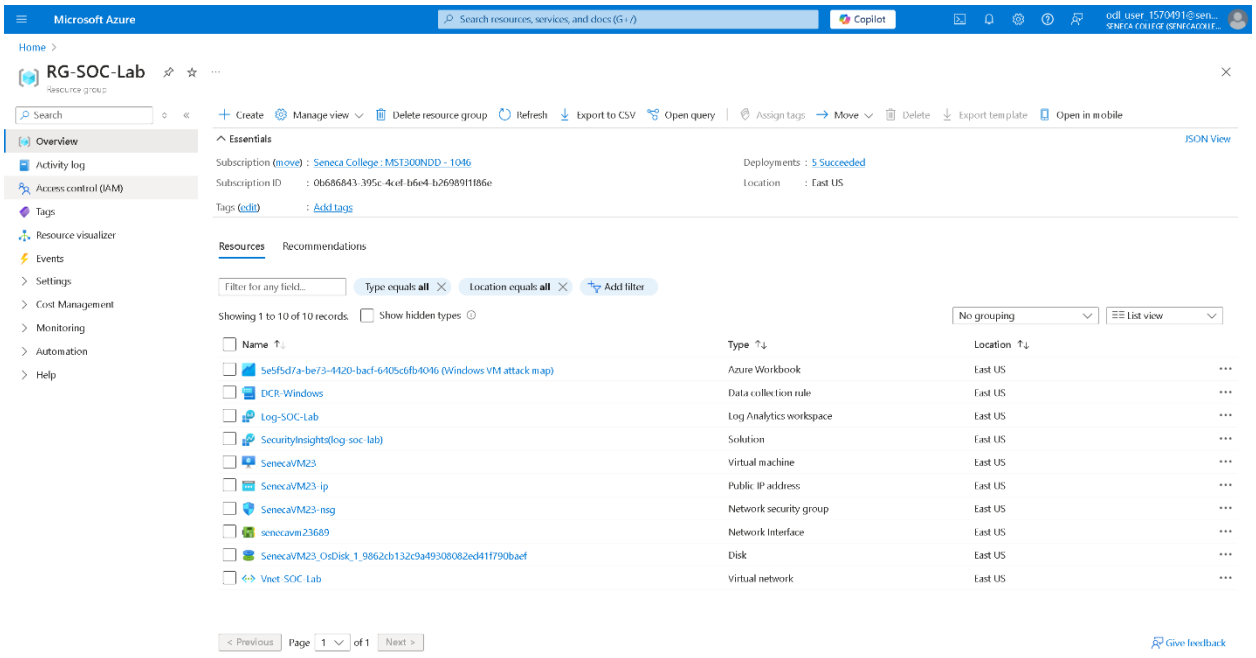
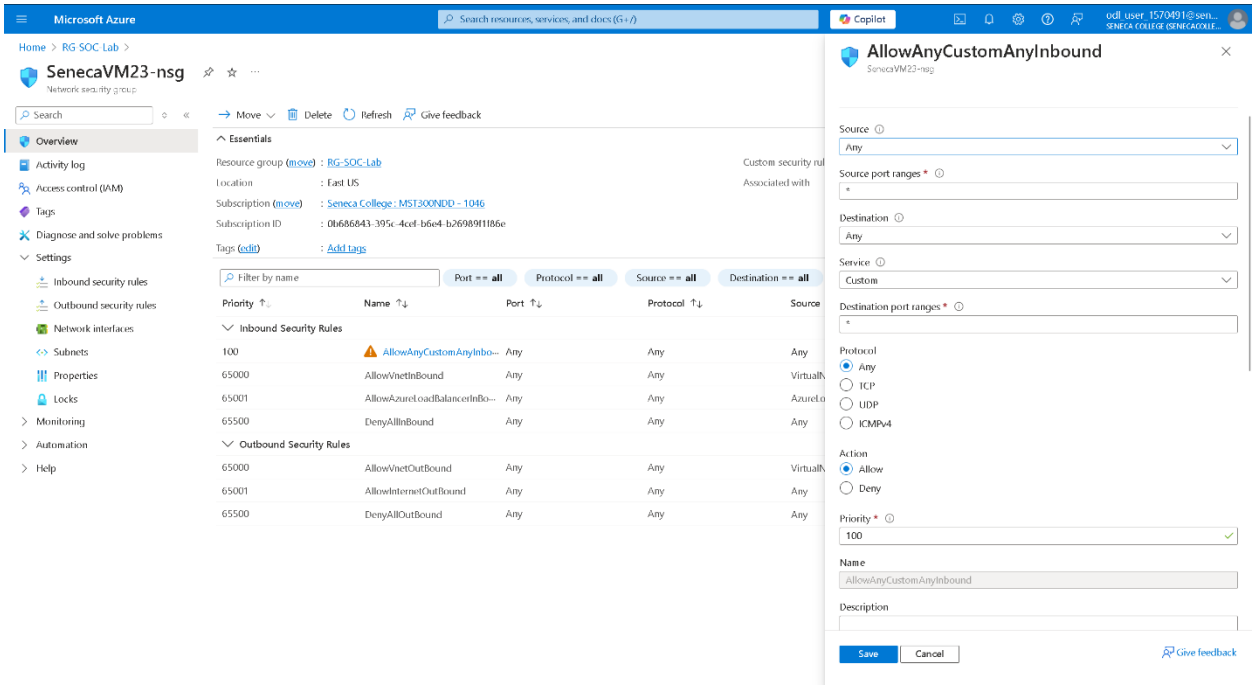
Azure Security Lab by Golam Tanvir Rahman

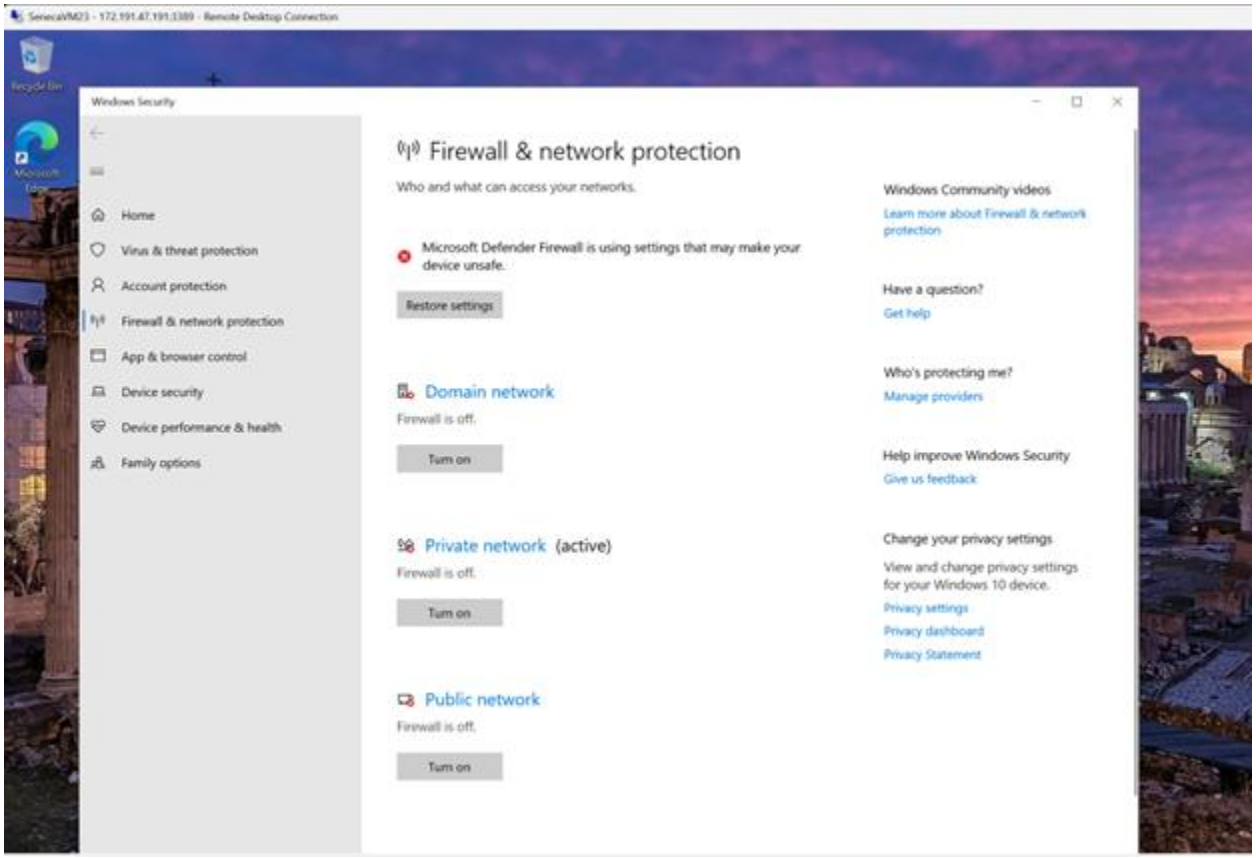
