A Novel Approach Towards Analysis of Attacker Behavior in DDoS Attacks

Himanshu Gupta, Tanmay Girish Kulkarni, Lov Kumar, Neti Murthy

A Novel Approach towards Analysis of Attacker Behavior in DDoS Attacks

Himanshu Gupta, Tanmay G. Kulkarni, Lov Kumar and N.L. Bhanu Murthy

BITS Pilani, Hyderabad Campus, Hyderabad, India
{f20150339,f20150647,lovkumar,bhanu}@hyderabad.bits-pilani.ac.in

Abstract. Traditionally, research in Network Security has largely focused on Intrusion Detection and the use of Machine Learning techniques towards identifying malicious agents as well as work on methods towards protecting ourselves from such attacks. In this paper, we wish to make use of the same techniques to analyze the profile of the attacker in the case of a DDoS attack on a distributed honeypot.

Keywords: Distributed Denial of Service Attacks · Honey Pot · Machine Learning · Clustering Algorithms · Attacker Profiling.

1 Introduction

The username password combination is one of the primary methods of authentication in most of the organizations portals. Many methods such as the man in the middle attack[3], DNS spoofing [6], and phishing attacks[16] are used to obtain username password combinations. All of these activities are examples of penetration attacks as they allow an attacker to intercept the connection and make them believe that they are on the right website.[1] In the aforementioned approaches, the user is fooled into giving their access credentials. Here, we analyze another type of attack, known as a brute force attack. In this approach, the attacker attempts to guess the username and password with the help of tools that make use of dictionaries of a username and password combinations. This approach leads to an increase in load on the server, which in turn block the actual user from logging in, this is an example of a denial of service attack. In the scenario in which, such an attack is distributed, it is an example of a distributed denial of service attack. [7, 5, 13]

In this paper, we make use of Kippo honeypot[4, 10], which helps us log brute force attacks and help us understand the behavior patterns of the hacker. The hacker attempts to gain access with the help of a Secure Shell session. Here, we have made use of the data obtained from a honey pot deployed within the Information Security Lab of BITS Pilani, Hyderabad Campus.[14, 17]

The primary reason for targeting SSH sessions is due to the fact that a significant number of servers are not well maintained and often make use of weak credentials which make a perfect target for malicious agents.[12] A preliminary analysis of credentials and passwords on SSH remote login servers from securehoney.net gave the following results:

Table 1. Most common SSH Usernames and Passwords.

Username	Frequency	Password	Frequency
root	89%	123456	41%
test	6%	admin	19%
user	2%	password	11%
admin	2%	root	15%

The primary motive of our research is to find out how data with respect to login credentials propagates[15], once a hacker has been successful in obtaining access to an SSH server. Fig.1 shows how successful attacks on the honey tend to be clustered around certain locations.[9]

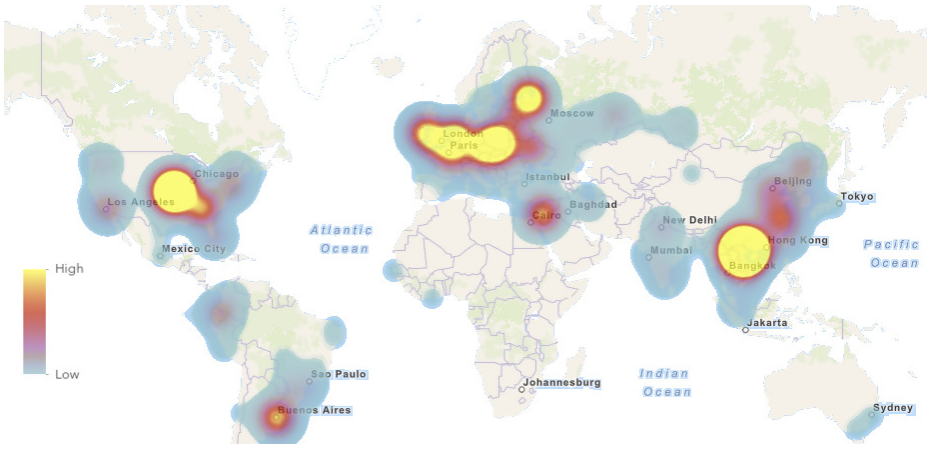

Fig. 1. From the above heatmap, we can see that most of the successful attacks seem to be stemming from North America, Europe, and Southeast Asia.

