Building a SIEM to Analyze RDP Attempts

by: Jake Enea

February 2022

Introduction

This lab will utilize Microsoft Azure and some of its features to build a SIEM through Azure Sentinel. This SIEM will receive data from a virtual machine built to accept packets from everywhere and act as a honeypot for attacks from around the world. These attackers will attempt to remotely access the virtual machine using brute force to try and guess the username and password of the machine. A PowerShell script will be run on the virtual machine to output all failed remote desktop protocol (RDP) attempts to a log file which will then be used to display where these RDP attempts are coming from on a map.

This lab was inspired and based off a video by Josh Madakor on YouTube.

Process

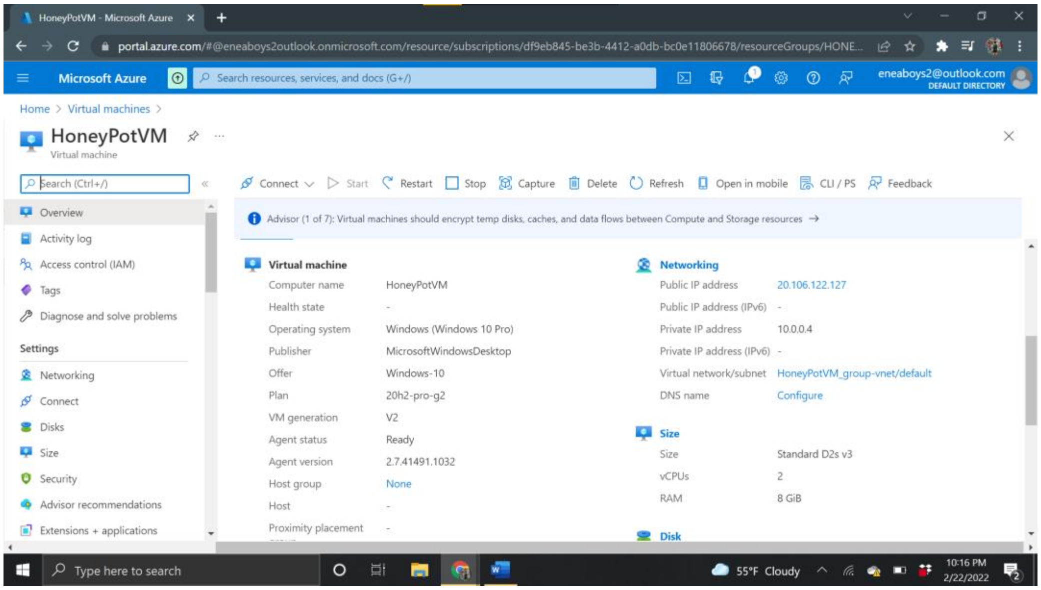
Azure Setup

To begin, you must first register for a free Microsoft Azure account by going to azure.microsoft.com. The website will require you to enter a credit card, but if you choose the free version of Azure, you will not be charged.

Once your Azure account has been created, go to portal.azure.com to access your Azure portal. The first step we are going to take is creating the **virtual machine** that will be designed to act as a honeypot. The goal of the virtual machine is for it to be left out on the internet unprotected to attract attackers.

Virtual machine configuration:

- Resource group: HoneyPotVM_group
- Name: HoneyPotVM
- Region: US West 3
- Image: Windows 10 Pro
- Username: eneavm
- NIC Network Security Group: Advanced
    - Create new inbound rule (allow all traffic from the internet into virtual machine)
        - Destination port ranges: * (allow all ports to be accessible)
        - Priority: 100 (low)



HoneyPotVM

Virtual machine

Advisor (1 of 7): Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources →

Virtual machine

Computer name	HoneyPotVM
Health state	-
Operating system	Windows (Windows 10 Pro)
Publisher	MicrosoftWindowsDesktop
Offer	Windows-10
Plan	20h2-pro-g2
VM generation	V2
Agent status	Ready
Agent version	2.7.41491.1032
Host group	None
Host	-
Proximity placement	-

Networking

Public IP address	20.106.122.127
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	HoneyPotVM_group-vnet/default
DNS name	Configure