1. I created all the resources for this project under one resource group



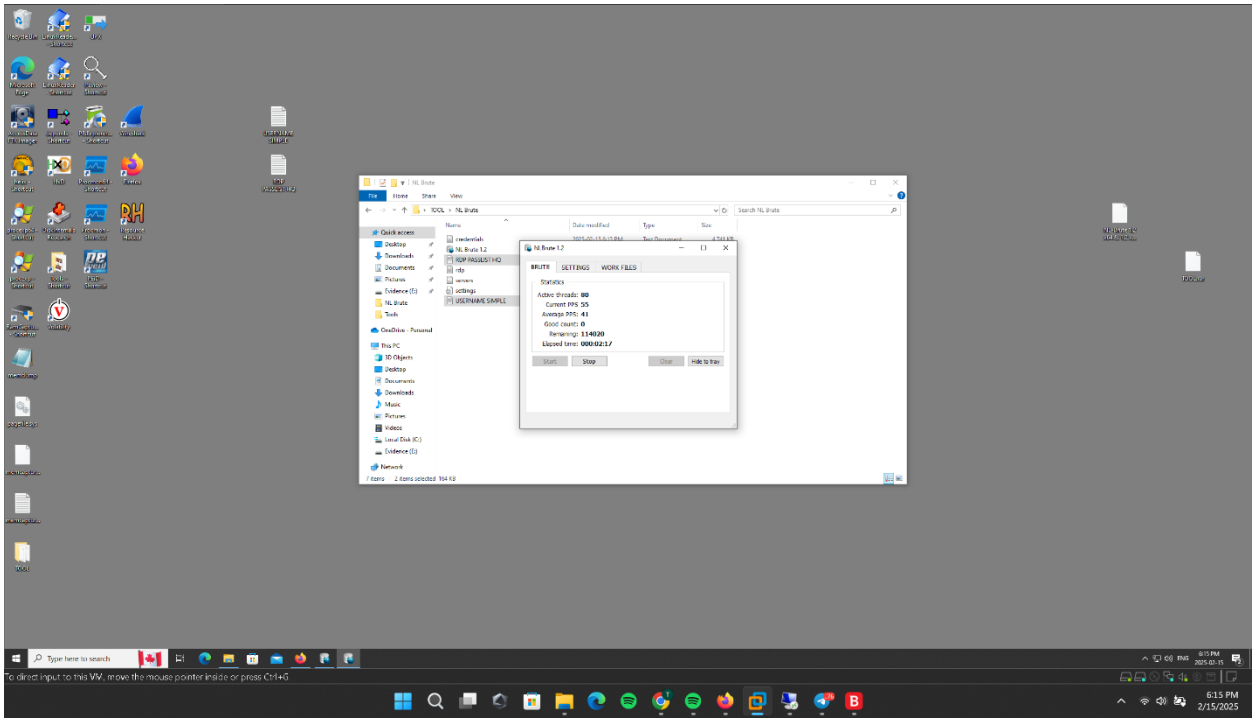
