fidélitas Virtual

Computación Forense

Ataques Informáticos

Clase 4a

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Ataques Informáticos

- **Ataques de Malware**

  - La lista es amplia, pasando desde los backdoors, botnet, rootkit, spam malware, programas de robo de credenciales, entre otros.

  - Su propagación es variada, utilizando programas falsos, downloads maliciosos, dispositivos removibles, link o adjuntos de correo electrónico, y muchos más.

  - El malware de hoy, dista mucho del malware de hace varios años, se han alcanzado niveles de sofisticación increíbles que buscan hacer más difícil su detección y las pericias forenses contra ellos.

Ataques Informáticos

- **Ataques de Malware**

  - El malware moderno cuenta con módulos de cifrado, de empaquetado, de ofuscación, entre otras técnicas de engaño.

  - El análisis de archivos de malware debe realizarse en ambientes controlados que permitan aislarlo de la red en producción, preferiblemente en ambientes virtuales en los cuales se puedan aplicar técnicas de snapshot para tomar “fotos” en el momento y poder revertir el proceso fácilmente.

  - No es necesario grandes infraestructuras para esto, existen soluciones gratuitas en el mercado como virtualbox o vmware player que pueden solventar esta necesidad.

Ataques Informáticos

- **Ataques de Malware**
  - Para su análisis, existen dos categorías, análisis estático y dinámico.
  - En los ambientes virtuales, es importante contar con herramientas que identifiquen el comportamiento y el tráfico de la red para poder determinar cuáles son las acciones que el malware está tratando de ejecutar.
  - Un punto de análisis obligatorio para buscar malware son los procesos de arranque del sistema operativo, de acuerdo con el utilizado, debe informarse sobre estas ubicaciones y determinar si existen elementos extraños a los mínimos necesarios.

Ataques Informáticos

- **Redes de Datos**

  - Es necesario contar con herramientas que permitan detectar intrusos o amenazas avanzadas de forma automatizada y no depender de análisis humanos que se realicen esporádicamente.

  - Normalmente, los ataques utilizan la red para extraer información o ejecutar movimientos de un equipo a otro, la capacidad de capturar todos los eventos de la red para su análisis posterior es complicado por la gran cantidad de recursos que se requieren, por eso debemos ser inteligentes en la ubicación de estos puntos de control.

  - La detección del origen del incidente, del paciente cero y/o la ruta de intrusión se pueden determinar gracias a este tipo de dato.

Ataques Informáticos

- **Redes de Datos**
    - Las bitácoras se pueden analizar en tiempo real o post mortem.
- **Vulnerabilidades de la red**

Vulnerabilidades Internas

Vulnerabilidades Externas

Ataques Informáticos

- **Redes de Datos**

Ataques Comunes

- Escuchas ilegales
- Alteración de datos
- Suplantación de IP
- DoS
- Ataques de Hombre en el Medio
- Ataques fuerza bruta y Diccionario
- Malware

Ataques Específicos Wireless

- Punto de acceso no autorizado
- Asociación errónea de clientes
- Asociación no autorizada
- Suplantación de MAC
- Interferencia
- Ataques de Desconexión de usuarios

Ataques Informáticos

- **Redes de Datos**

  - En los laboratorios probaremos varias técnicas de ataques para que comprenda el proceso que un atacante sigue a la hora de comprometer información o recursos de la organización.

  - Mantener siempre un ojo en las bitácoras es muy importante.

Gracias

fidélitas Virtual