Back Orifice

A Virus, Trojan and Backdoor

Back Orifice Overview

Back Orifice (BO) is one of the first remote access tools

BO designed to run on MS Windows

BO was probably designed for nefarious use

Although Cult of the Dead Cow *claims differently*

BO is considered malicious

We will see this later

BO can be configured to be "stealthy"

BO is targeted at attacking Windows operating systems

Back Orifice Overview

BO is a client/server system

- *Server runs on the victim machine*
- *Client runs on the remote or attacker machine*

BO does not require installation on the victim computer because

- *It does not want itself known to Windows*
- *So it does not use the Registry*
- *Instead BO carries all its parameters with the BO server*
- *It is self contained except for things such as keylog files*

Back Orifice Design

Back Orifice is designed as a **framework** with a specification for plugins

But the BO framework has some "built-ins"

There have been a number of plugins written for BO by other than the original coders

Some benign

Some malicious

We will discuss the built-ins and some of the plugins

Later you can try them out

Back Orifice Built-Ins

BO has two built-ins

- *Startup*
- *Stealth*

The ***Startup*** Built-in tells BO what to do initially

- *What type of initial basic network plugin to use*
- *Initial port number*
- *Initial encryption plugin*
- *Initial password (or none)*
- *Idle timeout*

Back Orifice Built-Ins

The ***Stealth*** built-in can be configured to tell BO how stealthy to be on the server

- *Run BO when the computer boots*
- *Appears to disappear after starting*
- *Changes the BO process name by adding spaces and the letter "e" at the end, making it hard for Windows to delete it*
- *Copy and rename itself*
- *Hide itself from the Windows task list*
- *Attach itself to a legitimate executable*
  - This seems not to work for WinXP, Win2003Server or more advanced versions of Windows
- *Register as a service in the Windows registry*

Back Orifice Basic Plugins

io_tcp.dll

- *Both **server** and **client** plugins are needed*
- *Supports basic **TCP** communications via a specific server port*

io_udp.dll

- *Both **server** and **client** plugins are needed*
- *Supports basic **UDP** communications via a specific server port*

Back Orifice Basic Plugins

enc_null.dll

- *Both **server** and **client** plugins are needed*
- *Supports unencrypted operation*

auth_null.dll

- *Both **server** and **client** plugins are needed*
- *Supports operation without a password*

srv_control.dll

- ***Server only** plugin*
- *Supports basic server control by client*

Back Orifice Basic

With only

The built-ins and

The basic plugins

One can run Back Orifice

Encryption Plugins

There are a number of additional plugins, each of which uses a different encryption algorithm

Some of these are:

enc_serpent (client & server)

Supports Serpent encryption

128-bit block cipher with 128-bit key(I think)

enc_aes (client & server)

Supports NIST's Advanced Encryption Standard

enc_idea (client & server)

Supports the IDEA encryption algorithm

…

GUI Plugins

misc_bopeep.dll (client & server)

- *Provides a video stream from the server to the client*
  - User at client can see what a user at the server is doing
  - Can be made very stealthy with low network I/O by keeping the size of the "peep" window small
- *Can also take over (hijack) the mouse and keyboard*
  - Victim mouse or keyboard or both are disabled

srv_winman.dll (server only)

- *Provides ability to hide/show windows, disable special key combinations (Ctrl-Alt-Del, Alt-Tab...), hide the desktop, hide/show the taskbar…*

GUI Plugins

BoTool

- *Provides a graphical file browser and registry editor*
- *Windows Explorer type interface*
  - File browsing, renaming, copying, moving, upload, download, file start, compression
  - Registry browsing, creating and modifying keys & values
- *Commercial product*
  - No freeware version that I can find

Server Plugins

srv_interface (server only)

Performs key logging to a hidden keylog file

Enables/disables logging at startup

srv_regfile (server only)

Provides total file and registry control on the server machine

But it is not GUI-based

Cannot easily browse

srv_gbot (server only)

Supports accessing the BO server via IRC

Notify Plugins

simpleRicq.dll

Notifies client (through the ICQ paging system) when a server system comes online and provides IP address of server computer

srv_rcgi.dll

Notifies client when a server system comes online and provides IP address of server computer through a client web page

Need a special CGI script for the browser

Rootkit Plugins

There are at least 2 rootkit plugins

- *FU rootkit*
- *NT rootkit*

These both do a number of things to hide the malicious software

Both of these are detectable using antivirus software

- *When they enter a target computer*
- *Before they execute*

Back Orifice Lab

Experiment With BO Setup

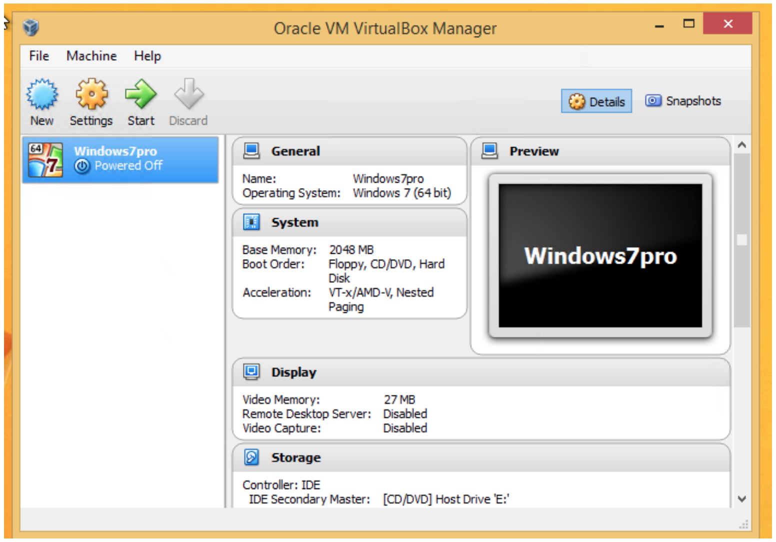
Find Oracle Virtual Box and put it on your desktop

Left click on Window button, lower left & type **virtual box**

Put a VB icon on your desktop

Open Oracle Virtual Box

You should get this



General

Name: Windows7pro
Operating System: Windows 7 (64 bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

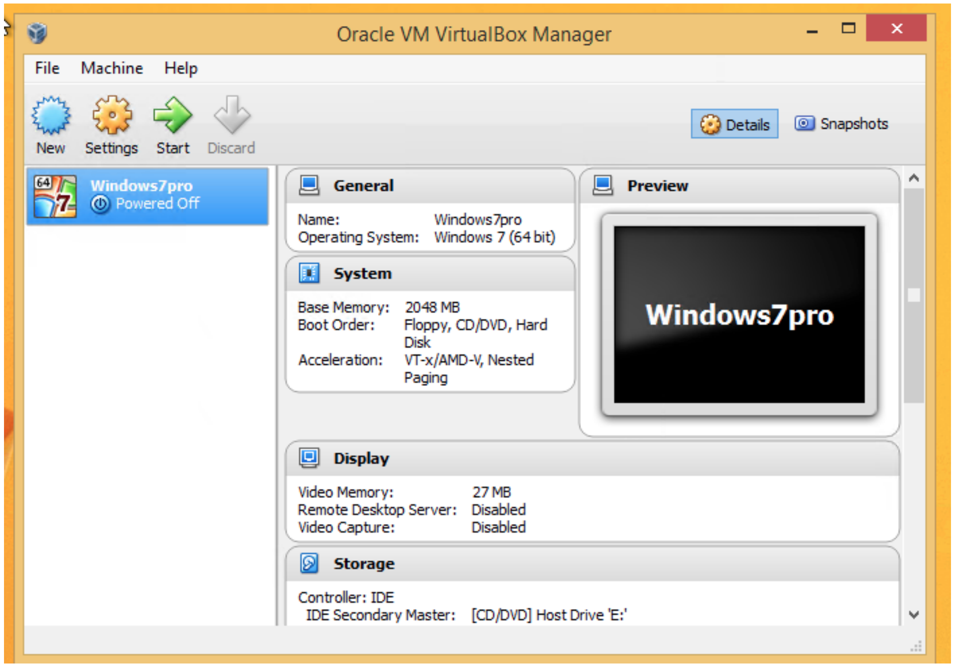
Video Memory: 27 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Host Drive 'E:'

