Backdoors & Remote Administration programs

By: *Eng. Ammar J. Mahmood*

Supervised By:Dr. Lo’ai Tawalbeh

New York Institute of Technology (NYIT)-Jordan’s Campus

Introduction

- A **backdoor** in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.(unauthorized persons/systems)
- Most backdoors are autonomic malicious programs that must be somehow installed to a computer. Some parasites do not require the installation, as their parts are already integrated into particular SW running on a remote host.

Introduction

- The backdoor may take the form of an installed program (e.g., Back Orifice or the Sony/BMG rootkit backdoor installed when any of millions of Sony music CDs were played on a Windows computer), or could be a modification to a legitimate program.

Ways of Infection

- Typical backdoors can be accidentally installed by unaware users. Some backdoors come attached to e-mail messages or are downloaded from the Internet using file sharing programs. Their authors give them unsuspicious names and trick users into opening or executing such files (Trojan horse).
- Backdoors often are installed by other parasites like viruses, worms or even spyware (even antispyware e.g. AdWare SpyWare SE). They get into the system without user knowledge and consent and affect everybody who uses a compromised computer.
- Some threats can be manually installed by malicious local users who have sufficient privileges for the software installation.

Ways of Infection

- Several backdoors are already integrated into particular applications. Even legitimate programs may have undocumented remote access features. The attacker needs to contact a computer with such software installed in order to instantly get full unauthorized access to the system or take over control over certain software.
- Some backdoors infect a computer by exploiting certain software vulnerabilities. They work similarly to worms and automatically spread without user knowledge. The user cannot notice anything suspicious, as such threats do not display any setup wizards, dialogs or warnings.

Hard coded (source code)

- A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system
- **Hard coded** refers to the software development practice of embedding output or configuration data directly into the source code of a program.
  - Ex: An attempt to plant a backdoor in the Linux kernel, exposed in November 2003, showed how subtle such a code change can be. In this case a two-line change appeared to be a typographical error, but actually gave the caller to the sys_wait4 function root access to the system.

Hard coded (source code)

- This is so hard to detected or know for sure how many or whether there is Backdoor or not in proprietary software (ie, software whose source code is not readily available for inspection).
- Programmers have even succeeded in secretly installing large amounts of benign code as “Easter eggs” in programs, although such cases may involve official forbearance, if not actual permission.
  - Easter eggs: are messages, graphics, sound effects, or an unusual change in program behavior, that mainly occur in a software program in response to some undocumented set of commands, mouse clicks, keystrokes or other stimuli intended as a joke or to display program credits.

Compiler (during compilation)

- It is also possible to create a backdoor without modifying the source code of a program, or even modifying it after compilation. This can be done by rewriting the compiler so that it recognizes code during compilation that triggers inclusion of a backdoor in the compiled output
- When the compromised compiler finds such code, it compiles it as normal, but also inserts a backdoor (perhaps a password recognition routine).

Compiler (during compilation)

- Trusting trust problem:
  - people only review source (human written) code, and not compiled (machine) code.
  - A program called a compiler is used to create the second from the first, and that version will usually be trusted to do an honest job.
  - Because the compiler itself was a compiled program, this extra functionality would not likely be noticed.
  - the subverted compiler also subverted the analysis program (the disassembler), so that anyone who examined the binaries in the usual way would not actually see the real code that was running, but something else instead.
  - Divers Double Compilers against trusting trust attack.

Attack on machine code

- It’s use to creat back door in clean legitimate SW
- This done by transferring the SW machine code into Assembly Language by specific tools such as HView, W32dasm. As a first step.
- Then adjust the code (inserting the backdoor) and return it to the machine language using the same tools.
- This practice actually widely used to crack the SW (SW piracy).

Kleptography

- A traditional backdoor is a symmetric backdoor: anyone that finds the backdoor can in turn use it.
- An asymmetric backdoor
    - can only be used by the attacker who plants it, even if the full implementation of the backdoor becomes public.
    - it is computationally intractable to detect the presence of an asymmetric backdoor

Kleptography

- The attacker, who is the programmer that is creating the RSA key generation algorithm, stores a secret seed in the key generation algorithm and the algorithm supplies this seed to pseudorandom number generator.
- This sequence is known to the attacker and can be the sole source of randomness for deriving output pairs (*p, q*).
- The attack amounts to replacing the “honest” random sequence that is inherent to a probabilistic Turing machine with a “dishonest” pseudorandom sequence that is completely reconstructable by the insider.
- An RSA key pair that is compromised in this way allows the insider to read anything encrypted using the user’s public key,

Hardware Backdoors

- **Standard BIOS backdoor passwords**
  - □ The first attempt to bypass a BIOS password is to try on of these standard manufacturer's backdoor passwords:
  - □ **AWARD BIOS:** AWARD SW, AWARD_SW, Award SW, AWARD PW, _award,…
  - □ **AMI BIOS:**AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD,…

Examples of Backdoors

- **Remote Connection**
  - Remote Connection, also known as RedNeck, is a dangerous backdoor that gives the remote attacker full access to a compromised computer. The parasite can shutdown or restart a PC, manage files, record user keystrokes, install and run various programs, take screenshots and perform other malicious actions. Remote Connection runs on every Windows startup.
- **Resoil FTP**
  - Resoil FTP is a backdoor that gives the attacker remote unauthorized access to an infected computer. This parasite runs a hidden FTP server, which can be used to download, upload and run malicious software. Resoil FTP activity may result in noticeable computer performance loss and user privacy violation.

How to Remove a Backdoor?

