Making Your Own Botnet – Premium Noob Proof 100% Working Guide

By D00MR4ZR

Hello and thanks on purchasing this e-book fellow hackers, I want to greet you and teach you how to become a professional through easy to follow steps on making a network of infected computers. First you need to get a server, and we will start with getting a Virtual Private Server which are cheap and good for starters.
To start go here: http://www.joinvps.com/vps_hosting

And order desired VPS. After your order has been done you will need to install IRCd on your server. To do that you must connect to your server via Putty which you can get here:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Also in the JoinVPS Control Panel, access the server via ISP Manager and follow the wizard for choosing the root password, you can see about that in text which follows.
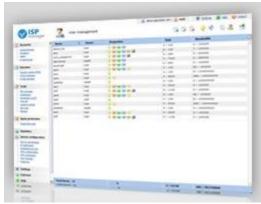
ISPmanager

ISPmanager Lite control panel works from the Internet browser and gives the great range of opportunities for Virtual hosting accounts and the full servers control.

Due to the Multi-level access system, each user who has an account on your VPS hosting, will have his own options set in ISPmanager Lite. User-friendly interface will help you to control your servers easily.

Buying our Virtual Private Server, you will get access to ISPmanager Lite. Just log in with your user name and password, and you will see that everything was made for your comfort.

The Multi-level access system allows every user access to the functions he/she needs. That means that Virtual Private server administrator can control all the VPS and all the sites hosted there. But in case of sites administrators, ISPmanager Lite is designed to manage their sites only.
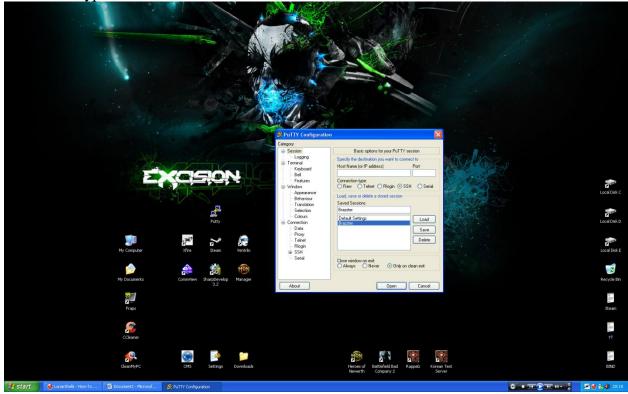

‣ Video channel
‣ Documentation
‣ Forum

We would like to offer you the control panel ISPmanager Professional. You can setup it on your VPS at extra cost.

When you are finally ready to connect open up Putty and type in Server's IP and port and select SSH access type like here:

When you press "Open" the server will load. Now it asks for login and you put in: root and press Enter.
After that it asks for password and you type the password you chose in ISP Manager.
Now you are connected and working on UNIX derivation called FreeBSD. More information about it you can find here:
http://www.freebsd.org/

Now it is time to install UnrealIRCd shell to your server. Some people like to use customized daemons, but I would recommend this one, just because of the reason that none of the skiddies tampered with it. To install it and configure it just follow these steps and type command after command in root:

Downloading and Untarring

1. wget http://unreal.brueggisite.de/Unreal3.2.8.1.tar.gz
2. tar zxvf Unreal3.2.8.1.tar.gz

Notice that it's case-sensitive. Everything in unix is case-sensitive. Keep that in mind for everything in the future.

3. rm Unreal3.2.8.1.tar.gz

Installing

1. cd Unreal3.2
2. ./Config

So we've got the script running. The first thing you're greeted with is the release notes for Unreal 3.2.8.1, now this is a lot of reading, and isn't really necessary, so just press enter once, then spacebar until you see:

==[ADDITIONAL INFO]==
* See ChangeLog
[Enter to continue]

Press enter and you'll be greeted with the first question.

Do you want to enable the server anti-spoof protection?
[No] ->

I've never actually come across a server that uses this, so just press enter to move on to the second question.

What directory are all the server configuration files in?
[/usr/local/username/Unreal3.2/] ->

Well we haven't changed the directory, so just press enter to move on to the third question.

What is the path to the ircd binary including the name of the binary?
[/usr/local/username/Unreal3.2/src/ircd] ->

Again, we haven't changed this path, so just press enter to move on to the fourth question.

Would you like to compile as a hub or as a leaf?
Type Hub to select hub and Leaf to select leaf.
[Hub] ->

If you're not going to link your server to any other IRC servers, just press enter. However, if you are going to link your server to another IRC server, and this server is going to be a leaf on that network, type 'Leaf' and press enter. If you are linking your server to another IRC server and your server will be the Hub, just press enter.

