



Protecting Databases From Brute Force Attacks

**2021
COMPUTER ENGINEER
GRADUATION PROJECT THESIS**

Onur SALTAŞ

Dr. Aslan KANAMGOTOV

Protecting Databases From Brute Force Attacks

Onur Saltaş

**Karabük University
Engineering Faculty
Department of Computer Engineering
Graduation Project Thesis
Prepared as.**

KARABÜK

June 2021

I confirm that this project titled "Protecting Databases From Brute Force Attacks" prepared by Onur SALTAT is suitable as a Graduation Project Thesis.

Doç. Dr. ASLAN KANAMGOTOV

.....

Graduation Project Consultant, Department of Computer Engineering

...../...../2021

Computer Engineering department has approved the Graduation Project Thesis with this thesis.

Prof. Dr. Mehmet AKBABA

.....

Bölüm Başkanı

“All the information in this project was obtained and presented in accordance with academic rules and ethical principles; I also declare that I have made all references not originating from this work, as required by these rules and principles..”

Onur SALTAŞ

ABSTRACT

Graduation Project Thesis

Protecting Databases From Brute Force Attacks

Onur SALTAŞ

Karabük University

Engineering Faculty

Department of Computer Engineering

.

Project Supervisor:

Doç. Dr. ASLAN KANAMGOTOV

June 2021, 44 page

Brute force attack is a method used to find information such as user password. In any brute force attack, it is an automatic and sequential attempt to unknown password or username. As an example of a brute force attack, we can state that it is known as a dictionary attack that can try all words in the dictionary created after the information gathering stage. Another other brute force attacks can be attempted by converting commonly used passwords or combinations of letters and numbers into a dictionary. well researched in terms of time and resources, a poorly crafted dictionary attack can cost time and money. For this reason, success in brute force attacks usually depends on the computational power and the good dictionary tried, rather than a good algorithm. In this study, how brute force attacks are done, how they are protected, how they are made, process improvements will be proposed on the relationship with tools and databases..

Key Words: Brute Force, Dictionary attack.

ACKNOWLEDGMENT

I have benefited from his deep knowledge and experience, and whose interest and support I have made use of in the planning, research, execution and formation of this thesis study. I would like to express my endless thanks to my esteemed professor ASLAN KANAMGOTOV, who helped me with his guidance and informations in the light of scientific foundations.

CONTENTS

	<u>Page</u>
APPROVAL.....	ii
ABSTRACT.....	Error! Bookmark not defined.
ACKNOWLEDGMENT.....	Error! Bookmark not defined.
CONTENT	Error! Bookmark not defined.
FIGURES INDEX.....	Error! Bookmark not defined.i
CHAPTER 1	Error! Bookmark not defined.
INTRODUCTION	Error! Bookmark not defined.
1.1. LITERATURE VIEW	1
1.2. RESEARCH PROPOSAL.....	3
1.3. PURPOSE	4
1.4. GOAL AND OBJECTIVES.....	Error! Bookmark not defined.
1.5. METHODOLOGY	5
1.5.1. Password Requirements.....	5
1.5.2. Informaction Collection.....	5
1.5.3. Brute Force Tools	6
1.5.4. Database Protection Simulation.....	6
CHAPTER 2	8
2.1. PASSWORD REQUIREMENT.....	Error! Bookmark not defined.
2.1.1. Symmetric Encryption	8
2.1.1.1. Data Encryption	9
2.1.1.2. Advanced Encrytion.....	Error! Bookmark not defined.
2.1.1.3.International Data Encryption Algorithm	Error! Bookmark not defined.
2.1.1.4. Blowfish.....	Error! Bookmark not defined.
2.1.2. Asymmetric Encryption	13
2.1.2.1. Diffie-Helman	13
2.1.2.2. Elliptic Curve Encryption	Error! Bookmark not defined.

2.1.1.3.Rivest-Shamir-Adleman	Error! Bookmark not defined.
	<u>Page</u>
2.1. INFORMATION COLLECTION	15
2.1.1. Active Data Collection	15
2.2.1.1. Nmap.....	16
2.2.1.2. Masscan	16
2.2.1.3. Nslookup	Error! Bookmark not defined.
2.2.1.4. Maltego	Error! Bookmark not defined.
2.2.2. Passive Data Collection	18
2.2.2.1. Whois	18
2.2.2.2. TheHarvester	Error! Bookmark not defined.
2.2.2.3. Netcraft	20
2.3. BRUTE FORCE TOOLS	21
2.3.1. Aircrack-ng	21
2.3.2. John The Ripper.....	22
2.3.3. RainbowCrack	23
2.3.4. Hashcat	23
2.3.5. Ncrack.....	24
2.3.6. Hydra	25
2.4.DATABASE PROTECTION SIMULATES	26
2.4.1. Brute Force Tool.....	24
2.4.2. Catch And Block.....	25
FINAL	30
REFERENCES.....	31
RESUME	32

FIGURE INDEX

	<u>Page</u>
2.1. Data Encrytion Standard Diagram.	9
2.2. Advanced Encrytion Standard Diagram.....	10
2.3. International Data Encryption Algorithm Diagram.	11
2.4. Blowfish Diagram.	12
2.5. Diffie-Helman Diagram.	Error! Bookmark not defined.
2.6. Elliptic Curve ECC Diagram.	Error! Bookmark not defined.
2.7. Rivest-Shamir-Adleman Diegram.....	Error! Bookmark not defined.
2.8. Nmap	16
2.9. Masscan	16
2.10. Whois	18
2.11. TheHarvester	19
2.12. Netcraft	19
2.13. Aircrack-ng	20
2.14. John The Ripper	21
2.15. Rainbowcrack	22
2.16. Hashcat	22
2.17. Ncrack	23
2.18. Hydra	24
2.19. Brute Force Tool.	25
2.20. Log File Viewer.	26
2.21. Login Audting.	26
2.22. Making Format.....	27
2.23. Sent Mail.	28
2.24. For Send Mail.....	28
2.25. Job Schedule.	28
2.26. Trigger.....	29

CHAPTER 1

INTRODUCTION

1.1. LITARATURE REWIEW

In recent years, brute force has come to an important position for cyber security. Every day, everyone started using technology and both positive and negative aspects started to emerge. Some people have forgotten their security while using all these technologies, some create a 10-digit password, while others create these passwords from a single 4-digit letter, with this project, we can protect their information consciously. As technology developed, the importance of data increased. This project is an awareness project. As the general purpose of the project, we will learn the answers to questions such as what is a brute force attack, how to do a brute force attack, how to protect from brute force attacks, how to keep our databases away from such attacks. Brute force main purpose is to try password on login page to access this data. Different methods have been developed to evaluate the brute force architecture. In [1] Goodchild stated, the subjects of Remote working due to the pandemic process and the effect of brute force on it are discussed. It has been explained that by disabling RDP on the Internet, using an additional authentication layer such as MFA or 2FA, it can be protected by setting up a virtual private network (VPN) gateway to mediate all RDP connections from outside the Local network.[1]

In[2] Bryan stated, SPI Dynamics, the topics of What are Brute Force Attacks and how can you prevent them are discussed. The following method was used to prevent: Incremental Delay. The Incremental Delay strategy can be summarized as follows; It is stated that preventing any brute force attack is a very good strategy, and this is explained as follows: It is the gradual delay of the page response after unsuccessful login attempts so the attacker waits for a while. While a normal brute force attack can try 50 passwords per second, this method can attempt far fewer passwords and saves the user time to check their account. [2]

In[3] ATT stated ,specifically discusses how individual users and businesses can use passwords to improve their cybersecurity. We have been told that by using two-factor authentication, we can take the necessary precautions by entering after making. sure that https is at the beginning of a website's URL, never sending passwords via email. [3]

In[4] Pavitra stated, Brute force attack tools were discussed. Extensive information was given about Aircrack-ng, John the Ripper, Rainbow Crack, L0phtCrack, Ophcrack, Hashcat, DaveGrohl, Ncrack, THC Hydra.[4]

In[5] Vladimir stated, Research has been done on Brute-Force attacks by strike pattern and. Username-password pairs are used for roles assigned by the administration: admin, user, etc. It doesn't need to be generically or semantically linked. First names or surnames can also be used, the second part is more useful than the first. Alphanumeric characters can be added to power the Password-Reliant Bfa . [5]

In[6] Darren stated, there was a research on online and offline brute force. As a result, it has been determined that you leave a trace in every attempt in online attacks. Therefore, it has been stated that it is necessary to be careful in online attacks. In offline attacks, there is a need for an information gathering stage because it is necessary to attack with files. This stage of knowledge may be the address where he lives, the name of the animal. These results are among the results obtained. [6]

In[7] James stated, a research has been made for the subject of Common Usernames and Passwords and the results are shared as follows: Commonly used usernames are usually used, such as test, guest or user, and passwords such as 123 password are used for the password, and this is a huge disadvantage. A few detailed analysis results are as follows: root 20.0, admin 1.7, test 1.4, guest 0.7 for username [7]

