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:

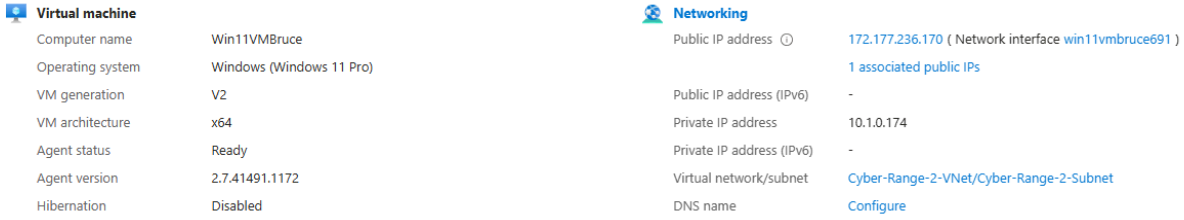
During routine maintenance, the security team is tasked with investigating any VMs in the shared services cluster (handling DNS, Domain Services, DHCP, etc.) that have mistakenly been exposed to the public internet. The goal is to identify any misconfigured VMs and check for potential brute-force login 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



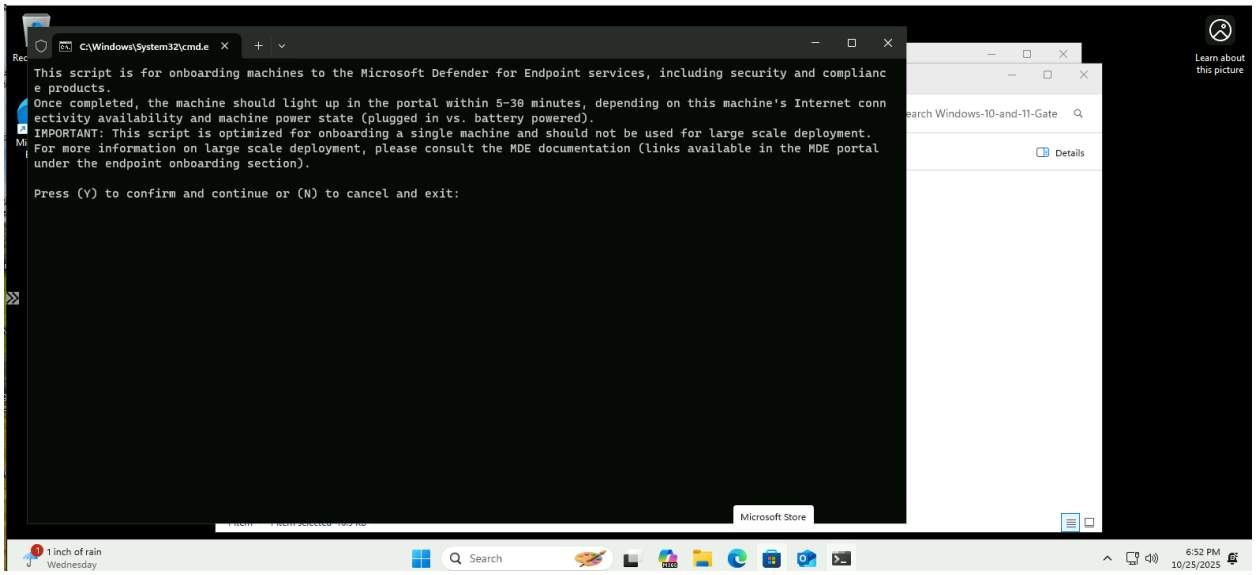
Virtual machine