What is the hostname of the server running your IRCd?
[pluto.lunarshells.com] ->

This question has already been answered for you by the configuration script, so just press enter to move on to the next question.

What should the default permissions for your configuration files be? (Set this to 0 to disable)
It is strongly recommended that you use 0600 to prevent unwanted reading of the file
[0600] - >

The default value for this question is the one you should use, so just press enter.

Do you want to support SSL (Secure Socket Layer) connections?
[No] ->

Not many servers use this method of connection, and I doubt you will need to, and if you did, you'd know if you did, so just press enter to move on.

Do you want to enable IPv6 support?
[No] ->

You definitely don't need this feature, so just press enter to move on to the next question.

Do you want to enable ziplinks support?
[No] ->

You don't really need this feature either, and if you did, you'd know you did (sound familiar?) so press enter.

Do you want to enable remote includes?
[No] ->

You don't really need this, so just press enter to move on to the next question. Getting monotnous now isn't it? Hang in there.

Do you want to enable prefixes for chanadmin and chanowner?
This will give +a the & prefix and ~ for +q (just like +o is @)
Supported by the major clients (mIRC, xchat, epic, eggdrop, Klient, PJIRC, etc.) with the notable exceptions of irssi, KVIrc and CGI:IRC.
This feature should be enabled/disabled network-wide.
[No] ->

Well now, this is a nice feature. It pretty much explains itself though... If you have registered the channel, you will be ~yournick instead of @yournick in the channel, and anyone who you have added to the SOP list, or who is +a in the channel, will be &theirnick instead of @theirnick. Either type 'Yes' if you want to enable this feature, or just press enter if you don't want it.

What listen() backlog value do you wish to use? Some older servers
have problems with more than 5, others work fine with many more.
[5] ->

This value doesn't need to be edited, so press enter to move on to the next question.

How far back do you want to keep the nickname history?
[2000] ->
This value doesn't need to be edited either, so press enter to move on.

What is the maximum sendq length you wish to have?
[3000000] ->

You guessed it, you don't need to edit this either. Press enter to move on to the next question.

How many buffer pools would you like?
This number will be multiplied by MAXSENDQLENGTH.
[18] ->

And yet again ... just press enter to move on.

How many file descriptors (or sockets) can the IRCd use?
[1024] ->

You do need to change this value to, however many users are allowed to connect to your IRCd.

Would you like any more parameters to configure?
Write them here:
[] ->

No, we don't want to configure anything else, so just press enter and sit back while it compiles itself. You might be thinking that there were a lot of questions that you didn't need to answer, but some networks do, so don't worry any more about that.

After that has finished compiling (it should take about a minute) you'll see the following message amongst some fancy borders and other information:

Now all you have to do is type 'make' and let it compile. When that's done, you will receive other instructions on what to do next.

Configuring IRCd

Compile is now complete. Minimize Putty and do the FileZilla part now to configure your IRCd. Configuration is kinda hard and edgy part, but to do it you must have FileZilla which you can get here:
http://filezilla-project.org/download.php

When you download and install FileZilla you must open it and in "QuickConnect" fields type the server's IP, username and password. IP is same as for Putty, Port is 22, username is "root" and password is same as for Putty. When you do it press Connect to the right.

After that you are connected to Home directory of your server and will see folder called "Unreal3.2".
Open that folder and you will see "doc" folder amongst many and open it also.
Now you see bunch of files, but you need "example.conf" and since you need it, download it to your desktop.
Now you need to edit that file. Open it up in Wordpad strictly because of the linings, which affect a lot. Now start searching for (using CTRL-F) and editing these values:

1.
```
/* FOR *NIX, uncomment the following 2lines: */
//loadmodule "src/modules/commands.so";
//loadmodule "src/modules/cloak.so";
```

Make this look like this:

```
/* FOR *NIX, uncomment the following 2lines: */
loadmodule "src/modules/commands.so";
loadmodule "src/modules/cloak.so";
```

2.
```
oper Bob {
        class           clients;
        from {
                userhost bob@smithco.com;
        };
        password "f00";
        flags
        {
                netadmin;
                can_zline;
                can_gzline;
                can_gkline;
                global;
        };
};
```