- Backdoors work in the same manner as the computer viruses and therefore can be found and removed with the help of effective antivirus products like Symantec Norton AntiVirus, Kaspersky Anti-Virus…etc.
- Some advanced spyware removers, which are able to scan the system in a similar way antivirus software does and have extensive parasite signature databases can also detect and remove certain backdoors and related components. Powerful anti-spyware solutions such as Spyware Doctor, Microsoft AntiSpyware Beta…etc.
- there are Internet resources such as 2-Spyware.com, which provide manual malware removal instructions. These instructions allow the user to manually delete all the files, directories, registry entries and other objects that belong to a parasite. However, manual removal requires fair system knowledge and therefore can be a quite difficult and tedious task for novices.

Remote Administration Tools

Introduction

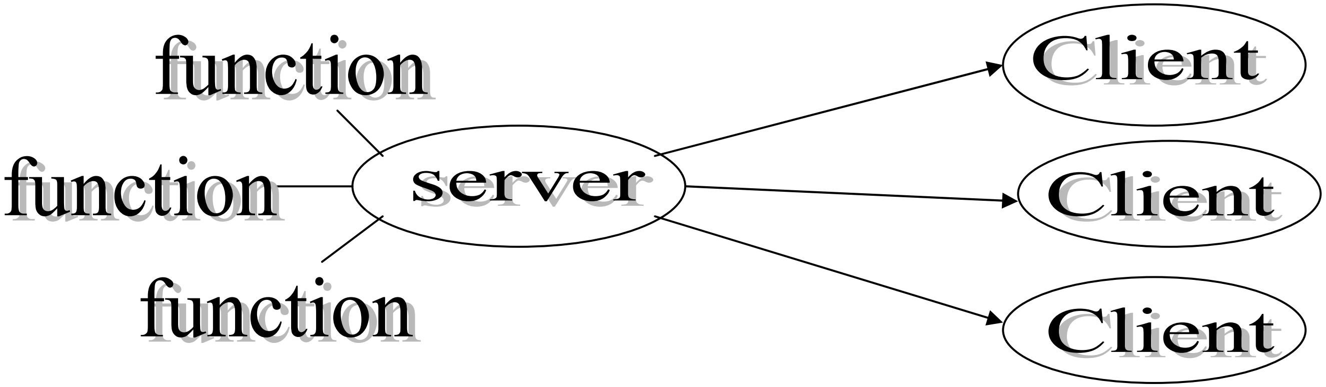
- A **Remote administration tool** is used to remotely connect and manage a single or multiple computers with a variety of tools, such as:
  - Screen/camera capture or control
  - File management (download/upload/execute/etc.)
  - Shell control (usually piped from command prompt)
  - Computer control (power off/on/log off)
  - Registry management (query/add/delete/modify)
  - Other product-specific function

Introduction

- Remote access trojans (RATs) are typically client-server programms.
- They are doing a similar job like official remote control and management tools. Symantec’s PCAnywhere can be named as an example for a remote control application.
- **RAT as a malware** :RAT installs itself hidden and runs invisible for the user. It gives an attacker full control over the infected machine as if he was sitting right in front of it. RATs are often used to upload and implant other malware.

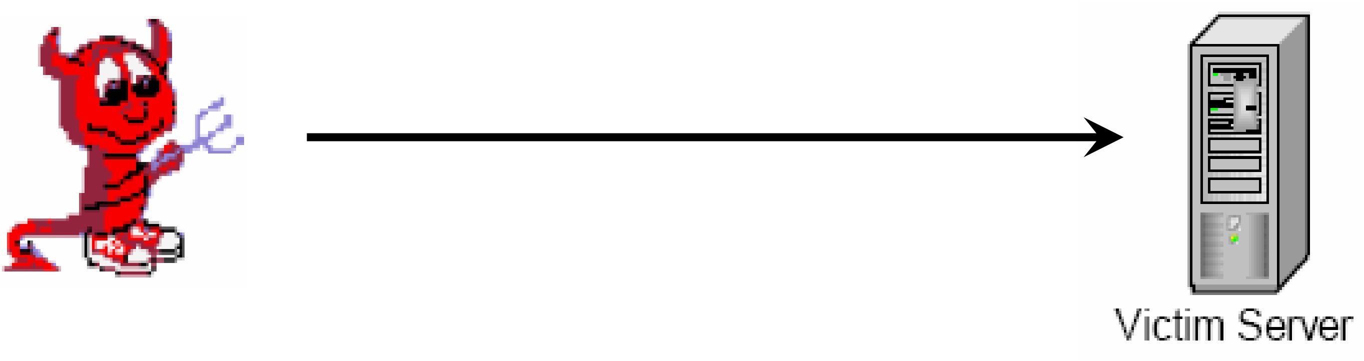
Types of connection

- Direct Connection
  - A direct-connect RAT is a simple setup where the client connects to a single or multiple servers directly. Stable servers are multi-threaded, allowing for multiple clients to be connected, along with increased reliability. A diagram below is shown to better illustrate the concept:



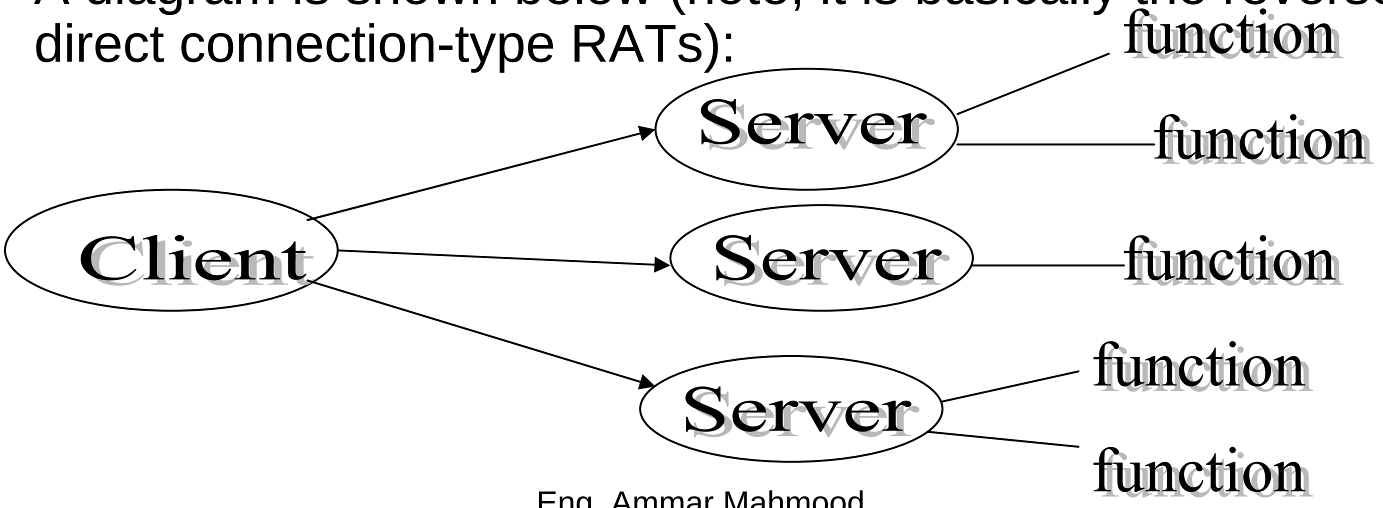
Types of connection

- Direct Attack
  - Very difficult: The Firewall between clients and servers prevents the TCP/IP from being penetrated from the outside



Types of connection

- **Reverse connection**
  - □ Reverse connection are a new technology that came around about the same time that routers became popular. A few advantages of a reverse-connection RAT are listed below:
    1. No problems with routers blocking incoming data, because the connection is started outgoing for a server
    2. Allows for mass-updating of servers by broadcasting commands, because many servers can easily connect to a single client.
  - □ A diagram is shown below (note, it is basically the reverse of direct connection-type RATs):



Client

Server

Server

Server

function

function

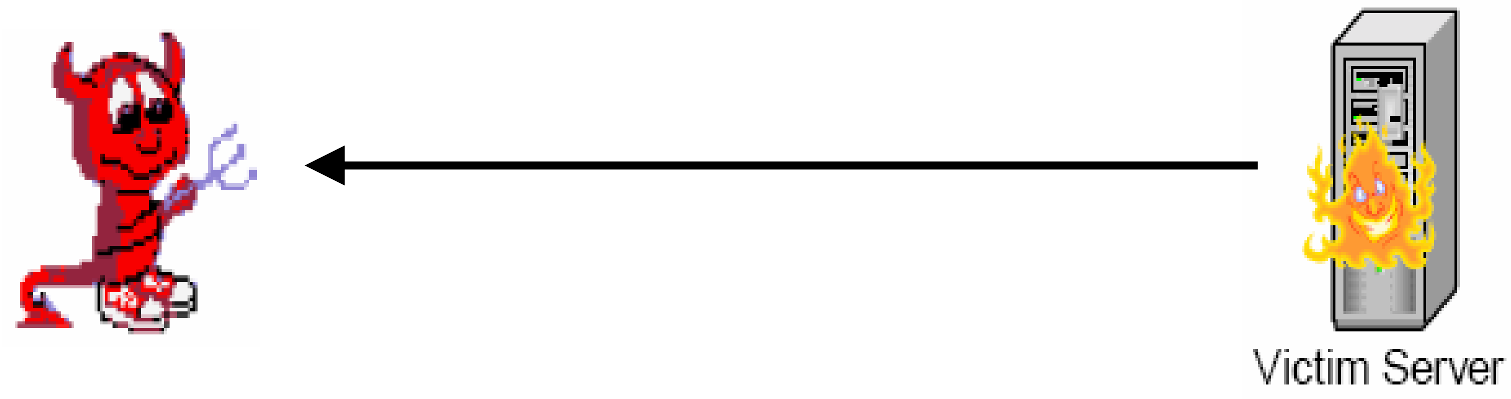
function

function

function

Types of connection

- Inside-out attack
  - To avoid firewall we start the connection from inside (trusted area) to outside(attacker) this done by traitor server (e.g. subseven)

