The Honeypot: A Cybersecurity Exercise in Brute-Force Attacks and Defense

Sam Noureddini[1], Neel Patel[2], Alan Kelly[3] and Diego Hernandez[4]

[1]University of San Diego/Fullstack Academy

[2]Virginia Tech/Fullstack Academy

[3]University of Oklahoma/Fullstack Academy

[4]University of Illinois at Chicago/Fullstack Academy

Cybersecurity remains a paramount consideration for many aspects of society. As the majority of operations for various entities progresses to cloud-based platforms, ensuring the confidentiality, integrity and availability of stored information is of utmost priority. Malicious actors have the aim of compromising data via the unauthorized access of target machines, thus, making defense against such attacks of particular import. Brute-force attacks via offline or automated means remain a threat to any cloud-base platform. Attackers utilize a vast number of username/password combinations in rapid succession to gain access. A primary defense against this type of breach lies in detection, with, namely, the use of SIEMs to review logs of failed and successful login attempts. In this study, a virtual machine (honeypot) was established on the cloud-based platform Microsoft Azure, configured with the SIEM application Microsoft Sentinel, with the linked-goals of demonstrating an automated brute-force attack, and observing and analyzing logs associated with them. After a controlled internal study, the virtual machine was opened to the public resulting in numerous attacks observed from locations around the world. Geolocation logic was introduced in the SIEM to pinpoint locations more accurately, providing better clues to potential brute-force access. The vast importance of SIEMs was established, proficiency with Sentinel developed, and stretch goals for further experimentation established. Herein, a detailed report of the setup and results of this experimental model is provided.

Key words: Cybersecurity, cloud-computing, SIEM, Microsoft Azure, Azure Sentinel, brute-force, dictionary attacks

INTRODUCTION

Cybersecurity has been defined as the art of protecting networks, devices, and data from unauthorized access or criminal use, as well as the practice of ensuring confidentiality, integrity, and availability (CIA) of information (CISA.gov 2023). As the reliance on cloud-based storage and applications for various aspects of society becomes more ubiquitous, especially in the post-COVID world, protection from malicious activities aimed to compromise data associated with such platforms is paramount. From global corporations to small businesses, healthcare, energy infrastructure, and finance, the world is more reliant on protection from malicious cyber actors than ever, with the integrity of associated information systems being only as viable as the weakest point in the cybersecurity chain (Bošnjak 2018). Credentialed-access to such systems via various login clients represents a critical aspect of cybersecurity, with this also serving as a point of departure for data-hackers seeking to establish connections to target machines. In terms of providing such login-credentialed security, a number of strategies have been employed to secure access to such systems, namely, knowledge based, physical, and inherent controls. Inversely, the theft of primary passwords by adversarial groups remains a threat to the CIA of data housed on such platforms.

One method of obtaining such login information is through the use of so-called brute-force password attacks (Bošnjak 2018). This malicious practice employs either; an offline approach where manual entry of usernames and passwords are attempted on the login client of a target machine, or an automated process in which numerous common login pairs are attempted in rapid succession. For the latter, text files created from both historical and novel lists of common usernames and passwords are utilized by various well-known software. Hydra and Metasploit for example, are two Linux-based programs that have successfully achieved such results in gaining access to target servers containing privileged information (Grover 2020). Certainly, practices such as these mandate the development of cybersecurity strategies that identify and address such attacks to mitigate or prevent access and data exfiltration.

In this exercise, the goal of observing such an attack by non-authorized actors, and employing the efforts and tools used by information-security personnel to identify such actions, were demonstrated in the Microsoft Azure cloud-based platform. A test environment was created on Azure with the goal of data collection and logging of attempts at brute-force login. To this end, the inherent software for security event and incident management (SIEM), namely, Azure Sentinel was used to generate log data for the login attempts. As defined in the information security landscape, the “red-team” was identified as the malicious actors, and “blue-team” as the security personnel charged with identification and prevention. Red-team attempts at login were made in the test environment by team members, and then opened to the general public for attempted breach. Logs associated with such attempts were analyzed and parsed for time, ip address, and ultimately geolocation, the latter being achieved via a script developed for such results. Herein, the details of the exercise are described, the results obtained, the conclusions made regarding defensive viability of the SIEM used, and future experimentation that can be developed to demonstrate more detailed information. Ultimately, this model provides an excellent resource in developing expertise in such red-team and blue-team strategies for brute-force attacks.

