Alumno: Christian Valdespin Bautista

Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Materia: Servicios de Seguridad en Sistemas Operativos Multiusuario.

Profesor: M. en C. Marcos Arturo Rosales García.

Actividad: Keylogger.

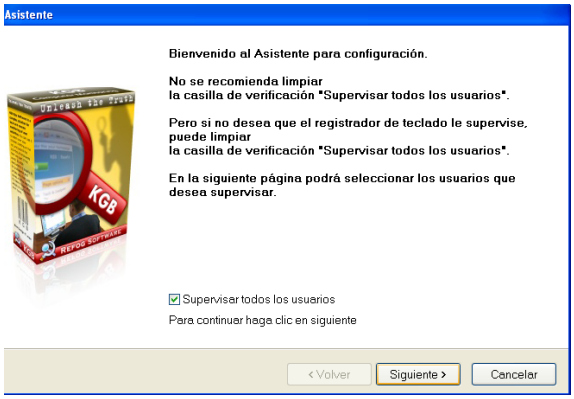
Reporte de Actividades:

1. **Instalar y configurar el Keylogger KGB.**
2. **Encubrir con el rootkit Nuclear**
3. **Vía remota instalarlo**

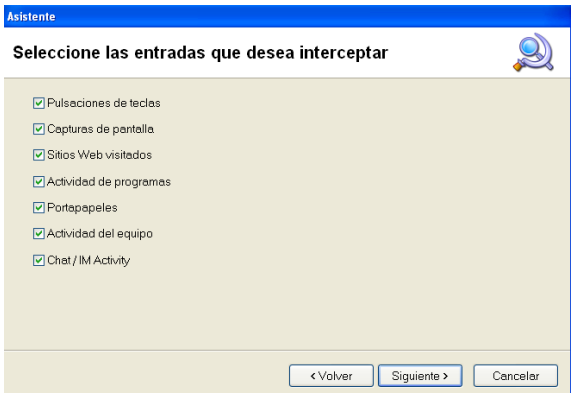
Punto numero 1

Ya una vez instalado nuestro keylogger KGB procedemos con la configuración del mismo

- Una vez iniciado el programa comenzamos con la configuración y seleccionamos la opción de “Supervisar todos los usuarios” y se presiona el botón de continuar.

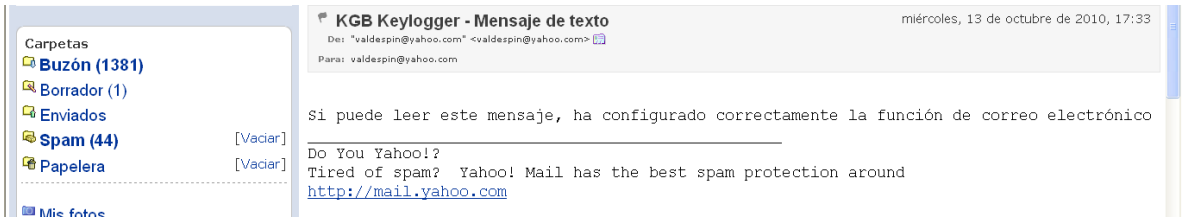


- Seleccionamos todas las opciones y se presiona el botón de continuar.

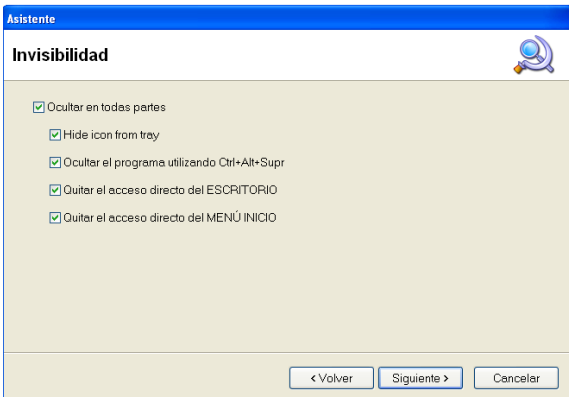


- Colocamos nuestros datos de correo para que sea enviada la información del equipo atacado en un principio se coloca que envía cada minuto o cada cinco pero en ambientes reales es recomendado cada 90 minutos, se presiona el botón de continuar.
    - **Nota**: se intentó configurar con gmail, Hotmail y live sin obtener éxito, y después de buscar en varios foros se encontró que el servidor de correo con el que funciona es yahoo.
    - Se configuro Outlook como se indicaba en algunos foros para usar la opción de "Usar SMTP predeterminado" y tampoco se obtuvo éxito, pese a que con el Outlook si se podían enviar y recibir mensajes.