Make this look like this:

```
oper YourDesiredName {
        class           clients;
        from {
                userhost bob@smithco.com;
        };
        password "Your Desired Password";
        flags
        {
                netadmin;
                can_zline;
                can_gzline;
                can_gkline;
                global;
        };
};
```

```
3.
listen          *:6697 <-Put desired port number here
{
      options
      {
            ssl;
            clientsonly;
      };
};

listen          *:6444; <-Put desired port number here
listen          *:6467; <-Put desired port number here


4.
link            hub.mynet.com
{
      username    *;
      hostname    1.2.3.4;
      bind-ip     *;
      port        7029;
      hub             *;
      password-connect "LiNk";
      password-receive "LiNk";
      class           servers;
            options {
                  /* Note: You should not use autoconnect when linking
services */
                  autoconnect;
                  ssl;
                  zip;
            };
};
```

Make this look like this:

```
link            hub.mynet.com
{
      username    *;
      hostname    1.2.3.4;
      bind-ip     *;
      port        7029;
      hub             *;
      password-connect "LiNk";
      password-receive "LiNk";
      class           servers;
            options {
                  /* Note: You should not use autoconnect when linking
services */
                  autoconnect;
            };
};
```
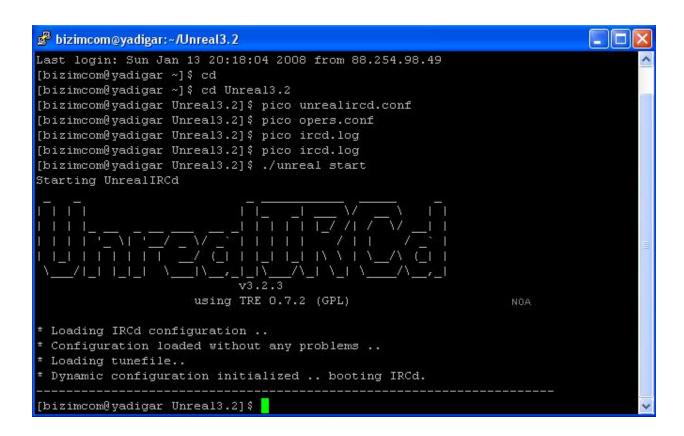
5.
```
tld {
     mask *@*.fr;
     motd "ircd.motd.fr";
     rules "ircd.rules.fr";
};
```
<-Remove this whole block from the script

6.
```
cloak-keys {
          "aoAr1HnR22w3sJ7hVz4Zb7x4YwpW"; <-Randomize this string
          "aoAr1HnR22w3sJ7hVz4Zb7kkjtpW"; <-Randomize this string
          "ao56zHnR22w3sJ7hVz4Zb7x4YwpW"; <-Randomize this string
     };
```


7.
```
set {
     kline-address "freedick@mail.com"; <-Put any mail address you want
     modes-on-connect "+ixw";
     modes-on-oper       "+xwgs";
     oper-auto-join "#opers";
     options {
          hide-ulines;
          /* You can enable ident checking here if you want */
          /* identd-check; */
          show-connect-info;
     };
```

You are now officially done with editing the config file. Save it as "unrealircd.conf" and delete "example.conf". Now upload "unrealircd.conf" file to your server in folder called "Unreal3.2". After you have uploaded "unrealircd.conf", you can start Unreal from Putty. So go back to the Putty window you have minimized and if you are in the "Unreal3.2" directory, type the following command, but if you are not you can use commands like "cd foldername" and "cd.." to navigate through folders. So the start command is:
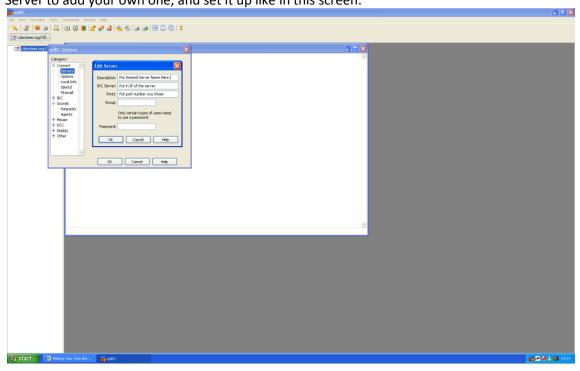
./unreal start

