GENERALITAT VALENCIANA
CONSELLERIA D'EDUCACIÓ, INVESTIGACIÓ, CULTURA I ESPORT

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURDAD

IES SAN VICENTE

MODULOS PROFESIONALES – CIBERSEGURIDAD – 720H TOTALES

- Normativa de ciberseguridad. → 1h semanales
- Puesta en producción segura. → 4h semanales
- Hacking ético. → 4h semanales
- Bastionado de redes y sistemas. → 7h semanales
- Incidentes de ciberseguridad. → 4h semanales
- Análisis forense informático. → 4h semanales

¿QUÉ SE ESTUDIA? - NORMATIVA DE CIBERSEGURIDAD.

- Cumplimiento normativo. ¿Es legal hacer un nmap?
- Responsabilidad penal
- RGPD
- ISO 270001
- Ley PIC (Protección de infrastructuras críticas)

¿QUÉ SE ESTUDIA? - PUESTA EN PRODUCCIÓN SEGURA

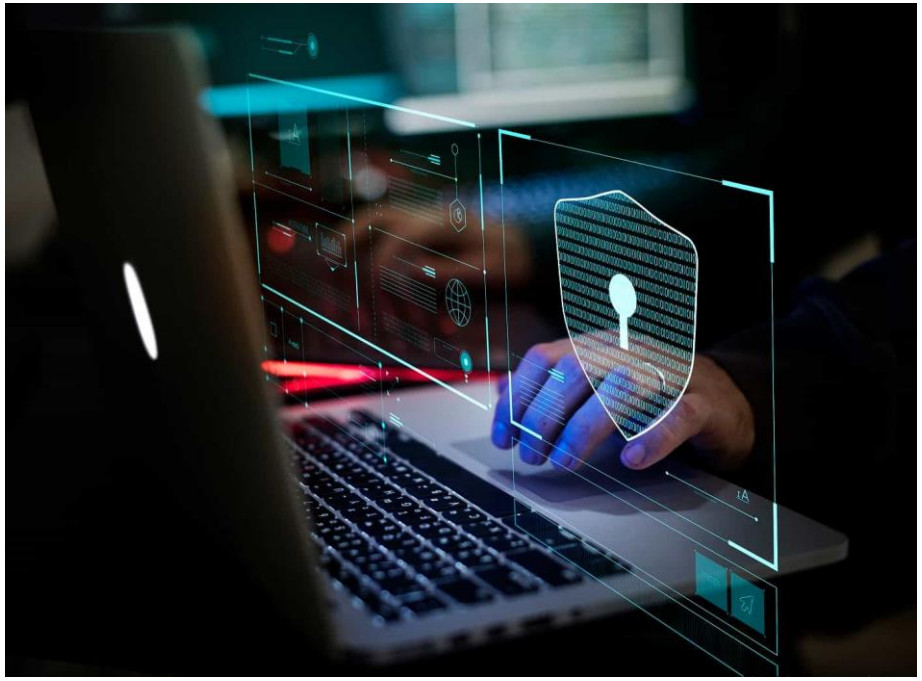
- Fundamentos del desarrollo de aplicaciones web
- Seguridad, autenticación y validación de datos en el servidor
- Desarrollo y seguridad de aplicaciones móviles
- Despliegue de aplicaciones web
- AWS y Azure
- Dockers, Docker-compose y Kubernetes

¿QUÉ SE ESTUDIA? - HACKING ÉTICO

- Privacidad y anonimato en Internet. VPNs, TOR, Proxy-Chains
- Recopilación pasiva: footprinting. OSINT, Maltego, FOCA
- Recopilación activa: fingerprinting. CVE, CVSS, Nmap
- Análisis de vulnerabilidades. Nessus
- Explotación de vulnerabilidades en hosts. MetaSploit, Payloads, Reverse Shells
- Explotación de vulnerabilidades Web. SQL Injection, XSS
- Explotación de vulnerabilidades en redes. Wifi cracking, Bettercap, ARP y DNS spoofing
- Técnicas Post-Explotación. Meterpreter, elevación de privilegios, pivotar, borrado de evidencias. Hashcat. Mimikatz

¿QUÉ SE ESTUDIA? - BASTIONADO DE REDES Y SISTEMAS

- Planes de securización.
- Firewalls
- Proxys
- IDS. Suricata y Snort
- VLANs



¿QUÉ SE ESTUDIA? - INCIDENTES DE CIBERSEGURIDAD.

- SOCs. Blue Team + Red Team + Purple Team
- Detección de Incidentes. SIEMs, Sysmon, ELK (Elastic Logstash Kibana)

- IOCs
- Análisis de incidentes. PrintNightmare, rgsvr32, ransomware.
- Respuesta a incidentes. Contención y recuperación
- Documentación del incidente para que no vuelva a ocurrir

¿QUÉ SE ESTUDIA? - ANÁLISIS FORENSE INFORMÁTICO.

- Analisis y recuperación de pruebas sobre delitos informáticos en los siguientes sistemas:
  - Windows.
  - Android e IOS.
  - Linux e IOT.
  - Cloud.

- Elaboración de informes informáticos periciales válidos en procesos judiciales.

EVALUACIÓN DE LOS MÓDULOS

- La evaluación de ciberseguridad, en general, va a tener un carácter principalmente **práctico**
- Hay **2 evaluaciones**: A finales de Enero y a finales de Mayo, aproximadamente.
- **No hay recuperación en julio o septiembre.**
- Las propias recuperaciones, se harán durante el curso.

ASISTENCIA

- La asistencia es obligatoria.
- Flexibilidad de asistencia.
- Justificantes de trabajo.

SALIDAS PROFESIONALES

- Forense informático
- Hackers éticos y asesor de Seguridad
- Consultor de Seguridad Informática.
- Administrador de Seguridad de Red.

Información de contacto

Para más información del curso de CiberSeguridad podéis contactar con Alvaro Pérez (Tutor del Curso) a través de Linkedin:

https://www.linkedin.com/in/alvaroies/