In[8] Sowmya stated, Some methods have been explored to help prevent brute force attacks. Therefore, with this research, it was aimed to work harder for the attackers. As a result, results such as Lockig of Accounts, Time bound login, Using CAPTCHA, Unique IP address Login, One time password authentication were obtained.[8]

In[9] Stephen stated, The purpose of the article is to create cyber attacks on databases. While creating this, the result was reached by following the steps such as How and Why, Detection, Prevention Targeted Attack. As a result of their research on database discovery techniques, which are part of their research, it was stated that they used this technique actively and passively. It has been shown that discovery is made by uploading it to DBA machines and scanning the internal network in oracle databases with nmap.[9]

In[10] Raşit stated, Database architecture, database performance improvement, database security issues have been investigated in the thesis. Tns (Transparent Network Substrate) is a network technology owned by Oracle. It supports p2p connections over protocols such as Tcp / Ip and sdp. The main purpose of tns is to provide connection to Oracle databases.. It listens for network connections and is a proxy to forward their communications to the appropriate database or security descriptor. And the components of the tns listener such as Tnslnsr, Lsnrctl, Sqlnet.ora, Listener.ora, Tnsnames.ora are described. [10]

1.2. RESEARCH PROPOSAL

Since everything has its good and bad sides, the concept of the internet certainly gets its share in this regard. In today's world, there is a situation where the more can be won against time, the more positive it is. For this reason, since time is very important, we can save time thanks to the transactions we do on the internet. Since many business activities are performed over Internet, we have reduced physical and face-to-face activities, but even though the internet is safe, are institutions and streets secure enough? Our project, which is the subject of Brute Force's attack, emerges at this point. Brute Force attack is one of the negative scenarios and its solutions are a highly important problem. The basic logic of the Brute force attack, which was developed to access private information in the background of all kinds of personal and corporate accounts, is to access the private information of the target account by breaking passwords with the try-all logic. probabilities by trial and error. The brute

force attack can be used in many areas such as username and passwords of social platform users, computer user passwords, admin panel passwords.

1.3. PURPOSE

With the application to be developed with this project, it is aimed to protect the attacks against databases and to introduce the tools that make brute force more closely. It will be applied to these databases first and then it will be applied to other platforms.. We use databases everywhere to store expense files or data on websites in a company or marketplace This project will help you maintain a database you manage. This application will protect your database from brute force attacks or prevent you from losing money and prestige in the face of possible attacks. By identifying the hacked IP address and adding it to the blacklist and from that IP address it is aimed to never be attacked again. Before these, the brute force tools will be introduced closely and Finally, the above-mentioned brute force detection application will be made. That way, they can't steal your employees' data. The application developed with this project will be used by companies and daily internet users who keep a lot of information in their databases to protect their data against brute force attacks.In summary, the project will try to protect databases and introduce brute force tools.

1.4. GOAL AND OBJECTIVES

My long term goal for the project is to be able to integrate the brute force detection application with many applications. It is to reduce data loss as a result of attacks with Brute force. The importance of integrating brute force detection has a really big role nowadays because it helps to prevent any brute force attack. purpose of the application developed with the project is to continue to detect, record, prevent and report the attack.. This process is for a database, as a continuation of the project it will be integrated into many applications.

In summary, the purpose of the application developed at the end of the project;how they are made, how they can be protected, and by producing Brute force detection by going deeper.

1.5. METHODOLOGY

As explained, the project consists of four parts. In the first part, the subject of algorithms related to the password was examined. In the second part, brute force applications for collecting active and passive information were investigated. In the third part, applications that could apply brute force were discussed. In the last part, when an attack is made on the SQL server database, the problems of creating brute force application, rough detection, blocking, reporting are simulated.

1.5.1. Password Requirements

One way of protecting against brute force attacks is to make sure that passwords are long and meet the security requirements. Passwords are used to access many sites. These passwords must consist of at least 8 characters and contain uppercase and lowercase symbols. Issues such as how long the password should be used during the password validity period, how often it should be changed will be explained.

Cipher algorithms were investigated in sub-branches such as Symmetric Encryption Algorithms, Data Encrytion Standard, Advanced Encrytion Standard, International Data Encryption Algorithm, Blowfish , Asymmetric Encryption Algorithms, Diffie-Helman, Rivest-Shamir-Adleman, Keyless Algorithms.

1.5.2. Information Collections

Information collection is divided into two parts as passive and active collection. Personal information such as location, age,birthday etc. can be obtained. Passive collection is performed without any connection to the attacked party. Active

collection is done with a connection with the attacked party and the other party can understand that we collect information about us.

Nmap, Masscan, Nslookup, Maltego applications were used to collect active information. Whois, Search engines, TheHarvester, Netcraft applications were used to collect passive information.

1.5.3. Brute Force Tools

There are many methods to perform brute force attack. There are many ready-made applications installed in Kali Linux operating system. While examining these tools, I searched for a few attributes. First of all, I searched for speed, as a result, using the faster one, the target can be reached faster. Then a study was conducted on its scope. The scope is very important in this regard, while some tools can attack on a limited part, some tools can be extensively attacked in many areas. Additionally, it was explored for usability. The applications examined at this stage are below.

Aircrack-ng, John the Ripper, Rainbow Crack, Hashcat, Ncrack, THC Hydra applications were discussed for brute force.

After giving information about the tools, the correct tool can be selected easily in case of any problem. In addition, a tool can be selected here for the application to be made with the project

1.5.4. Database Protection Simulation

In order to protect the SQL database, comprehensive information will be given about the databases. Sometimes the attacker may be someone working inside. A brute force attack on the local network occurs very quickly. As a simulation, a brute force tool will be used in windows installed on the virtual computer. This simulation will be done on the SQL server. There are applications that can make a brute force attack or anyone can write the brute force tool with many programming languages.

A tool will be made on Windows Forms App in .Net. Thus, this tool can be used in the project and in simulation.

Reporting, capturing and mailing application will be written with SQL codes to be written over the SQL server.

This simulation will also perform the steps of accessing the database with brute force, adding and deleting users. These will be presented step by step in a report as it can be seen in the simulation. The entry and result of each step will be specified in the report.

CHAPTER 2

2.1. PASSWORD REQUIREMENT

Encryption means converting data into an encrypted format. Thus, only the users you want can access the information. Cryptographic keys are combined with many mathematical operations and made possible. In this section, it will give information about encryption types under two titles: Symmetric and Asymmetric, and some information about the most commonly used encryption algorithms will be given.

2.1.1. Symetric Encryption

The same key is used to encrypt and decrypt a document. The algorithm itself is not kept secret, and the owner and recipient of the message must have backups of the secret key in a secure area. Using the same key is one of the major disadvantages of symmetric key encryption, because if anyone can obtain the key, it can decrypt your data.

2.1.1.1. Data Encryption

The DES data encryption standard is one of the best algorithms of the modern encryption era. In 1976, DES was approved as a cryptographic standard and published in FIPS. DES has recently been deemed unsafe. DES and double DES are no longer preferred, but triple DES with three keys is still the proposed algorithm. 3DES, also known as TDEA (triple data encryption algorithm), is an updated model of the DES algorithm. 3DES is an algorithm developed to overcome the shortcomings of the DES algorithm. DES is much slower than the AES algorithm, but is still used in electronic payments.

