JuanpabloSalado

Nivel: 1
Tipo: individual
Modo: obligatorio
Dificultad: intermedio

Skootik Mobile Technologies

https://skootik.com
info@skootik.com

Hay que ser consciente de que cuando se desarrolla un software y se despliega una infraestructura que soporte un servicio este tiene que ser lo más seguro posible. Para ello es importante conocer cuales son las posibles vulnerabilidades de la infraestructura digital y ponerle remedio

La seguridad es importante

En cuantas películas de Hollywood has visto al "típico hacker" con su peculiar y característica forma de vestir, sin amigos, introvertido, ... pues bien, hasta aquí todo ciencia ficción.

Para empezar, los hackers no tienen porqué parecerse a esta barata descripción hollywoodiense y para continuar la palabra "**hacker**" se refiere a la **persona capaz de introducirse en sistemas informáticos** ajenos pero sin fines ilícitos. De hecho, muchos hackers están contratados por empresas financieras, industriales incluso estatales para hacer de sus sistemas informáticos entornos más seguros. Las personas que además de ser capaces de entrar en sistemas ajenos, lo hacen con fines delictivos, son más conocidos en la jerga informática como "**crackers**".

En cualquier caso, la cruda realidad es que en los sistemas y arquitecturas digitales así como en los softwares informáticos, **SIEMPRE**, existen vulnerabilidades, agujeros de seguridad que si los descubre un cracker, puede tener el control absoluto de cualquier organización. Podríamos utilizar la analogía de la puerta de casa: no es lo mismo poner en nuestra vivienda una puerta de una fina chapa o de madera maciza, obviamente, la puerta gruesa aguantará más la envestida de cualquier caco; ahora, si este viene con un coche-ariete y utiliza la técnica del alunizaje, al final terminará por derribar la puerta aunque sea de madera maciza.

Con la informática ocurre algo parecido. Cuanto más seguro sea nuestro sistema informático mejor, cuanto más grueso y robusto sean nuestros filtros de seguridad mejor. PERO... no existe la seguridad al 100%. Eso no significa que debemos perder la guardia. Debemos estar atentos a los tipos de ataques informáticos que existen e intentar poner un remedio a la hora de construir nuestros software-s de Inteligencia Artificial. Imaginad por un minuto el desastre que supondría que un cracker se introdujese en el sistema informático que gestiona todos los coches de conducción autónoma Tesla.

Asumiendo que todos los sistemas son vulnerables, además de la seguridad, es igual de importante la segmentación de la información, y la restricción de accesos por niveles. De este modo se limitará el impacto cuando se produzca una brecha. Un buen sistema de copias de seguridad (backup) que permita en caso de ataque purgar el sistema también es vital.

Existe una larga lista de ataques informáticos y de malware-s. Así como los brotes de gripe se producen en una estación determinada del año y empiezan a extenderse entre la población, las epidemias para los PC, teléfonos inteligentes, tabletas y redes empresariales no son previsibles. Las computadoras enferman gracias a programas informáticos conocidos como **malware**, y existen de diferentes tipologías: *virus, troyanos, gusanos, spyware, ransomware, adware, ...* Algunas infecciones son sigilosas y otras nada sutiles. Pero siempre hay modos de prevenir nuestras computadoras contra la infección.

Además de estos malware-s existen diferentes tipos de ataques bastante comunes que es interesante nombrar para que los @eggers tengáis una radiografía genérica de a qué tipo de ataques os podéis enfrentar cuando desarrolléis una aplicación comercial:

1.- DDoS (denegación de servicio): Imaginad que tenéis una aplicación web de Inteligencia Artificial para la detección de objetos en imágenes. A esta aplicación se accederá escribiendo la URL (dirección) en el navegador. Pues bien, el servidor donde se ejecuta vuestra aplicación solo puede procesar una cierta cantidad de solicitudes de una vez, de modo que si un atacante sobrecarga el servidor con muchas solicitudes, el servidor no dará más de sí. El servidor se caerá y nadie podrá disfrutar del servicio que ofreces.