Size

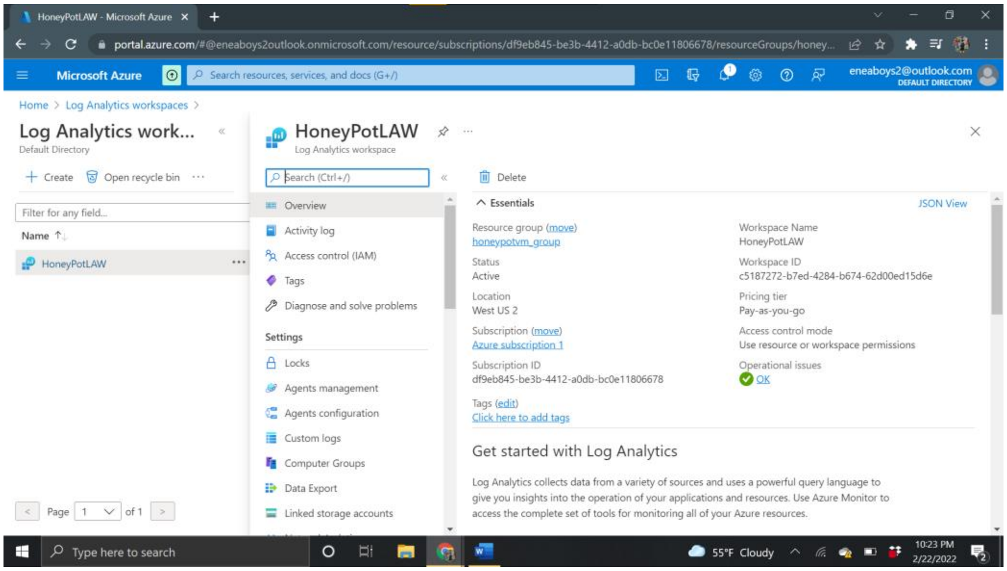
Size	Standard D2s v3
vCPUs	2
RAM	8 GiB

Disk

The next thing we will create is a **log analytics workspace** (LAW). This workspace will receive logs from the virtual machine that will allow it to build custom logs to derive geographic information of failed RDP attempts.

Log analytics workspace configuration:

- Resource group: HoneyPotVM_group
- Name: HoneyPotLAW
- Region: US West 2



HoneyPotLAW

Log Analytics workspace

Essentials

Resource group (move)
honeypotvm_group

Status
Active

Location
West US 2

Subscription (move)
Azure subscription 1

Subscription ID
df9eb845-be3b-4412-a0db-bc0e11806678

Tags (edit)
Click here to add tags

Workspace Name
HoneyPotLAW

Workspace ID
c5187272-b7ed-4284-b674-62d00ed15d6e

Pricing tier
Pay-as-you-go

Access control mode
Use resource or workspace permissions

Operational issues
✓ OK

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

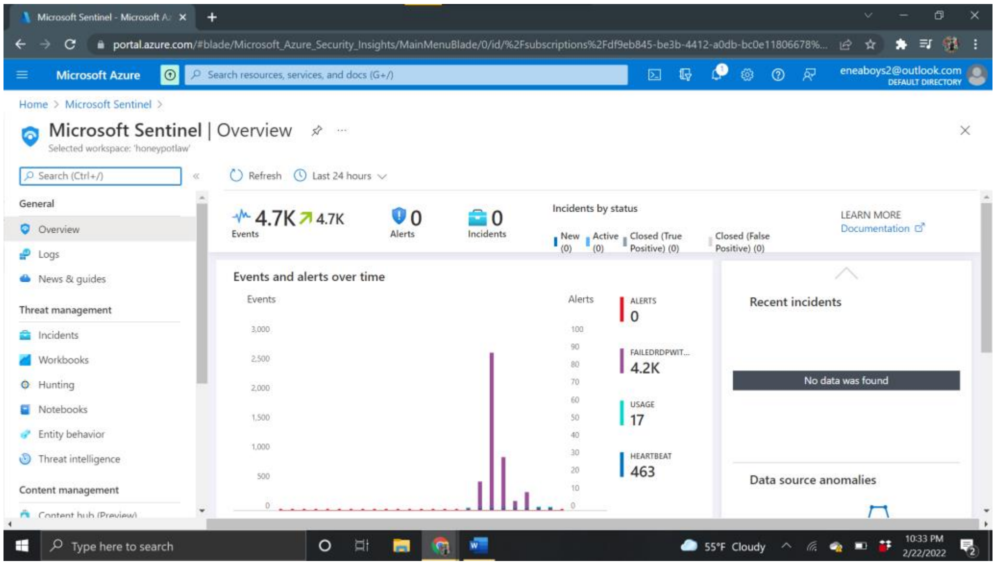
In order for the log analytics workspace to be able to receive logs from the virtual machine, we must first allow this in the Windows Defender for Cloud settings on Azure. Go to environment settings and do the following.

Windows Defender for Cloud configuration:

- Azure defender
    - SQL servers on machines: off
- Auto provisioning (data collection)
    - Log analytics for Azure VMs: on
        - Connect VMs to LAW
        - Store all events

Once these settings have been adjusted, we can now connect the LAW to the VM. This can be done through the LAW virtual machines tab.

