**UNIVERSIDAD TECNOLOGICA DE PANAMA**

**FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES**

**Profesor:** Mgtr. José Moreno

**Objetivo:** Desarrollar un proyecto de pentesting, test de intrusión, seguridad ofensiva, auditoría o hacking seguridad en las aplicaciones, del mundo real, aprovechando la falla de los tres pilares de la seguridad la confidencialidad, integridad y disponibilidad de la información protegida.

**Dirigido a:** Alumnos de los grupos de Seguridad en los Sistemas de Información, Seguridad Informática, Seguridad en Tecnologías e Computación.

**Perfil del Proyecto**

Debido a la situación política en Panamá, se ha analizado la sede del PRD, vinculado con numerosos escándalos de corrupción.

El equipos de investigación de la FISC, ha encontrado el archivo [.OVA](https://nextcloud-jm-2307191555.s3-eu-west-1.amazonaws.com/VM/Ubuntu+Server+Hack.ova) metadatos arrojados por los ficheros ofimáticos de este partido político, se ha llegado a la conclusión de la existencia del usuario “tokio” dentro del sistema pero del que desconocen la contraseña de acceso. Se piensa que es posible acceder desde los servicios TCP que la máquina tiene activos.

Se sabe también, analizando el tráfico de red (se adjunto el archivo .pcap) de la formación política, que la dirección IPv4 es 1.0.0.1/24 y que soló permite conexiones TCP desde una dirección IPv4 de ese segmento de red, no desde ninguna otra.

Por indicios arrojados de las pruebas, se piensa en la existencia de una base de datos dentro de la máquina, con una tabla de información muy sensible.

El reto consiste en encontrar la tabla dentro de la base de datos para saber la información que almacena.

***El proyecto final incluye los siguientes:***

* Presentar en formato Microsoft Word
* Página de Presentación
* Marco teórico
* Bibliografías, Conclusiones
* Debe entregar el documento como un informe en formato pdf, con todas las pruebas realizadas, la configuración del proyecto y resultados obtenidos,
* Se entrega en formato digital.

Criterios de Evaluación:

Evidencia de trabajo en equipo: 30%  
Trabajo escrito: 10%  
Sustentación (pruebas y metodologías realizadas): 30%  
Contenido/Completitud: 30%