International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3360

E-ISSN : 2454-6135

Volume.5, Issue 1
January -2019

Vulnerable Data Center and Developing of On-line Protection

Abdullah D. Salman[1] and Sarah Ali Abd[2]

Programmer[1] and Communication Engineer[2]

Ministry of Planning

Department of information Technology

Baghdad, Iraq

ABSTRACT

This study illustrates the importance of the existence of ethical hacking data center and what are the most important measures that must be taken and provided in data centers. In order to upgrade to the best ways to secure data and information and to encourage employees to constantly develop themselves because of the counting development of information communication technology (ICT). This study also refers to the security precaution that must be available in the data center to protect their data. And also what is the "ethical hacker" and what types and what are the advantages and disadvantages of using ethical hacker. Due to the orientation of the data center to a unified electronic connection, it is necessary to indicate the importance of information and the prevention of data leaks.

The importance of ICT development is key to success in every aspect for information processing. Online protection is of Mach importance in all data processing starting from the main data center room to the home and the individual interface with the internet. Protection s/w is now must to be installed in all levels of internet serving and the higher level of data processing, the higher and more efficient protection programs must be developed, The security team is responsible for monitoring the network and Internet charges for any breach. If there is an unauthorized access attempt on your device, the action will take effect immediately Such as disconnecting the Internet for a short time and making the block the device to try to enter for more than 3 consecutive Especially to data center devices.

It's important that employees receive institutional sessions by the specialist, alerting them not to use e-mail messages in Internet cafes, unknown devices (unknown source), and interacting with unknown links. The Information and Network Security Team is responsible for risk management and incident verification because they are familiar with all details of the organization, including information and data. In order to reduce the impact of cyber-attacks and to protect the data center, it became necessary to qualify a team to monitor e-security, protect information and provide a secure electronic environment.

Key Words: *Ethical, Hacking, unauthorized, Attacks, Passive Attacks, Active Attacks.*

1. INTRODUCTION

Communication contributes to the build a knowledge society through the creation of a strong infrastructure using the latest technologies. Communications play an important role in the economic and social life as well as the management of institutions through the exchange of documents and information. We must note the importance of information in our time and how to keep that information from tampering with unauthorized people to access these information .The process of protecting data center and companies has become necessary to develop policies and procedures to protect data through the use of protection devices (firewalls) in addition to the importance of developing cadres working in these institutions to address external attacks and prevent the access of unauthorized persons to the source of information in addition to finding weaknesses in those Institutions and choose a high quality system. Ethical hacking discovers program weaknesses, documents these vulnerabilities, and helps network security to defend and deter these types of potential attacks from future events.

2. DEFININATION OF HACKING

Before defining what the term is "hacking" lets know the difference between threat and attack. We can say the threat occurs before the problem in another sense before hacking. Hacking Is the process of connecting unauthorized persons to computer sources and manipulating and altering existing data and These unauthorized persons are highly experienced in programming As well as knowledge in all aspects of security systems Where systems are accessed through gaps and a lack of assessment of the risks facing institutions that surround all areas of work,.

According to reference [1], there are three basic and important elements of information security, The Figure 1.1 below shows the details.

- **Confidentiality**: This term covers two related concepts:

  Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

  Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- **Integrity**: This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability**: Assures that systems work promptly and service is not denied to authorized user.

