Amenazas Lógicas II

Adware

El adware es un software que despliega publicidad de distintos productos o servicios.

- Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes.
- Pueden agregan ícono gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo,etc

Backdoors

Estos programas son diseñados para abrir una “puerta trasera” en nuestro sistema de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él.

El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes denominadas botnets.

Botnet

Un malware del tipo bot es aquel que está diseñado para armar botnets.

- Una botnet es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida.
- Cuando una computadora ha sido afectado por un malware de este tipo, se dice que es un equipo es un robot o zombi.
- El grupo "propietario de la red" de zombies puede alquilar a otros grupos su red para realizar alguna acción ilegal.
- El objetivo de las redes zombies puede ser realizar ataques de DDoS, distribución de SPAM, etc.

Hoax

Un Hoax (del inglés: engaño) es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena.

- Algunos informan sobre virus desastrosos, otros apelan a la solidaridad con un niño enfermo o cualquier otra noble causa
- Otros contienen fórmulas para hacerse millonario o crean cadenas de la suerte como las que existen por correo postal.

Keylogger

Es un programa que registra y graba la pulsación de teclas (y algunos también clicks del mouse).
La información recolectada será utilizada luego por la persona que lo haya instalado.

Hardware

son pequeños dispositivos que se instalan entre nuestra computadora y el teclado.

Software

son los más comunes, muy utilizados por el malware orientado a robar datos confidenciales o privados del usuario.

Pharming

Es un ataque que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirte a una página Web falsa.

- El atacante logra hacer esto al alterar el proceso de traducción entre la URL de una página y su dirección IP.
- Comúnmente el atacante realiza el redireccionamiento a las páginas web falsas a través de código malicioso.

Rogue o Scareware

Un rogue software es básicamente un programa falso que dice ser o hacer algo que no es.
Con el tiempo fueron evolucionando creando desde “Falsos Optimizadores” de Windows, y en los más extendidos “ Falsos Antivirus ”.

Al ejecutarlos ‘siempre’ nos van a mostrar alguna falsa infección o falso problema en el sistema que si queremos arreglar vamos tener que comprar su versión de pago, la cual obviamente en realidad no va a reparar ni desinfectar nada, pero nos va a mostrar que sí.

Riskware

Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Rootkit

Los rootkits se compone de varias herramientas que, usadas en conjunto, permiten obtener acceso privilegiado a un dispositivo.

Lectura

https://latam.kaspersky.com/resource-center/definitions/what-is-rootkit

Spam

Se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero.

- En español, también es identificado como correo no deseado o correo basura.

Spyware

Software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento.

- El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.
- Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario.
- También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se visitan.

Ransomware ó Secuestradores

Es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos.

- La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

Lecturas Complementarias

El malware crece día a día, por lo que siempre podemos encontrar algo nuevo. Con el objetivo de mantenernos informados, recomiendo la lectura de los siguientes link, donde podrán encontrar ejemplos de casos reales.

Ransomware

http://www.welivesecurity.com/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/

Phishing vs Spam

http://www.welivesecurity.com/la-es/2014/06/03/phishing-spam-conoce-5-diferencias-entre-correos/

Etapas de un Ataques (Aproximación)

Etapas

1) Recolección de información

El primer paso es saber en que forma se recolecta la información y además que tipo de información se recolectará sobre el objetivo en cuestión.

Para recolectar información se pueden utilizar herramientas como las siguientes:

El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.

El programa TraceRoute puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico.

El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.

Servidores DNS pueden accederse para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).

El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.

El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar.

2) Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el atacante trata de probar cada uno de los servidores para debilitar la seguridad. Algunas de las herramientas que se pueden utilizar automáticamente para explorar individualmente los servidores residentes en una red

EJ: Una vez obtenida una lista pequeña de la vulnerabilidad de servicios en la red, un atacante bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión.

3) Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema.
Después de tener el acceso al sistema protegido, el atacante tiene disponibles las siguientes opciones:
a) Puede atentar destruyendo toda evidencia
b) Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como “caballos de Troya” protegiendo su actividad de forma transparente.
c) Pueden encontrar otros servidores que realmente comprometan al sistema.