MATERIALS AND METHODS

The setup for this project involved setting up a Microsoft Azure Sentinel, and connecting it to a live deployed virtual machine acting as a honey pot. This project was created on a platform of Microsoft Azure Cloud services. The custom Powershell script was used from a github resource to take a view of the attacker’s Geolocation information and plot it on the Azure Sentinel map (Madakor 2022). The steps to complete this project are described in the following paragraph.

The first step of this project began with deploying a Windows 10 Virtual Machine (VM) on the Microsoft Azure Cloud services after obtaining an Azure Cloud services subscription. During the process of deploying the virtual machine, the firewall rule was set to ALL IN for inbound rule to make it discoverable in the public. The next step involved configuring a Log Analytics Workspace in Azure and enabling the ability to gather Windows 10 VM logs from Security Center on Azure. The VM was successfully connected to the Log Analytics Workspace on Azure. Next step involves setting up the Azure Sentinel SIEM and connecting it to the Log Analytics Workspace. Now, the deployed VM is ready to be used. To collect a few failed logins in log data in Event Viewer through RDP, there were few failed attempts made intentionally. The Windows Firewall is turned OFF on the VM and verified by pinging from other machines. Then the custom Powershell script was obtained from a github resource to extract metadata from Windows Event Viewer (Madakor 2022). Its API key was replaced with a new key obtained from https://ipgeolocation.io/ in order to derive geolocation data of attackers (https://ipgeolocation.io 2021). The Powershell script is run to get geolocation data from an attacker trying to RDP login to the deployed Windows 10 machine. The custom logs were created in the Log Analytics Workspace to bring in our custom log containing geographical information that includes latitude, longitude, state/province, and country. The custom fields were created and the raw custom log data were ingested to extract into custom fields with the intent of mapping geolocation data in Azure Sentinel SIEM. The extract data was passed through testing to make the geolocating data more accurate for mapping purposes. The final stage involved configuring Azure Sentinel SIEM workbook to display RDP brute-force on the world map based on the physical location and magnitude of the attacks. The last few steps involved testing the functionality of the project through RDP brute-force by the team members to ensure that the logs are parsed out well and visualized on the world map. Some of the automation tools such as Hydra were used in the RDP brute-force to enhance the count of the cyber attacks and train the data again if needed in case of problems related to parsing of logs.

