

## Scenario 6: Devices Exposed to the Internet

### Threat Hunting Lab

10/24-25/2025

#### Tools Used:

Microsoft Azure <https://portal.azure.com/>

Microsoft Defender for Endpoint

#### Narrative Established for Purposes of the Lab:

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.

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.

#### Preparation

Develop a hypothesis based on threat intelligence and security gaps (e.g., "Could there be lateral movement in the network?")

#### Create a Virtual Machine. BruceVMSept24

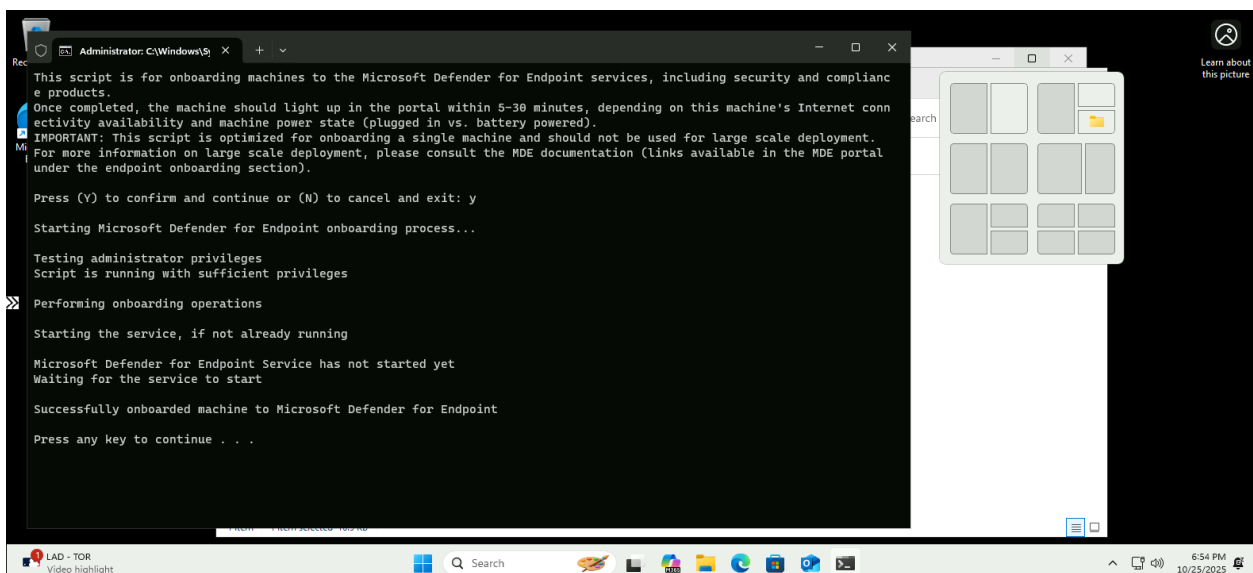
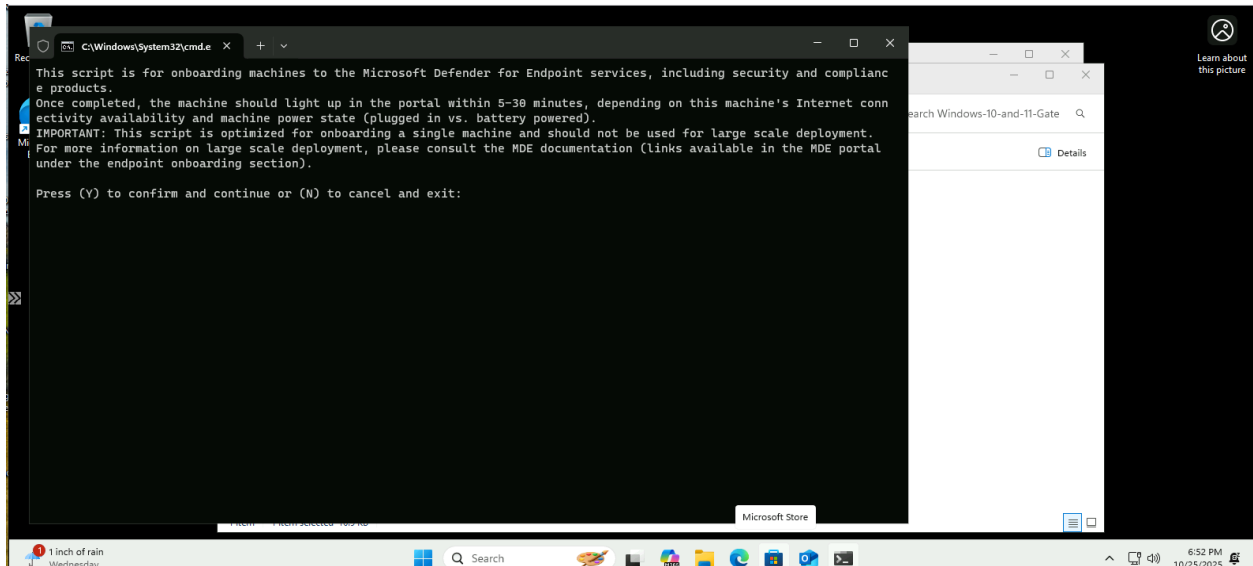
##### Virtual machine