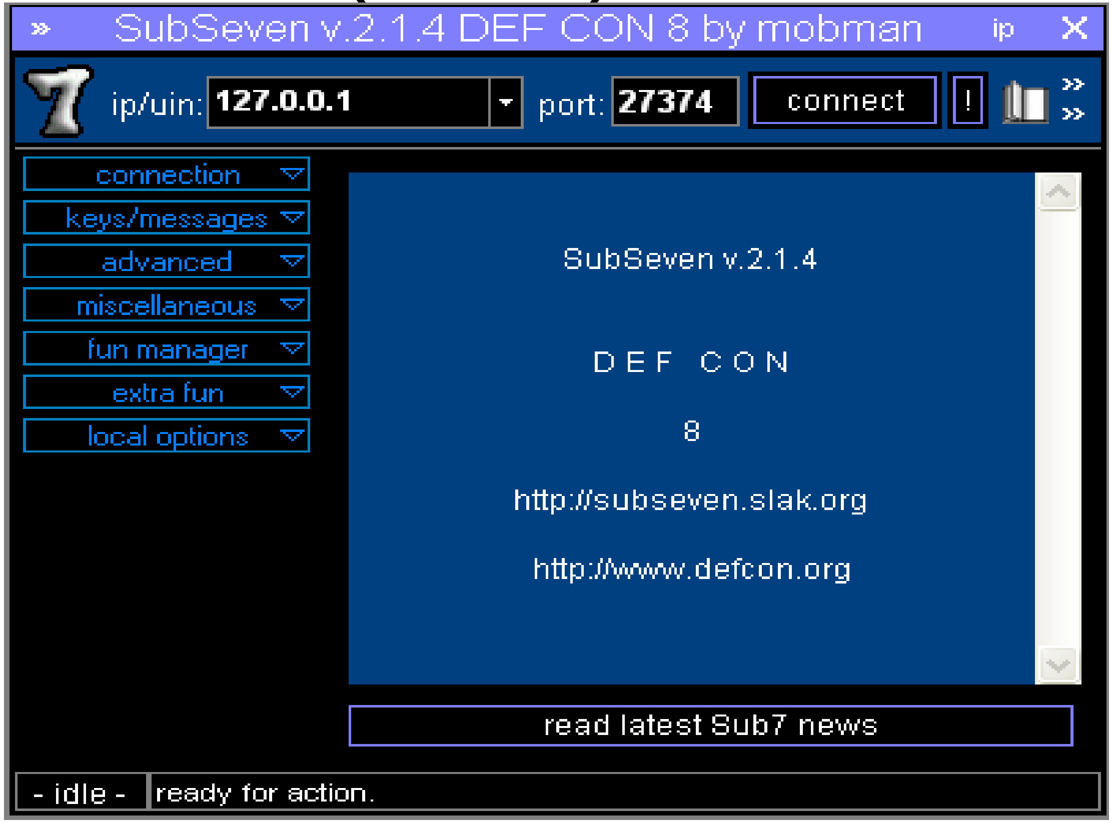


RAT Trojan Horses

- Many Trojans and backdoors now have remote administration capabilities allowing an individual to control the victim's computer.
- Many times a file called the server must be opened on the victim's computer before the trojan can have access to it. These are generally sent through email, P2P file sharing software, and in internet downloads

Ex. Of RAT\Subseven

- Subseven client (R.A.T):



SubSeven v.2.1.4 DEF CON 8 by mobman

ip/uin: 127.0.0.1

port: 27374

SubSeven v.2.1.4

DEF CON

8

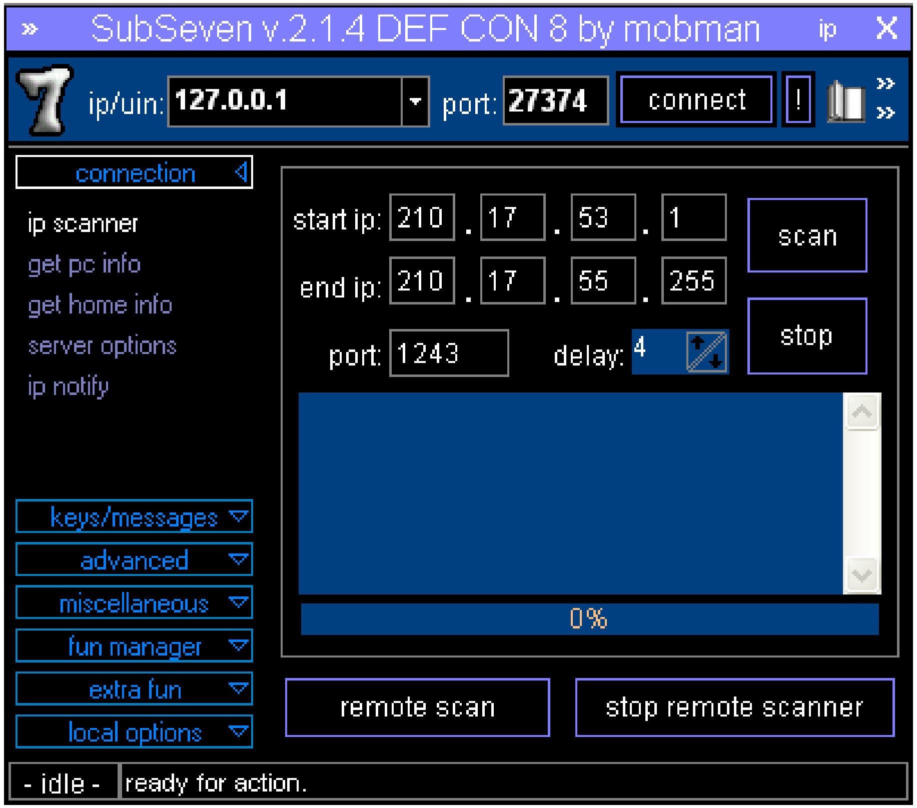
http://subseven.slak.org

http://www.defcon.org

- idle - ready for action.

Subseven\connection

- IP scanner:
- To search the net for a host that infected with subseven server after you inter the port no. you should enter the range which should not more than 255.