Experiment With BO Setup

START Windows7
Login: Same as your ForSec Lab login
Password: ***forsec***



General

Name: Windows7pro
Operating System: Windows 7 (64 bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 27 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Host Drive 'E:'

Experiment With BO Setup

Create the following folders in Windows7 on your Virtual Machine

*C:\Users\**yourUserName**\itmX48\*

Experiment With BO Setup

Make sure that both your firewall and AV software are OFF

- *BO was widely used by black hats*
- *Today any malware detection software knows its signature and will detect and delete it*

Experiment With BO Setup*Turn Off Windows Firewall*

Start > Control Panel > Windows Firewall

Click on: ***Turn Windows Firewall on or off***

Turn off Windows Firewall in all 3 places

Click ***OK***

Experiment With BO Setup*Turn Off Anti Virus Software*

Right click on the **Start** icon go to **Control Panel**, and click Windows Defender

You'll get this window

Choose ***Settings***

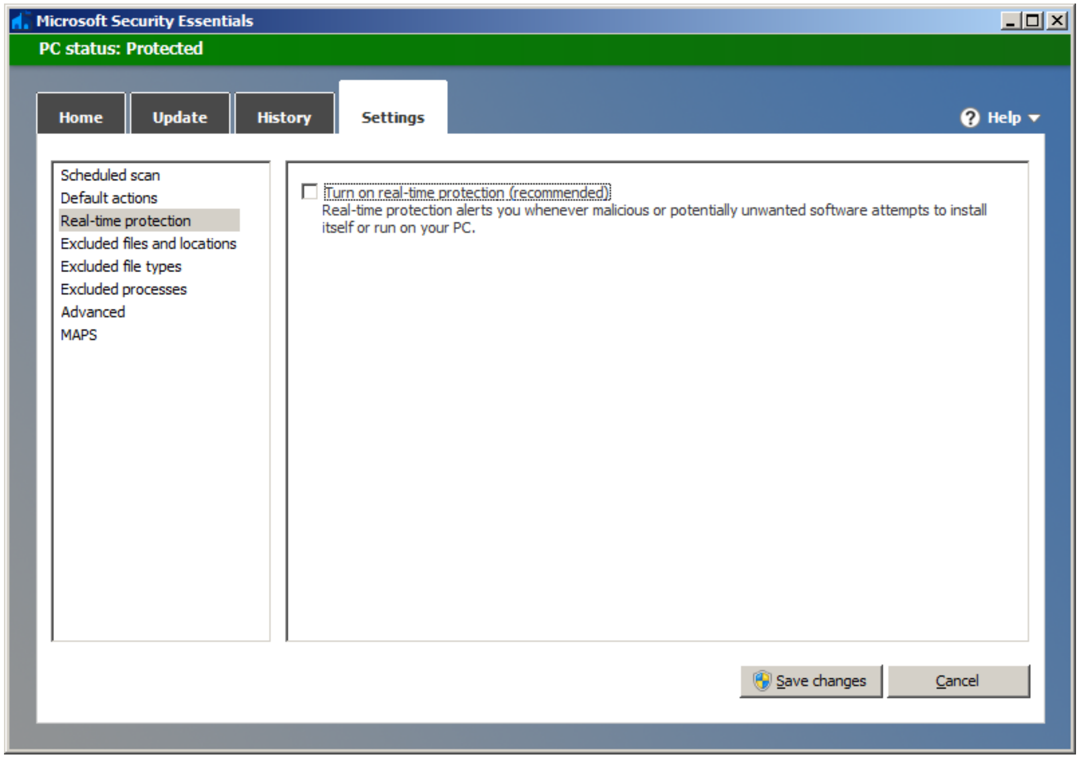
Choose ***Real time Protection***

Turn off real-time protection

Save changes

Close the window

The green icon will change to red in a few seconds



□ Turn on real-time protection (recommended)

Real-time protection alerts you whenever malicious or potentially unwanted software attempts to install itself or run on your PC.

Experiment With BO Setup

Disable UAC (User Account Control)

Control Panel -> User Accounts -> Change User Account Control settings -> Specify "Never notify" and hit OK

Restart Win7

Getting & Installing BO

Copy the entire folder W:\BO\ to

*C:\Users\**yourUserName**\itmX48\*

You should now have in your

*C:\Users\**yourUserName**\itmX48\ BO\ folder*

Two sub folders

bo2kClient\

bo2kServer\

BO Server

- I’ve already configured the BO server
- It is completely self-contained
  - *It doesn't need any installation on the target computer*
    - So it can be surreptitiously installed by a virus or worm and activated later
  - *It can be configured so that it*
    - Doesn't appear on the task list in the Windows Task Manager
    - Cannot be seen by users
    - **But we will not do that here**

BO Server

The BO <u>server</u> executable runs on the target's computer

- *The program's name is* **bo2k.exe**

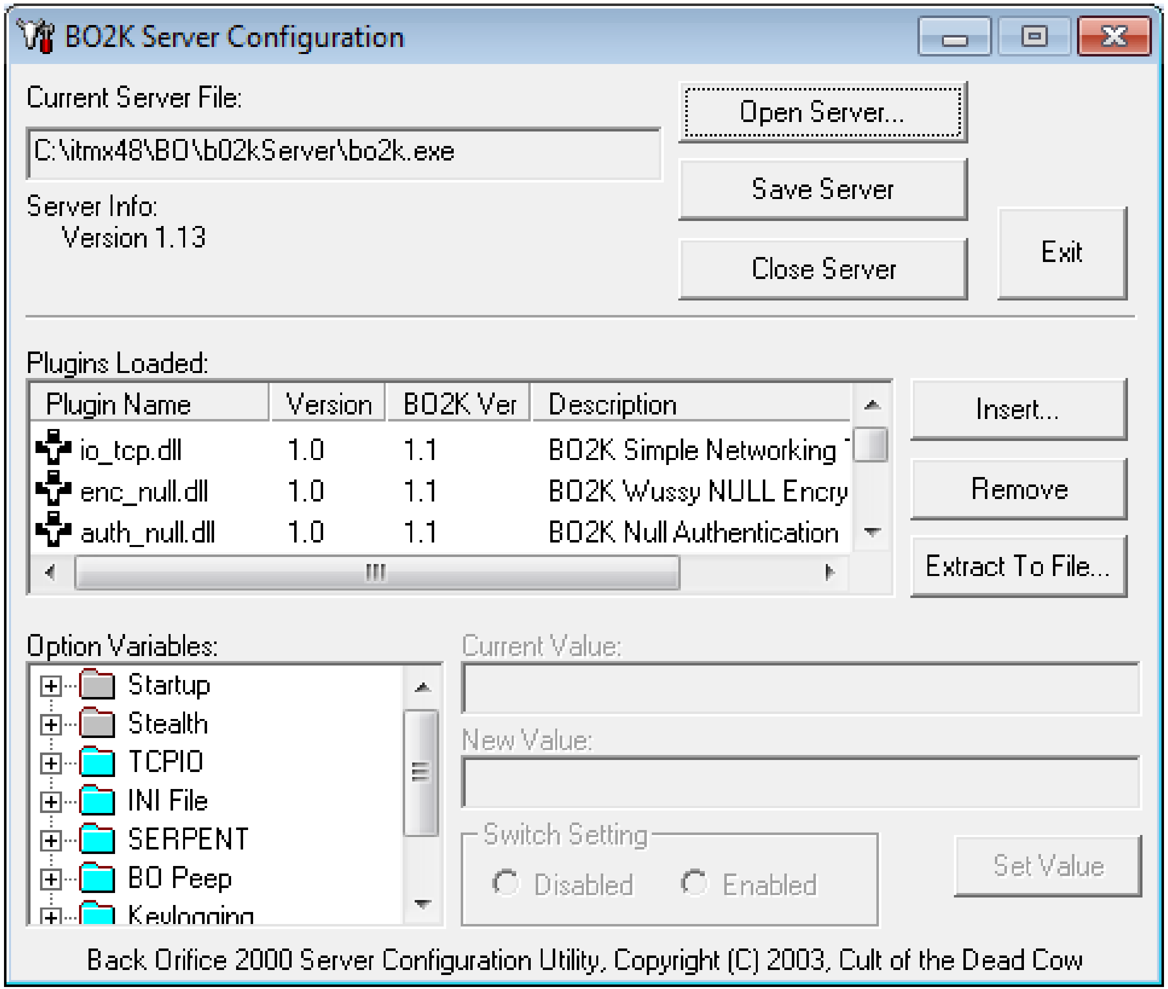
Go to the ***bo2kServer*** folder where you will find the file ***bo2kcfg.exe***