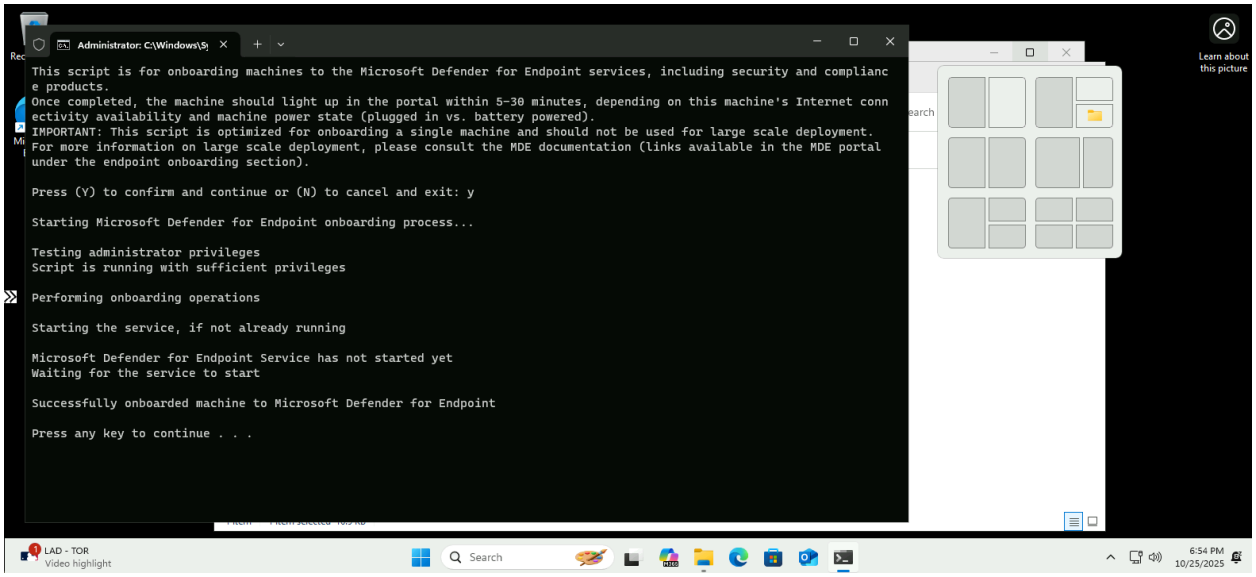
Computer name	Win11VMBruce
Operating system	Windows (Windows 11 Pro)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1172
Hibernation	Disabled

Networking

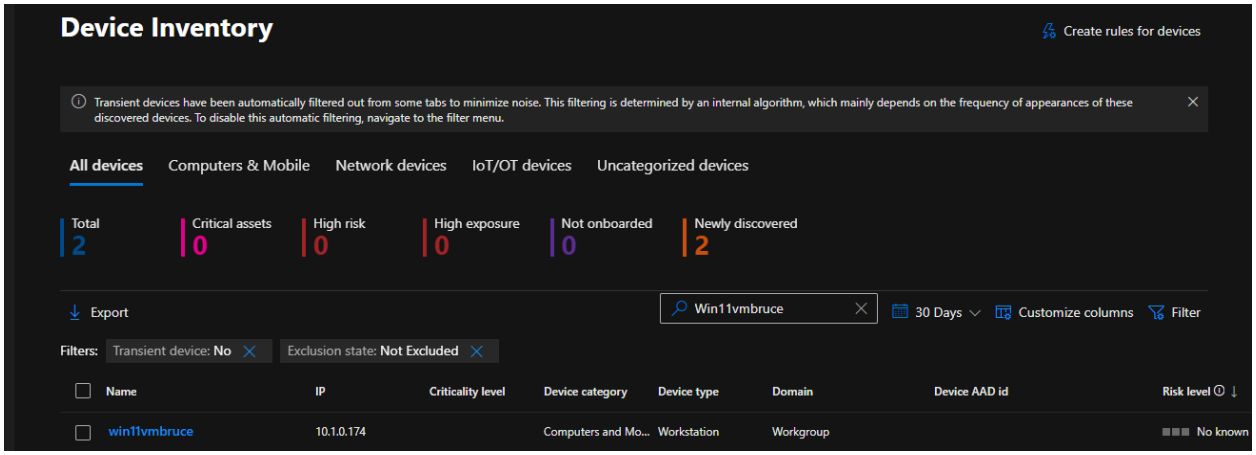
Public IP address	172.177.236.170 (Network interface win11vmbruce691)
	1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.1.0.174
Private IP address (IPv6)	-
Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet
DNS name	Configure

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.