SubSeven v.2.1.4 DEF CON 8 by mobman

ip/uin: 127.0.0.1

port: 27374

start ip: 210 . 17 . 53 . 1

end ip: 210 . 17 . 55 . 255

port: 1243

delay: 4

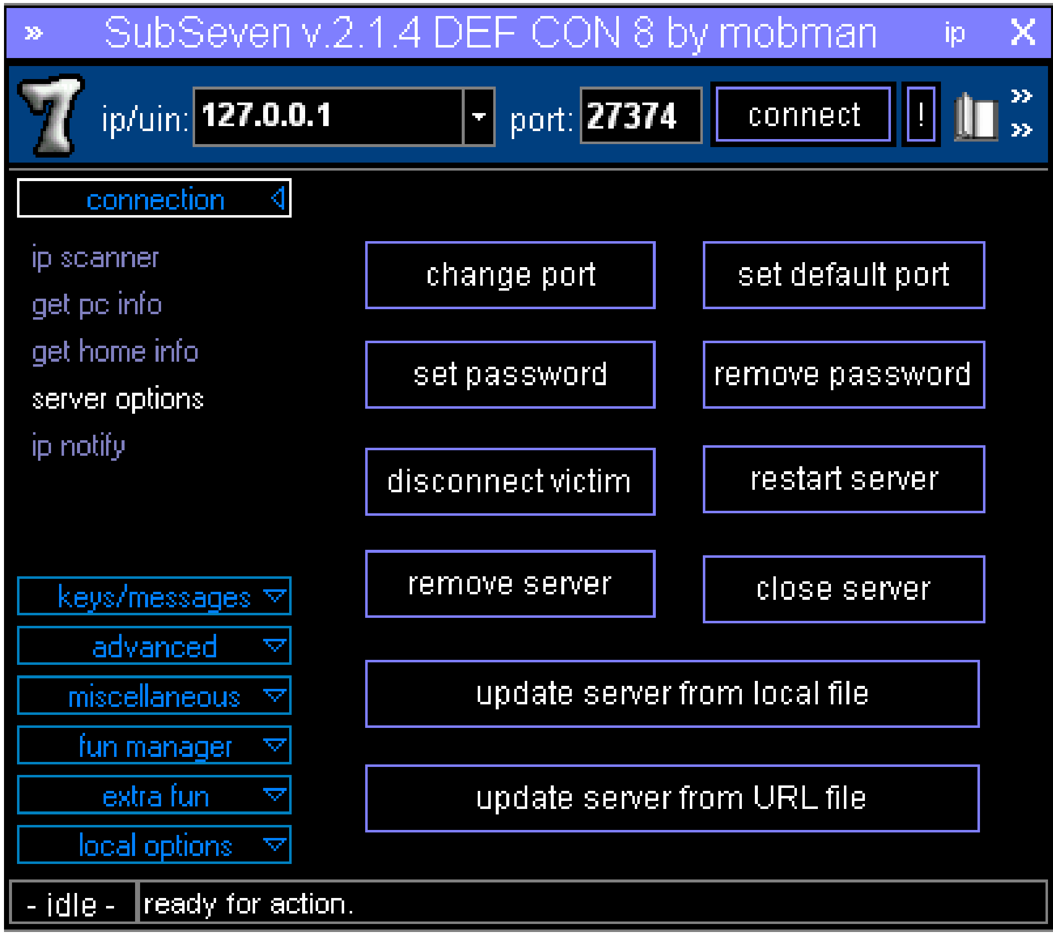
0%

- idle -

ready for action.

Subseven\connection

- Server options: this is help you to control your sever by put a password, remove password, update it …etc.



SubSeven v.2.1.4 DEF CON 8 by mobman

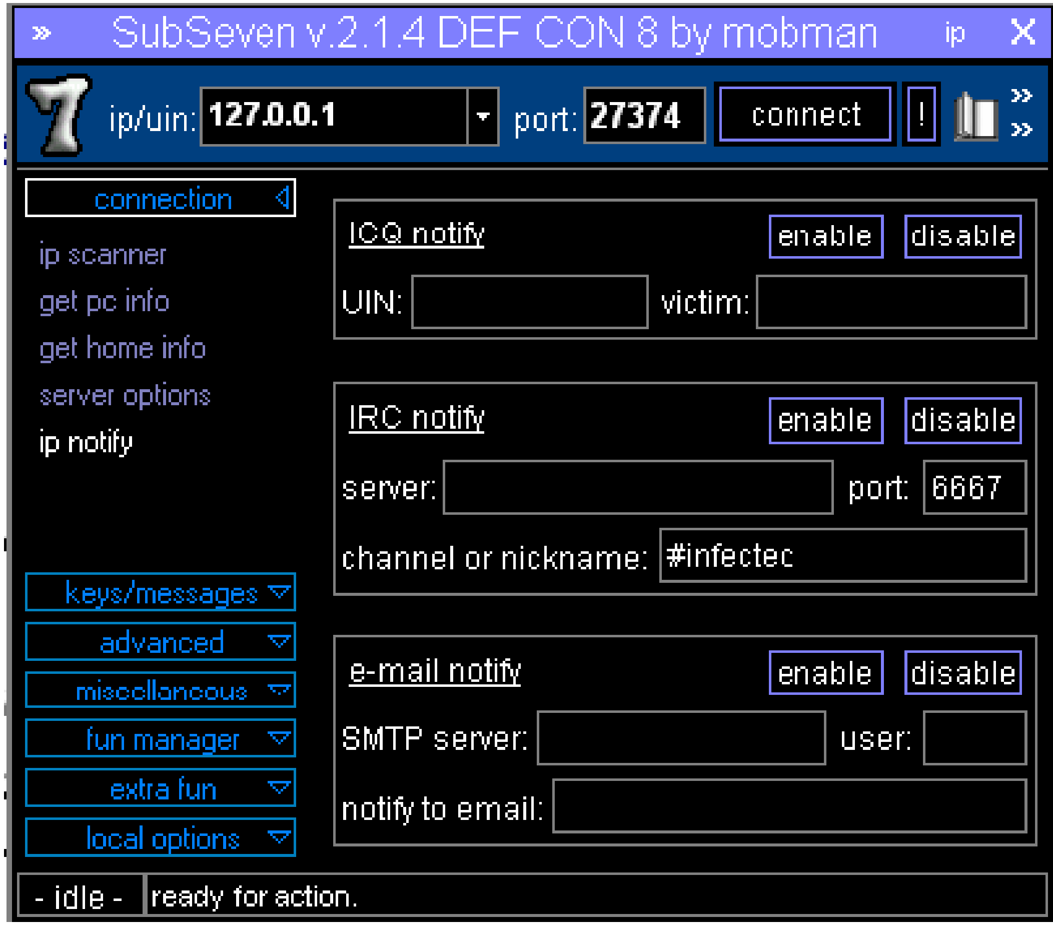
ip/uin: 127.0.0.1

port: 27374

- idle - ready for action.