Computer name	Win11VMBruce
Operating system	Windows (Windows 11 Pro)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1172
Hibernation	Disabled

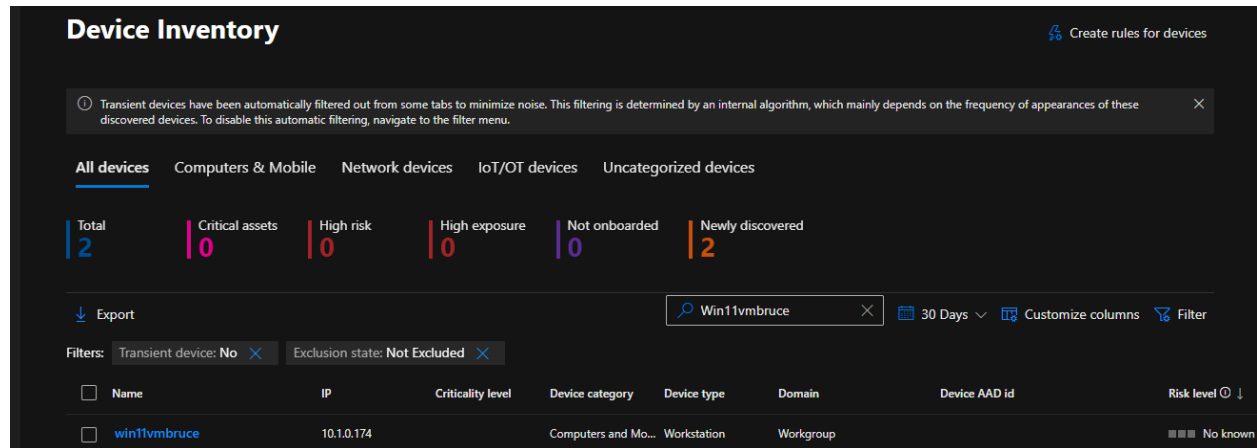
##### Networking

Public IP address ⓘ	172.177.236.170 ( Network interface win11vmbruce691 ) <a href="#">1 associated public IPs</a>
Public IP address (IPv6)	-
Private IP address	10.1.0.174
Private IP address (IPv6)	-
Virtual network/subnet	<a href="#">Cyber-Range-2-VNet/Cyber-Range-2-Subnet</a>
DNS name	<a href="#">Configure</a>

## Onboard to Microsoft Defender for Endpoint.



## Successfully Onboarded.



There are two that have been onboarded with this device name so I will ensure that the public IP address "172.177.236.170" is included in queries to ensure identification.

## Data Collection

I will ensure data is available from all key sources for analysis.

I will gather relevant data from logs, network traffic, and endpoints taking into consideration inspecting the logs to see which devices have been exposed to the internet and have received excessive failed login attempts. Also taking note of the source IP addresses and number of failures.

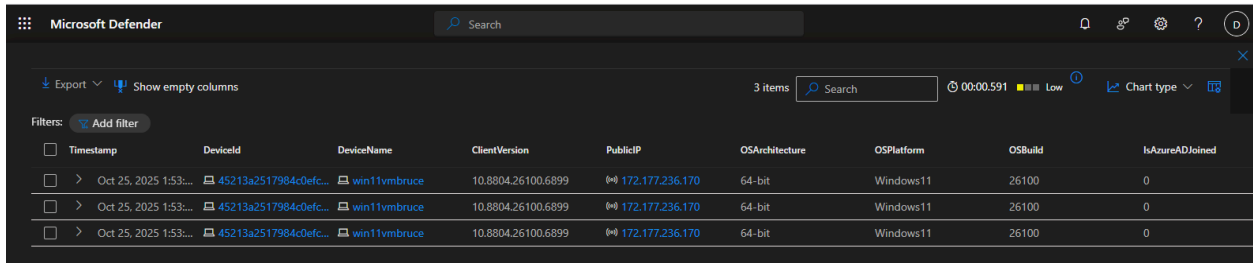
## Query Used:

DeviceInfo

| where DeviceName has "Win11VMBruce"

| where PublicIP has "172.177.236.170"

Return in screenshot:



Timestamp	DeviceId	DeviceName	ClientVersion	PublicIP	OSArchitecture	OSPlatform	OSBuild	IsAzureADJoined
> Oct 25, 2025 1:53:...	45213a2517984c0efc...	win11vmbruce	10.8804.26100.6899	(🌐) 172.177.236.170	64-bit	Windows11	26100	0
> Oct 25, 2025 1:53:...	45213a2517984c0efc...	win11vmbruce	10.8804.26100.6899	(🌐) 172.177.236.170	64-bit	Windows11	26100	0
> Oct 25, 2025 1:53:...	45213a2517984c0efc...	win11vmbruce	10.8804.26100.6899	(🌐) 172.177.236.170	64-bit	Windows11	26100	0

Win11VMBruce is onboarded and is creating log entries for MDE to discover.

## Verification

I will run these every 15–30 minutes:

### Query Used:

DeviceInfo

| where DeviceName =~ "Win11VMBruce"

| summarize LastSeen=max(Timestamp), PublicIPs=make\_set(PublicIP),

InternetFacing=any(IsInternetFacing)

**Why:** Quick check that MDE still sees it as internet-facing and tied to the right public IP.

## Evidence:

The screenshot shows the Microsoft Defender Advanced Hunting interface. The left sidebar contains navigation options: Schema, Functions, Favorites, Alerts & behaviors, Apps & identities, and Devices. The main area displays a query result for a Kusto query. The query is:

```
DeviceInfo
| where DeviceName =~ "Win11VMBruce"
| summarize LastSeen=max(Timestamp), PublicIPs=make_set(PublicIP), InternetFacing=any(IsInternetFacing)
```

The results table shows the following data:

Property	Value
LastSeen	Oct 25, 2025 1:56:26 PM
PublicIPs	["20.12.2.181","135.119.172.38","", "172.177.236.170"]
InternetFacing	True

Here's what my screenshot confirms:

LastSeen → The VM is currently visible to Microsoft Defender and actively reporting telemetry.

PublicIPs → It lists my new public IP 172.177.236.170 (alongside a few NAT-related ones – 20.x.x.x, 135.x.x.x, etc.). Those secondary IPs are Azure infrastructure or Defender service relay addresses.

This confirms the VM is exposed to the public internet, which means bots will eventually begin scanning and attempting RDP or SMB.

Now I will allow Win11VMBruce to be exposed to the Internet for some time and then investigate the findings. I will periodically run these commands to identify when suspicious activity begins and to begin investigation:

### Connection Detection, Verification of Inbound connections (any port) from public IPs:

#### Queries Used:

## DeviceNetworkEvents

| where DeviceName =~ "Win11VMBruce"

| where ActionType == "InboundConnectionAccepted"

| where RemoteIPType == "Public"

| project Timestamp, RemoteIP, LocalPort, InitiatingProcessFileName

| order by Timestamp desc

## Evidence:

The screenshot shows a PowerShell query in a dark-themed interface. The query is as follows:

```
28
29 DeviceNetworkEvents
30 | where DeviceName =~ "Win11VMBruce"
31 | where ActionType == "InboundConnectionAccepted"
32 | where RemoteIPType == "Public"
33 | project Timestamp, RemoteIP, LocalPort, InitiatingProcessFileName
34 | order by Timestamp desc
35
```

Below the query, the results are displayed in a table with the following columns: Timestamp, RemoteIP, LocalPort, and InitiatingProcessFileName. There are 2 items in the results.

Timestamp	RemoteIP	LocalPort	InitiatingProcessFileName
Oct 25, 2025 2:43:...	205.210.31.6	139	ntoskrnl.exe
Oct 25, 2025 1:57:...	64.62.197.227	49664	lsass.exe

The screenshot shows the Microsoft Defender interface. The top bar includes a search bar and a "Show empty columns" button. The main area displays a table with the following columns: Timestamp, RemoteIP, LocalPort, and InitiatingProcessFileName. There are 2 items in the results.

