# INTRUSION WINDOWS XP BY BACKDOOR TOOL

Eman Esmaeel Hamed and Muna Majeed Lafta

Baghdad University, College of Education for Women, Computer Department.

## Abstract

Sometimes operating system designer personal deliberately create a hole in the security of the system. This hole or backdoor allows them later to take control of the system. Attackers who have compromised a system to ease their subsequent return to the system often install backdoors.

This paper presents a tool for intrusion operating system (Windows XP) by using one of the system port the main reason for using this port to fabricate the firewall and the administrator on the server computer, where this tool can work by placed intrusion program into chess game then attach this game with email after attachment then send this email to any computer server. Tiny firewall used to test the proposed tool and check if intrusion occurred.

## 1-Introduction

A hackers use several techniques to break into a computer or network. One-way hacker programmer creates a backdoor (trap door), which is an entrance into a system that penetrates security. A programmer can intentionally leave backdoors in place, sometimes for legitimate reasons, such as giving service techs a way to check the system or application. A Backdoor is like a hidden secret-word entrance, the programmer knows the key to this door, but no body else even knows the door is there. Backdoor is a mechanism surreptitiously introduced into a computer system to facilitate unauthorized access to the system. While backdoors can be installed for accessing a variety of services, of particular interest for network security are ones that provide interactive access. These are often installed by attackers who have compromised a system to ease their subsequent return to the system [2].

## 2-Backdoor Functionality

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

- Be able to get back into a machine even if the administrator tries to

secure it, e.g., changing all the passwords.

- Be able to get back into the machine with the least amount of visibility. Most backdoors provide a way to avoid being logged and many times the machine can appear to have no one online even while an intruder is using it.
- Be able to get back into the machine with the least amount of time. Most Intruders want to easily get back into the machine without having to do all the work of exploiting a hole to gain access [3].

Backdoor are two–part program (server and client application). A small, virtually unnoticeable server component is installed on the victim's pc, which the attacker accesses remotely through a convenient client GUI (Graphical User Interface).

The attacker uses the server as a bi-directional surreptitious channel to sidestep existing security mechanisms and access the compromised system remotely- all without the victim's knowledge. Two TCP (Transmission Control Protocol) connections are established when the server application is accessed by an attacker using the client application. The attacker client sends commands via a connection to port number of the victim machine. The victim server transmits data in response via a connection to port number of the victim machine [4].

## 3-Intrusion by port

When a process on one host wants to communicate with a process on a different host, it identifies itself to the TCP/IP (Transmission Control Protocol/ Internet Protocol) protocol suite via one or more *ports*. A port identifies the application that is using the UDP *(User Datagram Protocol)* or TCP service and is represented by a 16-bit number in the UDP or TCP header. Port numbers between 1 and 1023 are called well-known ports because they enable clients to find servers easily without configuration information.

Port numbers between 1024 and 65535 are called ephemeral ports because they are used for a short period of time. Clients to initiate connections to servers use ephemeral ports. When the session with the server ends and the service is no longer needed, the port is released to the pool of available ports.

A higher-layer application that communicates across a TCP/IP internet work with another higher-layer application maintains an *association*, which takes the following form:

[Protocol, source IP address, source port, destination IP address, destination port].

This association uniquely identifies a connection in the network, and is made up of two half-associations, which take the following form:

[Protocol, source IP adresse, source port] Or [Protocol, destination IP adresse, destination port].

A half-association is generally called a socket. Thus, communication between two processes over a TCP connection is carried out via a TCP socket.

The port usage setting can be used to make certain that Windows XP clients don’t accidentally answer the phone and open a Backdoor onto network [5].

## 4-Proposed Tool (IT)

In this section a proposed intrusion tool (IT) introduced. It contains two parts, the first part IT server (ITS), the second part IT client (ITC). This tool can attack the server computer in local area network by the (ITC) where netbios of server computer must be active, where ITC works in client computer. Attack occurs when ITS works in server computer in secret manner without knowing of the server manger.

### *4-1. IT properties*

1-The ITS hidden in chess game as attachment with email.

2-The ITC used port (139) to connect with the server computer, this port is one of the system ports (NetBIOS Session (TCP), windows file and printer sharing. This is the single most dangerous port on the Internet, All "file and printer sharing" on a windows machine runs over this port. About 10% of all users on the Internet leave their hard disks exposed on this port, This is the first port hackers want to connect to, and the port that firewalls block).

IT can attack the server computer by using two operations

- Connection with server
- Sent any massage to the server computer.

### *4-2. IT server*

In the server computer the chess game is installed in hard disk .The ITserver.exe is hidden in this game and use port number (139) to connect with server computer or client. The IT server works in all time and can connect to the remote server if the game is running or stop running. Below is the algorithm described this operation:

1. Check if LAN card is available.
2. Read IP address of computer from the network.
2. Check the ports numbers of network.
3. Listen on port 139.
4. Ignore port 139 open.
5. If client tries to build connection then check if the client is a IT Client then send acknowledgement to client, else send refuse to client and try to build connection which depends on port 139.
6. Repeat steps 3 to 6 until operating system is shut down.
7. End.

