CHAPTER FIVE

CHAPTER FOUR

CHAPTER ONE

CHAPTER TWO

CHAPTER THREE

REFRENCES

الخلاصة

بسبب التوسع الحاصل في شبكات الحاسبات ونظرا للاستخدام الكبير لشبكات الإنترنت ، وبسبب الأهمية الكبيرة لأمن الحاسبات وشبكات الحاسبات صمم برنامج للتدريب على أمنية الحاسبات وذلك لجعل العديد من وسائل الهجوم والدفاع أكثر سهوله في الفهم والتطبيق من قبل الطلبة والناس المهتمين.

ينقسم المشروع بصورة عامة الى جزئين رئيسيين: جزء التطبيقات و جزء الشرح والتوضيح. في كل جزء، سينقسم المشروع الى جزئين اخرين ايضا هما : جزء الهجوم وجزء الدفاع. في كل جزء من هذه الأجزاء (الهجوم والدفاع) ستتم تغطية ادوات الأمنية الأكثر شهرة. حيث سيتم تطبيق برنامج عن كل اداة من ادوات الأمنية (الهجوم والدفاع) يساعد على تلبية متطلبات المشروع. اما في جزء الشرح والتوضيح ، ستتم كتابة شرح مختصر ومركز عن ماهية وطريقة عمل كل اداة من هذه الأدوات المختارة. كما ان لمستخدم النظام امكانية اضافة تطبيقات وبرامج جديدة الى جزء التطبيقات وذلك لتفحصها وتجربتها على النظام لغرض توسيع المشروع في المستقبل.

ABSTRACT

The expansion of computer networks and the use of Internet in every side of our life, and the importance of Computer and Network security, , computer aided learning Security System is utilized to make many security attacks and services easier to be applied and understood by students and other people.

The proposed system will mainly be divided into two parts, Application mode and Documentation mode. In the two modes, the system will be in two parts: Attack and Defense. In the Attack and Defense, the well known security tools will be covered. In the application part, each one of the tools will be applied by using a program that will help to obtain the project purpose. In the Documentation mode, a brief description that describes what each tool is doing. The user of the project will have the ability to add new programs and testing it in order to expand the system in the future in the application mode.

Acknowledgments

My deepest appreciation goes to Dr. Siddeeq Y. Ameen who wholeheartedly guided me through the preparation of this research and enlightened me many aspects of it.

My thanks are, as well, due to the Head of the Department of Computer Science Dr. Taha S. Bashaga and The Dean of the collage for their support and encouragement.

Finally, I owe deep gratefulness to my family for their overwhelming support and care; to my mother for her prayer, to my father for his attention and encouragement, to my brothers for their constant concern and their precious words that gave me strength and power when it was desperately needed.

السيرة الذاتية

الاسم: مصطفى ابراهيم عبد الجميلي

محل وتأريخ الولادة: الفلوجة ١٩٨١

عنوان السكن: الانبار- الفلوجة- الحي العسكري

رقم الهاتف: ٠٧٩٠١٦٧٣١٤٦

البريد الالكتروني: mustafa_aljumaili@yahoo.com

عنوان البحث: نظام تدريب امني بمساعدة الكومبيوتر

اسم المشرف: د. صديق يوسف امين

تأريخ المناقشة: ٢٠٠٧/٣/١٥

Supervisor Certification

I certify that this thesis was prepared under my supervision at the Department of Computer Science / College of Science / Al-Nahrain University, by **Mustafa Ibrahim Abid Al-Jumaili** as a partial fulfillment of the requirements for the degree of Master of Science in Computer Science.

Signature:

Name: Dr. Siddeeq Y. Ameen

Title: Professor

Date: 12 / 11 / 2006

In view of the available recommendations; I forward this thesis for debate by the examination committee.

Signature:

Name:

Title:

Date: / / 2006

Chapter One
Introduction

1.1 Background

The benefits and the properties used in information warfare system can be used to design a training security system that is used in laboratory to be a project that helps for understanding computer and network security.

So, Information warfare is closely related to infrastructural warfare, which involves the disruption of a government without necessarily causing direct loss of life. As more computers are connected to systems used by society as a whole, the capability to use computers to engage in infrastructural warfare has been increased. The engineer has historically been of significant value to those engaged in warfare. Today, computers are commonly used to affect computerized command and control systems for the modern, digitized battlefield. At their core, computers are developed, and remain today, as weapons [2].

One factor often overlooked in the engagement of warfare or conflict is the consequences to the adversary. Due to the wide and sweeping capacity of computers to operate systems critical to society and necessary for life (such as medical, traffic, and air-control systems), the aggressor must take special note to consider the consequences of any actions taken against computing platforms. The aggressor should not seek to perform reckless harm. While it may be convenient to consider it fundamentally wrong to inflict harm in any context. There are precedents for just war, and it is very difficult to conceive of any job or operation which is taken in the proper context. It is totally free of producing harm [3].

Many tools, which may be used to attack computers, are available for free, these include [1]:

i. Network Scanning Tools
ii. Password cracking tools
iii. Denial of service tools
iv. Cryptography tools

These tools may be used to identify the vulnerabilities present in computers attached to a company’s or government’s computer networks, crack and defeat password systems, effectively deny an organization’s computers, the ability to provide the services which are required to be performed, and establish private communications respectively [1].

1.2 Information Warfare:

Information warfare covers a broad subject and usually it only gets one-sided coverage. Too often these days all we hear about is how computer hackers have hacked into a bank or how a new virus has infiltrated our home and business computers. People read the paper, listen to the radio and watch the daily news only seeing and hearing what the media’s perception of what information warfare is. IW is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries. [13]

Operational Security (OPSEC) and Information Security (INFOSEC), also play a key role in information warfare. To protect your assets from an attack, you need to have a firm understanding on these topics and implement them in your daily personnel and business routine.

1.3 Operational Security (OPSEC)

OPSEC is the process of denying information to adversaries about capabilities or controlling and protecting unclassified evidence of the planning and execution of sensitive activities. OPSEC focuses on having a good understanding of enemies decision maker's ability to collect reliable, adequate, and timely intelligence and, when integrated with other capabilities, it can shape to our advantage the adversary's knowledge and beliefs about our operations. To implement OPSEC effectively, it's important to have an effective security awareness program. Some key items that should not be discussed in an unsecured manner are [13]

i. Usernames and/or passwords
ii. Specific network configuration, which could include internal IP addresses and placement of perimeter security devices.
iii. Specific private information related to key decision makers.
iv. Any critical information that if, in the wrong hands can, be detrimental to your company. (i.e. roll-out dates for new products or drawbacks due to competitor success)

It is clear from these examples that OPSEC is a critical part of everyone's daily routine and justifies why you need to develop ways to protect critical information that if in the wrong hands can be detrimental to you or your company [14].

1.4 Information Security (INFOSEC)

Information security merges the technology and techniques of computer security, communications security, emanations security, physical security, and personnel security to protect data, services and other resources. One of the first steps to making INFOSEC work for you is to put together a policy for you and your company. An effective INFOSEC policy should cover some of the following areas [13]:

i. Responsibilities; who is responsible for implementing and administering the security policy.
ii. Anti-Virus policy and update guidelines.
iii. Specific guidelines for users to include use of e-mail and the Internet.
iv. Firewall and Intrusion Detection System (IDS) policy.
v. Define a backup policy.

INFOSEC policy like OPSEC, user awareness is critical to making INFOSEC work for you. What good is it to define guidelines for the users if they don’t know or understand the policy? Understanding INFOSEC is important in guarding against hacker warfare and other attacks against the information systems

1.5 Information Warfare Types

Here is a brief look on the major information warfare types with a concentration on the computer network warfare or hacker warfare as follows [15].

i. **Electronic Warfare**

Electronic Warfare is any military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. Electronic Warfare is broken down into three sub-areas. Electronic attack, electronic protect and electronic support. Electronic attacks are actions taken to prevent or reduce an enemy’s effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception. Electronic protections are actions taken to counter an enemy’s use of EA against us. Electronic support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing [15].

ii. **Command and Control Warfare**

Command and control is the use of OPSEC, military deception, psychological operations and electronic warfare to deny information, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions [15].

iii. **Psychological Warfare**

Psychological warfare is planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of organizations, groups, and individuals. Psychological warfare can consist of dropping leaflets on the targeted audience to obtain the desired effect or goals [15].

iv. Hacker Warfare

Hacker warfare is probably the most familiar portion of information warfare. This type of warfare is also known as computer network operations and is often portrayed in movies and headlines. Hacker warfare is one of the biggest areas of IW where the military and civilian lines get mixed up and you start to see military attacks on civilian companies to gain a desired affect on an enemy. For example, to slow production of tanks for an enemy's army, our military could launch computer network attacks against the company's production line computers.

There are two areas of hacker warfare, offensive and defensive. Offensive or computer network attack is defined as operations to disrupt, deny, degrade, or destroy information in computers and computer networks, or the computers and networks themselves. Computer network attack can originate from an organized hacker group, a nationally supported hacker group or an individual. Nationally supported hacker activity appears to be on the rise [13].

Any time a firewall or anti-virus software installed, computer network defense were performed. Protection against computer network attack can include firewalls, intrusion detection system's. All of the above should be included in company's information security policy and personnel information systems.

v. Economic Intelligence Warfare

It can be defined as the economic impact of information warfare on a country or company. There are two areas of economic intelligence warfare, information blockade and information imperialism. Information blockade is a blockade of information channels similar to an economic blockade. A nation or company would cut-off the targeted countries access to outside information. This blockade would hopefully cripple the economy of the targeted nation. Information imperialism can be defined as nations holding new technology or information within its borders to offer national companies an advantage over competing companies. Whether information blockade or information imperialism can be called war is a debatable question [14].

1.6 Literature Survey

Research by Mary Gillam predicated upon the following premises: First, the exploitation of “information” as a weapon is changing the nature of warfare. Second, although there are many debates about the reality of the IW threat, postulates that adversarial IW tactics pose a legitimate threat to security infrastructure. Finally, the Department of Defense (DOD), the Joint Staff, and the Services must remain actively committed to combating the IW threat in the 21st century [4].

In Mostow j. research the Internet Attack Simulator (IAS) that simulates information attacks directed against networks was presented. The IAS simulates three attack scenarios: denial of service, unauthorized access and spoofing .It’s IAS environment is a high-fidelity real-time model [5].

The Eric J.Holdaway research shows that the passive defenses cannot shed their essential weaknesses, that they cede the initiative to the adversary and that they rely on fallible human activity to maintain them, there is still much that can be done to strengthen them before resorting to active defense. Active deception and counterattacks carried out by properly constituted units can contribute significantly to the defense strategies [6].

The security issues that are involved in establishing network interoperability were also considered in a thesis by Susan C. McGovern. The network environment is defined in terms of purpose, command structure, mission area, and control functions. Network and information protection were discussed in terms of minimizing the threats to information systems security. Information system user requirements are defined and some of the security mechanisms required to meet those requirements is discussed. Current solutions to secure network interoperability were surveyed [7].

Donald Welch and Greg Conti proposed and justified an outline framework for an information warfare simulation. The simulation model covers four categories of objects, these are node address, connection, interaction and infotron, and they also present analysis from two examples scenarios [8].

1.7 Thesis Objectives

The main objective of this thesis is to explore the new coming research area associated with the information systems, and information technology, called information warfare. This thesis explains the information warfare definition, types, and structure. Therefore, to achieve such objectives the following goals were proposed to:

1. Distinguish the attacks that affect computers and networks.
2. Distinguish defense strategies that deal with these attacks.
3. Design and Implement Computer Aided Learning System two parts: Application and documentation by simulating most office

common attacks actions in computers network and the corresponding defense actions in the application part and explaining each action in a brief description in the documentation part.

1.8 Thesis Layout

This thesis has been organized to be in five chapters:

- **Chapter two** presents the theory of computer networks basics, Internetworking, network security, security threats and defense.
- **Chapter three** It gives a detailed view about the computer network warfare parts, functions, and the IW techniques designed in attack and defense.
- **Chapter four** describes the attack and defense stages of the implemented warfare, presenting the implemented program in each of the six types of attack stage, and the six types of defense stage. The six types of the attack stage are cracking, hacking, password sniffing, e-mail activities, viruses and port scanning while the six types of the defense stage are intruder detection, security check, network monitoring, e-mail protection, virus scanning and encryption.
- **Chapter five** includes the conclusions and suggestion for future works.

Chapter Two

Network Security and Threats

2.1 Introduction:

The fields of computer networking and today's Internet trace their beginnings back to the early 1960's, at time at which the telephone network was the world's dominant communication network. The telephone network uses circuit switching to transmit information from a sender to a receiver – an appropriate choice given that voice is transmitted at a constant rate between sender and receiver. Given increasing importance (and great expense) of computers in the early 1960's and the advent of timeshared computers, it was perhaps natural to consider the question how to hook computers together so that they could be shared among geographically distributed users. The traffic generated by such users was likely to be intervals of activity, such as sending a command to a remote computer, followed by periods of inactivity while waiting for a reply the received response [25].

The work at MIT, Rand, and NPL laid the foundations for today's internet. But the internet also has a long history of a let's build it and demonstrate it attitude that also date's back to the early 1960s, J.C.R Licklider and Lawrence Roberts, both collegues of Kleinrock's at MIT, went to lead the computer science program at the Advanced Research Projects Agency (ARPA) in the United States [25].

By 1972, ARPAAnet has grown to approximately 15 nodes and was given its firs public demonstration by Robert Kahn at 1972 International Conference on Computer Communications. The first host-to-host protocol between ARPAnet end systems known as the network -control protocol (NCP) was completed. With an end to end protocol available, applications could now been written. The first e-mail program was written by Ray Tomlinson at BBN in 1972 [25].

2.2 Computer Networks Basics

The International Organization for Standardization (ISO) proposed a model for computer network protocol architecture, and as a framework for developing network protocol standards. As with TCP, the OSI model uses the structuring technique known as layering (as shown in Figure 2.1).

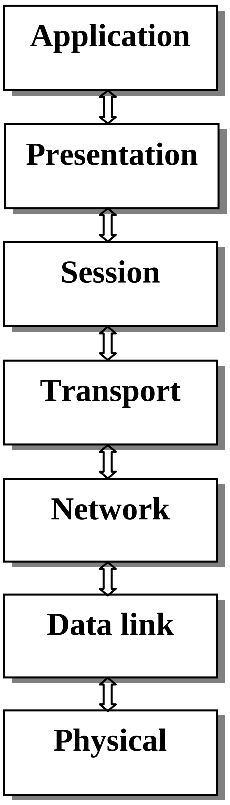


Fig.(2.1) OSI Layers

The seven layers that compose the OSI model are as follows from top to bottom [10]:

i. Application layer provides access to the OSI environment for users and also provides distributed information services.

ii. Presentation layer provides independence to the application processes from differences in data representation (syntax).

iii. Session layer provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications.

iv. Transport layer provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.

v. Network layer provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections.

vi. Data link layer provides the reliable transfer of information across the physical link; sends blocks (frames) with the necessary synchronization, error control, and flow control.

vii. Physical layer concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.

2.3 TCP/IP

The TCP/IP and the concept of internetworking is developed together, each shaping the growth of the other. An Internet under TCP/IP operates like a single network connecting many computers of any size and type. Internally the Internet is an interconnection of independent physical networks linked by Internetworking devices.

TCP was developed before OSI. Therefore the layers in the TCP/IP protocol do not match exactly with those in the OSI model. The TCP/IP protocol is made of five layers; physical, data link, network, transport, and application. The application layer in the TCP/IP can be equated with the combination of session, presentation, and application layers of the OSI model [7].

At the transport layers, TCP/IP defines two protocols; TCP and UDP. At the network layer, the main protocol is defined by TCP/IP is IP, although there are some other protocols that support data movement in this layer. At the physical and data link layers, TCP/IP does not define any specific protocol. A network, in a TCP/IP internet can be LAN, MAN, or WAN [7].

The TCP protocol is typically used by applications that require guaranteed delivery. It is a sliding window protocol that provides handling for both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number and is implemented as a finite state machine. The byte stream is transferred in segments. The window size determines the number of bytes of data that can be sent before an acknowledgement from the receiver is necessary.

The IP protocol is the transmission mechanism used by the TCP/IP protocols. It is unreliable and connectionless datagram protocol and also provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get transmission through to its destination. If reliability is important, IP must be paired with a reliable protocol such as TCP. IP transports data in is packets called datagram which may travel along different routers and may arrive out of sequence or duplicated. Further details about each field of IP header and their functions are shown in Appendix A [9].

2.4 Security Attacks

Attacks on the security of a computer system or network are best characterized by viewing the function of a computer system as providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user. The following are the four general categories of attack [12]:

i. *Interruption*: an asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability.

ii. *Interception*: an unauthorized party gains access to an asset. This is an attack on Confidentiality. The unauthorized party could be a person, a program, or a computer.

iii. *Modification*: an unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.

iv. *Fabrication*: an unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.

2.4.1 Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmission. The goal is to obtain information that is being transmitted. There are two types of passive attacks [12]:

i. Release of message content: the information transmitted could be e-mail messages, important files, or any important data. The idea is to prevent the opponent from learning the content of these transmissions.

ii. Traffic analysis: even if the information transmitted is protected by encryption or any other ways the opponent could determine the location and identity of communication hosts, the frequency and length of messages exchanged which might be useful in guessing the nature of communication.

2.4.2 Active Attacks

These attacks involve some modification of the data stream or the creation of false one; they can subdivide into four categories [12]:

i. *Masquerade*: takes place when one entity pretends to be a different entity. Authentication sequences enabling authorized entity with a few privileges can be captured and replayed to obtain extra privileges by impersonating another entity.

ii. *Replay*: involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.

iii. *Modification of messages*: means that some potion of legitimate message is altered or delayed or even recorded to produce an authorized effect.

iv. *Denial of service*: prevents or inhibits the normal use of management of communications facilities such as disabling the network or by overloading it with messages so as to degrade performance.