If you receive no errors, you should now be able to connect to your IRCd via mIRC client. If you do receive some errors you will get exact line where error is made in "unrealircd.conf" file and you can easily fix it by updating or changing data.

```
bizimcom@yadigar:~/Unreal3.2

Last login: Sun Jan 13 20:18:04 2008 from 88.254.98.49
[bizimcom@yadigar ~]$ cd
[bizimcom@yadigar ~]$ cd Unreal3.2
[bizimcom@yadigar Unreal3.2]$ pico unrealircd.conf
[bizimcom@yadigar Unreal3.2]$ pico opers.conf
[bizimcom@yadigar Unreal3.2]$ pico ircd.log
[bizimcom@yadigar Unreal3.2]$ pico ircd.log
[bizimcom@yadigar Unreal3.2]$ ./unreal start
Starting UnrealIRCd

 _   _                      _ _____     _
| | | |                    | |_   _| ___ \ / __ \   | |
| | | |_ __  _ __ ___  __ _| | | | | |_/ // /  \/ __| |
| | | | '_ \| '__/ _ \/ _` | | | | |    / | |    / _` |
| |_| | | | | | |  __/ (_| | |_| |_| |\ \ | \__/\ (_| |
 \___/|_| |_|_|  \___|\__,_|_|\___/\_| \_| \____/\__,_|
                           v3.2.3
                    using TRE 0.7.2 (GPL)                    NOA


* Loading IRCd configuration ..
* Configuration loaded without any problems ..
* Loading tunefile..
* Dynamic configuration initialized .. booting IRCd.
------------------------------------------------------------------------
[bizimcom@yadigar Unreal3.2]$
```
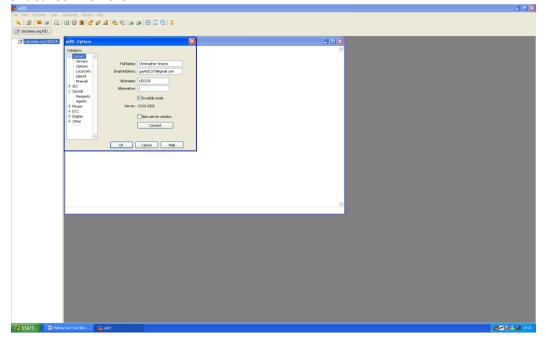
Connecting to IRCd via mIRC

Now we need to test what we have done and convince ourselves that we can start investing in bot binaries to spread and continue with our network of infected computers.
So to connect to our server fire up mIRC, go to Options andin Connect tab click on Servers and then Add Server to add your own one, and set it up like in this screen:

As you can see you do not need to edit group or put in password. After that press OK and put in random or desired info here:

Let us assume that you have succesfully connected to server and got the message of success. Now you must type in command to gain oper priviledges:

/oper username pass <-Where username and pass are the ones you typed in "unrealircd.conf".

Now you have oper priviledges and can do whatever you want from issuing Topics, which will be commands for bots, up to kicking and banning anyone who connects.

Ok, so now we have to find the bot binary. It is totally your choice on which bot you will choose, public or private, or super private ones, ranging in prices and features. For starters I would recommend IMBot, with which you can learn the basics, but if you plan to seriously work on your network, I would recommend Nasa Bot coded by fum7n which is available for 75$ and to get it contact me on MSN and I might be able to hook you up.

If you decide to buy the bot binary from anyone you will have to provide him with the server's IP, ports, and desired channel for the bots to come.
If you decide to get a public bot you will have to get one, and edit the Config.h or any similar file depending on the bot with your server information and you will have to compile it.

That's all folks from mine tutorial, I hope you have learned a lot and you are a step closer to being a professional hacker. Also I have included some of other work for you to read which can be found on the next page.

Additional Resources About Botnets

Q: What's a bot?
A: A bot is a malicious program which has several purposes. They are usually told what to do by a botnet admin although many of the features now are automated.

Q: What's a botnet?
A: A botnet is a network of infected computers that all connect to one area where they are commanded by the botnet admin.

Q: What can a bot do?
A: Usual features of a bot include...

- P2P Spreading (Limewire, uTorrent, etc.)
- IM Spreading (Sends to contacts on MSN, AIM, etc.)
- DDoS attacking (See "what's a DDoS attack?")
- Spam mailing to lists of emails (Often used to spread)
- Collecting personal information (Passwords, bank details and the like)

Q: How are bots told what to do?
A: Bots are usually commanded through an IRC channel by the user. Commands are built in and the bots listen for them.

Q: What's an IRC channel?
A: IRC stands for Internet Relay Chat. It's like a group messaging thing although you can also speak to people privately. To use IRC you need a client like ChatZilla, XChat or mIRC. You then connect to an IRC server and choose the channel you wish to join.