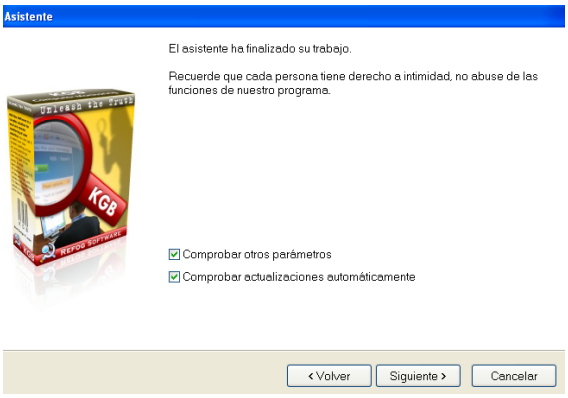
- Verificamos nuestra bandeja de entrada del correo y observamos el siguiente correo.



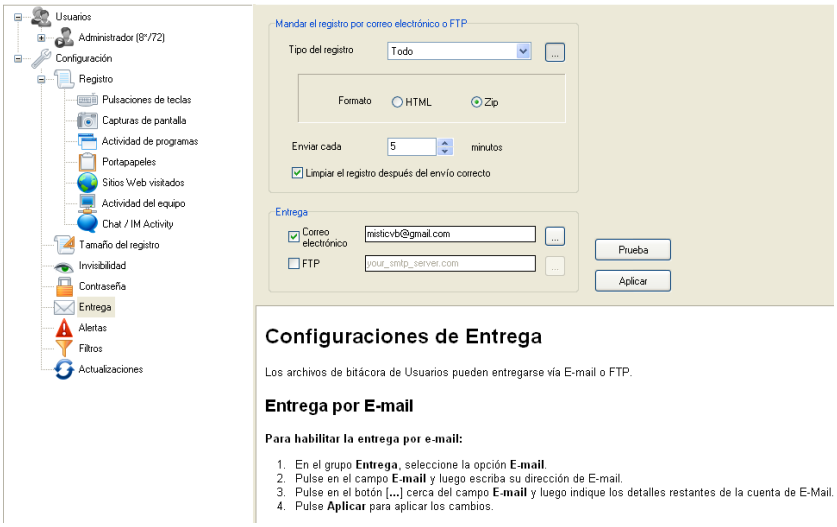
- Seleccionamos todas las opciones y se presiona el botón de continuar.



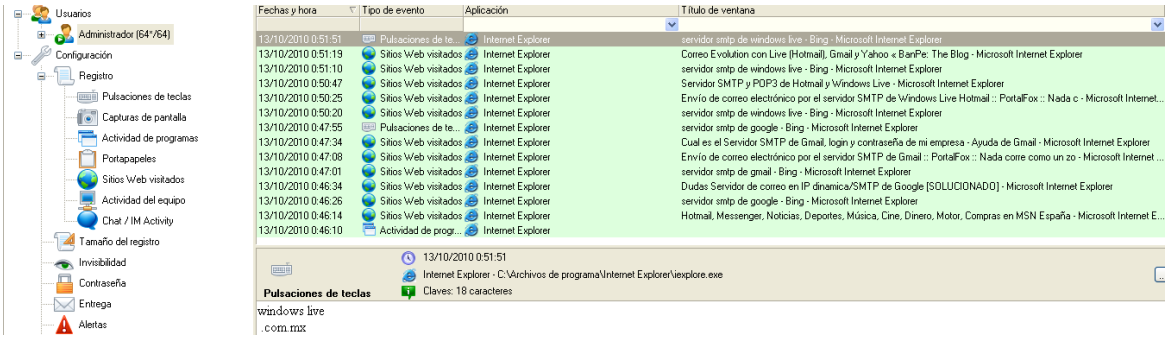
- Seleccionamos todas las opciones y se presiona el botón de continuar.



- Agregamos otras opciones para ser más detallado el reporte



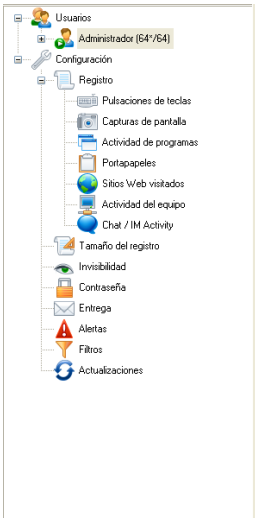
- Comenzamos a ver las capturas de pantallas, urls, teclado, etc
  - **Nota**: podemos observar lo introducido en por medio del teclado como paginas visitadas usuarios, contraseñas, etc.