Timestamp	RemoteIP	LocalPort	InitiatingProcessFileName
Oct 25, 2025 2:43:...	205.210.31.6	139	ntoskrnl.exe
Oct 25, 2025 1:57:...	64.62.197.227	49664	lsass.exe

And:

```
DeviceLogonEvents
| where DeviceName =~ "Win11VMBruce"
| where ActionType == "LogonFailed"
| summarize Attempts = count() by RemoteIP
| order by Attempts desc
```

## Evidence:

The screenshot shows the Microsoft Defender Security Center interface. At the top, there's a 'Run query' button and a 'Last 7 days' filter. Below the query editor, the query is displayed: 

```
1 DeviceLogonEvents
2 | where DeviceName =~ "Win11VMBruce"
3 | where ActionType == "LogonFailed"
4 | summarize Attempts = count() by RemoteIP
5 | order by Attempts desc
```

 The results tab is active, showing a table with one item. The table has columns 'RemoteIP' and 'Attempts'. The single row shows '149.50.96.98' and '100'.

RemoteIP	Attempts
149.50.96.98	100

This screenshot shows a closer view of the results table. The table has two columns: 'RemoteIP' and 'Attempts'. The single row shows '149.50.96.98' and '100'.

RemoteIP	Attempts
149.50.96.98	100

And:

DeviceInfo

| where Timestamp >= ago(24h)

| where DeviceName =~ "Win11VMBruce" and PublicIP == "172.177.236.170"

| summarize LastSeen=max(Timestamp),

InternetFacing=any(IsInternetFacing),

Seen=count()

by DeviceName, PublicIP

| order by LastSeen desc

## Evidence:

The screenshot displays the Microsoft Sentinel Advanced Hunting interface. On the left, there is a sidebar with navigation options: Schema, Functions, Search, Favorites, Alerts & behaviors, Apps & identities, and Devices. The main area shows a Kusto query being executed. The query is as follows:

```
15 DeviceInfo
20 DeviceInfo
21 | where Timestamp >= ago(24h)
22 | where DeviceName =~ "Win11VMBruce" and PublicIP == "172.177.236.170"
23 | summarize LastSeen=max(Timestamp),
24 |             InternetFacing=any(IsInternetFacing),
25 |             Seen=count()
26 | by DeviceName, PublicIP
27 | order by LastSeen desc
28
```

Below the query editor, the 'Results' tab is active, showing a single result item. The result is a table with the following columns: DeviceName, PublicIP, LastSeen, InternetFacing, and Seen. The data row shows:

DeviceName	PublicIP	LastSeen	InternetFacing	Seen
win11vmbruce	172.177.236.170	Oct 25, 2025 2:30:06 PM		6

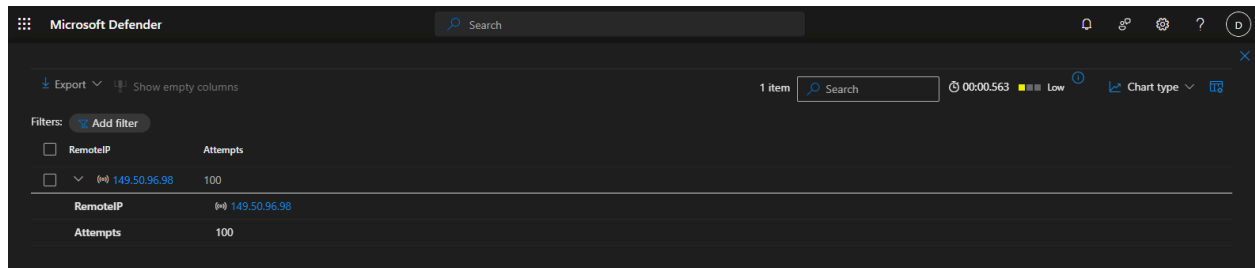
**Why:** First signs of scanners/bots actually touching the Virtual Machine Win11VMBruce from all three of these queries.

**There are confirmed attempts (100) that have been discovered.**

There is also evidence of benign entries indicating normal running processes that occur within the Microsoft Azure/Cyber Range environment. Those secondary IPs are Azure infrastructure or Defender service relay addresses. The 100 attempts are the evidence from "149.50.96.98"



## Evidence:



The screenshot shows the Microsoft Defender interface with a query result table. The table has two columns: 'RemotelIP' and 'Attempts'. A filter is applied to 'RemotelIP' with the value '149.50.96.98'. The result shows 100 attempts for this IP address.