We also have an image that shows us a zoomed-in perspective in China, from which the majority of the attacks had originally originated. As we can see from the image it appears as if all the attacks appear in pockets, which lends some preliminary support to the hypothesis that data of the credentials appears to spread in the vicinity of the original successful attempt. In the remainder of the paper, we make use of a variety of clustering methods to catch patterns that may escape the human eye.

2 Related Work

Babak Nabiyev in his work on the application of Clustering Techniques for the detection of DDoS attacks had made use of the KDD CUP 99 dataset which had been developed by DARPA. He attempted to differentiate between Normal

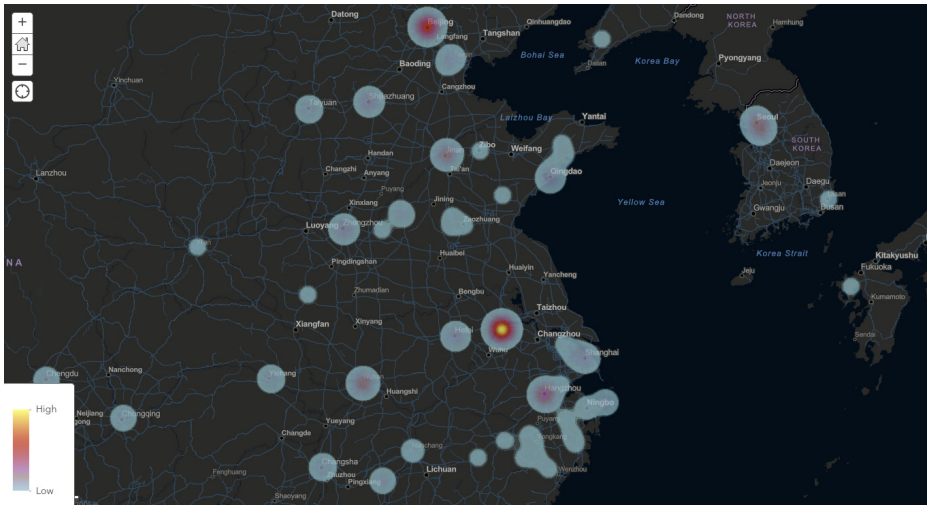

Fig. 2. Distribution of Login Attempts from China.

Traffic and DDoS traffic with the help of K-Means and EM Clustering techniques. He had clubbed together six cases of DoS attacks as a single type and he defined normal traffic flow to be the other type of behavior. Consquently, he made use of these two classes for the final clustering analysis.[8]

Shi Zhong also had made use of different clustering techniques for intrusion detection. In addition, he had also made use of the DARPA intrusion detection project for his dataset. Furthermore, he had done a comparative study on different clustering algorithms for intrusion detection, in which he concluded that unsupervised clustering algorithms performed better than supervised learning methods. Out of all the clustering algorithms, his proposed self-labeling heuristic performed the best with an overall accuracy of 93.6 %. [19]

Nikolskaia Kseniia analyzed IP traffic with the help of clustering on IP packet headers. He considered multiple parameters such as the classification parameters based on packet and transmission properties, choice of clustering methods and the number of clusters. He concluded that real-time data is too complex to dynamically change features or clustering algorithms. A hybrid neural network approach showed the best results with about 95% correctness. [11]

Jie Wang argues that clustering algorithms may not work very properly for intrusion detection because the similarity level of data points cannot be controlled. He proposes a two seed expanding algorithm that splits the attacks into different phases. The preprocessing includes creating a network flow and changing continuous-valued features to binary features. Based on these features, the algorithm selects seeds until all flows are divided into clusters. Their experiments show that two seed expanding algorithm performs better than the k -means and other clustering methods. [18]

