

Sistema de Red de Honeynets VenCERT



DERECHOS DE USO

La presente documentación es propiedad de la Superintendencia de Servicios de Certificación Electrónica SUSCERTE, tiene carácter privado y confidencial y está dirigido exclusivamente a su(s) destinatario(s), no podrá ser objeto de reproducción total o parcial, ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, digital, registro o cualquier otro, no podrá ser distribuido sin el permiso previo y escrito de SUSCERTE, bajo ningún concepto. Si usted ha recibido este mensaje por error, debe evitar realizar cualquier acción descrita anteriormente, asimismo le agradecemos comunicarlo al remitente y borrar el mensaje y cualquier documento adjunto. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será sancionada conforme a la ley.

Detección rápida de ataques con simulación de servidores débiles (Honeypots)

Para conseguir una mejor defensa de las plataformas tecnológicas de los sistemas de información del Estado y en las infraestructuras críticas de la Nación es imprescindible conocer en detalle los métodos de ataque más utilizados en la actualidad que, por otra parte, son muy variables. No basta con tener unas barreras de seguridad fortificadas, es necesario estudiar y aprender continuamente los nuevos intentos de ataque y, de este modo, conocer las técnicas empleadas en los mismos. Este es precisamente el principal objetivo del Sistema de Red de Honeypots (SRH) puesto en marcha por Suscerte, a través del VenCERT, que coadyuvará a identificar y aprender de forma temprana los ataques más novedosos y silenciosos a los sistemas de la Administración Pública de la República Bolivariana de Venezuela, mediante la simulación de servidores débiles que sean blancos fáciles para los atacantes.

El Ministerio del Poder Popular para Ciencia y Tecnología, a través de la Superintendencia de Servicios de Certificación Electrónica (Suscerte), ha iniciado el desarrollo de un Sistema de Red de Honeypots (SRH) que permite la detección y aprendizaje de nuevas técnicas de ataques, así como la identificación temprana del origen de los mismos. Este Sistema permitirá, no sólo detectar incidentes en su primera fase y generar las contra medidas más adecuadas para detener su impacto, sino que, además, posibilitará el aprendizaje de las técnicas más novedosas de ataque, así como la recopilación de muestras de malware y herramientas usadas para los ataques, que en gran medida son indetectables para los antivirus y sistemas similares basados en detección de patrones.

Conviene recordar que los códigos maliciosos (virus, troyanos, etc..) instalados en los equipos o en los navegadores de un organismo; los gusanos que intentan extenderse por la red; los ataques contra los servicios web de un ente público...son, en general, los ataques que más han crecido en los últimos años y a los que están expuestos los sistemas de cualquier organización. Este incremento se ve agravado por la interconexión de los sistemas y el uso masivo de Internet.

¿Cómo funciona el Sistema de Red de Sensores?

Para la puesta en marcha del SRH por parte del VenCERT es necesaria la instalación de un Honeypot en un punto externo con conexión a Internet, pero perteneciente a la red del organismo adscrito al servicio.

El Honeypot simula múltiples servicios públicos vulnerables (servicios web, ftp, correo electrónico, bases de datos, etc.), actuando como una “trampa” para posibles atacantes. Este a su vez, llegado el caso, puede incluso simular una pequeña arquitectura de red ficticia, haciendo creer a un posible atacante que ha conseguido introducirse en los sistemas del organismo. Por supuesto, ninguna de las acciones que

realice tendrán impacto real en la verdadera red y en sus servidores, todo quedará aislado en el Honeypot.

Posteriormente, toda la información recogida por el Honeypot (muestras de binarios inyectados al servidor o descargados, IP's de origen, fecha/hora, servicio y/o protocolo atacado, técnica de ataque usada, etc.) es recolectada y transmitida a un sistema central donde es consolidado en una base de datos, poniendo a disposición del ente público toda la información conseguida mediante sendos informes detallados, generados de forma automática o personalizada en cualquier momento.

Contar con Honeypots en la red de un organismo supone dos grandes ventajas:

- Aprender de nuevas técnicas de ataque y la recolección de muestras de malware avanzadas no detectables por antivirus.
- Ralentizar el tiempo al posible atacante, entreteniéndole en atacar al Honeypot (en principio, el punto más débil de la red, y por tanto el más fácilmente atacable) en lugar de a los servidores reales. De este modo, se gana tiempo y se puede bloquear el origen del ataque en las defensas perimetrales antes de que pueda llegar a tener éxito contra los servidores reales.

Todos los ataques y muestras de código dañino recibidas en el sistema central son examinados por el equipo altamente calificado del VenCERT. En caso de detectarse amenazas serias, este equipo notificará al ente afectado los ataques detectados y prestará ayuda y soporte para la mitigación del mismo.

