Guía Completa de Uso de LAN Turtle por Hak5

El LAN Turtle está diseñado para insertarse entre un dispositivo (ordenador, laptop) y la red de destino, lo que le permite realizar ataques de **Man-in-the-Middle (MiTM)** y ejecutar herramientas de auditoría de forma discreta.

Parte I: Aspectos Básicos y Conexión

1. Conexión por Primera Vez

La LAN Turtle utiliza un enfoque de "Plug and Pwn" (Conectar y Hackear), pero requiere una configuración inicial.

- **Propósito:** Acceder a la interfaz de administración (Shell) del dispositivo.
- **Proceso:**
    1. Conecte la LAN Turtle al puerto USB de su ordenador.
    2. Conecte un cable Ethernet entre el puerto **Out** de la Turtle y la red de destino (o su propia PC).
    3. El sistema operativo de su PC asignará una dirección IP al puerto USB. La Turtle se configura por defecto para usar la dirección **172.16.84.1**.
    4. Acceda a la interfaz web o el shell SSH a través de la dirección por defecto.

2. Configuración de una Nueva LAN Turtle

Una vez conectado, debe personalizar el acceso y asegurar el dispositivo.

- **Propósito:** Establecer una contraseña segura y actualizar la configuración.
- **Proceso:** Acceda por **SSH** a la dirección predeterminada (ssh root@172.16.84.1). Se le pedirá que establezca una **nueva contraseña** para el usuario root. Esto es crucial para proteger el dispositivo, ya que contiene sus *scripts* de ataque y acceso.

3. Power Considerations, Specifications y Factory Reset

Aspecto	Descripción y Uso
Consideraciones de Energía	El Turtle se alimenta del puerto USB al que está conectado. Es importante usar un puerto USB que suministre energía estable. El consumo es bajo, pero la inestabilidad puede causar fallos en la ejecución de *payloads* o pérdida de conectividad.
Especificaciones	Incluyen un procesador, memoria RAM limitada y capacidad de almacenamiento. Son relevantes para saber qué tan complejos pueden ser los *scripts* o módulos que se pueden ejecutar (ej: Metasploit consume muchos recursos).
Factory Reset (Restablecimiento de Fábrica)	Necesario para limpiar la configuración y la contraseña en caso de olvido o fallo. El proceso suele implicar mantener presionado un botón específico o un puente de pines durante el arranque. **Precaución:** Esto borra toda la configuración y módulos instalados.
Manual Upgrade (Actualización Manual)	Útil si la actualización automática falla. Implica descargar el *firmware* y cargarlo directamente al dispositivo a través de una conexión SSH o *bootloader* de emergencia.

Parte II: El Turtle Shell y el Sistema de Módulos

4. The Turtle Shell and Turtle Modules

El LAN Turtle funciona con una versión mínima de Linux y su funcionalidad principal se basa en **módulos**.

- **Turtle Shell:** Es la interfaz de línea de comandos del dispositivo. Permite al usuario interactuar directamente con el sistema operativo (Linux) e instalar herramientas.
- **Módulos (Modules):** Son *scripts* preconfigurados (principalmente en Bash o Python) que automatizan tareas

específicas de auditoría. Permiten activar y desactivar funcionalidades complejas con un solo comando (ej: MiTM, *sniffing*, *shell* inverso).

5. Instalación de Módulos

Los módulos son la clave para aprovechar el potencial del Turtle.

- **Proceso:** La Turtle viene con su propio gestor de módulos. Los módulos se instalan y gestionan desde la línea de comandos a través del repositorio oficial de Hak5.
    1. Conéctese por SSH.
    2. Utilice el comando del gestor para listar los módulos disponibles.
    3. Instale el módulo deseado (ej: install dnssnarf).
    4. Configure el módulo con los parámetros necesarios (ej: el dominio a suplantar).

6. First Boot And Software Update (Primer Arranque y Actualización)

Este paso garantiza que el dispositivo esté utilizando la última versión y tenga las protecciones y correcciones más recientes.

- **Proceso:** Después de la configuración inicial de la contraseña, el analista debe ejecutar el comando de actualización del *firmware* y de los módulos base.

Parte III: Funcionalidades de Ataque/Auditoría

Estas técnicas se utilizan para la **evaluación de la postura de seguridad** de una red.