2. I allowed all inbound traffic from all sources in NSG



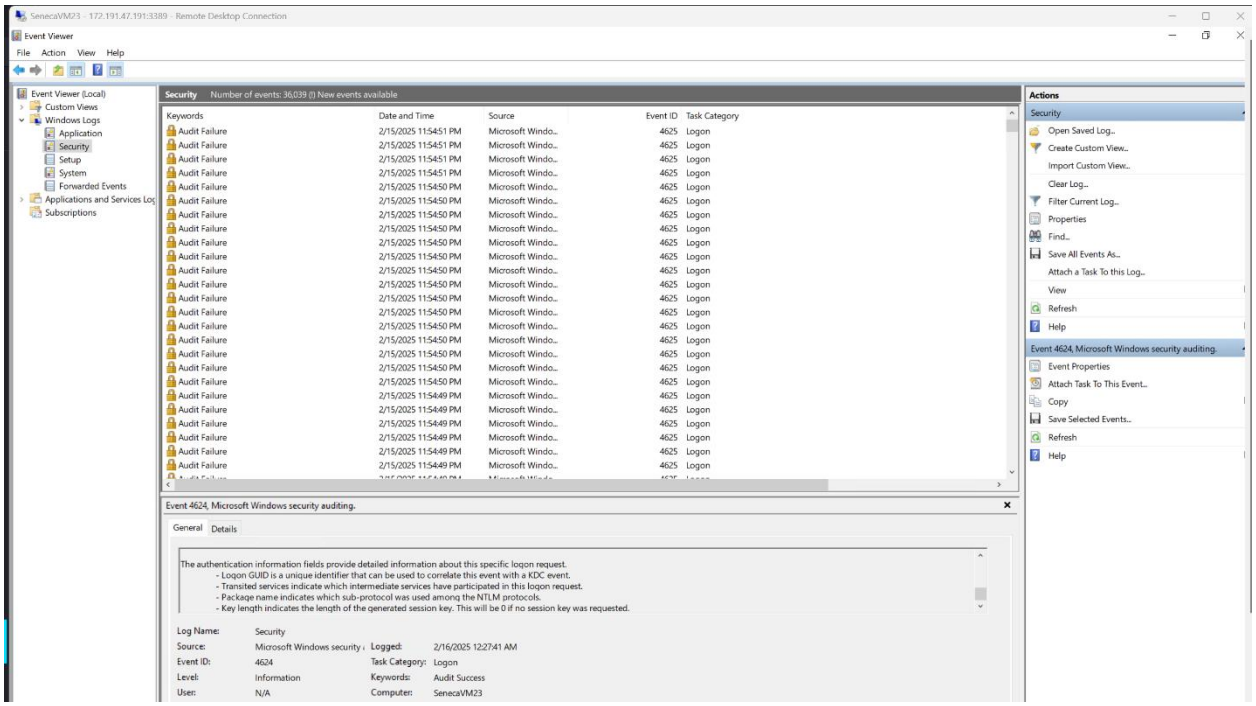
3. I made the vm vulnerable to the public internet