Subseven\connection

- IP notification:
  set or disable the notification methods when the server is activated and connected to the net.



SubSeven v.2.1.4 DEF CON 8 by mobman

ip/uin: 127.0.0.1

port: 27374

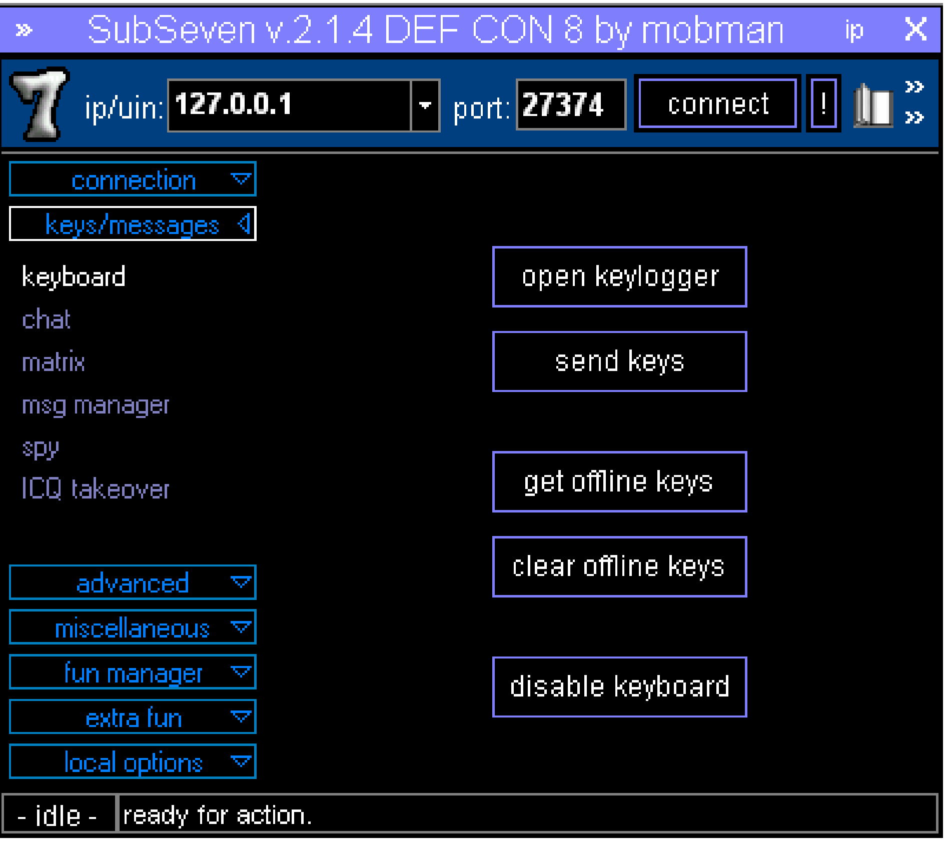
IRC notify port: 6667

channel or nickname: #infectec

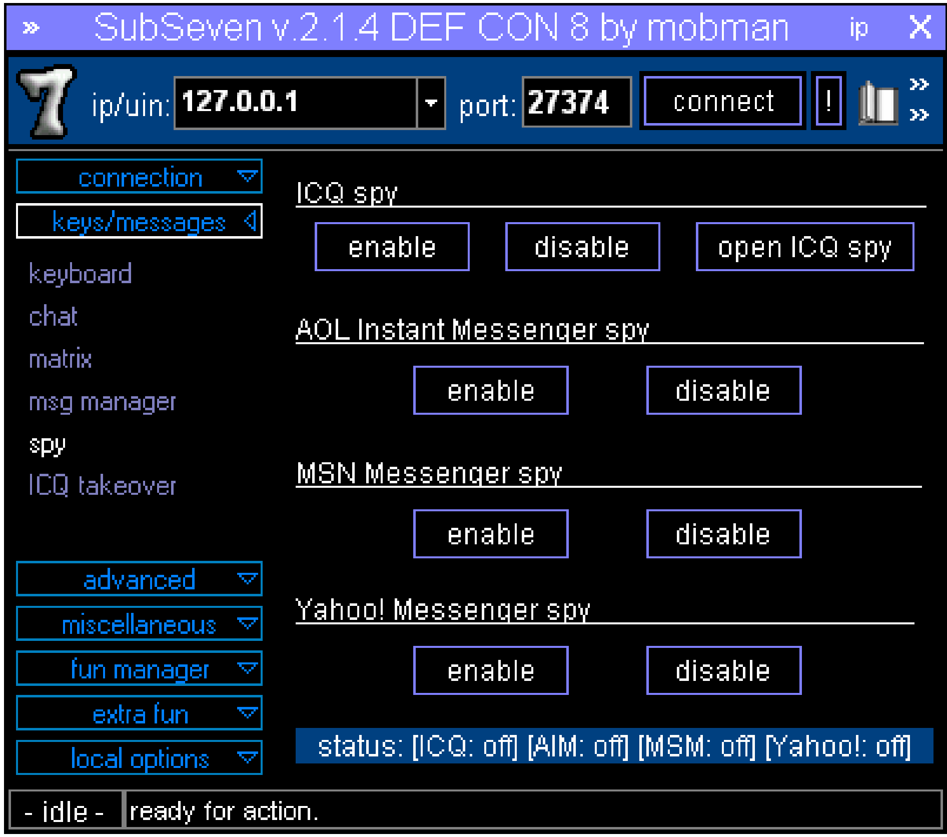
- idle - ready for action.