7. Man In The Middle With Dns Spoof (Suplantación de DNS)

- **Propósito:** Redirigir el tráfico de una víctima a una dirección IP diferente controlada por el atacante (generalmente un servidor *phishing* o de captura de credenciales).

- **Mecanismo:** La Turtle envenena las respuestas DNS. Cuando la víctima intenta acceder a un sitio legítimo (ej: banco.com), la Turtle intercepta la petición y le devuelve la IP falsa (la IP del atacante).
- **Mapeo de Seguridad:** Esta técnica revela vulnerabilidades en la confianza de la red local y la ausencia de DNS seguro (DNSSEC).

8. Man In The Middle With Url Snarf (Captura de URLs)

- **Propósito:** Interceptar y registrar todas las URLs visitadas por la víctima a través del tráfico HTTP no cifrado.
- **Mecanismo:** La Turtle se sitúa como intermediario y analiza el tráfico de Capa 7 (HTTP) que pasa a través de ella, registrando cada petición de página.
- **Mapeo de Seguridad:** Es una prueba de concepto para demostrar el riesgo de navegar sin HTTPS o en redes no cifradas.

9. Metasploit And Lan Turtle With Meterpreter (Shell Inverso)

- **Propósito:** Establecer un **canal de comunicación persistente y cifrado** desde la red comprometida hacia un servidor externo controlado por el atacante (el *listener*).
- **Mecanismo:** La Turtle se utiliza para enviar un *payload* de **Meterpreter** a una víctima. Este *payload* inicia una conexión de vuelta (shell inverso) al marco de Metasploit (o un *listener* similar). Una vez dentro, Meterpreter permite controlar el sistema, obtener capturas de pantalla, subir/descargar archivos, etc.
- **Mapeo de Seguridad:** Demuestra la capacidad de exfiltrar datos y mantener el control una vez que se ha obtenido acceso inicial.

10. Obtaining Credentials From A Locked Pc (Obtención de Credenciales de un PC Bloqueado)

- **Propósito:** Capturar *hashes* de contraseña (o credenciales) de un ordenador que está encendido pero bloqueado.
- **Mecanismo:** La Turtle puede utilizarse en ataques de ingeniería social o *hardware* directo (USB) para ejecutar *scripts* que extraen *hashes* NTLM o interceptan el tráfico de autenticación, a menudo mediante el *spoofing* de servicios de red.
- **Mapeo de Seguridad:** Evalúa la resistencia de la política de contraseñas y la configuración de seguridad en el inicio de sesión.

11. Persistent Shell Access With Autossh (Acceso Persistente)

- **Propósito:** Asegurar que la conexión *shell* a la Turtle se mantenga activa y se **reestablezca automáticamente** si se pierde.
- **Mecanismo:** Utiliza la utilidad **AutoSSH**, la cual supervisa la conexión SSH y la reinicia si detecta una caída. Esto es vital cuando la Turtle está desplegada en una ubicación física remota sin supervisión.
- **Mapeo de Seguridad:** Demuestra cómo un atacante puede mantener una **cabeza de playa** oculta en la red.

12. Remote File Systems With Sshfs (Sistemas de Archivos Remotos)

- **Propósito:** Montar un sistema de archivos remoto del LAN Turtle en su máquina de atacante, como si fuera una carpeta local.
- **Mecanismo:** Utiliza **SSHFS** (SSH File System). Esto permite una gestión de archivos muy sencilla: puede arrastrar y soltar archivos al Turtle o de la Turtle a su PC, facilitando la subida de *scripts* o la descarga de datos robados sin depender de comandos complejos.
- **Mapeo de Seguridad:** Facilita la exfiltración de datos.

Parte IV: Referencia Adicional

LAN Turtle Basics, Default Settings, The Module System, SSH Clients

- **LAN Turtle Basics:** Define la arquitectura de red básica (ej: el puerto USB es la interfaz de control, el puerto Ethernet es la interfaz de red).
- **Default Settings (Configuración por Defecto):** La dirección IP por defecto es **172.16.84.1** y el nombre de usuario inicial es root. Estas deben cambiarse inmediatamente.
- **The Module System:** Ya explicado, es la interfaz de *scripts* que permite activar funcionalidades complejas sin necesidad de programar.
- **SSH Clients:** Se refiere a las herramientas necesarias para interactuar con la Turtle (ej: PuTTY, Termius o el cliente SSH nativo de Linux/macOS).

