

# Azure Security Lab by Golam Tanvir Rahman

1. I created all the resources for this project under one resource group

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot button. The main content area displays the 'RG-SOC-Lab' resource group. The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The 'Overview' tab is selected, showing a list of resources. The resources listed are:

| Name   | Type                    | Location |
|--|-------------------------|----------|
| 5e5f5d7a-be73-4420-bac1-6405c6fb4016 (Windows VM attack map) | Azure Workbook          | East US  |
| DCR- Windows   | Data collection rule    | East US  |
| Log-SOC-Lab  | Log Analytics workspace | East US  |
| SecurityInsights(log soc lab)                                | Solution                | East US  |
| SenecaVM23   | Virtual machine         | East US  |
| SenecaVM23-ip  | Public IP address       | East US  |
| SenecaVM23-nsg   | Network security group  | East US  |
| SenecaVM23689  | Network interface       | East US  |
| SenecaVM23_OrDisk_1_9862cb132c9a49308062ed41f790baef         | Disk                    | East US  |
| Vnet SOC Lab   | Virtual network         | East US  |

2. I allowed all inbound traffic from all sources in NSG

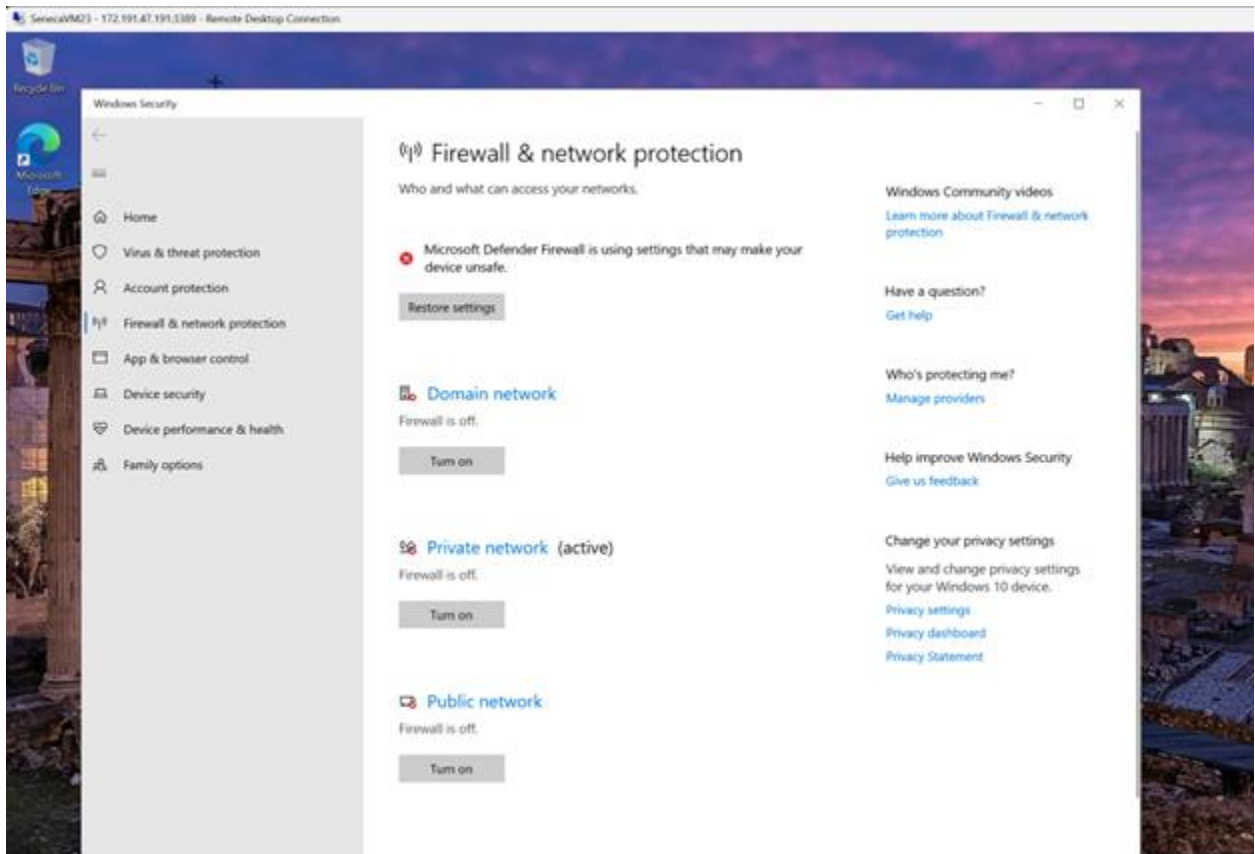
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot button. The main content area displays the 'SenecaVM23-nsg' network security group. The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, and Help. The 'Overview' tab is selected, showing a list of security rules. The rules listed are:

| Priority | Name                          | Port | Protocol | Source     |
|----------|-------------------------------|------|----------|------------|
| 100      | AllowAnyCustomAnyInbo...      | Any  | Any      | Any        |
| 65000    | AllowVnetInbound              | Any  | Any      | Virtual... |
| 65001    | AllowAzureLoadBalancerInBo... | Any  | Any      | AzureLo... |
| 65500    | DenyAllInBound                | Any  | Any      | Any        |
| 65000    | AllowVnetOutBound             | Any  | Any      | Virtual... |
| 65001    | AllowInternetOutBound         | Any  | Any      | Any        |
| 65500    | DenyAllOutBound               | Any  | Any      | Any        |