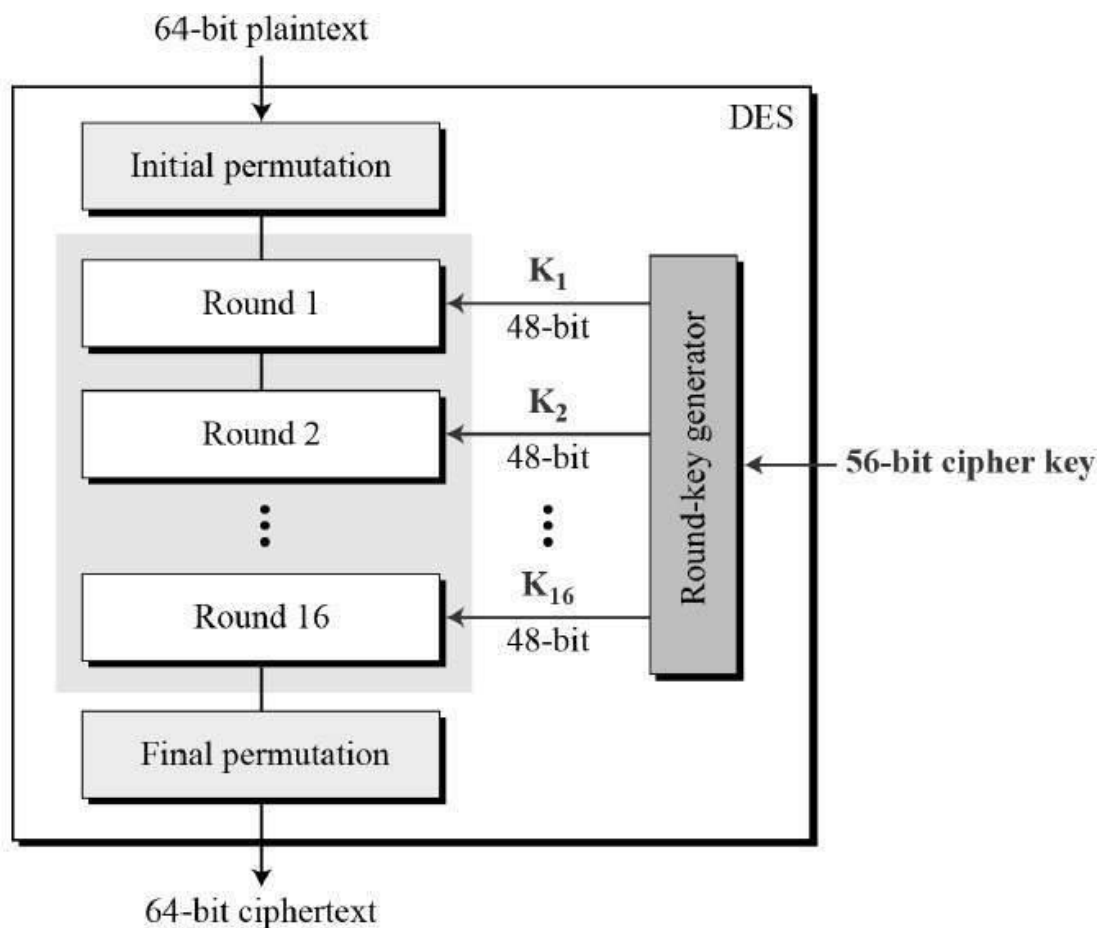


Figure 2.1. Data Encryption Standard Diagram

2.1.1.2. Advanced Encryption Standard

AES (advanced encryption system), also used as Rijndael, is one of the most used encryption algorithms. It was developed in addition to DES and became the new encryption standard after NIST was approved in 2001. AES is a block cipher standard with different key lengths and different block sizes. AES first unencrypted data is created in blocks. The next step is encryption using a key. During the encryption process, many operations such as row shifting, column mixing and key insertion can be applied. Depending on the length of the key, there may be 10, 12 or 14 such conversions. As the advantage of using the AES encryption algorithm, it can be said that AES is secure, fast and flexible. AES is much faster than DES. Variants with different key lengths are the most important feature, so the length of the keys makes them harder to break.

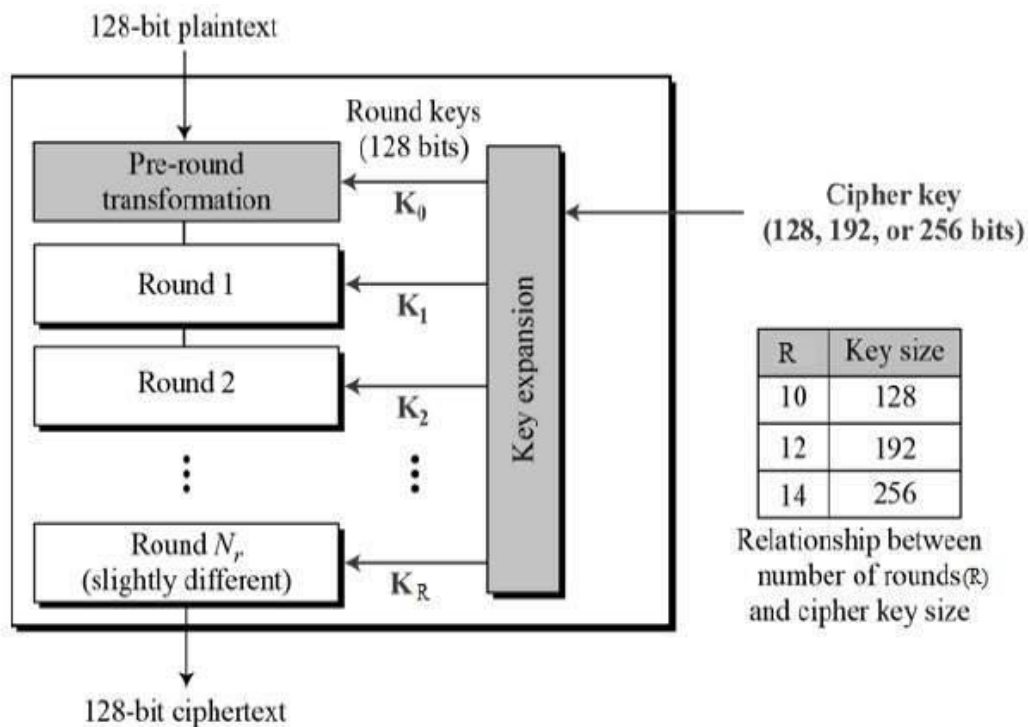
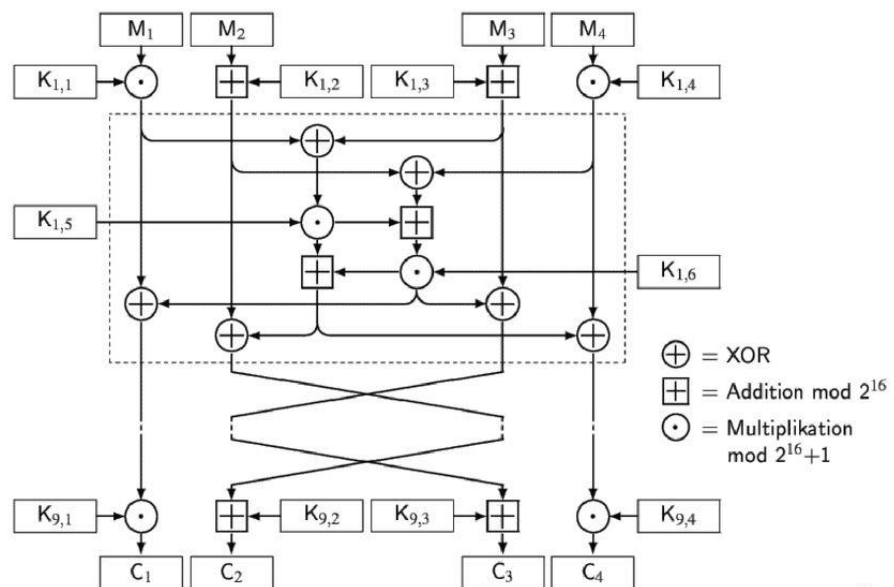


Figure 2.2. Advanced Encryption Standard Diagram

2.1.1.3. International Data Encryption

The International Data Encryption Algorithm (IDEA), originally called the Enhanced Recommended Encryption Standard (IPES), is a part of the Recommended Encryption Standard (PES), which is intended to be used instead of DES. It is not widely used recently. It also has no patent yet. Free to use but as a brand name. It is still a trademark. It worked on a 64-bit block using a 128-bit key and is still an optional algorithm in the OpenPGP standard.

IDEA – Block Diagram



5

Figure 2.3. International Data Encryption Algorithm Diagram

2.1.1.4. Blowfish

Blowfish has a 64-bit variable key block cipher. The algorithm consists of two parts, these can be said as key distribution and data encryption. For key expansion, it

converts a key up to 448 bits long into multiple subkey sequences for a total of 4168 bytes. Data encryption occurs in a simple process performed 16 times in sequence. Each stage consists of permutation bound to a key and permutation bound to a key and data. Only inclusions and XORs of 32-bit words are used. The only additional operations at each stage are four data extracts from the indexed array. Blowfish uses many subkeys. These subkeys must be calculated before attempting to encrypt or decrypt data.

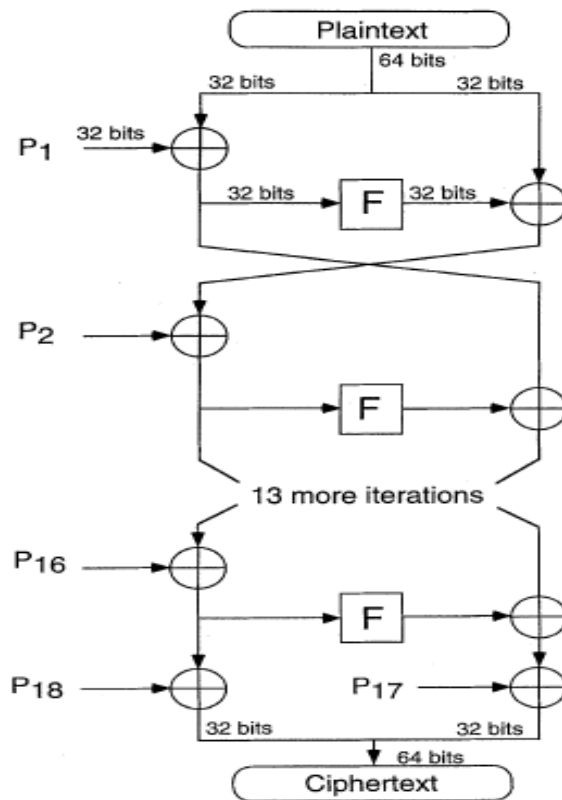


Figure 2.4. Blowfish Diagram

2.1.2. Asymmetric Encryption Algorithms

The same key is used to encrypt and decrypt a document. The algorithm itself is not kept secret, and the owner and recipient of the message must have backups of the secret key in a secure area. Using the same key is one of the major disadvantages of symmetric key encryption, because if anyone can obtain the key, it can decrypt your data.

