Ejercicio 1

Campaña de phishing vía Facebook Messenger busca robar claves de acceso.

Esta campaña esta diseñada para usuarios de dispositivos móviles, ya que cuenta con una cadena de validación para determinar si una potencial víctima accede al enlace desde un teléfono. De esta manera, si el usuario ingresa al enlace malicioso desde un equipo de escritorio, simplemente es direccionado a un video y evita la instancia del robo de información sensible.si el usuario accede al enlace desde un smartphone es dirigido hacia un sitio de phishing que simula ser la página oficial de inicio de sesión de Facebook donde el usuario debe supuestamente iniciar sesión ingresando la dirección de correo y contraseña que utiliza para acceder a la red social.

Arrestan en España a criminales relacionados con los troyanos bancarios Mekotio y Grandoreiro

La forma de actuación de ambos malware es a través de correos de phishing que parecen originales y suplantan la identidad de empresas u organismos gubernamentales. Los mismos incluyen un enlace malicioso para descargar el malware o un archivo adjunto para el mismo fin. Por ejemplo, en el caso de España se han visto correos haciéndose pasar por comunicaciones del Ministerio del Interior, la Agencia Tributaria y a la Dirección General de Tráfico (DGT), o utilizando en el asunto mensajes como “comprobante de transferencia bancaria”.

Ransomware REvil amenaza a Apple con divulgar blueprints robados de sus productos

Se trata de un grupo que está activo desde abril de 2019 y que apunta tanto a grandes compañías como a pequeñas empresas, adaptando los montos que exige por el rescate según las características de la víctima. Los vectores de ataque que más comúnmente ha utilizado son mediante fuerza bruta al RDP, correos de spearphishing, explotación de vulnerabilidades y exploit kits como Trickbot, por ejemplo.

Ejercicio 2

Si,

Noticia de robo de cuenta de Amazon, haciéndote creer que has ganado un premio.

Se trata de una campaña recurrente: suplantan la identidad de Amazon en una ‘encuesta con premio seguro’, este tipo de estafa puede llegar por correo electrónico, SMS o WhatsApp, aunque la parte ‘positiva’ es que la dinámica que utilizan los criminales es siempre la misma.

Se trata de un tipo de phishing que haciéndose pasar por la compañía busca conseguir tus datos personales y financieros. Además de emails y SMS, también se han detectado mensajes de WhatsApp.

Ejercicio 3

Objetivos principales de la seguridad informática.

Confidencialidad:
Se garantiza que está accesible únicamente al personal autorizado.

Integridad:
Tiene el objetivo de mantener los datos libres de modificaciones no autorizadas.

Disponibilidad:
Permite que la información esté disponible cuando lo requieran las personas o entidades autorizadas.
Alta Disponibilidad:
Es un protocolo diseñado del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un periodo de medición dado.

Autenticación:
Confirmación de la identidad de un usuario, aportando algún modo que permita probar que es quien dice ser

No Repudio:
Es la capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, es una comunicación o en la realización de una determinada acción.

Ejercicio 4

La 2 (c8m4r2nes) y la 4 (pr0mer1s&) podrían considerarse seguras.

De todas formas a la contraseña nº2(c8m4r2nes) para hacerla más segura le pondría alguna letra en mayúscula y un carácter especial.

Y la contraseña nº4 (pr0mer1s&) considero que es la más segura de todas a pesar de no incluir una letra en mayúsculas que igualmente no estaría mal añadirla.

Ejercicio 5

- 12345.
- 123456.
- 123456789.
- test1.
- Password.
- 12345678.
- Zinch.
- g_czechout.

A mi parecer, estas contraseñas para usarlas como medio de protección de un sistema en el que puede haber información bastante relevante, la mayoría de las contraseñas son muy obvias y no son para nada seguras.

Ejercicio 6

Activa, pasiva, lógica o física

1. Ventilador (equipo informático) → SEGURIDAD FÍSICA
2. Detector de incendios → SEGURIDAD FÍSICA
3. Detector de movimiento → SEGURIDAD FÍSICA
4. Cámara de seguridad → SEGURIDAD FÍSICA
5. Cortafuegos → SEGURIDAD LÓGICA
6. SAI → SEGURIDAD PASIVA
7. Control de acceso mediante huella dactilar → SEGURIDAD ACTIVA
8. Contraseña para acceder al sistema → SEGURIDAD ACTIVA
9. Control de acceso de un edificio → SEGURIDAD FISICA

Ejercicio 7

Usaría las siguientes prevenciones ante la seguridad activa en el aula de informática.

Emplear contraseñas seguras, las contraseñas deberán tener mínimo 8 caracteres, con mayúsculas, minúsculas, y números. Debido a que hay virus que intentan averiguar las contraseñas.

Encriptar solo los datos importantes que solo puedan leer las personas que sepan la clave.

Tener un antivirus actualizado.

Usar otros software de seguridad, además del antivirus, como el firewall o los anti espías.

Realizar copias de seguridad periódicamente de aquellas cosas que tengan valor

Analizar los equipos de forma periódica en busca de malware, puede que estén, pero no los tenga activos.

Tener un usuario auxiliar, debido a que hay virus que bloquean los perfiles de los usuarios.