

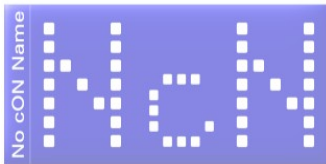
Concurso
Seguridad Informática
“Iluminación de Randa”
organizado por
No cON Name 2010

PATROCINADORES DEL EVENTO



COLABORADORES





BASES DEL CONCURSO

Los participantes adoptarán un papel de **Responsable de Seguridad** de una entidad bancaria, a partir de ahora “la Entidad”, la cual está sufriendo un severo incidente de seguridad, que se describe en el apartado “Descripción del incidente”.

Se pretende que las bases del concurso sean lo suficientemente abiertas, y sólo como punto de partida, para que los concursantes puedan desarrollar diferentes soluciones, profundizando hasta el nivel en que éstos consideren oportuno.

Se considerarán procedentes, por parte de los participantes, aquellas suposiciones organizativas y tecnológicas que estén debidamente argumentadas y sean consistentes con la realidad del sector al que pertenece “la Entidad”.

La solución al concurso deberá estar **compuesta de un grupo de tareas, de múltiples disciplinas**, algunas de las cuales podrán ser realizadas simultáneamente y otras tendrán dependencias por satisfacer.

Los participantes podrán presentarse al concurso de forma individual o en equipo, de hasta un máximo de 5 personas.

ESCENARIO DEL INCIDENTE

Sergei es un chico introvertido e influenciado, que se gana la vida administrando sistemas de un ISP. Al parecer, su prima *Irina* hace un tiempo mantuvo una relación con un empleado del departamento de tesorería de “la Entidad” y ahora quiere vengarse por algún asunto del que prefiere no hablar.

Sergei decide ayudar a *Irina*, para lo cual contacta con *Hackerparker*, un chaval con un oscuro pasado al servicio del mejor postor. En un correo que le manda *Sergei*, se pide comprar algún *Oday* o exploit que le permita realizar actividades de dudosa catadura moral. *Hackerparquer* pasa un tiempo buscando vulnerabilidades en aplicaciones comúnmente utilizadas, buscando el santo grial. Al final, después de un mes buscando, llega a encontrar una vulnerabilidad, que vende por 1000 euros, *PoC* incluido.

Por otra parte, *Sergei* conoce a un argentino que ha creado un software capaz de espiar un ordenador y actualizarse mediante módulos, todo integrado en una consola web, en la que sólo hay que esperar a que los datos interesantes lleguen a la misma. *Sergei* piensa que el software merece la pena, ya que, según dice el argentino, es casi indetectable.

Hasta la fecha, *Sergei* ha invertido 1.500 euros y aún no ha obtenido ningún rédito. Pero esto puede cambiar cuando *Sergei* consigue modificar el *PoC* para que éste baje el malware y ejecute el agente.

Con todas las cartas sobre la mesa, *Irina* manda un par de mails a su ex-pareja, *Andrés*. En el último de los emails enviados, le remite una foto subida de tono, bajo el



nombre, *irina.jpeg*. Andrés alertado y adoctrinado por el Departamento de Seguridad de “la Entidad”, activa todas las alertas, pero viendo que su antivirus no detecta nada sospechoso, decide abrirlo. Efectivamente, allí está Irina. Por debajo, el exploit ha hecho su efecto y el agente acaba de instalarse.

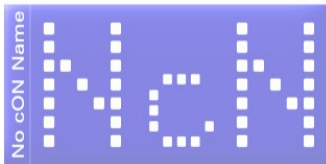
Un par de días después, *Sergei* decide visitar su portal y descubre 20 máquinas distintas conectadas desde diferentes IPs, aunque casi todas son la misma. La razón, Andrés decidió compartir con sus compañeros, y con otros Departamentos, los ficheros que Irina le mandó.

Varias semanas más tarde, el equipo del HelpDesk de “la Entidad”, mientras realizaba técnicas de mantenimiento rutinarias, se percató de un comportamiento inusual de la estación de trabajo de Andrés. En concreto, se ha constatado el establecimiento de comunicaciones sospechosas contra una IP externa y desconocida, así como la instalación de una máquina virtual con Windows Vista, dentro de su estación de trabajo.

Este hecho es reportado de inmediato al Departamento de Seguridad, por lo que rápidamente, tu equipo y tú os ponéis a investigar el caso. Al poco rato os dais cuenta de que la máquina, potencialmente comprometida, establece múltiples conexiones hacia el puerto 80 de otras IPs externas a “la Entidad”.

