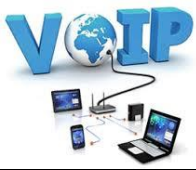
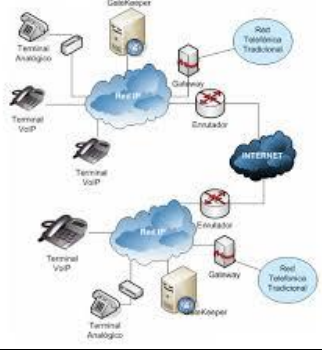
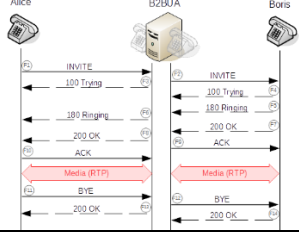


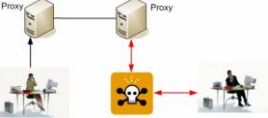
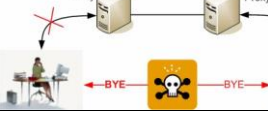
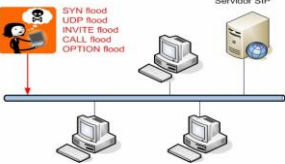


<p>¿Qué es VoIP?</p> 	<p>La tecnología VoIP trata de transportar la voz, previamente procesada, encapsulándola en paquetes para poder ser transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional.</p>
<p>Infraestructura básica VoIP</p> 	<p>Terminales: Son los dispositivos que utilizarán para comunicarse. Implementados tanto en hardware como en software</p> <p>Gateways: se encargan de conectar las redes VoIP con las redes de telefonía tradicional.</p> <p>Gatekeepers: Se encargan de realizar tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicios de facturación y temporización, etc.</p>
<p>Protocolos y estándares VoIP</p>	<p>Define los protocolos para la comunicación multimedia a través de redes de paquetes. Nacido originariamente para dar soporte audiovisual en las redes de área local a evolucionado rápidamente para dar soporte y convertirse en un estándar de VoIP</p>
<p>Introducción a SIP</p> 	<p>es un protocolo simple de señalización y control utilizado para telefonía y videoconferencia sobre las redes IP</p>
<p>Seguridad de las redes VoIP</p> 	<p>Políticas y Procedimientos</p> <p>Seguridad Física</p> <p>Seguridad de Red</p> <p>Seguridad en los Servicios</p> <p>Seguridad en el S.O.</p> <p>Seguridad en las Aplicaciones y protocolos de VoIP</p>
<p>Clasificación de los ataques</p>	<p>Accesos desautorizados y fraudes.</p> <p>Ataques de denegación de servicio</p> <p>Ataques a los dispositivos</p> <p>Vulnerabilidades de la red subyacente.</p> <p>Enumeración y descubrimiento.</p> <p>Ataques a nivel de aplicación.</p>
<p>Accesos desautorizados y Fraudes</p>	<p>Son los fraudes consecuencia de un acceso desautorizado a una red legal VoIP (por ejemplo haber obtenido anteriormente obtener datos de cuentas).</p>

	
Explotando la red subyacente	<p>O es El eavesdropping el cual se trata de tomar información de distintos ordenadores en busca de información delicada y confidencial según cual sea el usuario del equipo, ya que esto es sustraer información de forma ilegal y sin autorización, dicha información es más que todo el audio de los distintos ordenadores.</p>
Ataques de denegación de servicio	<p>son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema</p>
Ataques a los dispositivos 	<p>Los ataques realizador hoy en día por hackers y crackers hacia las redes de datos tienen como objetivo principal el hardware y el software de los dispositivos. Por lo tanto, en redes VoIP, los gateways, call managers, Proxy servers sin olvidar los teléfonos IP serán potencialmente objetivos a explotar por parte de un intruso.</p>
Descubriendo objetivos	<p>Una vez que el hacker ha seleccionado una red como su próximo objetivo, sus primeros pasos consistirán en obtener la mayor información posible de su victima</p>
Footprinting 	<p>l proceso de acumulación de información de un entorno de red específico</p>
Escaneando	<p>A partir de la dirección de red de la víctima, se pretende obtener un listado de direcciones IP y servicios activos en la red</p>
Enumeración	<p>La enumeración es una técnica que tiene por objetivo obtener información sensible que el intruso podría utilizar para basar sus ataques posteriores.</p>
Explotando el Nivel de Aplicación	<p>El nivel de aplicación de la red IP es quizás uno de los más vulnerables, debido en parte a que VoIP engloba gran cantidad de protocolos y estándares añadiendo cada uno ellos su propio riesgo de seguridad</p>
Autenticación en VoIP	<p>Esta autenticación mutua está basada en algún tipo de secreto compartido que es conocido a priori por los dos.</p>
Autenticación del protocolo SIP	<p>El protocolo SIP utiliza la autenticación digest para comprobar la identidad de sus clientes.</p>
Crackeo de contraseñas SIP	<p>Los métodos y las herramientas para romper esa autenticación y crackear los hashes digest con el fin de obtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa.</p>

