WarGame 2011

Asociación No cON Name

PATROCINADORES DEL CONCURSO

ackstorm Deloitte.

Elaborado por

internet security auditors

1. BASES DEL CONCURSO

El concurso presenta diversos retos de exploiting que deberán ser solucionados por los participantes. Los retos están catalogados por niveles (del 0 al 5), de manera que para poder realizar el reto de un nivel deben resolverse previamente los retos de niveles inferiores. Los participantes deberán demostrar que disponen de los conocimientos suficientes sobre el funcionamiento de diversos aspectos, como los procesos de un sistema o las redes de comunicaciones, para poder superarlos.

La solución del concurso debe estar compuesta de un documento en el que se explique de la forma más clara posible los métodos utilizados para superar cada una de las pruebas.

2. DESCRIPCION DEL ENTORNO

Los participantes reciben una máquina virtual VMware (http://www.vmware.com) que puede ser ejecutada mediante VMware Player. Esta máquina dispone de diversos usuarios, uno para cada nivel, de manera que explotando los diversos retos que se plantean el participante irá cambiando de usuario y elevando privilegios.

Las características del sistema operativo instalado son las siguientes:

- Debian GNU/Linux 5
- Kernel 2.6.32
- Servicios públicos:
    - Puerto 22: SSH (Secure Shell)

El participante debe asumir que la máquina proporcionada para el concurso es completamente remota, por lo que en ningún momento se aceptará como solución nada que requiera acceso físico a la máquina virtual (modificar la imagen, arrancar en modo single, hacer login a través de los terminales locales, etc). La única vía de acceso legítima es a través de la red y el servicio SSH instalado.

El sistema recibe una dirección IP de forma automática (DHCP), por lo que utilizando la arquitectura NAT de VMware Player es posible conocerla a través del propio panel de configuración. En caso de que VMWare no proporcione esa dirección IP, un script de arranque del sistema mostrará la IP por pantalla, para que pueda ser consultada desde los terminales locales.

Así mismo, cada uno de los usuarios tiene en su propio directorio *HOME* un fichero llamada *password.txt* que contiene la contraseña del siguiente nivel, por lo que el objetivo de cada uno de los retos es llegar a leer dicho fichero.

Para iniciar el reto se describe el primer nivel, o Nivel 0. La información de los consiguientes niveles se obtendrá como resultado de la superación de cada nivel.

LEVEL 0

A continuación se describe el primer nivel (level0) que deberán superar los participantes:

- **Objetivo:** Conectar por SSH con la máquina virtual empleando el usuario *level0* y la contraseña *uym0a*5Jb288;.!.*

- **Pista:** Analiza bien las comunicaciones. Analiza bien los paquetes enviados y recibidos. Por favor, no ignores ESTE mensaje, sólo lo que sea necesario.

2.1. OTROS DATOS

MD5SUM 6d45f2921da41d656865f84221c6bc79 - ncn11_vm.tar.bz2

3. JURADO

El jurado estará compuesto por:

- 1 persona de la asociación No cON Name
- 1 persona experta en seguridad de Internet Security Auditors

4. FECHAS

Habrá 3 ganadores del concurso.

Los participantes deberán elaborar un documento explicando como se han superado las pruebas.

Los criterios serán según:

- 1.Orden de recepción del documento.
- 2.Originalidad de las técnicas utilizadas.
- 3.Detalle de la explicación.

La fecha final de presentación de los documentos será el 15 de Septiembre de 2011 a las 15 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 el mismo día 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 participante con mayor puntuación.

La entrega se hará por correo electrónico a la dirección:

concurso.wargame_EN_noconname.org