2.5 Network Security Services

Computer and network security research and development have focused on three or four general security services that encompass the various functions required of an information security facility. One useful classification of security services is the following [11]:

i. Confidentiality: ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

ii. Authentication: ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

iii. Integrity: ensures that only authorized parties are able to modify computer system assets and transmitted information. Modifications include writing, changing, changing status, deleting, creating, and delaying or replying of transmitted messages.

iv. Nonrepudiation: requires that neither the sender nor the receiver of a message be able to deny the transmission.

v. Access Control: requires that access to information resources may be controlled by or for the target system.

vi. Availability: requires that computer system assets be available to authorized parties when needed.

2.6 Security Threats

For the fist few decades of their existence, computer networks were primarily used by university researches for sending email, and by corporate employers for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, tax returns, network security is looming on the horizon as a potentially massive problem [10].

Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone. Some of the most perpetrators are listed in table 2.1. It should be clear from this list that making a network secure involves a lot more than just keeping it free of programming error [10].

Table (2.1) some of the people who can cause
security problems and why

Adversary	Goal
Student	To have fun snooping on people's email
Hacker	To test out someone's security system, steal data
Sales representative	To claim to represent all of Europe, not just endora
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from company
Stockbroker	To deny a promise made to customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military strength
Terrorist	To steal germ warfare secrets

Network security problems can be divided roughly into four areas; Secrecy, authentication, nonrepudiation, and integrity control. Secrecy has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into business deal. Nonrepudiation deals with signatures, while the integrity is the assurance to the data to be received as it sent without any modification or duplication or any other changes. [11]

All these issues occur in traditional systems but with some significant differences secrecy and integrity are achieved by using registered mail and locking documents up. Every layer in OSI has something to contribute to security. In the physical layer, wiretapping can be enclosing transmission lines in sealed tubes containing argon gas high pressure. Any attempt to drill into a tube will release some gas, reducing the pressure and triggering an alarm [10].

In the data link layer, packets on a point to point line can be encoded as they leave one machine and decoded as they enter another.

In the network layer, firewalls can be installed to keep packets in or keep packets out. In the transportation layer, entire connections can be encrypted, end to end, that is, process to process. Although these solutions help with secrecy and many people are working hard to improve them, none of them solve the authentication or nonrepudiation problem in a sufficiently general way. This causes the numbers of reported computer security incidents and vulnerabilities have increased significantly, as shown in Figures (2.2) and (2.3) [12].

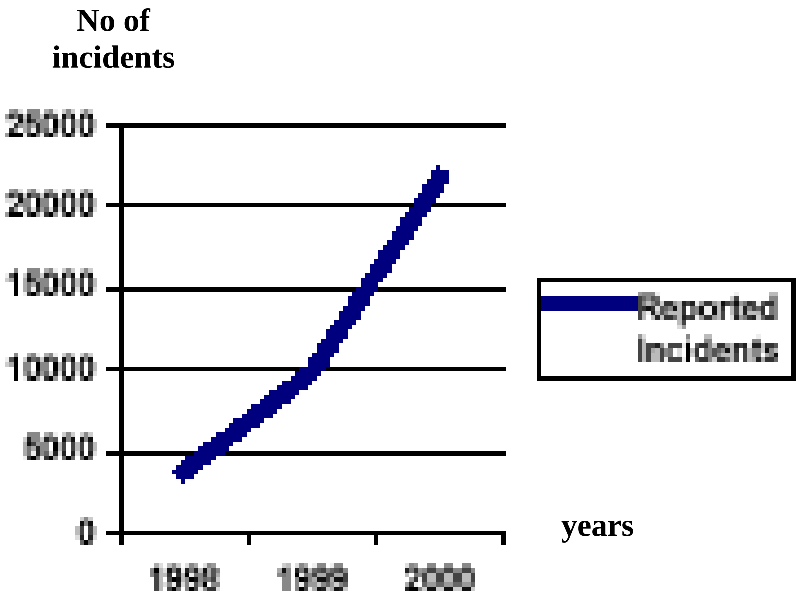


Fig.(2.2) Reported computer security incidents, 1998-2000

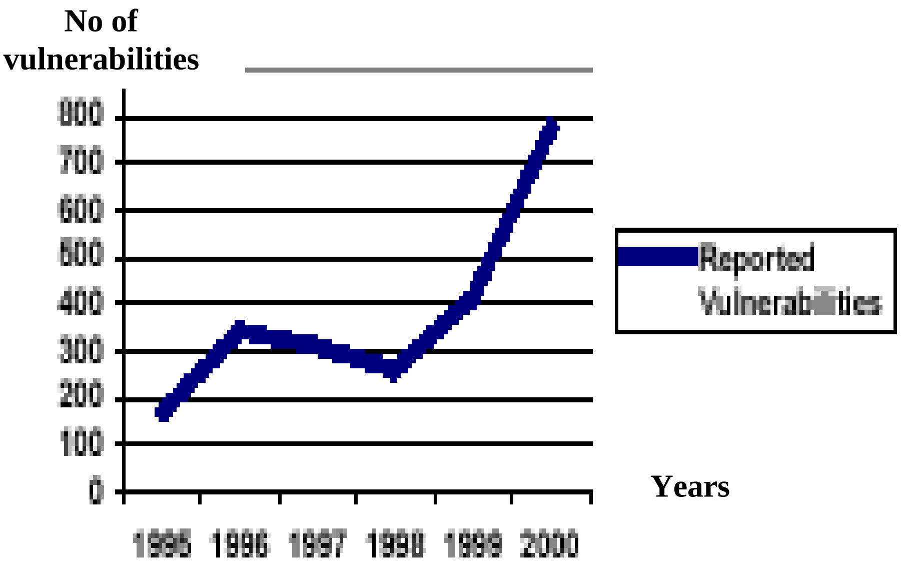


Fig.(2.3) Reported vulnerabilities, 1995-2000

2.7 Threat Assessments

Threat can be defined as the combination of capability and a hostile intent. The reason to concern about attacks upon information systems, or information war is that the means of offence are widely available, inexpensive and easy to use. Virtually anybody with a computer and technical skills could become a cracker or cyber terrorist. Moreover the progress in information technology makes the electronic tools available to conduct such attacks more sophisticated everyday, but the most dangerous feature of the IW is that it can be conducted from anywhere in the world and the possibility of discovering the attack origin, or even its presence is extremely difficult.[12]

A recent analysis listed the potential (enemies) according to the levels of threat, the lower level are the crackers, or the hackers with malicious intentions, sometimes highly knowledgeable in technical matters and very determined, but often isolated and without clear political purposes. Thus, there are some pressure groups or organizations come next that fight for specific political causes and might decide to acquire the technology in order to attack the information systems of other organization or even states. The terrorists come next in the scale: some groups are becoming increasingly sophisticated in the use of technology and conduct strategic offensive information warfare. At the higher level are the states, many of which now have access to extremely sophisticated technology and can acquire the necessary organizational infrastructure to conduct both offensive and defensive information warfare. In the last fifteen years the information systems have been subjected to attacks that have substantially increased with the growth of the internet. Due to the fast space of progress in information technology in the recent years, many actions are taken by the governments to reduce the vulnerability of nation’s infrastructure. Now if technology is helping the nations to establish better defenses, it also helps potential enemies improving their capabilities to attack. It is clear, even from the words of the most skeptical analysts ,that the security of information systems must be a high priority, with the increasing dependence on information technologies , all the vital infrastructure are potentially vulnerable to some sort of external attack. [12]

2.8 Security Defense Tools

Firewalls, anti-virus software, access control (with or without encryption), updates (patches) to software to correct security vulnerabilities and adaptive response tools currently constitute the majority of defenses against computer network attacks. Not only are these passive measures an important component of information assurance, should active defenses be employed in a preemptive or counterattack role, such defenses are likely to be encountered on hacker's systems. For this reason, we will now examine the main types of security defenses [4].

2.8.1 Firewalls

A firewall is either software, hardware or a combination of software and hardware. Analyzing incoming packets of data tries to prevent unauthorized users from accessing a network, and can be configured to do so in very specific ways. First, a firewall can screen users by point of origin; for example, restricted unclassified networks use a firewall configuration that allows only users from a recognized domain to have access. It can also be configured to allow only certain classes of users to access certain applications, third firewall can screen content; for example it can be taught to recognize and exclude executable code such as Java, or even a known attack signature. Also it can hide unused ports from scanners [4].

Configuring a firewall involves striking a balance between security and usability. The more restrictive the configuration, the less the ability to communicate freely through the network and/or between the network and the Internet. One way to work around this dynamic is to allow free access from systems known to be controlled by reputable administrators. This is called a trust relationship, and it allows efficient communication without needlessly compromising security as long as the trusted network is itself not compromised. If that happens, the attacker can exploit that trust relationship to bypass the firewall.

Effective firewall configuration also requires updates to ensure it can recognize and exclude newly discovered threats. For these reasons, a firewall is only as good as the system administrator who runs it. Once it’s penetrated, as was done to Microsoft◌ٔ s, it is no longer defending the network.

2.8.2 Antivirus Software

Effective use of antivirus software can be considered the second line of defense for a network. Viruses are simply self-replicating files, and two particular subsets of the virus family, trojans and worms, can be used to compromise a network’s security. Both contain code that will execute upon receipt of an external trigger, for example a date or a command sent by the attacker. Antivirus software can also complement a firewall by being configured to scan all incoming e-mail for known virus signatures. The increasing prevalence of centrally controlled operating systems (such as Windows NT/2000) makes it much easier for system administrators to automatically download and install updated virus signatures, and to schedule automatic virus scans, on every machine in the network[4].

2.8.3 Access Control

The simplest and longest running way to defend a network is through access control. Users are assigned different levels of permissions, which determine which directories and files they may or may not access, and may or may not alter. The most powerful access is root access, which has permission to access and alter any directory or file on the network. User access has the least permissions, and is typically restricted to those functions needed by the average account holder, for example, e-mail, web browsing, certain shared applications such as office automation, and a private directory where files created and stored [8].

Varying intermediate levels may exist, such as super user, allow the system administrators to delegate specific routine tasks. Access to an account is typically protected by a password, which creates vulnerability; e.g., if any account password can be cracked, a hacker can use various tools to crack the root account and gain access to the entire network. Passwords that are easy to remember are also easy prey for password crackers, conversely those that are difficult to guess offer increased security, but users are more likely to write them down because they are also difficult to remember, thus increasing risk of compromise.

System administrators can ensure effective password security only by encouraging users to choose passwords that are easy for each of them to remember but which are not made up of common words or phrases, and by regularly running their own password crackers to identify weaknesses. Once again, password security is only strong as long as the system administrator has the time, energy, and clout to enforce it [4].

Chapter Three

Training Systems and Computer Security

3.1 Introduction

There are many common methods which involve the computer in the training system, these methods differ from each other and the proper method will be chosen to suit the training simulator, these methods are:

i. The tutorial method: the way of showing the subjects designed to give the trainer the chance to dialogue with the computer.

ii. The drill and practice method: which is more successful in getting more skill and experience by programming the computer to give serial questions linked to feedback answers and by finishing, it will give final score and the way to avoid the wrong answers.

iii. The education games: it could be used as a serial lows and rules, works to lead the trainer for the proper reaction to accurate his skills and intelligence.

iv. The tests method: one of the most important methods which include test programs to get more accurate measurement of the trainer skills and frees the instructor from correcting the answers.

v. The problem solving method : since the (problem solving) is one of the earlier advantages of the computer, this method is preprogrammed problems executed to show the ways of solving problems by getting different results due to different inputs.

vi. Intelligent computer assisted instruction: due to the great improvement achieved in the computer system and artificial intelligence, a new field has been found to use these systems in training with computer aides by using the expert systems and simulation programs.

vii. Simulation method: this is the most useful method and used to clarify the systems basics and how it works by simulating them using similar circumstances with computer aides. This method is used to simulate the expensive and dangers systems, also it is very interesting and helps the trainer to build an imaginary picture very close to the real case which leads him to take the proper decision for a cretin situation, this gives the method the credit to be the most successful method that gives the trainer the experience and the knowledge to face the real expected problems and override them.

The information warfare simulator is quit similar to this method and uses the same techniques to simulate the most common threats that might face the user of the network systems in the information warfare field.

3.2 IW Attack Techniques

In this chapter chosen techniques have been discussed in order to cover the basics of the IW simulator design in attack mode:

3.2.1 Password Cracking

A password cracker is any program that can decrypt passwords or otherwise disable password protection. The basic idea of password crackers is a simulation tools used to utilize the same algorithm as the original password program. Through a comparative analysis, these tools try to match encrypted versions of the password to the original. Many so called password crackers are nothing but brute-force engines programs that try word after word, often at high speeds. These rely on the theory that eventually, will encounter the right word or phrase [16].

The password cracking process is divided into three steps [14]:

i. Obtaining a dictionary file, which is really no more than a flat file (plain text) list of words (these are commonly referred to as wordlists).

ii. These words are fed through any number of programs that encrypt each word.

iii. Each resulting encrypted word is compared with the target password. If a match occurs, there is better than a 90 percent chance that the password was cracked.

3.2.2 Hacking

Hacking is getting some access on a server we shouldn’t have. Servers are set up so that many people can use them. These people each have different ‘accounts’ on the server like different directories that belong just to them. The hacking process is done through certain points in the operating system commonly named as a backdoors [17].

The backdoor for most intruders provide two or three main functions:

i. Be able to get into a machine even if the administrator tries to secure it, e.g., changing all the passwords.

ii. Be able to get into the machine with the least amount of visibility.

iii. Be able to get into the machine with the least amount of time.

Also there is a backdoors types such as [17]:

i. Password cracking backdoors

ii. Login backdoor

iii. Kernel backdoor

iv. Process hiding backdoors

3.2.3 Password Sniffing

A sniffer is any device, whether software or hardware, that grabs information traveling along a network [18]. The network could be running any protocol such as:

i. Ethernet

ii. TCP/IP

iii. IPX, or others (or any combination of these).

The purpose of the sniffer is to place the network interface into promiscuous mode and by doing so, to capture all network traffic. Possible placement for sniffers is shown in Figure(3.2).

A sniffer is a significant threat because of the following [18]:

i. It can capture passwords.

ii. It can capture confidential or proprietary information.

iii. It can be used to breach security of neighboring networks.

Crackers typically sniff only the first 200-300 bytes of each packet. Contained within this portion is the username and password, which is really all most crackers, wanted. However, it is true that you could sniff all the packets on a given interface; if you have the storage media to handle that kind of volume, you would probably find some interesting things.

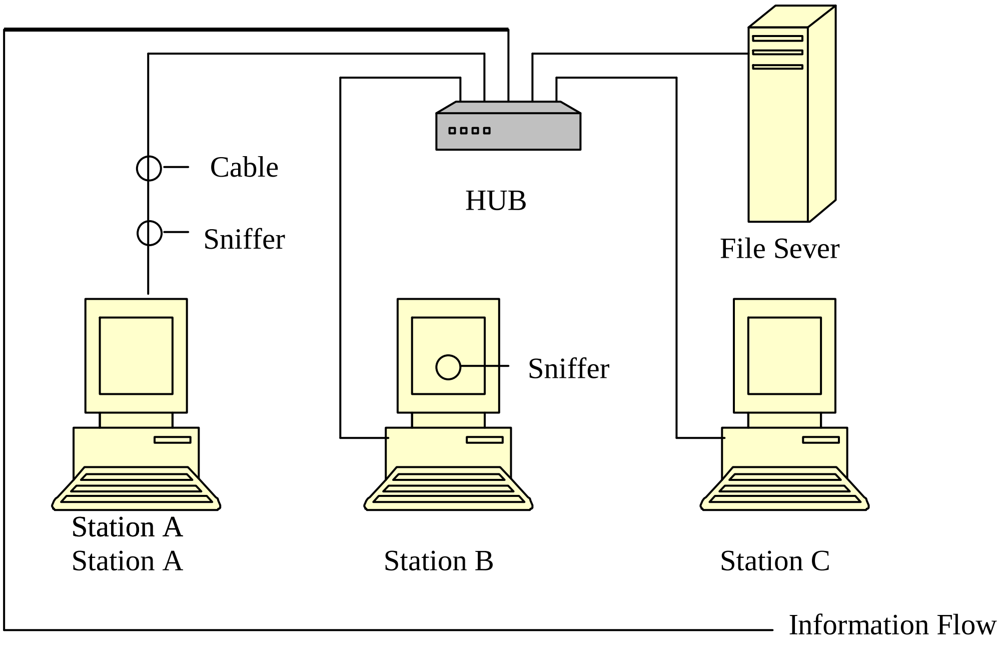


Fig.(3.2) the possible placement for the sniffer

3.2.4 E-Mail Activities

The most popular e-mail activities are [19]:

i. Worms

ii. Virus hoaxes

iii. Bombs

3.2.4.1 Worms

A worm is much like a virus, but it does not require a host program. Worms may make complete copies of themselves and spread through a network quickly, without parasitically attaching themselves to any existing files or programs [18].

Network worms run on more than one computer on an infected network at a time. Each infection on the network is referred to as "segment", with the segments making up the "body" of a network worm, and because of the way worms replicate, they often spread quickly through networked environments and e-mail, generally E-mail worms are rather new and quickly increasing type , regularly infecting large numbers of users .

3.2.4.2 Virus Hoaxes

E-mail hoaxes are becoming one of the top concerns and reported incidences. Users should not believe unsolicited e-mail, especially chain letters; it is much like junk mail. The basic idea is that an authoritative source is warning users not to read e-mail, pending disaster, and asking users to send the notice to everyone they know [18].

3.2.4.3 The e-mail Bomb

The e-mail bomb is a simple and effective harassment tool. A bomb attack consists of nothing more than sending the same message to a targeted recipient over and over again. It is a not so subtle form of harassment that floods an individual's mailbox with junk [19].

Depending upon the target, a bomb attack could be totally unnoticeable or a major problem. Some people pay for their mail service. To these individuals, an e-mail bomb could be costly. Other individuals maintain their own mail server at their house or office. Technically, if they lack storage, one could flood their mailbox and therefore prevent other messages from getting through. This would effectively result in a denial of service attack [19].

