Trabajo Práctico N°4

Conceptos de Seguridad

1. Explique y relacione los conceptos de:
   a Vulnerabilidad: debilidad.
   b Amenaza: condición que expone esa debilidad.
   c Incidente: es lo que se genera al explotar la amenaza. Es vulnerabilidad + amenaza.

2. Explique el concepto de seguridad "en capas".

Un sistema operativo consta de al menos cuatro niveles: hardware, kernel, sistema operativo y usuario. Estas constituyen capas separadas de seguridad en sí mismas.

Dado que la seguridad es un objetivo de calidad, es esencial que la política de seguridad sea coherente con el diseño del SO, mas aun, un buen diseño es un problema de seguridad.

La seguridad en capas se puede considerar en el diseño del SO como una serie de círculos concéntricos, con las operaciones más sensibles en las capas más internas. Entonces, la confiabilidad y los derechos de acceso de un proceso se pueden juzgar por la proximidad del proceso al centro: los procesos más confiables están más cerca del centro (el kernel). Esta separación es lógica, por lo tanto debe haber un responsable (el SO) que controle los accesos a todas las capas externas o superiores.

3. Investigue/analice los riesgos introducidos en una organización por uso de redes sociales y mensajería instantánea.

El correo no deseado es el riesgo mas considerable, tanto en correo electrónico como en mensajeria instantánea. Los creadores de correo no deseado aprovechan la popularidad de las redes sociales para diseñar nuevas técnicas de correo no deseado. Como estos servicios permiten enviar mensajes entre usuarios registrados, proporcionan un punto de entrada fácil para los remitentes de correo no deseado.

Donde las personas pueden escribir información normal, los spammers intentarán colocar anuncios.

El spam puede llegar como mensaje directo, actualización de estado, comentarios en videos, solicitudes de contacto, etc. Algunos métodos incluso generarán múltiples mensajes en diferentes canales. Por ejemplo, si un usuario envía invitaciones a eventos en Facebook, el usuario recibirá un mensaje de notificación dentro de Facebook, pero también una notificación por correo electrónico, a menos que el usuario haya deshabilitado explícitamente los correos electrónicos de notificación.

4. Términos relacionados: Busque la definición correspondiente a cada uno de los siguientes términos:
    a Exploit: Fragmento de datos o secuencia de comandos, utilizada para aprovechar una vulnerabilidad en un sistema informático.
    b Malware: Software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. Se lo considera hostil, intrusivo o molesto.
    c Buffer Overflow: error de software producido por un programa que no controla adecuadamente los limites del área de memoria reservada para él.
    d Troyano: malware que aparenta ser un programa legítimo e inofensivo, pero que al ejecutarlo, brinda a un atacante acceso remoto al equipo infectado.
    e Shellcode: exploit basado en un conjunto de órdenes inyectadas en la pila de ejecución de un programa, para obtener una shell.
    f Ransomware: (del inglés ransom, “rescate”) es un tipo de programa que restringe el acceso a archivos, y pide un rescate a cambio de quitar esta restricción.
    g Fuerza bruta: en criptografía, es la forma de recuperar una clave probando todas las combinaciones posibles.
    h DOS: es un ataque a un sistema o red para lograr que un servicio o recurso sea inaccesible a usuarios legítimos.
    i DDOS: es un ataque por denegación de servicios realizado en forma distribuida. Es decir, múltiples equipos atacando al mismo servicio para saturarlo.
    j Bot: programa que efectúa automáticamente tareas repetitivas a través de Internet.
    k Botnet: red de bots. Se trata de un conjunto de bots que se dispersan en una red, conel objetivo de colectar datos y realizar tareas en nombre de su lanzador.
    l Flooding: algoritmo de enrutamiento simple, basado en enviar los paquetes entrantes por

todas las interfaces.

m SPAM: mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario.

n Cracking: conducta delictiva en donde un individuo altera datos de un sistema informático para obtener un beneficio.

o 0day: vulnerabilidad que es desconocida para aquellos que deben mitigarla. Hasta que se mitigue, los atacantes pueden explotarla para afectar el sistema.

p MitM: ataque en el que se adquiere la capacidad de leer, insertar y modificar un mensaje a voluntad en un canal. El atacante intercepta mensajes del emisor y el receptor originales, sin que ninguno de ellos lo sepa.

q Hoax: noticia falsa, es un intento de hacer creer a un grupo de personas que algo falso es real.

r Rootkit: conjunto de herramientas para acceso root, en forma oculta al control de los administradores. Debe radicar en la maquina que pretende afectar.

s Backdoor: secuencias especiales o excepciones dentro del código, que permiten un acceso al sistema evitando los controles de seguridad.

t Phishing: suplantación de identidad, es un modelo de abuso informático destinado a obtener información confidencial de forma fraudulenta.

u Bug: error de software. Es un problema en un programa que desencadena un resultado indeseado.

v Pharming: es una alteración en el software de los servidores DNS (Domain Name System), que permite redirigir un nombre de dominio a una máquina distinta.

w Ingenieria Social: es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

x Sniffing: escucha de paquetes para obtener información. Es una técnica pasiva ya que no altera la comunicación, sólo la escucha.

y Spoofing: suplantación de identidad. El atacante se hace pasar por una entidad distinta a través de la falsificación. Puede falsearse la ip, arp, dns, web o email.

z Scanning: herramienta automatizada que escanea aplicaciones web, normalmente desde el exterior, para buscar vulnerabilidades de seguridad como cross-site scripting,

inyección SQL, inyección de comandos, configuración de paths y servidores.

aa Script Kiddie: persona falta de habilidades técnicas. Considerada un incompetente en una actividad específica, a pesar de llevar suficiente tiempo para aprender sobre ello.