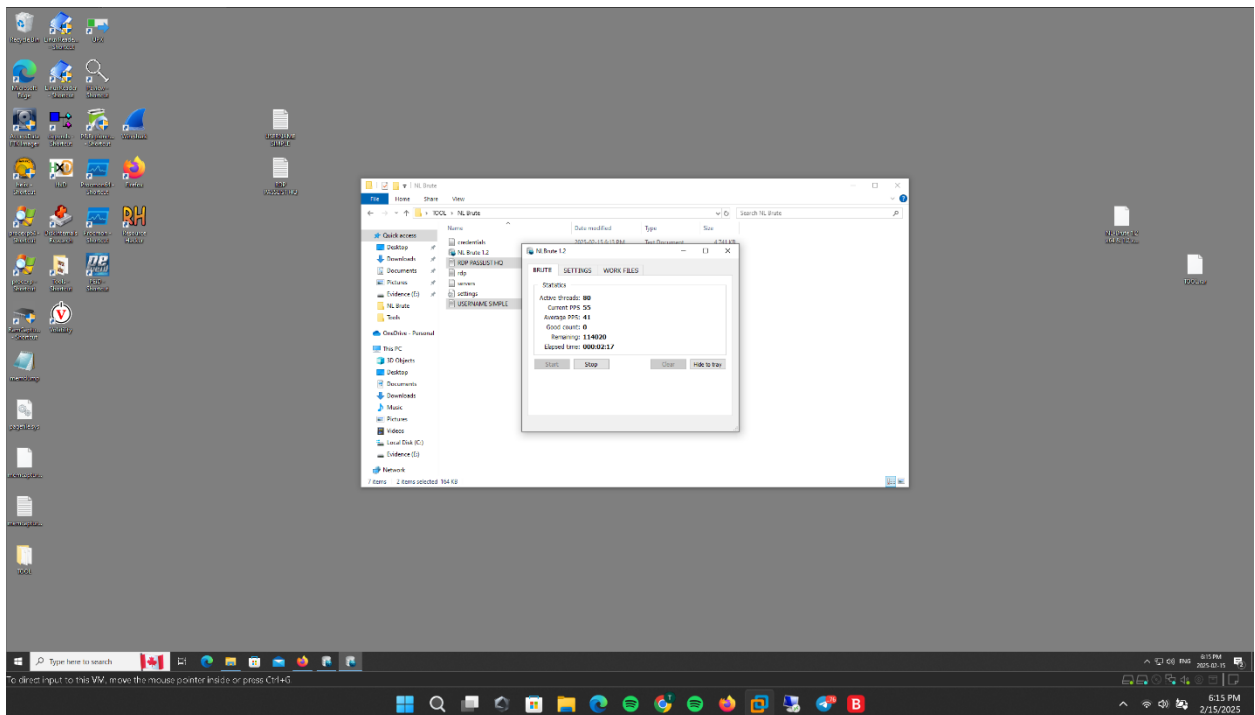
The 'Settings' tab is also visible, showing the configuration for the custom rule 'AllowAnyCustomAnyInbound'. The configuration includes:

|  |  |
| --- | --- |
| Source | Any |
| Source port ranges | \* |
| Destination | Any |
| Service | Custom |
| Destination port ranges | \* |
| Protocol | Any |
| Action | Allow |
| Priority | 100 |
| Name | AllowAnyCustomAnyInbound |
| Description |  |