3.2.5 Viruses

A virus is a small piece of software that piggy-backs on real programs. A virus might attach itself to a program like a spreadsheet program. Each time the spreadsheet program runs, the virus runs too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc [17]. There is a wide range of virus's types such as [20]:

i. Macro Viruses
ii. Partition-Table Viruses
iii. Boot-Sector Viruses
iv. Memory-resident Viruses
v. Executable Viruses

Computer viruses are programs that must be triggered or somehow executed before they can infect your computer system and spread to

Others below are some examples [20]:

i. Opening a document infected with a "macro virus".
ii. Booting with a diskette infected with a "boot sector" virus.
iii. Double-clicking on an infected program file.
iv. Sharing infected files on a diskette, network drive, or other media.
v. Exchanging infected files over the Internet via e-mail attachments.
vi. Downloading questionable files from the Internet.

3.2.6 Port Scanning

A scanner is a program that automatically detects security weaknesses in a remote or local host. True scanners are TCP port scanners, which are programs that attack TCP/IP ports and services and record the response from the target. In this way, they glean valuable information about the target host [21].

Although the scanners are commonly written for execution on UNIX workstations, scanners are now written for use on almost any operating system. Non-UNIX scanning tools are becoming more popular now that the rest of the world has turned to the Internet. There is a special push into the Microsoft Windows NT market, because NT is now becoming more popular as an Internet server platform; however the scanners are important to Internet security because they reveal weaknesses in the network, so this information is important to the administrator as well as to the hackers or crackers [21].

3.3 IW Defense Techniques

In this section a chosen technique has been discussed in order to cover the IW simulator design in the defense mode

3.3.1 Intruder Detection

Intruder is someone attempting to break into or misuse your system. The Intrusion Detection System or IDS for short, attempts to detect an intruder breaking into a system or a legitimate user misusing system resources. The IDS will run constantly on the system, working away in the background, and only notifying when it detects something it considers suspicious or illegal [18] .

The intruder could be outside or inside one, however the inside intruder is likely more dangerous because he knows the layout of system, where the valuable data is and what security precautions are in place .The characteristics of a good intrusion detection system are[17]:

i. It must run continually without human supervision.

ii. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.

iii. On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted. .

iv. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.

v. It must observe deviations from normal behavior.

vi. It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.

vii. It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.

3.3.2 Security Check

The security check includes different kinds of policies to guarantee the system is working in it's highly performance. These policies are divided into three categories [18]:

i. Account policies cover the password handling like the age, length, complexity...etc and also the account lockout duration and threshold.

ii. Local policies cover the events, logon, and the process tracking logs, also covers the user rights like accessing, debugging, managing, and modifying.

iii. Encryption policies cover the encryption file system and IP security.

3.3.3 Network Monitoring

The monitoring system is an automated mechanism to test, track, and report on the availability and condition of the systems, services, and networks that make up a web presence.

The monitoring should cover the following issues [22]:

i. Availability.
ii. Proliferations of servers.
iii. Proliferations of services.
iv. Remote users.
v. Remote locations.
vi. Exceptions.
vii. History data.
viii. Trends.

To obtain an active monitoring system the following activities must be checked frequently [22]:

i. Network availability; typically a “ping” or connectivity test.
ii. Service availability; such as page retrieval, mail service availability, database connectivity, etc.
iii. Server health; such as system uptime, device availability, and performance, etc.
iv. Network health; such as Link state changes, routing table updates, etc.
v. Security related information; such as Failed logins, repeated operations, etc.

3.3.4 E-mail protection

E-mail has become the most important method of communication in the enterprise but viruses and spiraling spam growth seriously threaten its usefulness. The e-mail protection strategy is based on two parts [19]:

i. Multi-layer spam filtering.
ii. Multi-engine virus scanning.

The required features of e-mail protection system are:

i. Attachment filter.
ii. Content filter.
iii. Policy filter.
iv. The ability to efficiently handle thousands simultaneous e-mail users.
v. Total confidentiality and security.
vi. Virus detection.
vii. Virus cleaning.
viii. High frequency virus definition updating.

3.3.5 Virus Scanning

The virus scanner is software used to detect, identify and remove computer viruses at the server level, including messaging servers. The virus scanner gives the user a several scanning options as follows [18]:

i. Scan during startup.
ii. On-access scanning.
iii. On-demand scanning.
iv. Scan during shutdown.
v. Scheduling comprehensive scans.

Also it gives convenient types of scanning such as:

i. All Files Scanning.
ii. Files & Folders canning.
iii. Internet & E-mail Scanning.
iv. Heuristic Scanning.
v. Program Only Scanning.

However the scanners must be updated frequently because of every day new virus’s appearance.

3.3.6 Encryption

The word cryptography refers to the science of keeping secrecy of messages exchanged between a sender and a receiver over an insecure channel. The objective is achieved by encoding data so that it can only be decoded by specific individuals as shown in Figure (3.4) [22].

The original message M being wanted to be encrypted is called plaintext since it is clearly intelligible, whereas the term used to refer to the message C being transited over an insecure channel is ciphertext.

The process E of transforming a plaintext into a ciphertext is called encryption, while the opposite procedure D that turns a ciphertext into a plaintext at the receiver’s side is said decryption.

$E(M) = C$

$D(C) = M$

K = Encryption and Decryption key

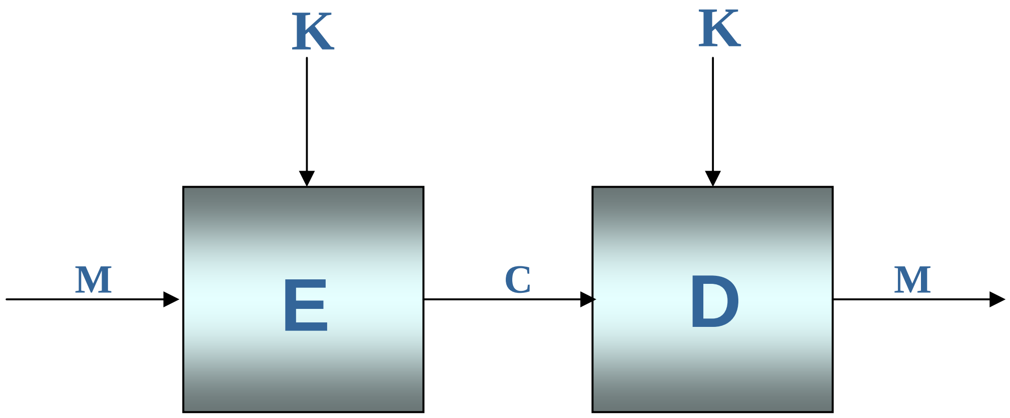


Fig.(3.3) Encryption & Decryption Processes.

A cryptographic algorithm is composed of the mathematical function used for encryption and its related inverse-function for decryption. A cryptographic algorithm is some times referred to as cipher. The security of an algorithm can rely on the secrecy of its function, when quality, standardization and mass utilization is not a concern. Cryptosystems can be classified into [22]:

i. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

ii. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.

iii. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block.

A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

3.3.6.1 Symmetric Key Cryptography

All cryptographic algorithms involve substituting one thing for another, for example, taking a piece of plaintext and then computing and substituting the appropriate ciphertext create the encrypted message. Caesar cipher is the well known old method for this type of cryptography [25].

3.3.6.2 Public Key Cryptography

For more than 2000 years (since the time of Caesar cipher and up to the 1970s), encrypted communication required that the two communicating parties share common secrets-the symmetric key used for encryption and decryption. One difficulty with this approach is hat the two parties must somehow agree on the shared key; but to do so requires (presumably secure) communication. Perhaps parties could firs meet and agree on the key in person and thereafter communicate with encryption. In a networked world, however, communicating parties may never meet and may never converse except over the network. It is possible for two parties to communicate with encryption without having a shared secret key that is known in advance? In 1976, Diffie and Hellman [Diffie 1976] demonstrated an algorithm known as Diffie-Hellman Key Exchange. To do just that- a radically different and marvelously elegant approach toward secure communication that has led to the development of today's public key cryptography systems. Public key cryptography systems have wonderful properties that make them useful not only for encryption but for authentication and digital signature as well [25].

3.3.6.3 Cryptographic Algorithms

There are many cryptographic algorithms. These are three of the most common [26]:

- DES (Data Encryption Standard) is the most popular encryption algorithm. DES is U.S. and international standard. It is a symmetric algorithm; the same key is used for encryption and decryption.
- RSA (named for its creators –Rivest, Shamir, and Adleman) is the most popular public key algorithm. It can be used for both encryption and digital signatures.
- DSA (Digital Signature Algorithm, used as part of Digital Signature Standard) is another public- key algorithm. It can not be used for encryption, but only for digital signatures.

3.4 Integrity

Think of the number of times you've signed your name to a piece o paper during the last week. You sign checks, credit card statements, legal documents, and letters. Your signature attests to the fact that you (as opposed to someone else) have acknowledged and/or agreed with the document's contents. In a digital world, one often wants to indicate the owner or creator of a document, or to signify one's agreement with document's content. A digital signature is a cryptographic technique or achieving these goals in a digital world [25].

3.4.1 Digital Signature

Handwritten signatures have been long used as proof of authorship of, or at least agreement with the contents of a document. What is about a signature that is so compelling [26]:

1. The signature is authentic. The signature convinces the documents recipient that the signer deliberately signed the document.
2. The signature is unforgeable. The signature is proof that the signer, and no one else, deliberately signed the document.
3. The signature is not reusable. The signature is part of the document an unscrupulous person can not move the signature to different document.
4. The signed document is unalterable after the document is signed, it can not be altered.
5. The signature can not be repudiated. The signature and the document are physical things. The signer cannot later claim that he or she didn't sign it.

In reality, none of these statements about signatures is completely true. Signatures can be forged, signatures can be lifted from one piece of paper and moved to another, and documents can be altered after signing. However, we are willing to live with these problems because the difficulty in cheating and the risk of detection [26].

We would like to do this sort of thing on computers, but there are problems. First, computer files are trivial to copy. Even if a person's signature were difficult to forge (a graphical image of a written signature, for example), it would be easy to cut and paste a valid document from one document to another document. The mere presence of such signature means nothing. Second, computer files are easy to modify after they are signed, without leaving any evidence of modification [26].

3.4.2 Algorithms of Digital Signature

There are many digital signature algorithms. All of them are public-key algorithms with secret information to sign documents and public information to verify signatures. Sometimes the signing process is called decrypting with public key. This is misleading and is only rue for one algorithm, RSA. And deferent algorithms have deferent implementations. For example, one way hash functions and timestamps sometimes add extra steps to the process of signing and verifying. Many algorithms can be used for digital signatures, but not for encryption [26].

In general, I will refer to the signing and verifying process without any details of the algorithms involved. Signing message with private key K is:

$$S_k(M)$$

And verifying a signature with the corresponding public key is:

$$V_k(M)$$

The bit string attached to the document when signed will be called the digital signature, or just the signature. The entire protocol, by which the receiver of a message is convinced of the identity of the sender and the integrity of the message is called authentication [26].

3.5 Authentication

Authentication is the process of providing one's identity to someone else. As humans, we authenticate each others in many ways: we recognize each other's voices on the telephone, we are authenticated by the customs official who checks us against the picture of our passport [25].

When performing authentication over the network, the communicating parties cannot rely on biometric information, such as visual appearance or a voiceprint. Indeed, that will be done through authentication protocol [25].

Typically, an authentication protocol would run before the two communicating parties run some other protocol (for example, a reliable data transfer protocol, an e-mail protocol). The authentication protocol first establishes the identities of the parties to each others' satisfaction; only after authentication do the parties get down to work at hand [25].

Chapter 4

Computer Aided Security System Design and Implementation

4.1 Introduction

Armies use firing ranges to train solders on individual weapons and firing systems. Likewise, the IW lab is a range where users and faculty may lunch and experiment the cyber attack from the firing poison (computer terminal) in the lab at a target computers. The weapons here could be viruses, worms, port scanners, Trojan horses, and vulnerability scanners without the risk of releasing malicious code onto production network or into the outside networks. Just as a solder would only fire a weapon on the range or in combat, the IW network policy should only permit users to use the malicious tools in controlled confines of the lab. This situation provides a safe and authorized location to conduct training since there is no physical connection to outside networks and to have more of the firing range. It is more recommended if the lab consists of several networks, each network with different operating system, in order to give the user the chance of dealing with multi operating systems and expand the capability of the firing range. Moreover, to be more organized the idea of making the first network operating with low level security and the second with high level security shows the benefit of targeting easy and difficult targets. The ideal target in the firing range is the server, because it has the high level security and damage occurs is greater than the damage occurs to the stations. More useful situation brought up by having multi-networks lab so it can be used to target a computer in the same network as well as a computer in the connected network. This improves the skills of the attack as well as the defense because the user must recognize the source of the attacker (the fire, in the military) in the first step and to defend his computer in the second step. This picture is shown clearly in the real world when the networks have an inside and outside intruders or hackers. To get more of the physical building of the IW range, it is useful to separate the other networks in a different location (out of sight) so it will simplify the administration and the setup of the lab [23].

4.2 Computer Aided Learning System Implementation:

The developed computer network warfare is designed to achieve both objectives of network security which are the attack stage and defense stage. Symmetrical correspondence is one of the important design objectives in order to clarify the attack and defense actions for each type. The main parts of the designed warfare are:

i. Application system.
ii. Documentation system.

The application system consists of an application of each technique in both cases, attack and defense; where the documentation system contains of a brief description about each one of these techniques.

The block diagram of the IW simulator is shown in Figures (4.1) and (4.2).

The attack system consists of six cases; these are cracking, hacking, password sniffing, e-mail activities, and viruses and port scanning. These six cases represent the major attack types, which are common in computer networks. It may be extended to include other types of attacks. The system involves description, concepts, demonstration, strategies, design and implementation of each case of the attack.

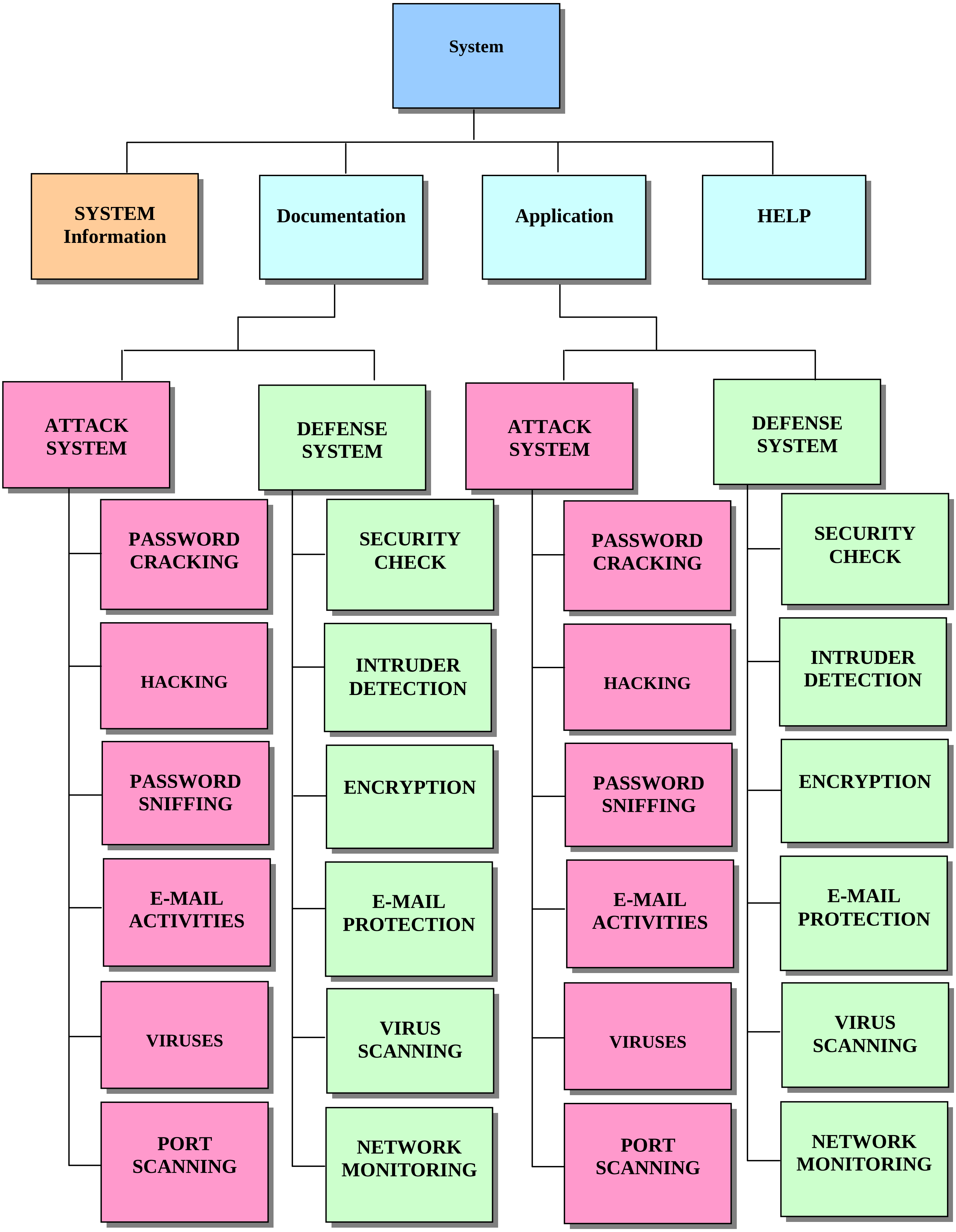


Fig. (4.1) block diagram of the IW simulator

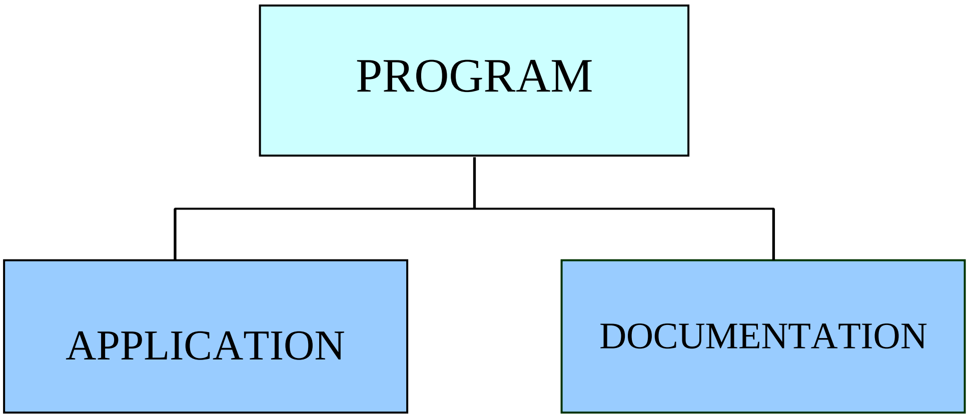


Fig.(4.2) corresponding application and documentation of each case

In the developed IW simulator these six cases can be called by user using the main menu of the attack mode shown in Figure (4.3).