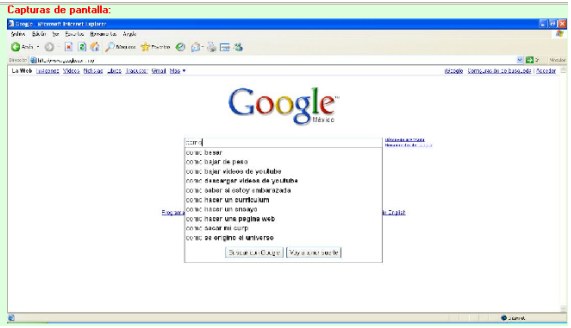
23. **Fecha:** 13/10/2010 0:41:15
Aplicación: Bloc de notas - C:\WINDOWS\system32\notepad.exe
Actividad de programas: **Salir**

24. **Fecha:** 13/10/2010 0:41:14
Aplicación: Administrador de tareas de Windows - C:\WINDOWS\system32\taskmgr.exe
Actividad de programas: **Salir**

25. **Fecha:** 13/10/2010 0:41:09
Aplicación: Administrador de tareas de Windows - C:\WINDOWS\system32\taskmgr.exe
Título de ventana: Administrador de tareas de Windows
Capturas de pantalla:



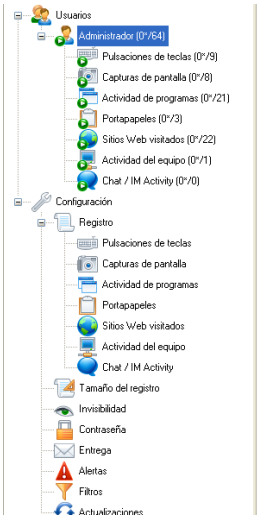
Capturas de pantalla:



30. **Fecha:** 13/10/2010 0:39:32
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: No se puede encontrar el servidor - Microsoft Internet Explorer
Pulsaciones de teclas: **goo**

31. **Fecha:** 13/10/2010 0:39:30
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: Google - Microsoft Internet Explorer
Sitios Web visitados: **http://www.google.com.mx/**

32. **Fecha:** 13/10/2010 0:39:23
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\IEXPLORE.EXE



Informe

Nombre del usuario: **Administrador**
Tipo del registro: **Todo (62)**
Intervalo de fechas: **Últimas entradas (13/10/2010)**

1. **Fecha:** 13/10/2010 0:51:51
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: servidor smtp de windows live - Bing - Microsoft Internet Explorer
Pulsaciones de teclas: **windows live**
.com.mx

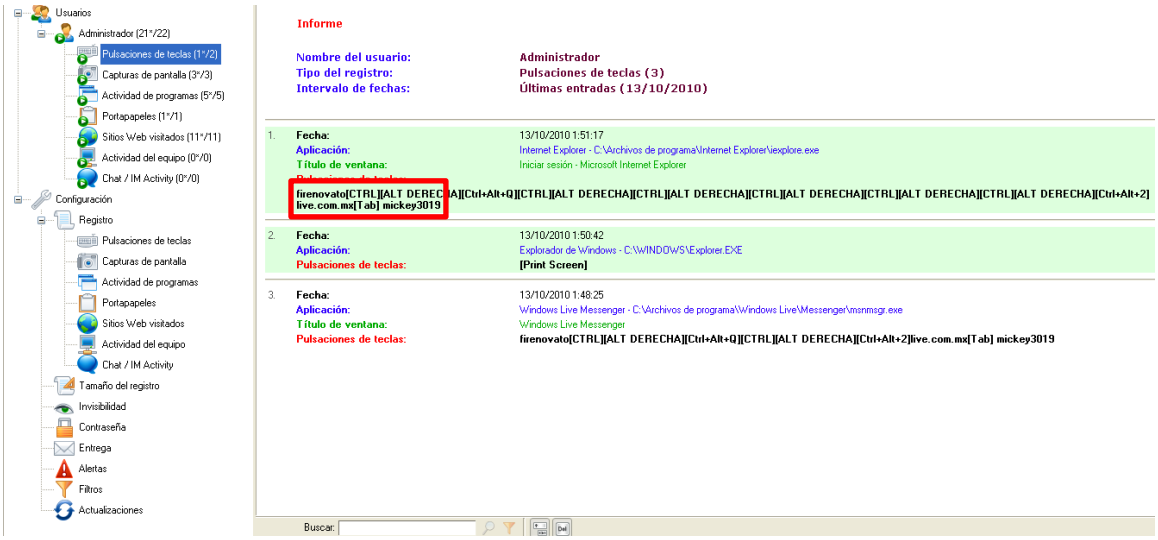
2. **Fecha:** 13/10/2010 0:51:19
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: Correo Evolution con Live (Hotmail), Gmail y Yahoo « BanPe: The Blog - Microsoft Internet Explorer
Sitios Web visitados: **http://banpetheblog.wordpress.com/2009/11/03/correo-evolution-con-live-hotmail-gmail-y-yahoo/**