Geoff Boeing used k-means clustering and dbscan techniques to cluster 1759 points of latitude and longitude data and they were reduced to 138 points and obtained 92% compression, without losing out on the key features of the information that had been spatially represented within the dataset.[2]

3 Research Framework

Experimental Setup We have deployed honey pots with the distributed architecture as shown in Fig. 3

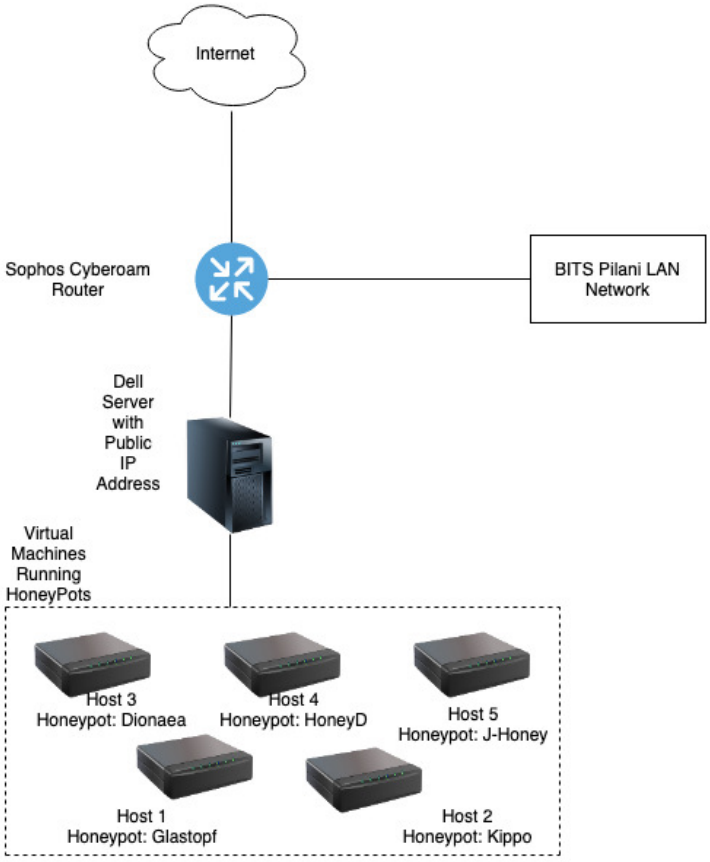

Fig. 3. The Honey Pot Architecture which was used For the D-DoS Attack .

The hypervisor runs five virtual machines, each of which runs a mini-Ubuntu 16.04. Each instance, in turn, runs a different honeypot. The traffic to the virtual machines is controlled with the help of a firewall and Network Address Translation(NAT) to assist us to communicate with the outside world. The server runs

within the Information Security Laboratory of BITS, Pilani-Hyderabad campus network. The server continuously monitors the activity that occurs on the public IP addresses.

Table 2. Spec table of the Honeypot used — Kippo.

Components	**Specs**
Processor	Intel Xeon
RAM	8GB
Hard Disk	400 GB
Operating System	Ubuntu 16.04

4 Analysis

4.1 Attackers origin

The origin of the attacker refers to the country or the city location from which the attack is being initiated. The source of their IP address help determines the location of the attacker. We made use of the urllib2 library to find the location of the attackers. However, IP addresses do not prove to be useful if the attacker makes use of a VPN or Tor Network. The results of the analysis have been mentioned in Table 3:

Table 3. Successful attempts city and country wise .

City	**Attempts**	**Country**	**Attempts**
Ho Chi Minh	3225	Vietnam	3586
Kansas City	1237	United States	1368
Radomsko	521	Poland	522
Saint Petersburg	306	Russia	354
Prague	251	Netherlands	326
Hanoi	193	China	323

We observe that there seem to be clusters of activity followed by patches of inactivity as seen in fig 4. Here, we observe there as spikes of activity in the second week and the last week of June as well as the second week of July as well as the end of October and the beginning of November. On the other hand, there seem to be very less attacks initiated in the months of August and September and hence they were not accommodated in the graph.