Suplantación de identidad en el registro 	El registro de usuarios es la primera comunicación que se establece en el entorno VoIP
Desregistrar Usuarios	es una necesidad para conseguir suplantar su identidad
Desconexión de Usuarios 	Los protocolos se utilizan sin encriptación alguna y de que los mensajes no se autentican de forma adecuada, es trivial para un intruso desconectar a los usuarios de sus llamadas enviando mensajes BYE con la identidad falsificada simulando ser el usuario del otro lado de la línea.
Redirección de llamadas.	Utilizan una herramienta como RedirectPoison que escucha la señalización SIP hasta encontrar una petición INVITE y responder rápidamente con un mensaje SIP de redirección, causando que el sistema envíe un nuevo INVITE a la localización especificado por el atacante
Eavesdropping	técnica de la interceptación de la comunicación
Inserción de Audio	es un protocolo que no da garantías en la entrega de sus mensajes y no mantiene ningún tipo de información de estado o conexión
Fuzzing	El objetivo es comprobar como manejan los dispositivos, las aplicaciones o el propio sistema operativo que implementa el protocolo
Ataques DoS 	ataques de denegación de servicio
SPIT: Spam over Internet Telephony	Tendencia de realizar llamadas y llenar los voicemail de los usuarios con mensajes pregrabados crecerá durante los próximos años a medida que se generalice el uso de telefonía por IP.
Vishing: Voip Phishing	Al igual que ocurría con el SPAM las amenazas de phishing suponen un gran problema para el correo electrónico. Las denuncias por robo de información confidencial de forma fraudulenta están a la orden del día y exactamente las mismas técnicas son aplicables a la plataforma VoIP. Esto es otra forma de robo de información por medio de correos.
Asegurando la red VoIP	Estos son algunos pasos para tener asegurado la red VoIP: Mantener los sistemas actualizados y parcheados. Cortafuegos bien administrados. Sistemas de antivirus. Modificar los protocolos y configurar dispositivos para que utilicen autenticación. Limitado los grupos. Corregir los protocolos que contestan diferente modo si el usuario existe o no. Configurar correctamente los servicios para que no muestren más información de la necesaria. No usar nombres por defecto par archivos de configuración No usar TFTP, FTP aunque tampoco sea seguro. LA mejor solución es usar un canal cifrado. Desactivar puertos de administración http y snmp. Cambiar el password por defecto de todos los lugares.

Roberto Gutiérrez Gil, 2012. Seguridad en VoIP recuperado de <http://www.it-docs.net/ddata/896.pdf> el día 11/04/17.

Panamcom, 2015. Voip yeastar yealink Recuperado de <https://www.panamcom.com/blogs/news/46087937-porque-preferir-telefonía-voip-yeastar-yealink-ii> el día 11/04/17.

Wikipedia, 2017. B2BUA recuperado de https://es.wikipedia.org/wiki/Session_Initiation_Protocol el día 11/04/17.

Slideshare, 2015. Recuperado de <https://es.slideshare.net/martinghost9999/glosario-de-virus-y-fraudes-desconocido> el día 11/04/17.

Milenio, 2017. Shutterstock recuperado de http://www.milenio.com/negocios/dispositivos_moviles-ciberataques-aplicaciones-hackers-empresas_0_531547007.html el día 11/04/17.