

## Preguntas y Respuestas

### Existe alguna entidad en panama que permita crear estos grupos en contra de los hacking?

No conozco ninguna entidad en Panamá de este tipo. Sin embargo, en Colombia existen comunidades de aprendizaje como hacklab y hackergirls. La OEA, también tiene grupos enfocados en seguridad informática que puedes consultar.

### Como banquero que no soy experto debo pagar a expertos para protegerme, pero como hago para no caer en la trampa de los expertos, ¿le pago a los hackers.?

Se debe pagar a los expertos y también adquirir las soluciones correctas. Sin embargo, para no caer en las trampas, se debe contar con buenos ingenieros (o hackers éticos) también al interior de tu organización, de manera que analicen las soluciones adecuadas para las necesidades específicas que se tienen, el mensaje es tener cuidado con soluciones que parecen perfectas (magia) pero tal vez no sean las adecuadas para los problemas que enfrenta tu banco en particular, entonces se cae en el error de invertir una gran cantidad de dinero que no genera los resultados esperados. Para esto es muy importante también tener en cuenta que la tecnología sola no agrega mucho valor, se debe contar con la persona adecuada detrás de esa herramienta que convierta los datos en información relevante y accionable para la toma de decisiones, esto además de los procesos adecuados.

### Nos puede mencionar Herramientas GPL que debemos considerar!

Control de acceso a la red - NAC: PacketFence  
Análisis de vulnerabilidades: OpenVas  
IDS/IPS: Snort, Suricata, Bro  
Monitoreo de infraestructura: Zabbix  
Correlación de logs-SIEM: SIEMonster, Alien Vault  
Respuesta a incidentes - IR: GRR

### Como se evalua el perfil de un hacker que quiere vulnerar sistemas bancarios?

Los ataques más importantes realizados en contra de entidades financieras son realizados por grupos organizados de hackers a nivel mundial, no necesariamente un hacker particularmente. El perfil de estas organizaciones cibercriminales se asocia con personas con gran conocimiento, herramientas fuente abierta, gran conocimiento del negocio e incluso insiders o empleados de las organizaciones que conocen claramente los procesos y las vulnerabilidades de las mismas.

### La seguridad es mas una percepcion que una realidad?

Podría decirse que si, ya que nunca estamos 100% seguros o podríamos estarlo hoy o en este instante pero en unos pocos minutos ya no: Todo el tiempo existen atacantes creando nuevos exploits o nuevas formas de vulnerar los sistemas. Por esta razón el mensaje presentado está enfocado en balancear las defensas con la capacidad de ataque, conociendo e imitando las características de los hackers.

### Conoce algunos web sites para capacitación en estos temas, que usted recomiende?

<https://www.infosecinstitute.com/>  
<https://www.cybrary.it>

Y en general en la red existen muchos recursos de información para aprender sobre temas de hacking desde lo más básico hasta lo más avanzado. Se puede tomar como guía las temáticas usadas para certificaciones reconocidas como CEH, Offensive security, etc.

## Preguntas y Respuestas

### What solutions can be found in the market that can help monitor and prevent cyber attacks?

TheFence: es una solución integrada por Aligo que consiste en una plataforma de seguridad integral que se ajusta a las necesidades específicas de las organizaciones y permite realizar monitoreo y prevenir siber ataques por medio de múltiples funcionalidades como:

- Análisis de Vulnerabilidades
- Inteligencia de Amenazas
- IDS/IPS
- DLP
- SIEM
- Captura y Análisis de tráfico

TheFence es una solución no licenciada y sin límite de usuarios que permite obtener múltiples beneficios de seguridad a elección de la organización (podría integrar una o varias de estas funcionalidades de forma centralizada y escalarlas gradualmente a múltiples sedes administrativas y sucursales)