- *This is the configuration tool for* **bo2k.exe**

Run it to check the configuration of the file ***bo2k.exe*** just to give you a feel that it is configured correctly

- *Do not change anything*

BO Server Configuration GUI



Current Server File:
C:\itmx48\BO\b02kServer\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
io_tcp.dll	1.0	1.1	BO2K Simple Networking T
enc_null.dll	1.0	1.1	BO2K Wussy NULL Encry
auth_null.dll	1.0	1.1	BO2K Null Authentication

Option Variables:

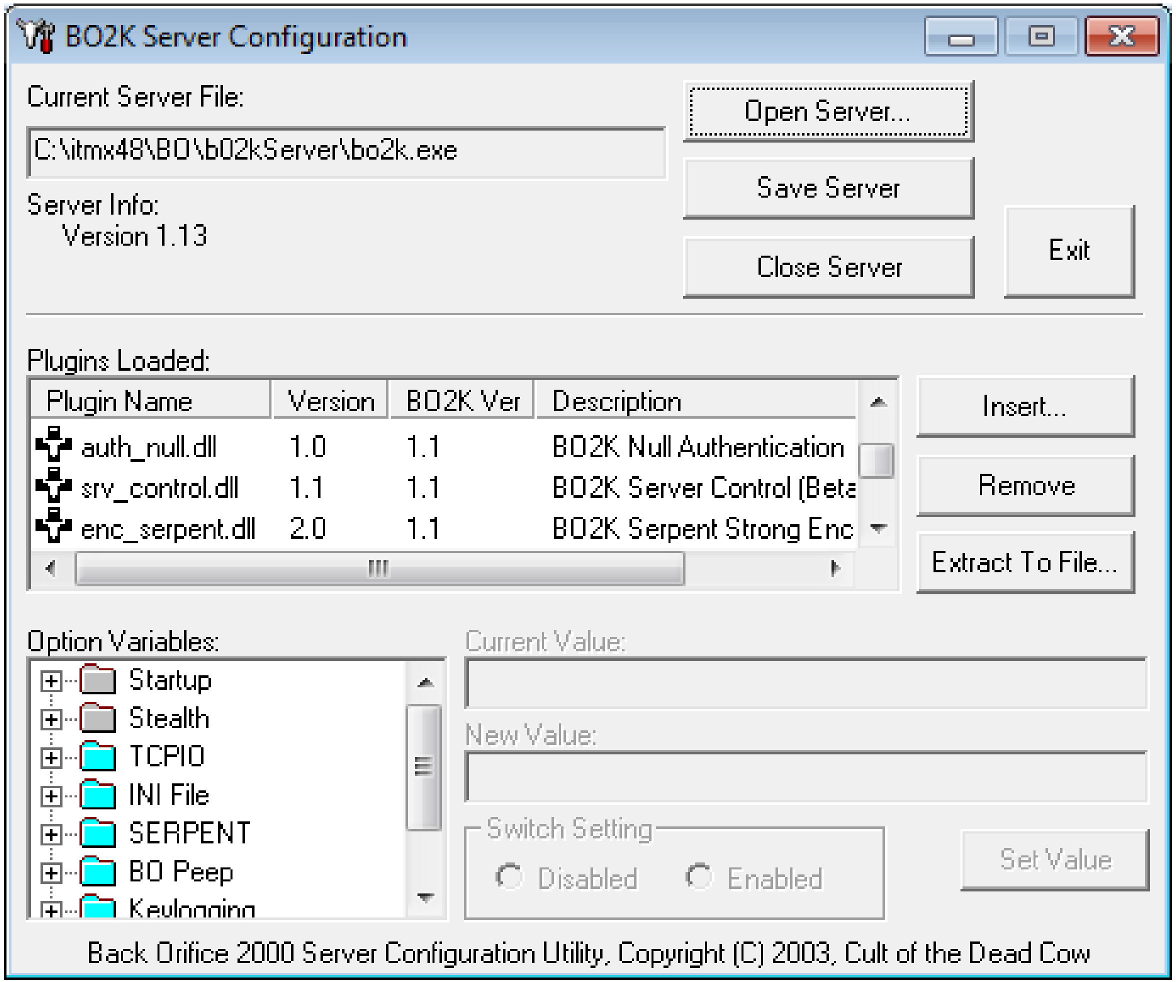
- Startup
- Stealth
- TCPIO
- INI File
- SERPENT
- BO Peep
- Keylogging

Current Value:

New Value:

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

BO Server Configuration GUI



BO2K Server Configuration

Current Server File:

C:\itmx48\BO\b02kServer\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
auth_null.dll	1.0	1.1	BO2K Null Authentication
srv_control.dll	1.1	1.1	BO2K Server Control (Beta
enc_serpent.dll	2.0	1.1	BO2K Serpent Strong Enc

Option Variables:

- Startup
- Stealth
- TCPIO
- INI File
- SERPENT
- BO Peep
- Keylogging

Current Value:

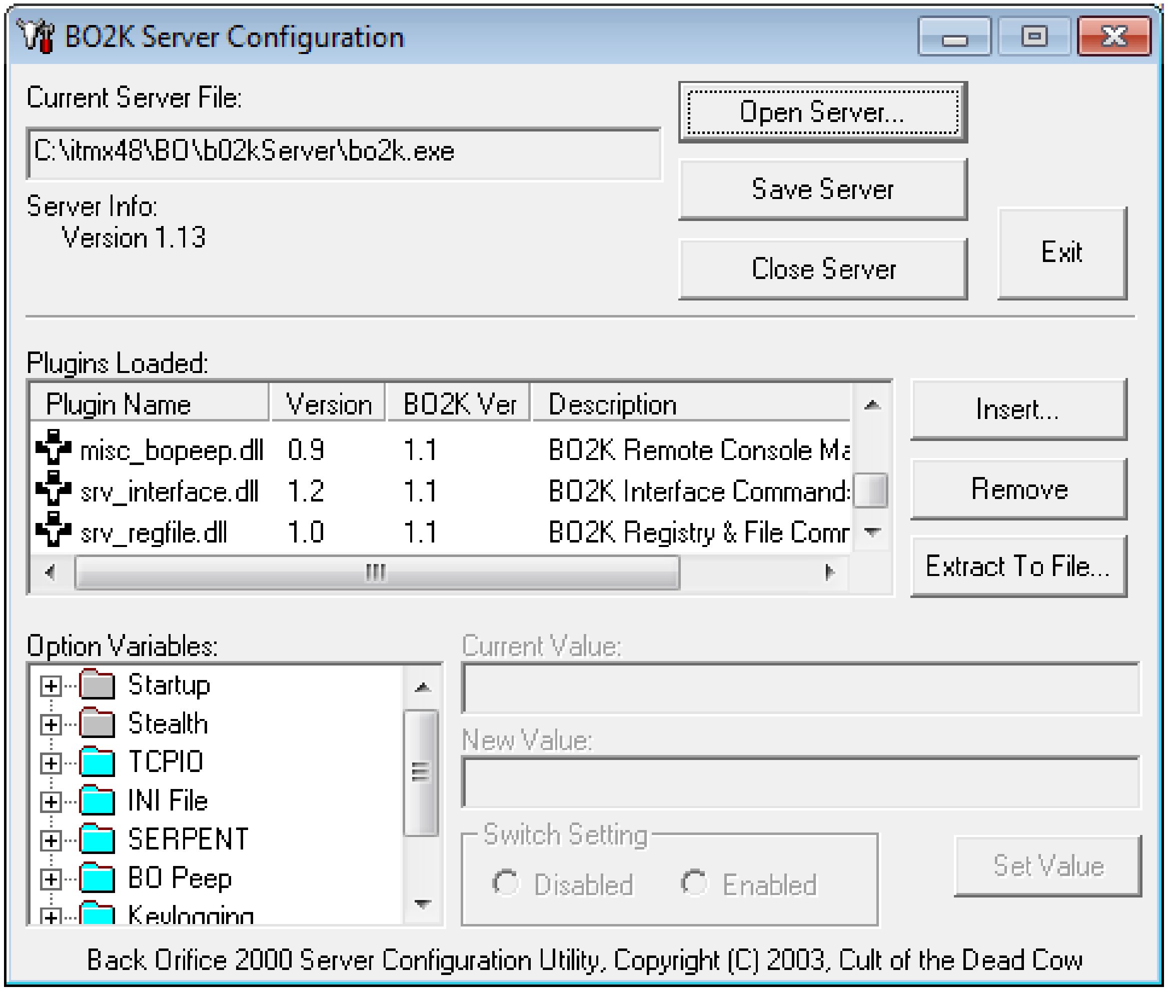
New Value:

Switch Setting

○ Disabled ○ Enabled

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

BO Server Configuration GUI



BO2K Server Configuration

Current Server File:

C:\itmx48\BO\b02kServer\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
misc_bopeep.dll	0.9	1.1	BO2K Remote Console Ma
srv_interface.dll	1.2	1.1	BO2K Interface Command:
srv_regfile.dll	1.0	1.1	BO2K Registry & File Comr

Option Variables:

- Startup
- Stealth
- TCPIO
- INI File
- SERPENT
- BO Peep
- Keylogging

Current Value:

New Value:

Switch Setting
○ Disabled ○ Enabled

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

BO Server Configuration GUI

Now **Exit** bo2kcfg.exe

Do not save anything

BO2k Client

Now let's check the configuration of the BO client

It will run it on the attacker computer

Go to the *bo2kClient* folder

Run ***bo2kgui.exe***

This is both the BO client and also the way you configure it

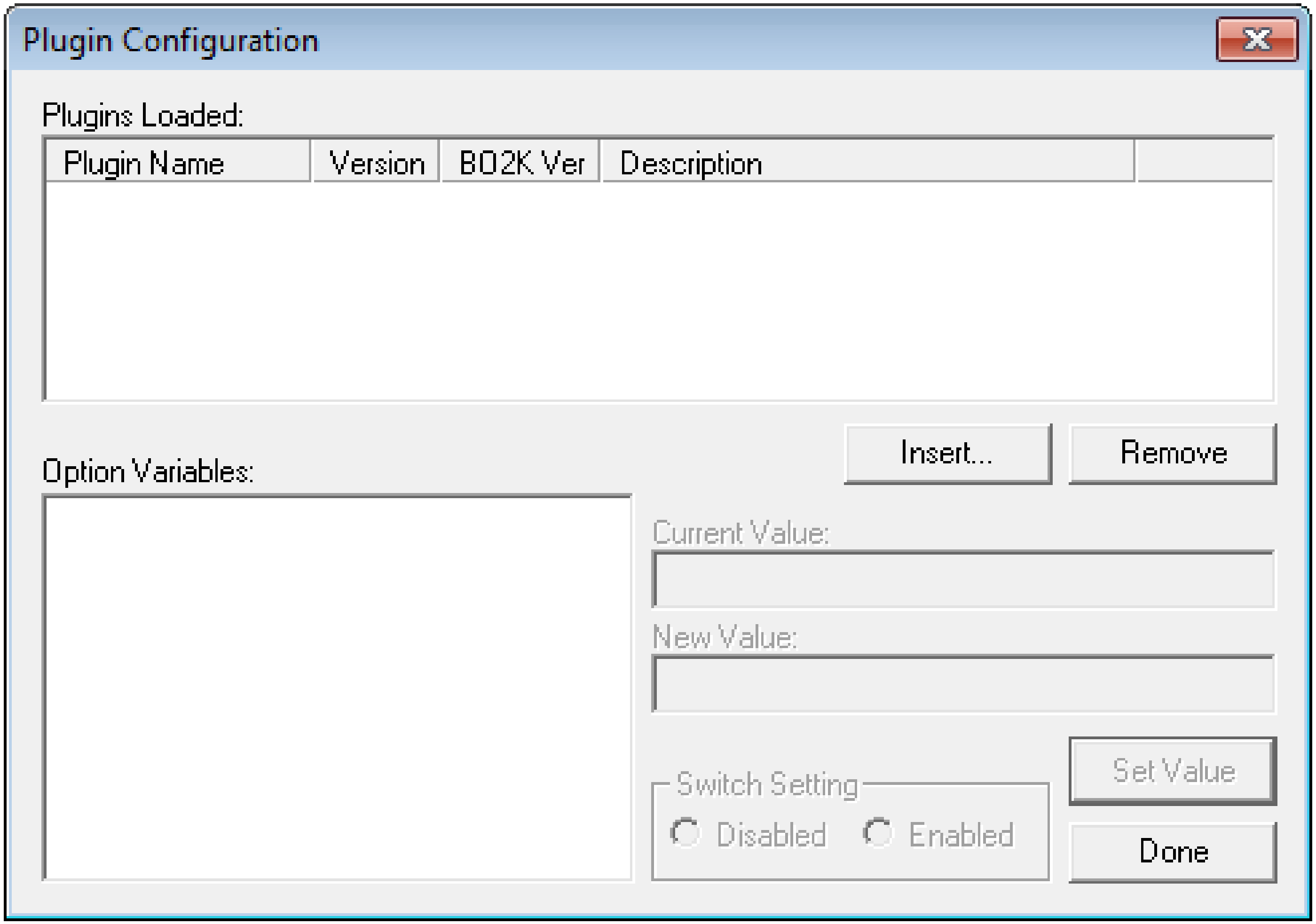
A GUI window should come up

Go to the menu *Plugins | Configure…*

You should see the GUI window shown on the next slide

You will need to insert the plugins and configure them

BO Client Configuration GUI

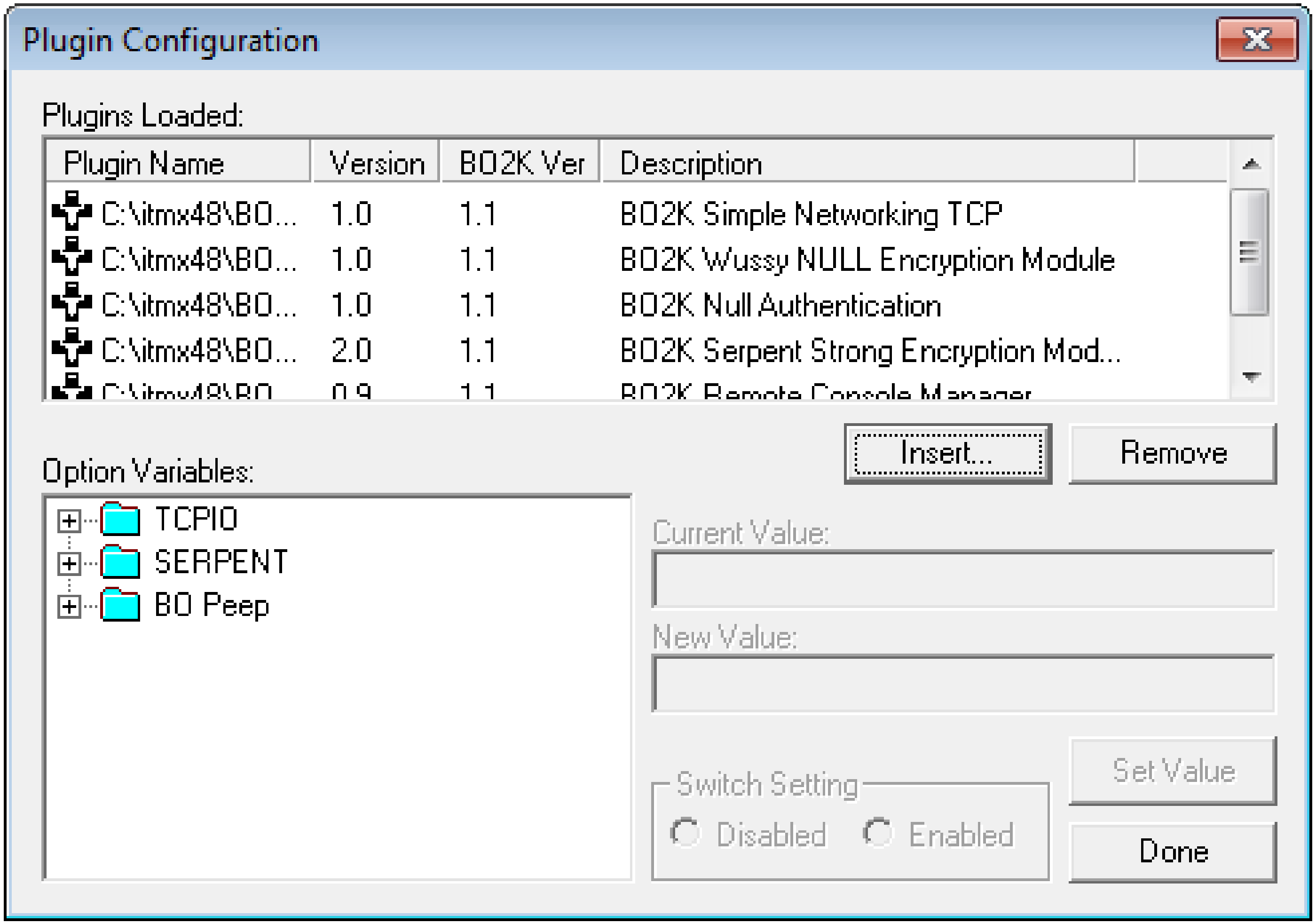


Experiment With BO

Load BO Client (Attacker) Plugins

```
.\plugins\io\io_tcp.dll
.\plugins\enc\enc_null.dll
.\plugins\auth\auth_null.dll
.\plugins\enc\enc_serpent.dll
.\plugins\misc\misc_bopeep.dll
```

BO Client Configuration GUI



Plugin Configuration

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
C:\itmx48\BO...	1.0	1.1	BO2K Simple Networking TCP
C:\itmx48\BO...	1.0	1.1	BO2K Wussy NULL Encryption Module
C:\itmx48\BO...	1.0	1.1	BO2K Null Authentication
C:\itmx48\BO...	2.0	1.1	BO2K Serpent Strong Encryption Mod...
C:\itmx48\BO...	0.9	1.1	BO2K Remote Console Manager

Option Variables:

- TCPIO
- SERPENT
- BO Peep

Current Value:

New Value:

Switch Setting: ○ Disabled ○ Enabled

Experiment With BO

Configure BO Client (Attacker) Plugins

TCPIO Default Port:	17006
Serpent Key String:	serpentkeystring

BO Peep VidStream settings

VidStream X Res	**640**
VidStream Y Res	**480**
VidStream Net Module	**TCPIO**
VidStream Bind Str	**15151**
VidStream Encryption	**SERPENT**
VidStream Auth	**NULLAUTH**

Experiment With BO
Configure BO Client (Attacker) Plugins

BO Peep Hijack settings

Hijack Net Module	**TCPIO**
Hijack Bind Str	**14141**
Hijack Encryption	**SERPENT**
Hijack Auth	**NULLAUTH**

Let's Play with Back Orifice

Experiment With BO
Server (Victim) Computer

On the target computer, run bo2k.exe

You should see bo2k.exe *in Task Manager*

Things that you can do to hide BO is to

Change its run time name

Keep it out of the Task Manager list

We have not done it here so that you can see that it's running

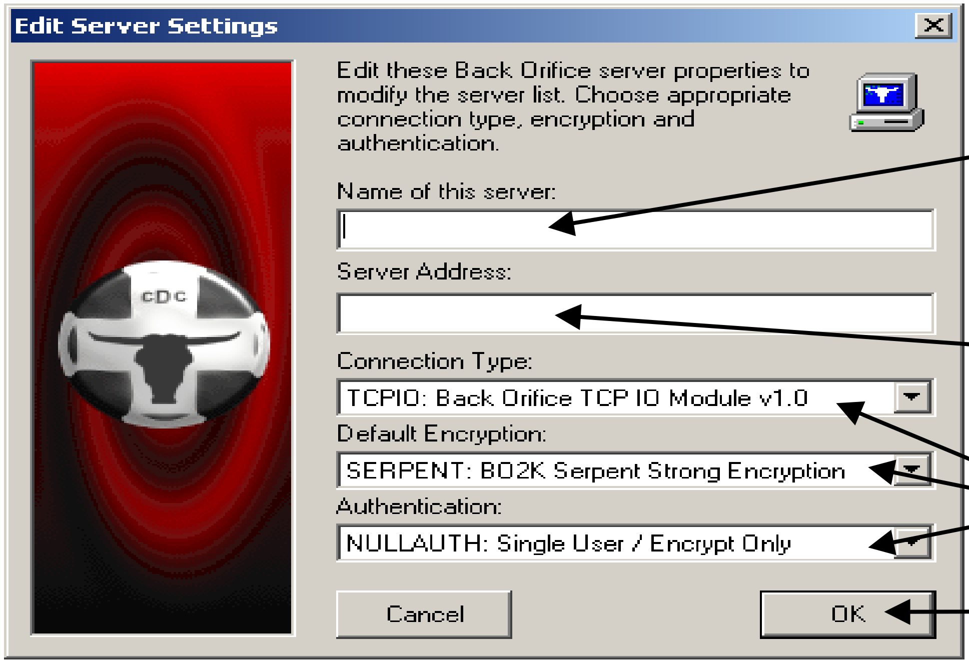
<u>Iconize</u> the Windows Task Manager

Experiment With BO*Client (Attacker)Computer Server Settings*

On the client (attacker) computer

Run bo2kgui.exe

In File | New Server create a server configuration



Edit Server Settings

Edit these Back Orifice server properties to modify the server list. Choose appropriate connection type, encryption and authentication.