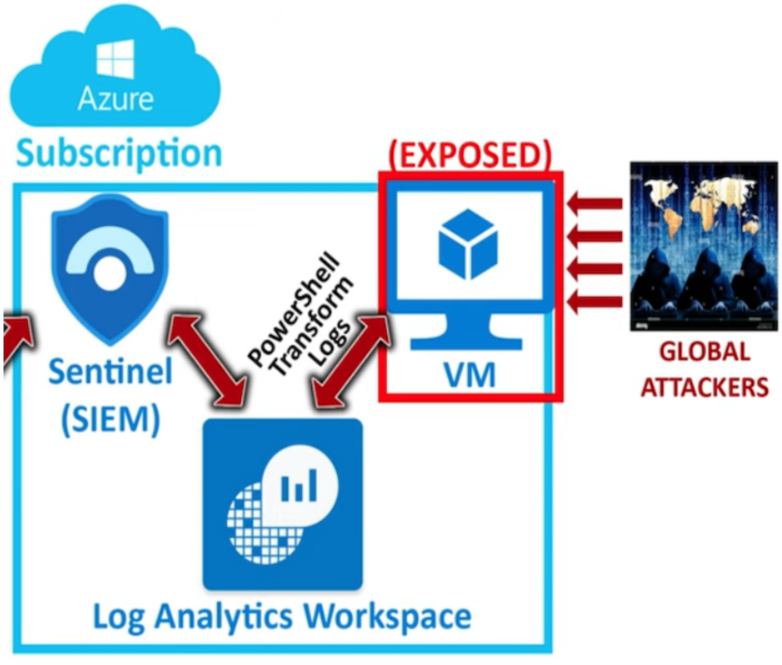
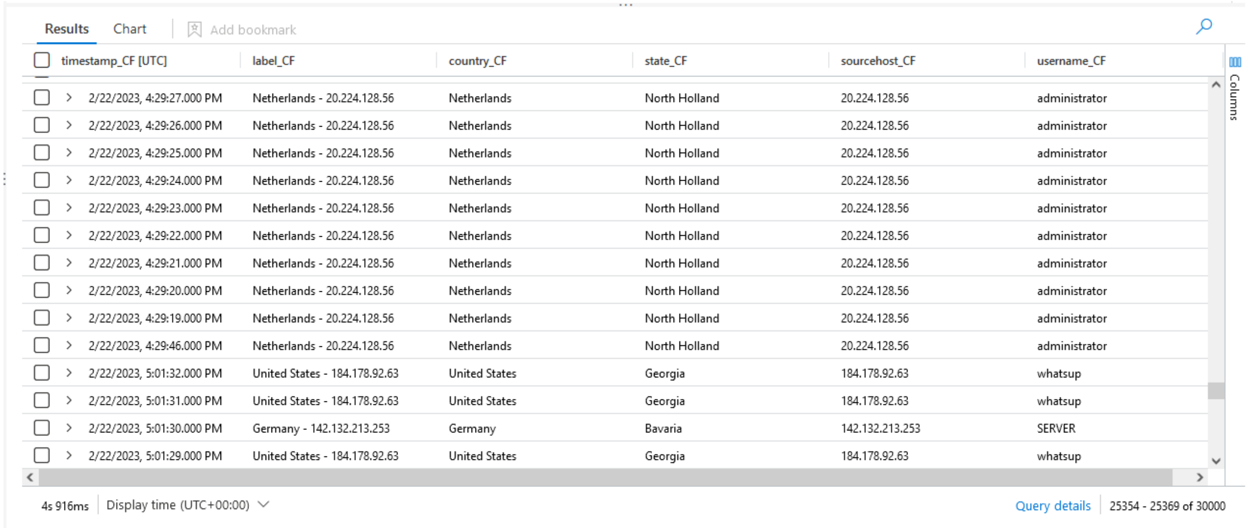


Figure 1.- Overview of the architecture behind the creation of project (Madakor 2021)

RESULTS

The results from the honeypot demonstrate how actors from over the internet are searching for open machines in order to exploit. In this project, the only open port for exploit was Remote Desktop Connection. Within an hour of setup of the virtual machine attackers, outside from our group began attacking our machine. As shown in **Figure 2**, an attacker, originating from the Netherlands and with an IPv4 of 20.224.128.56, attempted to gain access to our machine by using the username "administrator" by performing a brute-force dictionary attack for the password, with no success.