Configuración LAN de Hak5 Turtle

LAN Turtle es un adaptador Ethernet USB con algunos trucos de blindaje. Utilizar este dispositivo abre muchas posibilidades para especialistas, equipos de seguridad interna/administradores de sistemas y consultores. Te permite demostrar un dispositivo fácilmente oculto que dará acceso externo a un atacante. Con su sistema operativo Linux embebido y su propia interfaz Turtle Shell, ofrece una gama completa de opciones para evaluar redes sociales y capacidades de red. Esta guía cubrirá la configuración inicial usando Windows 10.

Equipamiento

- Local Area Network Turtle
- Windows 10 PC
- Internet Connection

Configuración inicial

Para iniciar una red local, necesitas configurar Tortoise. Los datos de inicio de sesión por defecto son los siguientes:

- IP address – 172.16.84.1
- SSH port – 22
- Username – root
- Password – sh3llz

La configuración inicial de LAN Turtle debería hacerse en un PC remoto. Dado cómo funciona Turtle, es importante recordar la orientación predeterminada de configuración de hardware. De serie, está configurado para que el lado USB (que es una tarjeta de red separada del lado Ethernet) sea el servidor DHCP y también la fuente de alimentación. La tarjeta de red Ethernet actúa como puerto WAN y recibe una dirección IP. La máquina Linux que los gestiona los ve como eth0 y eth1, y por defecto las conexiones están puenteadas.

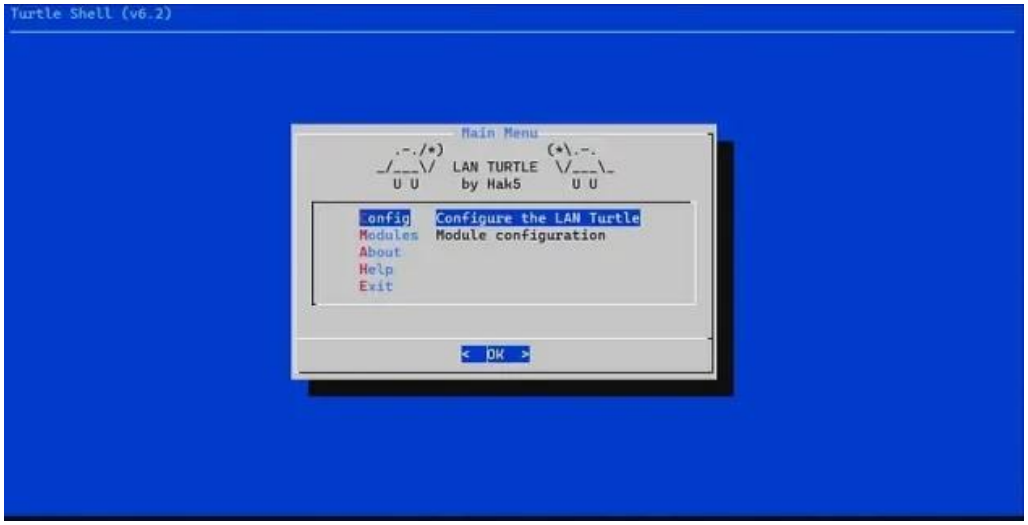
Una vez que el Turtle esté conectado al puerto USB, comenzará el proceso de arranque. El LED verde será fijo y el LED naranja empezará a parpadear durante unos 30 segundos (durante la primera configuración, el LED naranja seguirá parpadeando hasta que se complete la configuración inicial por SSH). Conectar el cable Ethernet a la red del laboratorio proporciona una dirección IP en el rango 172.16.84, permitiendo la comunicación vía SSH. Usar un terminal Windows para conectarse al Turtle vía SSH funciona bien.

```
1. ssh root@172.16.84.1
```

La contraseña predeterminada es sh3llz. Esto abrirá el caparazón de tortuga por defecto.

La primera vez que inicies sesión, se te pedirá que cambies tu contraseña.

Después de crear una nueva contraseña, te recibirás con Turtle Sh3ll.