A través del *Port Mirroring*, tu equipo y tú comenzáis a ver un ingente número de conexiones sospechosas hacia puertos 80. En la consola centralizada de recolección de logs de “la Entidad”, no tardáis mucho tiempo en comprobar una relación directa entre el crecimiento anómalo de históricos de conexiones a puertos 80 con un evidente caso de fraude, donde miles de clientes de “la Entidad” se vienen quejando, desde hace semanas, de compras ilegítimas que no han sido efectuadas por ellos. De hecho, se rumorea que este patrón de fraude está afectando a otras entidades bancarias. A partir de este momento se disparan todas las alertas dentro de “la Entidad”.

Como responsable de Seguridad de “la Entidad” debes apresurarte y tomar las decisiones y medidas adecuadas.



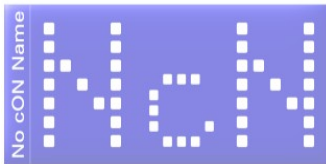
OBJETIVOS

El objetivo del concurso consiste en que los participantes proporcionen las estrategias, tácticas y operativas necesarias **(tanto organizativas, tecnológicas o legales)** para conducir el incidente de seguridad que está impactando contra “la Entidad”, entre los cuales deberán cubrirse los siguientes mínimos:

- Contención del incidente.
- Identificación de evidencias que aporten información sobre la naturaleza del incidente.
- Análisis de la causa raíz del incidente.
- Determinación de los controles que no han funcionado adecuadamente.
- Determinación de carencias, deficiencias o aspectos de mejora en los controles de seguridad.
- Establecimiento de medidas preventivas necesarias para que, en el futuro, un incidente de seguridad, de similares características, no impacte contra “la Entidad”.
- Planificación, en tiempo, necesaria para cubrir cada una de las fases en las que se desglose la solución propuesta.

Nota: Se espera que el participante trate, siempre que exista causa justificada, entre otros temas, los siguientes aspectos:

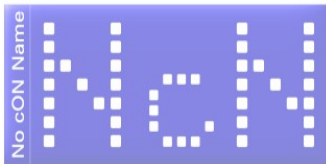
- Investigación en segundo plano de personal involucrado
- Análisis forense y temas éticos que pueden verse afectados durante el transcurso de la investigación forense.
- Ingeniería inversa de comunicaciones y sistemas.
- Ajuste/optimización de elementos de firewalling, IPs y correladores de eventos.
- Actividades legales contra el personal involucrado y posibles colaboradores. En el ámbito del territorio Español.



SISTEMA DE VALORACIÓN DE LAS SOLUCIONES RECIBIDAS

Las soluciones recibidas serán analizadas por un jurado multidisciplinar que valorará, entre otros, los siguientes aspectos:

- Análisis de la situación actual y esclarecimiento de lo sucedido.
- Eficacia y eficiencia de las soluciones proporcionadas, las cuales pueden ser soluciones tecnológicas, organizativas o legales.
- Nivel de detalle que el participante ha conseguido desarrollar.
- Viabilidad o impacto que las soluciones proporcionadas puedan tener sobre el negocio de “la Entidad”.
- Rapidez para contener el incidente.
- Realismo en la planificación para llevar a cabo la solución proporcionada.
- Claridad y detalle de las soluciones proporcionadas, donde se deberán diferenciar dos informes: uno resumido y otro detallado. El documento detallado no deberá ser superior a 30 páginas. Si fuese necesario, se permitirán anexos sin limitación de páginas, siempre y cuando esté justificado.
- Las soluciones deberán aportarse en formato pdf



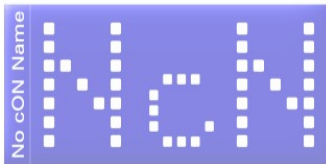
JURADO

El jurado estará compuesto por:

- 1 persona de la asociación No cON Name
- 1 persona experta en seguridad del sector banca.
- 1 persona de la administración pública catalana.
- 1 persona profesional de la seguridad, blueliv.com

FECHAS

- **La fecha final de presentación de los documentos será el 5 de Octubre de 2010 a las 14 horas.**
- Al entregarse la propuesta se puede entregar con los nombres reales o con un pseudónimo.
- Habrá un premio para los ganadores. Se les avisará días antes del comienzo del congreso para que puedan acudir a la entrega de premios.
- **Dichos ganadores deberán avisar y acudir al congreso para reconocer la victoria, en caso contrario, el premio lo recibirá el siguiente equipo con mayor puntuación.**
- La entrega se hará por correo electrónico a la dirección: concurso.randa_EN_noconname.org



ELEMENTOS TECNOLÓGICOS CON LOS QUE CUENTA “LA ENTIDAD”

Como Responsable de Seguridad de “la Entidad”, dispones de un equipo de 4 personas con los siguientes perfiles:

- 1 experto en seguridad de las telecomunicaciones.
- 1 experto en sistemas.
- 1 experto en ingeniería inversa.
- 1 experto en materia legal.