Todos los organismos participantes en el proyecto tienen a su disposición un portal web privado donde pueden consultar la información recopilada, a través de dos clases de informes: informes técnicos detallados e informes gerenciales de tipo estadístico, que podrán generarse automáticamente (diarios, semanales, mensuales, anuales) o bajo demanda del período que se desee.

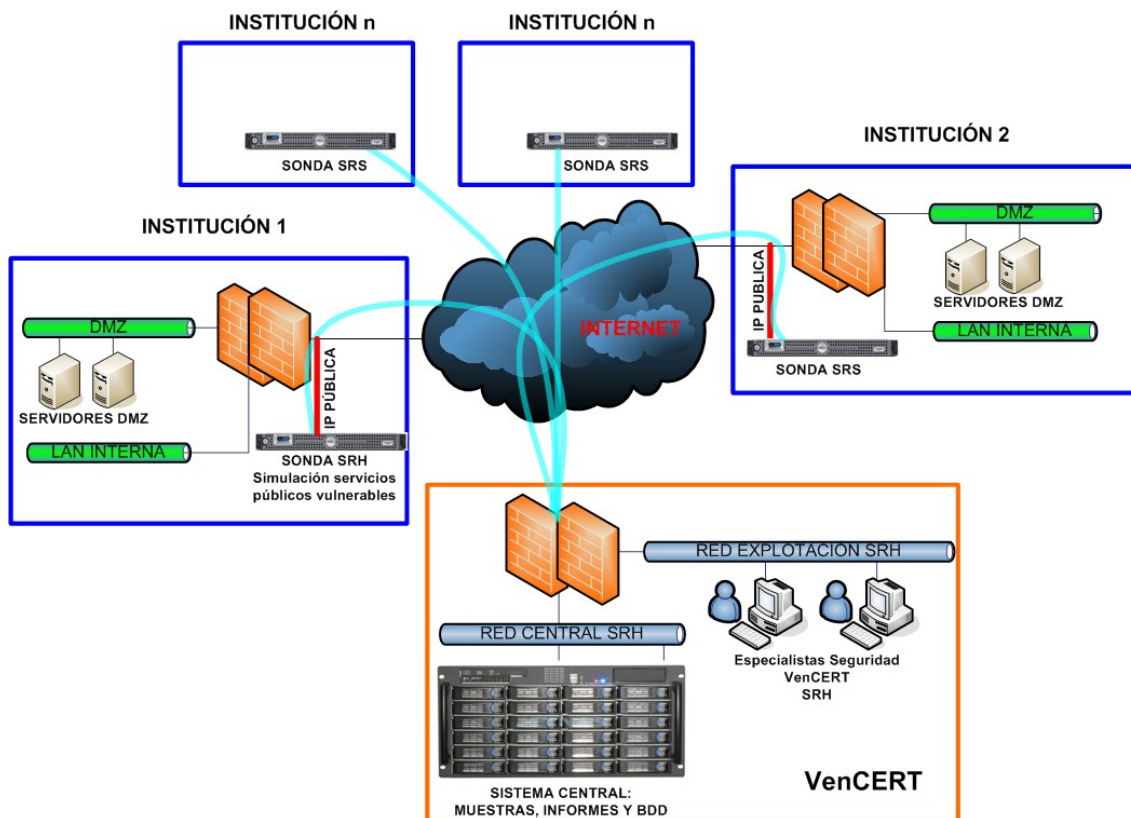


Figura 1. Arquitectura del Sistema de Red de Sensores Honeybots

¿Cómo adherirse?

Para beneficiarse de las numerosas ventajas que ofrece este SRH, los entes públicos que así lo deseen pueden firmar un convenio de adhesión con el VenCERT, a través del cual obtendrán información de gran relevancia para garantizar la seguridad telemática de sus sistemas.

No en vano, el Sistema va perfeccionándose día a día, con la mejora de los software de Honeybots y el desarrollo de arquitecturas de red dentro del mismo. Todas las mejoras irán propagándose a los sensores ya desplegados así como a las nuevas incorporaciones.

Por su parte, los organismos adheridos pueden actualizar o incluir más o menos servicios en el Honeybot, asignar más de una dirección IP o personalizar los contenidos falsos para dar más verosimilitud (por ejemplo, crear una réplica de la web original de la institución).

En definitiva, este SRH permite un aprendizaje avanzado de los ataques modernos, tanto genéricos de Internet como personalizados, así como ralentizar posibles ataques reales, ofreciendo una respuesta rápida y eficaz a los incidentes antes de que ocasionen daños serios a los sistemas de la Administración Pública Nacional.