**Forensic Investigations (FORIN)**

**REPORT**

Word Count: 3041

1

|  |  |
| --- | --- |
| **Section** | **Word Count** |
| Introduction | 550 |
| Design | 460 |
| Implementation | 369 |
| Results / Discussion | 1556 |
| Conclusion | 106 |
| **Total** | 3041 |

***Contents***

***1.0 Introduction......................................................................pg 3-4***

***2.0 Design.....................................................................................pg 4-8***

***3.0 Implementation.......................................................................pg 9-13***

***4.0 Results/Discussion....................................................................pg 14-26***

***6.0 Conclusion....................................................................................pg 27***

***7.0 references.........................................................................................pg28***

2

**1.0 introduction**

**Das (et.al 2018) A honeypot is a computer security mechanism which is setup as a decoy that’s mimics a real-life computer network infrastructure. Its purpose is to either redirect hackers from valuable information systems, detect any incoming attacks or intrusions attempts or to monitor and analyse what adversaries do once they are inside the system, such as the backdoors they use, what commands they run and the data there able to obtain. A honeypot is a combination of applications data and computers that emulate the behaviour of a real system. Hecker (et.al 2006) Honeypots can be one of the following:**

* **low interaction**

**This is where honeypots provide little interaction with the adversaries. An in-depth exploitation isn't possible and only a small number of services or emulated. An example of low interaction honeypots is Dionaea and Mailoney.**

* **Medium interaction**

**This is where honeypots simulate vulnerable services as well as file systems, shells and operating systems. Within this level or interaction, adversaries are able to complete a full exploitation. However due to the services running being a simulation, adversaries would be unable to complete any post exploitation attempts to the services not being fully functional. An example would be the SSH honeypot cowrie. SSH cowrie honeypot provides a secure connection for communication. It also logs brute force attacks and the interaction an attacker had with the system.**

* **High interaction**

**This is where honeypots are complete fully operations systems with vulnerabilities that adversaries can exploit. It is imperative that a high interaction honeypot is implemented carefully as it could lead the attacker to successfully exploiting the real system. SSH cowrie can also be setup as a high interaction honeypot.**

**Kelly (2021) Honeypots can be categorised into one of the following deployment categories:**

* **Internal honeypots**

**This is where honeypots are deployed within a LAN. The purpose of this method would be to monitor and identify any threats coming from within the network**

* **External honeypots**

**This is where honeypots are deployed on the internet and used to monitor and analyse attacks and threats from outside the LAN.**

**3**

**Singh (2011) There are two types of honeypots:**

* **Research honeypots**

**This is used in order to analyse in depth an adversary's activities and how to defend systems against their attempts.**

* **Production honeypots**

**This is where honeypots are used to divert adversaries from the real systems and give administrators time to assess the threat and address any weak spots within the system.**

**Kamow (2014) Benefits of honeypots:**

* **Gather threat intelligence of hackers, their methods and their objectives**
* **Learn about weaknesses and backdoors on your system in order to patch them**
* **Divert hackers from your real systems wasting their resources and time**
* **Opportunity for collection and analysis of real-world data**

**Drawbacks of honeypots:**

* **Hackers can distinguish it from real systems and avoid them**
* **Can be costly to setup and require high level skills to implement**
* **Can be used as a template for further attacks and leave other systems at risk**

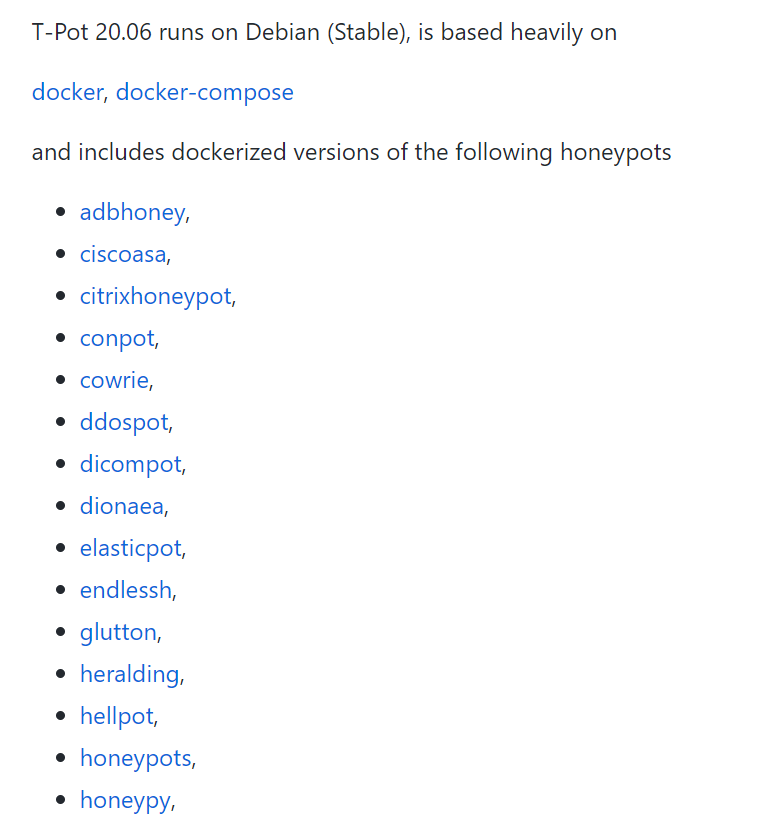
**Jackson (et.al 2004) A honeynet is a network consisting of multiple honeypots that are interconnected. By doing this practice it helps to convince the hacker that they’ve infiltrated the actual network and allows for a further analysis of how they interact with different network points.**

**2.0 design**

**For this assignment I will be utilising the T-pot honeypot. T-pot is a combination of multiple honeypots into one. The benefit of having multiple honeypots is that different honeypots adhere to different types of attacks. This will give me a wider range of data to collect and analyse. T- pot is open source and the honeypots are dockerised. This allows multiple honeypots and tools to run on the same network. T-pot also comes with some useful tools for better analysis and detection of the honeypot.**

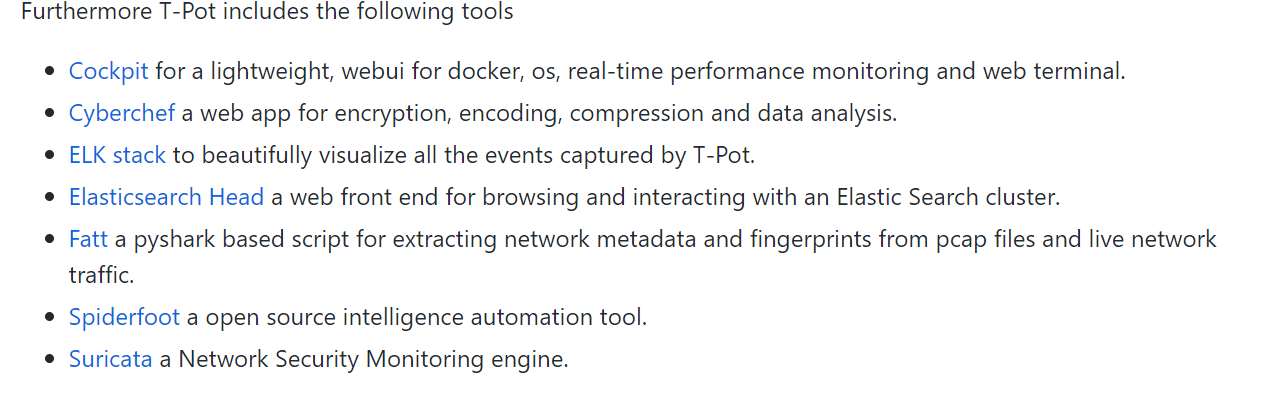
**4**

**Figure 2.1**



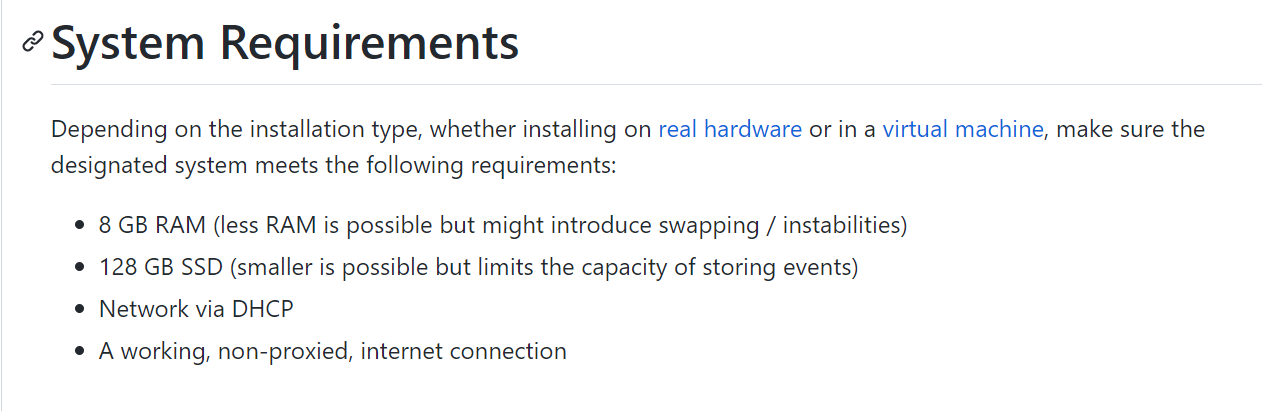
From figure 2.1 we can see some of the different honeypots that will be included. For example, cowrie is used to log SSH and brute force attacks whilst Dionaea is used to capture malware attacks.

**Figure 2.2**

From figure 2.2 we can see the lists of tools that t-pot comes with. One useful tool is the ELK stack. This will collect and store data but also generate stunning visualisation of the data such as graphs so that it's easier to read and understand. Another particular tool is Suricata. This is an intrusion detection and prevention system that logs any attempts to enter the honeypot or connect to any ports. Furthermore spider-foot is a tool that is used for reconnaissance. This can gather numerous details about a target such as their ASN, email, phone number, Ip address, hostname and so on.