4.2 Traffic Analysis

We had segmented the data into files of 1MB size and had a total of 250MB data. The configuration had allowed at most 21 attempts from a particular IP before the IP was banned. Total 870 usernames and 9027 unique passwords were attempted.

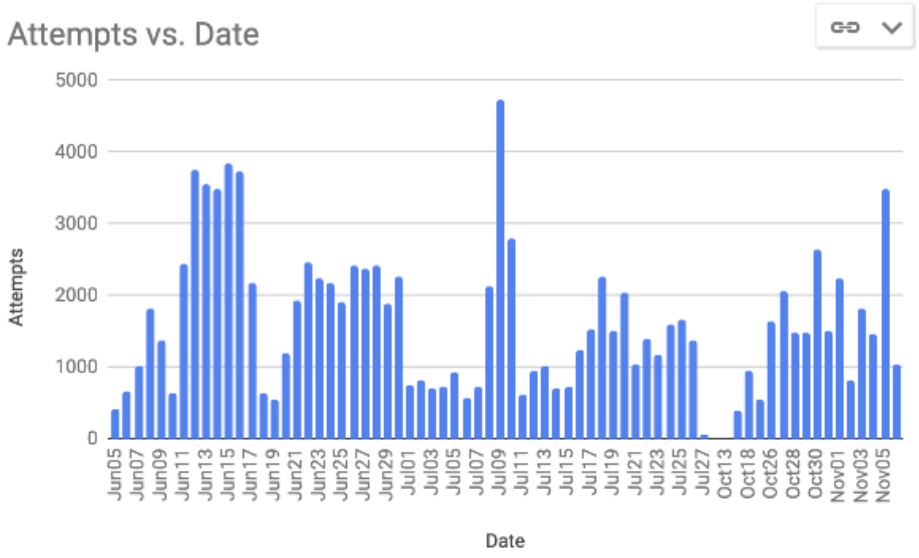

Fig. 4. Attempts Distribution over 6 months

Table 4. Most popular Passwords and Number of Attempts

Username	Counts	Username	Counts
root	190791	1234	1033
admin	27161	guest	838
ubnt	4056	test	816
support	3597	usuario	740
user	2533	pi	730

Table 5. Most popular Passwords and Number of Attempts

Password	Attempts	Password	Attempts
admin	13802	12345	2285
ubnt	4653	123456	2146
1234	4508	user	1962
support	3179	default	1690
password	2707	admin123	1341

The most attempted username was "root" and the most attempted password was "admin". In addition to the popular combination of *'root'* and *'admin'* we also get to see that the attackers tried other popular default passwords such as ubnt (as we made use of the Ubuntu operating system) as well as 1234, support and password. Furthermore, the hackers had also made use of popular usernames such as admin, user and guest. This analysis shows something as simple as setting a strong username password combination can reduce the number of successful breaches in security. Finally, we observe that an overwhelming majority of attacks on the distributed honeypot system appear to be coming from China.

4.3 Machine Learning Analysis

On this data, we have made use of three clustering methods which has helped us gain insight on the attacker's profile after obtaining access to the system. Here,

Table 6. Two Day of Interactions for the Ho Chi Minh City, Vietnam on 26th Juneand 27thJune, 2018 — Obtained by 2 gram Clustering Approach

IP	**Attempts**	**City**	**Country**
116.31.116.20	20350	Guangzhou	China
58.218.198.147	18817	Nanjing	China
58.218.198.153	7478	Nanjing	China
103.207.36.213	4545	Ho Chi Minh	Vietnam
58.218.198.167	2590	Jiangsu	China
91.211.1.100	2161	Vabalninkas	Lithuania
58.218.198.170	1969	Nanjing	China
31.207.47.50	1653	Amsterdam	Netherlands
116.31.116.21	1640	Guangzhou	China
58.218.198.172	1542	Nanjing	China

we have pooled the data in a manner that is similar to that used within n-gram models of Natural language processing. Thus, the data comes in three forms-

- Single day data
- Two days at a time
- Three days at a time

We have made use of 3 different clustering algorithms namely mean shift clustering, GMM Clustering and Kmeans clustering to gain a better insight on the information presented through the data. From the figures 5,6 and 7 we observe that most of the attacks seem to be concentrated only in certain parts of the world. This means that the information gained by the attacker seems to be spreading only to the vicinity to the earliest attack, rather than spreading randomly over the world.