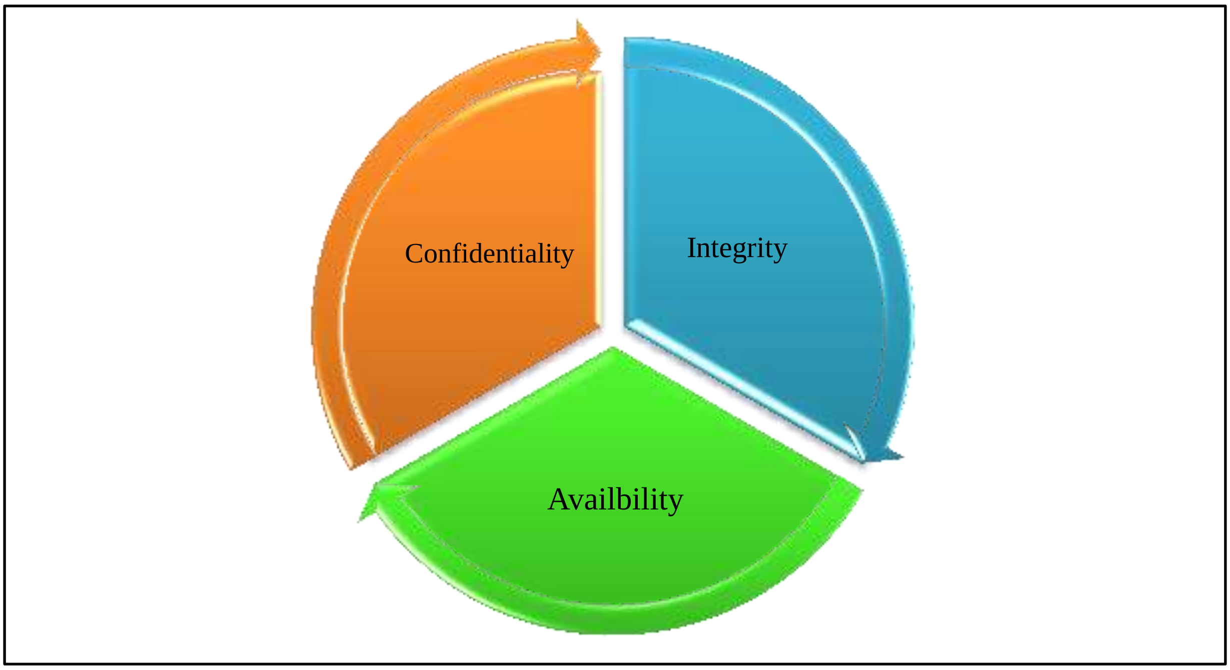

Figure 1.1 The Security Requirements (CIA)

3. HISTORY OF HACKING

Is hacking always bad? Not really. It only depends on how to use it. The Hacking is not limited to computers only According to references [2] will show same of history of the ethical hacking.

1- The first hackers appeared in the 1960 at the USA Institute of Technology, and their first victims were electric trains.
2- During the 1970, a different kind of hacker appeared: the phreaks or phone hackers
3- Robert T. Morris, Jr. launches the first self-replicating worm on the government’s ARPANET to test its effect on UNIX systems; he is the first person to be convicted under the Computer Fraud Act of 1986
4- In 1995 Kevin Mitnick, probably the world’s most prolific and best known hacker, is arrested and charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers Mitnick was also in possession of 20,000 credit card numbers. And Christopher Pile is the first person jailed for writing and distributing a computer virus.

4. TYPES OF HACKING

According to references [3], Can display hacking types to several denomination.

4.1. Website Hacking

Web sites are hacked by unauthorized people and control the web server and all related programs such as interfaces and data.

4.2. Network Hacking

DOI : 10.31695/IJERAT.2019.3360

Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Net stat, etc. with the intent to harm the network system and hamper its operation. Or the service can be disconnected from users (deny the service)

4.3. Email Hacking

It means unauthorized access to e-mail account and use without the consent or knowledge of its owner

4.4. Ethical Hacking

Is One of the types of hacking used in institutions and banks that contain important data and information to find the system vulnerabilities and avoid to problems.

4.5. Password Hacking

This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

4.6. Computer Hacking

This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

5. TYPES OF ATTACKS

According to reference [1]Attack is accesses to the data by another person (Not authorized) that means this data can be change and modify, attack divided in two type

5.1 Passive Attacks: Passive attacks are is actually the process of intonation and its purpose is to obtain information between the sender and the receiver there is no data modification can be done. There are two method of passive attacks.

5.1.1 Release of message contents it can be say the hacker (third person) can read the content sent between sender and receiver as shown in Figure 1.2**.**