Q: How do I get a botnet?
A: First you will need a source code and the programs required to compile it. Most bots are programmed in C++, but you don't need any programming experience to compile your own. There is usually one file named "Configs.h" or something similar that you have to edit, that's where you edit the bot names, the IRC channel and any other necessary information. Look for bot sources in the botnet section here and they'll usually come with some form of instructions.

Q: Which bot should I use?
A: I recommend IMBot v4.1, it's pretty simple to compile and use, I'm sure there are tutorials here for it as well.
You can download IMBot here. (Clean download, it's mine).

Q: Is this illegal?
A: Yes. Mass-spreading a bot illegally and stealing information can get you into real trouble if you're caught. 99% of the botnets that are shut down have over 10,000 bots, though, and I wouldn't expect anyone here to reach over 5,000. You will have to make sure your IRC server is secure and that your bot stays undetected.

Q: Is it true I can make money from this?
A: Yes, potentially. You could make the bots visit referral sites or download files. A lot of people sell the accounts they've taken from their bots for a price cheaper than the original. You don't have to do any of this, but as your botnet grows you will need more money to transfer to a professional IRC host.

Q: How can I secure/hide my botnet?
A: Offshore hosting first of all. Something in a country such as Sweden, for example. Dedicated hosting would be best, because that way you aren't sharing your hosted server with anyone and you can hold a much larger network. A password on your IRC channel is also recommended. Be sure to use a bot that is undetected, whether you have to crypt it or not.

Q: What do most people use botnets for?
A: The majority of them are used for DDoS attacks against websites when there are a lot of them. Many people set up large botnets just to sell their bots, though. With the rate they spread at, you could sell a large amount of bots to someone for a nice profit with only a small amount of work done.

Q: How can I spread my bot?
A: Most bots are spread through torrenting websites or warez boards. A lot of bots also have auto-spread features, so you could have 50 bots and then gain 150 more through the auto-spreading without doing any work at all. A lot of people also buy bots off other botnet admins to start their botnet off with a nice amount.

Q: What type of bot would be best?
A: Java bots seem to be the most popular right now since a lot of them are still fully undetectable, but you have to bear in mind that your victim will need Java. The same with bots coded in VB.NET, your bots will need the .NET framework. Some VB6 bots may also need missing .ocx files, so in my opinion the best choice of bot would be one coded in C++ such as IMBot.

Q: How much should I pay for bot installs?
A: A good price would be 10 cents per bot, which works out at $10 for 100. Some botnet admins may charge you more, but I don't think it's worth paying much more than that. Another risk of buying from other botnet owners is that they still keep the bots to themselves as well, so be sure to find someone trustworthy. Bear in mind that some may not be able to remove their own.

Q: How do I configure my bot to connect to my IRC server?
A: Most bots come with some sort of instructions text file. There are also a lot of tutorials for different bots here at HF, just search the name of your bot. If you can't find anything, there is usually a file named "config.h" (C++) or something similar. Open that and edit the parts that you're supposed to, it should be clear which parts to change.
Example: *//"server","pass",6667,"channel","channelpass","-ix";* needs to be your info in that order.

Q: Is it easy to set everything up?
A: It is usually easy to configure and compile a bot, but setting up your IRC server, keeping it secure, paying for larger off-shore hosts, managing your bots and staying hidden are not easy tasks for beginners. Once you've done it all several times it will be easier though, as with anything. There are usually people here who would be able to help you out if you're having any problems with your bots.

Q: Can I have a botnet without an IRC?
A: Yes. There are other great bots. Some can connect to PHP pages to read commands, some can be commanded over MSN and other clients, and some come with their own clients, e.g. DDoSeR. http://ddoser.info is a nice place to start if you're not sure what you're doing. It's really simple to use and only $35.

This e-book was written by D00MR4ZR and you may not resell this e-book under any circumstances and in any form possible, and you are not allowed to share it or anyhow dispatch it anywhere but your own computer. Of course due to Internet today, I can not enforce you to do it but I can nicely ask for it so please do not share this to anyone but your closest friends. The only thing I can do is terminate your connection if you will not comply.

CREDITS:
Fum7n – the undisputable e-thug who owns bigger part of Internet and introduced me to botnets.
Vaqxine – for making the BotNet Q&A.
Pts – for harrasing me about playing HoN with him cuz he loses all the time and wants free PSR when I was making this guide.
JohnnyRodger – for supplying me with Porn Accounts and satisfying my needs.