Ejercicios propuestos – Módulo 1

En este documento se proponen una serie de ejercicios para realizar en clase con el alumnado. Con estos ejercicios se busca una mayor comprensión de los aspectos vistos en la teoría. De cara al curso de incidentes de ciberseguridad del CEP, **solo es obligatorio realizar el ejercicio 1 y subirlo a la plataforma**. El resto de ejercicios son solo propuestas opcionales.

Criterio de evaluación 1a:

Ejercicio 1: En este ejercicio vamos a usar gpg para el envío de mensajes cifrados. De esta manera pondremos en práctica el principio de la confidencialidad. Concretamente vamos a realizar lo siguiente:

1. Generar unas claves para nuestro equipo mediante gpg.
2. Exportar nuestra clave pública.
3. Importar la clave pública anteriormente exportada de gpg.
4. Cifrar un archivo de texto con un mensaje con la clave pública anterior.
5. Descifrar un archivo recibido con nuestra clave privada.
6. Listar todas las claves privadas almacenadas en nuestro equipo.
7. Listar todas las claves públicas almacenadas en nuestro equipo.

Ejercicio 2: Actualmente existe un debate moral sobre hasta cuánto es necesario y moralmente aceptable una cesión de información a cambio del uso de un servicio. Existen páginas webs que analizan estos aspectos, como: https://foundation.mozilla.org/es/privacynotincluded/

Por ejemplo:

https://foundation.mozilla.org/es/privacynotincluded/products/amazon-halo/

Además, es habitual que se usen las redes sociales para exponer datos sin conocer los riesgos que ello implica.

1. Buscar distintos productos que te llamen la atención en dicha web o en otras similares.

2. Establecer un debate en clase sobre la privacidad en la sociedad actual.

Criterio de evaluación 1b:

Ejercicio 3: Para proteger el puesto de trabajo es interesante establecer una normativa de obligatorio cumplimiento. Para ello vamos a realizar lo siguiente:

1. Define una empresa ficticia (o describe una empresa real que conozcas). Es decir, ámbito de negocio, activos críticos, tipos de empleados, roles de los mismos y posibles riesgos. La empresa no necesariamente debe tener un modelo de negocio relacionado con la informática. La cultura de la ciberseguridad es algo que debe existir en cualquier empresa actual (contabilidad, dentista, transporte…).

2. Define una serie de políticas de obligado cumplimiento en la empresa. Estas políticas formarán la normativa de protección del puesto de trabajo. El objetivo debe ser el de minimizar la superficie de ataque. Ayúdate de lo visto en la teoría para realizarlo.

Criterio de evaluación 1c:

Ejercicio 4: Dentro de la concienciación en ciberseguridad encontramos el uso de contraseñas únicas, con cierta complejidad, y que no estén anotadas en papeles cerca de las mesas. Para lograr estos objetivos existen los gestores de contraseñas. Uno de los gestores de contraseñas más conocidos y de código abierto es bitwarden. En este ejercicio debes instalar la extensión bitwarden para tu navegador y hacer uso de ella para generar una contraseña, así como almacenarla de forma segura en él.

Ejercicio 5: El phishing es una técnica de envío de correos de forma masiva, suplantando la identidad de un tercero. Mediante estos ataques se busca que la víctima realice alguna acción contraproducente para ella, ya sea enviando información privada, contraseñas, instalando algún malware en su dispositivo… En este ejercicio se propone:

1. Buscar noticias de phishing u otras estafas y coméntalas. Para encontrarlas se puede hacer uso de los buscadores de internet, o a través de las redes sociales, mediante los #estafa, o #nopiques, #phishing...
2. Busca recomendaciones para identificar y evitar caer víctima de phishing. ¿Qué consejos darías para no caer en ellos?
3. Busca en tu correo, posiblemente en la carpeta de spam, si tienes emails de phishing y analízalos. Si vas a hacer clic en los enlaces, se recomienda emplear una máquina virtual o un navegador con javascript desactivado. Si quieres indagar aún más, puedes buscar quién es el propietario del dominio del enlace, buscar más información del dominio en buscadores de internet, etcétera.

Ejercicio 6: Para poder lograr establecer una cultura de la ciberseguridad en la empresa, es necesario que se establezca un plan para implementarla. En nuestro caso, la cultura de la ciberseguridad se realizará mediante un plan de concienciación.