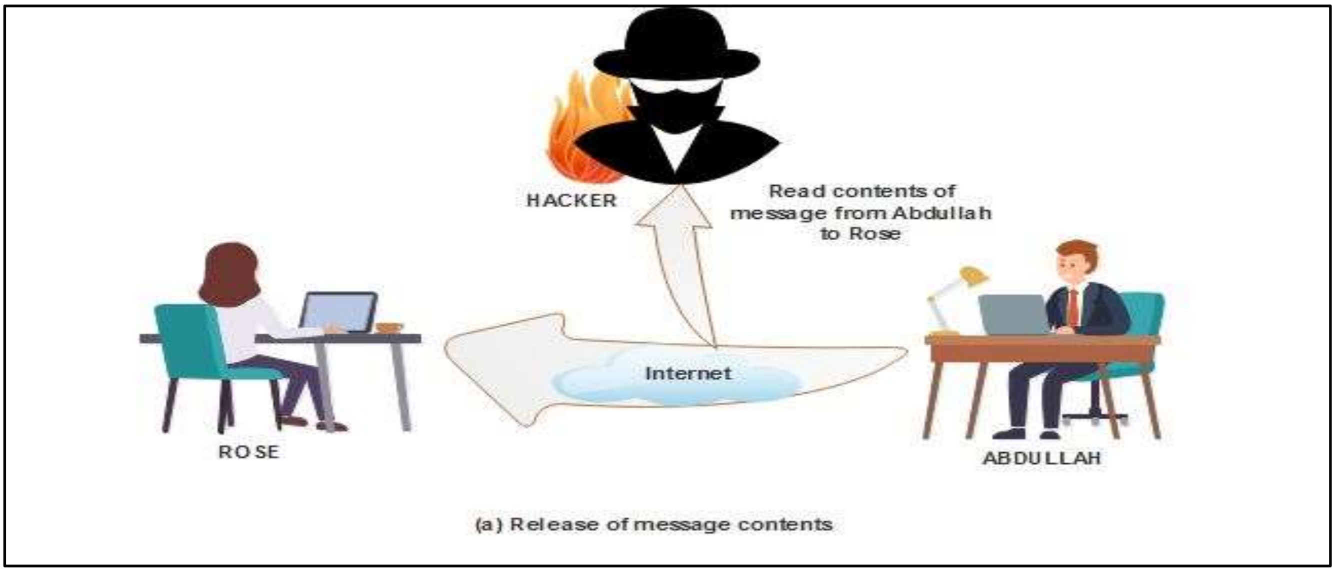
HACKER
Read contents of message from Abdullah to Rose
Internet
ROSE
ABDULLAH
(a) Release of message contents

Figure 1.2 Release of Message Contents

5.1.2 Traffic analysis in this way messages are tracked from the sender to the receiver through the third person (the unauthorized person) in this process no data modification can be done, as shown in figure 1.3.

