Computer Forensics Linux
Post Mortem In Situ
TechnologyInt

1) Justificación

Cada delito informático sigue un modus operandi, que se convierte en el desafío para el investigador en informática forense. En su proceso de investigación interna o judicial, su labor termina cuando sus habilidades le permiten determinar y establecer una hipótesis de lo sucede. En esta charla se demostrará cómo se realiza un análisis de datos forense en sistemas muertos en un Servidor Linux comprometido por un atacante, por medio de técnicas forenses internacionalmente aceptadas que entreguen como producto final un buen informe, que sea punto de partida para la investigación judicial y el aporte de los elementos probatorios.

2) Objetivos del programa

El Objetivo principal es un proceso de inclusión del participante en el conocimiento práctico de las técnicas de informática forense en sistemas Linux y sus sistemas de archivos, con base en un escenario real de análisis forense informático que permita generar una hipótesis de los sucesos, evidencias y artefactos del estado real de una imagen o segundo original de un servidor comprometido, para determinar el que, como, cuando, donde, etc., se determinó como objetivo militar.

TechnologyInt realizara la transferencia de conocimiento y documentación base para el desarrollo y solución de entornos virtualizados por parte de los inscritos al taller.

3) Competencias Adquiridas(Ventajas y Beneficios)

- Conocer y aplicar los conceptos de análisis de evidencias digitales
- Conocer las técnicas de Identificación y recolección de evidencia digital
- Desarrollar prácticas de recolección de evidencia conociendo las diferentes Herramientas
- Manejar técnicas modernas de peritaje de sospechosos en casos de delito Informático
- Analizar sistemas muertos (Post Mortem In Situ)
- Manejar herramientas de identificación técnica de evidencias
- Realizar Análisis Informático Forense en Sistemas Linux

4) Dirigido a:

- Gerentes de Tecnología
- Especialistas de Seguridad Informática
- Auditores de Seguridad
- Oficiales de Seguridad
- Asesores y Consultores de TIC
- Administradores de red u Operadores de sistemas
- Ingenieros de Sistemas
- Auditores de Sistemas e Informática
- Individuos y entusiastas interesados en la Seguridad Informática

Prerrequisitos:

- Conocer los conceptos básicos de Sistemas Operativos
- Conocimiento Básico de Linux
- Conocimientos Básicos de Red y TCP / IP

5) Metodología de la Actividad

1. Escenario a Analizar
2. Estación forense DEFT
3. Esterilizando el contenedor de medios
4. Adquisición de la Imagen Forense (Segundo Original)
5. Identificando los dispositivos (Original – Contenedor del Medio)
6. Identificando Información para anclar cadena de custodia y embalaje de medios
7. Revisando los Hash de Integridad
8. Iniciando la estación forense DEFT
9. Haciendo uso de Mount Manager para identificar los medios
10. Identificando Dispositivos por consola
11. Presentando alternativas para adquisición de Imagen
12. Generando Hash de Integridad con DHASH
13. Proceso de Adquisición de Imagen con GUYMAGER
14. Montando la imagen con MOUNTMANAGER
15. Inconvenientes del Proceso de Análisis Digital Forense con AUTOPSY
16. Montando Imagen por Consola
17. Creando Bitácora del Perfil del Objetivo Digital Forense
    i. Versión del SO
    ii. Puntos de Montaje
    iii. Resolución de Nombres
    iv. Zona de Tiempo
    v. Hostname
    vi. Sistemas de Archivos (FileSystem)
    vii. Mensajes del Día
    viii. Papelera de Reciclaje
    ix. Profile usuarios
    x. Certificados de seguridad
    xi. Configuración de Red
    xii. Puertos y Servicios
    xiii. PATH
    xiv. Tareas programadas
18. Generando Líneas de tiempo (LOG2TIMELINE)
19. Explorando el Sistema
20. Revisando Logs y Mensajes de Consola
21. Visualizando accesos y salidas del sistema
22. Identificando vectores de ataque en el Servidor Linux
23. Análisis imagen forense Linux (LVM)

24. Otras dificultades en el Montaje de una imagen forense Linux (LVM)
25. Identificando LVM
26. Analizando imagen forense (LVM)
27. Creando Bitácora del Perfil del Objetivo Digital Forense
    a. Versión
    b. Hardware
    c. Profile user
    d. Hosts
    e. SELinux
    f. Puntos de montaje
    g. Archivo de usuarios y password
    h. Configuración inicios del sistema
    i. Configuración de Red