3. **Fecha:** 13/10/2010 0:51:10
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: servidor smtp de windows live - Bing - Microsoft Internet Explorer
Sitios Web visitados: **http://www.bing.com/search?q=servidor+smtp+de+live.com.mx&form=QBRE&filt=all**

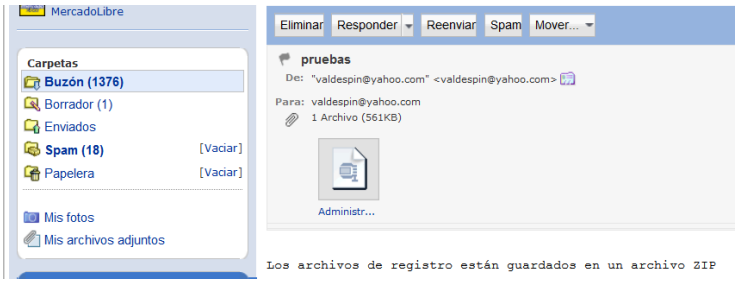
4. **Fecha:** 13/10/2010 0:50:47
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: Servidor SMTP y POP3 de Hotmail y Windows Live - Microsoft Internet Explorer
Sitios Web visitados: **http://www.codigomaestro.com/internet/servidor-smtp-y-pop3-de-hotmail-y-windows-live/**

5. **Fecha:** 13/10/2010 0:50:25
Aplicación: Internet Explorer - C:\Archivos de programa\Internet Explorer\iexplore.exe
Título de ventana: Envío de correo electrónico por el servidor SMTP de Windows Live Hotmail :: PortalFox :: Nada c - Microsoft Internet Explorer
Sitios Web visitados: **http://www.portalfox.com/index.php?name=News&file=article&sid=2677**

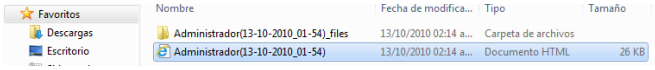
En esta captura podemos observar el usuario y la contraseña.

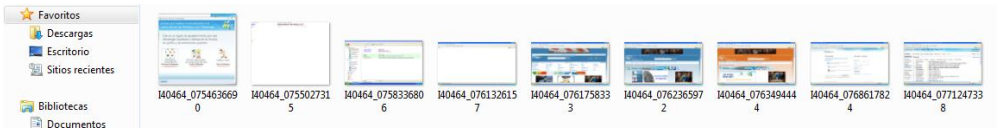


- Observamos el reporte que envía nuestro keylogger.



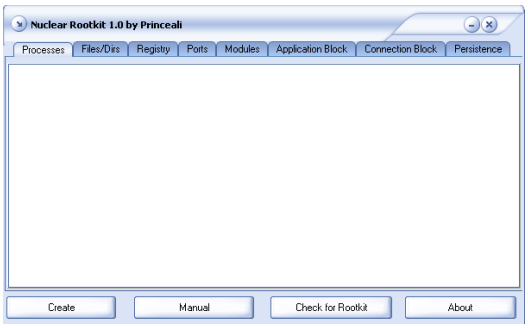
Los archivos de registro están guardados en un archivo ZIP