Name of this server:

Server Address:

Connection Type: TCPIO: Back Orifice TCP IO Module v1.0

Default Encryption: SERPENT: BO2K Serpent Strong Encryption

Authentication: NULLAUTH: Single User / Encrypt Only

Enter the name of the target (server) computer.
This is optional.

Enter target IP address:
172.xx.yy.z

Make sure that these are selected.

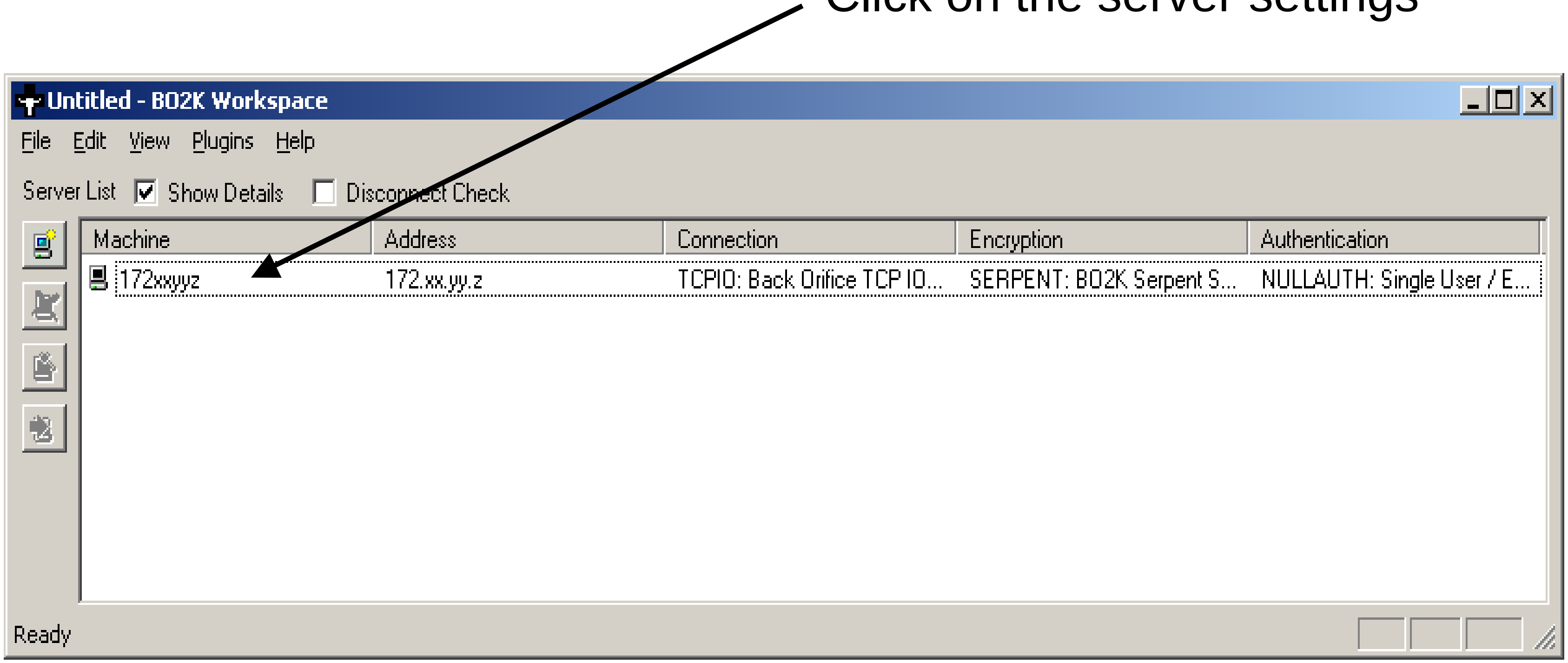
Click OK

Experiment With BO

Client (Attacker)Computer Server Settings

You will get this screen with your configuration of the client shown

Click on the server settings



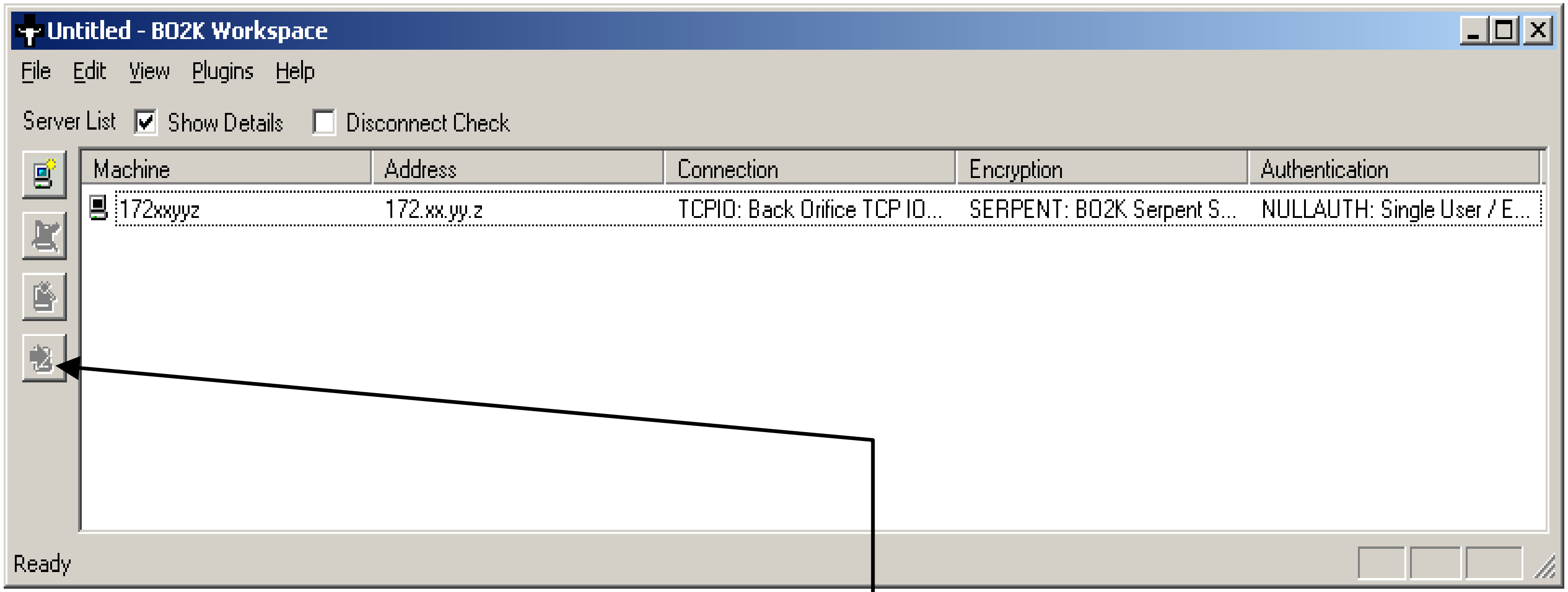
Untitled - BO2K Workspace
File Edit View Plugins Help
Server List ☑ Show Details □ Disconnect Check
Ready

Machine	Address	Connection	Encryption	Authentication
172xxyyz	172.xx.yy.z	TCPIO: Back Orifice TCP IO...	SERPENT: BO2K Serpent S...	NULLAUTH: Single User / E...