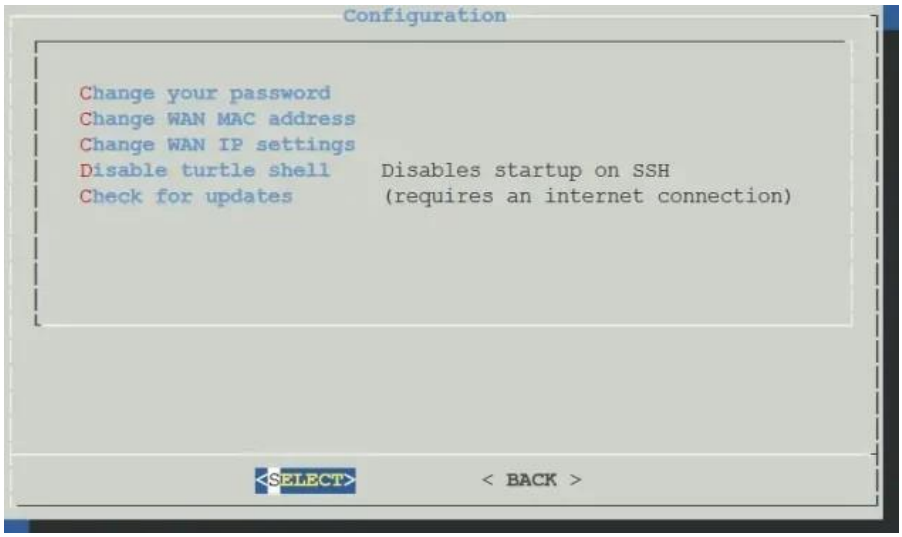


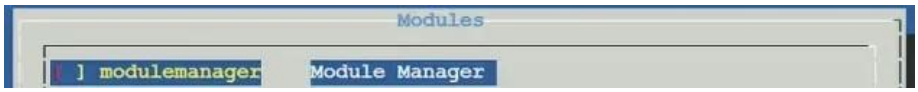
A partir de aquí, la configuración comienza con la opción "Configuración", seguida de la opción "Comprobar actualizaciones" en la página siguiente. Si la conexión de red es buena, Turtle buscará la última versión de Hak5, la descargará e instalará. Esto restablecerá todos los datos y restaurará el dispositivo a los ajustes de fábrica. Los LEDs parpadearán durante aproximadamente 10 minutos durante esta operación.

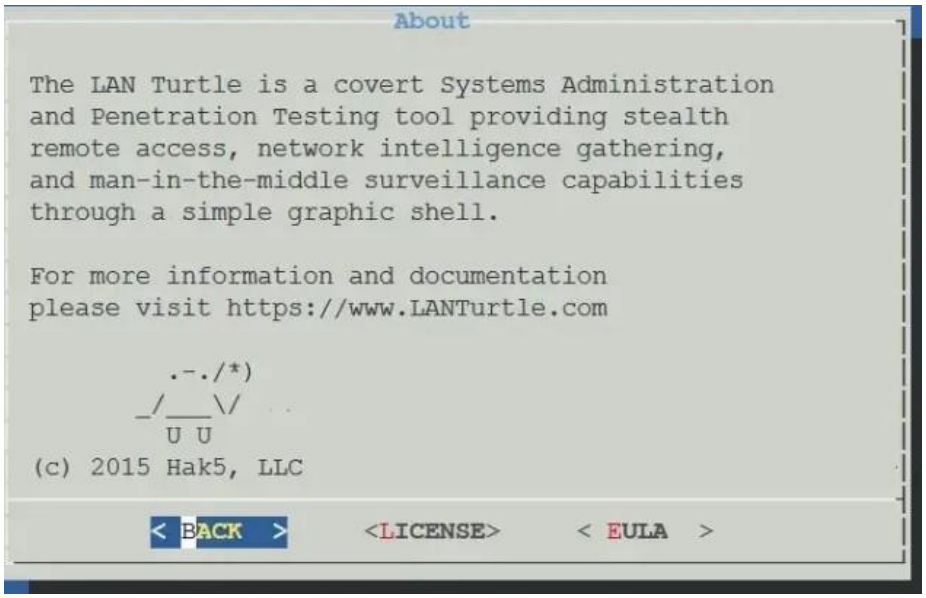
Es extremadamente importante que se aplique energía durante todo el proceso de instalación del nuevo firmware, de lo contrario podrías dañar el dispositivo. Una vez completada la