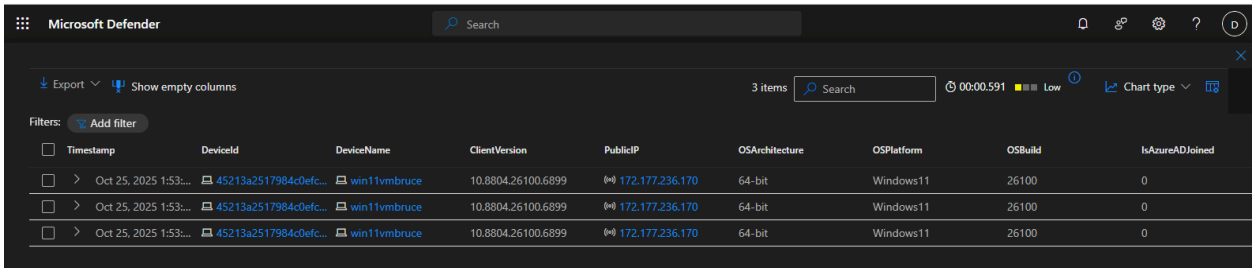
Query Used:

```
DeviceInfo

| where DeviceName has "Win11VMBruce"

| where PublicIP has "172.177.236.170"
```

Return in screenshot:



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

Verification

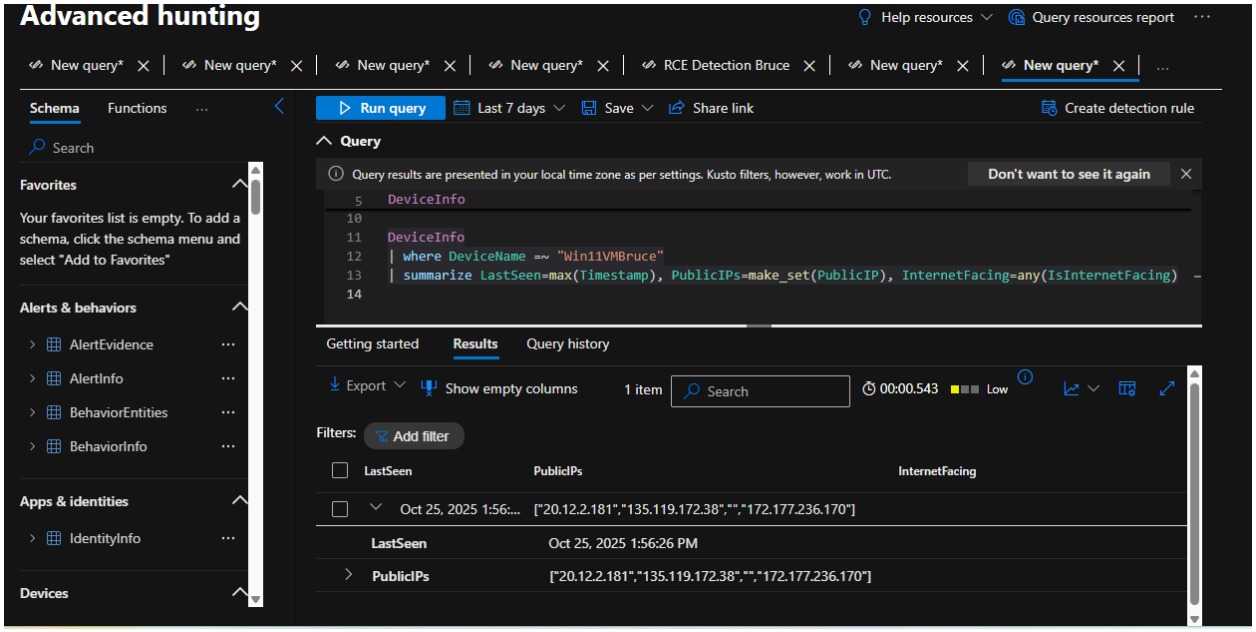
I will run these every 15–30 minutes:

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:



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.