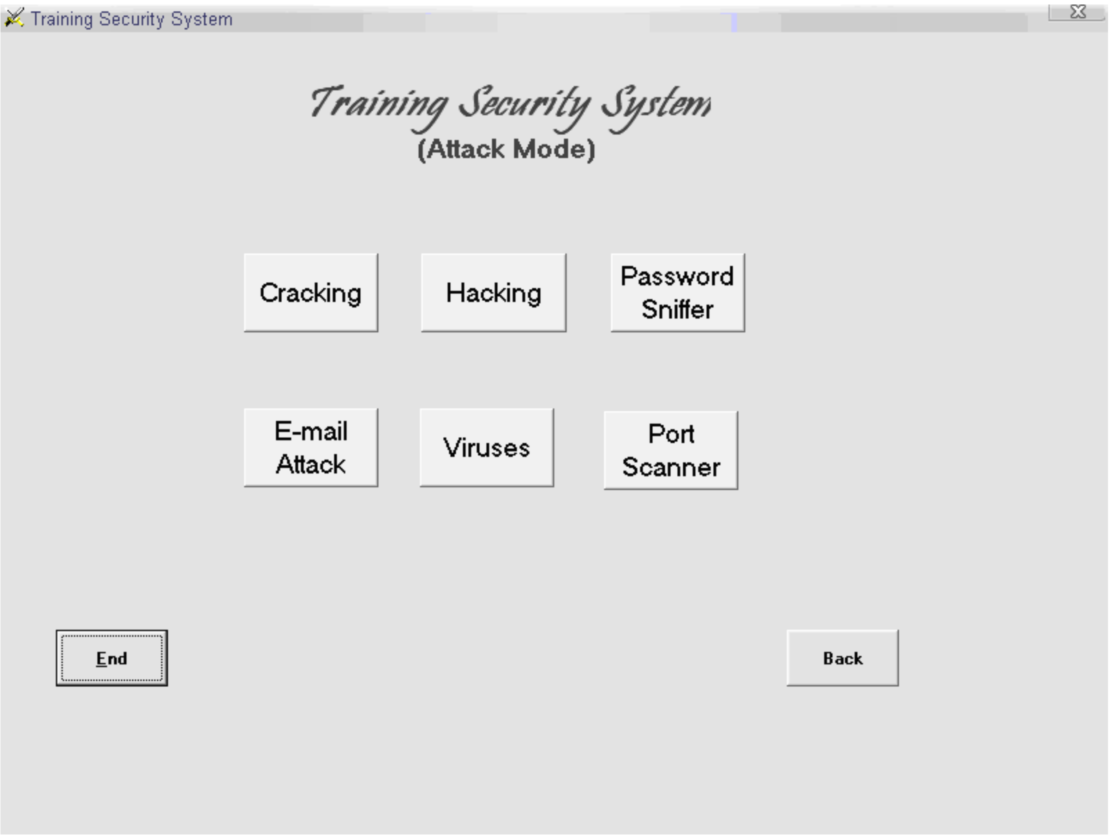


Fig.(4.3) Attack system window

In the defense system also six cases are considered, these are: intruder detection, security check, network monitoring, e-mail protection, virus scanning and encryption. These six categories of defense actions can be considered as the proper defense action for each of the corresponding attack action in the attack system. The concept, strategy, and implementation for each one of these six defense actions will be considered individually.

In the developed IW simulator these six cases can be called from the main defense menu shown in Figure (4.4).

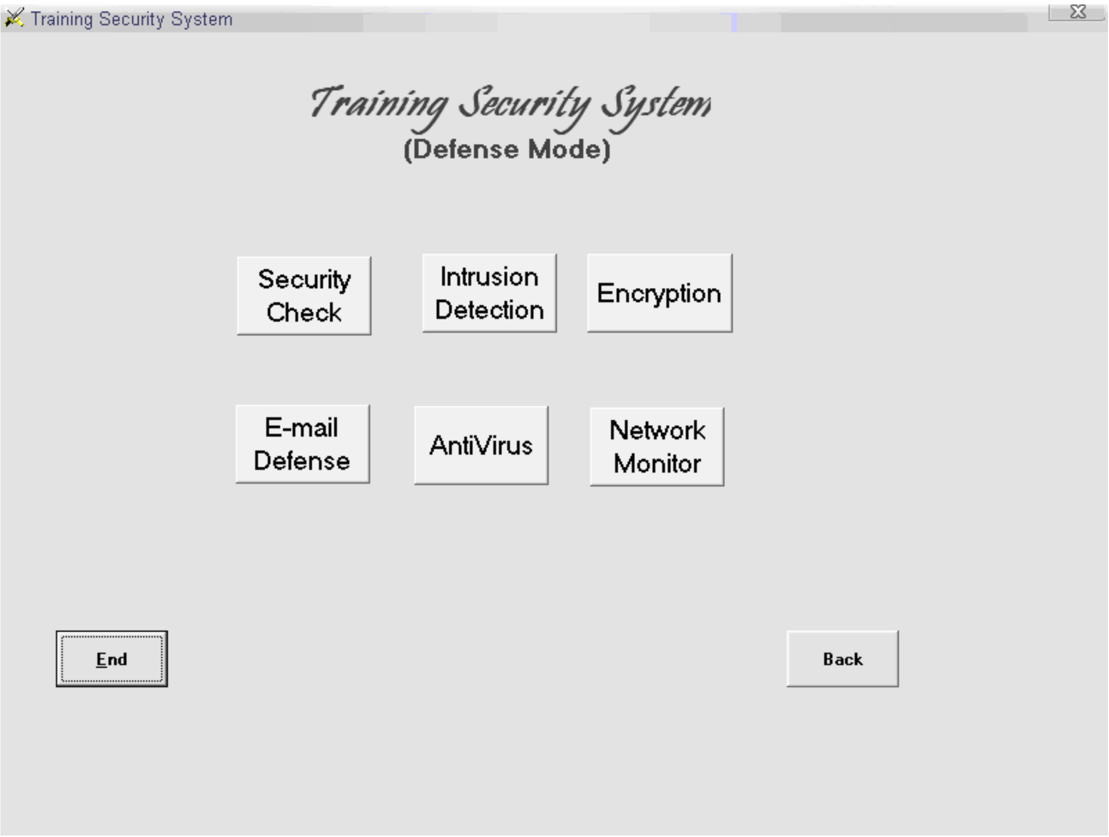


Fig.(4.4) Defense system window

There are action correspondence between attack system and defense system as shown below:

Cracking → Security Check

Hacking → Intruder Detection

Password sniffing → Encryption

E-mail activities → E-mail protection

Viruses → Virus Scanning

Port scanning → Network monitoring

In both systems of defense and attack a basic documentation for each individual case is included to give the end user an idea about the strategy of each defense or attack action. The documentations are collected from different resources and were embedded in the warfare program as shown in Figures (4.5) and (4.6).

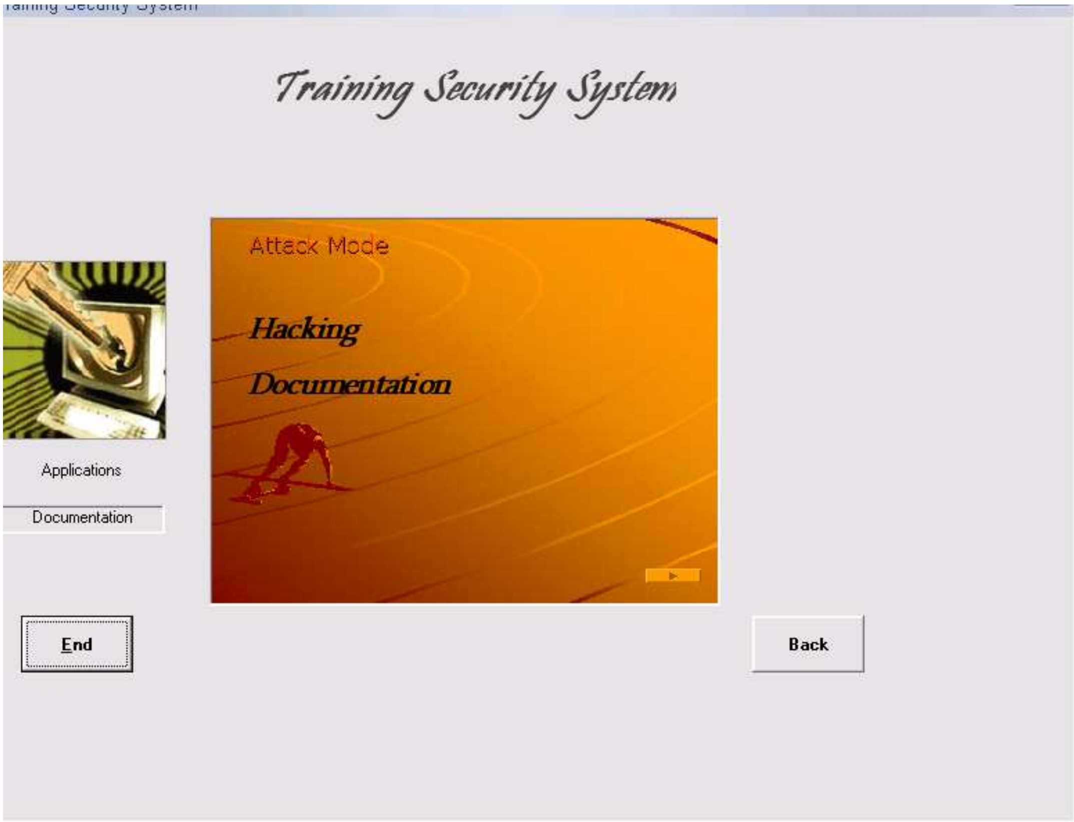


Fig.(4.5) Attack system documentation window

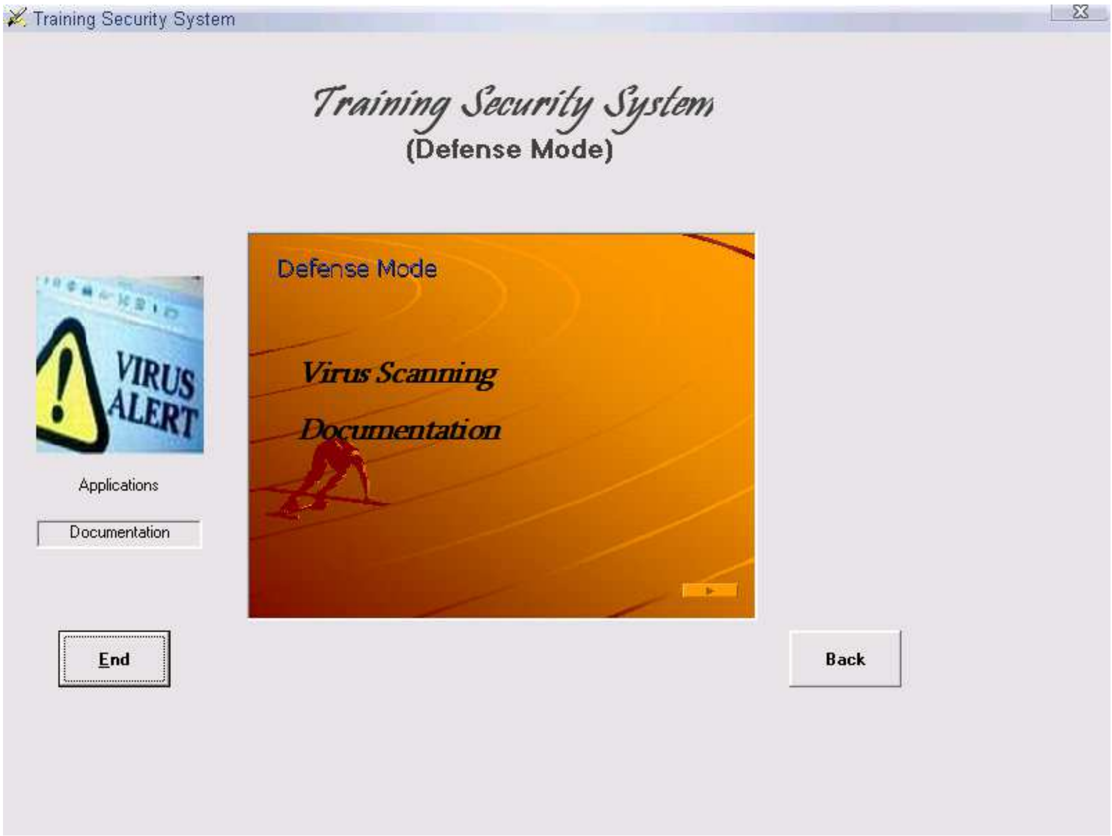


Fig.(4.6) Defense system documentation window

The user interface is developed using visual basic. The (e-mail activities, e-mail protection, and viruses, virus scanning, and encryption) programs are developed and implemented using visual basic as simulation programs that works on LAN. While the rest of the programs are included inside the warfare as ready programs taken from different resources.

One program of each one of the attack and defense activities has been added. This program is one of the well known programs of each activity. The user has the ability to run that program, to view the information regarding that program, or to remove that program as in shown Figure (4.7).

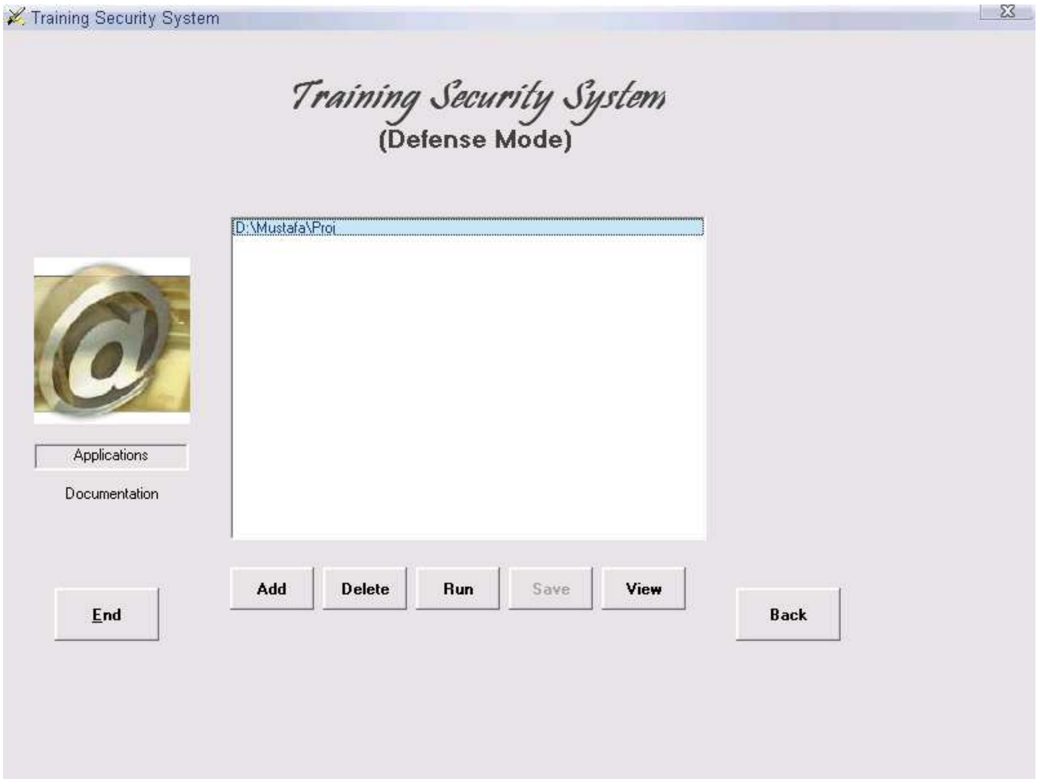


Fig.(4.7) how to delete, run or remove a program

The user can view the attributes o each program in the program list as entered during the program addition as in Figure (4.9).

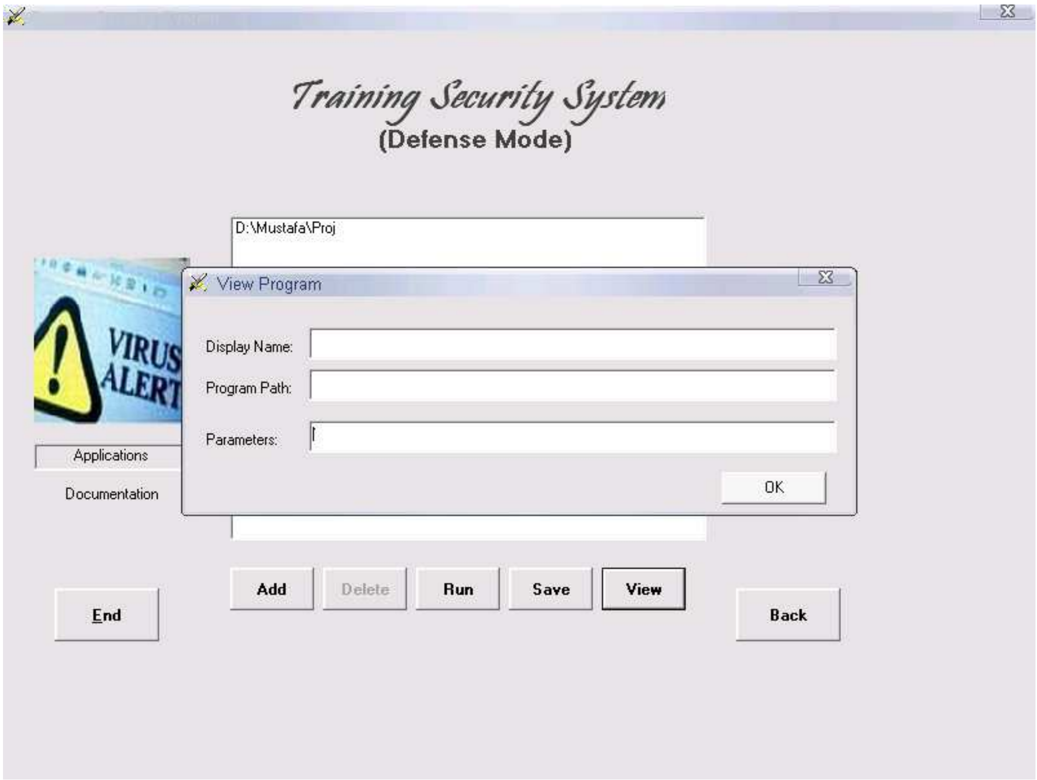


Fig.(4.9) viewing program info.