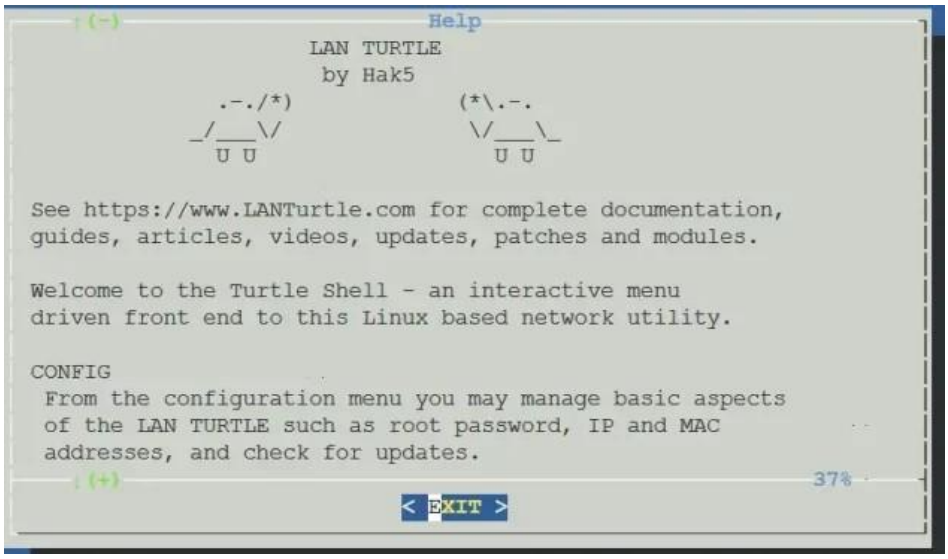
actualización, puedes volver a iniciar sesión usando los mismos datos de inicio de sesión predeterminados que antes. Crea una nueva contraseña de nuevo, ya que la actualización eliminará la que creaste anteriormente y ahora estás en una versión actualizada de Turtle Shell.

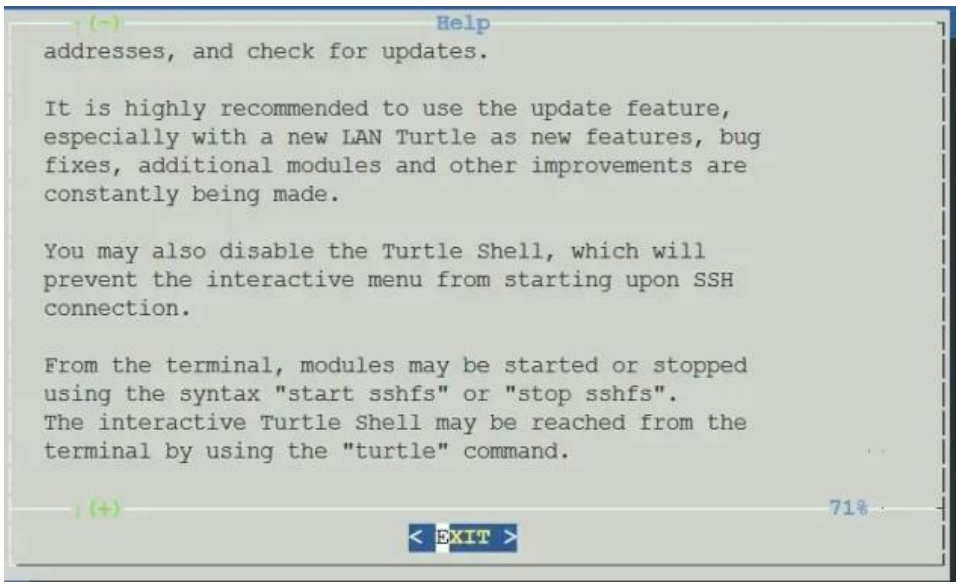
Capturas de pantalla del menú en Turtle Sh3ll