28. Analizando información con Bulk extractor
29. Analizando información con FLAG

30. Estación forense CAIN
31. Cain Interface
32. Adquisición de Imagen con AIR
33. Conociendo los Scripts Forensics de CAIN
34. Creando imágenes virtuales con XMOUNT

35. Analizando información con PTK

36. Estación forense SANSFORENSICS
37. Haciendo uso de offset para generar Imágenes forenses
38. Uso de STRINGS para filtrar información
39. Haciendo uso de FIND
40. Haciendo uso de SORT

6) Metodología de la Actividad

El curso está basado en el Desarrollo de **2 ESCENARIO PRACTICOS DE ENTRENAMIENTO** de Servidores Linux Comprometidos.

Aplicación del curso:

- Exposición magistral con el apoyo de medios audiovisuales.
- Información en Medios Electrónicos del curso y las herramientas a utilizar
- Elaboración de Laboratorios Prácticos en un ambiente controlado de cada tema por parte del instructor.
- Practicas por los asistentes al curso de los Laboratorios anteriores
- Conclusiones y Síntesis del Curso

30% Magistral 70% Practico.

7) Certificación

TechnologyInt

8) No. de horas y horario

Total Horas: 16

Dos días en la semana con sesiones diarias de 8 Horas para un total de 16 Horas.

9) Facilitador

JHON JAIRO HERNANDEZ HERNANDEZ (Dinosaurio / Dino) Administrador de Empresas, con experiencia en Gerencia en Consultoría Empresarial.

Tecnólogo Profesional en Sistemas de Información y con Especialización en Administración de la Información. Con veinte (22) años de experiencia en Sistemas e Informática y doce (12) años de experiencia en Seguridad Informática, Columnista de diversos artículos de seguridad Informática, Hardening, Análisis Informática Forense, Hacking Ético en revistas Electrónicas.

Analista en Seguridad Informática e Investigador en Informática Forense. Vinculación con las Empresas SWAT Security-IT (Director de Proyectos), ThemuroGroup, Password S.A., DEFERO SAS, SEGURIDAD ATLAS, Desarrollando Proyectos de Seguridad Informática y Seguridad de la Información (Aseguramiento / Hardening, Análisis de Seguridad, Análisis Informático Forense, Auditorias de Sistemas, ISO 27000) a Organizaciones Gubernamentales, Estatales, Sector Público y Privado.

Asesor y Consultor de TICS. Capacitador en Pregrado, Diplomados y Especializaciones de Seguridad Informática en Universidades (Universidad Autónoma de Occidente UAO, Universidad del Valle, Universidad Cooperativa de Colombia, Universidad Libre de Colombia, Universidad del Pacifico) y Capacitador cursos de Ethical Hacking en Centros de Entrenamiento.

Ponente Nacional e Internacional en temas de Seguridad Informática en diversos eventos:

4 Congreso Nacional de Hacking Ético y Computo Forense UNIMINUTO, Conferencia y taller de Análisis Informático TechnologyInt Republica Dominicana, Forense VII CONGRESO DE PREVENCION DEL FRAUDE Y SEGURIDAD Asobancaria, TecnoPyme-FENALCO 2013, Webinar Security Zone 2012, Security Zone 2012, Security Zone 2011, Campus Party 2012, Campus Party 2011, Campus Party 2010, Seminario Tecnológico - SISTEMAS COMPUTACIONALES ATRAVES DE MEDIOS TECNOLOGICOS - UNIVALLE, Bar camp Security, Securinf, Freedomday, Flisol, HackingDay, Congreso de Virtualidad UNAD. Seminarios y Universidades (Universidad del Valle, Universidad Javeriana, Universidad Santiago de Cali, Universidad Libre, Universidad Autónoma de Popayán, UNAD de Neiva).

Blog : http://world-of-dino.blogspot.com/ (EL MUNDO DE DINOSAURIO)
Twitter: @d7n0

10) **Ayudas audiovisuales**

_X_ Computador	_X_ Video Proyector	_X_ Pantalla
___ Sonido	___ Proyector de acetatos	__ DVD
___ Televisor	___ VHS	_X_ Internet

Otros:

Trae Portátil para dictar sus clases? SI _X NO __