RemotelIP	Attempts
149.50.96.98	100

From this Query:

```
DeviceLogonEvents
| where DeviceName =~ "Win11VMBruce"
| where ActionType == "LogonFailed"
| summarize Attempts = count() by RemotelIP
| order by Attempts desc
```

---

**Next Step — Check for Any Successful Logons from Same IP: "149.50.96.98"**

## Investigation

I will run this correlation check:

### Query Used:

```
DeviceLogonEvents
| where DeviceName =~ "Win11VMBruce"
| where RemotelIP == "149.50.96.98"
| where ActionType == "LogonSuccess"
| project Timestamp, AccountName, LogonType, RemotelIP, ActionType
| order by Timestamp desc
```

If I see any hits here, that means the brute-force **succeeded** — attackers found valid credentials and gained interactive access.

So far, no evidence of any brute-force attempts have succeeded from any of the suspicious IP addresses:

## Evidence:

The screenshot shows the Microsoft Sentinel Advanced Hunting interface. The query editor contains the following Kusto query:

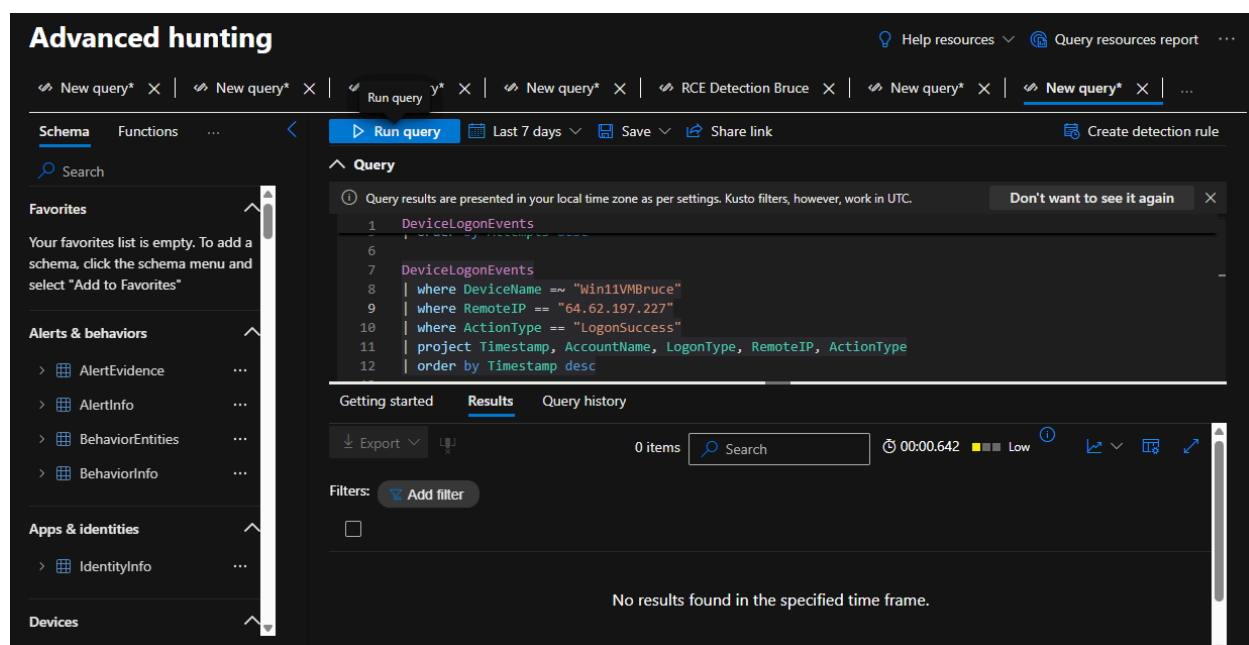
```
DeviceLogonEvents
| where DeviceName == "Win11VMBruce"
| where RemoteIP == "149.50.96.98"
| where ActionType == "LogonSuccess"
| project Timestamp, AccountName, LogonType, RemoteIP, ActionType
| order by Timestamp desc
```

The results pane shows "0 items" and a message: "No results found in the specified time frame." The interface includes a sidebar with navigation options like Favorites, Alerts & behaviors, Apps & identities, and Devices. The top bar shows the "Advanced hunting" title and various toolbars for running queries and managing results.

The screenshot shows the Microsoft Sentinel Advanced Hunting interface with a different query. The query editor contains the following Kusto query:

```
DeviceLogonEvents
| where DeviceName == "Win11VMBruce"
| where RemoteIP == "205.210.31.6"
| where ActionType == "LogonSuccess"
| project Timestamp, AccountName, LogonType, RemoteIP, ActionType
| order by Timestamp desc
```

The results pane shows "0 items" and a message: "No results found in the specified time frame." The interface is identical to the first screenshot, showing the same sidebar and top bar.