2.- Inyección SQL: Son fragmentos de código que generalmente el cracker introduce utilizando una puerta de entrada que siempre está accesible como son los campos de los formularios de cualquier aplicación web (*por ejemplo, el buscador de google es un campo de un formulario, formularios para el inicio de sesión, formularios de contacto, ...*) para obtener información de las bases de datos o alterarlas. Es necesario poner filtros de seguridad detrás de todo formulario e incluso cifrar la información relevante escrita en las bases de datos por si alguien externo a la organización accediese a ellas.

3.- Man in the middle: Ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Hasta hace pocos años Tom (persona 1 ficticia) podía escribir una carta a Lisa (persona 2 ficticia) en la que le expresaba su amor. Podría ocurrir que el mensaje lo interviniera un cartero entrometido. Imaginad que abre la carta y decide reescribirla a su gusto. Este acto podría provocar que Lisa termine odiando a Tom de por vida.

Ahora piensa lo que podría hacer un cracker si interviene tus comunicaciones cuando inicias una sesión en tu red social favorita. Podría interceptar y capturar cualquier información que enviamos al servidor, como credenciales de inicio de sesión o información financiera, por ejemplo.

4.- XSS (Cross-Site Scripting): Cuando el atacante es capaz de inyectar un script, normalmente Javascript, en la salida de una aplicación web de forma que esta se ejecutará en el navegador del cliente. Por ejemplo, una ventana emergente que enlace a otra aplicación web.

5.- Ingeniería social: Trata del arte de manipular a las personas para que compartan su información confidencial: contraseñas, información bancaria, ... Existen muchas técnicas de persuasión. Imagina por un momento que eres un alto ejecutivo de una importante multinacional y que dispones de información privada sobre las cuentas de las empresa en el ordenador del trabajo. Según subes por el ascensor... QUÉ SUERTE! Te acabas de encontrar un pendrive en el suelo y decides mirar el contenido. Introduces el pendrive en el ordenador y... la curiosidad mató al gato! El atacante acaba de instalar software malicioso en tu ordenador que le dará acceso a toda la información de la corporación. El atacante a dado con el eslabón más débil de toda la cadena de acontecimientos: TÚ!

Por si esto no fuera poco, y con el ánimo de explotar aún más estas vulnerabilidades, existe una técnica que hemos sufrido todos nosotros alguna vez: el PHISING. Es una técnica muy común de ingeniería social. Así que, CUIDADO!

6. ...

Ante grandes problemas grandes soluciones: Hoy en día, existe un modo de evitar estos problemas: **la prevención**. Para esta prevención se utilizan técnicas y metodologías de Pentesting. Es una abreviatura de las palabras inglesas *penetration* y *testing*. Se refiere a la práctica de atacar diversos entornos con la intención de descubrir errores, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas. Es una rama de estudio relativamente reciente y en auge (sobrevenido por los importantes ataques y filtraciones sufridos por varias empresas importantes durante los últimos años).

Herramientas útiles:

1.- Wireshark: Herramienta gratuita y multiplataforma con interfaz gráfica para el análisis de red. Enlace de descarga

2.- Advanced Port Scanner: Explorador de redes gratuito que permite encontrar con rapidez los puertos abiertos de los equipos conectados a la red e identificar las versiones de los programas que se están ejecutando en los puertos detectados. El programa cuenta con una interfaz muy intuitiva y una gran variedad de funcionalidades. Enlace de descarga

3.- ...

Recuerda que nadie estamos a salvo de un ataque digital pero tenemos que procurar prevenir lo máximo posible para reducir la probabilidad al mínimo.

#HASHTAGS *(etiquetas de ayuda para búsqueda de información relevante)*

#seguridad-informática #pentesting #tipos-de-ataques-informáticos

LINKS DE INTERÉS

https://www.youtube.com/watch?v=gwEq0-ACUr8
https://www.youtube.com/watch?v=Fj9TwMTxGuc
https://www.youtube.com/watch?v=c8XS1CB_nUg
https://www.youtube.com/watch?v=JDHdW9kof4w

DICCIONARIO

Pentesting | XSS | Inyección SQL | Ataque informático | Ataque DDoS | Ingeniería social | hacker | cracker | Man-in-the-middle | Phising

PUNTUACIÓN

Programación: 2
Redes: 2
Seguridad: 6
Algoritmia: 2