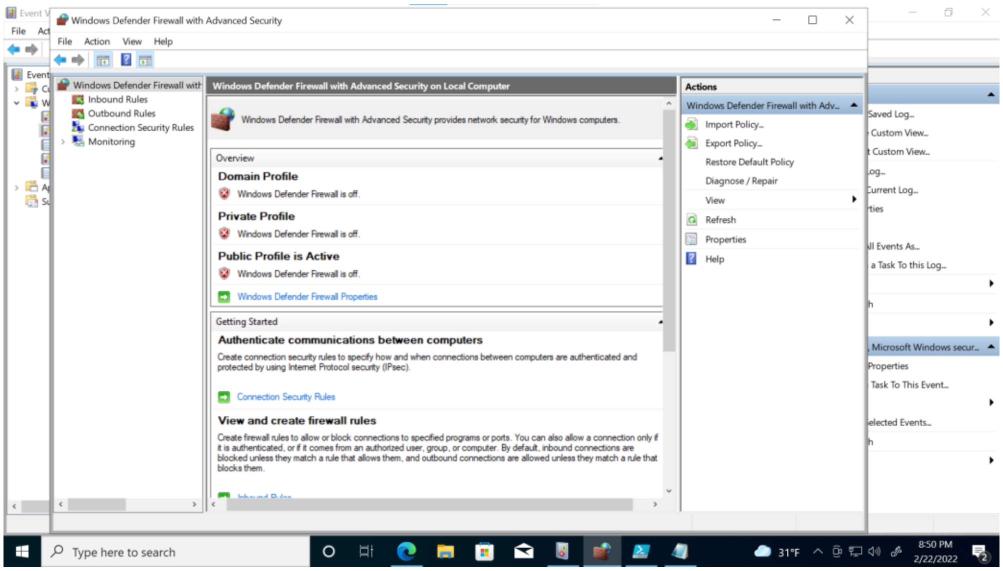
After connecting the LAW to the VM, we can now create the **Azure Sentinel**, which will act as the SIEM in this lab. This can simply be done by creating a new sentinel and connecting it to our LAW.



Accessing the VM and Getting the Logs with Geographic Data

Now that Azure has been configured, we need to access our VM and obtain the logs needed to continue. To access the VM, simply use Remote Desktop Connection and type in the public IP address of the VM. After that enter the credentials needed to log in to the virtual machine and accept any certificates needed.

The first thing we want to do is **turn off the firewall in the VM**. To do this we type wf.msc into the Windows search bar and turn off all firewall profiles in the Windows Defender Firewall Properties.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile
Windows Defender Firewall is off.

Private Profile
Windows Defender Firewall is off.

Public Profile is Active
Windows Defender Firewall is off.

Windows Defender Firewall Properties

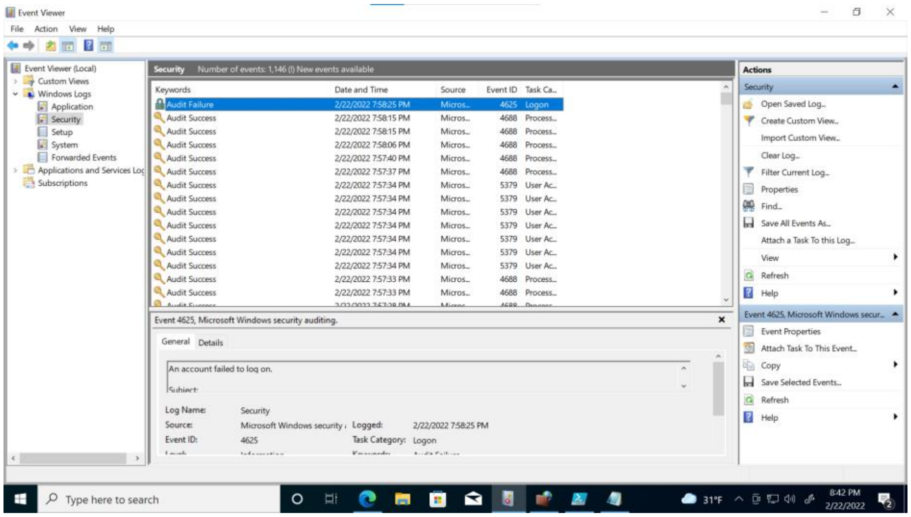
Getting Started

Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

You can use **event viewer** to see security events going on, including audit successes and failures, which is what will be saved in log files. You can also test this out by trying to remotely log into the VM again but with incorrect credentials.



Security Number of events: 1,146 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit Failure	2/22/2022 7:58:25 PM	Micros...	4625	Logon
Audit Success	2/22/2022 7:58:15 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:58:15 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:58:06 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:57:40 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:57:37 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:34 PM	Micros...	5379	User Ac...
Audit Success	2/22/2022 7:57:33 PM	Micros...	4688	Process...
Audit Success	2/22/2022 7:57:33 PM	Micros...	4688	Process...

Event 4625, Microsoft Windows security auditing.