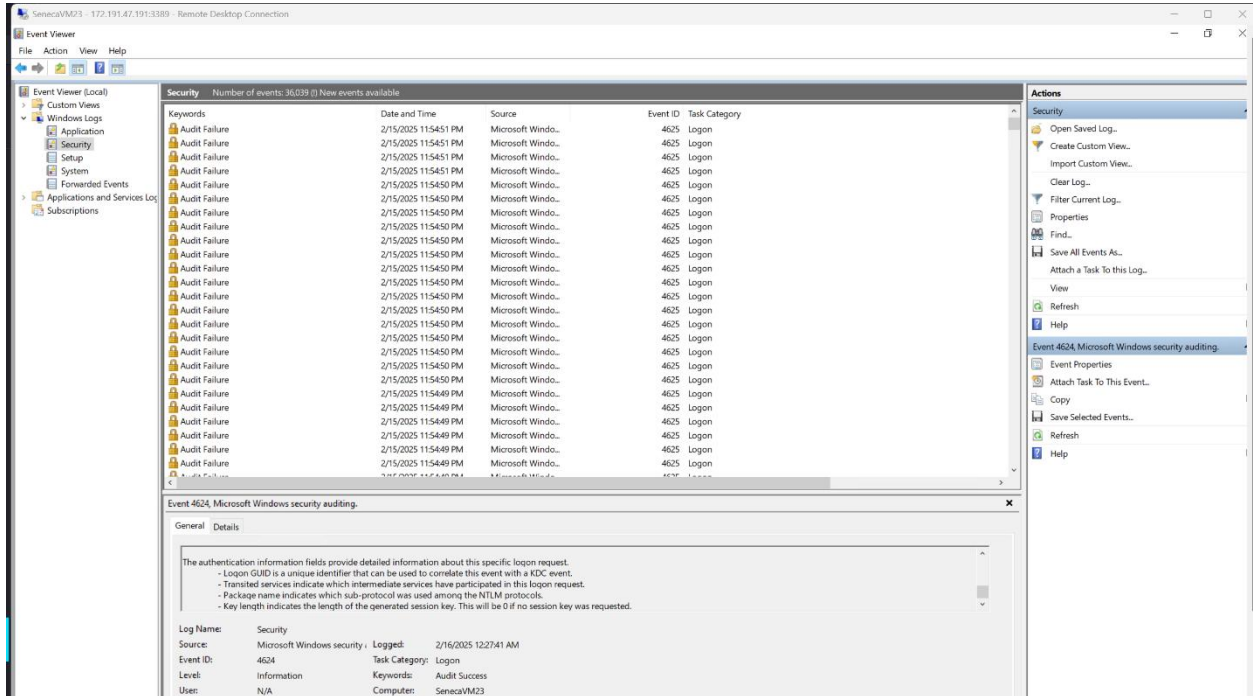
3. I made the vm vulnerable to the public internet



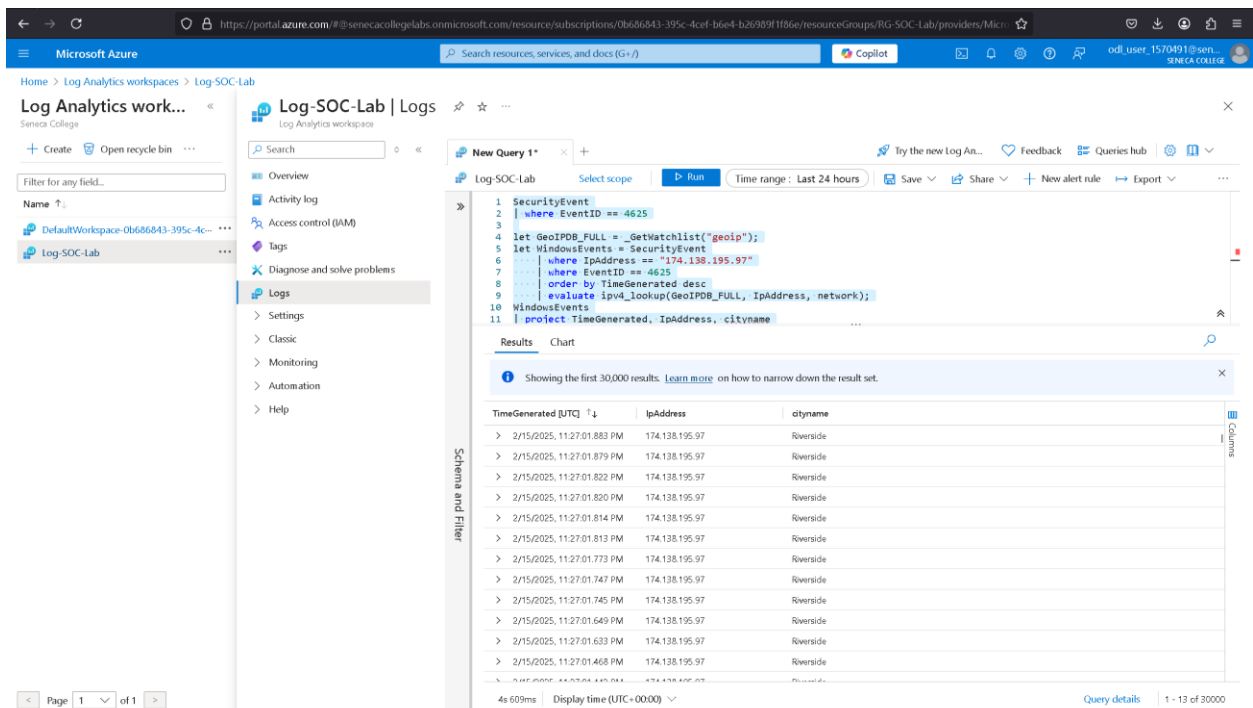
4. I simulated failed login using a brute force tool called NLbrute



## 5. Inspected the security log via the event viewer



## 6. I configured a Microsoft Sentinel instance and connected it to the workspace to query the log from the VM



## 7. Created an attack map within a sentinel