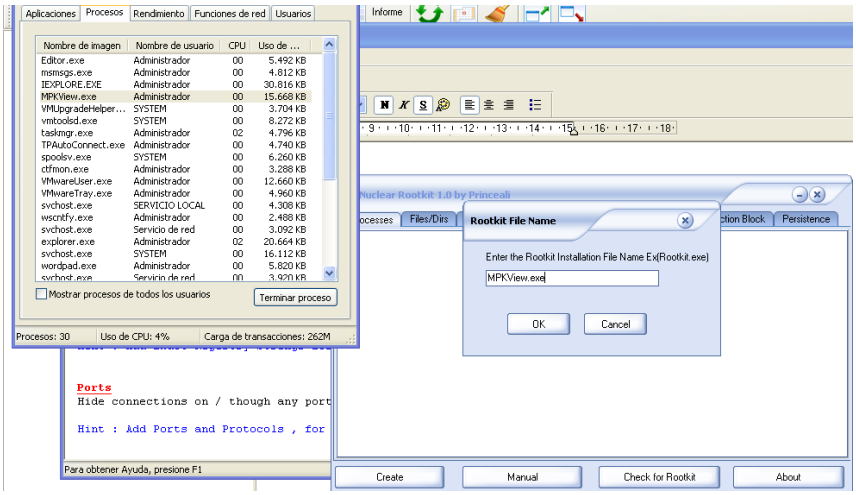


Punto numero 2

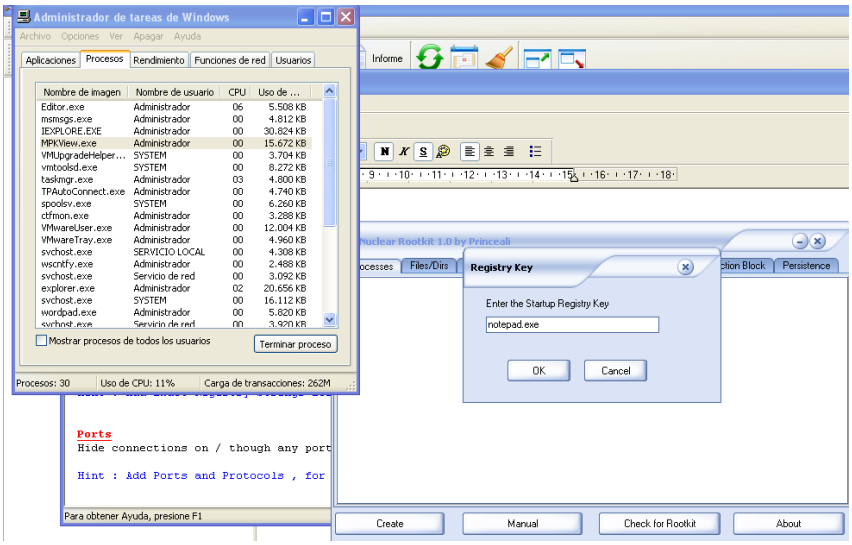
- Una vez descargado el rootkit nuclear procedemos a instalarlo y a ejecutarlo.



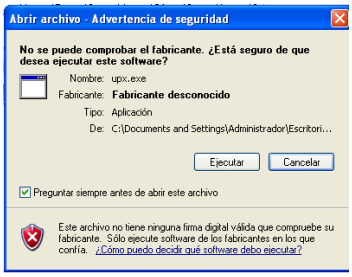
- En la configuración empezamos a buscar los procesos asociados a nuestro keylogger.
- Posteriormente seleccionaremos el botón de “create”.
- Colocamos el nombre de nuestro proceso a ocultar.



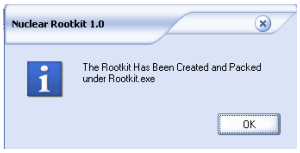
- Tecleamos el proceso con el que lo vamos a asociar o a ocultar



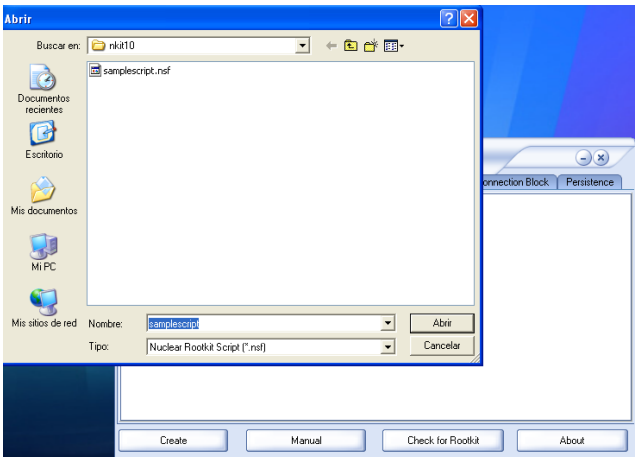
- Windows nos manda una advertencia



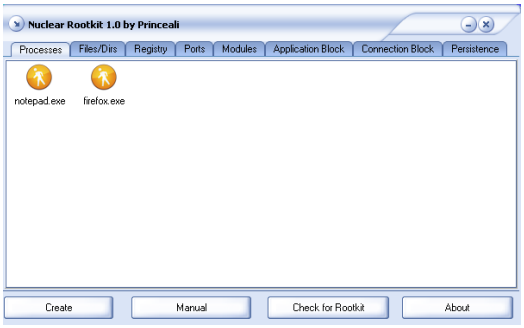
- Finalmente quedo hecho el proceso falso