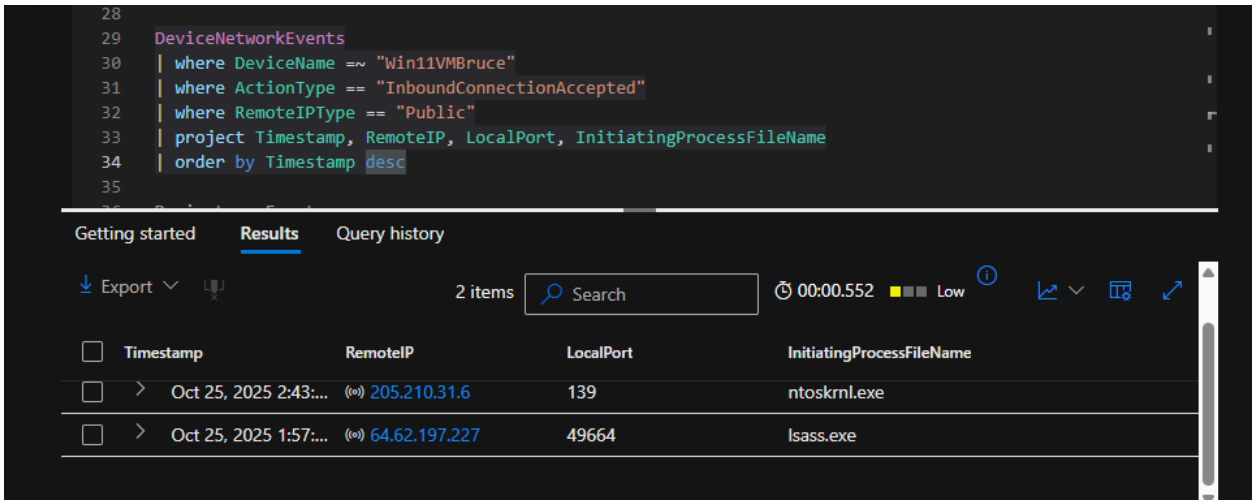
Now I will allow Win11VMBruce to be exposed to the Internet for some time and then investigate the findings. I will periodically run these commands to identify when suspicious activity begins and to begin investigation:

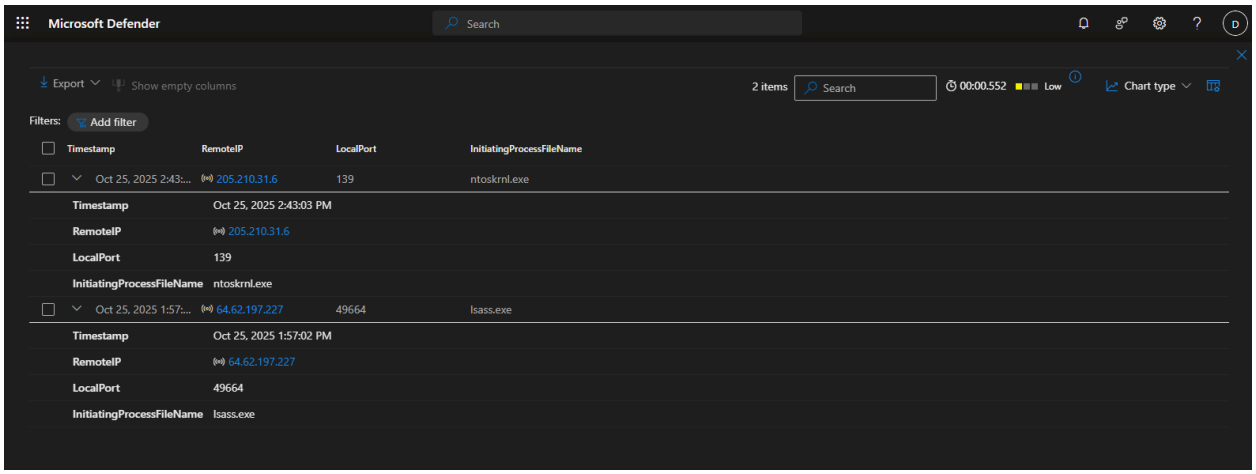
<u>Connection Detection, Verification of Inbound connections (any port) from public IPs</u>:

Queries Used:

```
DeviceNetworkEvents
| where DeviceName =~ "Win11VMBruce"
| where ActionType == "InboundConnectionAccepted"
| where RemoteIPType == "Public"
| project Timestamp, RemoteIP, LocalPort, InitiatingProcessFileName
| order by Timestamp desc
```