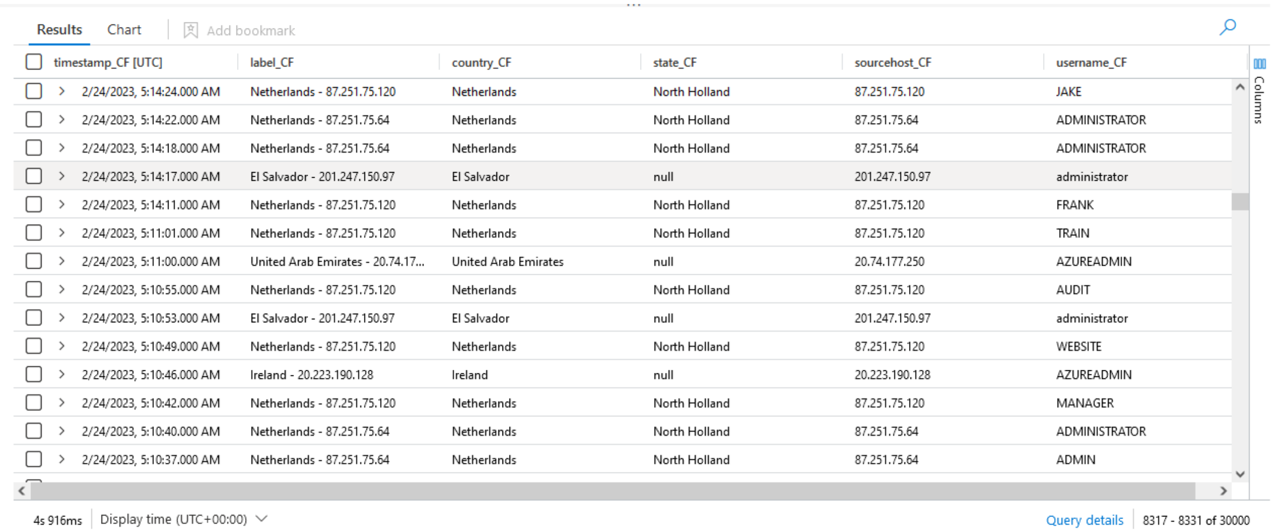


timestamp_CF [UTC]	label_CF	country_CF	state_CF	sourcehost_CF	username_CF
2/22/2023, 4:29:27.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:26.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:25.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:24.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:23.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:22.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:21.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:20.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:19.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 4:29:46.000 PM	Netherlands - 20.224.128.56	Netherlands	North Holland	20.224.128.56	administrator
2/22/2023, 5:01:32.000 PM	United States - 184.178.92.63	United States	Georgia	184.178.92.63	whatsup
2/22/2023, 5:01:31.000 PM	United States - 184.178.92.63	United States	Georgia	184.178.92.63	whatsup
2/22/2023, 5:01:30.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SERVER
2/22/2023, 5:01:29.000 PM	United States - 184.178.92.63	United States	Georgia	184.178.92.63	whatsup

25354 - 25369 of 30000

Figure 2. Sentinel log 1 - Logs generated on the first day of experiment showing attacks from the US, Germany, and Netherlands, including their state

The attacker begins this attack at 4:29:31:00 pm lasting until 4:42:17:00pm with hundreds of attempted passwords. The rapid timing of this attack suggests an automated process at brute-force access. As shown in **Figure 3**, there were many brute-force attacks originating from many places in the world, using two types of brute-force methods. As shown, manual attempts at login were seen from IP addresses originating from El Salvador and Ireland, while an automated attack was conducted from The Netherlands. The latter is observable by the rapid timing of the logins suggesting that a program was conducting the attempts.

