RECOLECCION DE EVIDENCIA

5.1. Protocolo De Recoleccion De Evidencia

Fases de adquisición De Evidencia

1. IDENTIFICAR 2. ASEGURAR 3. DOCUMENTAR
4. GENERAR CADENA DE CUSTODIA

Compu Apagada

Fotografiar escena y equipo, mantener apagado,desconectar alimentación,documentar conexiones,desconectar conexiones

Compu Encendida

Fotografiar escena y equipo, extraer info volatil,generar imagen de disco,apagar equipo

Asegurar Evidencias

-Protección antiestática
-Embalaje Protegido
-Etiquetado De Evidencia
-Recopilar información Documental

Orden de Volatilidad

1.CPU,cache y contenido de registro
2.Tablas De enrutamiento, cacheARP,tabla de proceso y estadísticas de kernel
3.Memoria RAM
4.ficheros temporales y espacio de intercambio
5.DD
6.Datos almacenados en recursos remotos
7.Soportes digitales externos

5.2 ALMACENAMIENTO DE EVIDENCIAS

Necesidades deAlmacenamiento
-gran cant de almacenamiento
-largos plazos de almacenamiento
-proteccion contra robo o sabotaje

Precauciones
-Inventario de evidencia
-Acceso Restringido
-Control ambiental
-proteccion de red eléctrica
-evitar polvo ocorrocion
-aislamiento antiestático

Dispositivos Moviles
-Jaulas de Faraday
-Pack de Baterias
-info volátil
-clave de desbloqueo
-tarjetas memoria extraíble

Proteccion Frente a Corrupcion De Datos
-Aislamiento de incidente
-Identificacion de incidente
-Compartimentacion

5.4.COPY DE SEGURIDAD

a-Clonado De Discos
-duplicados físicos
-copy bit a bit
-disco de destino(sobreescrito en 0s E igual al original)

b-Imagen de Discos
-De disco a archi org
-Ventajas(Duplicable,manejabley copiable)
-desventaja(Mas espacio de memoria)
Herramientas De Copias
-db hacer copy bit a bit
-Db proteger contra escritura
-Db calcular hashes
-Db docum registro de errores
-Db generar reportes

5.4.RECUPERAR DATOS DE NAVEGADORES

Basicos(-historial-Favoritos-Lista de lectura)
Tecnicos(-cache-cookies-Datos de seciones-contraseñas)

EVIDENCIAS BASADAS EN RED

6.1.REGISTROS DE FIREWALLS

CATEGORIAS
a.Filtro de paquetes en base a info del datagrama
b.Inspector de Paquetes en base a la infor y contenido del datagrama

6.2.DETECTAR INTRUSIONES EN LA RED

Teardrop-AtaqueLAND-Smurg(envio masivo de ICMP) yFraggle(envio masivo de UDP)

6.3.EVIDENCIAS EN LOS ROUTERS

Modificacion del firmware-Denegacion de serv
Q hacer:
-No reiniciar el router
-Buscar manual
-Contraseña de acceso
-Extraer config y registros

INV FOR WINDOWS

7.2.REGISTRO DE EVENTOS DE WINDOWS

Tipos de registro
(Seguridad-Aplicaciones-Sistema)

7.3.Directorios especiales de Windows

Dir Claves

Los números HASH, considerados como números de resumen son obtenidos mediante la aplicación de un algoritmo de HASH. Este algoritmo crea un número en base al contenido de un grupo de bits, de tamaño uniforme (dependiendo del algoritmo utilizado), sin tomar en cuenta la cantidad de bits sobre la que se aplica el algoritmo. Este número tiene una dependencia del contenido evaluado por el algoritmo permitiendo que si se realice un cambio en los datos, el numero HASH cambiara
Existen dos tipos de algoritmos hash; los no cifrados y los cifrados.
Los algoritmos de HASH más usados son:
MD5 (Message-Digest Algorithm 5 o Algoritmo de Firma de Mensajes 5)
SHA-1 (Secure Hash Algorithm 1 o Algoritmo de Hash Seguro 1)
Digital Signature Algorithm (DSA)
RJPEMD-160