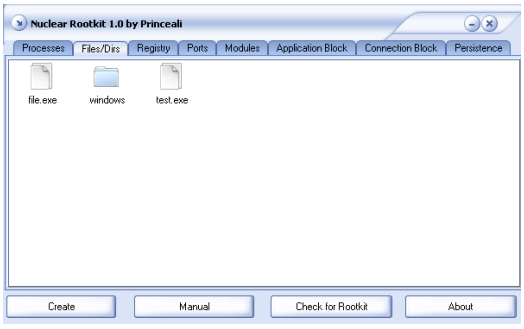
- Con la herramienta abrimos el programa que creo para emular los procesos.

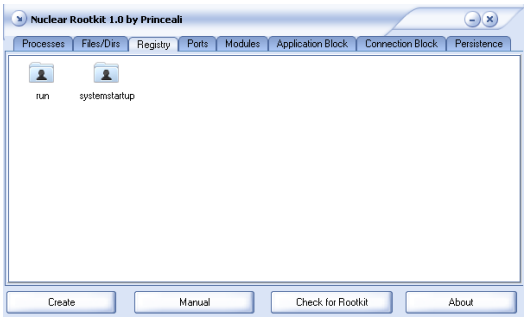


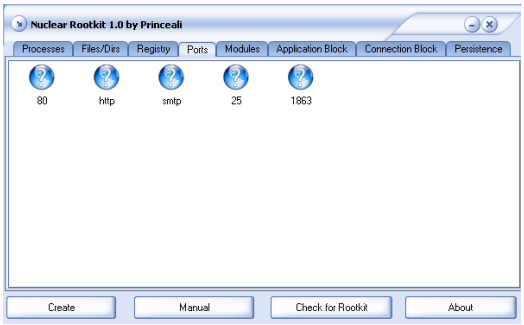
- Observamos los procesos con los que se ocultó nuestro programa.
    - **Nota**: el proceso de Firefox es para ocultar el nuclear.

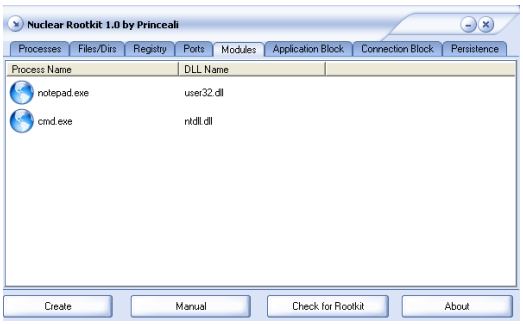


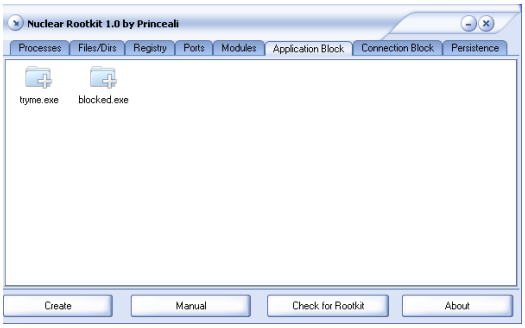
- En estas imágenes podemos observar algunas características de nuestro programa oculto.

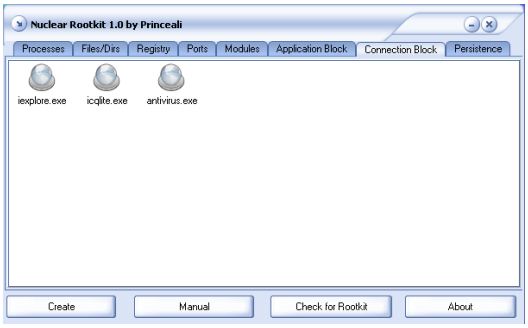


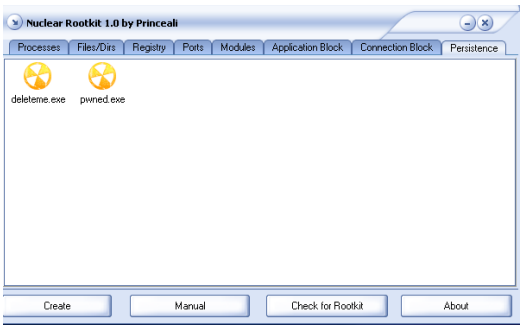

Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
run
systemstartup
Create
Manual
Check for Rootkit
About


Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
80
http
smtp
25
1863
Create
Manual
Check for Rootkit
About


Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
Process Name
DLL Name
notepad.exe
user32.dll
cmd.exe
ntdll.dll
Create
Manual
Check for Rootkit
About


Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
tryme.exe
blocked.exe
Create
Manual
Check for Rootkit
About

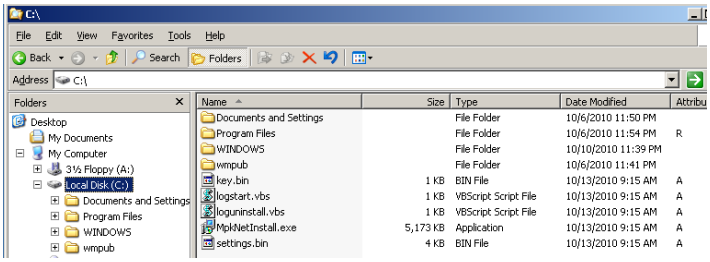

Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
iexplore.exe
icqlite.exe
antivirus.exe
Create
Manual
Check for Rootkit
About


Nuclear Rootkit 1.0 by Princeali
Processes
Files/Dirs
Registry
Ports
Modules
Application Block
Connection Block
Persistence
deleteme.exe
pwned.exe
Create
Manual
Check for Rootkit
About

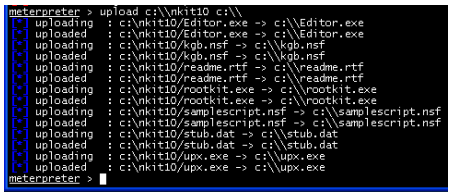
Punto numero 3

- Ocupamos la puerta trasera creada en la práctica anterior para subir los archivos al servidor que es nuestra víctima (192.168.1.105).
    - Nota los archivos que subimos fueron creados con la opción del keylogger en el menú “Archivo” → “Crear Instalador”

- Comprobamos y nuestros archivos ya fueron subidos.

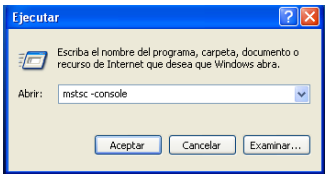


- Ahora subimos el nuclear

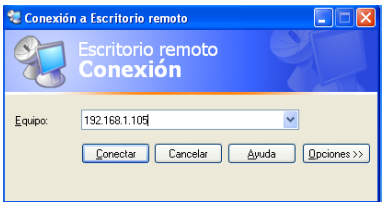


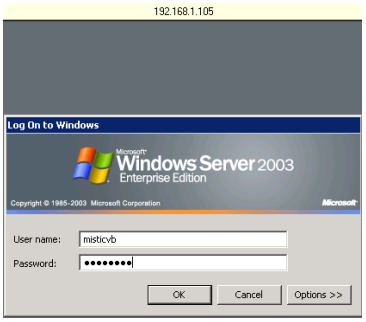
- Creamos unas llaves de registro para que ejecute el nuclear y el KGB al iniar.

- En prácticas anteriores creamos un usuario y habilitamos el escritorio remoto, así que lo utilizaremos para instalar los programas

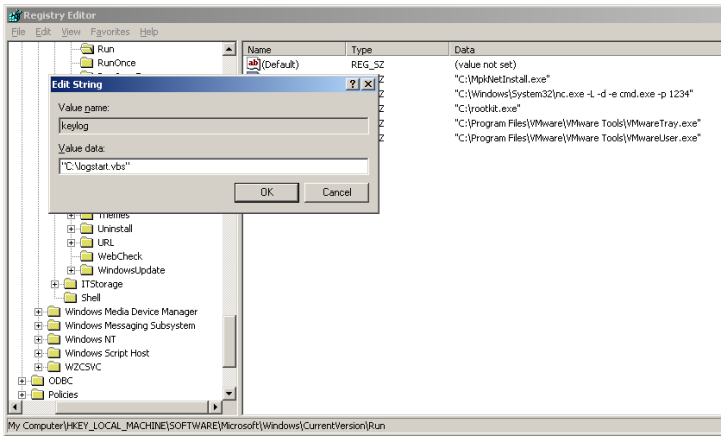


- Tecleamos la ip del servidor victima (192.168.1.105)

