

Actividad de clase: Un hacker experto nos muestra cómo se hace Objetivos

Comprender las vulnerabilidades de las tecnologías inalámbricas y de otras tecnologías comunes **Parte 1:**

Ver el Video TEDx "Top Hacker nos enseña como se hace; Pablos Holman at TEDxMidwests" Parte

2: Responder a las siguientes preguntas

Antecedentes / Escenario

Prácticamente todos los sistemas “seguros” que se utilizan actualmente pueden ser vulnerables a cualquier tipo de ciberataque.

Recursos necesarios

- Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Parte 1: Ver el vídeo “Top Hacker Shows Us How It’s Done; Pablos Holman at TEDxMidwests” (“Un hacker experto nos muestra cómo se hace; Pablos Holman en TEDxMidwests”) de TEDx

- Localice el video en Internet y visualícelo.
- Elijan uno de los ataques que menciona el Sr. Holman en el vídeo y utilicen su motor de búsqueda favorito para seguir investigando el ataque.
- Para el ataque que se eligió en el Paso 1b, respondan las siguientes preguntas. Estén preparados para compartir su trabajo con toda la clase.

Parte 2: Respondan las siguientes preguntas.

- ¿Cuál es la vulnerabilidad que se está atacando?

Escriba sus respuestas aquí.

Usb swicthblade

- ¿Qué datos o información puede obtener un hacker al atacar esta vulnerabilidad?

Escriba sus respuestas aquí.

- Claves de registro
- Actualizaciones instaladas.
- Hashes de contraseñas.
- Historiales de navegación.
- Copiar archivos de carpetas.

- ¿Cómo se realiza el ataque?

Previamente hay que preparar un pen drive, por ejemplo con la herramienta GonZors SwitchBlade que se insertará en el equipo víctima. Modificar el Autorun.inf para que se inicien una serie de sentencias.

Escriba sus respuestas aquí.

Es posible gracias a la opción AUTORUN que había en sistemas operativos hasta Windows XP SP3 que permanecía activada por defecto

♥ 2017 -2020 Cisco y/o sus filiales. Todos los derechos reservados. Información pública de Cisco Página 1 de 2 www.netacad.com

Actividad de clase: Un hacker experto nos muestra cómo se hace

d. ¿Qué fue lo que les interesó específicamente sobre este ataque?

Escriba sus respuestas aquí.

No lo conocía

e. ¿Cómo creen que podría mitigarse este ataque en particular?

Escriba sus respuestas aquí.

Sistema operativo actualizado último parches.

Escanear siempre pendrives que no sean de confianza.

En el caso de ese sistema operativo deshabilitar el autor run de dispositivos USB.