The user also has the ability to add new program to each activity. This property enabled the user to execute new programs which makes the system more flexible and increases the benefits that the system was designed for as shown in figure (4.8).

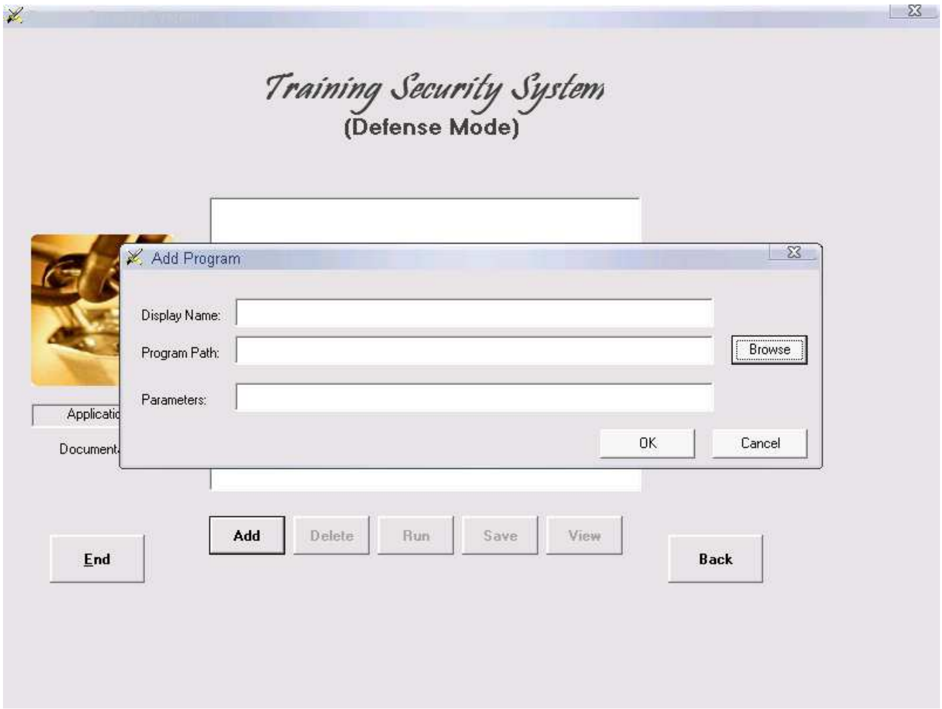


Fig.(4.8) adding new programs

4.3 Attack System Design and Implementation

4.3.1 Password Cracking

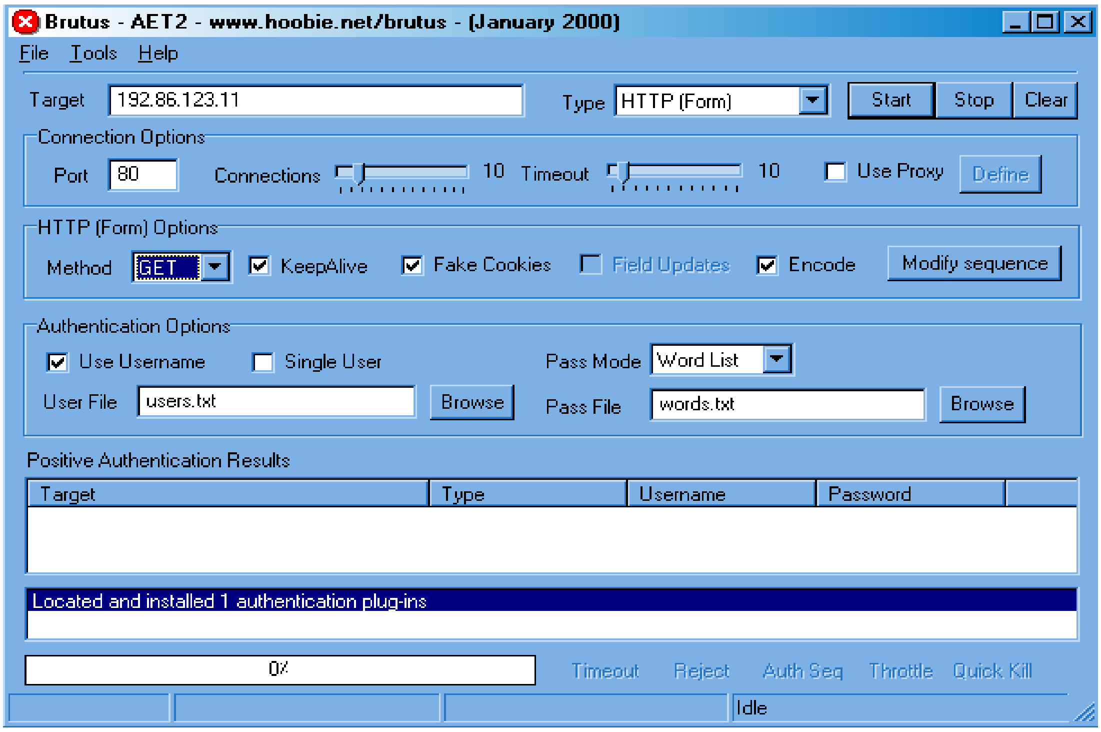
The cracking techniques can be achieved by the following steps:

i. Obtaining a dictionary file, which is really no more than a flat file (plain text) list of words (these are commonly referred to as wordlists).

ii. These words are fed through any number of programs that encrypt each word. Such encryption conforms to the DES standard.

iii. Each resulting encrypted word is compared with the target password. If a match occurs, there is better than a 90 percent chance that the password was cracked.

The implemented program that achieves the above procedure called Brutus AET2 as shown in Figure (4.9).



Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

Target 192.86.123.11 Type HTTP (Form)

Connection Options

Port 80 Connections 10 Timeout 10 ☐ Use Proxy

HTTP (Form) Options

Method GET ☑ KeepAlive ☑ Fake Cookies ☐ Field Updates ☑ Encode

Authentication Options

☑ Use Username ☐ Single User Pass Mode Word List

User File users.txt Pass File words.txt

Positive Authentication Results

Target	Type	Username	Password

Located and installed 1 authentication plug-ins

0%

Idle

Fig.(4.9) Brutus program for password cracking

In simple terms, Brutus is an online or remote password cracker. More specifically it is a remote interactive authentication agent. Brutus is used to recover valid access tokens (usually a username and password) for a given target system. Examples of a supported target system might be an FTP server, a password protected web page, a router console a POP3 server… etc. It is used primarily in two contexts:

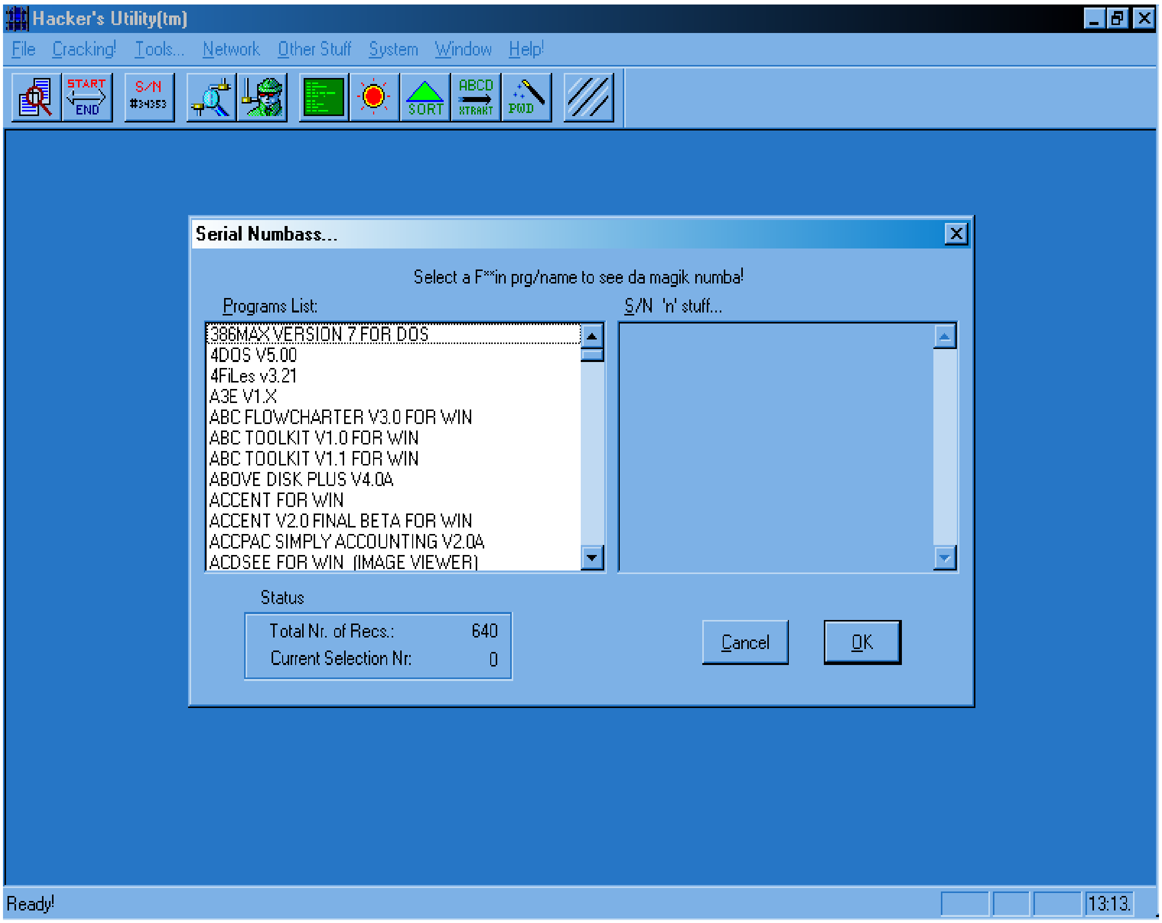
i. To obtain the valid access tokens for a particular user on a particular target.

ii. To obtain any valid access tokens on a particular target where only target penetration is required.

An attack method in the context of Brutus is a service provided by the target that allows a remote client to authenticate against the target using client supplied credentials. For instance a UNIX server sat on a network somewhere may be offering Telnet and FTP services to remote users. Both telnet and FTP require the remote user to authenticate themselves before access is granted. For both these services the required credentials are usually a username and a password. Therefore we have two available attack methods, FTP or Telnet. Some target systems will provide no opportunity for attack (at least not a remote authentication attack). They might offer no remote services, anonymous remote services (that require no authentication) or perhaps they offer authenticated remote services but use mechanisms to prevent authentication attacks such as account lockout or one time passwords of some sort.

4.3.2 Hacking

The hacker’s utility program v1.02 provided by DirectX and ATAPI is used as an example for hacking tools as shown in Figure (4.10).



Select a F**in prg/name to see da magik numba!

Programs List:

386MAX VERSION 7 FOR DOS
4DOS V5.00
4FiLes v3.21
A3E V1.X
ABC FLOWCHARTER V3.0 FOR WIN
ABC TOOLKIT V1.0 FOR WIN
ABC TOOLKIT V1.1 FOR WIN
ABOVE DISK PLUS V4.0A
ACCENT FOR WIN
ACCENT V2.0 FINAL BETA FOR WIN
ACCPAC SIMPLY ACCOUNTING V2.0A
ACDSEE FOR WIN (IMAGE VIEWER)

S/N 'n' stuff...

Status

Total Nr. of Recs.:	640
Current Selection Nr:	0

Fig.(4.10) Hacker’s utility program V1.02 window

The features and capabilities provided by hacker's utility 1.02

a. Manual Extract with specified offsets and outfile name.
b. It is good for ripping much stuff...
c. Low-Level System Functions (like: Run, NT Remote Shutdown, etc.)
d. Cracks password protected .ZIP archives!
e. Creates dummy files with random & optional buffer
f. Include a Hacker's Test
g. Binary file(s) compare...
h. Cracks password files
i. Full cracking status

j. Extract words from text or binary files.

k. Sort words

l. Words Wizard

m. Network/TCP-IP tools...

n. Ideated Server with custom ID

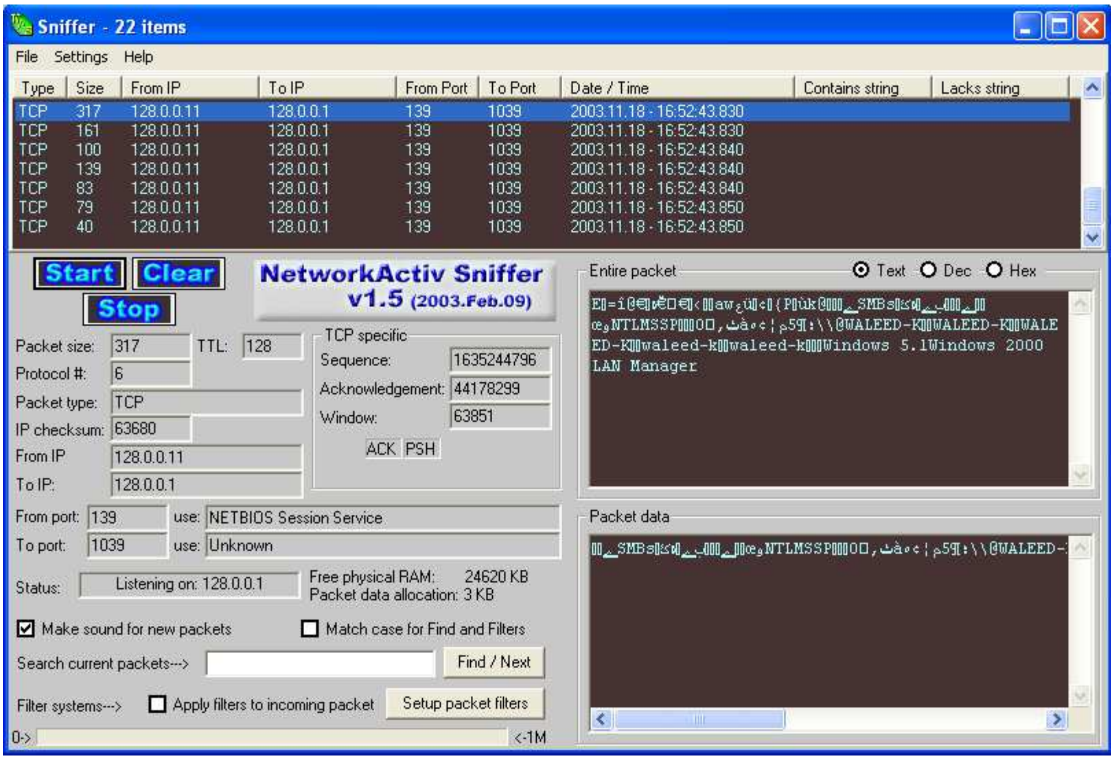
o. Finger

p. Port Scanner

4.3.3 Password Sniffing

The implemented program is the networkactiv sniffer V1.5 provided by NetworkActiv. This program has two sniffer modes:

i. Packet sniffer mode; used for the reception of all TCP/IP packets form a network interface (NIC/Modem) as shown in Figure (4.11).