4) Ataques remotos

Escaneos de puertos (portscan)

Una de las primeras actividades que un potencial atacante realizará contra su objetivo será sin duda un escaneo de puertos.

- Esto le permitirá obtener en primer lugar información básica acerca de qué servicios estamos ofreciendo en nuestras máquinas y, adicionalmente, otros detalles de nuestro entorno como qué sistema operativo tenemos instalados en cada host o ciertas características de la arquitectura de nuestra red.
- Analizando qué puertos están abiertos en un sistema, el atacante puede buscar agujeros en cada uno de los servicios ofrecidos:

cada puerto abierto en una máquina es una potencial puerta de entrada a la misma.

Los escaneadores de puertos

Por lo general, no se usará telnet para realizar un escaneo de puertos masivo contra un sistema o contra toda una red para esto existen herramientas como **nmap** que pueden realizar esta tarea de una forma más o menos cómoda y automatizable.

Los escaneadores de puertos actuales implementan diferentes técnicas que permiten desde detectar desde la versión del sistema operativo usado en la máquina atacada hasta pasar inadvertidos ante diferentes sistemas de detección de intrusos.

Spoofing

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada.

- la idea de este ataque es que desde su equipo, un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

DNS Spoofing

Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP).

ARP Spoofing

El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

Ej: algunos Man in the Middle contra ciertos protocolos cifrados.

Web Spoofing

Este ataque permite visualizar y modificar cualquier página Web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL.

- un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima,
- a partir de ahí, enruta todas las páginas dirigidas al equipo atacado

Interceptación (sniffing)

La interceptación de datos en tránsito o en proceso por parte de usuarios no autorizados se puede lograr tanto en forma fisica (**sniffers de alta impedancia**) como en forma logica.
La interceptación lógica de datos más conocida y extendida es el sniffing:
Es muy común que el sniffing se produzca utilizando programas (sniffers) y no elementos hardware.

Proceso:

- En las redes de difusión, cuando una máquina envía una trama a otra indica en un campo reservado la dirección del host destino, todas las máquinas del dominio de colisión ven esa trama, pero sólo su receptora legítima la captura y elimina de la red.
- Existe un modo de funcionamiento de las interfaces de red denominado modo promiscuo, en el cual la tarjeta lee todas las tramas que circulan por la red, tanto dirigidas a ella como a otras máquinas, el leerlas no implica el eliminarlas de la red, por lo que el host destino legítimo la recibirá y eliminará sin notar nada extraño.

Ejemplo: resultado del uso de wireshark

Prevencion:

Para evitar que programas de este tipo capturen nuestra información existen diferentes aproximaciones más o menos efectivas:

1- Sustituir los HUBs de nuestra red por switches que aíslan dominios de colisión (esto dificulta el ataque pero no lo imposibilita)
2- Implantar redes privadas virtuales.
3- Usar de protocolos cifrados siempre que nos sea posible (que lo suele ser casi siempre)
4- Sustituir telnet y rlogin por SSH y FTP por scp o sftp

Ataques potenciales
Ingenieria social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.

Las técnicas de Ingeniería Social han evolucionado!
http://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/
Crónica de una estafa real por e-mail
http://www.welivesecurity.com/la-es/2012/11/13/cronica-engano-e-mail/

Shoulder Surfing

Consiste en “espiar” físicamente a los usuarios, para obtener claves de acceso al sistema.

Masquerading

- Masquerading o mascarada consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático esta suplantación puede realizarse electrónicamente
- un usuario utiliza para acceder a una máquina un login y password que no le pertenecen - o en persona.

Ej: con una tarjeta de identificación robada que un lector acepta, o con un carné falsificado.

Basureo

La técnica del basureo (en inglés, scavenging) está relacionada tanto con los usuarios como con la seguridad física de los sistemas

- consiste en obtener información dejada en, o alrededor, de un sistema informático tras la ejecución de un trabajo.

El basureo puede ser físico: como buscar en la basura (trashing, traducido también por basureo), listados de impresión o copias de documentos.

El Basureo puede ser lógico: como analizar buffers de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información.

Gracias…