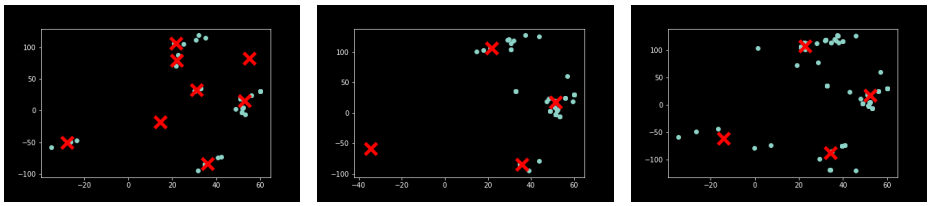

Fig. 5. Mean Shift Clustering (a) 1 gram (b) 2 gram (c) 3 gram

All three techniques seem to give us the **similar results**-

- All techniques give cluster centers which are very close to one another.
- The cluster centers obtained are similar across 1 gram, 2 gram and 3 gram

On the other hand there seem to be some **key differences**-

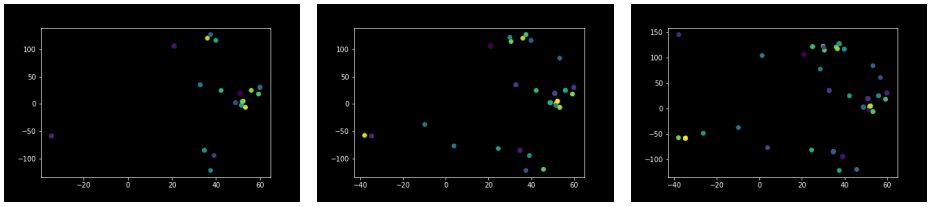

Fig. 6. GMM Clustering (a) 1 gram (b) 2 gram (c) 3 gram

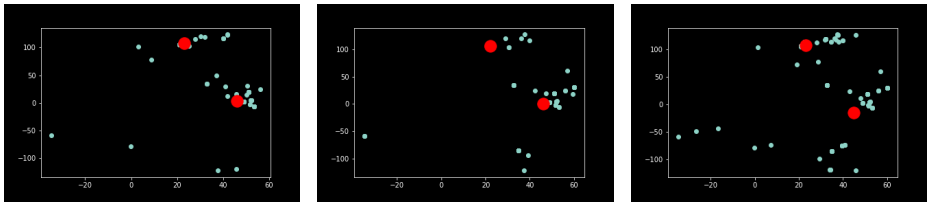

Fig. 7. Kmeans Clustering (a) 1 gram (b) 2 gram (c) 3 gram

- The mean shift algorithm appears to be more susceptible to outliers, which causes it to detect a greater number of clusters.
- On the other hand, the algorithm behaves better when we increase the number of data points as in the case of 2 gram and 3 gram.

To better understand why the clustering algorithms have singled out these locations, we have probed the data from 1 gram, 2 gram and 3 gram on specific geographic locations so as to search for patterns that could help us better understand how the attack seems to propogate.

Table 7. One Day of Interaction for the Date 27th October,2018 from China on - Obtained from the 1 gram clustering approach