Evidence:

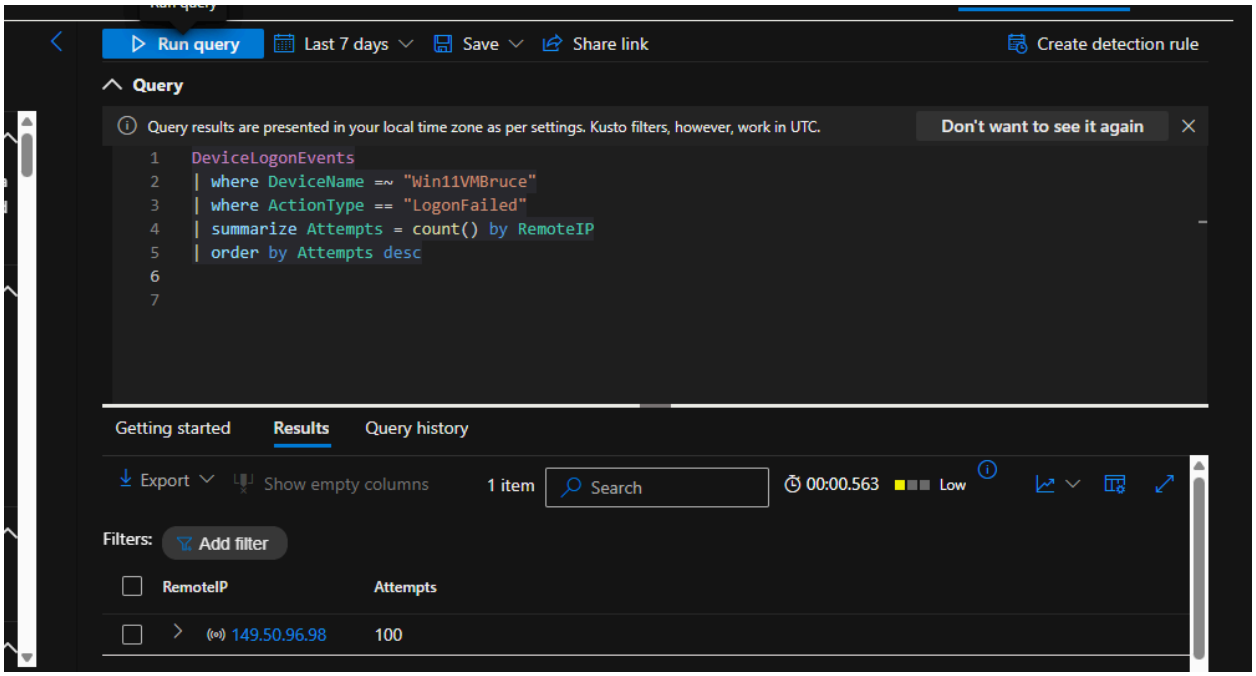


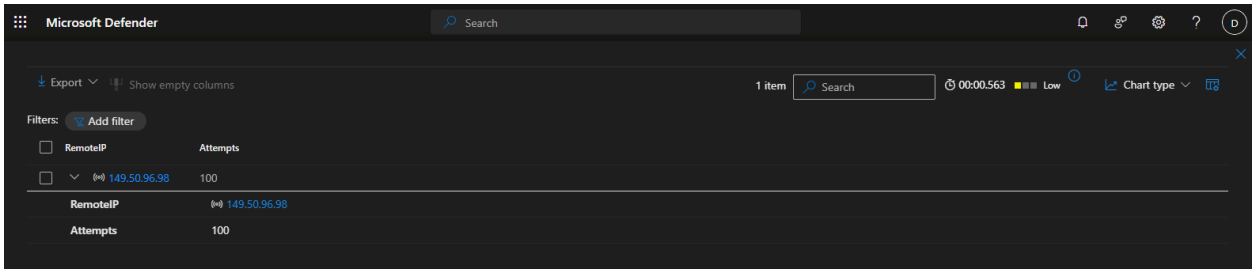


And:

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

Evidence:

