**CIBERSEGURIDAD Y HACKING ÉTICO**

2ª Evaluación: Prácticas guiadas, inyección html y phishing. Y una de explotación. Y exámen que vale menos.

* **Phishing:**

**Definición:**

*Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace)*

**Método**:

*Para realizar el engaño, habitualmente se hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. También mediante la adulación de la víctima, explotando su intrínseca vanidad o necesidad de ser reconocido, baja autoestima, o una persona que busca trabajo. Por ejemplo, enviando correos electrónicos o mostrando publicidades a la víctima diciéndole que ha ganado un premio y que siga un enlace para recibirlo, siendo aquellas promesas falsas (un cebo). A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.*

**Origen:**

*El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión a utilizar un cebo y esperar a que las víctimas "muerdan el anzuelo".*

**Tipos:**

*\* Phishing general, phishing tradicional, Bulk Phishing o Spray and pray. Consiste en la emisión masiva de correos electrónicos a usuarios. Estos correos suplantan a entidades de confianza (ejemplo bancos) y persiguen el engaño del usuario y la consecución de información. Por ejemplo en el mensaje se incluyen enlaces a dominios maliciosos. Para camuflar estos enlaces es habitual*

*que el texto del enlace sea la URL correcta, pero el enlace en sí apunte al sitio malicioso.*

*\* Vishing. Es similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica. El término deriva de la unión de dos palabras en inglés: ‘'voice'’ y ‘'phishing’'.*

*\* Smishing. Es similar al phishing tradicional pero el engaño se produce a través mensajes de texto ya sean por SMS o mensajería instantánea (como WhatsApp).*

*\* URL Phishing. Se trata de engañar al usuario haciendo que una URL de un sitio malicioso parezca la de un sitio confiable. A ellas a veces se accede de forma inadvertida al escribir nombres de dominio mal escritos que están muy cerca del dominio legítimo, o siguiendo un enlace malicioso que parece correcto, o por engaños al usar caracteres unicode parecidos difícilmente detectables.*

*\* Whaling. Se diferencia de los otros tipos de intentos de phishing en que el objetivo son personas importantes como por ejemplo ejecutivos de alto rango. Las solicitudes de información contenidas en el ataque están más adaptadas a la persona concreta.*

* + <a href=”192.168.1.234”>Banco Santander</a>
  + <a href=”www. caixa.es”>Caixa</a>
    - **carácter “ilegal”**
    - **DNS**
      * Ip verdadera
      * Ip falsa →Servidor DHCP/DNS/WEB
      * Registros que lleven a otros sitios, aunque quieras acceder comunmente a www.caixa.es
* **Injection:**

**Definición:**

*Sql Injection ó Inyección SQL es una vulnerabilidad que permite al atacante enviar o “inyectar” instrucciones SQL de forma maliciosa y malintencionada dentro del código SQL programado para la manipulación de bases de datos, de esta forma todos los datos almacenados estarían en peligro. La finalidad de este ataque es poder modificar del comportamiento de nuestras consultas a través de parámetros no deseados, pudiendo así falsificar identidades, obtener y divulgar información de la base de datos (contraseñas, correos, información relevante, entre otros), borrar la base de datos, cambiar el nombre a las tablas, anular transacciones, el atacante puede convertirse en administrador de la misma.*

*Esto ocurre normalmente a la mala filtración de las variables en un programa que tiene o crea SQL, generalmente cuando solicitas a un usuario entradas de cualquier tipo y no se encuentran validadas, como por ejemplo su nombre y contraseña, pero a cambio de esta información el atacante envía una sentencia SQL invasora que se ejecutará en la base de datos.*

* + select\* from usuarios where usuario=’admin(variable nombre)’ and clave=’1234(variable clave)’
* **Exploiting:**

*Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.*

(Fuente: Panda Security, https://www.pandasecurity.com/es/security-info/exploit/)

*Exploit es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.*

*Su uso principal es como vector para la inyección de una carga útil (en inglés payload) que ofrezca al atacante algún tipo de acceso y/o control del equipo comprometido. Un payload puede ser usado por varios exploits y un mismo exploit puede utilizar varios payloads.*

**Metasploit:** herramienta para explotar la máquina **METASPLOITABLE**

-Vulnerabilidad: fallo/debilidad en la seguridad de un sistema que podría ser aprovechado por alguien.

-Exploit: software que se va a aprovechar de una vulnerabilidad de un sistema, que nos va a permitir ganar acceso a un servidor, escalar privilegios (lograr ser root, con lo que podríamos hacer cualquier acción en la máquina), ataques DOS…

\* Se define como los módulos que utilizan payloads

\* Una vulnerabilidad sin una capacidad de payload es un módulo auxiliar

-Riesgos: pérdida de rendimiento del servidor, filtración de información, dejar un backdoor de forma que alguien podría utilizarlo.

-Payload: es la carga que se ejecuta en esa vulnerabilidad, es decir, la carga que activamos a la hora de aprovechar dicha vulnerabilidad.

\* Los Payloads consisten en código que se ejecuta de forma remota

\* **Codificadores** asegurar que los Payloads llegan a su destino

\* **Nops** mantener los tamaños de los payloads constante.

* **Auditing:**

*Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.*

*Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes*

*deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.*