Type	Size	From IP	To IP	From Port	To Port	Date / Time	Contains string	Lacks string
TCP	317	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.830		
TCP	161	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.830		
TCP	100	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.840		
TCP	139	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.840		
TCP	83	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.840		
TCP	79	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.850		
TCP	40	128.0.0.11	128.0.0.1	139	1039	2003.11.18 - 16:52:43.850		

Packet size: 317 TTL: 128
Protocol #: 6
Packet type: TCP
IP checksum: 63680
From IP 128.0.0.11
To IP: 128.0.0.1

TCP specific
Sequence: 1635244796
Acknowledgement: 44178299
Window: 63851
ACK PSH

From port: 139 use: NETBIOS Session Service
To port: 1039 use: Unknown

Status: Listening on: 128.0.0.1
Free physical RAM: 24620 KB
Packet data allocation: 3 KB

☑ Make sound for new packets
□ Match case for Find and Filters
Search current packets--->
Filter systems--->
□ Apply filters to incoming packet

Entire packet ● Text ○ Dec ○ Hex

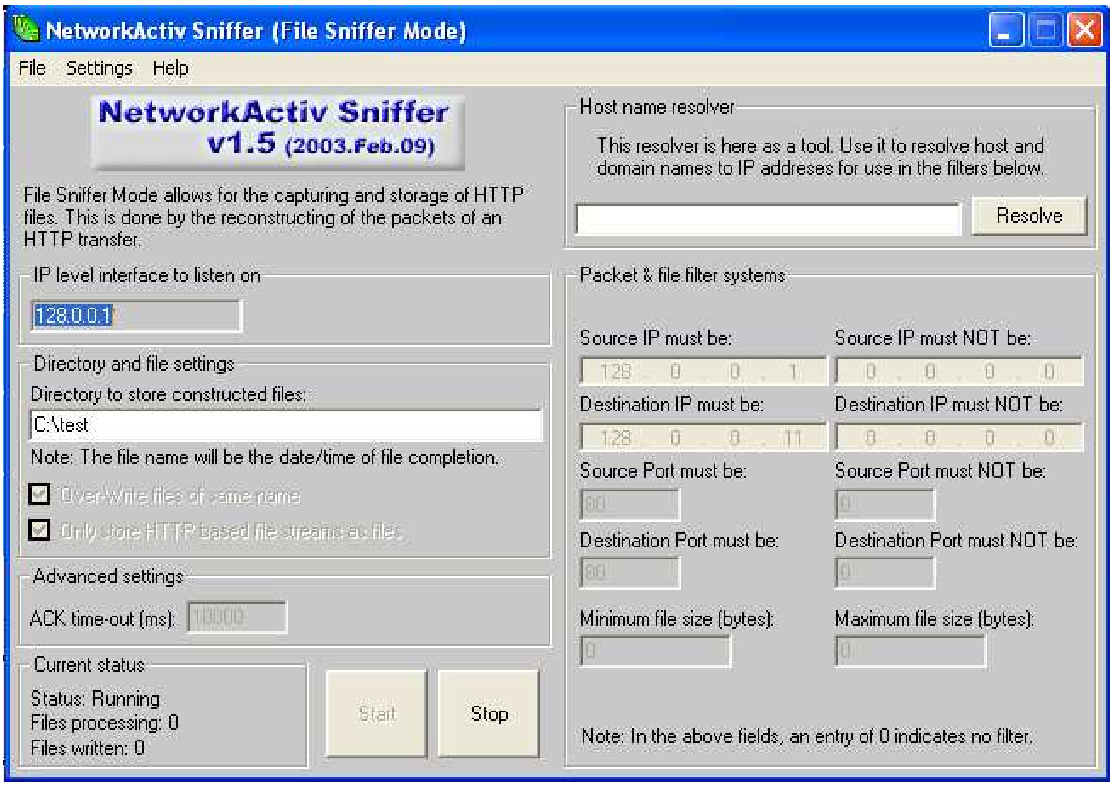
```
E=î@€ê€<aw¿ü¢{Pùk@_SMBs_ب__
œ,NTLMSSPOO,ثà∘¢¦م5¶:\\@WALEED-KWALEED-KWALE
ED-Kwaleed-kwaleed-kWindows 5.1Windows 2000
LAN Manager
```

Packet data

```
_SMBs_ب__œ,NTLMSSPOO,ثà∘¢¦م5¶:\\@WALEED-
```

Fig.(4.11) Packet sniffer mode

ii. File sniffer Mode; used for capturing and storage of HTTP based files form a network interface (NIC/Modem) as shown in Figure (4.12).



File Sniffer Mode allows for the capturing and storage of HTTP files. This is done by the reconstructing of the packets of an HTTP transfer.

IP level interface to listen on: 128.0.0.1

Directory and file settings

Directory to store constructed files: C:\test

Note: The file name will be the date/time of file completion.

☑ OverWrite files of same name

☑ Only store HTTP based file streams as files.

Advanced settings

ACK time-out (ms): 10000

Current status

Status: Running
Files processing: 0
Files written: 0

Host name resolver

This resolver is here as a tool. Use it to resolve host and domain names to IP addresses for use in the filters below.

Packet & file filter systems

Source IP must be: 128 . 0 . 0 . 1

Source IP must NOT be: 0 . 0 . 0 . 0

Destination IP must be: 128 . 0 . 0 . 11

Destination IP must NOT be: 0 . 0 . 0 . 0

Source Port must be: 80

Source Port must NOT be: 0

Destination Port must be: 80

Destination Port must NOT be: 0

Minimum file size (bytes): 0

Maximum file size (bytes): 0

Note: In the above fields, an entry of 0 indicates no filter.

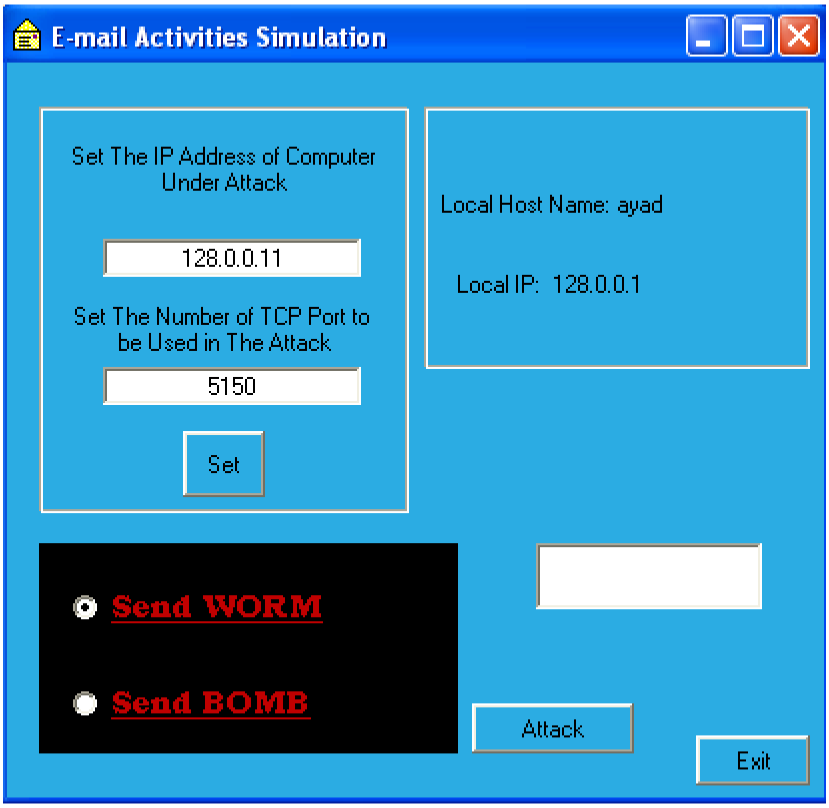
Fig.(4.12) File Sniffer mode

This program will only capture packets on the IP level protocol and above. Under normal circumstances (an Ethernet adapter with standard LAN style setup), this program will usually capture all packets that have a destination IP address of the local machine, and all packets that have a source IP address of the local machine. However, under running the program on the server of Internet connection sharing or with VPN, the program may capture packets that have neither a source nor destination IP address of the local machine. It must be noted that this program does not put the network card/device into promiscuous mode. Thus the program will only capture packets destined for or sent from the machine in which it is running.

4.3.4 E-mail Activities

The implemented program for e-mail activities program used in this attack is implemented using visual basic programming language in order to simulate the attack action of making worms and bombs spread through messages. This program works on LANs to transmit codes of worms and bombs that must be detected by the corresponding e-mail protection program mentioned in defense stage. The two programs must work at the same time on different PC's of a single LAN.

The program shows information about the host computer name and IP. The IP address of the computer to be attacked must be entered with a port number to be used in the attack. Therefore the program makes a winsock connection and sends the codes correspondingly to the node under the simulated attack as shown in Figure (4.13).



Set The IP Address of Computer Under Attack: 128.0.0.11

Set The Number of TCP Port to be Used in The Attack: 5150

Local Host Name: ayad

Local IP: 128.0.0.1

● Send WORM

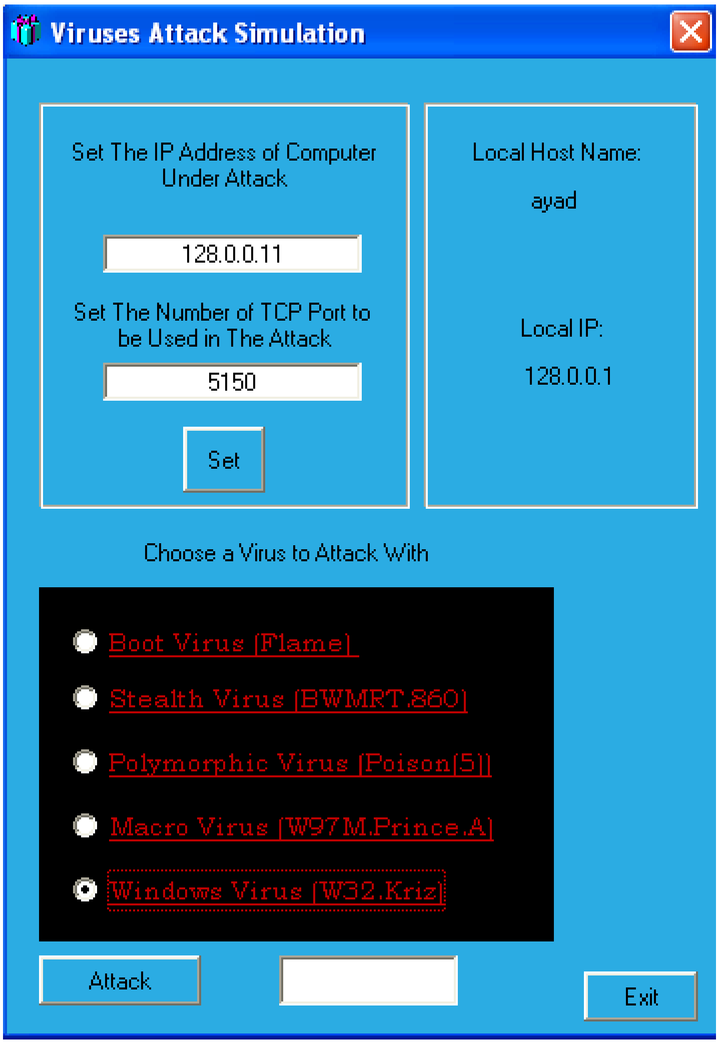
○ Send BOMB

Fig.(4.13) The e-mail activities simulation window

The figure shows an example of an e-mail attack activity, an IP address of the computer to be attacked (128.0.0.11) is set also the TCP port (5150) to be used for establishing the connection with target computer. By clicking on (set) button, the winsock connection will initiate. The second step is to choose the type of attack (worm or bomb) and finally by pressing the (attack) button the target computer will be attacked by the specified action.

4.3.5 Viruses

Viruses attack used in this attack type was implemented using visual basic programming language in order to simulate the virus attack action through networks. This program works on LANs and sends codes of viruses to be detected by the corresponding virus scanning defense program. The two programs must work at the same time on different PC's of a single LAN. The program shows information about the host computer name and the local IP address. IP address of the computer to be attacked must be entered with a port number so that the program makes a winsock connection before sending virus codes as shown in Figure (4.14).



Viruses Attack Simulation

Set The IP Address of Computer Under Attack

128.0.0.11

Set The Number of TCP Port to be Used in The Attack

5150

Local Host Name:

ayad

Local IP:

128.0.0.1

Choose a Virus to Attack With

○ Boot Virus (Flame)

○ Stealth Virus (BWMRT.860)

○ Polymorphic Virus (Poison(5))

○ Macro Virus (W97M.Prince.A)

● Windows Virus (W32.Kriz)

Fig.(4.14) virus attack simulation program

In the figure shown, the target computer with IP address (128.0.0.11) is chosen, also the TCP port number is set in the field in order to initiate a winsock connection. By pressing the (set) button the connection should be initiated, after choosing the type of virus as shown in the list, (W32.Kriz). For example, a button (attack) finally will start the virus attack simulation.

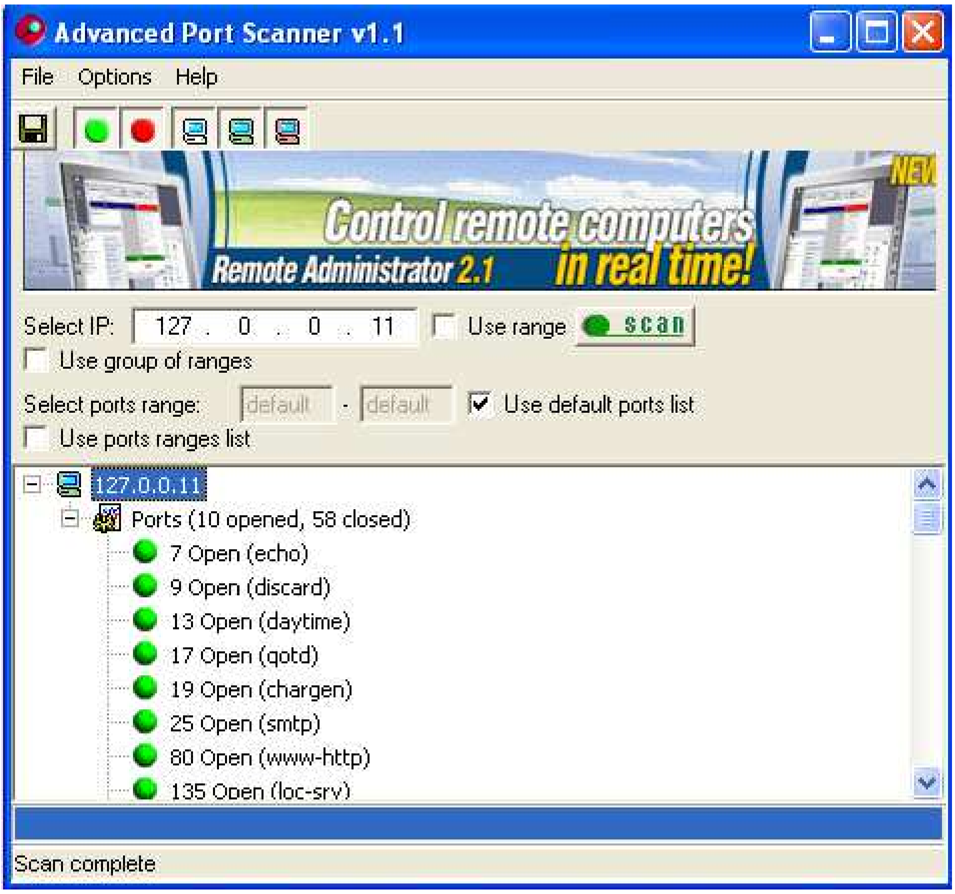
4.3.6 Port Scanning

The implemented program (Advanced port scanner V1.1) provided by www.radmin.com is used as an example for sniffing programs. Advanced port scanner is a small, very fast, easy-to-use and robust port scanner for the Win32 platform. It is multithreaded, so on fast machines; it can scan ports in very a few seconds. It has descriptions for the common ports and can perform scan on predefined port ranges.

By default, there is one edit box to enter a target IP, two edit boxes to enter the first and last ports in a range to be scanned, a checkbox to use the default port range and the scan button. By clicking on the use range checkbox, the edit box for the second IP will show up so we can scan a range of IP's.

To perform a complex scan on different networks, one can select the use group of ranges checkbox. In this mode, additional options have to added, deleted and/or updated groups of IP's. You can also save and load a list of IP's. The same options can be called for ports to scan a complex variety of ports with the maximum speed.

Pressing the scan button initiates the scan. The toolbar has another scan button that you can use at any time. When scanning, the computer's icons are shown in the report window. Clicking on a computer's icon and then its ports, it will display a list of the ports being scanned on each machine as shown in Figure (4.15).



Select IP: 127 . 0 . 0 . 11 □ Use range
□ Use group of ranges
Select ports range: default - default ☑ Use default ports list
□ Use ports ranges list

```
⊟ 127.0.0.11
   ⊟ Ports (10 opened, 58 closed)
        ● 7 Open (echo)
        ● 9 Open (discard)
        ● 13 Open (daytime)
        ● 17 Open (qotd)
        ● 19 Open (chargen)
        ● 25 Open (smtp)
        ● 80 Open (www-http)
        ● 135 Open (loc-srv)
```

Scan complete

Fig.(4.15) the advanced port scanner V 1.1

4.4 Defense System Design and Implementation

4.4.1 Intruder Detection

The implemented program SuperScan 3.00 is used to give an example about the way used to keep intruders away or at least detecting them. SuperScan is a TCP port scanner, pinger and hostname resolves as shown in Figures (4.16) and (4.17) it can do the following:

i. Perform simple ping tests to tell whether a remote computer is alive.

ii. Resolve hostnames into IP addresses and reverse lookup IP addresses into hostnames.

iii. Attempt to connect to other computers on a TCP network to see what services they are running.

iv. Read responses from connected hosts.

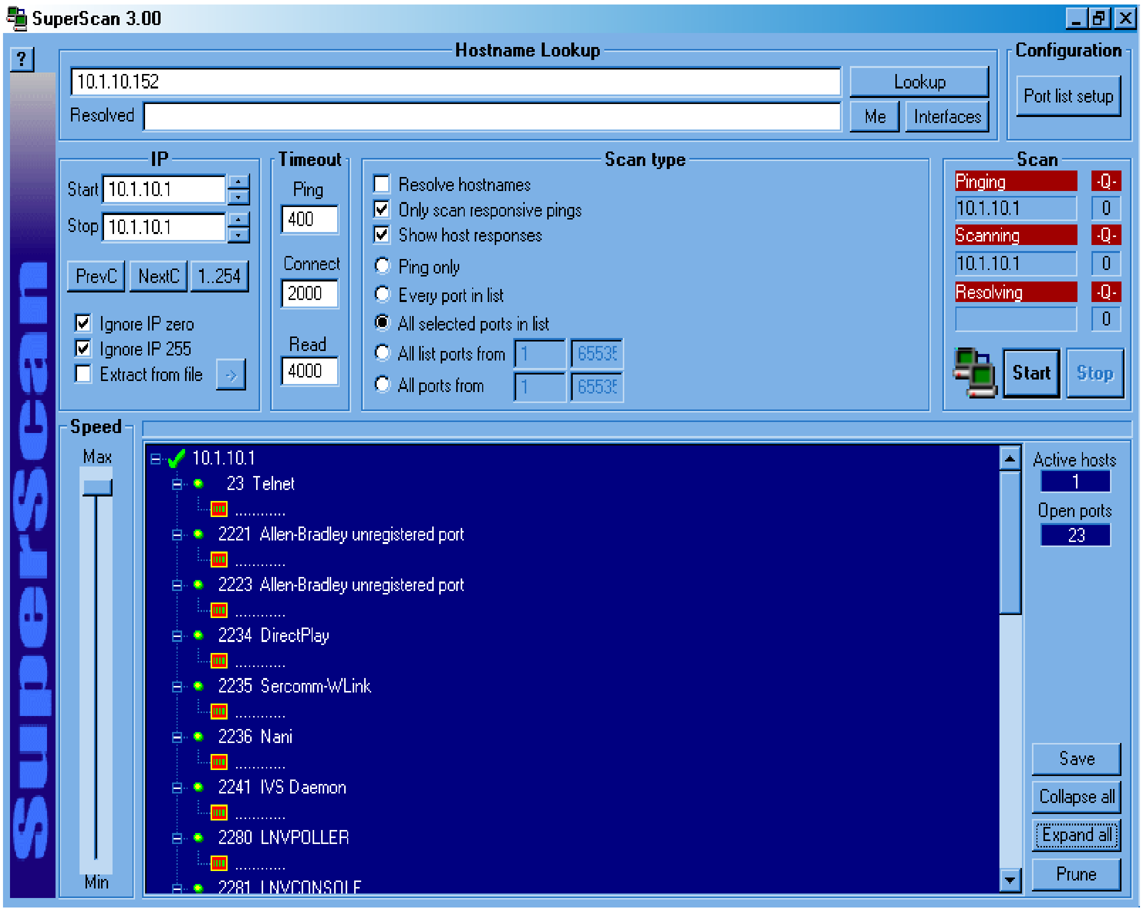
v. Scan from a range of addresses and ports.

vi. Scan from a list of ports.

vii. Scan from selected ports from a list.

viii. Scan a list of hostnames contained in a text file.

ix. Detect a trojan port.