2.1.2.1. Diffie-Hellman

Diffie-Hellman is one of the first recorded examples of asymmetric cryptography. Traditionally, for a secure encrypted conversation, both parties must first exchange keys with private secure physical channels. Diffie-Hellman has completely eliminated the need for secure exchange, thanks to an additional key, the public key. Diffie-Hellman is no longer used as a standard encryption algorithm, as it can be detected to be vulnerable to many attacks.

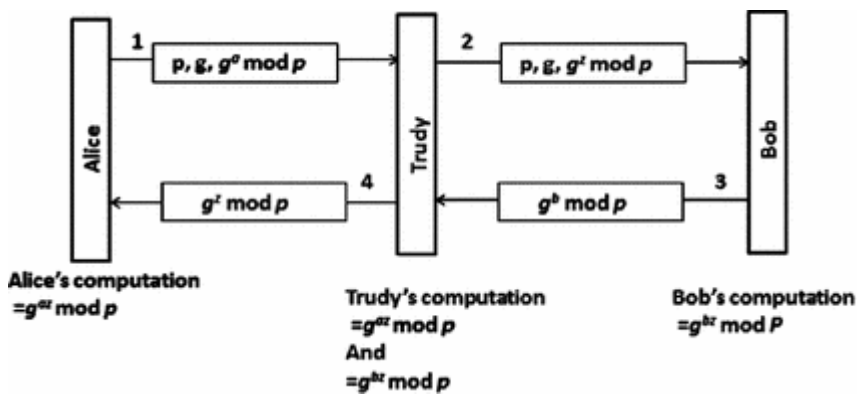


Figure 2.5. Diffie-Hellman Diagram

2.1.2.2. Elliptic Curve ECC

ECC stands for Elliptic Curve Encryption. Cryptographic algorithms are often used in mathematical operations to decrypt keys. SSL / TLS certificates often use RSA keys, and the size required for the bunkar increases very often to keep sufficient encryption strength stable. A standard similar to RSA is ECC. Both types of keys share the same important property of asymmetric algorithms, one for encryption key and the other for decryption. However, ECC can offer the same level of encryption strength at much smaller key sizes, meaning it offers better security with less computing and storage capacity.

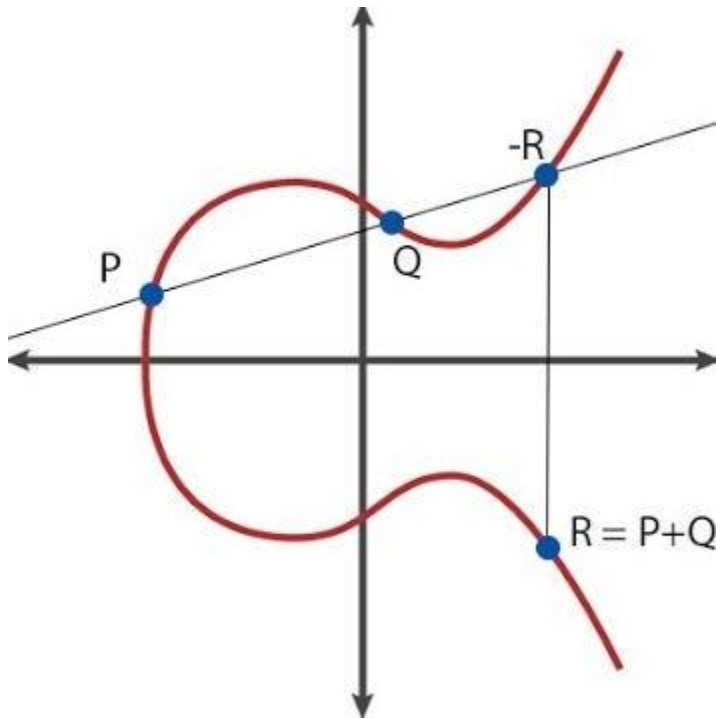


Figure 2.6. Elliptic Curve ECC Diagram

2.1.2.3. Rivest-Shamir-Adleman

Rivest-Shamir-Adleman algorithm, which is generally used as RSA, is the most frequently preferred asymmetric encryption standard of recent times. RSA uses prime factorization. RSA is generally a slow system, so it is used to encrypt and decrypt symmetric keys. These keys are also used to encrypt and decrypt messages. Symmetric switches do a lot of the work. RSA sets a reliable and secure standard.

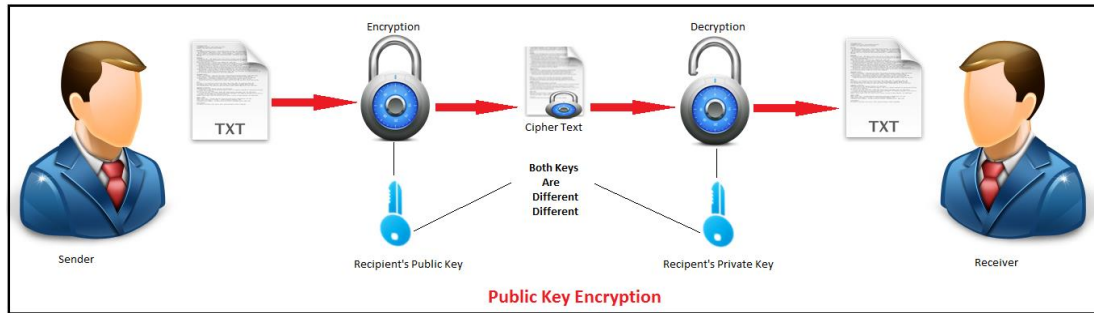


Figure 2.7. Rivest-Shamir-Adleman Diagram

2.2. INFORMATION COLLECTION

Active information gathering and passive information gathering methods can be used for information gathering.

2.1.1. Active Data Collection

It is the process of collecting information through direct communication with a source. First of all, because it is a direct action to the source, we get more logical and better results. Its disadvantage is that it leaves a trace as it is a direct contact. Very careful attention should be paid to the trace left. The source can find the person who performed this action with this trace.

2.2.1.1. Nmap

Network Mapper is a free tool used by system administrators to discover networks and check their security. Nmap is fast, comes with detailed documentation and graphical interface, supports data transfers, network inventory and more. It is a tool written to detect open ports in target systems, manage active services and present them as outputs. Information about software, operating system, physical device types, uptime, firewall, and network card information can be obtained from other sources connected to the target system's network.

```

Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

```

Figure 2.8. Nmap Help Table

2.2.1.2. Masscan

In general, it is preferred because it is very fast and it can scan the whole internet in less than 6 minutes by transmitting 10 million packets per second. Its syntax is very similar to nmap. Its disadvantage is that it can get erroneous results when examining wide port ranges because it is high speed.

```

-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p 111,137,80,139,8080
TIMING AND PERFORMANCE:
  --max-rate <number>: Send packets no faster than <number> per second
  --connection-timeout <number>: time in seconds a TCP connection will
    timeout while waiting for banner data from a port.
FIREWALL/IDS EVASION AND SPOOFING:
  -S/--source-ip <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
OUTPUT:
  --output-format <format>: Sets output to binary/list/json/grepable/xml
  --output-file <file>: Write scan results to file. If --output-format is
    not given default is xml
  -oL/-oJ/-oG/-oB/-oX <file>: Output scan in List/JSON/Grepable/Binary/XML format,
    respectively, to the given filename. Shortcut for
    --output-format <format> --output-file <file>
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
MISC:
  --send-eth: Send using raw ethernet frames (default)
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  masscan -v -sS 192.168.0.0/16 10.0.0.0/8 -p 80
  masscan 23.0.0.0/0 -p80 --banners -output-format binary --output-filename internet.scan
  masscan --open --banners --readscan internet.scan -oG internet_scan.grepable
SEE (https://github.com/robertdavidgraham/masscan) FOR MORE HELP

```

Figure 2.9. Masscan Help Table

2.2.1.3. Nslookup

Nslookup is an application that is used to collect information in DNS resource. In short, it collects information about the specified resource via the command line. Also known as part of the BIND Server suite. Also the nslookup tool works in two ways, known as interactive and non-interactive. Interactive mode can help you check name servers for information about many computers and their areas of influence, or print out source machines in a domain. Non-interactive mode allows the source machine to print the requested information.

2.2.1.4. Maltego

Maltego Kali comes free on Linux operating system. It is a tool that provides information about the target through browsers, social media memberships, e-mail accounts, etc. Many things such as e-mail address and social media account can be put. It has two versions as Commercial and Community version. Maltego can give a visual output by grouping its results. It has a very good graphical interface and information can be understood in a simple way thanks to this interface. It is stated that the following information can be accessed in many sources; Domain names, Whois information, IP address or determination of a network, E-mail address collection, Telephone, fax numbers, Social sharing networks, People's personal information, Social networks, Companies, websites, Using Internet infrastructure to obtain domains, IP addresses.