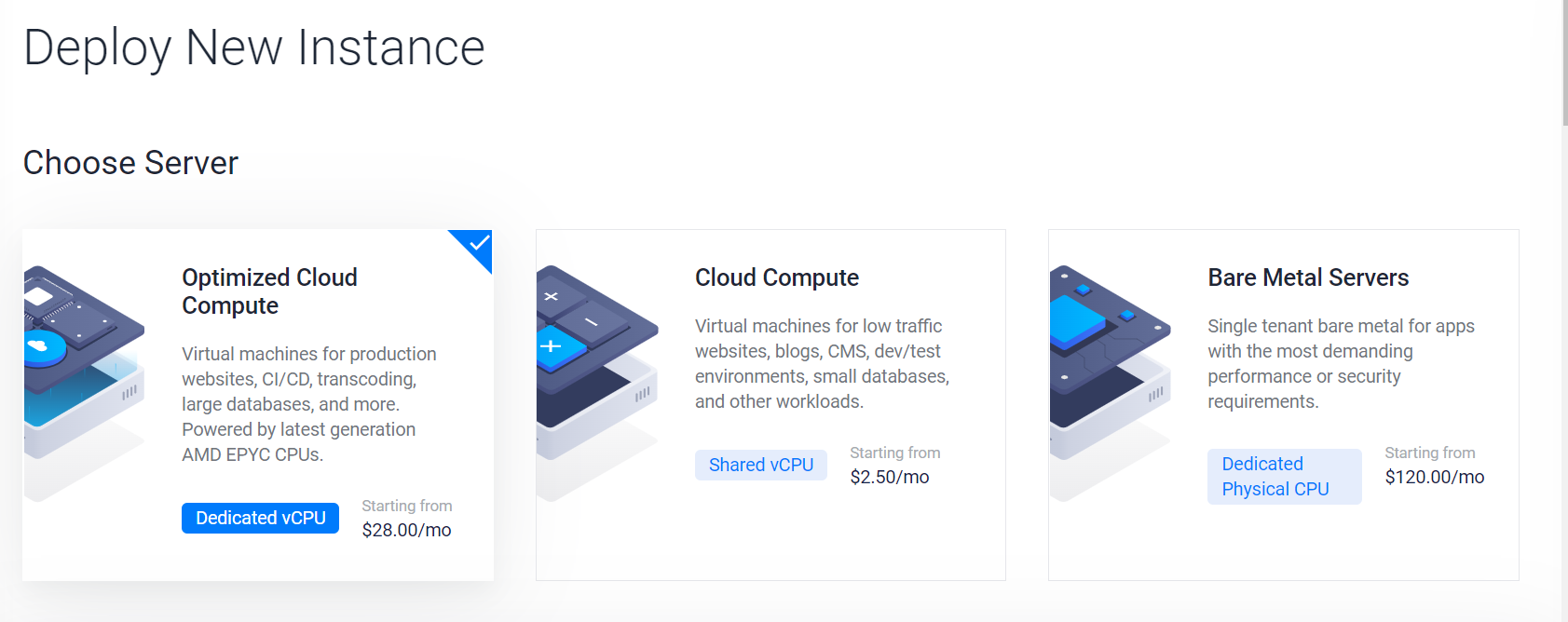
5

**Figure 2.3**



To host this honeypot, I will be using google vultr. This is because they give you free $100 when you sign up. This will come useful as it will allow me to provide enough resources for the honeypot to function properly.

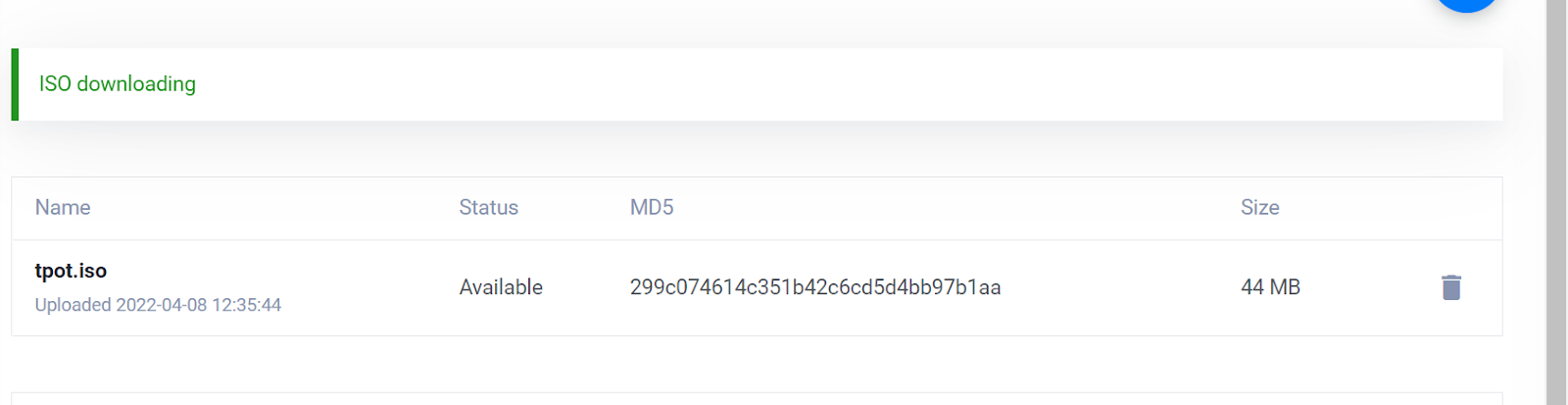
**Figure 2.4**



From figure 2.4, we can see how vutr allows me to create my own virtual machine instance off the cloud. Here I have selected optimized cloud compute for this server as its more powerful than cloud compute.

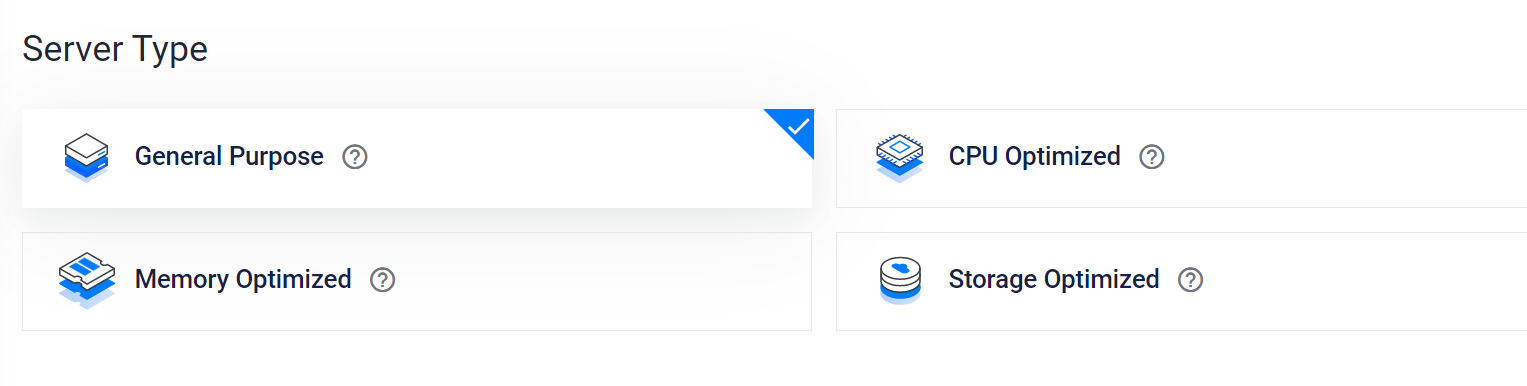
**6**

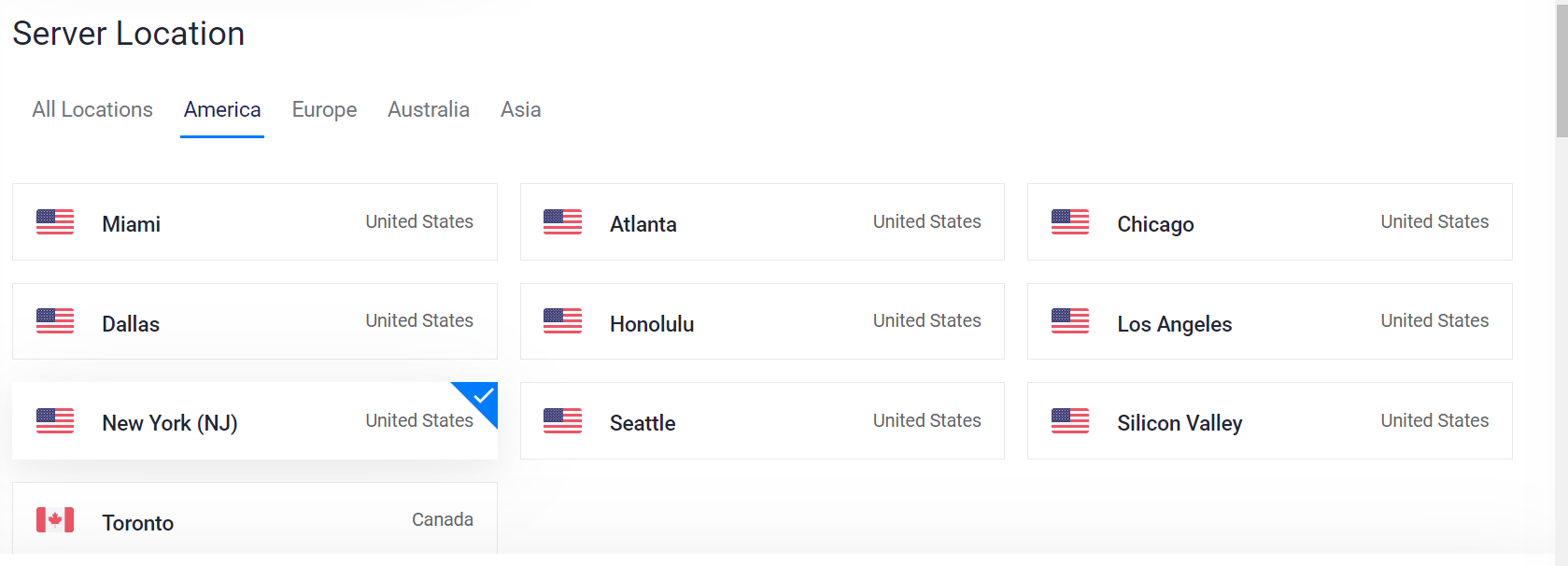
**Figure 2.5**



From figure 2.5 we can see the downloading of the iso image. This iso image was copied from the t-pot website. This will help in doing all the configurations for me. For example, it will set the operating system to Debian version 10 as that is what t-pot runs on.