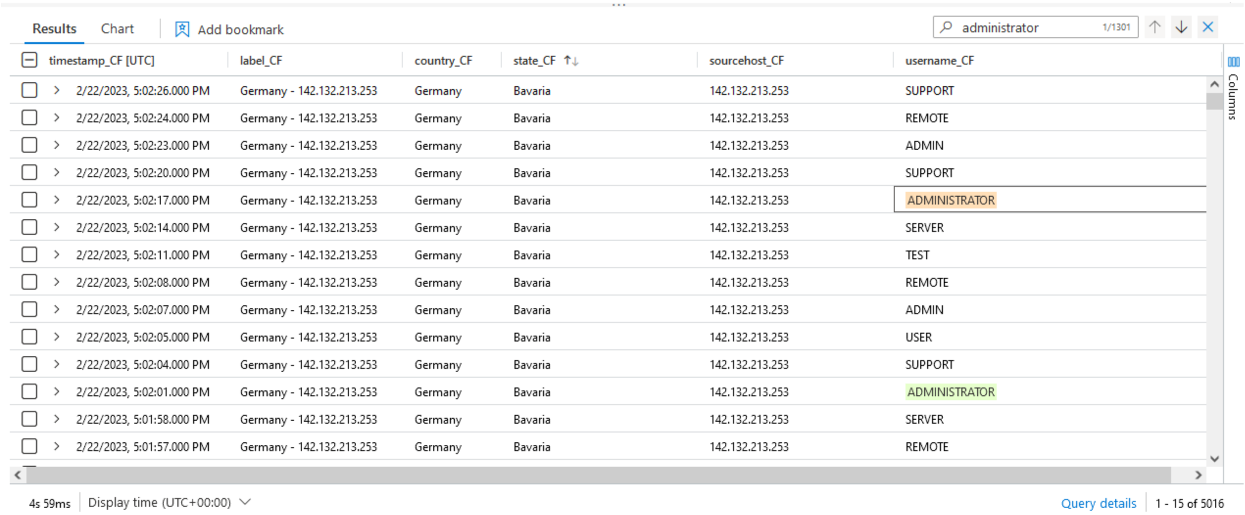


timestamp_CF [UTC]	label_CF	country_CF	state_CF	sourcehost_CF	username_CF
2/24/2023, 5:14:24.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	JAKE
2/24/2023, 5:14:22.000 AM	Netherlands - 87.251.75.64	Netherlands	North Holland	87.251.75.64	ADMINISTRATOR
2/24/2023, 5:14:18.000 AM	Netherlands - 87.251.75.64	Netherlands	North Holland	87.251.75.64	ADMINISTRATOR
2/24/2023, 5:14:17.000 AM	El Salvador - 201.247.150.97	El Salvador	null	201.247.150.97	administrator
2/24/2023, 5:14:11.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	FRANK
2/24/2023, 5:11:01.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	TRAIN
2/24/2023, 5:11:00.000 AM	United Arab Emirates - 20.74.17...	United Arab Emirates	null	20.74.177.250	AZUREADMIN
2/24/2023, 5:10:55.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	AUDIT
2/24/2023, 5:10:53.000 AM	El Salvador - 201.247.150.97	El Salvador	null	201.247.150.97	administrator
2/24/2023, 5:10:49.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	WEBSITE
2/24/2023, 5:10:46.000 AM	Ireland - 20.223.190.128	Ireland	null	20.223.190.128	AZUREADMIN
2/24/2023, 5:10:42.000 AM	Netherlands - 87.251.75.120	Netherlands	North Holland	87.251.75.120	MANAGER
2/24/2023, 5:10:40.000 AM	Netherlands - 87.251.75.64	Netherlands	North Holland	87.251.75.64	ADMINISTRATOR
2/24/2023, 5:10:37.000 AM	Netherlands - 87.251.75.64	Netherlands	North Holland	87.251.75.64	ADMIN

8317 - 8331 of 30000

Figure 3. Sentinel log 2 - Logs generated on day 3 showing additional attacks were observed from Ireland, El Salvador, United Arab Emirates, and Netherlands, including their state.

Other attackers, as those shown in **Figure 4**, tried to not only brute-force the password but also performed an automated dictionary attack for the username. IPv4 142.132.213.253, originating from Germany, attempted a set of usernames that were cycled through. Meaning, after the password failed, it will change the username and the next attempt and so on until the last username in the list is reached. After this the next attempt will be a new password with the username cycling back to the beginning, restarting the process again. As shown in **Figure 4**, many attackers tried to brute-force only the password while using a common username, like administrator. The username, administrator, was used 1301 times from different attackers, showing they will most likely attempt common usernames when they have little knowledge of their target machine. No matter the method, they were unable to gain access due to a strong password established for the virtual machine.