2.2.2. Passive Data Collection

This is done without access to any system or server the organization uses and the people we will receive the information from. There are many platforms for collecting passive information. For example, platforms such as Search engines (Google), Social networking sites (Facebook) and Personal information collection sites (pipl.com) can be used. In summary, it is the stage of collecting information about the source without the knowledge of it.

2.2.2.1. Whois

The name server for the domain of the source machine is used in a passive method of collecting information such as the administrator's personal information. Whois is a TCP-based request / response protocol that is widely used to collect passive information for Internet users. It can be used because it can output the domain and IP address of the destination. Domain name and IP address, date, status etc. It can provide specific information about. Whois TCP is active on port 43. The following output can be obtained from a whois transaction;

Whois Sorgulama
Sorgulamak için aşağıdaki kutucuğa alan adını giriniz.

automationpractice.com **Whois Sorgula**

automationpractice.com Whois Sonucu

Registrar Bilgileri

Barındırıldığı Firma	Tucows Domains Inc.
IANA ID	69
Kötüye kullanım bildirimi e-mail	domainabuse@tucows.com
Kötüye Kullanım bildirimi telefon	+1.416.535.0123

Name Server (DNS) Bilgileri

NS.INMOTIONHOSTING.COM	74.124.210.242
NS2.INMOTIONHOSTING.COM	70.39.150.2

Domain Sahibi Hakkında

Adı Soyadı	REDACTED FOR PRIVACY
Şirketi	REDACTED FOR PRIVACY
E-mail adresi	https://itedaccess.com/contact/5b8f33ef-b4f3-472c-b6a7-7e804cb96ad5
Telefonu	REDACTED FOR PRIVACY
Mahalle/Semt/Cadde	REDACTED FOR PRIVACY
Şehir	REDACTED FOR PRIVACY
Ülke	US

Domain Üzerindeki Korumalar

Transfer Koruması	Pasif
Silme Koruması	Pasif
Güncelleme Koruması	Pasif

Önemli Tarihler

Kayıt tarihi	19.11.2014
Güncelleme	4.11.2020
Bitiş Tarihi	20.11.2021
Kalan Gün	244
Domain Yaşı	6

Figure 2.10. Whois

2.2.2.2. TheHarvester

It scans the area and target information. Checks DNS data. Search engines mostly use Bing, Yahoo, Google. You can also check the data on social media, here you can use main social media platforms such as LinkedIn, Twitter. The tool is very simple and straightforward to use. It can provide fairly accurate information output in the early stages. It can be used to get passive target information on the Internet.

```

Usage: theharvester options

-d: Domain to search or company name
-b: data source: google, googleCSE, bing, bingapi, pgp
    linkedin, google-profiles, people123, jigsaw,
    twitter, googleplus, all

-s: Start in result number X (default: 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 50 to 50 results,
    -h: use SHODAN database to query discovered hosts
        google 100 to 100, and pgp doesn't use this option)

Examples:
theharvester -d microsoft.com -l 500 -b google
theharvester -d microsoft.com -b pgp
theharvester -d microsoft -l 200 -b linkedin
theharvester -d apple.com -b googleCSE -l 500 -s 300

```

Figure 2.11. TheHarvester

2.2.2.3. Netcraft

Netcraft is a passive information gathering tool used for resource's site / domain information. With this tool, it provides information about location, operating system, web service, kernel version, uptime outputs, old IP addresses and the last time the target machine was restarted, when it was installed, and what kind of services it has on it.

Background			
Site title	Not Present	Date first seen	January 2015
Site rank	135922	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English
Network			
Site	http://automationpractice.com	Domain	automationpractice.com
Netblock Owner	InMotion Hosting, Inc.	Nameserver	ns.inmotionhosting.com
Hosting company	InMotion Hosting	Domain registrar	unknown
Hosting country	US	Nameserver organisation	whois.tucows.com
IPv4 address	198.46.81.188 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS54641	DNS admin	machinemessages@forum.inmotionhosting.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ecb2165.inmotionhosting.com		

Figure 2.12. Netcraft

2.3. BRUTE FORCE TOOLS

The process of obtaining the encryption of data transmitted from a source or stored in a source is called password cracking. As a general logic, it is to try all the predictions you have in order. The process of password cracking can be helpful for those who forget the computer password when used useful. However, in general, it is seen that password cracking process is used to access confidential data today. The process of obtaining a password varies according to the length and complexity. The password should not only contain letters and numbers, also ^% & / (); When characters such as are also present, the complexity of the password increases

2.3.1. Aircrack-ng

Aircrack-ng is generally considered not only a password finder, but also one of the very good Wi-Fi hacking tools. Its work is essentially a tool that helps manipulate and infiltrate wireless networks. Aircrack-ng can be connected to wifi router using WPA / WPA2 - PSK encryption. During this WiFi attack, to prevent WPA / WPA2 negotiation during authentication and access PSK with aircrack-ng. If you want to enforce WPA PSK passwords only with CPU power, Aircrack-ng is one of the tools you can use. One of the disadvantages of this tool is that it doesn't use a graphics card. Another disadvantage is the lack of support for masks, rules, and other brute force parameters. The second drawback is compensated by the fact that Aircrack-ng can be paired with other programs that instantly support the same masks, rules, and password creation. As an example query, the following can be said:

\$ aircrack-ng -w wordlist.dic -b 00: 14: 24: 34: 45: 58 WPACrack.cap

```
> Executing "aircrack-ng --help"
Aircrack-ng 1.6 - (C) 2006-2020 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:
  -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
  -e <essid> : target selection: network identifier
  -b <bssid> : target selection: access point's MAC
  -p <nbcpu> : # of CPU to use (default: all CPUs)
  -q : enable quiet mode (no status output)
  -C <macs> : merge the given APs to a virtual one
  -l <file> : write key to file. Overwrites file.

Static WEP cracking options:
  -c : search alpha-numeric characters only
  -t : search binary coded decimal chr only
  -h : search the numeric key for Fritz!BOX
  -d <mask> : use masking of the key (A1:XX:CF:YY)
  -m <maddr> : MAC address to filter usable packets
  -n <nbits> : WEP key length : 64/128/152/256/512
  -i <index> : WEP key index (1 to 4), default: any
  -f <fudge> : bruteforce fudge factor, default: 2
```

Figure 2.13. Aircrack-ng

2.3.2. John The Ripper

John the Ripper is known as a password cracking tool and uses a dictionary attack method where the phrases found in the dictionary are likened to an encrypted string to find hits with various combinations. John The Ripper is a heavily used brute force technique and its applicability is directly proportional to the strength of the password chosen by the user. Like all brute force methods, it gives a positive result, but the most important feature that distinguishes it from others is the very short time it spends doing it. It is designed to break various types of hash used in software and operating systems. Tool performs this attack as password brute force, dictionary-based password guessing and hybrid attack.

```
$ /usr/sbin/john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-xop]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]          "single crack" mode
--wordlist[=FILE] --stdin   wordlist mode, read words from FILE or stdin
                             like --stdin, but bulk reads, and allows rules
--pipe                      like --wordlist, but fetch words from a .pot file
--loopback[=FILE]          PRINCE mode, read words from FILE
--dupe-suppression          suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                             doc/ENCODING and --list=hidden-options.
--rules[=SECTION]          enable word mangling rules for wordlist modes
--incremental[=MODE]       "incremental" mode [using section MODE]
--mask=MASK                mask mode using MASK
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=LEFT]              show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN[UID[...]] [do not] load this (these) user(s) only
--groups=[-]GID[...]]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[...]]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]    load salts with[out] COUNT [to MAX] hashes
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--format=NAME              force hash of type NAME. The supported formats can
                             be seen with --list=formats and --list=subformats
```

Figure 2.14. John The Ripper

2.3.3. Rainbowcrack

The RainbowCrack tool uses rainbow tables to crack hashes, is a hash cracking tool for RainbowCrack that uses a large-scale time-memory trade-off, as many sources have said. It can be used to crack passwords to identify weak passwords or break authentication. and can offer various password cracking features in one tool. It can automatically detect the type of hash used in a password, so you can also run it against encrypted password storage. It can run on Linux, Microsoft Windows and MAC OS X. It tries texts sequentially, which it thinks might take time for strong passwords. With this process, it can be faster in brute force attacks.


```

root@kali:~# rcrack
RainbowCrack 1.7
Copyright 2017 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: ./rcrack path [path] [...] -h hash
./rcrack path [path] [...] -l hash_list_file
./rcrack path [path] [...] -lm pwdump_file
./rcrack path [path] [...] -ntlm pwdump_file
path:          directory where rainbow tables (*.rt, *.rtc) are stored
-h hash:       load single hash
-l hash_list_file: load hashes from a file, each hash in a line
-lm pwdump_file: load lm hashes from pwdump file
-ntlm pwdump_file: load ntlm hashes from pwdump file

implemented hash algorithms:
lm HashLen=8 PlaintextLen=0-7
ntlm HashLen=16 PlaintextLen=0-15
md5 HashLen=16 PlaintextLen=0-15
sha1 HashLen=20 PlaintextLen=0-20
sha256 HashLen=32 PlaintextLen=0-20

examples:
./rcrack . -h 5d41402abc4b2a76b9719d911017c592
./rcrack . -l hash.txt

```

Figure 2.15. Rainbowcrack

2.3.4. Hashcat

Before examining the hashcat, it should be known that the hashcat is divided into 4 in itself; Hashcat is Hashcat-gui oclHashcat-lite and oclHashcat-plus.

