Sentinel Azure write up

We created a Microsoft azure account and created a new virtual machine. We created a new resource group called HoneyPotLab\_group and named it HoneyPotLab. The region is set to US East, because there seems to be an error with US West. The image we have chosen is Windows 10 pro (it’s free).

Admin: SpingyAdmin

Password: Sp1ng%@dminn

After we check the checkbox at the bottom, we go next until we hit networks. There, we look for NIC network security group, which seems to be similar to a firewall. In this section, we will use advanced and create a new one. In the next page, we will need to delete the default rules, so that we can let in everything. Next, we can add our own inbound rules and we set the Destination port ranges to \*, so that traffic can come in. We also change the priority to 100 and change the name to DANGER\_IN. Now we have all traffic coming into the virtual machine. We want the VM to be discoverable and to be attacked, hence the name honeypot.

Now we need to make a log analytic workspace. So we can type it in the search at the top while the VM is being created. Here, we can find where the attackers are coming from. We hit create, pick our honeypot resource group and name it law-honeypot1.

Next, we head into security center to enable the ability to gather logs from the VM and then into the log analytics workspace. This has been changed to Microsoft Defender for Cloud. Next we head into Environment settings, click on Azure subscription 1, and then click on law-honeypot1. We’re supposed to turn on Azure Defender and Servers on, but I think as long as we turn on Cloud Security Posture Management and Servers, it’ll be okay. Leave SQL servers on machines off. Remember to click save and head into data collection when it finishes saving. Here, we click All Events and then Save.

We can now head into Log analytics and connect it to the VM. After we search for log analytic workspace, we can click on law-honeypot1 and find virtual machine on the left side scroll. Now we can click our VM and then connect to it. As we’re connecting to the VM, we can open a new tab to set up Sentinel. This is our SIEM, Security Information and Event Management, so we can visualize our attack data. We click out honeypot and then add it. While that’s going, we can head into our VM. To do this, we go into virtual machine, click on our honeypot, and then copy the public IP. Now we head into remote desktop on our own machine. We paste in the IP, click on more options, enter the admin and password, accept the certificate and finally head in. I would also recommend making the resolution smaller. When we’re in, say no to all of the privacy settings. Now we can set up Edge and head into event viewer. Inside, we can head to Windows Logs and then security. We will be focusing on Event ID 4625, which is a login failure. If we double click the error, we can find the IP of who tried to connect to the VM and then take that IP to ipgeolocation.io to find their longitude and latitude or country. We can then use Sentinel to take that info and put it on a map.

Now we need to turn off the firewall in order to get some traffic. We tried to ping it from the host machine, but it was timed out. We can type wf.msc into the windows search of our VM, click on the firewall settings and turn off Domain profile, Private profile, and public profile. Hit apply and then try to ping from the host machine again.

Ping <VM> -t

Now that echo requests are allowed, our pings go through.

Next we can download the powershell script from the description, and save it to the desktop. Now we need a ipgeolocation api key. After we get that, we can paste the key into the PS script and run it. We can see that we already have someone from Singapore fail to login to our VM.

Now we can create a custom log inside of our log analytic, so that we can bring the geo data into our workspace. So, we go into our LAW > custom logs > add custom log. Now we go into our VM, into our C drive > ProgramData > failed\_rdp file (hidden btw) > copy everything > go host machine > paste into text document. This trains log analytics what to look for. We add the sample to azure > next > Collections Paths. Here we type in the path to the failed rdp file within our VM.

C:\ProgramData\failed\_rdp.log

Next, we name it FAILED\_RDP\_WITH\_GEO, and create it.

We can check out current logs by going into Logs on the left side, and typing in

SecurityEvent | where EventID == 4625

This brings up our failed logins from the VM.

If we type in FAILED\_RDP\_WITH\_GEO\_CL, we can see nothing lol. It takes some time for the logs from the VM to go to the ipgeolocation API to the failed\_rdp.log file and back to us. After that’s loaded up, we need to extract the raw data from it to have their own fields, like it’s own latitude and longitude field. To do this, we can right click on any of them and click Extract fields from ‘FAILED…’.

When we are in the extract window, we just have to highlight the value and give it a title. So, to get our latitude from latitude:11.11111, we highlight the numbers and create a field for it. This step is tedious.

Title for latitude is Latitude\_CF and the field type is numeric. There is then a pop up on the right side of the screen with our values highlighted. If any of them are wrong, we can edit with the pen looking button on the right side of each one. After we finish for each. To edit our fields, we have to go into custom logs > custom fields. To see our fields within logs, we have to click on Columns on the right side and click each of our custom fields to show them. Now when we get new logs, they will be inserted into these custom fields. Before we head into Sentinel to set the workbook, make sure the fields we created have data in them. In my testing, mine is having trouble finding where the source host it. I have deleted and added it about five times now. I’m not sure what I’m doing wrong.

Now we can head back into Sentinel and create a new Workbook. First, we need to get rid of the existing widgets, so we can go to the right and hit the three dots and then remove. After that we can create a new query. We can enter the following into the text box:

FAILED\_RDP\_WITH\_GEO\_CL | summarize event\_count=count() by Label\_CF, Latitude\_CF, Longitude\_CF, Country\_CF, Destination\_Host\_CF

| where Destination\_Host\_CF != "samplehost"

| where Label\_CF !=""

After that we get a pop up to change some settings on a world map and we can see where the attacks are coming from. In my case I had a ton of attacks come from India. After tinkering with some settings we can save it as Failed RDP World Map.

After 24 hours, here’s what our map looks like.