DOI : 10.31695/IJERAT.2019.3360

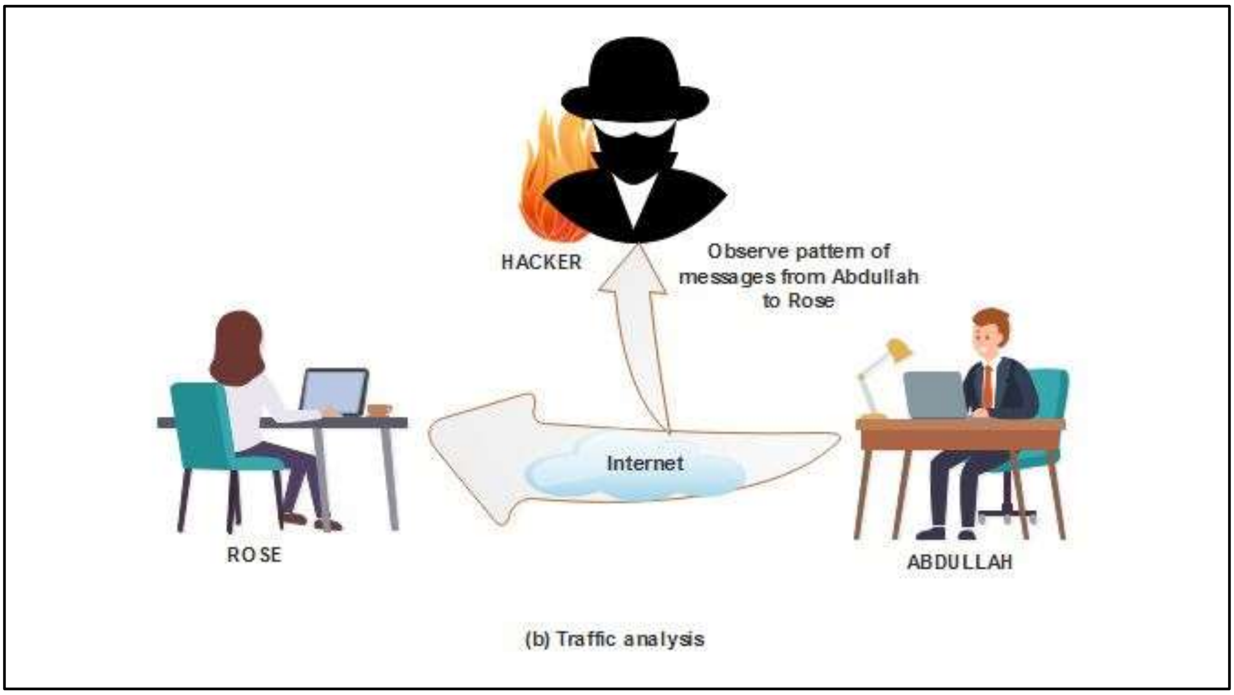

Figure 1.3 Traffic Analysis

5.2 Active Attacks: Active attacks include some modification of the data, the data can be changed between the sender and receiver there are four method of active attacks.

5.2.1 Masquerade: Sending the data and messages by the third person (unauthorized person) but using the name of the sender. The receiver does not know that from other person as show in Figure 1.4

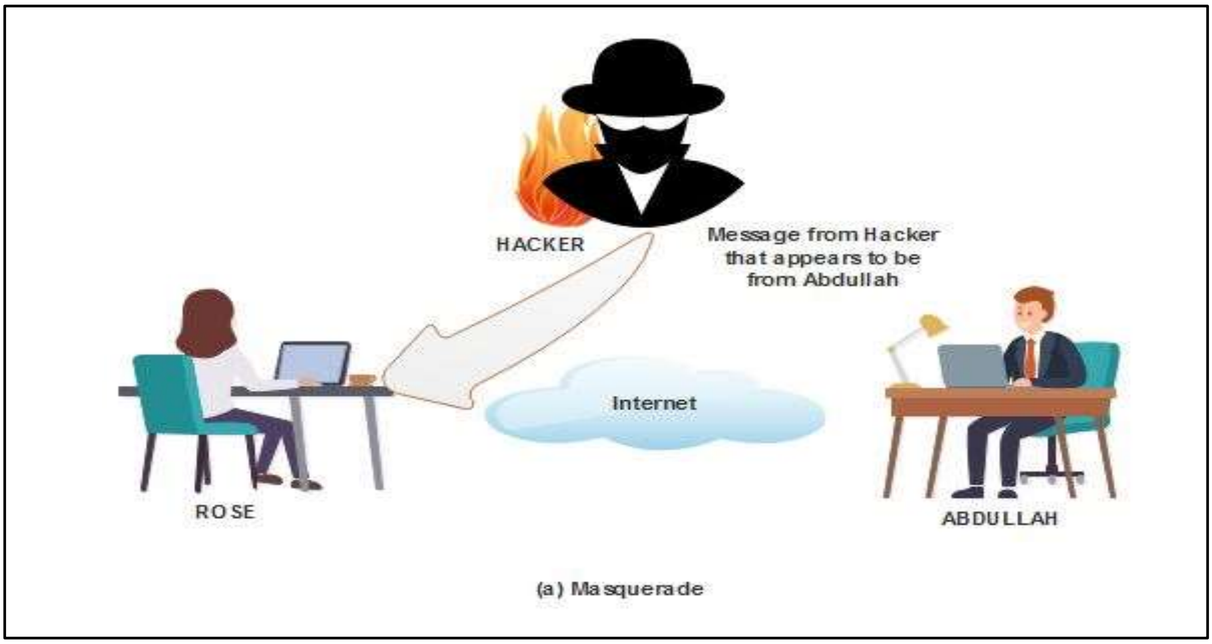

Figure 1.4 Masquerade

5.2.2 Replay: When sending the message from the sender to the receiver, the message will go to the third person (unauthorized) and will be modified and then sent to the receiver. The receiver of the message will receive two messages and do not know who correct.as show in Figure 1.5.