Experiment With BO

Connect to bo2k.exe on the Target

To connect to bo2k.exe on the target computer



Server List ☑ Show Details □ Disconnect Check

Machine	Address	Connection	Encryption	Authentication
172xxyyz	172.xx.yy.z	TCPIO: Back Orifice TCP IO...	SERPENT: BO2K Serpent S...	NULLAUTH: Single User / E...

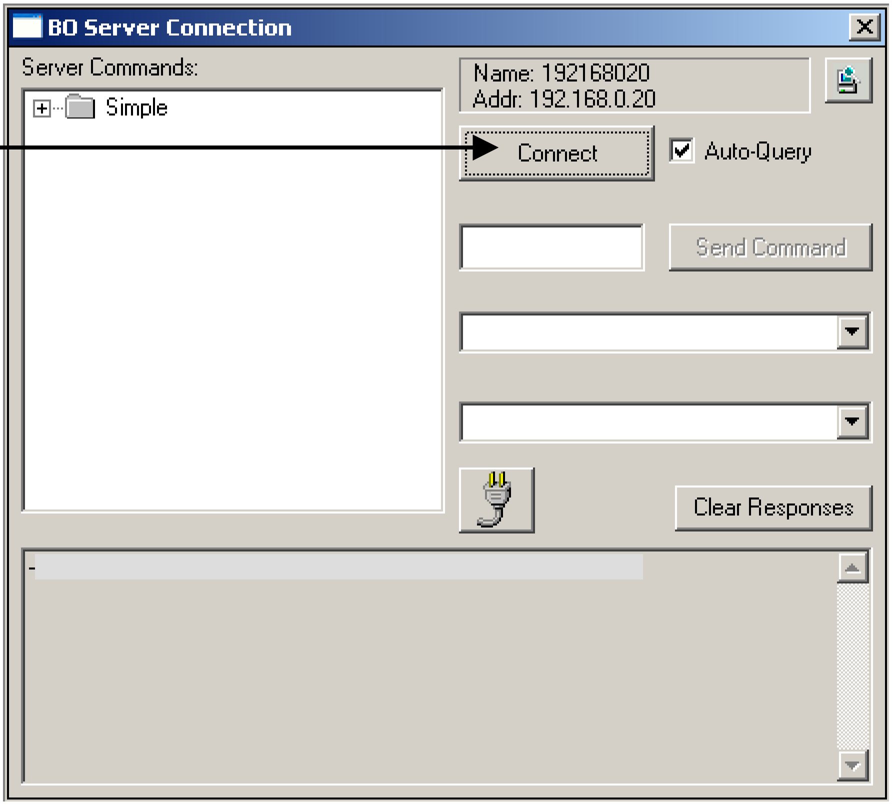
Ready

connect

Experiment With BO

Connect to Server (Victim)

If you did things right you should get the following screen



Click

BO Server Connection

Server Commands:

Name: 192168020
Addr: 192.168.0.20

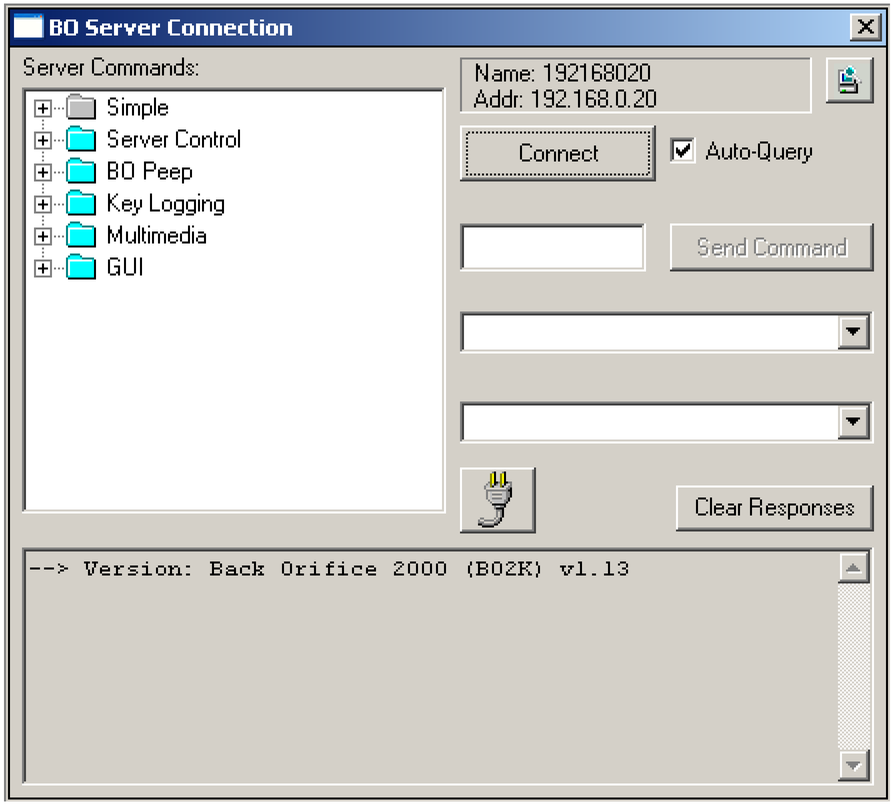
☑ Auto-Query

Experiment With BO

Connect to Server (Victim)

You should now see the screen shown

If you have this, then let's open up some of the blue folders and try different items



BO Server Connection

Server Commands:

- Simple
- Server Control
- BO Peep
- Key Logging
- Multimedia
- GUI

Name: 192168020
Addr: 192.168.0.20

☑ Auto-Query

```
--> Version: Back Orifice 2000 (BO2K) v1.13
```

Experiment With BO
GUI --> System Message Box

Open the ***GUI*** folder on the attacker

Highlight ***System Message Box***

Enter a **Title** and a **Message**

e.g., Warning

I can see what you're doing.

Click on the ***Send Command*** button

QUESTION: What's on the target machine?

Experiment With BO
Log keystrokes

Open Key Logging

Click on ***Log Keystrokes***

Give the file path and location on the victim

C:\keylog

Click ***Send Command*** button

Type a short sentence on the victim computer

Doesn't need to be in any application

Click ***View Keystroke Log*** and then ***Send Command***

Click ***End Keystroke Log*** and then ***Send Command***

QUESTION: Where is the file C:\keylog?

Experiment With BO

Try some Other Things

Now try some other BO "features"

But don't try BO Peep yet

BO Peep is a bit more complicated to explain, so I'll show you

Now Let’s Do BO Peep

Bo Peep VidStream

Make sure that you're still connected.