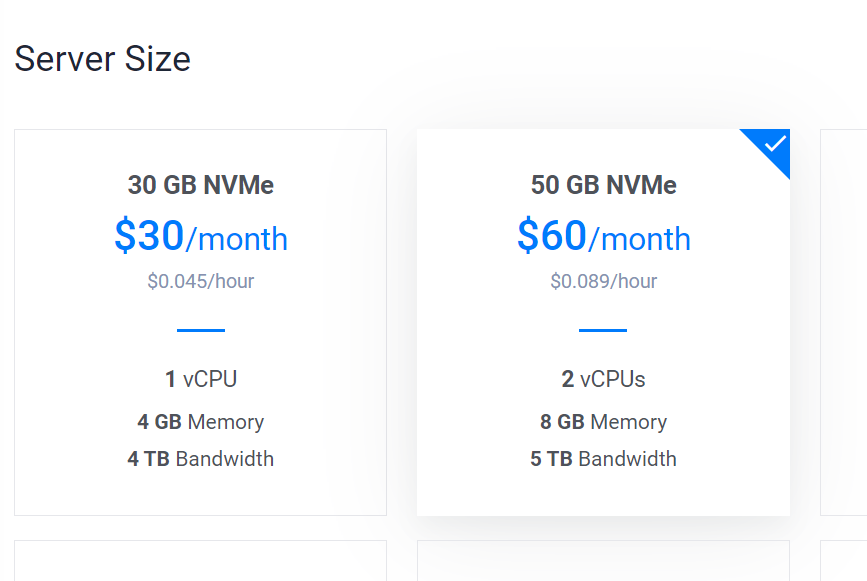
**Figure 2.6**

**Figure 2.7**



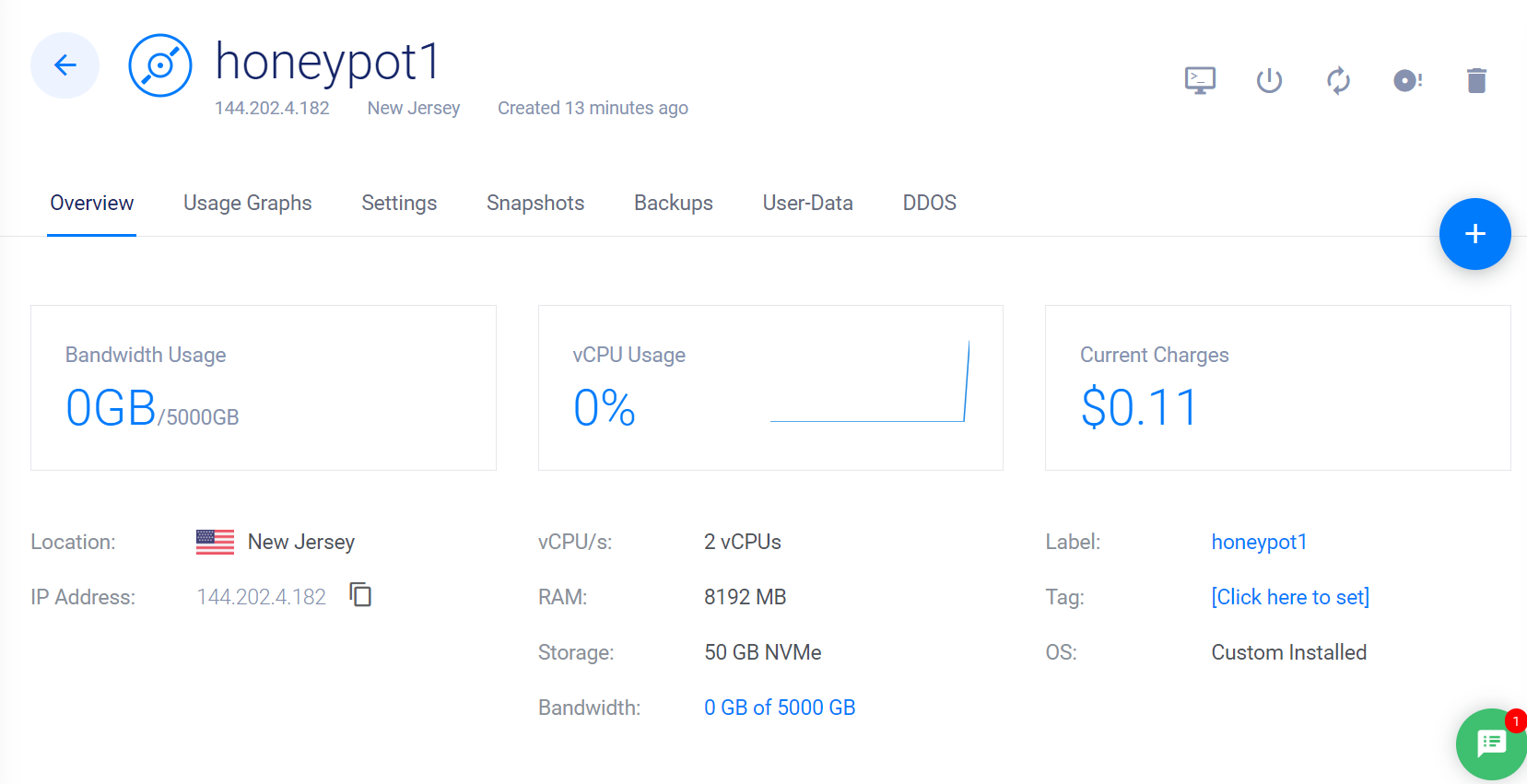
**7**

**Figure 2.8**



From figure 2.6,2.7 and 2.8 we can see more of the configurations I've made. I set the location and zone in America. I've made it general purpose as I'm not performing any specific tasks where I would want the machine to optimize A certain feature. For the machine type I set it to 2vCPU 8GB as from looking at figure 2.3, that selection matches the recommended requirements for the installation.

**Figure 2.9**

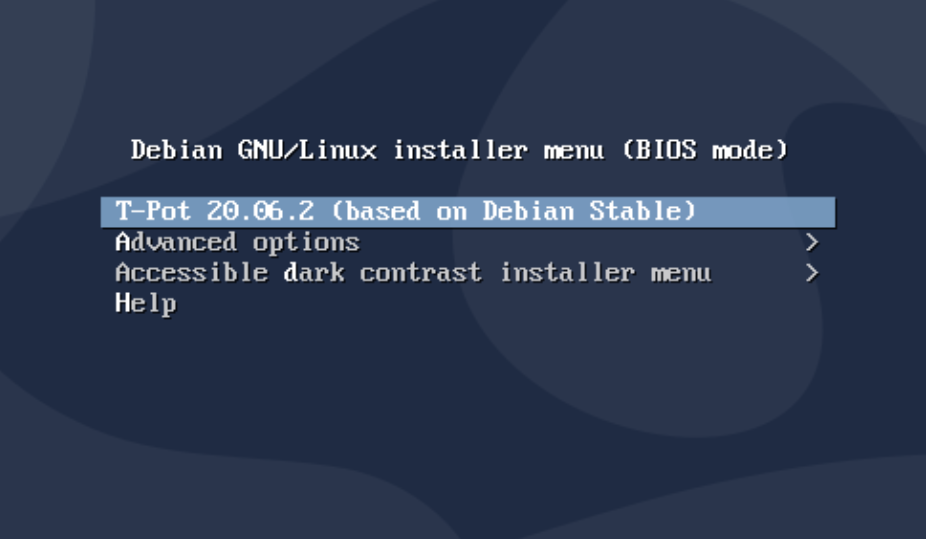


From looking at figure 2.9, we can see how my vm instance has been successfully created with the configurations I made during the setup. Furthermore, I have been allocated an Ip address.

**8**

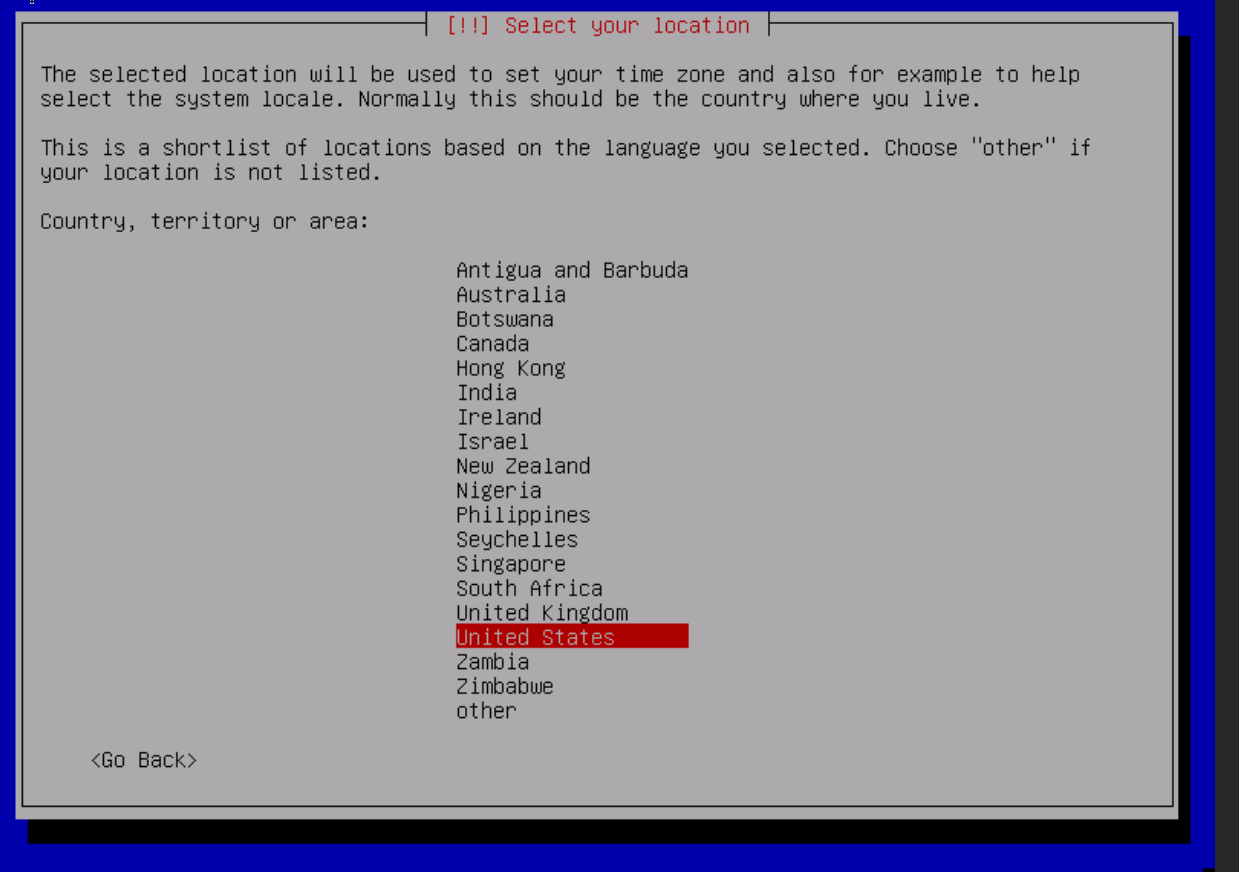
**3.0 implementation**

**Figure 3.1**



From figure 3.1 I have initiated the console now I will start the installation.