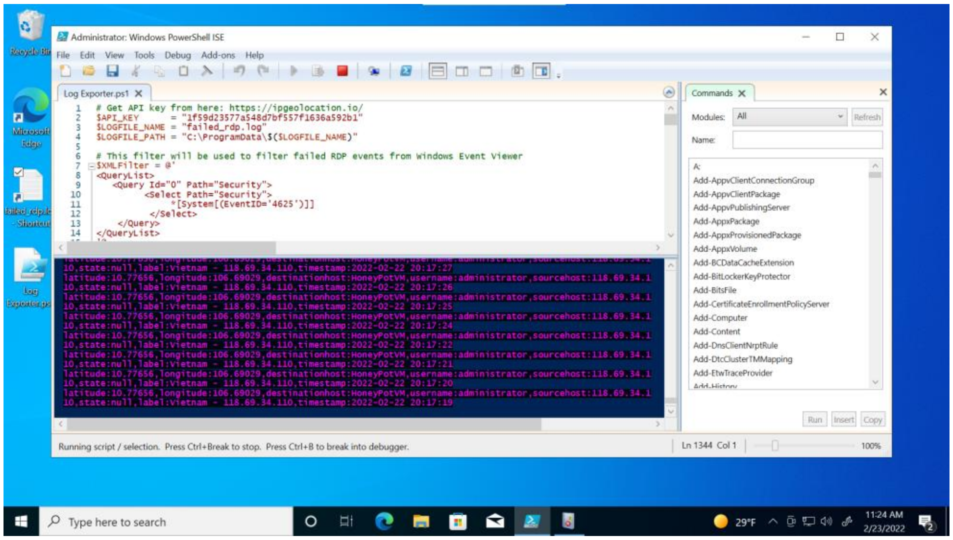
General Details

An account failed to log on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/22/2022 7:58:25 PM
Event ID:	4625	Task Category:	Logon

Since we are only looking for failed RDP attempts, we can use a **PowerShell script** to automatically send all failed RDP attempts and the accompanying information into a log file. This script can be downloaded at https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1. We can copy and paste this code and start a new PowerShell command with it (run as administrator). Make sure to keep this command running to continue processing incoming RDP attempts. Only start this command when the rest of the process has been completed or else problems will start to occur if RDP attempts are coming in fast.



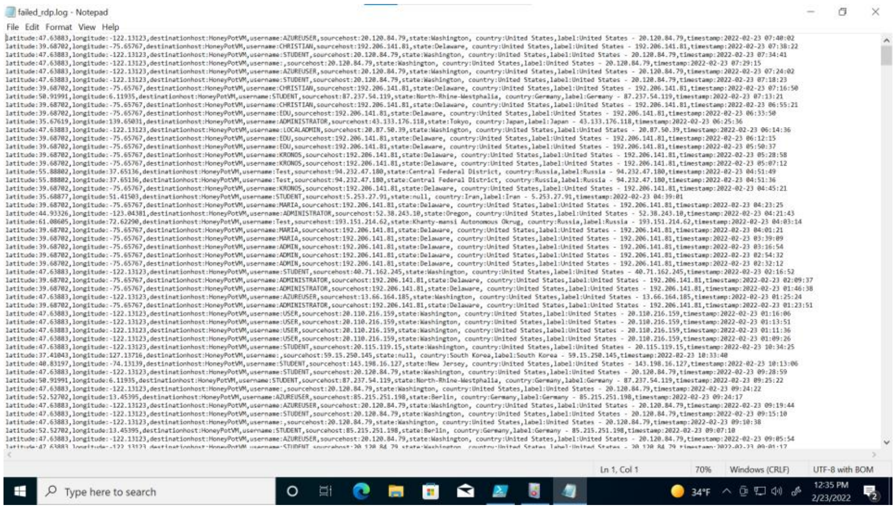
```
# Get API key from here: https://ipgeolocation.io/
$API_KEY      = "1f59d23577a548d7bf557f1636a592b1"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"

# This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
   <Query Id="0" Path="Security">
         <Select Path="Security">
              *[System[(EventID='4625')]]
          </Select>
    </Query>
</QueryList>
```

```
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:27
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:26
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:25
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:24
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:22
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:21
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:20
latitude:10.77656,longitude:106.69029,destinationhost:HoneyPotVM,username:administrator,sourcehost:118.69.34.1
10,state:null,label:Vietnam - 118.69.34.110,timestamp:2022-02-22 20:17:19
```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

An important step to take before running the PowerShell command is to **get an API key for ipgeolocation.io**. Paste this API key into the API_KEY variable on the top of the script. This API is what will provide us with geographical information about the attacker based on their IP address. The PowerShell script will send the IP address of the attacker to the API which will then send the geographical data back to the script and outputted into the log file.