Then in the ***BO Server Connection*** window open the ***BO Peep*** folder

Click on ***StartVidStream***

Set ***FPS*** to **5**, ***Xres,Yres*** to **500, 375**, ***Bind to*** to **15151**

The last two are the numbers configured in the BO Peep plugin in the bo2k server

Next click on ***Send Command***

You should see "VidStream started on <ipaddr>:15151

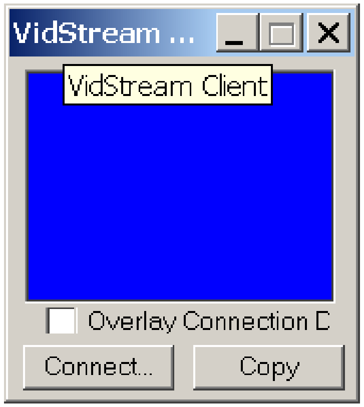
BoPeep VidStream

Now in the ***BO Workspace*** window, click on

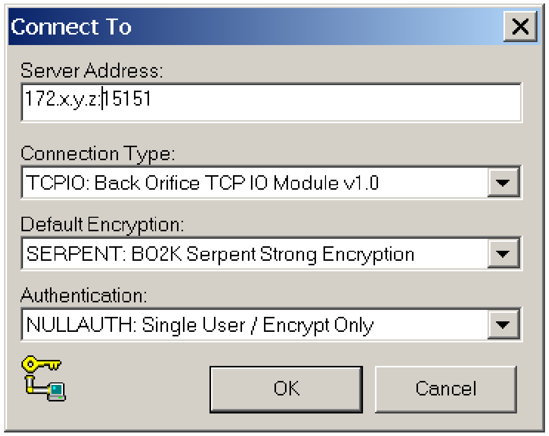
Plugins > BO Peep > VidStream Client

You should see a small window.

Click on Connect



A window will pop up that allows you to configure the VidStream Client



Server Address: 172.x.y.z:15151

Connection Type: TCPIO: Back Orifice TCP IO Module v1.0

Default Encryption: SERPENT: BO2K Serpent Strong Encryption

Authentication: NULLAUTH: Single User / Encrypt Only

BoPeep Hijack

In the BO Server Connection click on Start Hijack

You'll get this window

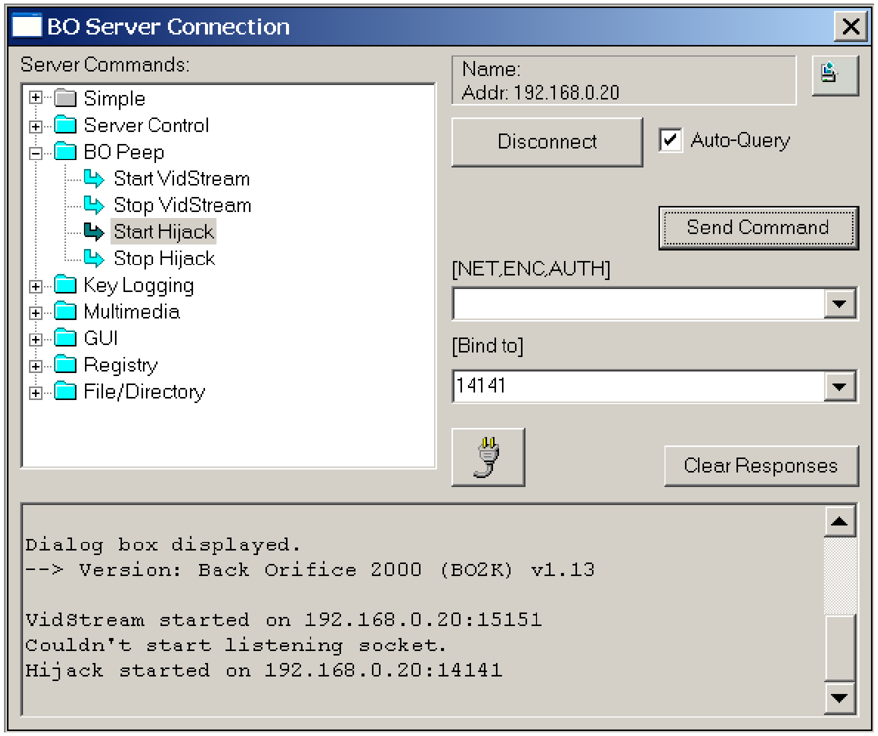
Leave [NET,ENC,AUTH] empty

Bind to 14141

Send Command

You shoud see

Hijack started on <ipaddr>:14141



Name:
Addr: 192.168.0.20

☑ Auto-Query

[NET,ENC,AUTH]

[Bind to] 14141

```
Dialog box displayed.
--> Version: Back Orifice 2000 (BO2K) v1.13

VidStream started on 192.168.0.20:15151
Couldn't start listening socket.
Hijack started on 192.168.0.20:14141
```

BoPeep Hijack

In the BO2K Workspace window

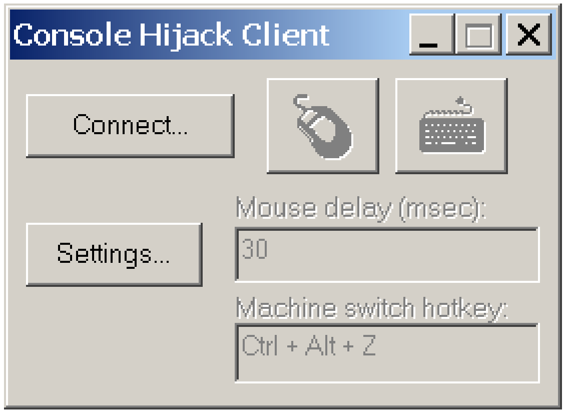
Click on Plugins > BO Peep > Hijack Client

You should get

Click on Connect

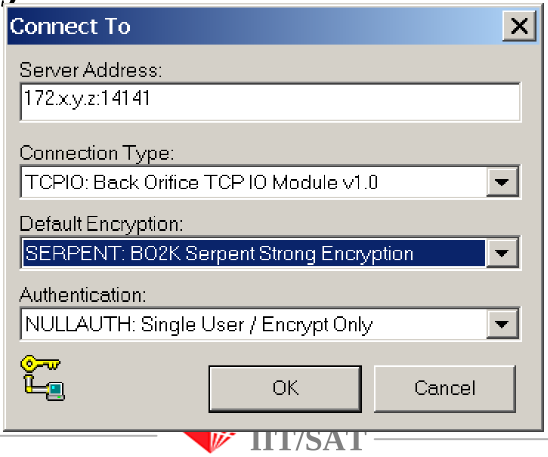
You get

Configure the Hijuac Client as shown



Mouse delay (msec): 30

Machine switch hotkey: Ctrl + Alt + Z



Server Address: 172.x.y.z:14141

Connection Type: TCPIO: Back Orifice TCP IO Module v1.0

Default Encryption: SERPENT: BO2K Serpent Strong Encryption

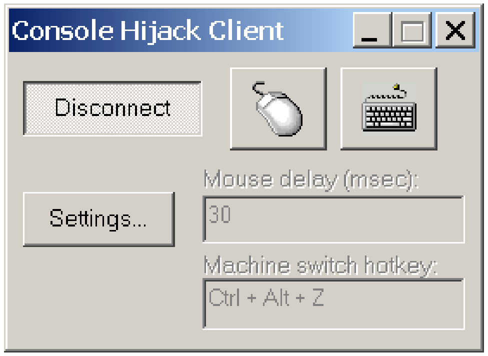
Authentication: NULLAUTH: Single User / Encrypt Only

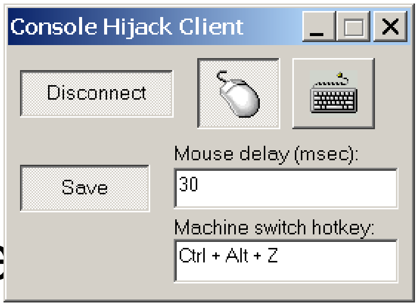
BoPeep Hijack

You should get

THEN, click on Settings…

You get





To take over the mouse, click on the mouse

Ditto for the keyboard

To take over both, click on both

Then type Ctrl + Alt + z