Tú, como líder del equipo eres un experto en gestión de respuesta ante incidentes.

Adicionalmente, “la Entidad” cuenta en la actualidad con los siguientes elementos tecnológicos que puedes gestionar:

- Pareja balanceada de firewalls perimetrales.
- Un IPS perimetral.
- Sistema centralizado de correlación de logs.
- Antivirus reconocido (McAfee), correctamente actualizado y distribuido en todas las estaciones de trabajo.

Dentro de “la Entidad” existe un departamento encargado de la gestión de Sistemas, el cual no tiene competencias en el ámbito de la Seguridad pero se recomienda que exista una buena coordinación entre ambos departamentos.

A título informativo, el parque tecnológico es el siguiente:

- VLAN para la red interna, con 1000 estaciones de trabajo basadas en Windows 7. Por política de seguridad, ningún usuario de las estaciones de trabajo debería tener privilegios administrativos sobre sus máquinas.
- VLAN para la red de 50 servidores, basados fundamentalmente en Linux RedHat adecuadamente actualizados, 1 sistema Host.
- VLAN para la DMZ.

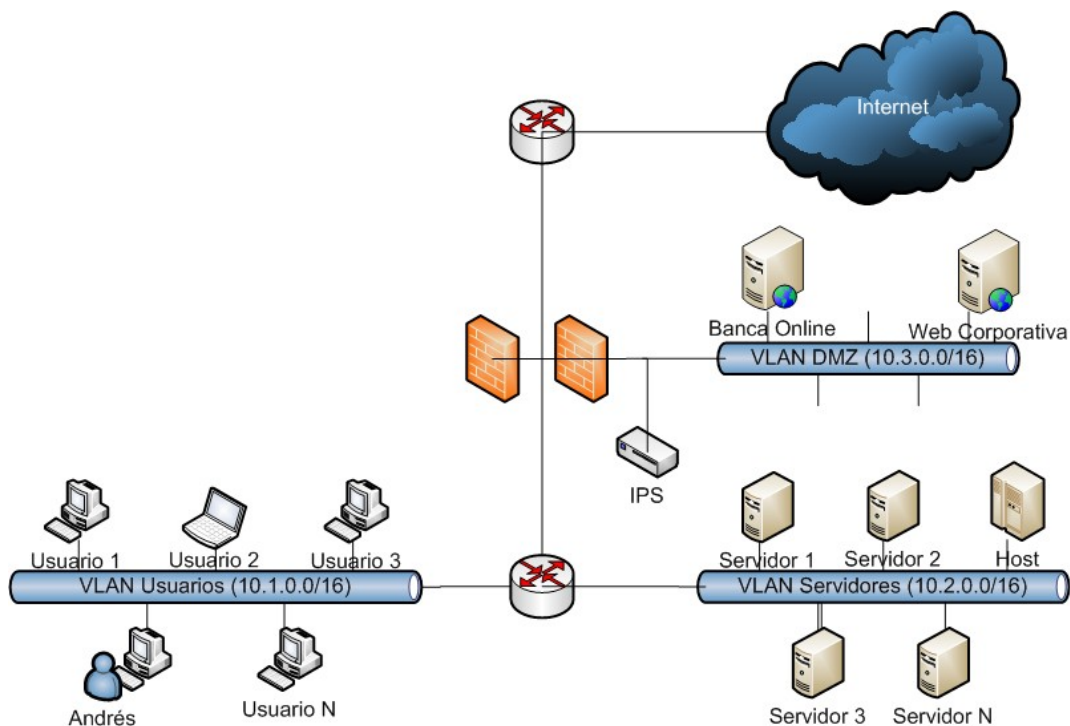


Diagrama generalista de red de "la Entidad"

EVIDENCIAS TECNOLÓGICAS PROPORCIONADAS

Los participantes, en función del detalle tecnológico que quieran abordar, disponen de las siguientes evidencias tecnológicas:

- Volcado de memoria de la máquina virtual.
- Trazas del tráfico capturado en la red.

Dicha información puede ser descargada desde:

http://noconname.org/concursos/NcN_2010_Randa_Evidencias_Concurso.tgz