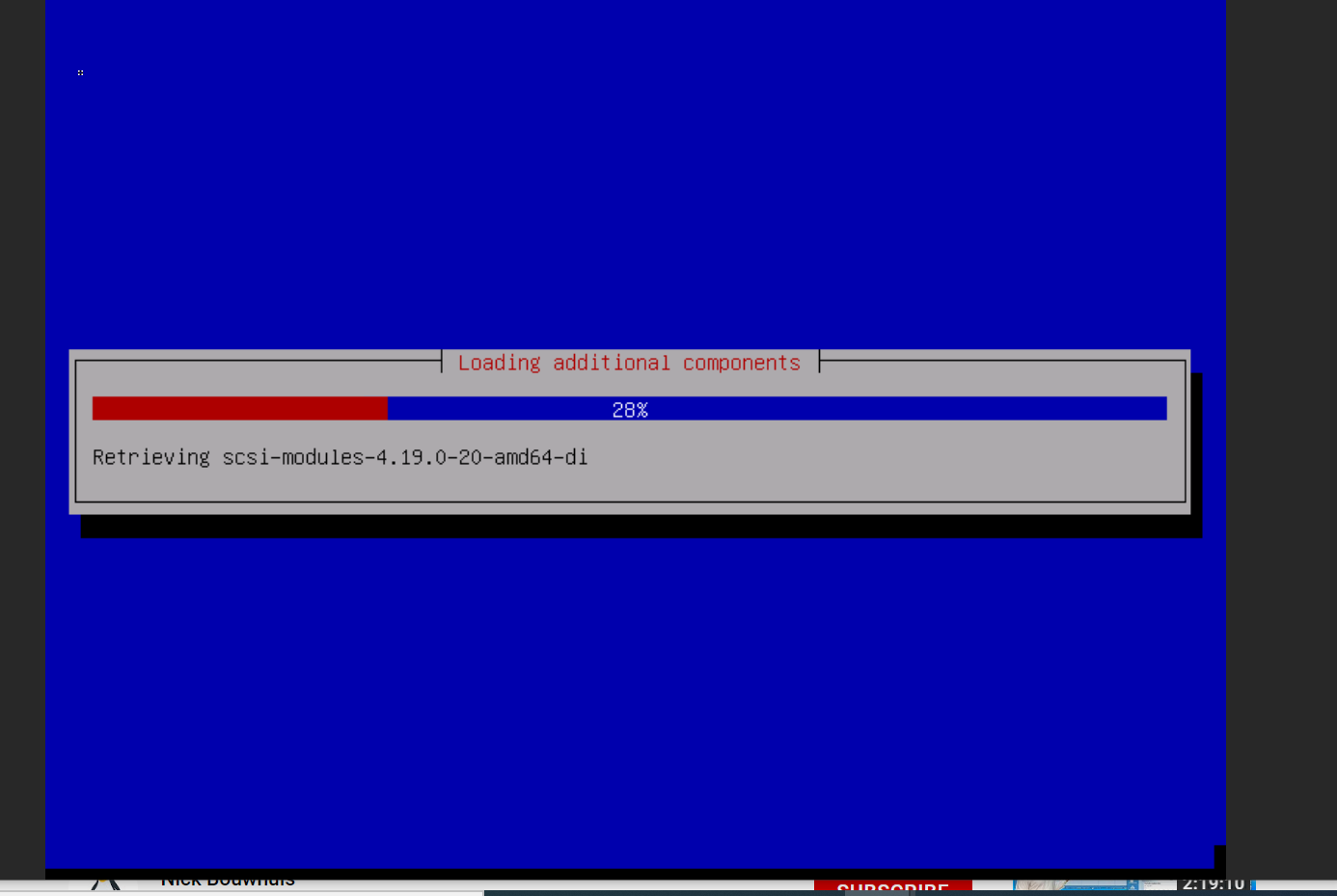
**Figure 3.2**



From figure 3.2 I am prompted to select a location. This for instance will be used to set my keyboard layout so I will choose United Kingdom English.

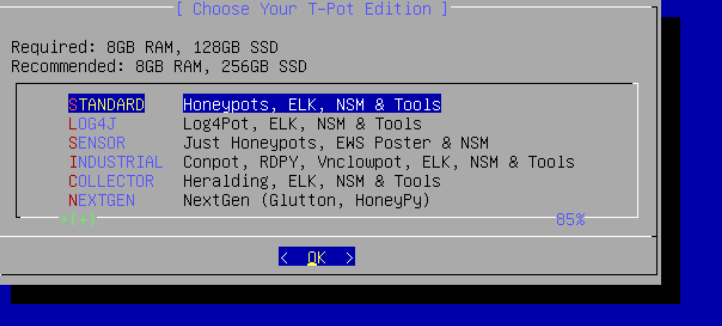
**9**

**Figure 3.3**



After which, from figure 3.3 it shows the installation locating and installing the required files from the internet. When it is completed, it will reboot automatically.

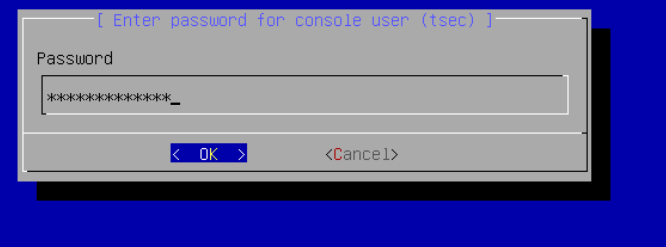
**Figure 3.4**



After it is rebooted, I remove the iso image and initiate the console again. Then the t-pot installation begins. From figure 3.4, I am prompted to select the type of t-pot that I want. Here I choose the standard one as it will come with all the necessary honeypots and tools that I need.

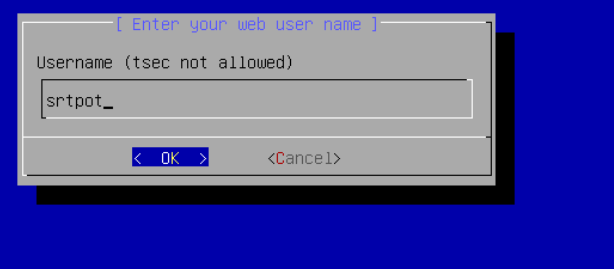
**10**

**Figure 3.5**



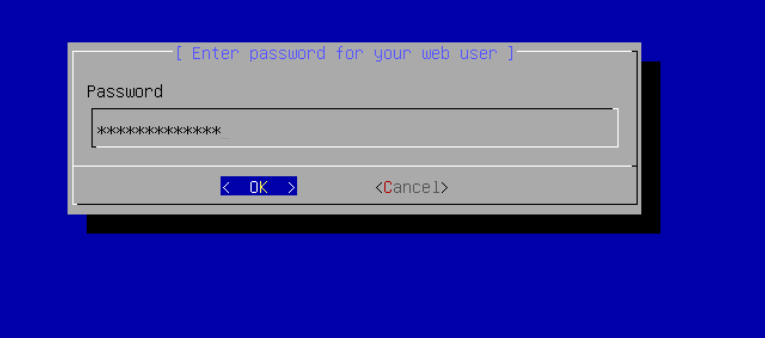
From figure 3.5 it shows how I am prompted for a password. I enter a secure password and its asks me to repeat it so that I don’t forget it.

**Figure 3.6**



From figure 3.6 we can see how I'm prompted for a username.

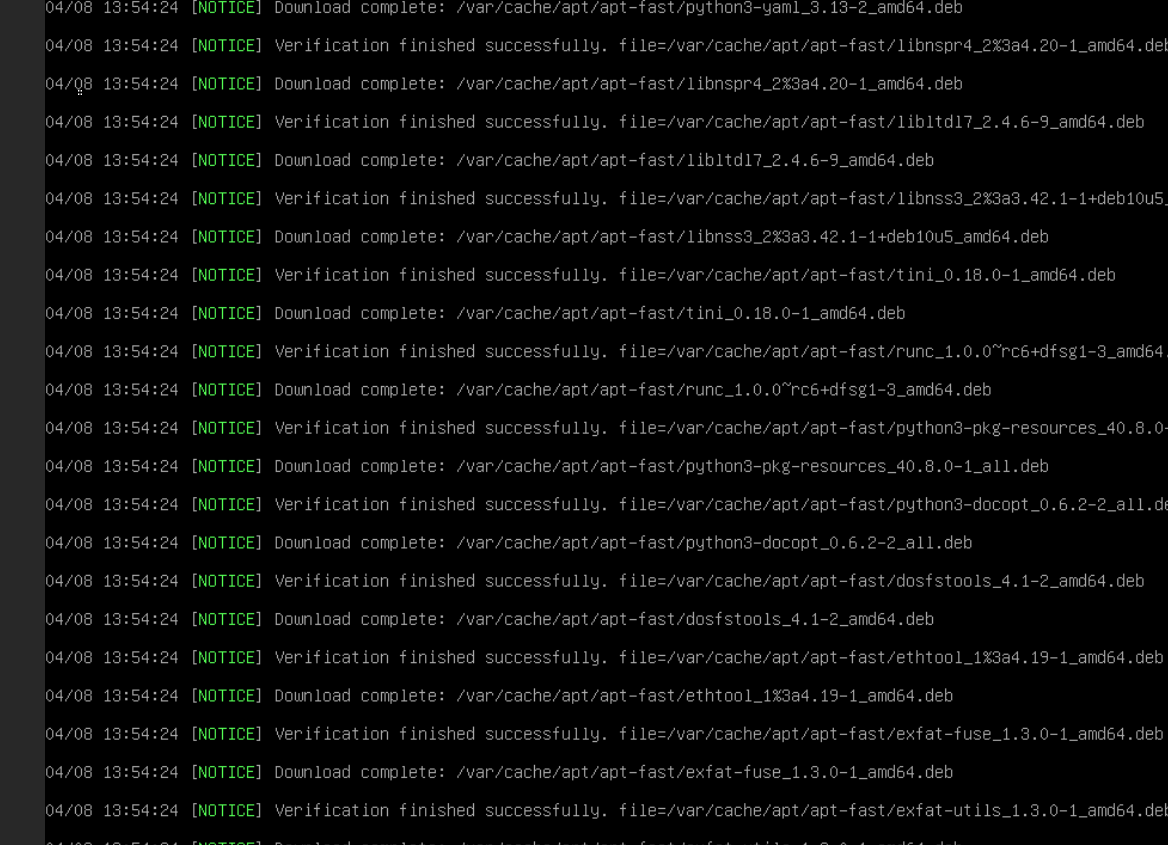
**Figure 3.7**



From figure 3.7 we can see how I'm prompted for a password. I enter a secure password then I am asked to repeat the password for security.

**11**

**Figure 3.8**



From figure 3.8 we can see how the t-pot begins to install the other honeypots and tools. This will take a couple minutes.

**Figure 3.9**



12

From looking at figure 3.9, we can see how the t-pot has successfully finished installing. I have been allocated an Ip address. To access my t-pot I will enter the web address shown in figure 2.18 and point it to the port 64297.

