Ejército Argentino
Escuela Superior Técnica

Curso "**Formación en Ciberdefensa"**

Del 4 al 8 de septiembre

Dirigido a personal gerencial o administradores de SSII y redes, con conocimientos de Redes y TI

Las clases se dictarán durante una semana intensiva de lunes a viernes en el horario de 18:00 a 22:00 horas. Se utilizarán para concurrir al Laboratorio para efectuar las prácticas técnicas y trabajos experimentales.

Se desarrollaran trabajos prácticos sobre todos los temas teóricos de la currícula del curso.

ESTRUCTURA CURRICULAR:

Bloque I (Ciberseguridad)

a. Presentación, conceptos y situación de Ciberseguridad. ¿De quién nos defendemos?
b. Estrategias de Ciberseguridad en grandes redes (Seguir y perseguir - proteger y proceder).
c. Ciberdefensa en profundidad y en altura (la conquista de las cumbres).
d. Ciberseguridad: La importancia de los procesos.
e. Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red.
f. Ciberseguridad: Cómo son las entrañas de esta gran red mundial.
g. Ciberseguridad: empleo de SOC y NOC.
h. Ciberseguridad: la importancia de saber gestionar "Logs".

Bloque II (Organización de la Seguridad)

a. Organización de la Seguridad (Gobierno, Planificación y Operación).
b. Procesos:
- Creación de planta.
- Gestión de accesos.
- Gestión de cambios.
- Gestión de Logs.
- Gestión de Backups.
- Gestión de configuración / inventario.
- Gestión de Incidencias.

c. Seguridad en centrales o CPDs
- Ubicaciones.

- Seguridad en los accesos físicos al edificio.
- Control medioambiental.
- Seguridad interna de salas.
- Seguridad en los Racks de comunicaciones.
- Control de energía.

Bloque III (Seguridad en Redes)

a. Qué son las redes de gestión y servicio.
b. Plataformas de autenticación.
c. Plataformas de de control de acceso.
d. Plataformas de Centralización y correlación de Logs.
e. Empleo de máquinas de salto.
f. Switchs.
g. Routers.
h. Firewalls.
i. Auditoría de Redes.

Bloque IV (Prácticas)

a. Empleo de máquina virtual.
b. Empleo de Sistema Operativo Linux con la distribución “Kali”.
c. Herramientas de análisis de tráfico.
d. Herramientas de captura.
e. Herramientas de análisis de red.
f. Herramientas de análisis configuración de switchs y routers.
g. Planteo de diferentes casos de estudio
- Análisis práctico empleando lo desarrollado.
- Presentación de lo analizado por los participantes.

h. Empleo de túneles SSH (redirección de puertos).
i. Metodologías de análisis de protocolos inseguros.
j. Breves ideas y ejercicios de programación en bash.
k. Análisis de cuentas de usuario y fortaleza de contraseñas.