En el ejercicio 2 hemos generado una empresa ficticia, y sobre ella hemos desarrollado una serie de políticas de protección del puesto de trabajo. Reutiliza la misma empresa para realizar este ejercicio. En este caso el objetivo es generar una cultura de concienciación en ciberseguridad en los empleados de la misma. Para ello realiza un documento donde detalles, **al menos**, los siguientes apartados:

1 Planificación

1.1 Identificar necesidades

1.2 Destacar debilidades

1.3 Adaptaciones necesarias de tu programa de concienciación

1.4 Exponer qué metodología vas a emplear para desarrollarlo

2 Cómo lo vas a implementar (implementación del plan de concienciación)

2.1 Alcance y objetivos

2.2 Cómo se va a involucrar a TODO el personal (recuerda que no solo es tarea del Dpto de IT)

3 Cómo lo vas a operar y mantener esa concienciación: Indicar una serie de ejercicios que vas a realizar con ellos para que se asiente la conciencia sobre los aspectos que hemos mencionado arriba.

4 Cómo vas a monitorizar y evaluar el grado de consecución

4.1 Qué métricas aplicarías para saber si ha funcionado o no

Establecer un plan de concienciación para lograr establecer una cultura de la ciberseguridad en una empresa. Para desarrollarlo, no olvides consultar fuentes a través de internet, como por ejemplo: https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/

Criterio de evaluación 1d:

Ejercicio 7: El objetivo de esta práctica es que os familiaricéis con cómo se realiza una campaña de emails masivos. Esta práctica es una de las partes del entrenamiento del empleado, y como tal, debería formar parte del plan de concienciación. Es una manera de "entrenar" a los usuarios para que eviten el phishing. El objetivo de la práctica es:

1. Instalar gophish y configurarlo.
2. Registrar un usuario.
3. Crear un perfil de envío. Es posible que con las cuentas de gmail debáis activar el inicio de sesión en aplicaciones no seguras. Si no os sentís cómodos, podéis usar una cuenta con otro proveedor de emails, como yahoo u outlook, por ejemplo.
4. Crear una landing page.
5. Crear una plantilla de correo. Recuerda meter en la plantilla los textos {{.FirstName}} {{.LastName}} {{.Position}} {{.Email}} {{.From}} para hacerlo más creíble y personalizado para cada receptor.
6. Crear un grupo de envío de correos.
7. Configura un “reporting email”, es decir, un email al cual los empleados deberían reenviar los emails que crean que son fraudulentos. Es una de las configuraciones posibles que permite gophish.
8. Lanzar dos campaña de phishing con éxito.
9. Ver los resultados y comprobar la adquisición de payloads por parte del usuario.

Ejercicio 8: Para poder implementar el plan de concienciación se suele emplear distintos materiales o avisos publicitarios. Desde el Incibe por ejemplo, se nos propone la creación de trípticos, posters, o presentaciones, lo cual podemos incrementarlo con el envío de emails con consejos de seguridad o recomendaciones a la hora de usar los productos o servicios corporativos de una empresa.

1. En esta actividad se propone elaborar nuevos posters, trípticos o presentaciones con consejos para concienciar en ciberseguridad. Existen herramientas online, como canva.com, que facilitan la creación de este tipo de material.

Ejercicio 9: En este ejercicio vamos a concienciar frente a malware. Para ello descarga el kit de concienciación de incibe, concretamente la carpeta de “Ataques dirigidos”. Para descomprimirlos tienes que usar la contraseña "INCIBE". Una vez los descomprimas, es muy posible que salte algún antivirus. Los archivos son totalmente seguros, simplemente incluyen un pequeño script para hacer ping cuando se abren.

En la carpeta "Herramienta_seguimiento" hay un servidor para lanzar. Hay dos posibilidades, o usar el .py (Python) o usar el .exe (ejecutable de Windows). Hacen lo mismo. Simplemente abren un servicio para escuchar si alguien ha lanzado un ping al abrir uno de los archivos maliciosos.

En la carpeta "Archivos_maliciosos" lo que hay son troyanos, que al hacer clic en ellos, si está bien configurada la IP, debería de lanzar un ping a la herramienta de seguimiento anterior.

La práctica consiste en:

1. Montar el servidor.
2. Picar en algún archivo.
3. Ver a la web que redirige.
4. Ver que al cerrar el servidor, se guardan los logs en un archivo.

Criterio de evaluación 1e:

Ejercicio 10: Para verificar el cumplimiento del plan de concienciación y de la normativa de protección del puesto de trabajo, se debe realizar una verificación de que los distintos aspectos se están llevando a cabo por los miembros de la organización.

Para poder realizar una auditoría de forma sistemática, una posible técnica a emplear es el uso de listas de comprobación (checklists).

1. Realiza una checklist, donde indiques qué elementos o políticas se van a comprobar y cómo. Además debes de indicar valores posibles que esperas para esa verificación. Por ejemplo:

Elemento a verificar	Cómo se va a verificar	Qué es un fallo	Qué es un acierto
Verificación del conocimiento de la normativa de protección del puesto de trabajo	Se enviará un formulario de Google a los empleados a través del email con una serie de preguntas.	El empleado responde de forma errónea más de un 35% de las veces.	El empleado acierta un 65% de las preguntas.