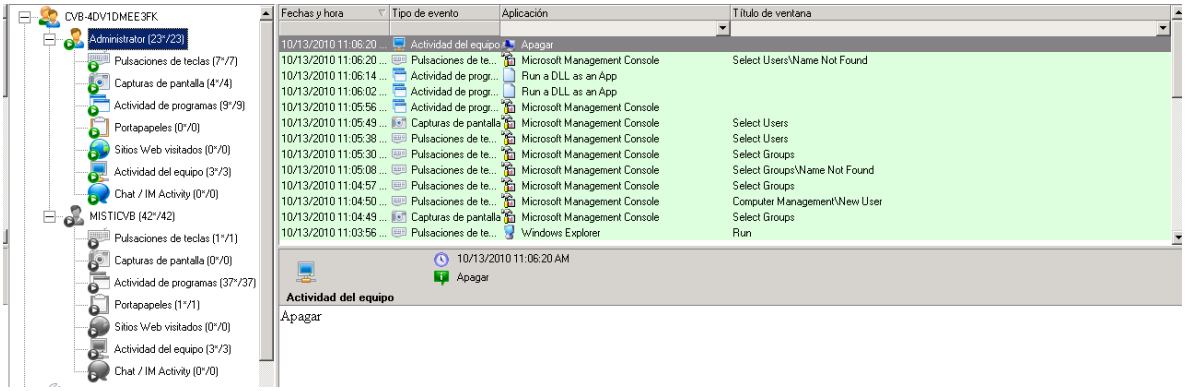


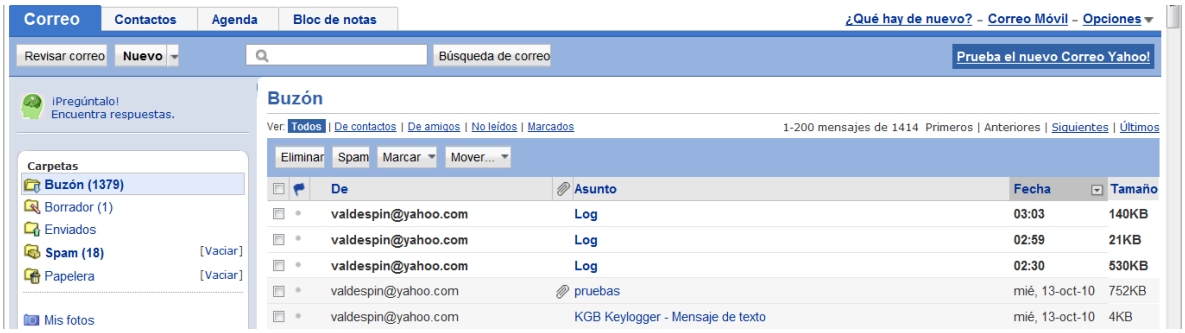


- Vemos el registro



- Instalamos y configuramos como se explicó en el paso 1
- Configuramos que solo queremos monitorear al usuario administrador y no al nuestro.
- Dejamos que el programa haga lo suyo y nosotros nada más checamos nuestro correo.




Correo
Contactos
Agenda
Bloc de notas
¿Qué hay de nuevo? - Correo Móvil - Opciones
Revisar correo
Nuevo
Búsqueda de correo
Prueba el nuevo Correo Yahoo!
¡Pregúntalo!
Encuentra respuestas.
Carpetas
Buzón (1379)
Borrador (1)
Enviados
Spam (18) [Vaciar]
Papelera [Vaciar]
Mis fotos
Buzón
Ver: Todos | De contactos | De amigos | No leídos | Marcados
1-200 mensajes de 1414 Primeros | Anteriores | Siguientes | Últimos
Eliminar
Spam
Marcar
Mover...
De
Asunto
Fecha
Tamaño
valdespin@yahoo.com Log 03:03 140KB
valdespin@yahoo.com Log 02:59 21KB
valdespin@yahoo.com Log 02:30 530KB
valdespin@yahoo.com pruebas mié, 13-oct-10 752KB
valdespin@yahoo.com KGB Keylogger - Mensaje de texto mié, 13-oct-10 4KB