DOI : 10.31695/IJERAT.2019.3360

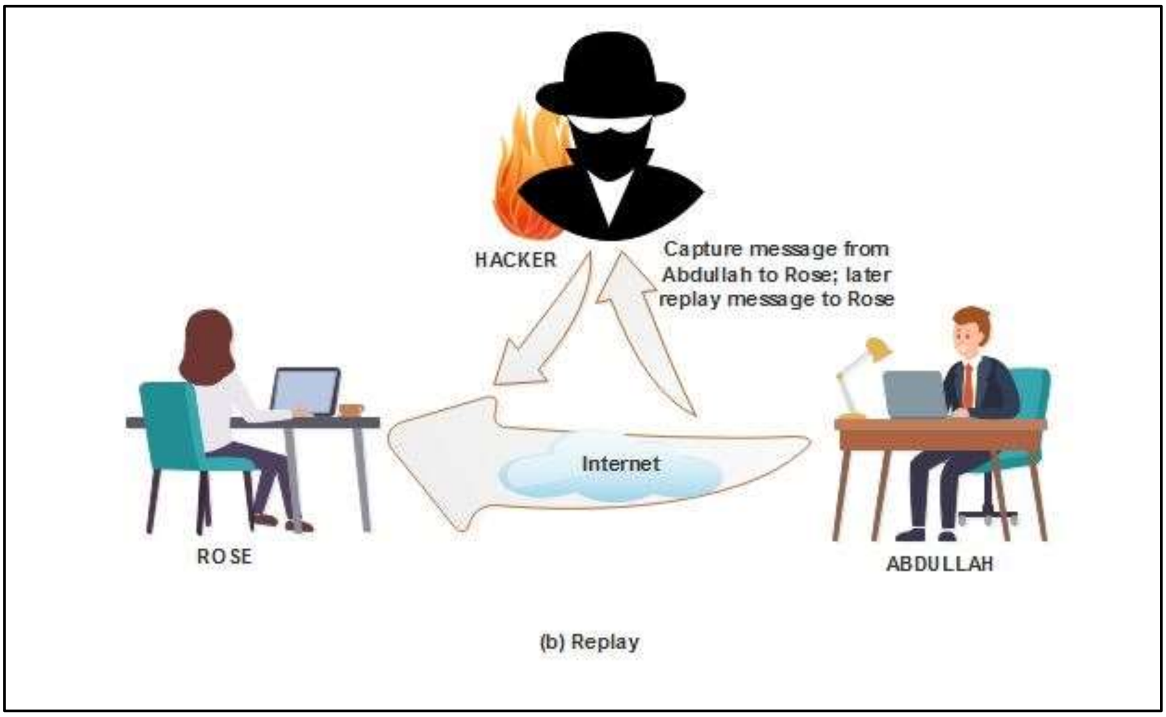
HACKER
Capture message from Abdullah to Rose; later replay message to Rose
Internet
ROSE
ABDULLAH
(b) Replay

Figure 1.5 Replay

5.2.3 Modification of messages: When sending a message from the sender to the receiver, it will go directly to the third person (authorized) and is modified and then sent to the receiver, the receiver does not know that there is a change in the message as show in Figure 1.6.

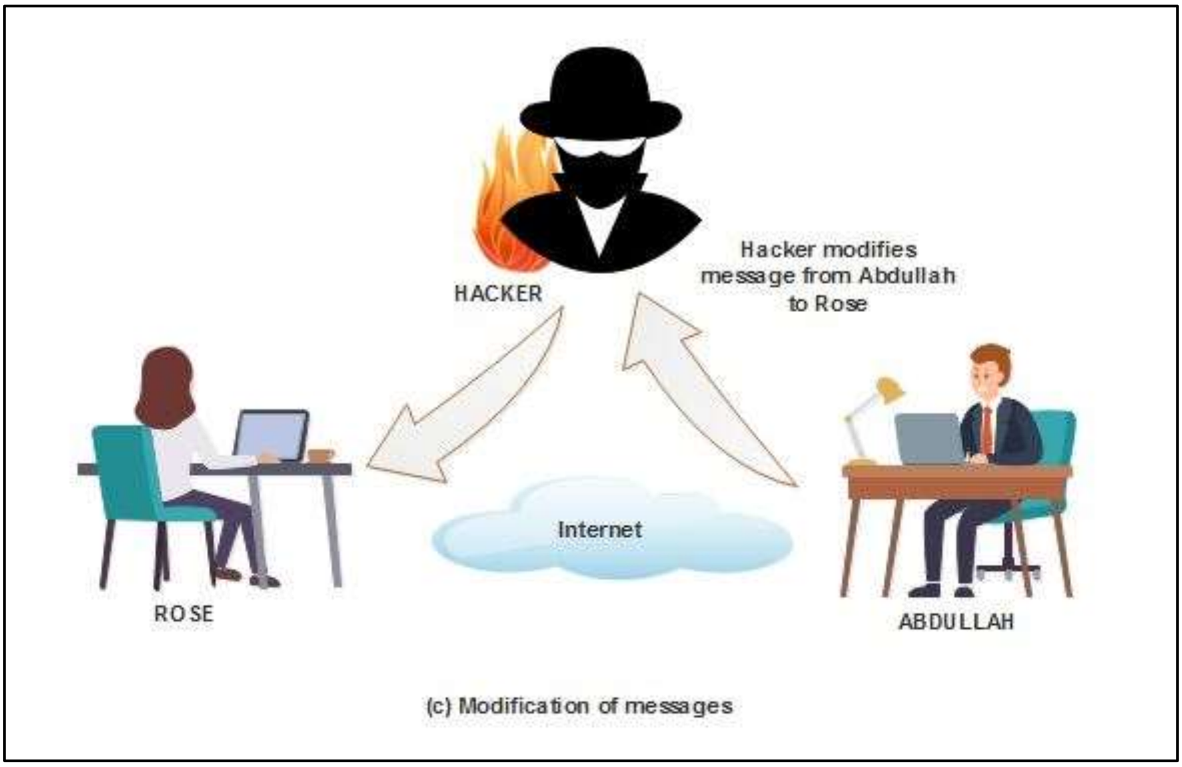
HACKER
Hacker modifies message from Abdullah to Rose
Internet
ROSE
ABDULLAH
(c) Modification of messages