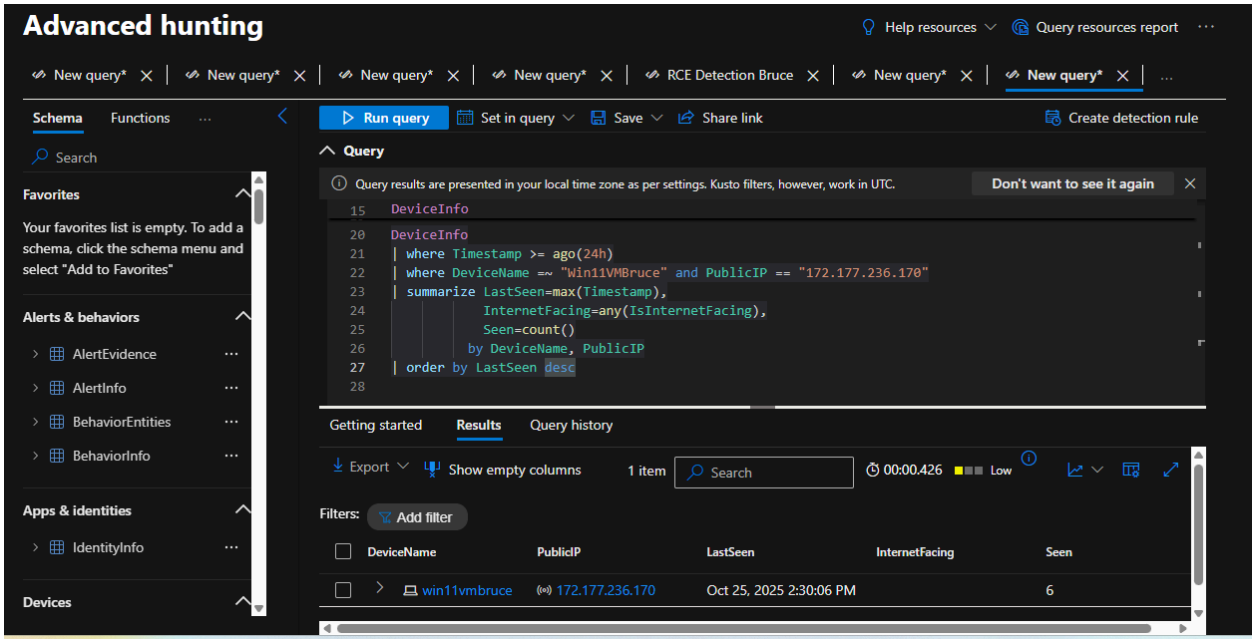




And:

```
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:

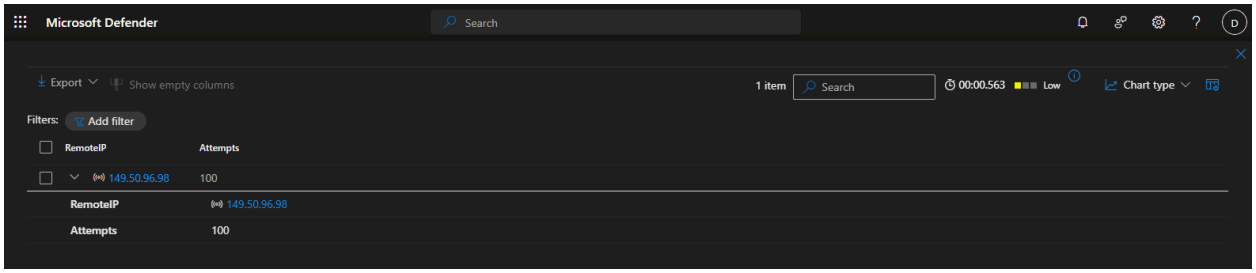


Why: First signs of scanners/bots actually touching the Virtual Machine Win11VMBruce from all three of these queries.

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:



From this Query:

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

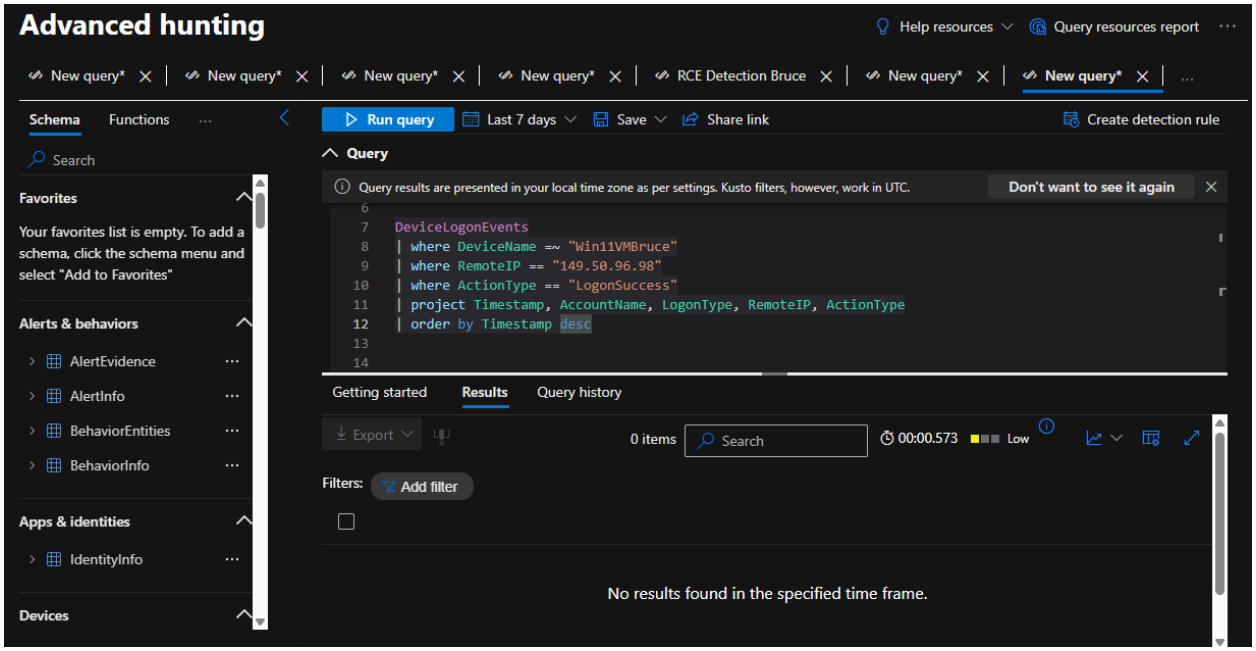
Query Used:

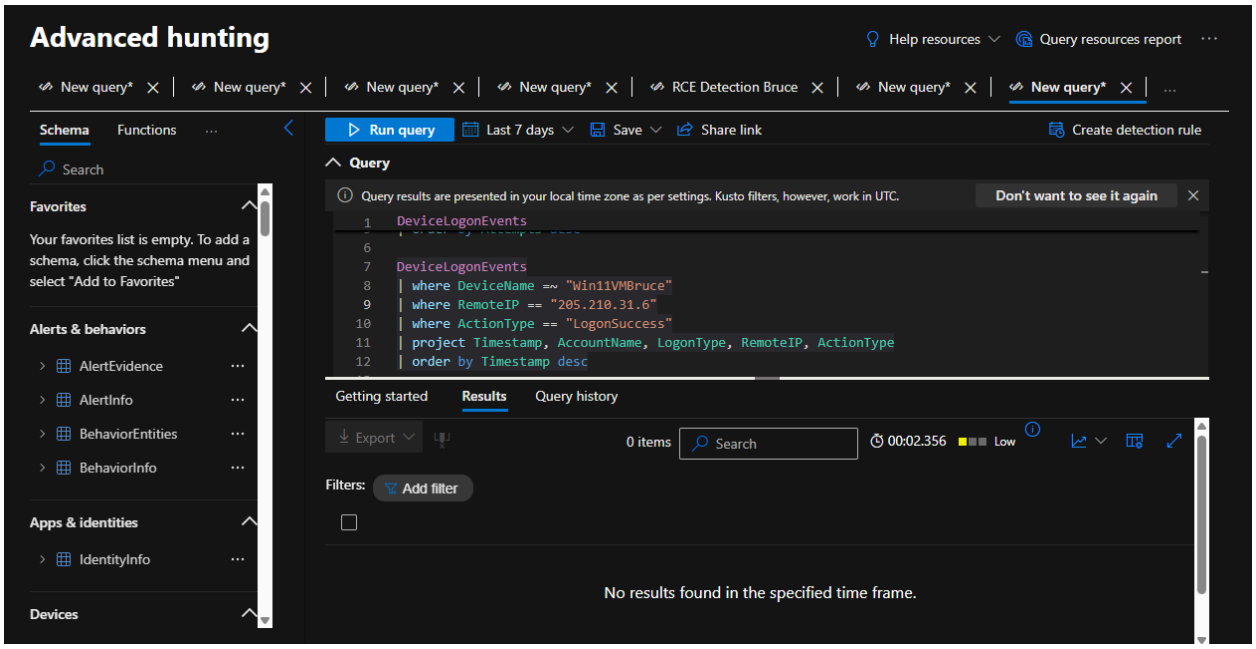
```
DeviceLogonEvents
| where DeviceName =~ "Win11VMBruce"
| where RemoteIP == "149.50.96.98"
| where ActionType == "LogonSuccess"
| project Timestamp, AccountName, LogonType, RemoteIP, ActionType
| order by Timestamp desc
```