To introduce these tools;

Hashcat - It is a tool that can crack with its CPU feature with its multithreading structure.

oclHashcat-gui - Known as the OS powered graphical interface for Hashcat.

oclHashcat-lite - Can crack with Gpu support.

oclHashcat-plus - A tool that can crack simultaneously by creating and using wordlists.

Kali hashcat installed by default on linux. It is also said to have 200 password algorithm information as stated in many sources. One of the most important features of many brute force tools is that it can use not only cpu but also gpu.

```

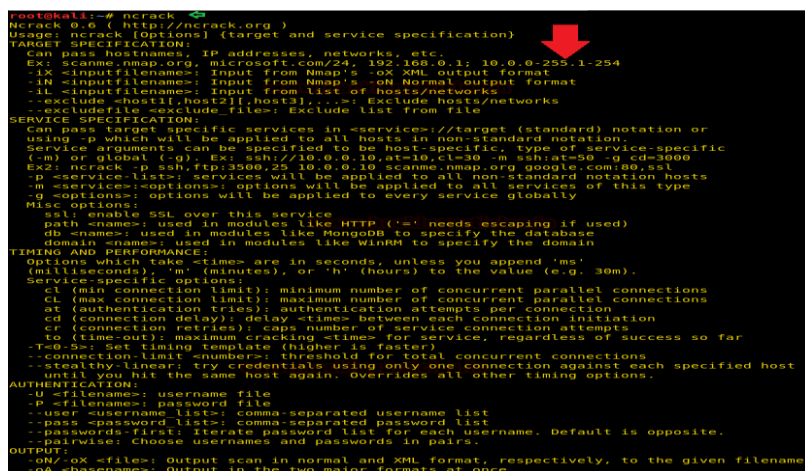
* Hash types:
0 = MD5
10 = md5($pass.$salt)
20 = md5($salt.$pass)
30 = md5(unicode($pass).$salt)
40 = md5($salt.unicode($pass))
50 = HMAC-MD5 (key = $pass)
60 = HMAC-MD5 (key = $salt)
100 = SHA1
110 = sha1($pass.$salt)
120 = sha1($salt.$pass)
130 = sha1(unicode($pass).$salt)
140 = sha1($salt.unicode($pass))
150 = HMAC-SHA1 (key = $pass)
160 = HMAC-SHA1 (key = $salt)
200 = MySQL
300 = MySQL4.1/MySQL5
400 = phpass, MD5 Wordpress, MD5 phpBB3
500 = md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
800 = SHA-1(Django)
900 = MD4
1000 = NTLM
1100 = Domain Cached Credentials, mscash
1400 = SHA256

```

Figure 2.16. Hashcat

2.3.5. Ncrack

Ncrack is a high-speed network authentication cracking tool used to check computers and network devices for low-security passwords. Ncrack is preferred by many security experts due to its use and comments. It is very similar to nmap with the use of a dynamic engine. It enables fast, yet reliable large-scale control of multiple hosts. It has a simple and straightforward interface. Ncrack tool can be used for the following protocols: SSH, RDP, FTP, Telnet, HTTP (S), Wordpress, POP3 (S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSSQL, MongoDB, Cassandra, WinRM, OWA, DICOM.



```
root@kali:~# ncrack
Ncrack 0.9.0 ( http://nmap.org )
Usage: ncrack [Options] (target and service specification)
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0.0-255.1-254
  -iN <inputfilename>: Input from Nmap's -oN Normal output format
  -iL <inputfilename>: Input from list of hosts/networks
  -e <hostname|host|host/|host/|...>: Exclude hosts/networks
  -x <excluderfile>: Exclude list from file
SERVICE SPECIFICATION:
  Can pass target specific services in <service>://target (standard) notation or
  using -p which will be applied to all hosts in non-standard notation.
  Service arguments can be specified to be host-specific, type of service-specific
  (-m) or global (-g). Ex: ssh://10.0.0.10,at=10,cl=30 -m ssh,at=30 -g cd=3000
  Ex2: ncrack -p ssh,ftp:3500-25 10.0.0.10 scanme.nmap.org google.com:80,ssl
  -p <service-list>: services will be applied to all non-standard notation hosts
  -m <service>: options will be applied to all services of this type
  -g <options>: options will be applied to every service globally
Misc options:
  -ssl: enable SSL over this service
  path <name>: used in modules like HTTP ('=' needs escaping if used)
  db <name>: used in modules like MongoDB to specify the database
  domain <name>: used in modules like WinRM to specify the domain
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, unless you append 'ms'
  (milliseconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
Service-specific options:
  cl (min connection limit): minimum number of concurrent parallel connections
  CL (max connection limit): maximum number of concurrent parallel connections
  at (authentication tries): authentication attempts per connection
  cd (connection delay): delay <time> between each connection initiation
  cr (connection retries): caps number of service connection attempts
  to (time-out): maximum cracking <time> for service, regardless of success so far
  -T=0-S: Set timing template (higher is faster)
  --connection-limit <number>: threshold for total concurrent connections
  --stealthy-linear: try credentials using only one connection against each specified host
  until you hit the same host again. Overrides all other timing options.
AUTHENTICATION:
  -U <filename>: username file
  -P <filename>: password file
  --user <username-list>: comma-separated username list
  --pass <password-list>: comma-separated password list
  --passwords-first: Iterate password list for each username. Default is opposite.
  --pairwise: Choose usernames and passwords in pairs.
OUTPUT:
  -oN <file>: Output scan in normal and XML format, respectively, to the given filename.
  -oA <basename>: Output in the two major formats at once.
```

Figure 2.17. Ncrack

2.3.6. Hydra

Hydra is a very commonly used tool for BruteForce. Most commonly used protocols are FTP, SSH, SMTP, Telnet, HTTP / HTTPS, POP3, RDP.

It can be used to apply force. Its important feature is that it can brute force attack on services such as Hydra POSTGRES, Radmin, TeamSpeak, Oracle and additionally supports SSL.

hydra -V -f -t 4 -l test -P / root / wordlist ssh: //192.168.60.50

-V - show login + password pair during brute-force

-f - stop as soon as the specified login password is found

-P - the path to the dictionary with passwords

ssh: //192.168.60.50 - service indicator and victim's IP address

```
[ATTEMPT] target 192.168.60.50 - login "test" - pass "soccer7" - 2492 of 14344400 [child 3] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "rammstein" - 2493 of 14344400 [child 4] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "louie" - 2494 of 14344400 [child 7] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "cotton" - 2495 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "althea" - 2496 of 14344400 [child 2] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "shamrock" - 2497 of 14344400 [child 15] (0/1)
[22][ssh] host: 192.168.60.50 login: test password: rammstein
[STATUS] attack finished for 192.168.60.50 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

```
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE]
[-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]
[-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s POR]