Figure 1.6 Modification of Messages

5.2.4 Denial of service: The service is disconnected (denial) from the server to the sender by the third party (unauthorized) As show in Figure 1.7.

DOI : 10.31695/IJERAT.2019.3360

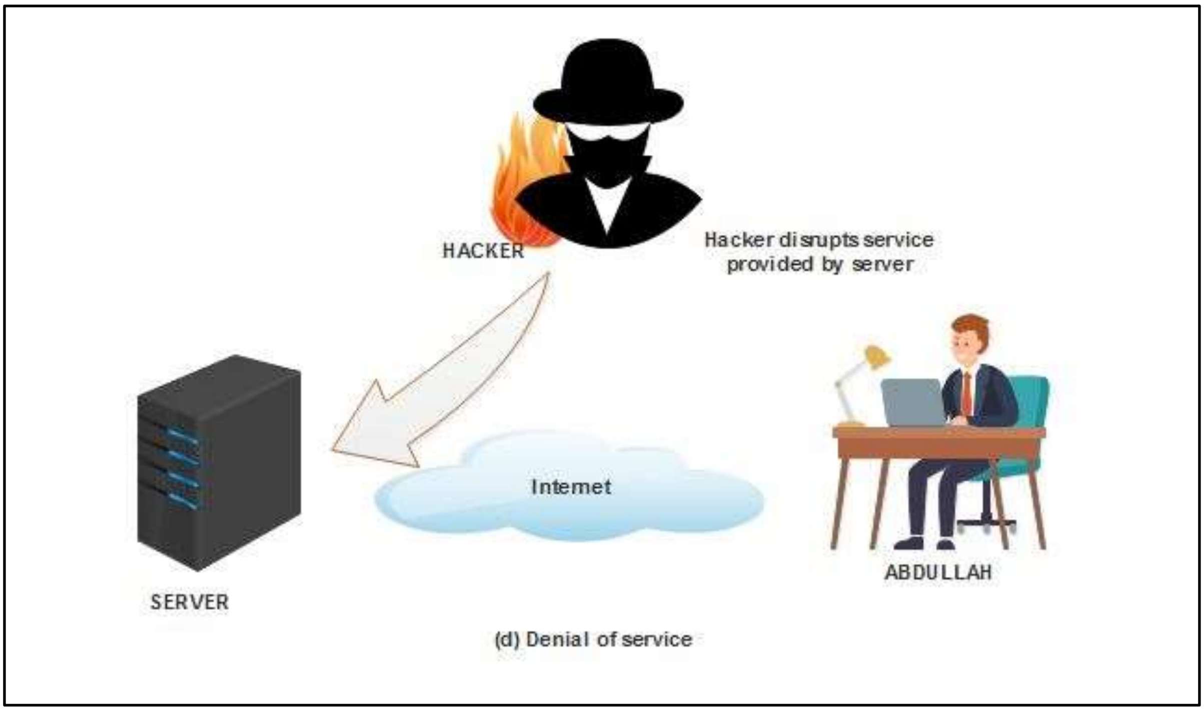

Figure 1.7 Denial of Service

6. DEFINITION OF ETHICAL HACKING

Expert in computer systems and networks the first task is to find vulnerabilities in systems and protection from malicious hackers, The ethical hacker may differ from the malicious hacker to make all his information and experience in protecting the systems and not reaching unauthorized persons. It is no longer enough to buy and install a simple software package and let it work, and also Use different algorithms to encrypt data It is necessary to have a cadre of people in institutions that protect systems from penetration from outside the institution and from the inside institution. And also raising awareness of the employees of the institution on the importance of risk management and the possibility of not being exposed to attacks.

7. ADVANTAGES OF ETHICAL HACKING

The need for further development of the use of information security has become clear. Organizations face security threats and must modify their security policies and structures. Institutions should consider the importance of ethical hacking services, which are of primary concern where ethical hackers can be used in government institutions that contain important data and information and protect it from theft. Add litigation protection if hackers enter company systems and steal customer information, the company may face potential litigation. Consumers can sue an organization for failing to protect their personal information. Ethical piracy can help prevent the possibility of such litigation. Organizations may also have to meet some regulatory and regulatory requirements related to the safety of consumer information. Ethical piracy helps them to do these tasks.

8. DISADVANTAGES OF ETHICAL HACKING

All kinds of activities that have a bad side, there will be people who are dishonest. Potential disadvantages of ethical hacking include:

- Ethical hackers can carry out malicious hacking activities and work against the organization in which they operate.
- Allow to see financial and banking details of enterprises and all important data

9. MALWARE TYPES

Malware is software which is intended to cause harm to anyone uses computer, especially those who uses the internet. Malware have the ability to spread itself through the network, causes damage and bring down the computer performance. When the computer becomes infected and is no longer usable, the data inside becomes unavailable. These are some of the malware types. As showing in reference [1] Table 1.1.