## Response

### **Goal:**

Mitigate any confirmed threats.

### **Activity:**

Work with security teams to contain, remove, and recover from the threat.

### **Response Summary:**

Once suspicious inbound connections and multiple failed logon attempts were confirmed on the VM (Win11VMBruce), immediate containment actions were considered to prevent potential compromise. The system's network exposure was evaluated, and security group rules were reviewed to confirm that inbound RDP and SMB access were intentionally open for observation purposes only.

Although no successful logons were detected, the repeated brute-force attempts from the external IP 149.50.96.98 and earlier scanning behavior from 205.210.31.6 and 64.62.197.227 demonstrated active reconnaissance and intrusion attempts. If this had been a production environment, the following mitigation steps would be implemented:

- **Containment:** Restrict RDP and SMB access to trusted IP ranges only or disable them entirely.
- **Credential Hardening:** Enforce complex passwords and implement account lockout policies to limit brute-force opportunities.
- **Monitoring:** Enable continuous alerting in Microsoft Defender and Sentinel for repeated LogonFailed events or unusual inbound traffic patterns.
- **Investigation:** Perform reverse IP lookups and threat intelligence checks (AbuseIPDB, VirusTotal) to verify attacker infrastructure.

No signs of post-compromise activity were identified, indicating the system remained secure throughout the engagement.

---

### **Documentation Summary**

The investigation confirmed that the publicly exposed Virtual Machine attracted multiple external scans and failed login attempts. The key findings include:

- Inbound connection attempts from public IPs 205.210.31.6, 64.62.197.227, and 149.50.96.98.
- Repeated LogonFailed actions (100 attempts) originating from 149.50.96.98, indicating brute-force activity.
- Associated system processes observed: lsass.exe, svchost.exe, and ntoskrnl.exe during connection attempts.
- No LogonSuccess events recorded — no confirmed intrusion.

### **Actions Taken:**

- Verified the system's internet exposure via DeviceInfo and confirmed inbound events via DeviceNetworkEvents.
- Correlated IP addresses across logs and confirmed brute-force attempts in DeviceLogonEvents.
- Mapped findings to MITRE ATT&CK techniques:
  - **T1046** – Network Service Scanning
  - **T1110** – Brute Force
  - **T1133** – External Remote Services
  - **T1078** – Valid Accounts (potential future risk)

All evidence (queries, screenshots, and results) was documented for reporting and future analysis.

Between October 25, 2025, at approximately 15:00 UTC, Virtual Machine: **Win11VMBruce** received 100 failed logon attempts from public IP 149.50.96.98.

The activity aligns with typical brute-force password attacks targeting RDP or SMB.

MITRE ATT&CK mapping: T1110 (Brute Force), T1133 (External Remote Services).

No successful logons were detected at this stage, indicating that the attempted intrusion did not result in unauthorized access.

---

**Improvement Summary:** This hunt demonstrated the effectiveness of exposing a controlled Virtual Machine for real-world observation. However, several improvements could enhance both detection and efficiency in future hunts:

### **Prevention Enhancements:**

- Configure **Network Security Groups (NSGs)** to allow only known IPs or use **Just-In-Time (JIT)** VM access in Azure to reduce attack surface.
- Deploy **Multi-Factor Authentication (MFA)** and **Network Level Authentication (NLA)** for RDP services.
- Regularly audit and close unnecessary ports on internet-facing systems.

### **Detection Enhancements:**

- Automate detection rules in Microsoft Sentinel for:
  - Repeated LogonFailed events from a single public IP.
  - Inbound traffic on unusual or high-numbered ports.
- Correlate logs across Defender and Sentinel to improve real-time awareness.

### **Process Improvements:**

- Set clear baselines for what constitutes normal inbound activity to reduce false positives.
- Schedule recurring hunts and implement watchlists for known malicious IPs.
- Continue refining KQL queries for greater efficiency and context correlation (e.g., linking DeviceLogonEvents with DeviceProcessEvents automatically).

### **Lesson Learned:**

Even though the firewall in the Virtual Machine was disabled, and the NSG settings within the Virtual Machine have a rule allowing “any” and “all,” the exercise confirmed that public exposure quickly attracts malicious activity. Preventing exposure through segmentation, hardening, and monitoring remains the most effective defense. As well as ensuring proper firewall settings and Network Security Group rules remain effective and running.