Options:
-R restore a previous aborted/crashed session
-I ignore an existing restore file (don't wait 10 seconds)
-S perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
-y disable use of symbols in brute-force, see above
-e nsr try "n" null password, "s" login as pass and/or "r" reversed login
-u dosval loop around users, not passwords (effective! implied with -x)
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-o FILE write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME wait time per login attempt over all threads (enforces -t 1)
-4 / -6 use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-o use old SSL v2 and v3
-q do not print messages about connection errors
-U service module usage details
-h manual.txt more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
```

Figure 2.18. Hydra

2.4. DATABASE PROTECTION SIMULATION

Simulation consists of two parts. First, a brute force tool was written. In the last part, the stage of capturing and blocking the attack made with this tool was passed. They will be able to use the project written on capture and blocking, which many people can use both in their personal life and in their business life.

2.4.1. Brute Force Tool

The tool was written in c # on .Net. The language and environments can change. The event here is to show how easily an attacker can attack a system.

You can manually design the environment for the tool, or you can do it with code.

You have prepared it manually here.

The target ip is written for the Server Ip. The name used for the target database access is written for the UserName. The number is written in the Count section. Achieving the result of a remote attack would be extremely slow, but an attack from within would achieve a rapid result.

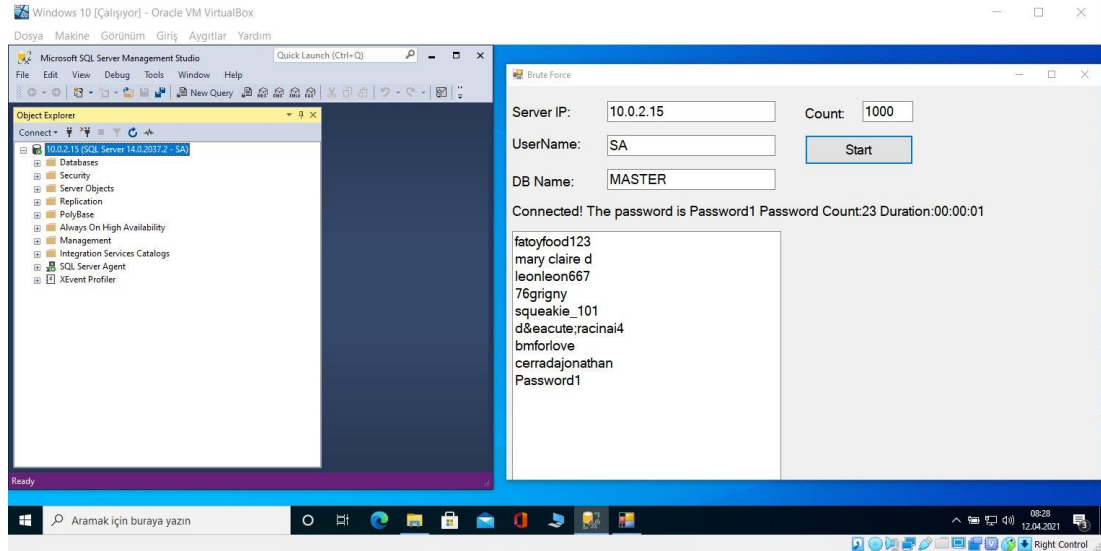


Figure 2.19. Brute Force Tool

2.4.2. Catch and Block

In order to prevent the attack, it is necessary to catch the attack at the beginning. SQL itself has sql server logs records in the Management folder. In fact, these logs will be used in the whole project. There are many records such as successful and unsuccessful log records. This log filtering has been offered to us as an option. These filters can be accessed from the security tab in the server properties, where optional log records can be obtained.

The main purpose of our project is to reach these records here and to prevent it by determining the specified IP address.

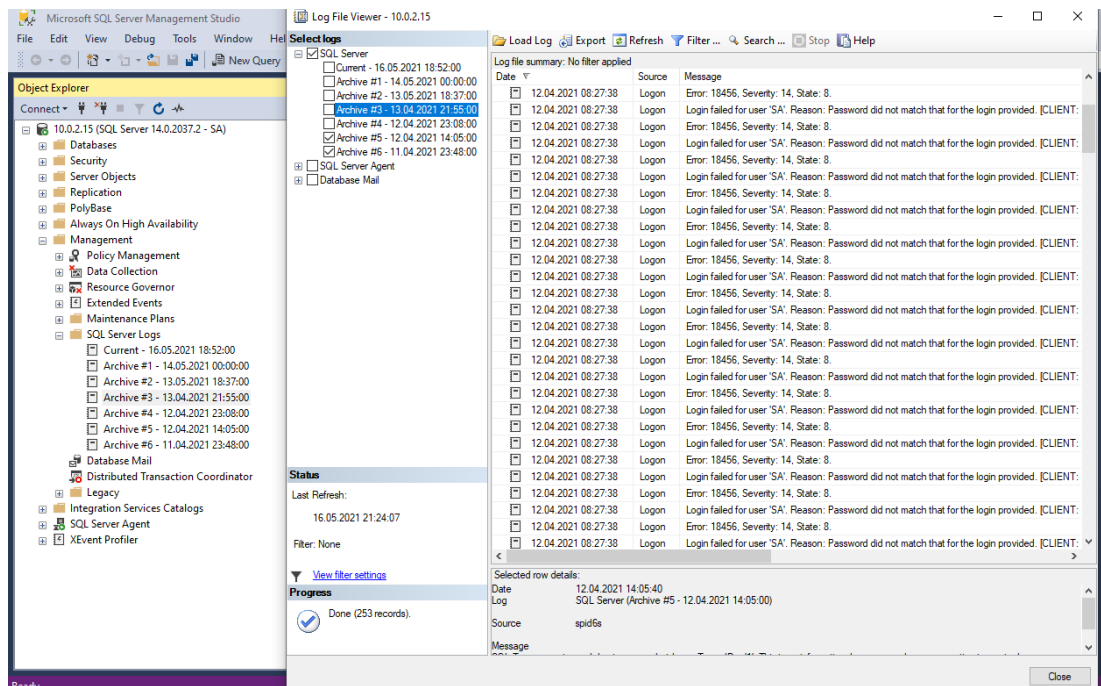


Figure 2.20. Log File Viewer

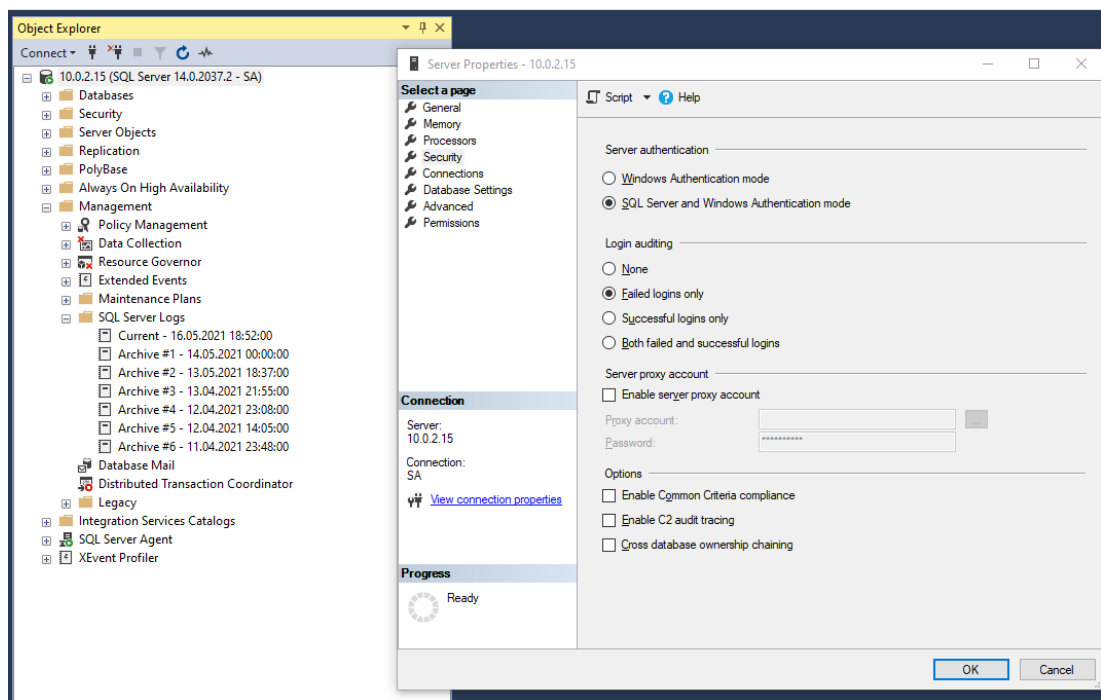


Figure 2.21. Login Auditing

With the information on the Log File Viewer, the brute force will be tested first. In the next step, the information about how often the system is attempted to password

will be obtained. By recording these password attempts, the system administrator is notified and the attack is prevented.

In this section, the log records were taken and placed in a table. The necessary preparations were made to send mail by obtaining information such as start time, end time, IP address and number from the log records. Dynamically, the data is sent in a format. Here, some functions are used to make the data usable after extracting it.

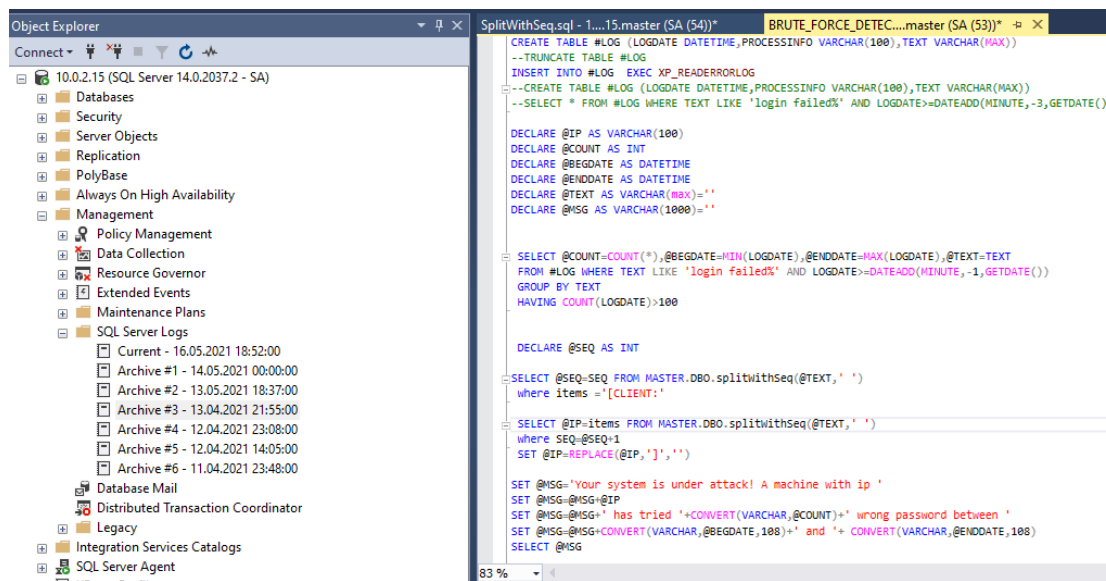


Figure 2.22. Making Format

While preparing the mail format, attention was paid to be dynamic. When the mail reaches the administrator, it should be able to understand the attack information in a basic way because. In order to transmit the mail, the mail should be saved to the Database Mail section in the Management. In this project, I entered my own mail account. Multiple mails can be defined.

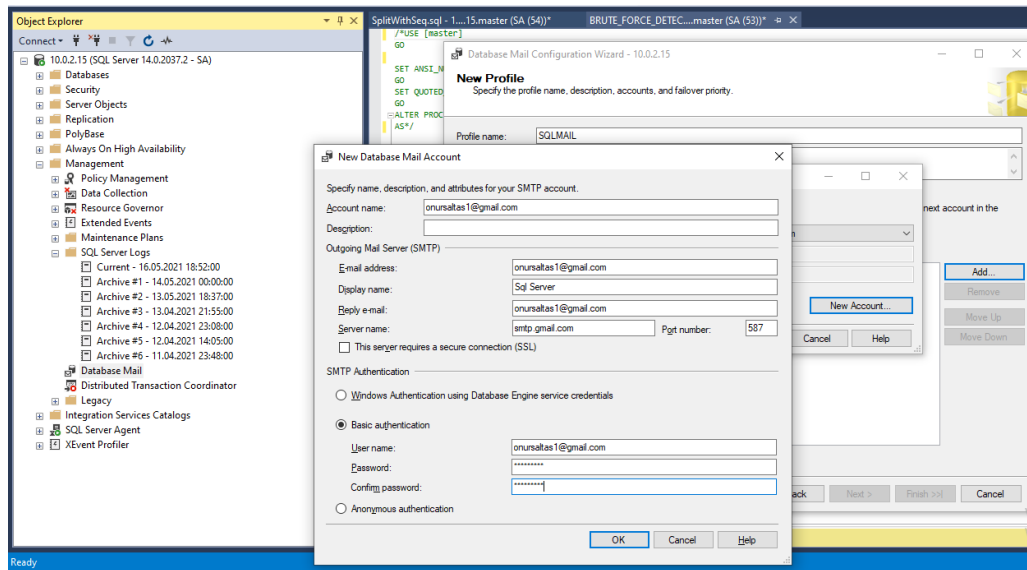


Figure 2.23. Sent Mail