DOI : 10.31695/IJERAT.2019.3360

Table 1.1 Malware Types

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it Succeeds the code is said to be infected. When the infected code is executed, the virus also Executes.
Worm	A computer program that can run independently and can propagate a complete working Version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined Condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting Legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access To functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged To a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader Is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a Denial-of-service (Dos) attack.
Key loggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained Root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other Machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a Browser to a commercial site.

10. RISK AND VULNERABILITY MANAGEMENT

Risk management is the process of dealing, measuring and making decisions with risks and practical methods and developing the best ways to avoid and minimize damage. We can say that the risk is the probability of loss and occurrence of a natural event to an unexpected result, leading to many problems.

Vulnerabilities are weaknesses that can be exploited to access or violate the system. According to reverence [5] the Weaknesses can be assessed in terms of means, such as

- Lost tapes during transport to the storage facility
- Devices and Programs that are not preserve allow unauthorized access over the Internet, Leading to easy penetration of confidential information
- The information is read by an unauthorized person
- Loss of unintentional data by theft.
- Accidental or intentional deletion or modification of information.
- Unsecured computers and portable devices such as laptops, or USB devices.

Risk reduction Risk reduction is the use of strategically limited resources to change unacceptable risks to acceptable risks. At the discretion of [6] risk reduction is a combination of technical and non-technical changes.

1. Technical changes include security equipment (access controls, physical security, firewalls, intrusion detection systems, backups, and anti-virus software)
2. Non-technical changes may include changes in policy, training of cadres, and increased security awareness.

DOI : 10.31695/IJERAT.2019.3360

11. PROCEDURES TO BE PROVIDED FOR SECURE ELECTRONIC ENVIRONMENT

When you provide a secure environment, it is essential that you have the necessary procedures and standards can be divided into a number of points:

- The existence of a data center according to international standards in institutions and banks, Including refrigeration equipment, surveillance cameras, fire alarm, power supply and only authorized people enter the data center.
- All servers and client are licensed for ongoing updates and with good specifications.
- There is a special server for an antivirus program that receives updates and distributes them on all networked computers routinely, at least once a week.
- Engage staff in courses in network security to reach professionalism in order to assess risks and found Weaknesses and protect institutions from any permeation.
- To enhance the performance of network against attacks, it is better to supply different firewalls provenance.
- Documentation and backups are one of the most important procedures where it is necessary to document all the work and carry out the backup of all data in the servers and transfer them in alternative sites outside the data center.
- The importance of having a risk management team as it is an essential part in all institutions. And this enhances the efficiency, finding and identifying the levels of potential risks before they occur especially in communication and information technology which helps to protect data security and also Risk assessment periodically.
- The importance of policies and work procedures for IT staff. Includes password policies Passwords must be strong and difficult to guess and should be changed over time ,The user policy is to give the validity of users connected to the network with the possibility of locking social networking sites that have a lot of penetration, As well as the division of tasks and responsibilities.

According to reference [4] Policies and work procedures are essential in institutions. The Ministry of Planning / Central Statistical Organization made a survey to assess the readiness of state institutions for the transition to e-governance in 2015, among these results is the knowledge of counting policies and procedures working in institutions The level averaged 33% of the total, The level was significant 24% followed by the weak level of 18% and the level completely was 12% As shown in Figure 1.8.

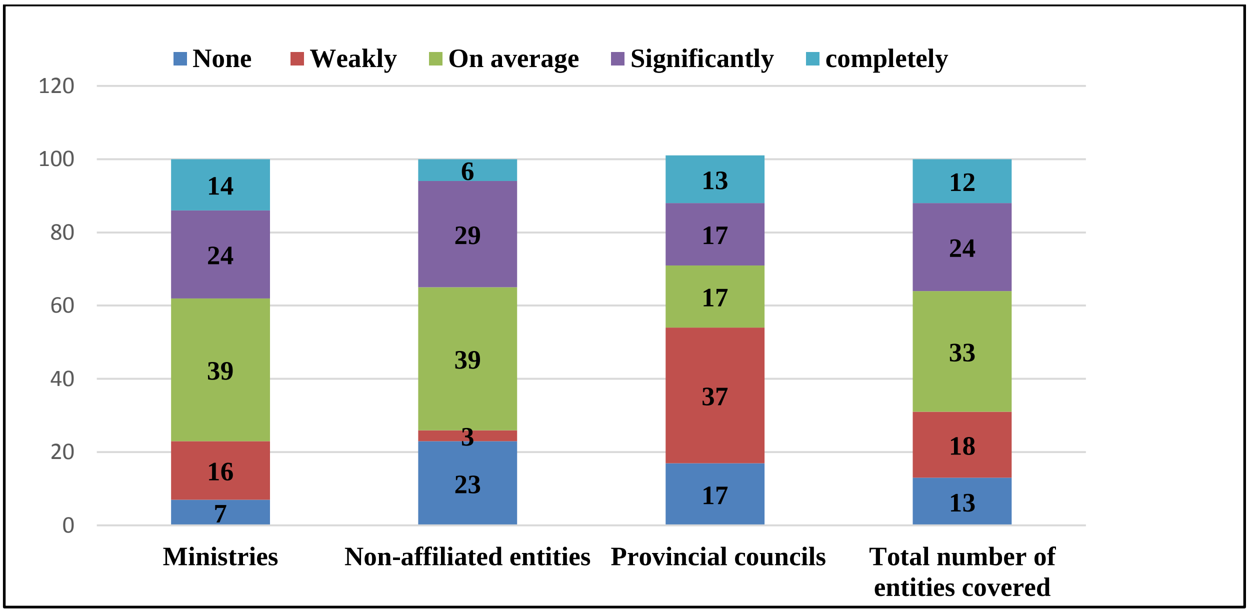

Figure 1.8 Policies and procedures adopted in e-governance for 2015

REFERENCES

[1] William Stallings (2011), “Cryptography and network security”, fifth Edition

[2] Zuley Clarke, James Clawson and Maria Cordell (2003), “A brief history of hacking”, http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf.

[3] Ethical Hacking (2018), “Tutorials point”, Simply Easy Learning, www.tutorialspoint.com.

[4] Ministry of Planning, Central Statistical Organization, https://www.cosit.gov.iq.

[5] Cyber Security Risk Management Guide (2012), http://www.dhses.ny.gov/ocs/.

[6] Thomas M. Chen, “Information Security and Risk Management”, http://engweb.swan.ac.uk/~tmchen/papers/info-sec-risks.pdf.