Subseven: Key\messages

- control victim keyboard by disable the keys or change their functions…etc.
- spy on victim chat messages



ready for action.

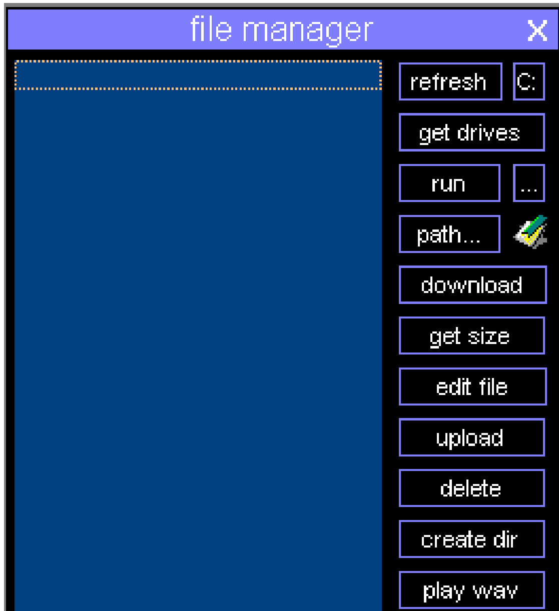


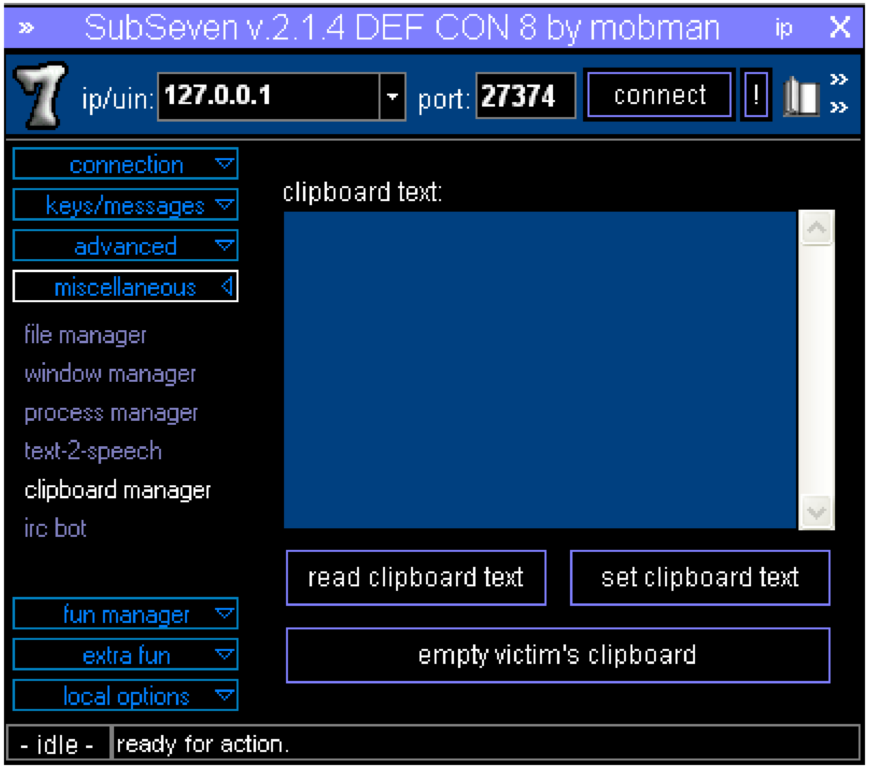
status: [ICQ: off] [AIM: off] [MSM: off] [Yahoo!: off]

ready for action.

Subseven: miscellaneous

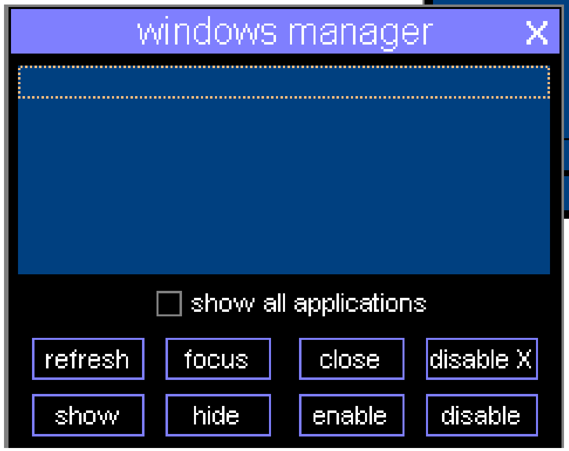
- File manager
- Windows manager
- Clipboard manager: display all victim keystrokes




