LA PROFESIONAL ESPECIALIZADA DE TALENTO HUMANO
DE LA ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL

CERTIFICA:

Que de conformidad con lo establecido en el Artículo 21 de la Ley 1150 del 16 de Julio de 2007, el artículo 3° del decreto 1737 de 1998 modificado por el artículo 1° del decreto 2209 de 1998, hace constar que no existe personal suficiente en la planta global de la Escuela Tecnológica Instituto Técnico Central con funciones específicas relacionadas con:

OBJETO: "PRESTACIÓN DE SERVICIOS PROFESIONALES COMO PERSONA NATURAL PARA REALIZAR EL ANÁLISIS DE VULNERABILIDADES A LOS SISTEMAS DE INFORMACIÓN DE LA ESCUELA TECNOLOGICA INSTITUTO TECNICO CENTRAL Y SUS SEDES."

El contratista se compromete a cumplir con las siguientes Obligaciones Específicas:

1. El contratista deberá realizar Plan de Trabajo en conjunto del supervisor encargado.
2. El contratista deberá realizar el Acta de inicio del presente contrato en conjunto con el supervisor encargado.
3. El contratista deberá cumplir con las obligaciones y actividades mencionadas a continuación:

Servicio de análisis de vulnerabilidades.

- Detección de vulnerabilidades de las direcciones IP y de las URLs, identificando el nivel de exposición y criticidad teniendo como referencia la lista CVE, CWE, OWASP entre otros marcos de referencia
- Escaneo de vulnerabilidades (identificar puntos débiles o malas implementaciones que puedan ser aprovechadas por un ciberdelincuente y realizar ataques informáticos hacia la ETITC)
- Realizar análisis de caja negra ejecutando de actividades a través de herramientas OpenSource y especializadas en auditorías de seguridad utilizando las mejores prácticas de organismos internacionales EC-Council y a nivel de aplicaciones Web, se tomará como referencia el marco de pruebas top 10 de OWASP (Open Web Application Security Project).
- Recolección de información y enumeración (rastrear los elementos de red como lo son servidores, switch, entre otros)

- Análisis de la información recabada (nivel crítico de los dispositivos o servicios, análisis de riesgo de los dispositivos o servicios, recomendaciones a seguir, sellos de confianza en las aplicaciones cuando se requiera)
- Pruebas adicionales a sugerencia

Servicio de asistencia técnica para mitigación de vulnerabilidades usando técnicas de pentesting.

- La asistencia técnica deberá realizarse en las instalaciones de la ETITC
- La asistencia técnica se desarrollara en los siguientes aspectos: Técnica y Disciplina Reconocimiento, OSINT, Búsquedas Avanzadas, Scripts, Herramientas Avanzadas, Toma de Huellas de Sistema, Ingeniería Social, Rastreo, Análisis de Puertos, Enumeración, Detección, Selección, Ruptura de Contraseñas, MitM, Ataques DNS, Explotación, Buffer Overflow, iNOPS, Ejecución Remota, Análisis de Vulnerabilidades, Fallos en Configuración, Malware, Virus, Troyanos, Gusanos, Ejecución de Scripts Automáticos, Ofuscación, Proxy, Tunneling, VPN, I2P, DoS, DDoS, Ataques a nivel de WEB, SQLi, XSS, Parameter Tamperin, Ruptura WEP, WPA – WPA2 - WPS
- La asistencia técnica deberá constituirse por una bolsa de al menos 24 horas.
- Por el nivel de complejidad de la actividad la empresa deberá respaldar las competencias de los ingenieros con al menos las siguientes certificaciones: CISSP, CEH, ECSA, ENSA, CHFI, LPT, CSSA, ECSS, CEI, ECVP, CQGSS, Auditor ISO 27001, Auditor ISO 22301, ABCP, CCSK.

4. Ejecución de las actividades se deberá desarrollar por las siguientes etapas:
   - **Obtención de información:** Fase preparatoria donde el consultor obtiene toda la información necesaria para crear una estrategia para el ataque (ataque pasivo)
   - **Enumeración**: fase que el consultor utiliza toda la información que obtuvo en la Fase de obtención de información para identificar vulnerabilidades específicas. Posterior realizará un ataque activo donde se involucra.
     - Descubrimiento de puertos (TCP y UDP)
     - Detección de conexiones
     - Detección de Servicios

5. El contratista una vez realizado las anteriores actividades deber presentar los siguientes entregables:
   - **Informe externo:** Consolidación de evidencias para la generación de informe con su correspondiente metodología análisis de vulnerabilidades externo de Black Box que contenga conclusiones y plan de remediación de los hallazgos encontrados a nuestros objetivos críticos de base de datos, servicios, y sitio web institucional.
   - **Informe interno:** Consolidación análisis de vulnerabilidades interno de Black Box a la red WLAN de la sede principal que contenga conclusiones y plan de remediación de los hallazgos encontrados.

- **Entrega de equipamiento físico de tecnología**: referencia equipo laptop similar a estás especificaciones para el desarrollo de actividades con un equipo laptop similar o superior a las siguientes características:

GIGABYTE G5KE/i5 12500H+16G(2x8)3200+NVMe512+6G RTX3060+15,6"144Hz+FREE+RGB
Windows 11 Home (Incluido máquinas virtuales de KALI LINUX)
NVIDIA® GeForce RTX™ 30 Series Laptop GPUs
12th Gen Intel® Core™ i5 H-Series Processor
WINDFORCE Cooling System
15.6”FHD 144Hz Display
Supports PCIe Gen 4 SSD
DTS: X™ Ultra Audio Technology
Thunderbolt™ 4
https://www.gigabyte.com/Laptop/G5--Intel-12th-Gen#kf

Se expide la presente certificación a los 2 días del mes de agosto de 2023, de acuerdo con solicitud realizada por la Vicerrectoría Administrativa y el área Jurídica de Contratación.

LUCIBETH BLANCHAR MAESTRE
Profesional Especializado de Talento Humano
Escuela Tecnológica Instituto Técnico Central

Revisó: Lucibeth Blanchar – Profesional Especializado de Talento Humano
Elaboró: Eliana Garzón – Técnico Administrativo de Gestión de Talento Humano

∗ Certificado con firma digital autorizada.