**Figure 3.10**

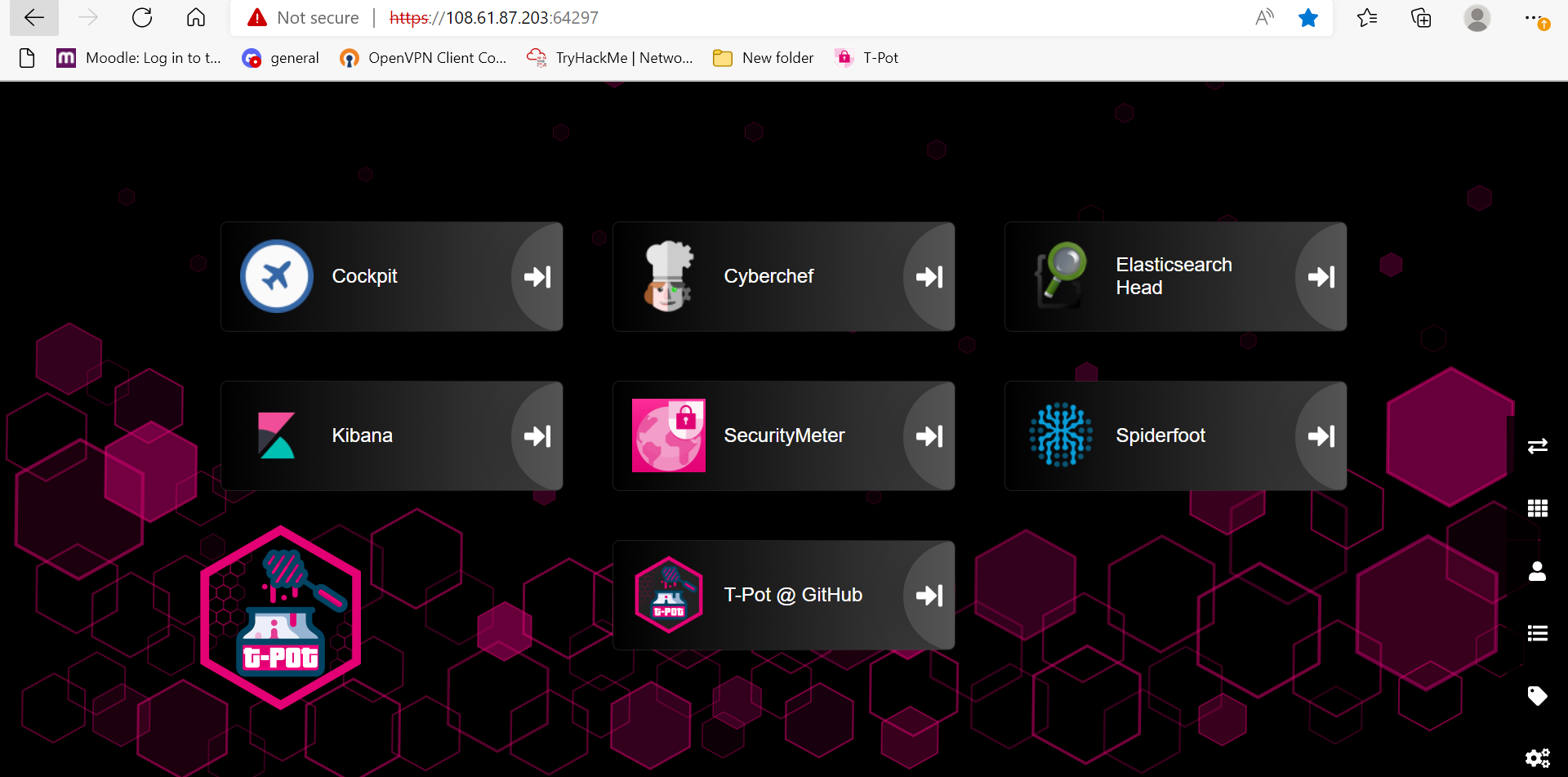


Figure 3.10 shows how I have successfully accessed the dashboard for my honeypot using the web address from the previous figure image. Here I am presented with the different tools for viewing and analysing the data collected from my honeypot. One tool that will be extremely useful is Kibana. This is the tool that will display the data in graphs that will be more readable.

**Figure 3.11**

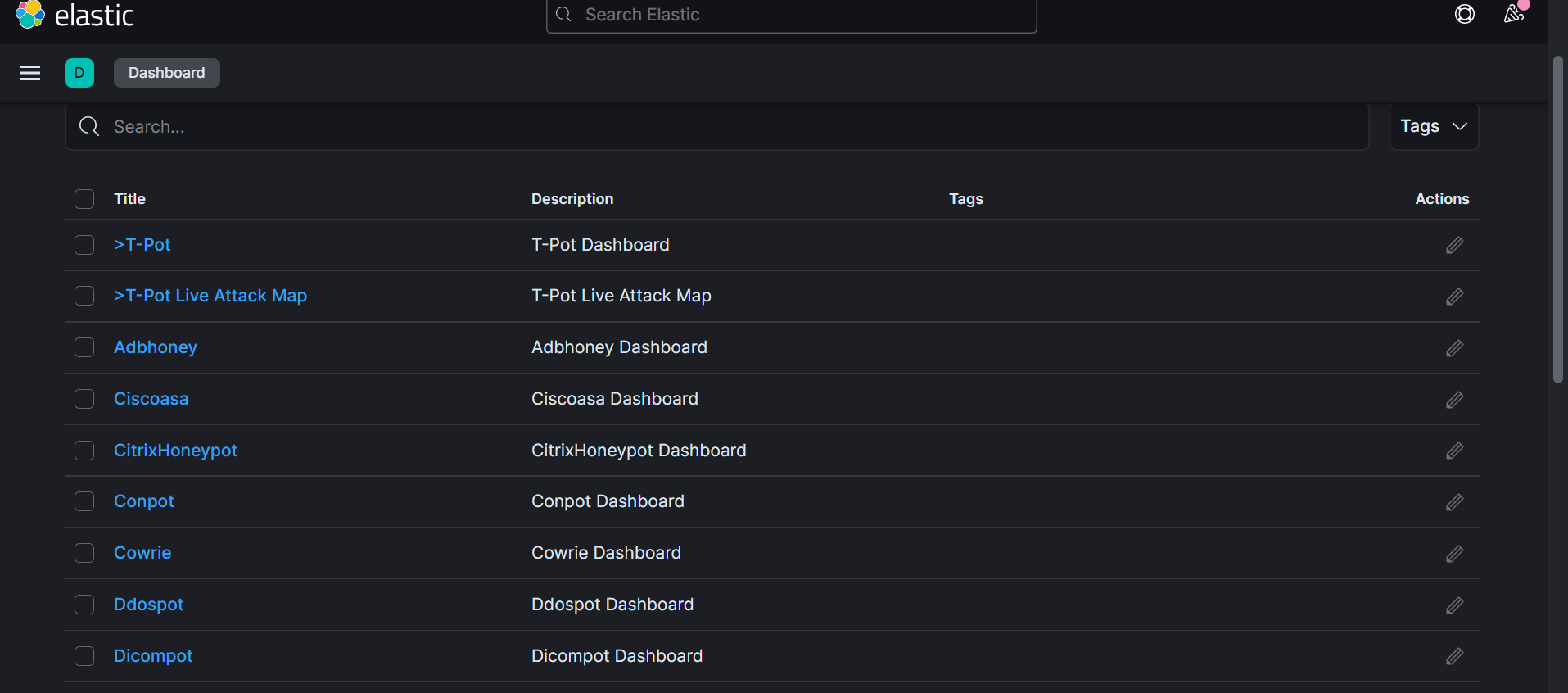


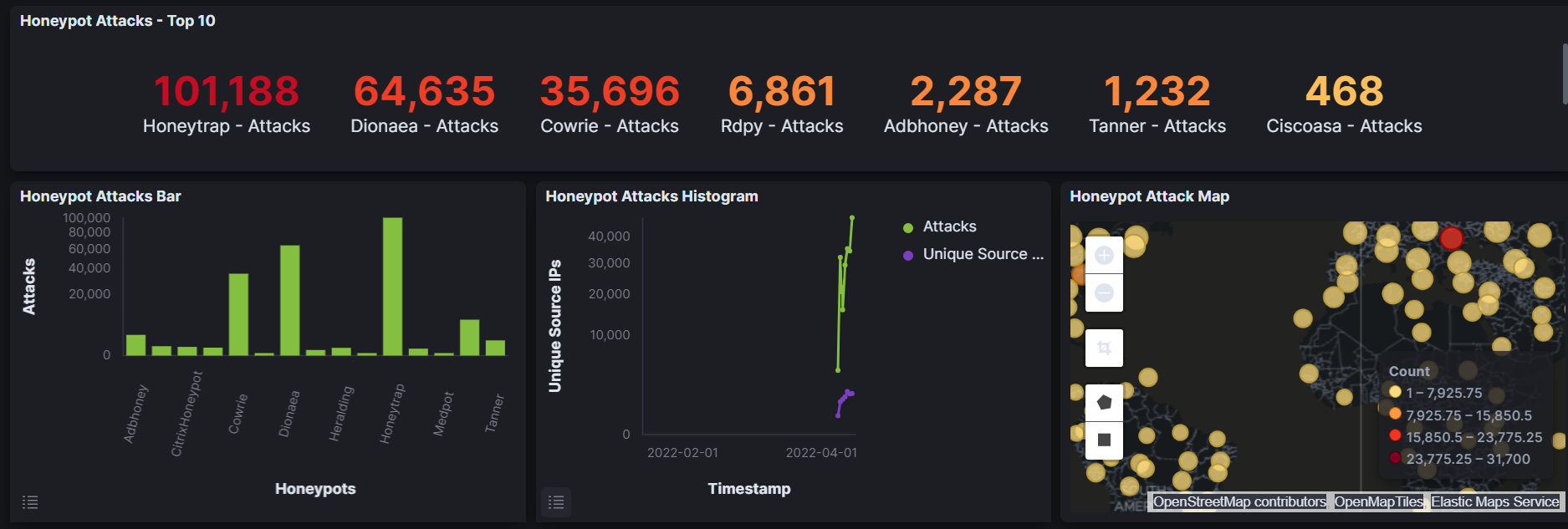
Figure 3.11 displays the numerous amounts of honeypots that are installed on the t-pot. Here I can view the data for the individual honeypots or I can select the t-pot dashboard which will group together data from all the honeypots for a data analysis comparison.

**13**

**4.0 Results and discussion**

**For this t-pot I allowed it to run for seven days straight. This would provide enough time for adversaries to pick up my honeypot and proceed to attack and gather information using their various methods and techniques. This in turn would provide me with enough data to analyse. From analysing the data, I can proceed to gather numerous information such as the adversaries ip address, their geographical locations, ports that they attacked, methods they used to gain access and what they did on my system and what they were able to gather.**

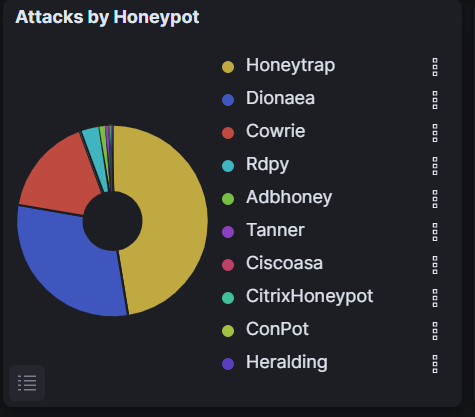
**Figure 4.1**



For this analysis I select the t-pot dashboard in order to see the various honeypots that where being attacked. From figure 4.1 we see can see the top 10 honeypot attacks with honeytrap being the highest at 101,188 attacks. This is a large amount. From this I can make the assumption that the adversaries' main goal was to intercept data within my system. This is because honeytrap is used to capture tcp and udp service attacks. These protocols are responsible for data transmission.

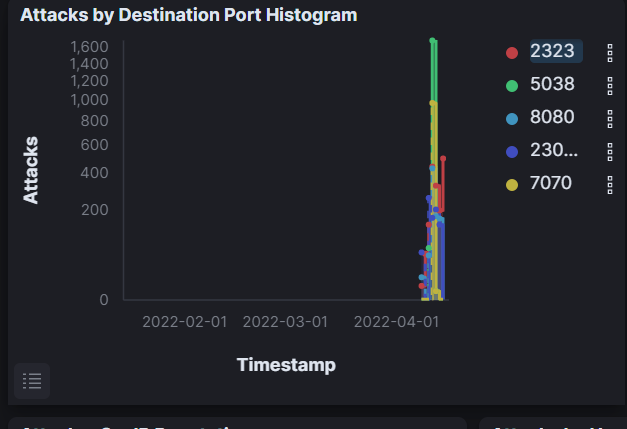
14

**Figure 4.2**



Furthermore, the graph in figure 4.2 shows the percentage of honeypots attacked with honeytrap taking almost half at 47%. Based on these figures it is apparent that honeytrap is the most vulnerable honeypot and security measures must be taken to reduce adversaries exploiting it.