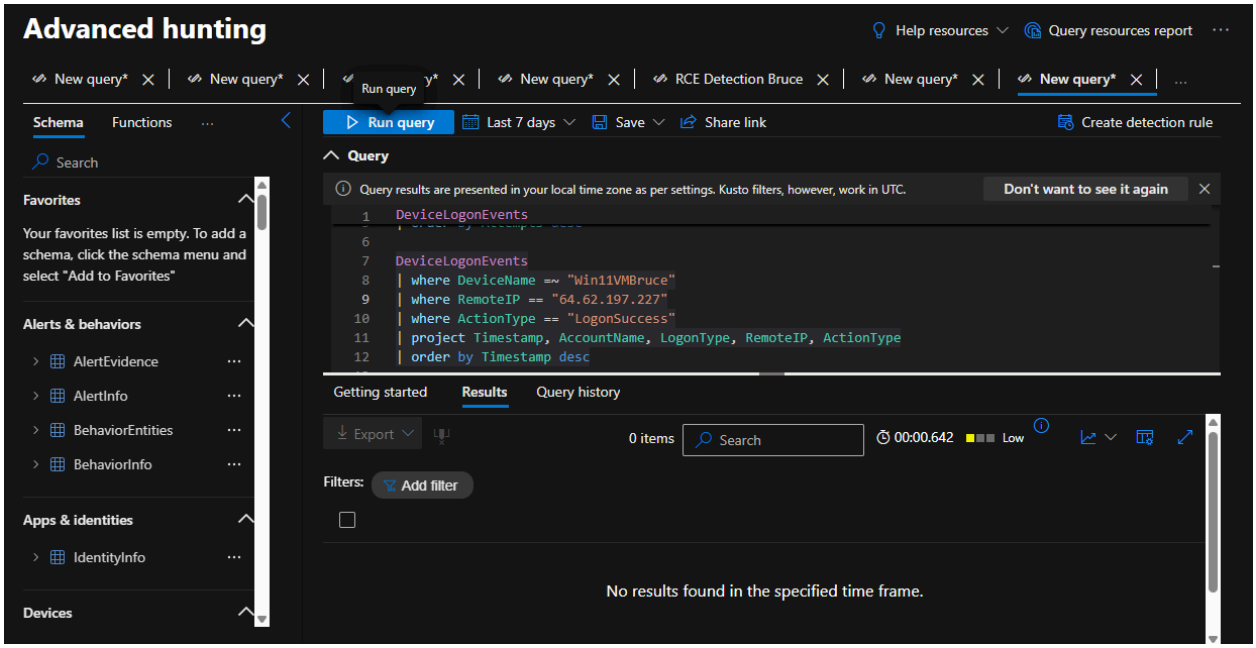
If I see any hits here, that means the brute-force **succeeded** — attackers found valid credentials and gained interactive access.

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

Evidence:







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 honeypot 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.