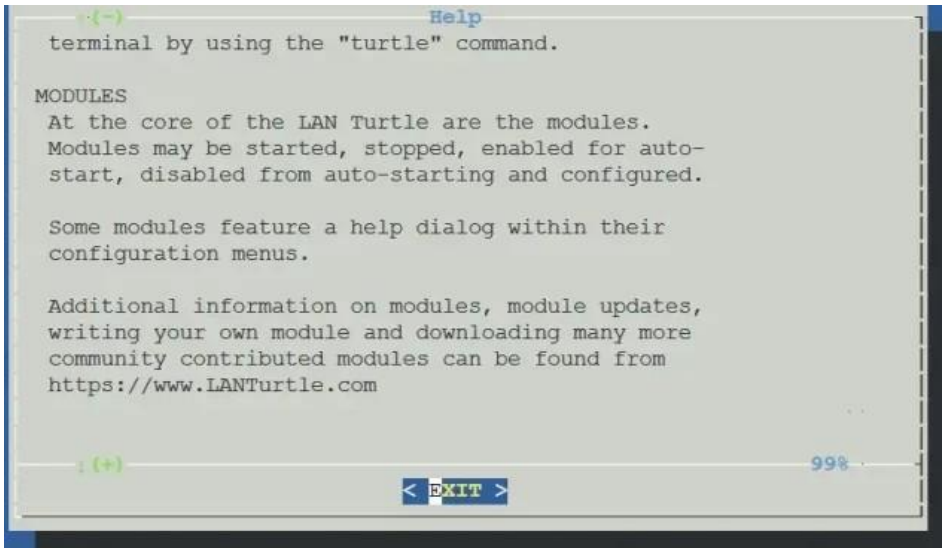


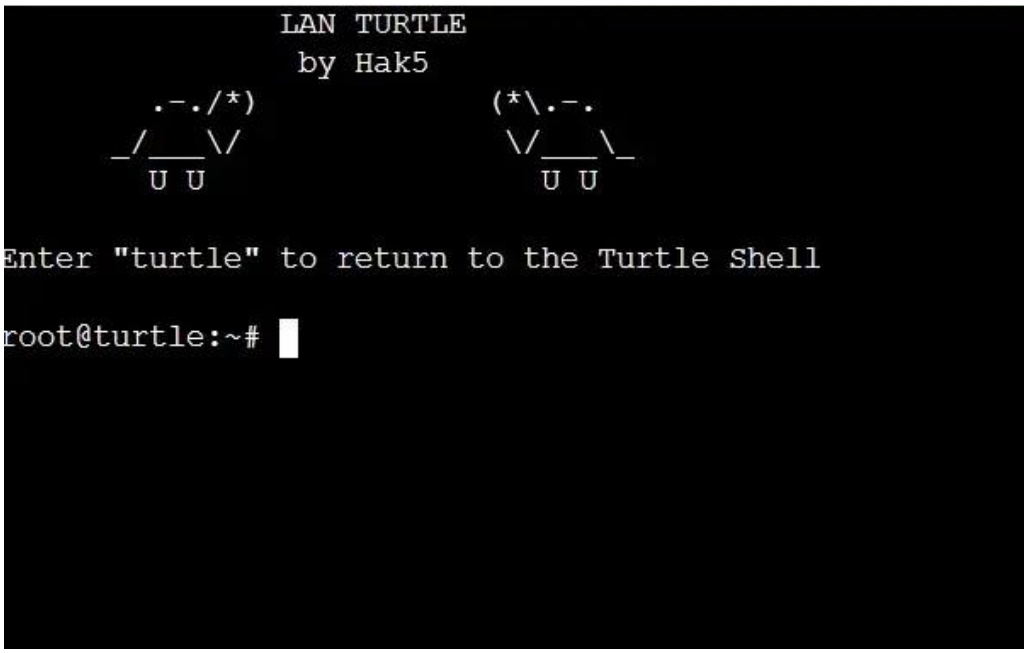





Help
LAN TURTLE
by Hak5
See https://www.LANTurtle.com for complete documentation,
guides, articles, videos, updates, patches and modules.
Welcome to the Turtle Shell - an interactive menu
driven front end to this Linux based network utility.
CONFIG
From the configuration menu you may manage basic aspects
of the LAN TURTLE such as root password, IP and MAC
addresses, and check for updates.
37%
< EXIT >


Help
addresses, and check for updates.
It is highly recommended to use the update feature,
especially with a new LAN Turtle as new features, bug
fixes, additional modules and other improvements are
constantly being made.
You may also disable the Turtle Shell, which will
prevent the interactive menu from starting upon SSH
connection.
From the terminal, modules may be started or stopped
using the syntax "start sshfs" or "stop sshfs".
The interactive Turtle Shell may be reached from the
terminal by using the "turtle" command.
71%
< EXIT >