SuperScan 3.00

Hostname Lookup: 10.1.10.152

Resolved:

IP

Start 10.1.10.1

Stop 10.1.10.1

☑ Ignore IP zero

☑ Ignore IP 255

☐ Extract from file

Timeout

Ping 400

Connect 2000

Read 4000

Scan type

☐ Resolve hostnames

☑ Only scan responsive pings

☑ Show host responses

○ Ping only

○ Every port in list

● All selected ports in list

○ All list ports from 1 65535

○ All ports from 1 65535

Scan

Pinging -0-

10.1.10.1 0

Scanning -0-

10.1.10.1 0

Resolving -0-

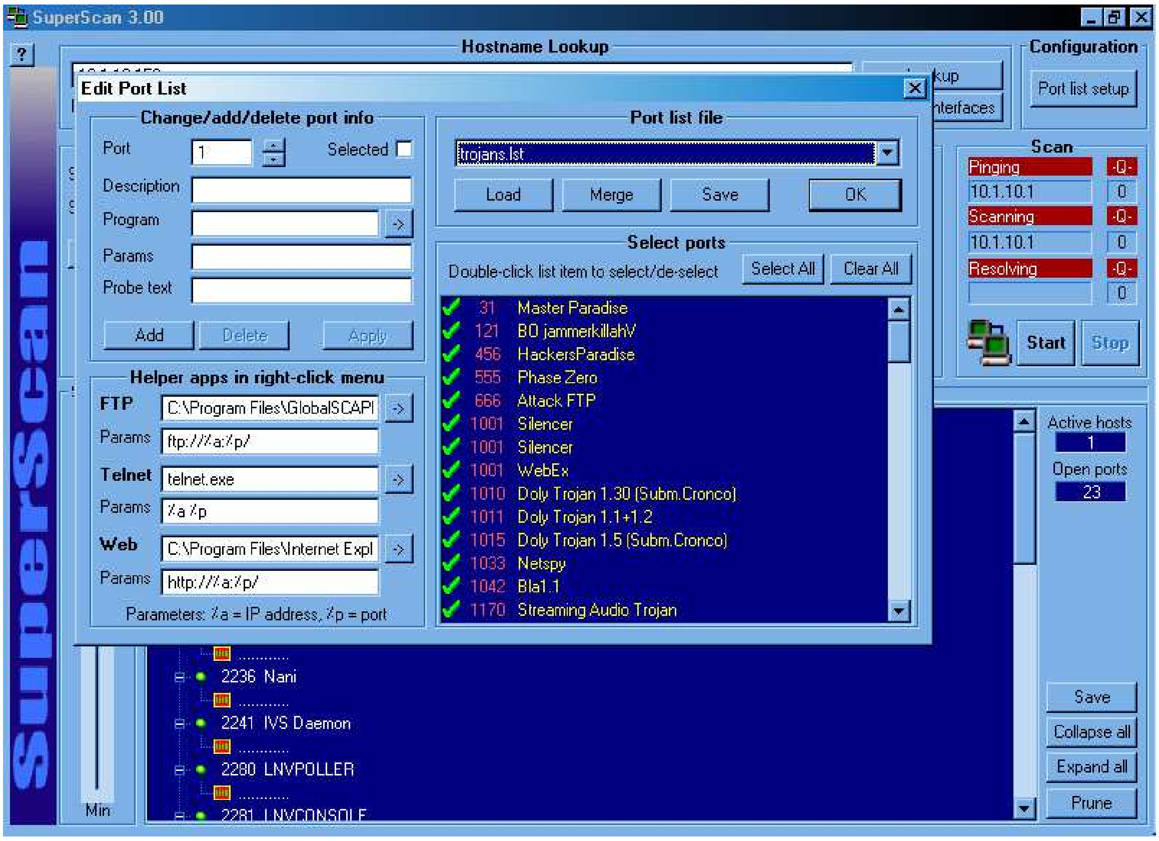
0

```
10.1.10.1
    23  Telnet
        ...........
    2221  Allen-Bradley unregistered port
        ...........
    2223  Allen-Bradley unregistered port
        ...........
    2234  DirectPlay
        ...........
    2235  Sercomm-WLink
        ...........
    2236  Nani
        ...........
    2241  IVS Daemon
        ...........
    2280  LNVPOLLER
        ...........
    2281  LNVCONSOLE
```

Active hosts 1

Open ports 23

Fig.(4.16) shows the program after scanning a node



Port 1 Selected □
Description
Program
Params
Probe text

FTP C:\Program Files\GlobalSCAPI
Params ftp://%a:%p/
Telnet telnet.exe
Params %a %p
Web C:\Program Files\Internet Expl
Params http://%a:%p/
Parameters: %a = IP address, %p = port

trojans.lst

Double-click list item to select/de-select

✓ 31 Master Paradise
✓ 121 BO jammerkillahV
✓ 456 HackersParadise
✓ 555 Phase Zero
✓ 666 Attack FTP
✓ 1001 Silencer
✓ 1001 Silencer
✓ 1001 WebEx
✓ 1010 Doly Trojan 1.30 (Subm.Cronco)
✓ 1011 Doly Trojan 1.1+1.2
✓ 1015 Doly Trojan 1.5 (Subm.Cronco)
✓ 1033 Netspy
✓ 1042 Bla1.1
✓ 1170 Streaming Audio Trojan

Pinging -0-
10.1.10.1 0
Scanning -0-
10.1.10.1 0
Resolving -0-
0

Active hosts 1
Open ports 23

2236 Nani
2241 IVS Daemon
2280 LNVPOLLER
2281 LNVCONSOLE

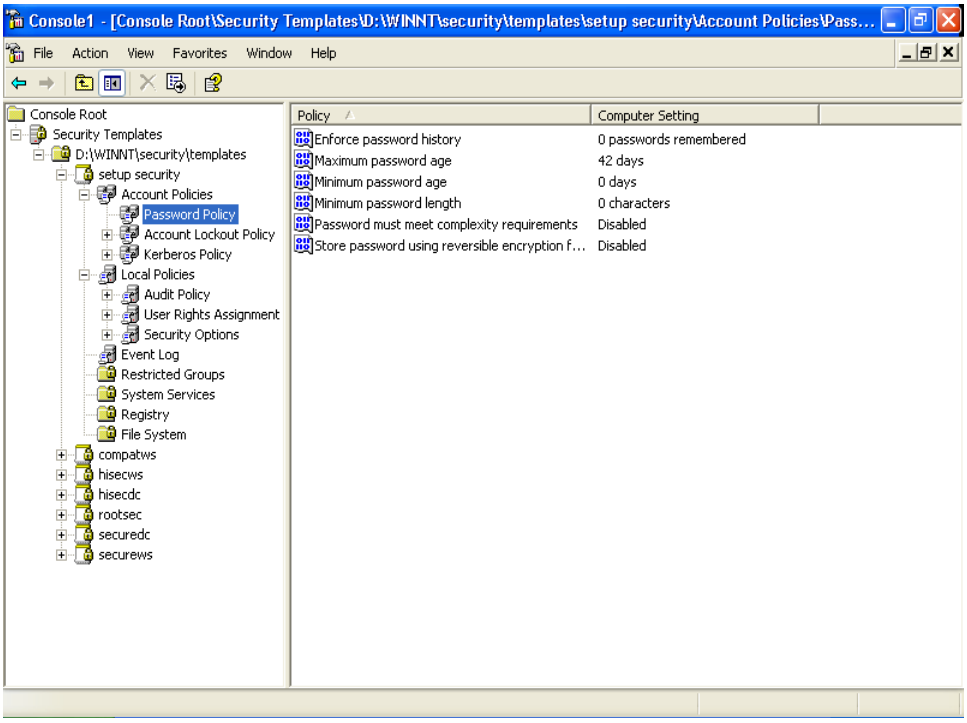
Min

Fig.(4.17) setting the port list figure

4.4.2 Security Check

The implemented program to quite fulfill the requirements of security check program has been found by Microsoft in Windows 2000, and Windows XP. This program is called Microsoft Management Console (MMC) that ships with Windows 2000, and Windows XP. First run this program then add the security templates component available at add snap in as shown in figure 4.18.

This component gives the user (should log as system administrator) a full control on all of the policies settings mentioned above. This program developed for warfare works under Windows 2000 and XP only.



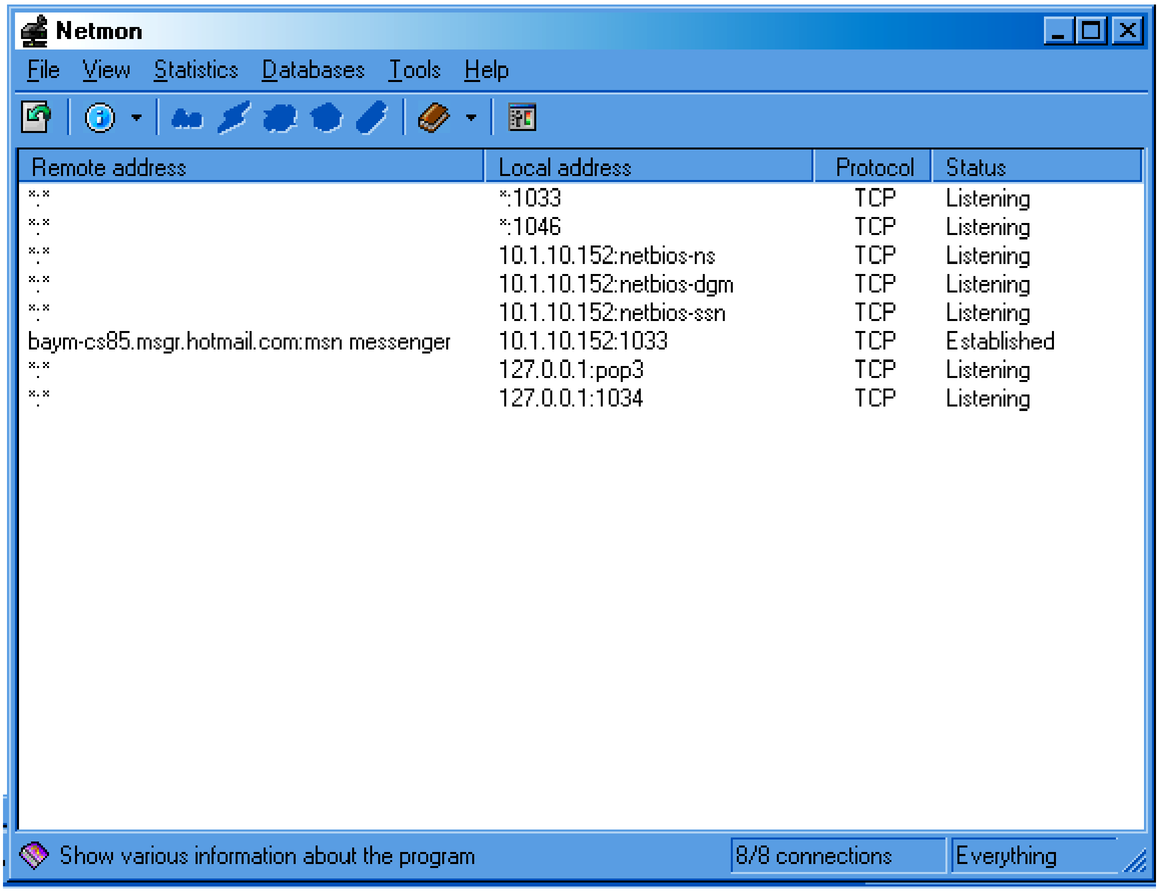
Policy	Computer Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption f...	Disabled

Fig.(4.18) security check program

4.4.3 Network Monitoring

The implemented program Netmon v 1.6 provided by Johan Samuelson was used as an example of network monitoring programs that can help in defense strategy.

Netmon is a compact, easy-to-use network information utility. It displays information pertaining to the IP, TCP, UDP and ICMP protocols. Its main purpose is viewing connections made using TCP and UDP protocols from or to your computer. This information may prove very useful in hunting trojans (or other suspicious activity) present in your system as shown in Figure (4.19).



Remote address	Local address	Protocol	Status
:	*:1033	TCP	Listening
:	*:1046	TCP	Listening
:	10.1.10.152:netbios-ns	TCP	Listening
:	10.1.10.152:netbios-dgm	TCP	Listening
:	10.1.10.152:netbios-ssn	TCP	Listening
baym-cs85.msgr.hotmail.com:msn messenger	10.1.10.152:1033	TCP	Established
:	127.0.0.1:pop3	TCP	Listening
:	127.0.0.1:1034	TCP	Listening

Show various information about the program | 8/8 connections | Everything

Fig.(4.19) netmon program v 1.6 window

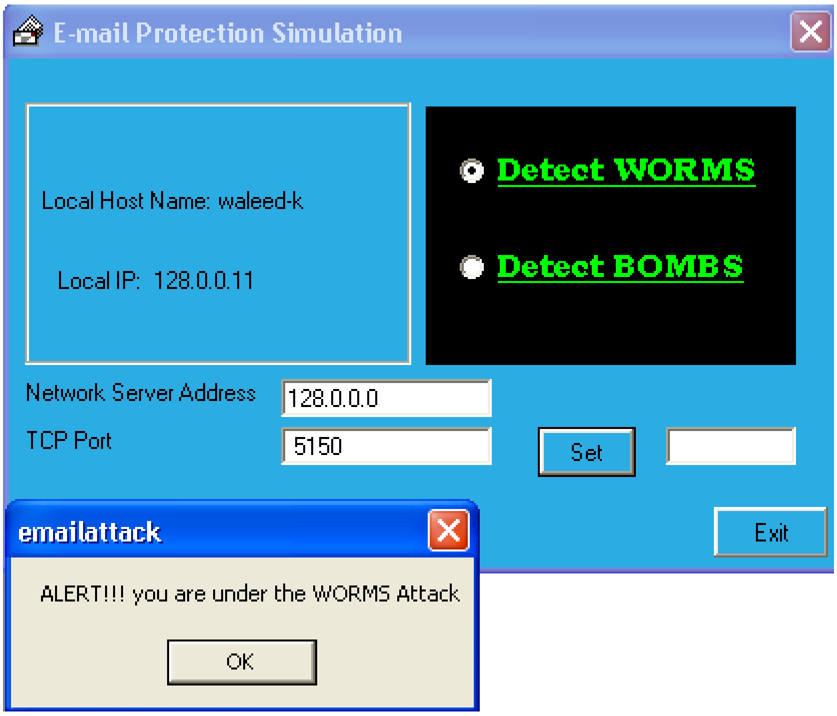
Netmon is a graphical conversion of the "netstat" utility shipped with Windows. Its main advantages over the console based version, is the graphical user interface (GUI), the database of common trojan ports and the complete list of well-known ports (the ports that are numbered below 1024 and reserved for different applications). Users familiar with the netstat utility should feel at home with the GUI and the information presented.

4.4.4 E-mail Protection

The implemented program for e-mail protection used in this defense type is implemented using visual basic programming language.

In order to simulate the defense action taken by e-mail protection, programs are designed to run in e-mail servers and actually scans the messages being sent. These programs work on LANs to detect the simulated worm-attack code and bomb-attack code that being initiated by the corresponding e-mail activities program mentioned in the attack system. These two programs must work at the same time on different PC's of a single LAN.

The program shows information about the host computer name and IP. The LAN server address should be entered with a port number, so that the program makes a winsock connection to the server in order to be able to listen to the simulated attack (listed in the corresponding program in figure 4.15) and detect it as shown in Figure (4.20).