```
EXEC msdb.dbo.sp_send_dbmail
    @profile_name = 'SQLMAIL',
    @recipients = 'qquestionanswerr@gmail.com',
    @body = @msg ,
    @subject = 'Brute Force Attack Detected' ;
END
```

Figure 2.24. For Send Mail

In order to make this structure work continuously by making it automatic, necessary settings are made on Sql. For this, the desired settings are performed by creating a job in the jobs folder in the sql server agent, respectively.

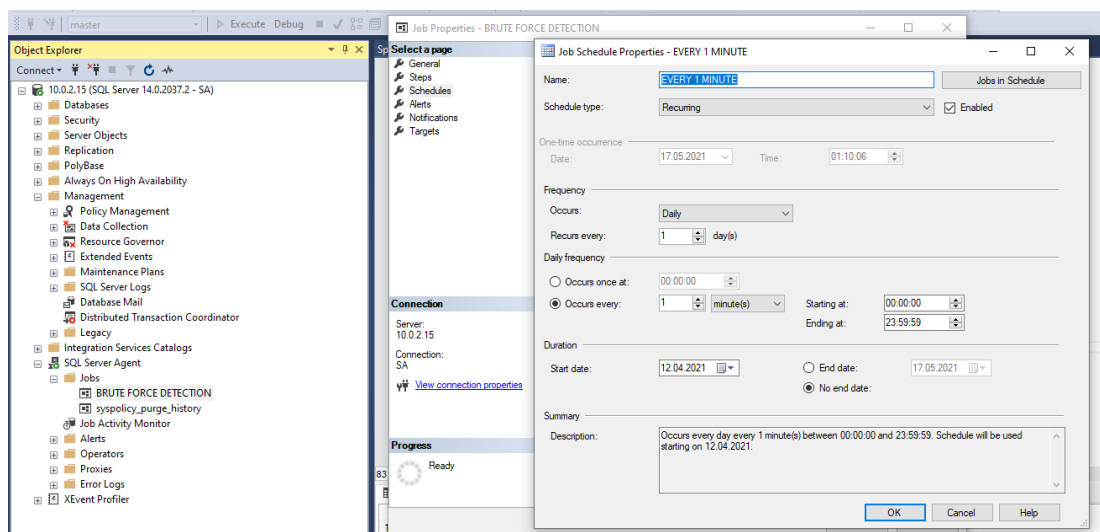


Figure 2.25. Job Schedule

It can be said to prevent the last attack. This can be done with the trigger. You need to be very careful for this. In a wrong case, even the database user may not be able to access it himself.

```
CREATE TRIGGER BRUTE_FORCE_LOGON_CONTROL
ON ALL SERVER
FOR LOGON
AS
BEGIN
    DECLARE @COUNT AS INT
    SELECT @COUNT=COUNT(*) FROM AUDIT.DBO.BRUTE_FORCE_ATTACK
    WHERE COMPUTERIP=CONNECTIONPROPERTY('client_net_address')
    IF ISNULL(@COUNT,0)>0
    BEGIN
        ROLLBACK
    END
END
```

Figure 2.26. Trigger

CHAPTER 3

FINAL

In recent years, where security is important at every stage, a lot of information has been given to users about password requirements, active-passive information collection, database protection.

With the password requirements, this was able to answer the question of how to make the passwords used in daily life strong to the user. By explaining the structure of encryption algorithms, it was shown how many systems are stored in our passwords. These algorithms can be used both by keeping our own passwords and in our systems.

It was shown how easily the information can be accessed with active and passive information collection. With these information collection stages, the importance of the information to the user was emphasized and the importance of not being shared everywhere was emphasized.

Protecting the database has actually been shown to be of utmost importance, demonstrating this on password requirements and active-passive information collection. Learning the logic of algorithms in password requirements, the user will now use his password in a strong structure, and the user who sees the active-passive information collection stages will no longer share his information on social platforms, etc environments.

At this stage, an attack can be made on a user who takes care of them, and at this stage, the database will be protected with database protection. At the last stage, it is aimed to protect our information by protecting the database. Until the last stage, but to give the attacker very little information about us, password requirements and active - passive collection stages should be taken seriously.

REFERENCES

1. Internet : Joan Goodchild, “Remote Work Pushes Brute-Force Attacks Higher”, <https://securityboulevard.com/2020/07/remote-work-pushes-brute-force-attacks-higher/>. (2020)
2. Bryan Sullivan and SPI Dynamics, “Preventing a Brute Force or Dictionary Attack: How to Keep the Brutes Away from Your Loot”, Physical Review E,3-4
3. Internet: ATT Company, “making the most of passwords”, <https://www.att.org.uk/cyber-security-making-most-passwords>. (2020)
4. Internet: Pavitra Shankdhar, “Popular Tools for Brute-force Attacks”, <https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/>. (2020)
5. Internet: Vladimir Unterfingher, “Popular Tools for Brute-force Attacks”, <https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/>. (2020)
6. Internet: Darren Richardson, “INFORMATION SECURITY”, <https://www.theseus.fi/bitstream/handle/10024/92691/Darren.Richardson.Final.pdf?sequence=1&isAllowed=y>. S. 13 (2015)
7. Internet: James P. Owens, Jr., “A Study of Passwords and Methods Used in Brute-Force SSH Attacks”, https://people.clarkson.edu/~owensjp/pubs/Owens_MS_thesis.pdf S. 11 (2008)
8. Internet: G. Sowmya , 2 D.Jamuna, 3 M. K. Reddy, “BLOCKING OF BRUTE FORCE ATTACK”, <https://www.ijert.org/research/blocking-of-brute-force-attack-IJERTV1IS6133.pdf> . S. 3 (2012)
9. Internet Stephen Kost, “Detecting and Stopping Cyber Attacks against Oracle Databases”,https://www.integrigy.com/files/Integrigy%20Detecting%20and%20Stopping%20Cyber%20Attacks%20against%20Oracle%20Databases_0.pdf . (2015)
10. Internet: Raşit özcan, “Çevre VE Şehircilik Bakanlığı Merkezi Oracle Veritabanlarını Performans ve Güvenlik Yönünden İncelenmesi ve İyileştirme Önerileri”, https://webdosya.csb.gov.tr/db/cbs/icerikler/ras-t_ozcan_tez-20180925134553.pdf . (2017)

RESUME

Onur SALTAŞ was born in 1997 in Istanbul; He completed his primary and secondary education in Istanbul. He completed the first 3 years of his high school education in Çorlu Anatolian High School and the last year through open education. He started his education at Karabük University Engineering Faculty Computer Engineering Department in 2016 and is currently continuing his working life as a software test engineer at Burgan Bank..

CONTACT INFORMATION

E-mail: 2016010213032@ogrenci.karabuk.edu.tr onursaltas1@gmail.com;