### *4-3. IT client*

This part of IT tool can connect to the server computer without telling it. Three operations implemented by this tool

- Connect with remote server.
- Disconnect with remote server.
- Massage sent to the remote server.

***Connection of the Remote Server or Client Algorithm:***

1. Open the connection dialog.
2. Read the input IP address of remote IP address field.
3. Convert the IP address to Long number.

4. Send message to operating system to tell it try to connect with IP address.
5. Received the reply of operating system of connection operation.
6. Check the unused ports of network in LAN card.
7. Send connection command to server or client computer by using the inputting IP address.
8. If there is acknowledgment from server to accept connection then send to server or client to assign the hard disk, else display message in client saying user cannot connect with server or client.
9. End.

***Disconnection of the Remote Server or Client Algorithm:***

1. Open the disconnect dialog.
2. IT Client asks you (Do you wish to disconnect from (remote server or client).
3. If wished click "**yes**" then send command disconnection to server to close connection and port, else click "**no**".
4. If you ignore this operation then click "**cancel**".
5. End.

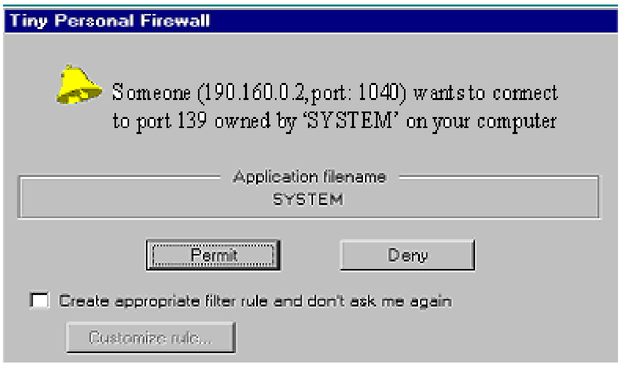
***Massage sent to the remote server algorithm:***

1. Send command "sent message" to server or client to open message received dialog and received the message.
2. Send the message to server or client.
3. Receive acknowledgement from server or client if not then client repeats sending the message.
4. Check if there is a message sent from server and displays it.
5. End.

## 5-Test and Result

To test the result of the implementation, and ensure that intrusion was occurred, a firewall called tiny personal firewall engine version 2.0.9 was used. There are many type of firewall, we use this type because this type could specify the connection type and we can fabricate this firewall.

This firewall product check all connections to server computer then asked the administrator if he accepts to implement or refuse the connection, during starting of IT implementation the firewall shows the screen, as shown in Fig. (1).



Tiny Personal Firewall

Someone (190.160.0.2,port: 1040) wants to connect to port 139 owned by 'SYSTEM' on your computer

Application filename
SYSTEM

☐ Create appropriate filter rule and don't ask me again

***Fig. (1) : Resulted of Tiny Firewall.***

When the Firewall displays this screen with sound, the administrator will accept to implement the implementation of connection because IT uses one of computer ports where that mean IT passing through tiny firewall.

## 6-Conclusions

1.IT has achieved the purpose of intruding Windows XP.

2. Tiny Personal Firewall supply a good results because IT tool can pass through it without discover it.
3. IT introduce two prosperities first the using of system ports (139) and the second that this port is usually open during the connection only.

## Reference

[1] Kantor B, "BSD Rlogin", RFC 1282, Network Information Center, SRI International, Menlo Park, CA, Dec. 1991.

[2] Mansfield R.,"Hacker Attack", Published Sybex Inc, USA, 2000.

[3] Paxson V. and Floyd S., ``Wide-Area Traffic: The Failure of Poisson Modeling," IEEE/ACM Transactions on Networking, 3(3), pp. 226-244, June 1995.

[4] Korba J.,"Windows NT attacks for the evaluation of Intrusion Detection Systems", MSc thesis, Massachusetts Institute of Technology, June 2000.

[5] Strebe M. , Perkins C. , and Moncur G.,”NT4 Network Security”, Published Sybex, Inc, 1998.

## الخلاصة

في بعض الاحيان مصمم نظام التشغيل يقوم متعمدا بخلق فجوة في امنية النظام هذه الفجوة او ماتسمى الباب الخلفي تسمح له لاحقا بالسيطرة على النظام. المهاجم يقوم بخداع النظام من اجل تسهيل العودة لاحقا الى النظام والاختراق عن طريق الباب الخلفي .

في هذا البحث تم تصميم اداة لاختراق نظام تشغيل (نافذة -xp ) من خلال استغلال احدى منافذ النظام والغرض الرئيسي من استخدام هذا المنفذ هو عملية خداع الحاجز الناري Firewall وبالتالي خداع الشخص المسؤ ول عن تمرير الاتصال. حيث ان هذه الاداة تستطيع العمل بواسطة تعشيقها برنامج الاختراق مع لعبة الشطرنج ثم الحاق هذه اللعبة مع البريد الالكتروني وارسال هذا البريد الى اي حاسبة رئيسية ( computer server ) .حيث تم استخدام الحاجز الناريFirewall لاختبار الاداة المقترحة وللتأكد من حصول الاختراق .