Lab #3: **Simulate an External Attacker (Failed Authentication & Log Observation)**

Purpose:

- We'll create a 3rd VM to simulate an external attacker. Afterwards, we'll use this VM to attempt to access unauthorized accounts.

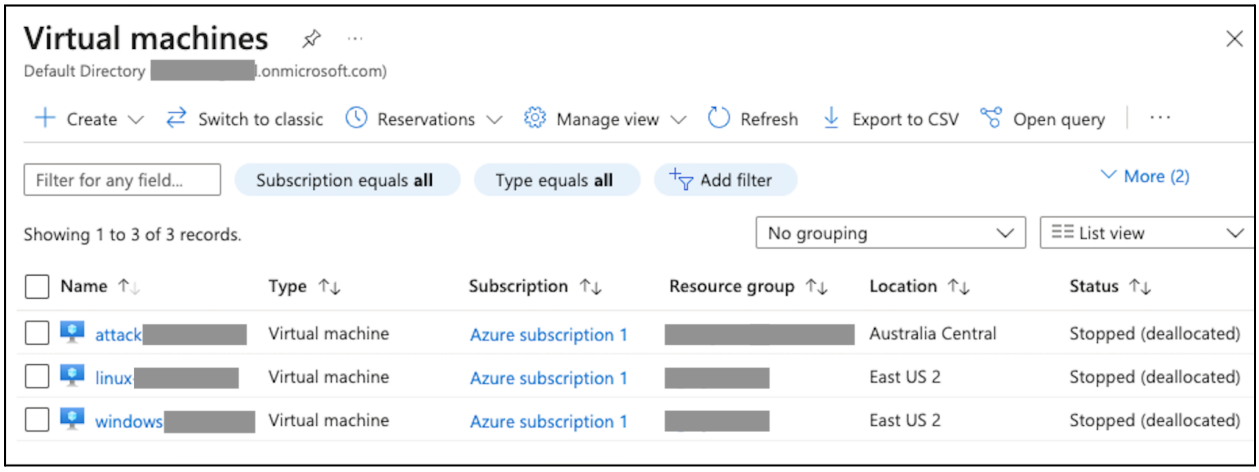
Tasks:

1. **Create a 3rd VM (Attacker VM)**
2. **Attempt unauthorized access (simulate an attacker)**
    - to windows-vm
    - to MS SQL
    - to linux-vm
3. **Inspect the failed login attempts**

Task 1: **Create a 3rd VM (Attacker VM)**

1. **Azure** account > **+Create a resource** > **Virtual Machines** > **Create**.
2. Assign the subscription, resource group, VM name ("attacker-vm"), region (Australia Central), image (Windows 10 Pro), admin credentials, and CPU usage.
3. Create a new **Virtual Network**.
4. Select **Review and Create**.

Note: *The screenshot below displays the 3 newly created lab VMs.*



5. Add this new VM to your PC's **Windows Remote Desktop** application.
    a. Locate the new VM's **public IP address** > add the new PC to the app > enter creds.

Task 2: **Attempt unauthorized access (simulate an attacker)**

to windows-vm:

1. Generate some failed **RDP logs** against windows-vm**:**
    a. From within attacker-vm, attempt to RDP into windows-vm using **incorrect credentials** (3x).

to MS SQL:

1. Generate some failed **MS SQL Auth logs** against windows-vm:
    a. Still within attacker-vm, install **SSMS** (if not already installed).
    b. Open SSMS > Authentication: SQL > attempt to log in using **incorrect credentials** (3x).
    c. In SSMS, now log in using **correct credentials**.
    d. Disconnect from the server, and close the app.

to linux-vm:

1. Generate some failed **SSH logs** against linux-vm:
    a. Still within attacker-vm, attempt to SSH into linux-vm with the wrong credentials (3x).
    b. Shut down attacker-vm.

Task 3: Inspect the failed login attempts

1. Log into windows-vm > open **Event Viewer** and inspect the failures and successes (Security Log for RDP, Application Log for SQL).

    Note: *Take note of the EventIDs, messaging, Source IP Addresses, etc.*

2. Open terminal/PowerShell on your personal PC.

    Note: *We'll now SSH into linux-vm (to observe its logs).*

    - **ssh labuser@<Linux VM IP>**
    - **cd /var/log**
    - **ls** (we can see __.log files)
    - Try **ls -lasht** to get a better view.
    - Dump the contents of this log, and search for "password" → **cat auth.log | grep password**

```
4.0K drwxr-xr-x   2 root      root            4.0K Oct 25 21:54 apt
4.0K drwxr-xr-x  13 root      root            4.0K Oct 25 21:51 ..
4.0K drwxr-xr-x   2 root      root            4.0K Mar 14  2023 dist-upgrade
4.0K drwxr-xr-x   2 _chrony   _chrony         4.0K Aug 25  2020 chrony
labuser@linux-vm:/var/log$ cat auth.log | grep password
Nov  3 16:41:47 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 16:41:51 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 16:41:52 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 16:41:55 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 16:41:58 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 16:42:02 linux-vm sshd[13559]: Failed password for invalid user ubnt from 211.199.84.78 port 51536 ssh2
Nov  3 17:00:29 linux-vm sshd[13579]: Accepted password for [redacted] from [redacted] port 54485 ssh2
Nov  3 18:23:01 linux-vm sshd[13842]: Failed password for root from 104.248.26.212 port 44732 ssh2
Nov  3 18:23:06 linux-vm sshd[13844]: Failed password for root from 104.248.26.212 port 53916 ssh2
Nov  3 18:23:10 linux-vm sshd[13846]: Failed password for root from 104.248.26.212 port 53918 ssh2
Nov  3 18:23:13 linux-vm sshd[13848]: Failed password for invalid user ossuser from 104.248.26.212 port 59894 ssh2
Nov  3 18:30:40 linux-vm sshd[13870]: Failed password for invalid user josh from 20.213.250.233 port 50466 ssh2
Nov  3 18:30:48 linux-vm sshd[13870]: Failed password for invalid user josh from 20.213.250.233 port 50466 ssh2
Nov  3 18:30:54 linux-vm sshd[13870]: Failed password for invalid user josh from 20.213.250.233 port 50466 ssh2
Nov  3 18:45:50 linux-vm sshd[13907]: Accepted password for [redacted] from [redacted] port 55714 ssh2
labuser@linux-vm:/var/log$
```

    - Now, disconnect from the SSH session: **exit**

3. Stop all of the running VMs.

End:

- We've created a 3rd VM to simulate an external attacker. We then used this VM to attempt to access unauthorized accounts.