**Figure 4.3**

 15

From looking at figure 4.3 we can see that the port that adversaries attacked the most within honeytrap was port 5038. In order to reduce the amount of honeytrap attacks we could close port 5038. From further analysis it seems port 23023 is the most secure as it was accessed the least number of times.

**Figure 4.4**

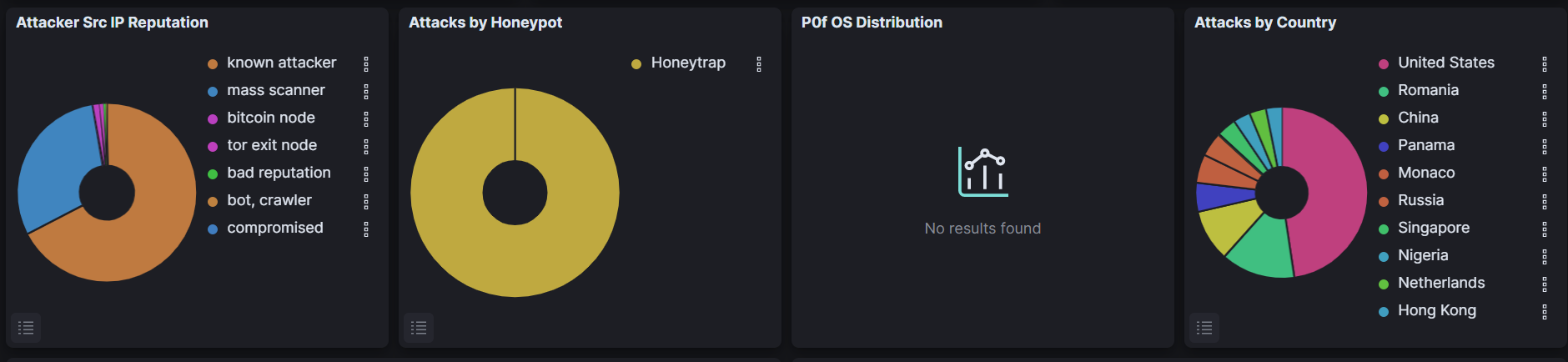
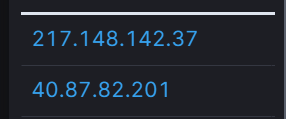
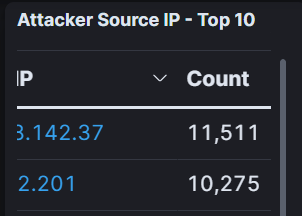


Figure 4.4 tells me that the 67% of the attacks that are aimed at the honeytrap are coming from a known Ip address. Meaning the Ip address has been connected to other cyber-attacks. Furthermore, the figure shows us that majority of these attacks are coming from America. This could be due to the honeypot location being set in America.

**Figure 4.5**



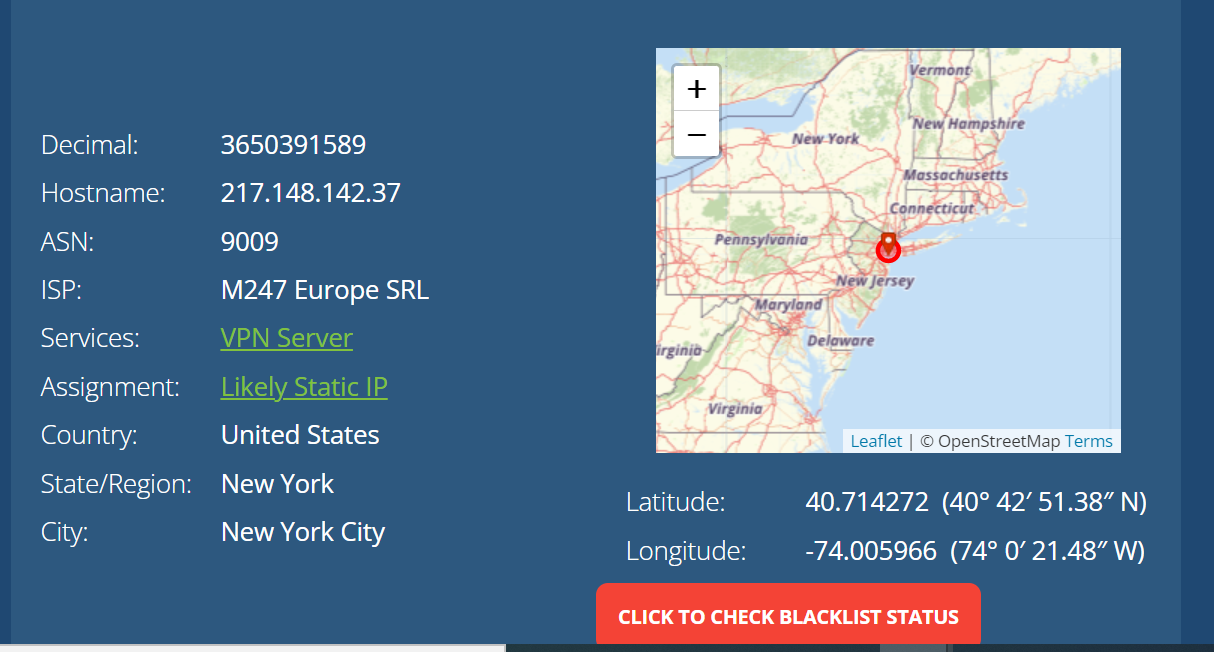
**Figure 4.6**



16

From looking at figure 4.5 and 4.6 I can see the Ip addresses that are responsible for the most attacks. The top 2 are particularly important as they have over 10,000 recorded attacks.

**Figure 4.7**

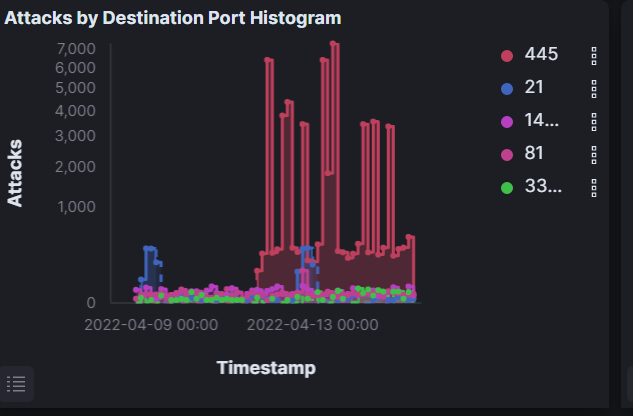


I took the first Ip address and searched it on Ip address lookup. From figure 4.7 I can see numerous details about the Ip such as the ASN, ISP and location. All these details can be used to generate a picture on who the adversary is and what they are after. I searched the Isp on google and found that the ISP has a medium risk of being fraudulent. Furthermore, I found that it runs a cloud service. This could indicate that the Ip is potentially a spoofed Ip address and not the attackers actual Ip.

The second largest honeypot that was attacked was Dionaea. This honeypot is responsible for capturing and analysing malware attacks. This is especially crucial as if an adversary is able to successfully mount their malware, they could take over the entire system and access confidential information or potentially shut down the network with a ddos attack. This makes it imperative that any malware discovered should be quarantined and added to a database of known malware that can be cross referenced against future attacks.

**17**

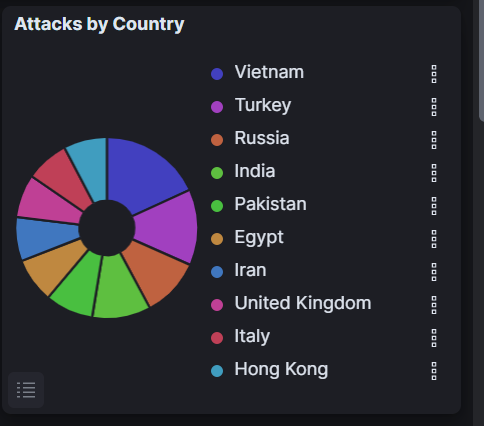
**Figure 4.8**



From looking at figure 4.8 we can see that port 445 is the most desired port in terms of Dionaea attacks. This port is responsible for file sharing, communication and authenticating users. From that knowledge I can make the assumption that the adversaries are attempting privilege escalation in order to give themselves access to files that lower privileged users wouldn't have access to. A recommendation would be to ensure proper authentication protocols are put in place and to ensure data is kept secure so that adversaries can't compromise the C.I.A od the data.

**18**

**Figure 4.9**

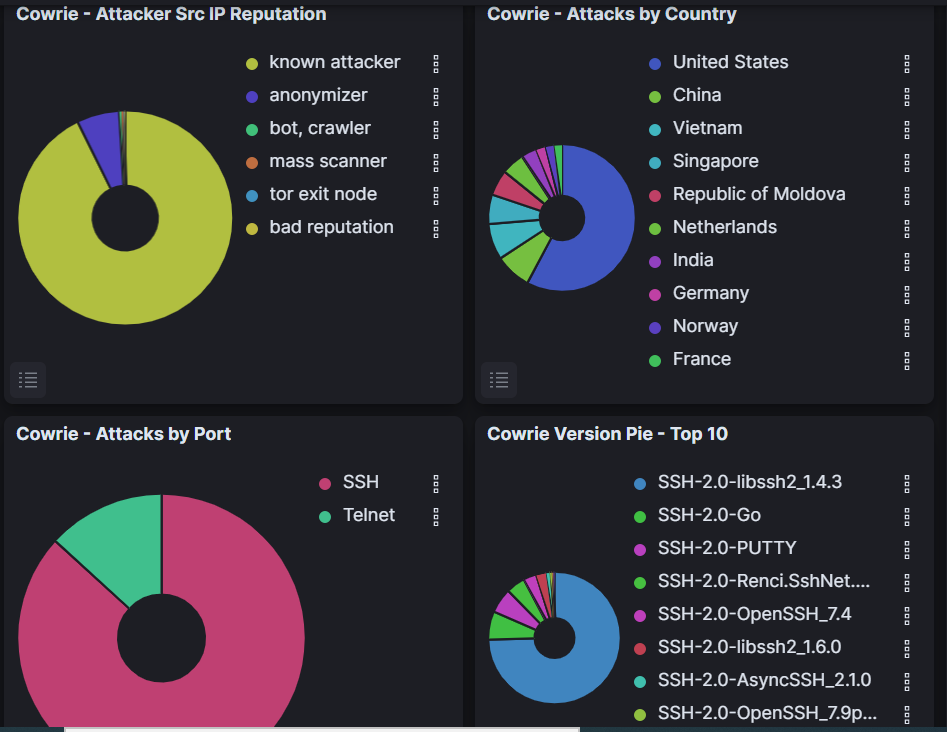


19

From looking at figure 4.8 I can see that these Dionaea attacks are coming from a fair distribution of different countries with Vietnam being slight above the rest. This demonstrates how port 445 is a global desirability for adversaries.