timestamp_CF [UTC]	label_CF	country_CF	state_CF ↑↓	sourcehost_CF	username_CF
2/22/2023, 5:02:26.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SUPPORT
2/22/2023, 5:02:24.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	REMOTE
2/22/2023, 5:02:23.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	ADMIN
2/22/2023, 5:02:20.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SUPPORT
2/22/2023, 5:02:17.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	ADMINISTRATOR
2/22/2023, 5:02:14.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SERVER
2/22/2023, 5:02:11.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	TEST
2/22/2023, 5:02:08.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	REMOTE
2/22/2023, 5:02:07.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	ADMIN
2/22/2023, 5:02:05.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	USER
2/22/2023, 5:02:04.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SUPPORT
2/22/2023, 5:02:01.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	ADMINISTRATOR
2/22/2023, 5:01:58.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	SERVER
2/22/2023, 5:01:57.000 PM	Germany - 142.132.213.253	Germany	Bavaria	142.132.213.253	REMOTE

4s 59ms | Display time (UTC+00:00) | Query details | 1 - 15 of 5016

Figure 4. Sentinel log 3 - Logs generated on day 2 filtered for username "administrator"

From the logs, we extracted their ip location, longitude and latitude, and used Sentinel to create a world map to display where the attacks are originating from and the number of attempts for each country. **Figure 5** demonstrates attacks on the first day the virtual machine was up. Several attacks from multiple countries across the world attempted to gain access, from Mexico to Hong Kong to the Netherlands, etc.

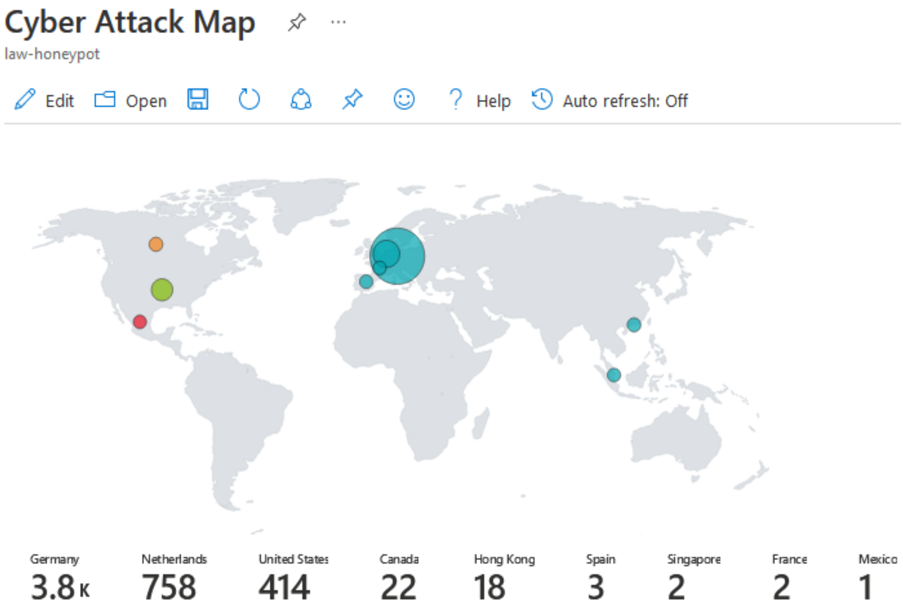
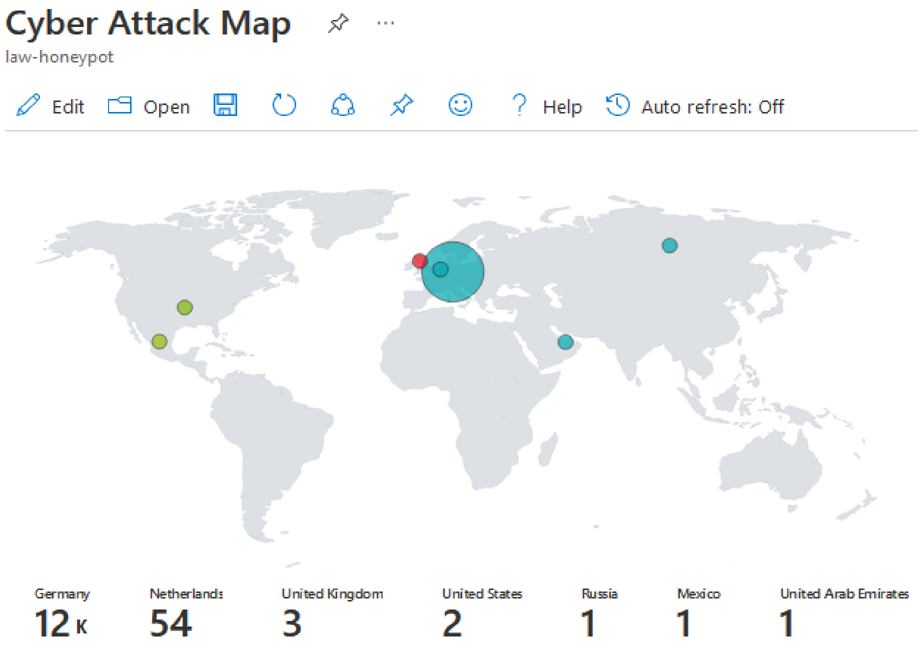