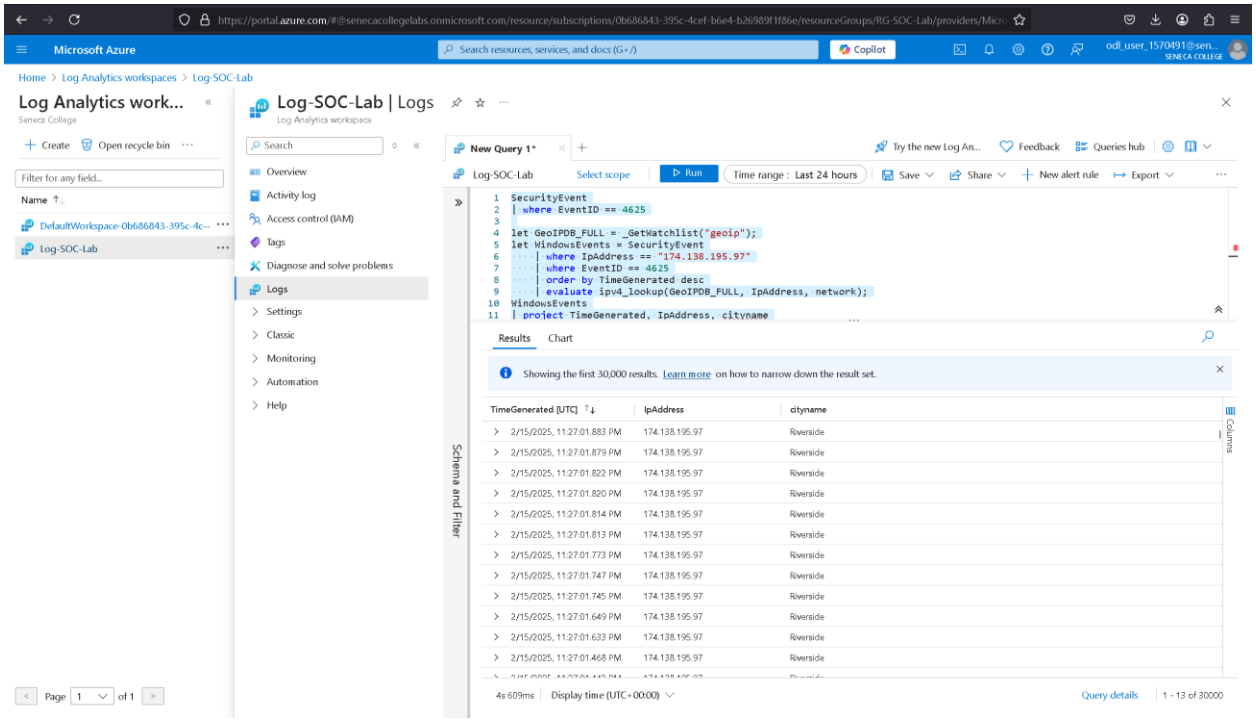
4. I simulated failed login using a brute force tool called NLbrute



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