Help
terminal by using the "turtle" command.
MODULES
At the core of the LAN Turtle are the modules.
Modules may be started, stopped, enabled for auto-
start, disabled from auto-starting and configured.
Some modules feature a help dialog within their
configuration menus.
Additional information on modules, module updates,
writing your own module and downloading many more
community contributed modules can be found from
https://www.LANTurtle.com
99%
< EXIT >



Una vez completada la configuración inicial, Turtle puede personalizarse para tu interacción con módulos comunitarios e incluso módulos personalizados según tus necesidades. Escribiré más instrucciones paso a paso sobre cómo instalar y usar los módulos en el futuro. También puedes consultar https://docs.hak5.or g/lan-turtle/ para instrucciones detalladas de Darren Kitchen, fundador de Hak5.

Mayor automatización y sigilo

Después de implementar con éxito la tortuga LAN en una red de prueba, es importante no solo tener acceso remoto, sino también garantizar su estabilidad, sigilo y autonomía. Para garantizar una conexión confiable después de cada reinicio del sistema, asegúrese de que el autosh, htpdate, sshfs se inicie automáticamente.

Utilice /etc/rc.local para agregar con confianza los servicios para comenzar:

/usr/bin/htpdate -s 1.1.1.1

/etc/init.d/sshfs start

/etc/init.d/autossh start

Alternativa: añadir los servicios adecuados a init.d y activarlos a través de update-rc.d.

Ofuscación y enmascaramiento

Para evitar la detección del dispositivo por parte del administrador del sistema.

Cambie la dirección MAC de la interfaz Ethernet a una inofensiva:

```
ifconfig eth0 down

ifconfig eth0 hw ether 00:13:37:AA:BB:CC

ifconfig eth0 up
```

Cambios de nombre de host y banner:

```
uci set system.@system[0].hostname='usbeth0'

uci commit system

/etc/init.d/system reload
```

Borrar los banners MOTD y SSH:

```
echo "" > /etc/motd

echo "" > /etc/banner
```

Almacenamiento de registro

Para un control adicional sobre la actividad en el dispositivo, puede almacenar los registros en la RAM o en un servidor de puesta en escena (a través de sshfs):

```
logread > /sshfs/logs/boot_$(date +%F_%T).log
```

Y añadir esta línea a /etc/rc.local para un monitoreo constante.

Rotación de claves y cifrado

Para sesiones largas:

- Configure la rotación regular de la clave SSH a través de keymanager o crontab, descargando nuevos pares desde un repositorio centralizado.
- Cifre los scripts críticos a través de gpg y descifra en el inicio (solo si el almacenamiento local es confiable).

Detección de dispositivos: protección

En caso de detección de tortugas, es importante tener un "interruptor de hombre muerto" – eliminación o desactivación automática:

Configure la rotación regular de la clave SSH a través de keymanager o crontab, descargando nuevos pares desde un repositorio centralizado.

Cifre los scripts críticos a través de gpg y descifra en el inicio (solo si el almacenamiento local es confiable).

Detección de dispositivos: protección

En caso de detección de tortugas, es importante tener un "interruptor de hombre muerto" – eliminación o desactivación automática:

```
if ! ping -c1 yourC2server.com > /dev/null; then
  rm -rf /root/.ssh
  poweroff
fi
```

O bien, en la versión systemd:

```
[Service]

ExecStart=/bin/bash /root/self_destroy.sh

Restart=always
```

Conclusión

La tortuga LAN es más que un simple adaptador USB. Es una herramienta completa para el acceso profundo a la red, capaz de operar de forma autónoma, sigilosa y segura. En esta guía, hemos pasado por todo el proceso, desde la configuración inicial y la actualización del dispositivo, hasta la configuración del túnel inverso, el almacenamiento de datos en un servidor remoto, el inicio automático de los servicios después del reinicio, así como la garantía de sigilo a través del enmascaramiento, el cambio de direcciones MAC y el registro.

También hemos agregado elementos de seguridad importantes, como la limpieza automática de claves en caso de pérdida de conexión al servidor de administración y el cifrado de las configuraciones. Todo esto hace que Turtle no solo sea un punto de entrada accesible, sino un poderoso implante que puede permanecer activo y desapercibido incluso en un entorno corporativo complejo.