Time	**IP**	**CIty**	**Country**	**Time**	**IP**	**CIty**	**Country**
13:45:41+0530	60.182.212.131	Jinhua	China	13:58:45+0530	112.236.177.74	Qingdao	China
13:46:03+0530	60.255.146.181	Chengdu	China	14:04:46+0530	125.92.182.50	Shiqi	China
13:46:11+0530	110.184.170.247	Zhongba	China	14:05:30+0530	121.14.7.244	Guangzhou	China
13:49:10+0530	182.44.84.228	Jinan	China	14:06:51+0530	110.249.217.82	Xingfeng	China
13:52:27+0530	210.51.191.26	Beijing	China	14:07:03+0530	58.218.198.147	Nanjing	China
13:52:53+0530	58.48.178.200	Shuiguo	China	14:07:52+0530	218.60.136.106	Chaoyang	China
13:54:21+0530	60.185.214.42	Zhoushan	China	14:08:52+0530	111.121.192.6	Guiyang	China
13:54:49+0530	222.47.26.139	Hangzhou	China	14:10:41+0530	153.34.109.60	Chaowai	China
13:55:29+0530	124.243.216.102	Beijing	China	14:14:27+0530	122.190.252.82	Xiangfan	China
13:58:08+0530	218.108.124.26	Hangzhou	China	14:15:32+0530	113.122.34.247	Jinan	China
13:58:11+0530	113.122.5.6	Jinan	China	14:19:16+0530	113.206.115.125	Beiwenquan	China
13:58:11+0530	210.51.191.26	Beijing	China	14:23:03+0530	123.149.128.181	Henan	China

In the 1 gram analysis for table 7, we observe that all the successful attacks have appeared to have taken place one after another after short intervals of time. In addition, we can see that once an attacker gains access, it seems like the others in the vicinity gain access after a short interval of time.

In Table 8, we observe the following observation. The set of IP addresses that make a successful attempt on the first day are the same as those which are obtained on the following day. However, we notice that now there is a new IP from the same location that is now able to successfully gain access to the honeypot. This means either the attacker has gained access to a new IP or another attacker has received information about the same from another attacker in the same geolocation.

Table 8. Two Day of Interactions for the Ho Chi Minh City, Vietnam on 26th June and 27th June, 2018 — Obtained by 2 gram Clustering Approach

Date	**IP**	**Count**	**Date**	**IP**	**Count**
2018-06-26	142.54.189.114	90	2018-06-27	142.54.189.114	104
2018-06-26	173.208.187.66	2	2018-06-27	192.187.103.2	223
2018-06-26	192.187.103.2	204	2018-06-27	192.69.95.132	4
2018-06-26	69.197.135.10	23	2018-06-27	69.197.135.10	15

Table 9. 3 Days of Interactions for the country of Vietnam from 6th June to 8th June 2018 — Obtained by 3 gram Clustering Approach

Date	**IP**	**Count**	**Date**	**IP**	**Count**	**Date**	**IP**	**Count**
2018-06-06	103.207.36.117	1	2018-06-06	116.98.0.212	1	2018-06-07	116.103.77.175	2
2018-06-06	103.207.36.9	2	2018-06-06	117.3.47.59	2	2018-06-07	116.105.225.86	2
2018-06-06	103.207.37.239	4	2018-06-06	117.5.195.121	1	2018-06-07	117.3.47.59	1
2018-06-06	103.207.39.43	3	2018-06-06	123.16.32.196	3	2018-06-07	125.212.226.227	1
2018-06-06	103.207.39.54	1	2018-06-06	123.19.170.93	1	2018-06-07	14.176.232.175	5
2018-06-06	103.79.141.153	2	2018-06-06	14.167.67.203	1	2018-06-07	27.70.150.55	1
2018-06-06	103.79.141.39	1	2018-06-06	14.176.232.175	3	2018-06-07	58.186.98.43	1
2018-06-06	103.79.143.136	6	2018-06-06	27.78.21.103	2	2018-06-08	103.207.39.159	2
2018-06-06	103.89.88.11	9	2018-06-06	42.118.152.107	1	2018-06-08	103.79.141.153	1
2018-06-06	113.170.210.40	1	2018-06-07	103.207.37.239	4	2018-06-08	103.89.88.11	9
2018-06-06	113.22.152.202	2	2018-06-07	103.207.39.228	1	2018-06-08	116.103.147.230	6
2018-06-06	116.104.79.5	1	2018-06-07	103.207.39.43	2	2018-06-08	116.98.44.241	1
2018-06-06	116.105.225.86	4	2018-06-07	103.79.141.153	2	2018-06-08	14.176.232.175	4
2018-06-06	116.110.160.11	2	2018-06-07	103.79.143.136	4	2018-06-08	27.70.151.209	2
2018-06-06	116.97.24.95	1	2018-06-07	103.89.88.11	9	2018-06-08	27.78.21.103	2

In Table 9, the pattern in the data obtained from the 3 gram analysis further strengthens the observations that we had made in the case of 2 gram. Here, we can clearly observe that the same set of IP addresses make attack in regular intervals of time. In addition, to those we see additional IP addresses which orig-

inate from the same or nearby locations which gives weight to the argument that the information about the credentials is spreading to the geographical vicinity.