The third largest honeypot attacks where cowrie attack with 35,696 attacks. Cowrie is a honeypot used to log brute force attacks and the interaction adversaries undertake when gaining access to a system. Cowrie also provides SSH and telnet services.

**Figure 4.9**



From looking at the figure above we can see a large majority of attacks where on port 22. This is the default port for SSH. Based on this it would be strategic to ensure that this port is secured to reduce the number of attacks. Furthermore, we can see a repeated pattern as majority of the attacks are from America and are known attackers. 75% of the cowrie versions were done on SSH-2.0-libssh2\_1.4.3. Based on this large number, it can be assumed that there is known vulnerability that adversaries have full knowledge of. By searching this on google I discovered that this version of SSH is susceptible to denial-of-service attacks. To counteract this, we can implement a firewall to restrict the traffic that comes in and out of the network.

**20**

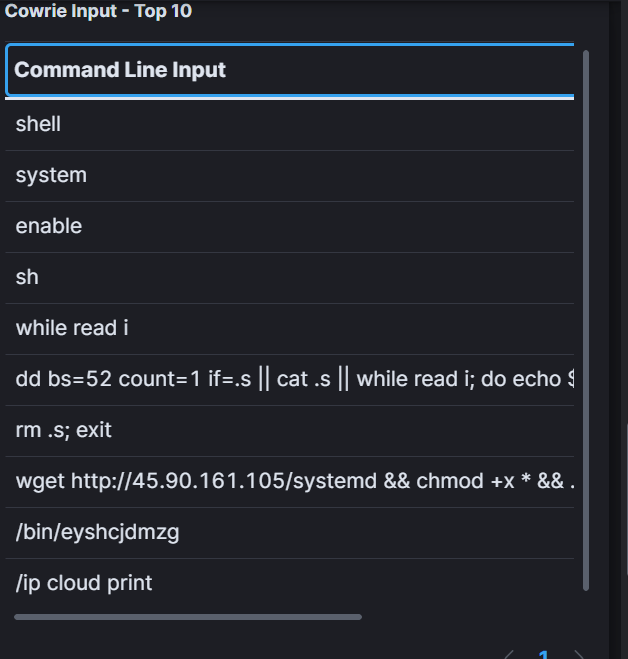
**Figure 4.11**



From figure 4.11 we can see the combination of usernames and passwords that adversaries used. Here I can see simple usernames such as root, user and admin being used. These tend to be default usernames on systems. The passwords also seem to be weak passwords with a lot of them just being numbers or simple words. From this I can make the assumption that the adversaries are using brute force and dictionary attacks. To protect against this, we can set a limit on the amount of failed login attempts that are allowed. Furthermore, we can implement a policy where users have to have a strong password which contains a combination of different characteristics such as upper/lowercase letters numbers and characters. A username that stood out was the GET/HTTP/1.1. This is a HTTP request and tells me that an attacker tried to gain information from the server. To combat this, we can implement input validation.

**21**

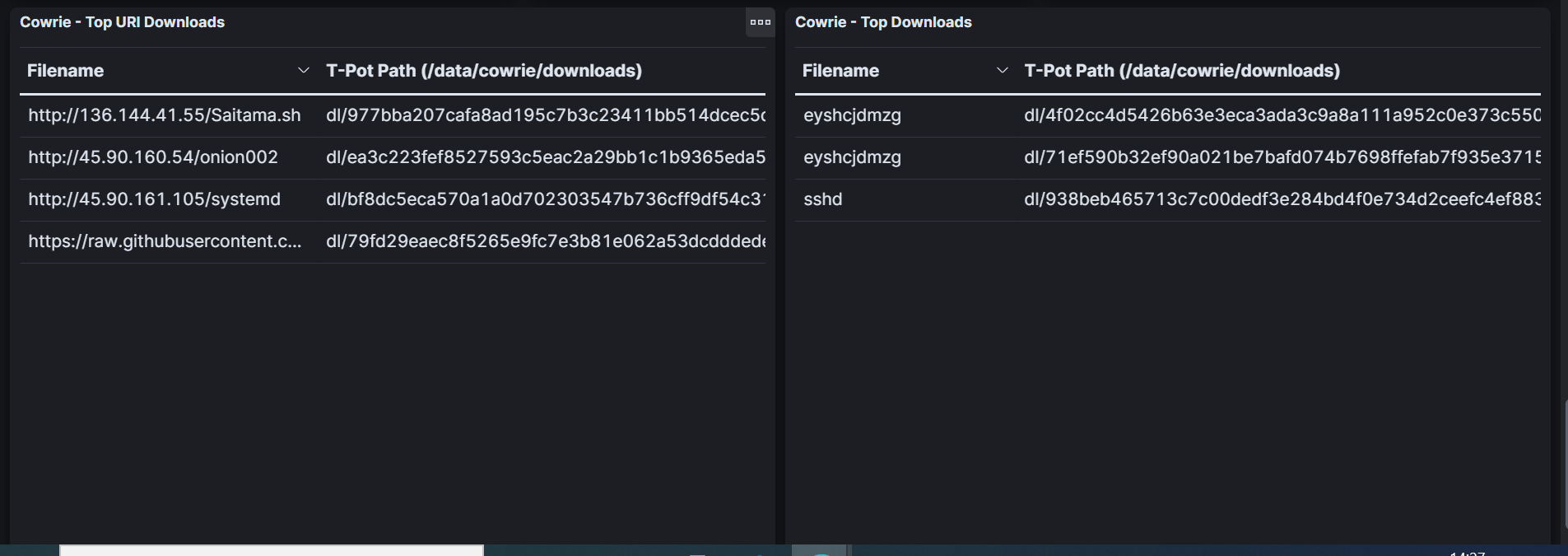
**Figure 4.12**



From looking at the figure above we can see the top 10 command that attackers inputted. Shell commands are commands that the system what actions to perform. Because the top 3 are shell system enable, I can make the assumption that attackers tried to disable any system restrictions that would prevent them from gaining further access to the honeypot. It also seems they used a python script and read through and saved the information they were able to retrieve.

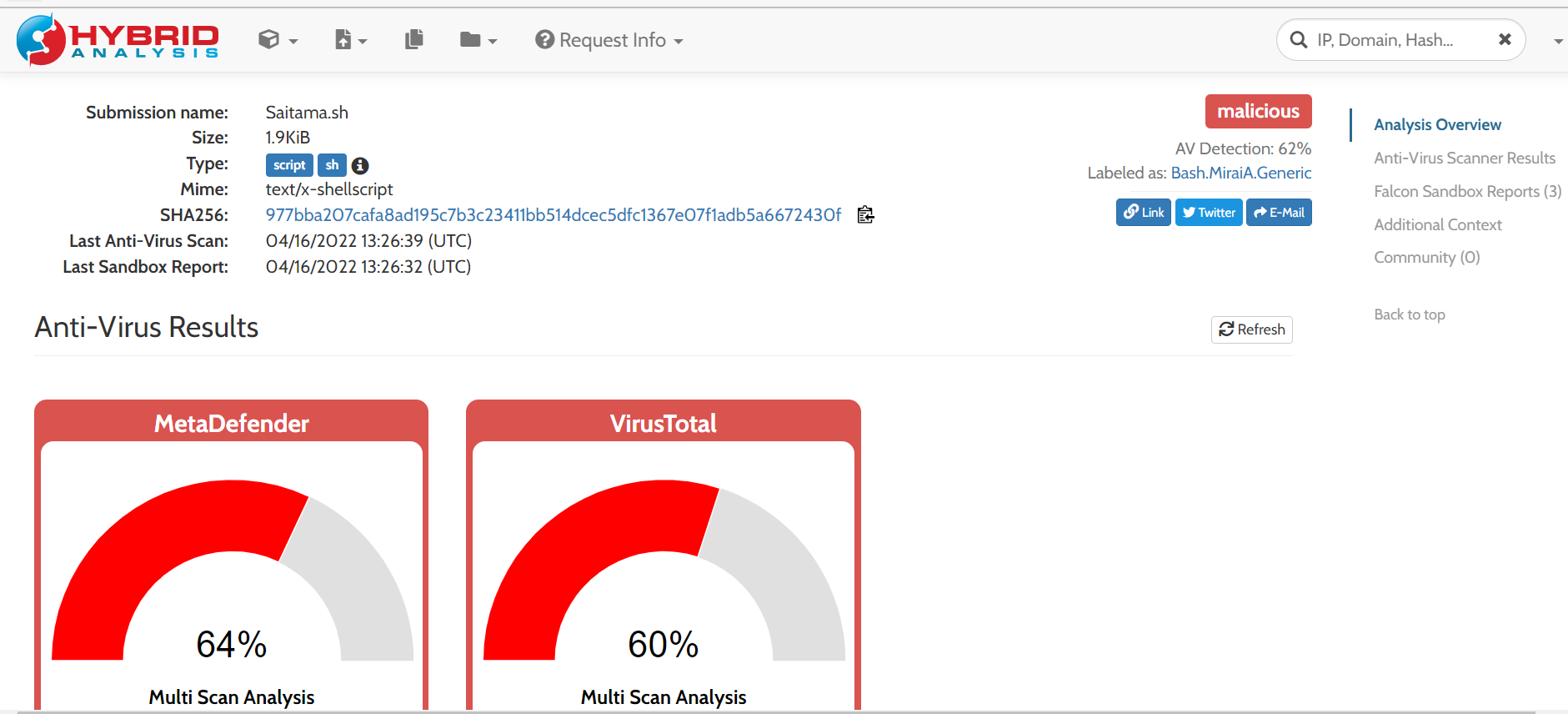
**22**

**Figure 4.13**



From looking at the figure above, I can see what files they adversaries tried to download or retrieve to and from my system.