Figure 5. Sentinel Map 1 - Mapped attacks from day 1 showing failed attempts from across the world, primarily Germany

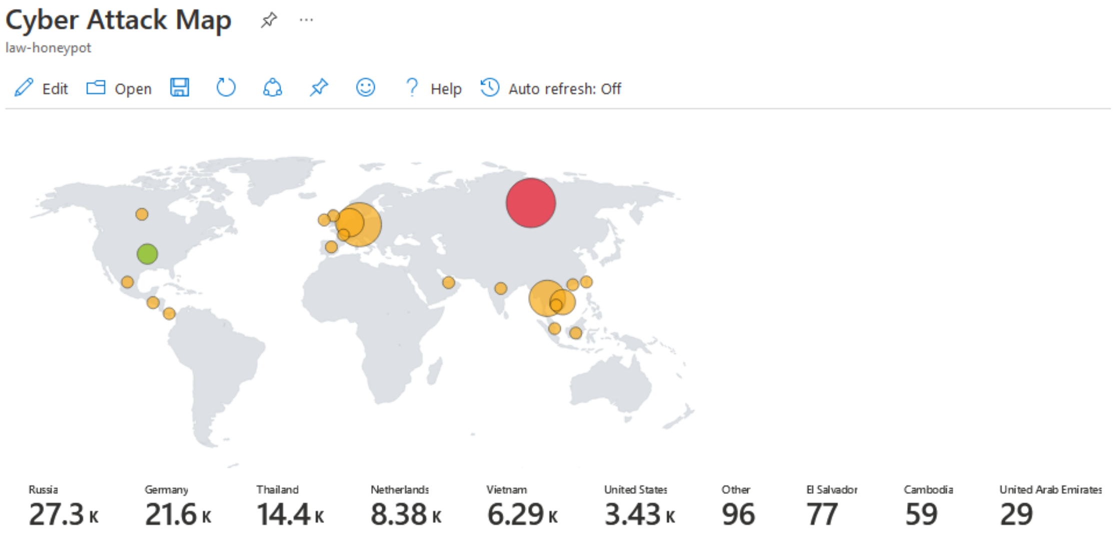
From the second day of having the virtual machine up, the number of attempts increased significantly, especially in Germany. As shown in **Figure 6**, more attackers, either from the same region or a new region, attempt to gain unauthorized access. If an actor, from a new region, attacked, then that country was plotted and displayed in the map.



