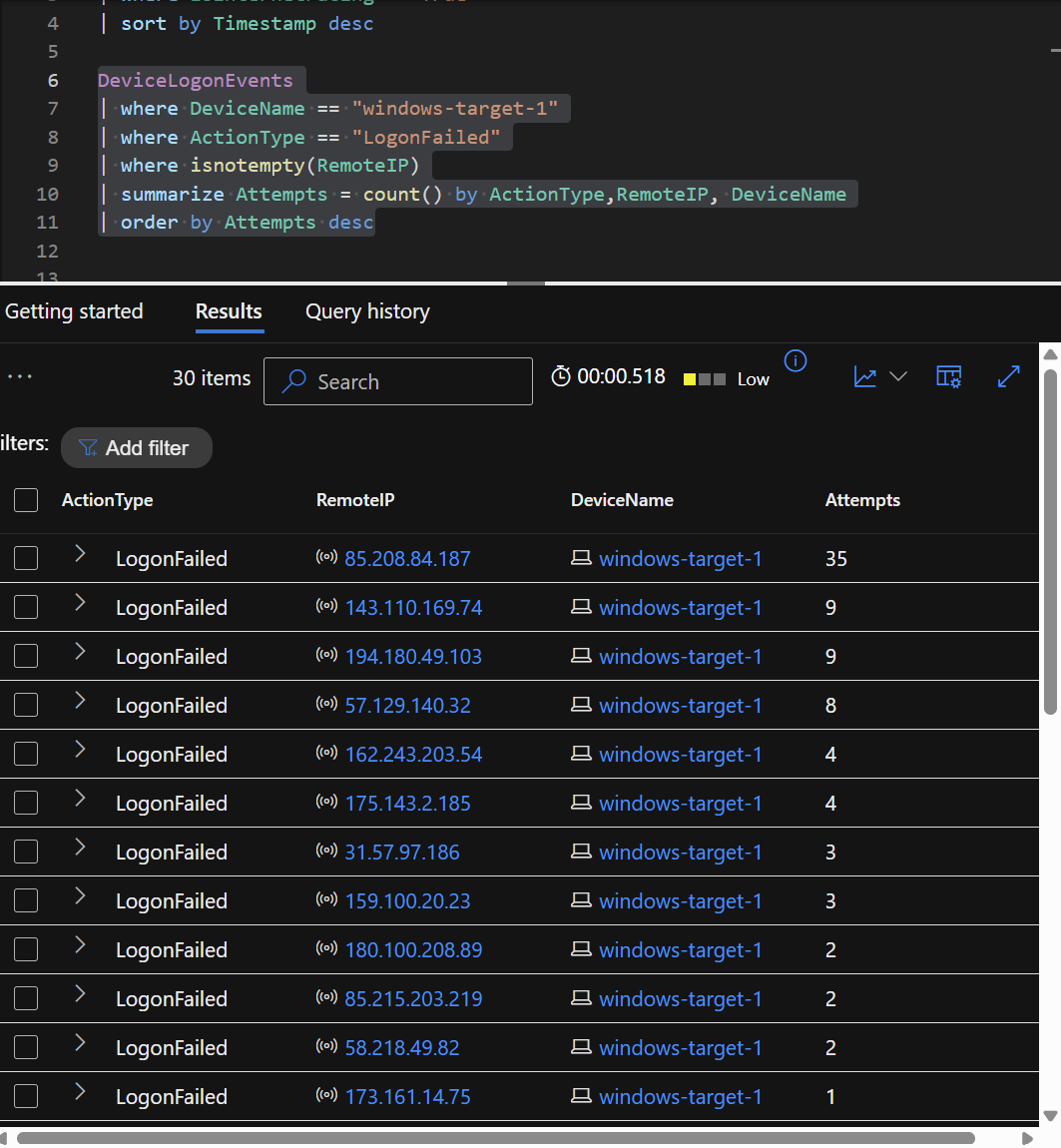
| where DeviceName == "windows-target-1"

| where ActionType == "LogonFailed"

| where isnotempty(RemoteIP)

| summarize Attempts = count() by ActionType,RemoteIP, DeviceName

| order by Attempts desc



**— — — —**

The top 10 RemoteIP addresses that attempted to login were not successful:

let SuspectRemoteIPs = dynamic(["85.208.84.187","143.110.169.74","194.180.49.103","57.129.140.32", "162.243.203.54","175.143.2.185","31.57.97.186","159.100.20.23","180.100.208.89","85.215.203.219"]);

DeviceLogonEvents

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

| where LogonType has\_any ("Interactive","Network","Unlock","RemoteInteractive")

| where ActionType == "LogonSuccess"

| where RemoteIP has\_any (SuspectRemoteIPs)

<Empty query results>

**— — — —**

There were zero successful login attempts in the last 7 days on this device:

DeviceLogonEvents

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

| where ActionType == "LogonSuccess"

<Empty query results>

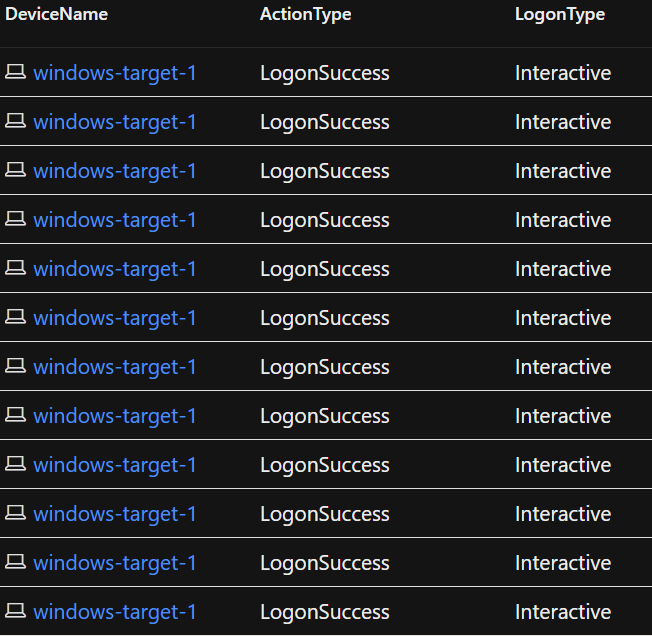
Additionally, verified there was no unusual activity in the last 30 days:

DeviceLogonEvents

| where Timestamp > ago(30d)

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

| where ActionType == "LogonSuccess"



There were 12 successful interactive logins (local). Nothing unusual.

**— — — —**

Though multiple brute force attempts to login to the device have been made over the last 7 days, there is no evidence of successful breaches or unauthorized access.

**— — — —**

Relevant MiTRE ATT&CK TTPs:

T1595.001 - Active Scanning: Attackers scanned public IP ranges to discover exposed RDP services.

T1133 - External Remote Services (RDP): Attempts to gain access to a system through exposed RDP on port 3389.

T1110 - Brute Force: Repeated login attempts using guessed or stolen credentials to gain unauthorized access.

**— — — —**

**Incident Response Actions:**

* **Hardened NSG attached to windows-target-1 to only allow RDP traffic from specific endpoints.**
* **Implemented account lockout policy.**
* **Implemented MFA**

**— — — —**