5 Conclusion

We would like to draw the conclusion that attacks appear to be concentrated in certain regions. Furthermore, it appears as if the data with respect to the access credentials does not seem to spread randomly rather, it appears as if the success with respect to successful attacks seems to spread in the near vicinity of the first attack.

References

1. Bacudio, A., Yuan, X., Chu, B., Jones, M.: An overview of penetration testing. International Journal of Network Security Its Applications **3**, 19–38 (11 2011). https://doi.org/10.5121/ijnsa.2011.3602
2. Boeing, G.: Clustering to reduce spatial data set size. arXiv preprint arXiv:1803.08101 (2018)
3. Callegati, F., Cerroni, W., Ramilli, M.: Man-in-the-middle attack to the https protocol. IEEE Security & Privacy **7**(1), 78–81 (2009)
4. Doubleday, H., Maglaras, L., Janicke, H.: Ssh honeypot: Building, deploying and analysis. International Journal of Advanced Computer Science and Applications **7** (05 2016). https://doi.org/10.14569/IJACSA.2016.070518
5. Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D.: Statistical approaches to ddos attack detection and response. In: Proceedings DARPA information survivability conference and exposition. vol. 1, pp. 303–314. IEEE (2003)
6. Klein, A., Golan, Z.: System and method for detecting and mitigating dns spoofing trojans (Sep 11 2012), uS Patent 8,266,295
7. Mirkovic, J., Reiher, P.: A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Computer Communication Review **34**(2), 39–53 (2004)
8. Nabiyev, B.: Application of clustering methods network traffic for detecting ddos attacks. Problems of Information Technology **09**, 98–107 (01 2018). https://doi.org/10.25045/jpit.v09.i1.11
9. Najafabadi, M.M., Khoshgoftaar, T.M., Kemp, C., Seliya, N., Zuech, R.: Machine learning for detecting brute force attacks at the network level. In: 2014 IEEE International Conference on Bioinformatics and Bioengineering. pp. 379–385. IEEE (2014)
10. Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C., Schönfelder, J.: A survey on honeypot software and data analysis. arXiv preprint arXiv:1608.06249 (2016)
11. Nikolskaia, K.: Network attacks detection based on cluster analysis (10 2017)
12. Owens, J., Matthews, J.: A study of passwords and methods used in brute-force ssh attacks (2008)
13. Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A., Zamboni, D.: Analysis of a denial of service attack on tcp. In: Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097). pp. 208–223. IEEE (1997)
14. Sochor, T., Zuzcak, M.: Study of internet threats and attack methods using honeypots and honeynets. In: International Conference on Computer Networks. pp. 118–127. Springer (2014)

15. Tatlı, E.: Cracking more password hashes with patterns. IEEE Transactions on Information Forensics and Security **10**, 1–1 (08 2015). https://doi.org/10.1109/TIFS.2015.2422259
16. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., Bursztein, E. (eds.): Data breaches, phishing, or malware? Understanding the risks of stolen credentials (2017)
17. Valli, C., Rabadia, P., Woodward, A.: Patterns and patter-an investigation into ssh activity using kippo honeypots (2013)
18. Wang, J., Yang, L., Wu, J., Abawajy, J.H.: Clustering analysis for malicious network traffic. In: 2017 IEEE International Conference on Communications (ICC). pp. 1–6. IEEE (2017)
19. Zhong, S., Khoshgoftaar, T.M., Seliya, N.: Clustering-based network intrusion detection. International Journal of reliability, Quality and safety Engineering **14**(02), 169–187 (2007)