Germany	Netherlands	United Kingdom	United States	Russia	Mexico	United Arab Emirates
12 K	54	3	2	1	1	1

<u>Figure 6.</u> Sentinel Map 2 - Mapped attacks from day 2 showing additional new regions and failed attempts

After the final day of having our virtual machine up, as expected based on the first two days, there was a significant increase in attempts. There were not only new attackers but, as shown in **Figure 7**, new countries and regions where these attacks originated from. The longer you leave your machine up, the increasingly likely it is to be attacked. And as seen, it does not matter what part of the world you are in, attackers are always on the hunt.



Russia	Germany	Thailand	Netherlands	Vietnam	United States	Other	El Salvador	Cambodia	United Arab Emirates
27.3 K	21.6 K	14.4 K	8.38 K	6.29 K	3.43 K	96	77	59	29

<u>Figure 7.</u> Sentinel Map 3 - Day 7, Russia overtakes Germany in failed attempts while new attack regions were added

DISCUSSION

Malicious actors use brute-force attacks to access online accounts and servers. This method of attack is favorable because it requires little effort on their part by letting computers do the work. SIEMs can identify fraudulent attempts at logging into an account or server. In this study, a test environment was set up to assess brute-force attacks on a server with a confirmed and operational SIEM in place.

This project involved setting up a honeypot, opening it to the internet, and using a SIEM to view the various attempts at off-line attacks and automated brute-force attacks from bots and individual hackers. Using a PowerShell script (Bošnjak 2018), a heat map was created with the IPs utilizing this API (Madakor 2021). The attacks observed were a confirmed combination of automated attacks from the likes of hydra and manually entered RDP attacks.

Throughout this project, the dangers of brute-force attacks and the utmost importance of using uncommon and non-default usernames with strong passwords (reference photo of logs) was observed. This study illustrates that no matter where a machine is, if it is open to the internet someone is going to try and break into it within hours of it going live. Furthermore, the usefulness of SIEMs allowing for the visualization of different logs in multiple different formats was observed, as well as allowing the group to understand what attack vectors people are taking against machines.

During this study, a further understanding of how brute-force attacks are carried out by penetration/red-team members was developed, as well as the observation of the utility of SIEMs as a vital component of cyber defense. Further experimentation would be adding different types of machines that would typically be on a home, small business, or university network. With multiple different types of machines on the network they would be susceptible to more sophisticated types of brute-force. Those more sophisticated attacks could be a RDP as a DDoS attack. The consequences of such attacks can cause loss of data, revenue, and worked hours(Arntz 2021).

LINKS

- GitHub project URL : *https://github.com/neelspatel999/The-Honeypot*

REFERENCES

1. CISA. What is Cybersecurity? | CISA. www.cisa.gov. Published November 14, 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-001
2. Bošnjak, L., Sres, J. & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. 1161-1166. doi:https://doi.org/10.23919/MIPRO.2018.8400211.
3. Grover V. (2020) An Efficient Brute Force Attack Handling Techniques for Server Virtualization. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3564447
4. Madakor J. (2022) Failed RDP to IP Geolocation Information. GitHub. https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1
5. Madakor J. (2021), SIEM Tutorial for Beginners | Azure Sentinel Tutorial MAP with LIVE CYBER ATTACKS! www.youtube.com. Accessed February 24, 2023. https://www.youtube.com/watch?v=RoZeVbbZ0o0&t=1938s
6. Free IP Geolocation API and Accurate IP Geolocation Database. ipgeolocation.io. Published 2021. Accessed February 24, 2023. https://ipgeolocation.io
7. Arntz, P. (2021). *RDP abused for ddos attacks: Malwarebytes labs*. Malwarebytes. Retrieved February 27, 2023, from https://www.malwarebytes.com/blog/news/2021/01/rdp-abused-for-ddos-attacks

ACKNOWLEDGEMENTS

Michael Veenstra, *Instructor, Fullstack Academy*
Colin Reyes*, Co-Instructor, Fullstack Academy*
Garbo Loo*, Mentor, Fullstack Academy*
Josh Madakor, *Instructor, Software Engineer, Content Creator - Youtuber*