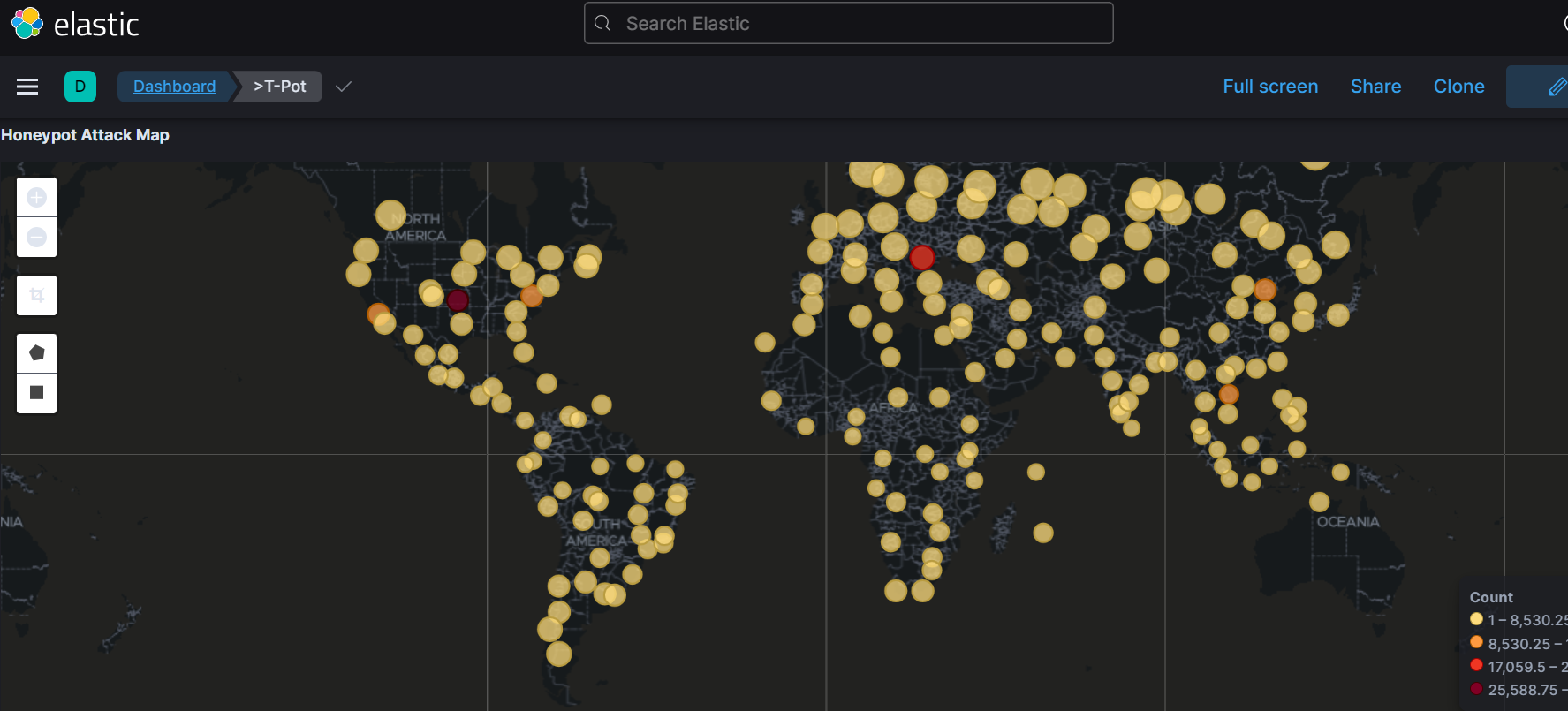
**Figure 4.14**



I took one of the files and analysed it on hybrid analysis. From the figure above we can see that the file is malicious and most likely malware. Here we can see further attempts of adversaries either trying to gain information or take remote control of the system.

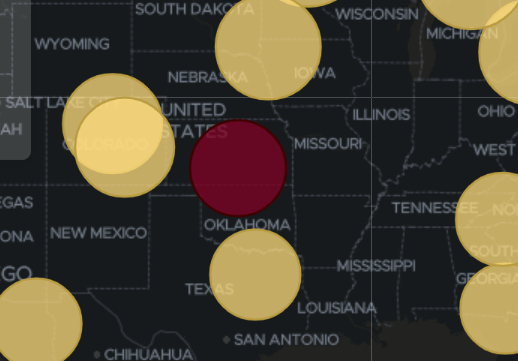
**23**

**Figure 4.15**



From this figure above we can see that attacks are coming from all across the globe. There's one area in particular where a high count of attacks is coming from. This is shown by the dark red circle.

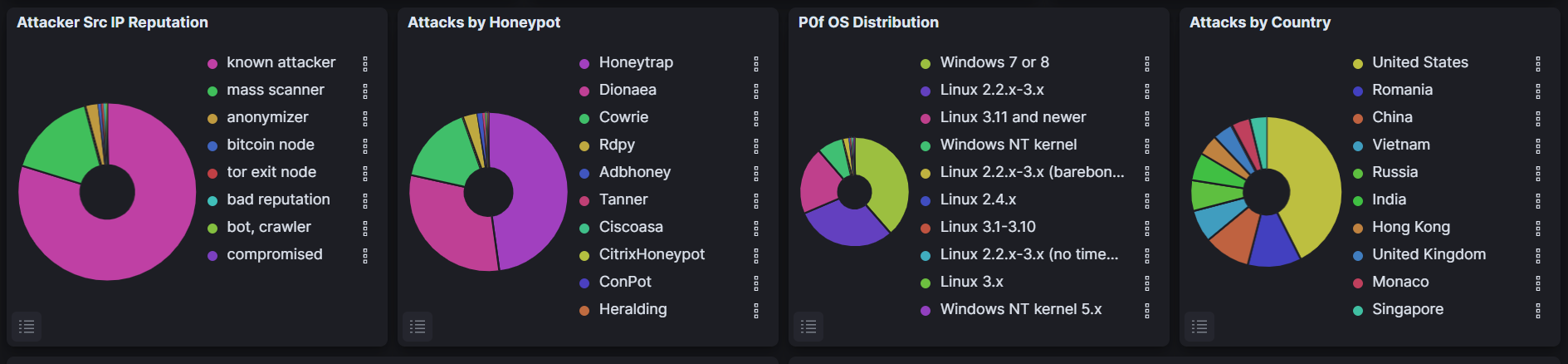
Figure 4.16



When I zoom in, we can see from the figure above that the highest number of attacks are coming from Oklahoma. This can give more insight into who the attackers are and could suggest that they are based in Oklahoma.

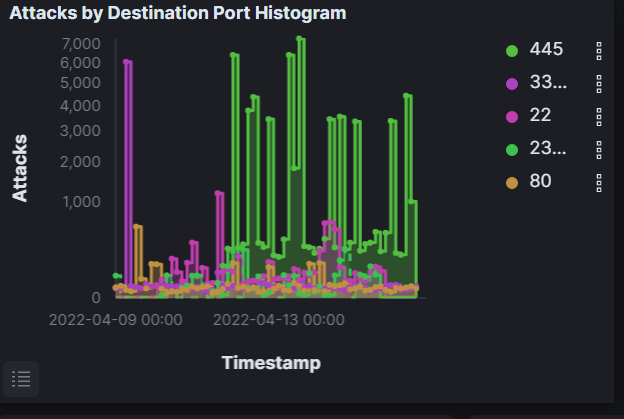
24

Figure 4.17



From the figure above, we can see that across all the honeypots, the Ip addresses that are administering the attacks are known attackers. From this it narrows down who the adversaries are as they’ve already been flagged for previous attacks. This could mean that they have already been identifies by government authorities and Arnt a new threat. We can also see the operating system that they use. This can help us to understand what systems the network is most vulnerable to. Furthermore, it can give an indication into the attackers computing expertise. Because windows 7 &8 are number 1, it shows how the honeypot is vulnerable to old os as this was released in 2009. To combat this, it would be ideal to patch the network against vulnerabilities that old os can exploit. Also, to note, majority of attacks on the honeypots worldwide are coming from the United States. This could mean the attackers are from America.

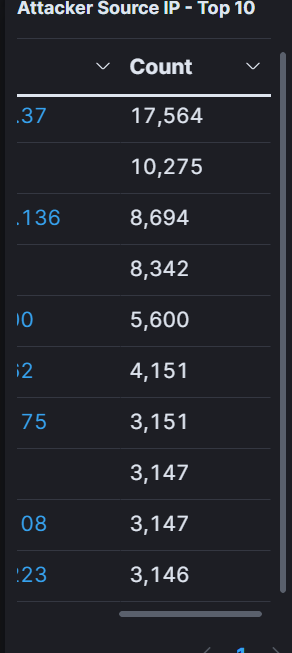
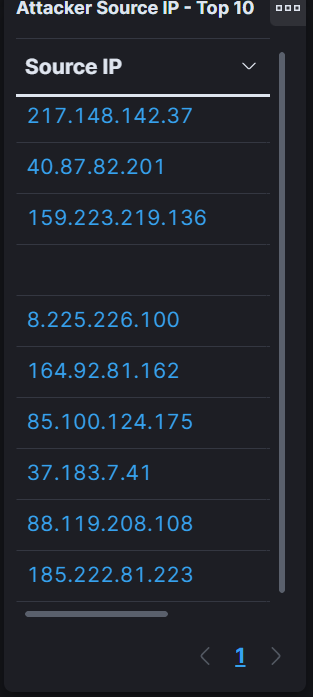
**Figure 4.18**



From the graph above it is apparent that port 445 is the most vulnerable port. This makes it critical that the port is properly secured. As stated, its used for networking and communication, so if comprised, attackers can syphon off confidential transmissions. Closing the port would be a reasonable approach.

**25**

**Figure 4.19**



The figure above shows the top 10 Ip addresses and records how many attacks they are responsible for. Based on this we can further identify the adversary. Because so many attacks are coming from the same Ip addresses, I can assume that the same adversary has tried to attack the network more than once. The top 2 Ip address was previously identified when I was discussing the honeytrap. It's important to point out that although most of these attacks and Ip addressed are from America, its unlikely to be the adversaries actual Ip. This is because they are most likely spoofing Ip addresses to hide their identity. Alternatively, we could block the Ip addressed to stop them from launching future attacks.

**26**

**5.0 conclusion**

**Honeypots are a useful asset to implement. They can provide a client with useful data that they can analyse in order to gain a better understanding of their attackers. This could be information such as their attack methods, location, Ip address, and motivation. Furthermore, it provides the client with useful information on their security weaknesses. This can then be used to patch any critical vulnerabilities. Setting up t- pot was especially useful as it gave me numerous amounts of data**

**From different honeypots which I could compare. Furthermore because of its different tools and graphical presentation of data, it made it easier to read and understand.**

**27**

**7.0 references**

**Baykara,M, Das,R, (2018) *a novel honeypot based security approach for real- time intrusion detection and prevention systems, journal of information security and applications,41,103-116,<https://doi.org/10.1016/j.jisa.2018.06.004>***

***Hecker, C, Nance, K. L, Hay, B. (2006). Dynamic honeypot construction. In Proceedings of the 10th Colloquium for Information Systems Security Education,95-101,102,*** [Dynamic Honeypot Construction (psu.edu)](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.5761&rep=rep1&type=pdf)

***Jackson, T. R., Levine, J. G., Grizzard, J. B., & Owen, H. L. (2004) An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network. IEEE, (pp. 9-14). https://doi.org/10.1109/IAW.2004.1437791***

***Jain, Y. K., & Singh, S. (2011). Honeypot based secure network system. International Journal on Computer Science and Engineering, 3(2), 612-620. ,Doi=10.1.1.444.1707&rep=rep1&type=pdf***

***Kambow, N., & Passi, L. K. (2014). Honeypots: The need of network security. International Journal of Computer Science and Information Technologies, 5(5), 6098-6101.,***[Microsoft Word - 21. IJCSIT-paper format \_1\_ (psu.edu)](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.567.3334&rep=rep1&type=pdf)

***Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S, Buchanan, W. J. (2021). A Comparative Analysis of Honeypots on Different Cloud Platforms. National library of medicine,2433, 21(7), https://doi: [10.3390/s21072433](https://dx.doi.org/10.3390%2Fs21072433)***

**28**