E-mail Protection Simulation

Local Host Name: waleed-k

Local IP: 128.0.0.11

● Detect WORMS

○ Detect BOMBS

Network Server Address: 128.0.0.0

TCP Port: 5150

emailattack

ALERT!!! you are under the WORMS Attack

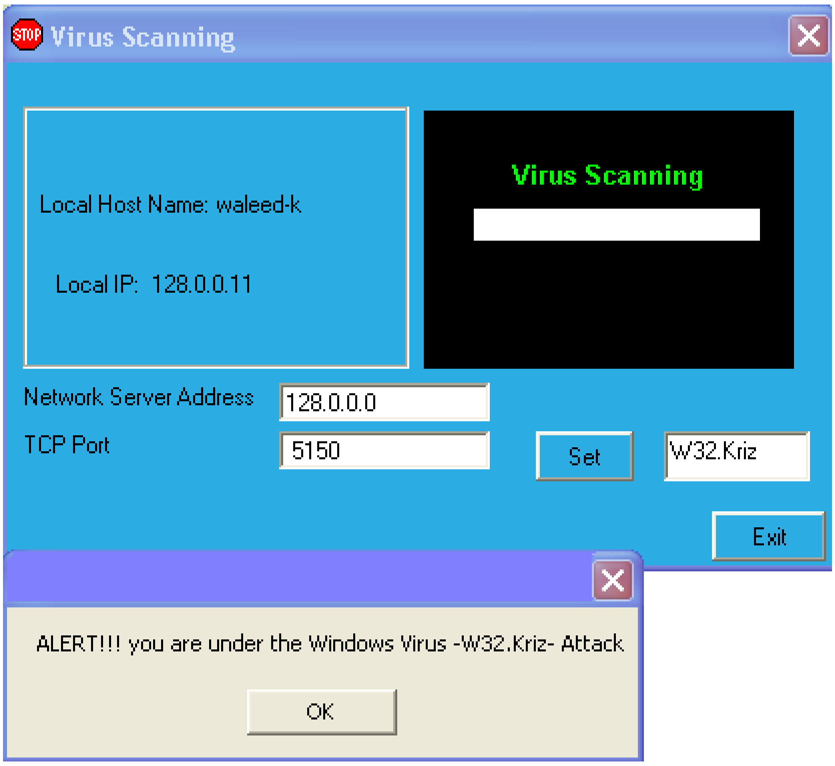
Fig.(4.20) e-mail protection simulation program window

In this program the attack type that is intended to be detected must be set as shown in the figure 4.20, the (detect worms) has been chosen for example, so when the program is set the detection of any worm code on the winsock connection will initiate a warning message says that worm attack has been detected on the LAN. Locating that, the network server address and the TCP port must filled in the fields.

4.4.5 Virus Scanning

The implemented program for virus scanning program used in this defense type was implemented using visual basic programming language in order to simulate the defense action that must be taken in a case virus is being spread through messages. This program works on LANs to detect the simulated viruses attack initiated by the corresponding viruses attack program mentioned in the attack system. These two programs must work at the same time on different PC's of a single LAN.

The program shows information about the host computer name and IP. The LAN server address should be entered with a port number so that the program makes a winsock connection to the server in order to be able to listen to the simulated virus -being sent by the attacker as a code and detect it as shown in Figure (4.21).



Local Host Name: waleed-k

Local IP: 128.0.0.11

Network Server Address 128.0.0.0

TCP Port 5150

W32.Kriz

ALERT!!! you are under the Windows Virus -W32.Kriz- Attack

Fig. (4.21) the virus scanning program window

As soon as the winsock connection has been established, the virus scanning process proceeds so that if any virus code detected on any winsock connection would initiate an alarm message says that the virus of the corresponding type (listed in the corresponding program in figure 4.14) was detected in the LAN.

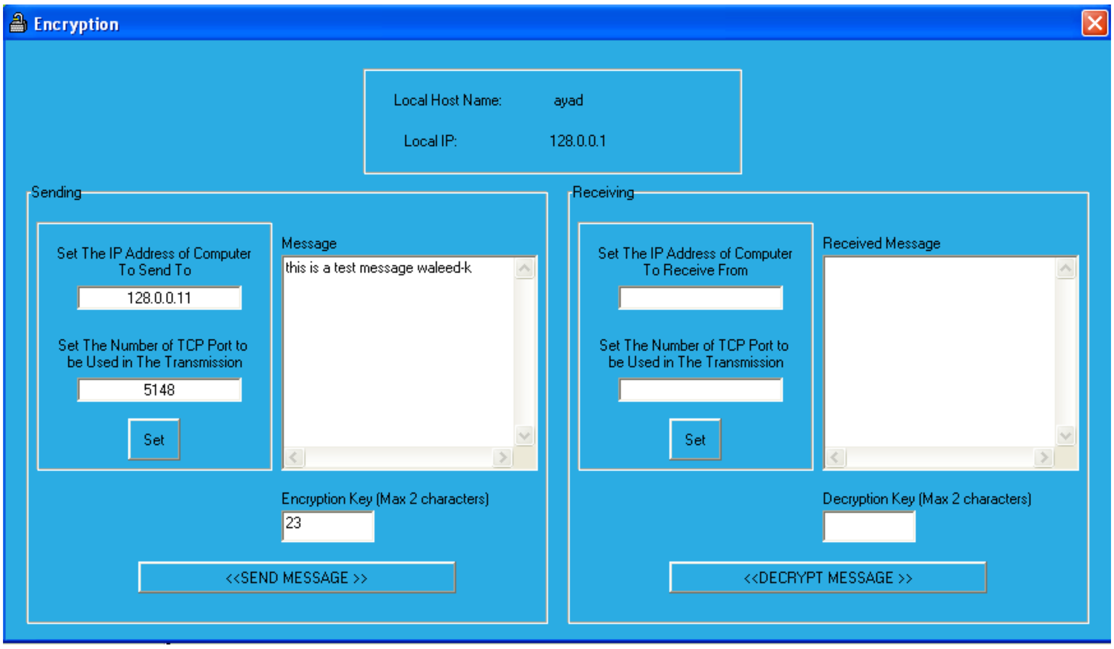
4.4.6 Confidentiality

The implemented program used for encryption is designed to clarify the basic idea of encryption and how messages can be sent encrypted between computers of a single LAN. The program uses simple method of encryption which is XORing (adding) the value of a 16 bit key (2 characters) with each 16 bit block of the message being sent. It is secret key (Symmetric) encryption method. The same thing happens during decryption at the destination node to retrieve the original message.

This program was developed using visual basic programming language. The message can be received by the sending machine also, so the encryption/decryption process can be demonstrated even on a single computer.

To run the program on two computers connected by LAN, both nodes must run the program at the same time, and each node must set the IP address of the other according to whether it is sending or receiving, so they will be connected through the same port.

Figure (4.22) shows an example message to be sent. To send the message the fields of destination IP and the port must be valid. The next step is to confirm the address by pressing the button (set) and send the message.


Local Host Name: ayad

Local IP: 128.0.0.1

Sending

Set The IP Address of Computer To Send To: 128.0.0.11

Set The Number of TCP Port to be Used in The Transmission: 5148

Message: this is a test message waleed-k

Encryption Key (Max 2 characters): 23

Receiving

Set The IP Address of Computer To Receive From:

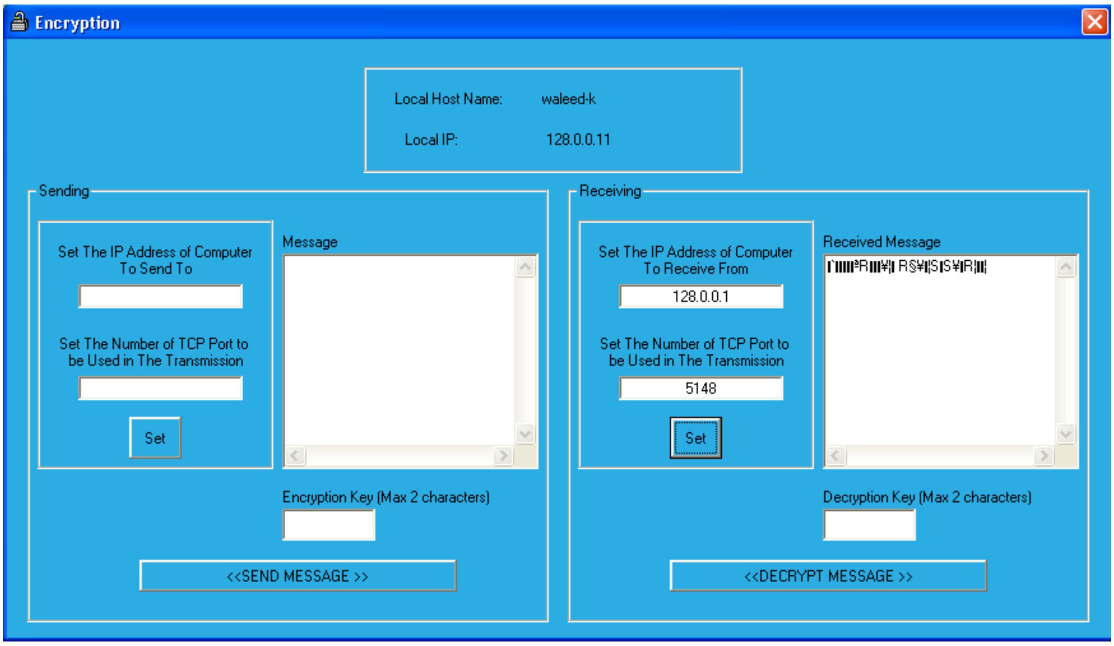
Set The Number of TCP Port to be Used in The Transmission:

Received Message:

Decryption Key (Max 2 characters):

Fig.(4.22) encryption program sending a test message

The destination computer will receive the message encrypted noticing that the fields of sending IP address and the port used must valid as shown in Figure (4.23).


Encryption
Sending
Set The IP Address of Computer To Send To
Set The Number of TCP Port to be Used in The Transmission
Set
Message
Encryption Key (Max 2 characters)
<<SEND MESSAGE >>
Receiving
Set The IP Address of Computer To Receive From
Set The Number of TCP Port to be Used in The Transmission
Set
Received Message
Decryption Key (Max 2 characters)
<<DECRYPT MESSAGE >>

Local Host Name: waleed-k

Local IP: 128.0.0.11

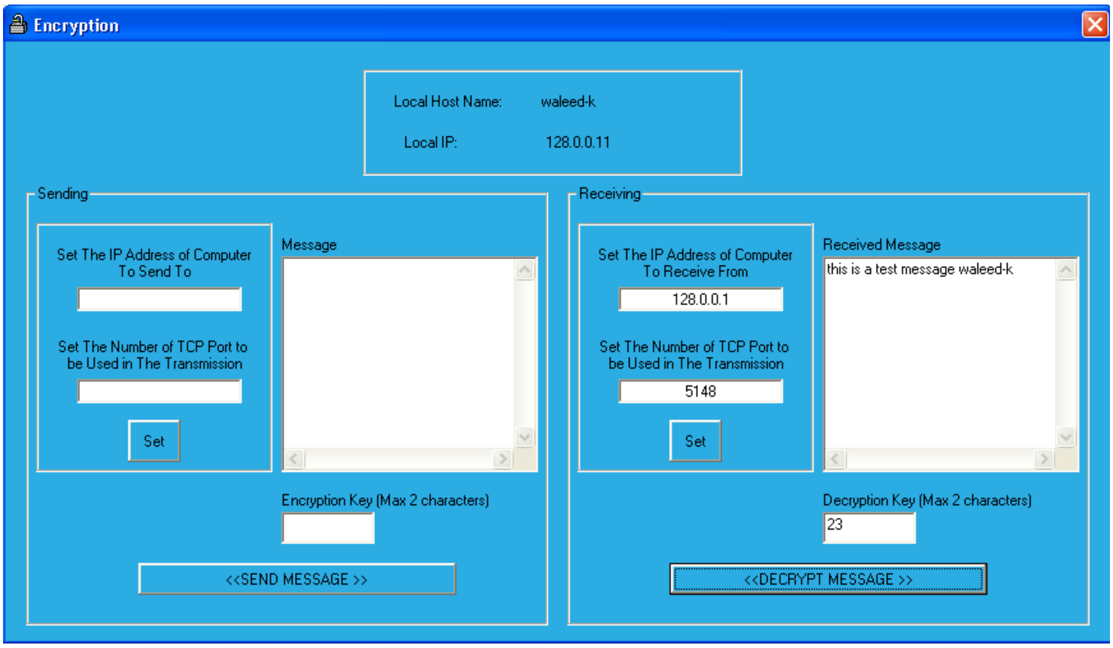
Set The IP Address of Computer To Receive From: 128.0.0.1

Set The Number of TCP Port to be Used in The Transmission: 5148

Received Message: ▌`▌▌▌▌ªR▌▌▌¥¦▌ R§¥▌¦S▌S¥▌R¦▌▌¦

Fig.(4.23) the destination computer receiving the encrypted message

Finally by using the proper key, the message decrypted to the original one as shown in Figure (4.24)


Encryption
Sending
Set The IP Address of Computer To Send To
Set The Number of TCP Port to be Used in The Transmission
Set
Message
Encryption Key (Max 2 characters)
<<SEND MESSAGE >>
Receiving
Set The IP Address of Computer To Receive From
Set The Number of TCP Port to be Used in The Transmission
Set
Received Message
Decryption Key (Max 2 characters)
<<DECRYPT MESSAGE >>

Local Host Name: waleed-k

Local IP: 128.0.0.11

Set The IP Address of Computer To Receive From: 128.0.0.1

Set The Number of TCP Port to be Used in The Transmission: 5148

Received Message: this is a test message waleed-k

Decryption Key (Max 2 characters): 23

Fig.(4.24) the decryption of the message using the proper key

Chapter Five

Conclusions and Future Work

5.1 Conclusions

The developed learning security system represents a step in simplifying security learning in our country. It supposed to represent a first step towards the development of security faculties and generally training systems. The developed system will help to enhance the national security learning in our schools and universities because it make it easier for the teachers as well as the students to learn the security methods and to realize how it will work practically. The establishment can use such simulator also to help the students to avoid hackers, viruses or any network threats.

5.2 Future Works

Some recommendations for the future work are:-

i. Developing the system to be a training security system that focuses on the training part as an important part of learning.

ii. Designing and implementing more techniques of the applied ones in the application system.

iii. Extending the system to fulfill most of the security attacks and defense techniques to be applied as a learning system for university.

DEDICATED TO

My Parents ...
My Brothers ...
My Sisters ...

To everyone
Taught me a letter
Specially staff member

Mustafa

بسم الله الرحمن الرحيم

((وأن لَـيْسَ للإنســـــن
إلاّ مـــا ســــعى))

صدق الله العظيم
النجم٣٩

References

[1] Schwartau, W.; "**Information Warfare**, Chaos on the Electronic Superhighway"; first trade paperback edition, Thunder's Mouth Press, 1995.

[2] Aequilla, J. ; Ronfeldt, D.; "**Preparing For Conflict In The Information Age** "; Santa Monica, Rand, 1997.

[3] Adams J.;" **The Next World War** "; Hutchinson, 1998.

[4] Gillam, Major M.; "**Information Warfare**: computing the threat in the 21st century"; research paper presented to the research department, Air Command and Staff College, March 1997.

[5] Roberts, M. j.;"**Integration Of An Attack Simulator In The Environment**"; west point, NY, June 2000.

[6] Holdaway, Eric J.; "**Active Computer Network Defense**"; a graduation research, USAF, Maxwell Air Force Base, Alabama, April 2001.

[7] McGovern, Susan C. "**Information Security Requirements For A Coalition Wide Area Network**", Msc. Thesis, graduate School, Monterey, California, June 2001.

[8] Welsh, D.; Conti, G., "**Workshop On Information Assurance And Security** ", US Military Academy, NY, June 2001.

[9] Forouzan, B., "**Data Communications And Networking**", McGraw-Hill, 1998.

[10] Stallings, W., "**Business Data Communications**", 4th Edition, Prentice-Hall Inc., 2001.

[11] Halsall, F., "**Data Communications, Computer Networks And Open Systems**", 4TH edition, Eddison-Wesley, 1996.

[12] Institute for Telecommunication Sciences (ITS), "**Operations Security**", January 2003.
URL: http://www.its.bldrdoc.gov/fs-1037/dir-5/_3695.html

[13] Ehlers, V. J., "**Information Warfare And International Security**" General report, octoper 1999. URL:http://www.naa.be/publications/comrep/1999/as285stc-e.html

[14] Goldberg, Dr. Ivan K. “**Information Warfare**" Glossary of IW Terms. URL: http://www.psycom.net/iwar.2.html , 2006.

[15] Department of Defense, "**Joint Doctrine for Information Operations**" Joint Pub 3-13, January 2003. URL:http://www.dtic.mil/doctrine/jel/new_pubs

[16] Lewis, Brian C. "**Information Warfare**", 2006. URL: http://www.fas.org/irp/eprint/snyder

[17**]** Raymond, E. S., "**How To Be A Hacker**", URL:http://www.toxedo.org/~ers/faqs/hacker-howto.html

[18] Taber, M., "**Maximum Security**", Macmillan computer pub.

[19] Robichaux P., "**The Administrator Shortcut Guid To E-Mail Protection**", Realtime Publishers, 2002.

[20] Mateti, P. "**INTERNET SECURITY**", College of Engineering and CS, Wright Stall UN. Dayton, Ohio, June 2001.

[21] E. j. Holdaway, " **Active Computer Network Defense** ", USAF Maxwell Air Force Base, Alabama, April 2001.

[22] Stallings W., "**Cryptography And Network Security Principles And Practice** ", 2nd Edition, Prentice-Hall Inc., 1999.

[23] Schafer, J., Ragsdale, D. J.,"**THE IWAR RANGE: A LABORATORY FOR INFORMATION ASSURANCE EDUCATION**", Middlebury, Vermont, 2001.

[24] US Military Academy "**Information Warfare Laboratory**", 2003, URL:http://www.itoc.usma.edu/iwar.html

[25] Kurose, James F., Keith W. Ross, "**Computer Networking**", Addison Wesley Longman Inc., 2001.

[26] Bruce Schneier, "**Applied Cryptography**", Whitfield Diffie, 2001.

List of Contents

Republic of Iraq
Ministry of Higher Education
and Scientific Research
Al Nahrain University
College of Science

Computer Aided Learning for Network Security

A Thesis
Submitted to college of Science, Al-Nahrain University in partial fulfillment of the requirements for the Degree of Master of Science in Computer Science

BY

Mustafa Ibrahim Abid

(B. Sc. 2003)

Supervisor

Dr.
Siddeeq Y. Ameen

Shawal 1427 **November 2006**

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم

نظام تعليمي امني بمساعدة الكومبيوتر

رسالة مقدمة الى كلية العلوم، جامعة النهرين كجزء من متطلبات نيل
شهادة الماجستير في علوم الحاسوب

تقديم

مصطفى ابراهيم عبد

(بكالوريوس ٢٠٠٣)

إشراف

د. صديق يوسف امين

تشرين الثاني ٢٠٠٦ شوال ١٤٢٧

```
[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21815
```