WARNING: The free API key only allows for a maximum of 1000 requests per day. Once that limit is reached, it will send back the same location for the rest of your data, even though it might not be coming from that location.



```
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 07:40:02
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:CHRISTIAN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 07:38:22
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 07:34:41
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 07:29:15
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 07:24:02
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 07:18:23
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:CHRISTIAN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 07:16:50
latitude:50.91991,longitude:6.11935,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:87.237.54.119,state:North-Rhine-Westphalia, country:Germany,label:Germany - 87.237.54.119,timestamp:2022-02-23 07:13:21
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:CHRISTIAN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 06:55:21
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:EDU,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 06:33:50
latitude:35.67619,longitude:139.65031,destinationhost:HoneyPotVM,username:ADMINISTRATOR,sourcehost:43.133.176.118,state:Tokyo, country:Japan,label:Japan - 43.133.176.118,timestamp:2022-02-23 06:25:36
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:LOCALADMIN,sourcehost:20.87.50.39,state:Washington, country:United States,label:United States - 20.87.50.39,timestamp:2022-02-23 06:14:36
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:EDU,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 06:12:15
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:EDU,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 05:50:37
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:KRONOS,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 05:28:58
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:KRONOS,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 05:07:12
latitude:55.88802,longitude:37.65136,destinationhost:HoneyPotVM,username:Test,sourcehost:94.232.47.180,state:Central Federal District, country:Russia,label:Russia - 94.232.47.180,timestamp:2022-02-23 04:51:49
latitude:55.88802,longitude:37.65136,destinationhost:HoneyPotVM,username:Test,sourcehost:94.232.47.180,state:Central Federal District, country:Russia,label:Russia - 94.232.47.180,timestamp:2022-02-23 04:51:36
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:KRONOS,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 04:45:21
latitude:35.68877,longitude:51.41503,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:5.253.27.91,state:null, country:Iran,label:Iran - 5.253.27.91,timestamp:2022-02-23 04:39:01
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:MARIA,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 04:23:25
latitude:44.93326,longitude:-123.04381,destinationhost:HoneyPotVM,username:ADMINISTRATOR,sourcehost:52.38.243.10,state:Oregon, country:United States,label:United States - 52.38.243.10,timestamp:2022-02-23 04:21:43
latitude:61.08605,longitude:72.62290,destinationhost:HoneyPotVM,username:Test,sourcehost:193.151.214.62,state:Khanty-mansi Autonomous Okrug, country:Russia,label:Russia - 193.151.214.62,timestamp:2022-02-23 04:03:14
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:MARIA,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 04:01:21
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:MARIA,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 03:39:09
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMIN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 03:16:54
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMIN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 02:54:32
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMIN,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 02:32:12
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:40.71.162.245,state:Washington, country:United States,label:United States - 40.71.162.245,timestamp:2022-02-23 02:16:52
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMINISTRATOR,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 02:09:37
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMINISTRATOR,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 01:46:38
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:13.66.164.185,state:Washington, country:United States,label:United States - 13.66.164.185,timestamp:2022-02-23 01:25:24
latitude:39.68702,longitude:-75.65767,destinationhost:HoneyPotVM,username:ADMINISTRATOR,sourcehost:192.206.141.81,state:Delaware, country:United States,label:United States - 192.206.141.81,timestamp:2022-02-23 01:23:51
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:USER,sourcehost:20.110.216.159,state:Washington, country:United States,label:United States - 20.110.216.159,timestamp:2022-02-23 01:16:06
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:USER,sourcehost:20.110.216.159,state:Washington, country:United States,label:United States - 20.110.216.159,timestamp:2022-02-23 01:13:51
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:USER,sourcehost:20.110.216.159,state:Washington, country:United States,label:United States - 20.110.216.159,timestamp:2022-02-23 01:11:36
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:USER,sourcehost:20.110.216.159,state:Washington, country:United States,label:United States - 20.110.216.159,timestamp:2022-02-23 01:09:26
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.115.119.15,state:Washington, country:United States,label:United States - 20.115.119.15,timestamp:2022-02-23 10:34:25
latitude:37.41043,longitude:127.13716,destinationhost:HoneyPotVM,username:,sourcehost:59.15.250.145,state:null, country:South Korea,label:South Korea - 59.15.250.145,timestamp:2022-02-23 10:33:40
latitude:40.83197,longitude:-74.13139,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:143.198.16.127,state:New Jersey, country:United States,label:United States - 143.198.16.127,timestamp:2022-02-23 10:13:06
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:28:59
latitude:50.91991,longitude:6.11935,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:87.237.54.119,state:North-Rhine-Westphalia, country:Germany,label:Germany - 87.237.54.119,timestamp:2022-02-23 09:25:22
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:24:22
latitude:52.52702,longitude:13.45395,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:85.215.251.198,state:Berlin, country:Germany,label:Germany - 85.215.251.198,timestamp:2022-02-23 09:24:17
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:19:44
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:15:10
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:10:38
latitude:52.52702,longitude:13.45395,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:85.215.251.198,state:Berlin, country:Germany,label:Germany - 85.215.251.198,timestamp:2022-02-23 09:07:10
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:AZUREUSER,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:05:54
latitude:47.63883,longitude:-122.13123,destinationhost:HoneyPotVM,username:STUDENT,sourcehost:20.120.84.79,state:Washington, country:United States,label:United States - 20.120.84.79,timestamp:2022-02-23 09:01:17
```