SubSeven v.2.1.4 DEF CON 8 by mobman

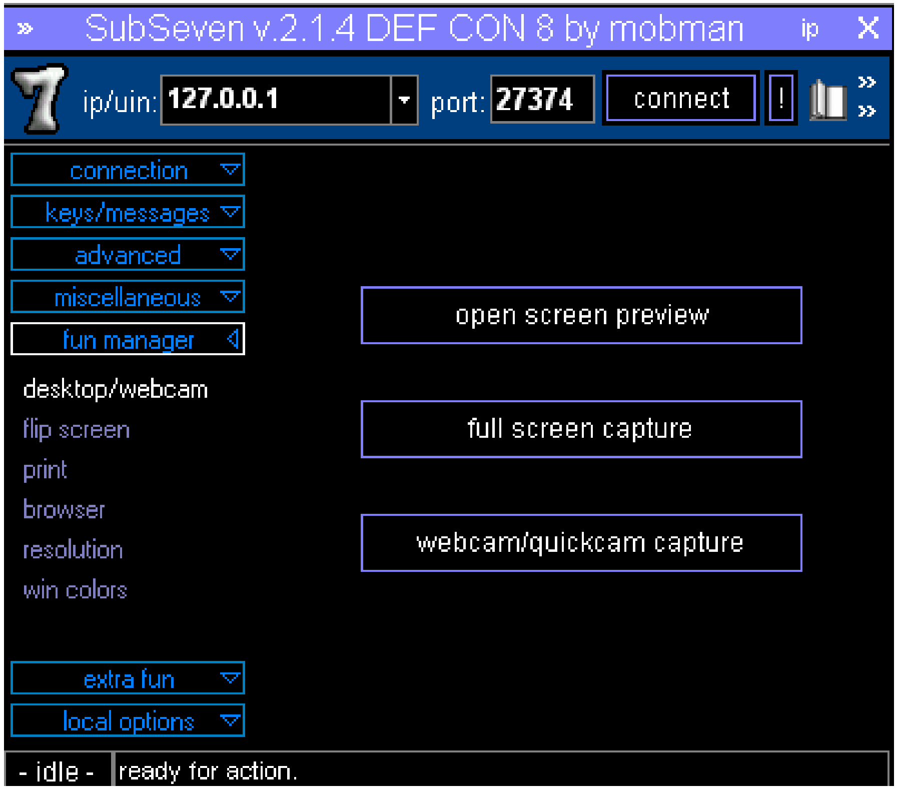
ip/uin: 127.0.0.1 port: 27374

- idle - ready for action.



Subseven: fun manager

- Desktop/webcam from this option you can see the victim desktop or his web camera if its open



SubSeven v.2.1.4 DEF CON 8 by mobman

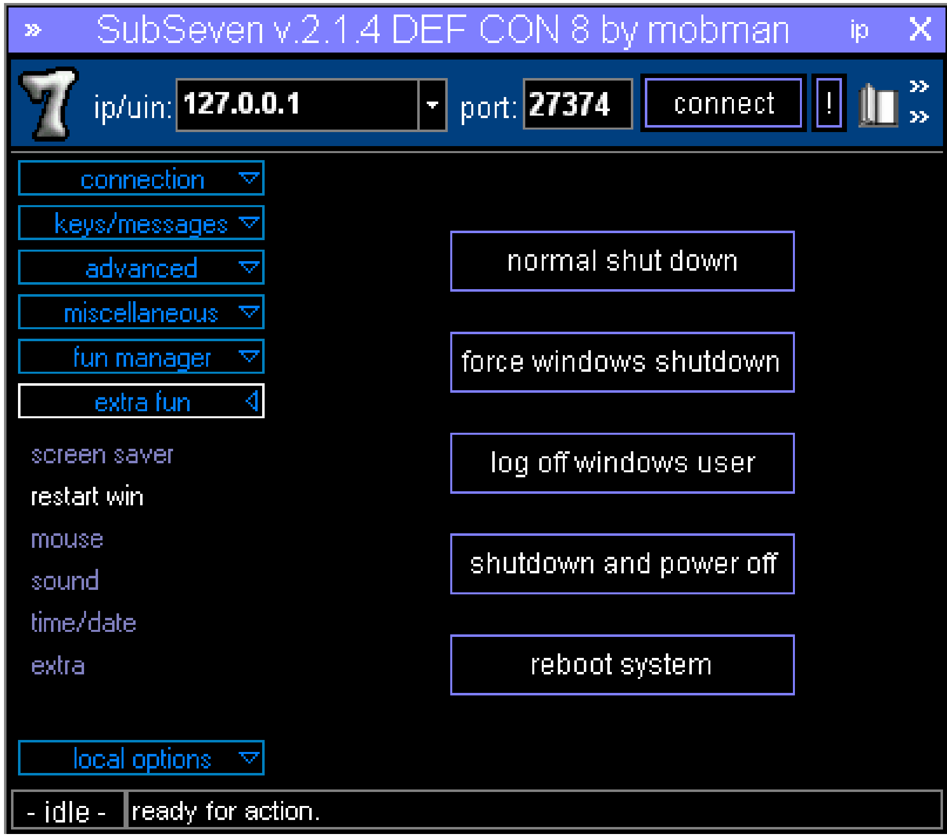
ip/uin: 127.0.0.1

port: 27374

- idle - ready for action.

Subseven: extra fun

- Restart win: another option to control the victim PC that enable you to shutdown it's PC, restart…etc.



SubSeven v.2.1.4 DEF CON 8 by mobman

ip/uin: 127.0.0.1

port: 27374

- idle -

ready for action.

Resources

- http://en.wikipedia.org/wiki/Remote_administration_tool
- http://en.wikipedia.org/wiki/Backdoor
- http://www.2-spyware.com/backdoors-removal
- Mitigating Insider Threats to RSA Key Generation (white paper)
- http://www.elfqrin.com/docs/biospw.html
- http://www.trojan.ch/papers/SANS04.pdf