5. ¿Qué problemas de seguridad puede provocar un ataque de sniffing sobre tráfico SMTP, POP o HTTP? ¿Desde qué red/redes tiene sentido dicho ataque?

El contenido no esta cifrado. Este ataque tiene sentido en una LAN, donde el trafico puede ser escuchado por hosts que no son necesariamente el destinatario.

6. Una dirección MAC: ¿Se puede falsificar? ¿Desde qué red tiene sentido dicho ataque? ¿Con qué objetivo alguien malintencionado lo haría?

Si, es posible clonar una MAC. Este ataque tiene sentido en capa 2, ruteo a nivel de switch, para vulnerar la estrategia de ruteo de los switches. Al invadir al switch con MAC's cambiantes se lo obliga a reordenar su tabla de ruteo, agregando nuevas MAC's hasta colapsar. Llegado este caso, el atacante podría escuchar cierto paquetes especiales de configuración de la red y sus host.

7. Analice cómo funciona el protocolo ARP. ¿Qué ataque podría realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque?

Podría atacar con una técnica de suplantación de ARP (ARP spoofing), que consiste en enviar mensajes ARP falsos a la red, para que el switch mas próximo asocie la MAC del atacante con la dirección IP de otro nodo (el atacado). Estos ataques tienen sentido en una LAN.

8. Una dirección IP: ¿Se puede falsificar? ¿Desde qué red tendría sentido dicho ataque? ¿Con qué objetivo alguien malintencionado lo haría?

Si, puede falsificarse. Esto tendría sentido en LAN e INTERNET.

El primero en caso que la red use autenticación basada en direcciones IP. Es decir, los sistemas internos confíen entre sí y los usuarios pueden iniciar sesión sin un nombre de usuario o contraseña.

El segundo caso se aplica a ataques de denegación de servicio, donde el objetivo es inundar un servidor con un volumen abrumador de tráfico. Estos paquetes no son rastreables (y por tanto difíciles de filtrar) ya que parecen provenir de direcciones diferentes.

9. Analice cómo funciona el protocolo ICMP. ¿Qué ataque puede realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque?

Podría realizar ataques de re-direccionamiento ICMP, en donde se envían mensajes a varios gatweays para redireccionar el trafico. Ataque del "hombre en el medio".

También podría ser un ataque de denegación de servicio distribuida (o ataque smurf), en donde un gran número de paquetes ICMP con IP origen falsificada (se pone el de la victima) se transmite a la dirección de la red. Los dispositivos responderán a la dirección IP de origen, inundandola de tráfico.

10. Analice cómo funciona el protocolo DNS. ¿Qué ataque podría realizar alguien malintencionado usando este protocolo? ¿Desde qué red tendría sentido dicho ataque? ¿Qué mejoras se han propuesto sobre DNS?

Los tipos de ataques DNS incluyen:

- Ataque del día cero: el atacante aprovecha una vulnerabilidad aun desconocida en el software del servidor DNS.
- Envenenamiento de DNS: el atacante corrompe un servidor DNS reemplazando una dirección IP legítima en el caché del servidor por otra para redirigir el tráfico a un sitio web malicioso, recopilar información o iniciar otro ataque.
- Denegación de servicio: un ataque en el que un bot envía más tráfico a un servidor de lo que puede atender. El objetivo es no resolver solicitudes legítimas.
- Amplificación DNS: el atacante aprovecha un servidor DNS que permite búsquedas recursivas para propagar su ataque a otros servidores DNS.

11. OWASP:
    a Describa brevemente el objetivo de la organización.

Es una comunidad abierta dedicada a permitir a las organizaciones concebir, desarrollar, adquirir, operar y mantener aplicaciones en las que se pueda confiar. Según ellos, la seguridad de las aplicaciones es un problema de personas, procesos y tecnología, y sus enfoques incluyen mejoras en todas estas áreas.

b ¿Cuáles fueron los tres riesgos más críticos de seguridad en aplicaciones web en el año 2017?

1. Inyección

   Las fallas de inyección, tales como SQL, NoSQL, OS e inyección de LDAP, ocurren cuando los datos que no son de confianza se envían a un intérprete como parte de un comando o consulta. Los datos hostiles pueden engañar al intérprete para que ejecute comandos no deseados.

2. Autenticación rota

   Las funciones relacionadas con autenticación y administración de sesiones a menudo se implementan incorrectamente, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación.

3. Exposición de datos sensibles

   Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como financieros, de atención médica, etc. Los atacantes pueden robar o modificar estos datos para realizar fraude con tarjetas de crédito, robo de identidad u otros delitos.

c ¿Qué información puede encontrar acerca de Ransomware?

1. Guías de protección ante estos ataques

   https://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project.

2. Descripción de un ataque de este tipo

   https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwiztKXXj5_bAhWHslkKHReeApEQFgg-MAM&url=https%3A%2F%2Fwww.owasp.org%2Fimages%2F0%2F04%2FOWASP_-_Anatom%25C3%25ADa_de_un_ataque_ransomware_v2.pdf&usg=AOvVaw33_mEm7Jg5-Exd9Fc9xPNI.