Sending the Logs to Sentinel SIEM

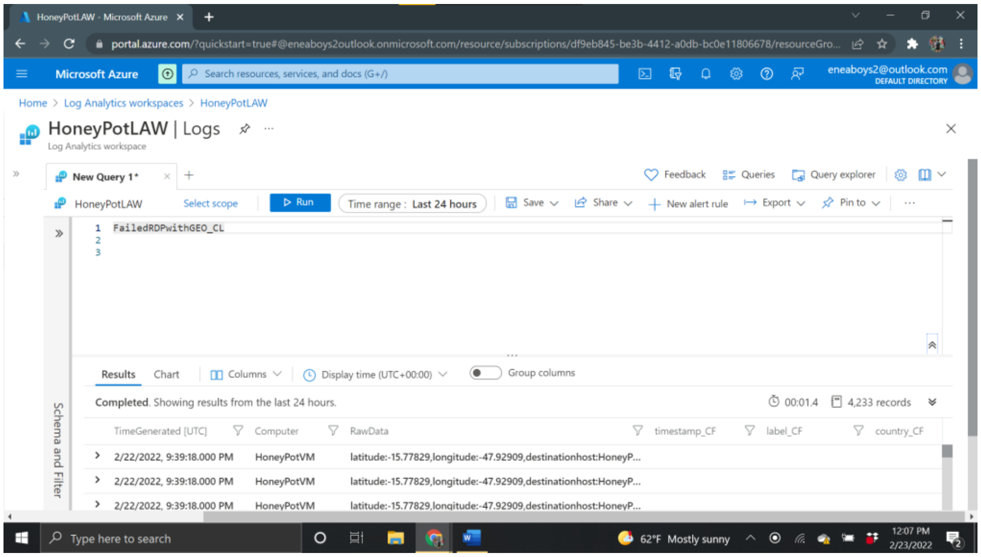
Back on Azure and in the LAW, we will make a **custom log** that will take information from the log file on the VM.

The custom log will request a sample log to base its data off. To do this, we can copy and paste a sample of what we have in the VM's log file into a note file on the host machine. This file can then be loaded into Azure to serve as the sample log.

Next, we must give the custom log the directory path of the log file on the VM so that it can retrieve it.

We can then give the custom log a name, which in this case will be FailedRDPwithGEO_CL.

Then we can head to the logs tab and start a query to retrieve these custom logs from the VM by simply typing in the custom log name into the query box.

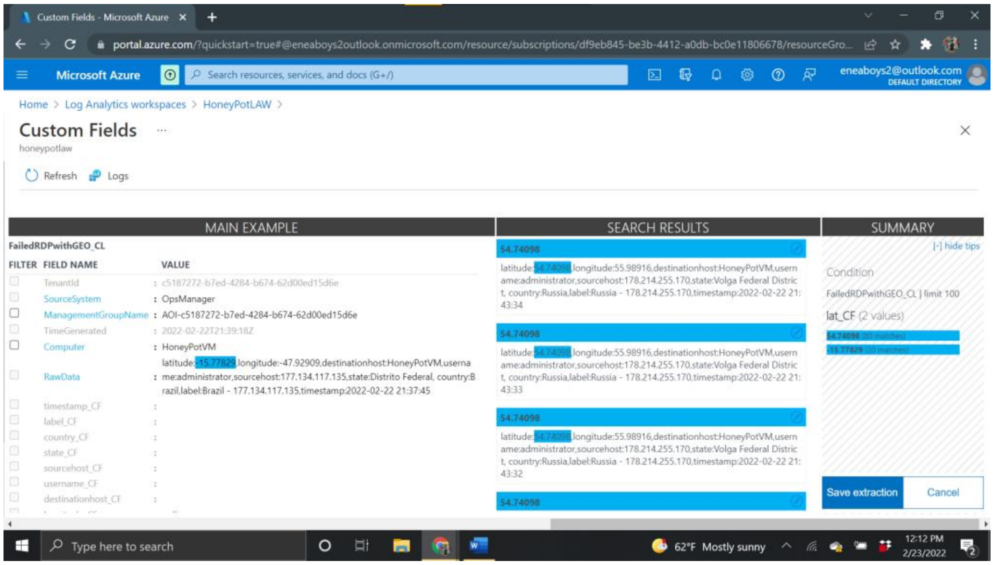


```
FailedRDPwithGEO_CL
```

Completed. Showing results from the last 24 hours. 00:01.4 4,233 records

TimeGenerated [UTC]	Computer	RawData	timestamp_CF	label_CF	country_CF
2/22/2022, 9:39:18.000 PM	HoneyPotVM	latitude:-15.77829,longitude:-47.92909,destinationhost:HoneyP...			
2/22/2022, 9:39:18.000 PM	HoneyPotVM	latitude:-15.77829,longitude:-47.92909,destinationhost:HoneyP...			
2/22/2022, 9:39:18.000 PM	HoneyPotVM	latitude:-15.77829,longitude:-47.92909,destinationhost:HoneyP...			

The next step is to **extract custom fields** from the data entries retrieved into variables for the Sentinel SIEM. To do this, all we have to do is expand one of the entries and click on the 3 dots that appear below. For each field included in the query, we must highlight the information and save it as a custom field. Before saving each field, make sure the automated formatting is correct in the samples to the side.


