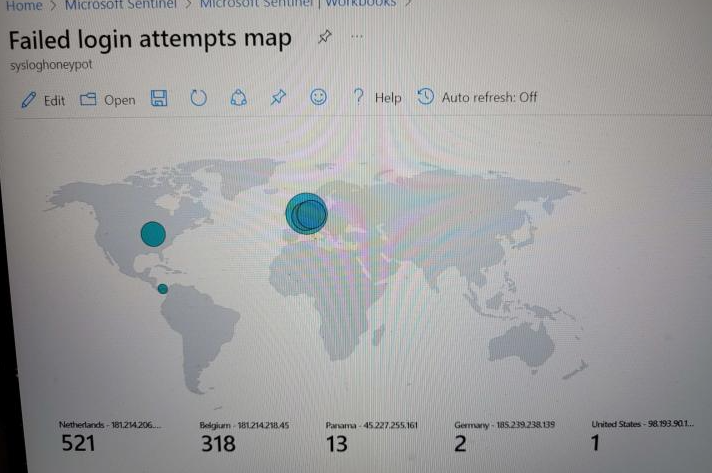
Just to get some experience with setting up a SIEM, I decided to tinker around in MS Azure, as I have some work experience with the software.

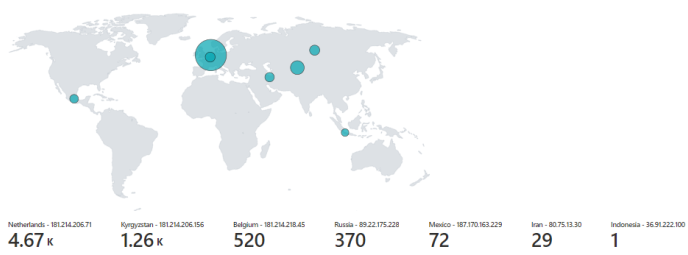
First, I spun up a VM to act as a honeypot, then permitted RDP connections, and removed a lot of the necessary firewall restrictions for external threat actors to find and attempt connection to the VM.

Within the virtual desktop, I set up a powershell script from [this github repo](https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1) to pick up information from Windows Event viewer event ID 4625 (account login failure), and pipe out to a .log file. The information contained included the username used to access the VM, the IP of the user, and the location using the [ipgeolocation](http://ipgeolocation.io/) api.

Within azure, I permitted connections from the VM to a log workspace to collect info from the .log, and use Microsoft Sentinel. Within Sentinel, I created a personalized workbook to plot the location of the attackers on the globe, and associating with the IP of any attackers.

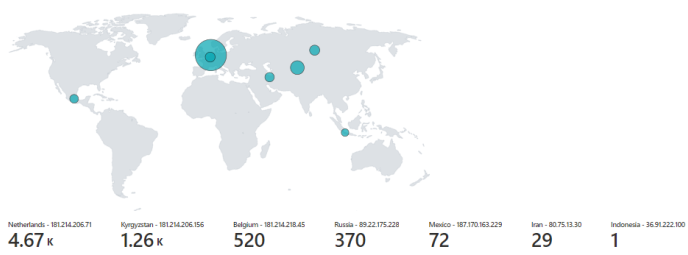
I set up the VM on Thursday evening, 2/2/23 8:23PM CST, and by 12:09PM, Friday 2/3/23 the workbook logged the following attackers and associated location:

  
Now, mind you, I never posted the IP address of the VM anywhere. Just a brief reminder that even if info isn’t published directly, attackers can, and will find it using IP vulnerability scanners



The next image was taken on 2/4/23 at 12:05PM CST, showing that existing attackers, once they found a vulnerability persisted, and other attackers also joined in. Now, of course, one can never be too sure if these attackers are located where they are, thanks to IP spoofing and usage of VPNs.

The last picture was taken at 2/4/23 at 2:23PM CST, shortly before decommissioning the VM:

  
  
As you can see, there wasn’t much change after the couple of hours between pictures. Regardless, within 48 hours, assuming no IP spoofing, there were seven different attackers able to find and attempt to login. I have no doubt that if I kept the machine running, more attackers would find it, either naturally or by bots used to dig around and locate vulnerable networks.

This shows, that no matter what network you work in, there needs to be a policy for a solid firewall to minimize unwarranted logins, along with strong passwords and MFA to ensure the integrity of the network and to put a stop, if not greatly slow down brute force attacks.