Custom Fields - Microsoft Azure
portal.azure.com/?quickstart=true#@eneaboys2outlook.onmicrosoft.com/resource/subscriptions/df9eb845-be3b-4412-a0db-bc0e11806678/resourceGro...
Microsoft Azure
Search resources, services, and docs (G+/)
eneaboys2@outlook.com
DEFAULT DIRECTORY
Home > Log Analytics workspaces > HoneyPotLAW >
Refresh
Logs
MAIN EXAMPLE
SEARCH RESULTS
SUMMARY
[-] hide tips
Save extraction
Cancel
Type here to search
62°F Mostly sunny
12:12 PM
2/23/2022

Custom Fields

honeypotlaw

FailedRDPwithGEO_CL

FILTER	FIELD NAME		VALUE
□	TenantId	:	c5187272-b7ed-4284-b674-62d00ed15d6e
□	SourceSystem	:	OpsManager
□	ManagementGroupName	:	AOI-c5187272-b7ed-4284-b674-62d00ed15d6e
□	TimeGenerated	:	2022-02-22T21:39:18Z
□	Computer	:	HoneyPotVM
□	RawData	:	latitude:-15.77829,longitude:-47.92909,destinationhost:HoneyPotVM,username:administrator,sourcehost:177.134.117.135,state:Distrito Federal, country:Brazil,label:Brazil - 177.134.117.135,timestamp:2022-02-22 21:37:45
□	timestamp_CF	:	
□	label_CF	:	
□	country_CF	:	
□	state_CF	:	
□	sourcehost_CF	:	
□	username_CF	:	
□	destinationhost_CF	:	

54.74098

latitude:54.74098,longitude:55.98916,destinationhost:HoneyPotVM,username:administrator,sourcehost:178.214.255.170,state:Volga Federal District, country:Russia,label:Russia - 178.214.255.170,timestamp:2022-02-22 21:43:34

54.74098

latitude:54.74098,longitude:55.98916,destinationhost:HoneyPotVM,username:administrator,sourcehost:178.214.255.170,state:Volga Federal District, country:Russia,label:Russia - 178.214.255.170,timestamp:2022-02-22 21:43:33

54.74098

latitude:54.74098,longitude:55.98916,destinationhost:HoneyPotVM,username:administrator,sourcehost:178.214.255.170,state:Volga Federal District, country:Russia,label:Russia - 178.214.255.170,timestamp:2022-02-22 21:43:32

54.74098

Condition

FailedRDPwithGEO_CL | limit 100

lat_CF (2 values)

54.74098 (80 matches)

-15.77829 (20 matches)

Once all custom fields have been properly extracted, they can then be used to **create a map of where all RDP attempts are coming from**. Back in the Sentinel tab, create a new workbook and add a new query widget to the workbook. In the query box, enter the following command:

```
FailedRDPwithGEO_CL | summarize event_count=count() by sourcehost_CF, latitude_CF, longitude_CF, country_CF, label_CF, destinationhost_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""
| where country_CF != ""
```

This will ingest all incoming custom logs and the derived custom fields from the LAW.

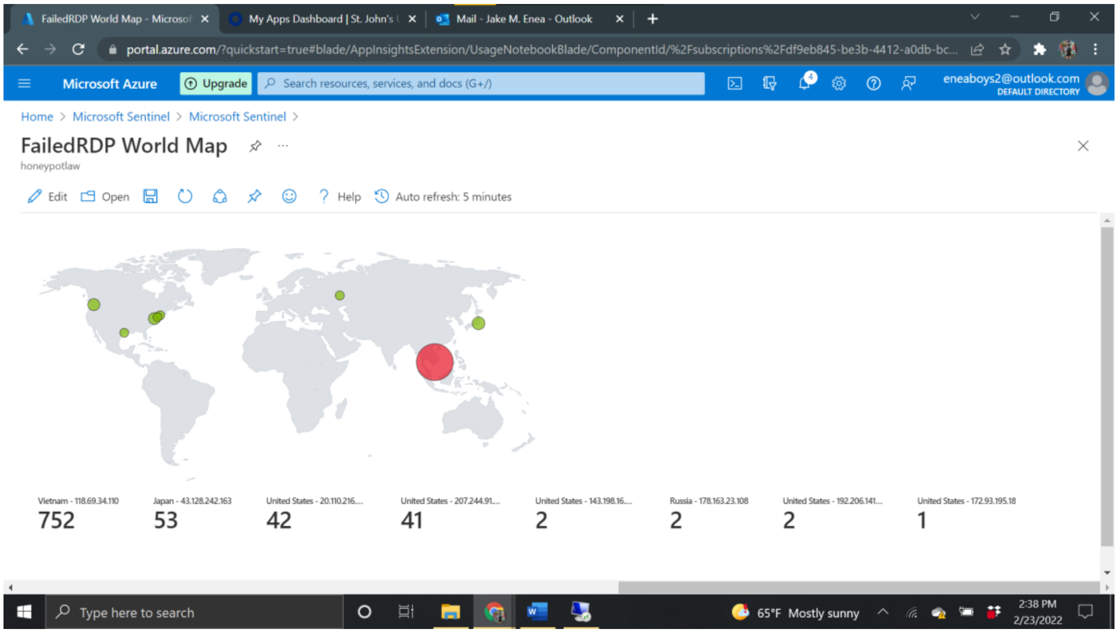
Change the visualization to map and click map settings to edit the map.

Map configuration:

- Location info using: Country or region
- Country/region field: country_CF
- Size by: event_count
- Color by: event_count
- Metric value: event_count

Displaying the Map

Run the query and watch the map populate. As time goes on, more and more people from around the world will discover and try to access your VM, further populating the map. Below is an example map from running the project for about 30 minutes.

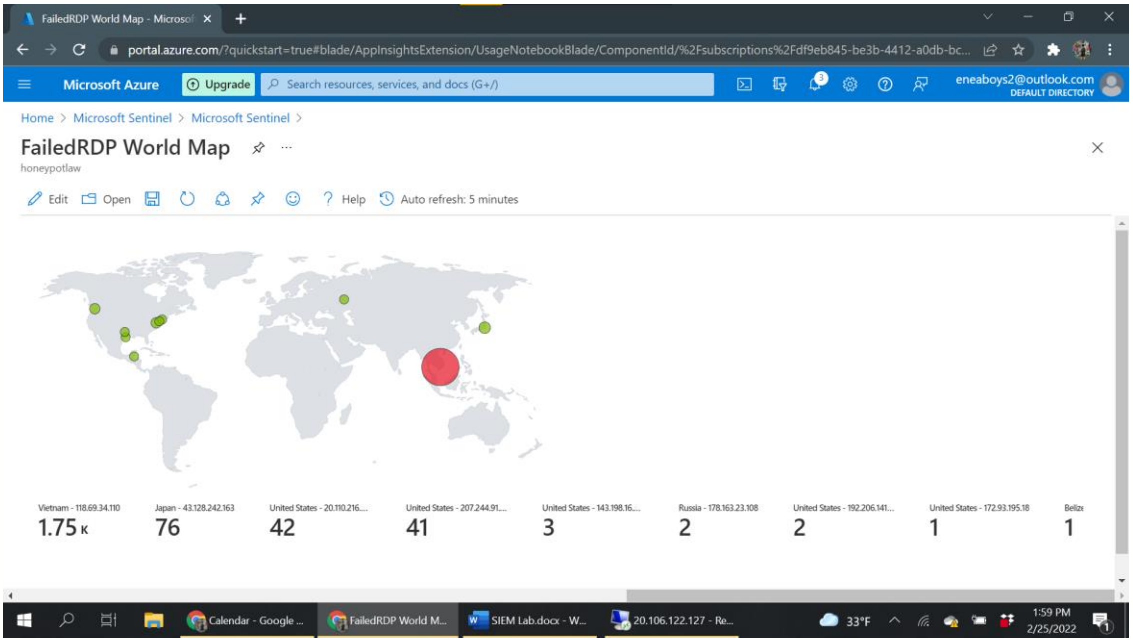

FailedRDP World Map - Microsof
My Apps Dashboard | St. John's
Mail - Jake M. Enea - Outlook
portal.azure.com/?quickstart=true#blade/AppInsightsExtension/UsageNotebookBlade/ComponentId/%2Fsubscriptions%2Fdf9eb845-be3b-4412-a0db-bc...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
eneaboys2@outlook.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Microsoft Sentinel >
Edit
Open
Help
Auto refresh: 5 minutes
Type here to search
65°F Mostly sunny
2:38 PM
2/23/2022

FailedRDP World Map

honeypotlaw

Vietnam - 118.69.34.110	Japan - 43.128.242.163	United States - 20.110.216....	United States - 207.244.91....	United States - 143.198.16....	Russia - 178.163.23.108	United States - 192.206.141....	United States - 172.93.195.18
752	53	42	41	2	2	2	1

As you can see, Vietnam was evidently trying to brute force its way into my VM as shown by 752 failed RDP attempts from the same IP address. Additionally, Japan gave it a few tries, as well as a few different IPs throughout the US. Let's see what the map looks like after a second day of running the command.


FailedRDP World Map - Microsof
portal.azure.com/?quickstart=true#blade/AppInsightsExtension/UsageNotebookBlade/ComponentId/%2Fsubscriptions%2Fdf9eb845-be3b-4412-a0db-bc...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
eneaboys2@outlook.com
DEFAULT DIRECTORY
Home > Microsoft Sentinel > Microsoft Sentinel >
Edit
Open
Help
Auto refresh: 5 minutes
Calendar - Google ...
FailedRDP World M...
SIEM Lab.docx - W...
20.106.122.127 - Re...
33°F
1:59 PM
2/25/2022

FailedRDP World Map

honeypotlaw

Vietnam - 118.69.34.110	Japan - 43.128.242.163	United States - 20.110.216....	United States - 207.244.91....	United States - 143.198.16....	Russia - 178.163.23.108	United States - 192.206.141....	United States - 172.93.195.18	Belize
1.75 K	76	42	41	3	2	2	1	1

After the second day, Vietnam was still trying hard to break into the machine with more than 1,750 attempts. Japan also gave it a few more tries but gave up much quicker than Vietnam.

Takeaways

This personal lab gives great introductory experience to working with a SIEM, along with setting one up and witnessing one of the many ways in which it can be implemented. I found it really interesting seeing how quickly bots tried to brute force their way into my VM just because they saw that the firewall was down and the machine was left vulnerable. One thing to take away from this lab is to never use ‘administrator’ as your username. This was by far the most common username in the RDP attempts. If my VM was set up with the username ‘administrator’ and a weak password, the machine could certainly get hacked into fairly easily. Overall, I enjoyed seeing all the attempts take place and looking into where they were coming from and what credentials and strategies they were using to get into my machine.