TÉRMINOS Y CONDICIONES
Bootcamp Hacker Girls Barranquilla

Hacker Girls es una iniciativa que tiene como fin apoyar y generar espacios de educación y oportunidad laboral para las mujeres, basados en el fortalecimiento de sus conocimientos en áreas asociadas a la ciberseguridad ética y la equidad de género.

El Bootcamp que se realizará en Barranquilla está orientado a mujeres técnicas e ingenieras con conocimientos en ciberseguridad, y tendrá una jornada de dos días con una intensidad horaria de 20 horas, donde ampliarán sus conocimientos en hacking ético, cloud computing, seguridad de la información, liderazgo femenino, análisis forense, técnicas de hacking utilizadas por los ciberdelincuentes y laboratorio de hacking.

Estos son conocimientos necesarios para generar capacidades que permitan contrarrestar cualquier vector de ataque contra sistemas informáticos de instituciones o empresas.

Se espera que este programa sea el punto de partida para el primer grupo “Hacker Girls” de la región Caribe, que a futuro será la Selección Femenina de Hackers Colombianas, quienes tendrían un protagonismo y liderazgo relevante en esta materia.

QUIÉNES PARTICIPAN

50 estudiantes o profesionales de carreras afines con Ingenierías de Sistemas/Electrónica/Telecomunicaciones, que obtuvieron la mejor calificación en la prueba técnica, seleccionadas de 95 inscritas en la convocatoria realizada con el apoyo de universidades y clusters de la región.

ALCANCE TÉCNICO

Primer Bootcamp Hacker Girls Barranquilla, se realizará bajo las siguientes características:

- ✓ **Tipo de actividad:** Presencial.
- ✓ **Modalidad:** Ejercicios Teórico-prácticos
- ✓ **Intensidad:** 20 horas, en dos días intensivos de entrenamiento 27 y 28 de **abril** de 2018.
- ✓ **Número de participantes:** Hasta 50 participantes locales.

PROGRAMA ACADÉMICO

1. HACKERGIRLS

- Por qué ser una HackerGirl.
- Algunas cifras que demuestran la necesidad de HackerGirls.
- Habilidades Blandas requeridas por una HackerGirls.

2. INTRODUCCION AL CURSO

Experiencias y recomendaciones contadas por Mujeres en los diferentes campos de la ciberseguridad:

- Auditoria
- Analista Forense
- Analista de Malware
- Hardening de sistemas (Servidores, Redes, DB, Web)
- Desarrollo seguro
- CISO
- Sistemas de Gestión de seguridad"
- Overview general

CODIGO DE ETICA Y COMPROMISO PROFESIONAL

3. INTRODUCCION AL ETHICAL HACKING

- Ética y cuestiones legales
- Black Hat Hackers
- White Hat Hackers
- Ventajas de contratar este tipo de servicios

- No divulgación de datos
- Aceptación de pruebas sobre los sistemas
- Black Box Penetration Test
- Gray Box Penetration Test
- White Box Penetration Test
- Etapas de un Penetration Test

4. CONFIGURANDO EL LABORATORIO

Descripción del laboratorio y software requerido:

- Instalación de Kali linux como máquina virtual
- Instalación de Metasploitable como máquina virtual
- Instalación de Windows como máquina virtual
- Creación de snapshots
- Laboratorio

5. LINUX BASICO: Introducción a Kali Linux

- La terminal y los comandos de Linux
- Actualización de fuentes e instalación de programas
- Laboratorio Linux

6. INTRODUCCION A REDES: Modelo OSI

- TCP/IP
- Arquitectura de red
- Dispositivos de interconexión
- Tecnología de ethernet
- Protocolo ARP
- Laboratorio Redes

7. INFORMATION GATHERING

Introducción reconocimiento

- Search engines
- Google Hacking
- Maltego
- Reconocimiento Web
- Reconocimiento email
- Técnicas de inteligencia competitiva

- Reconocimiento WHOIS
- Reconocimiento DNS
- Reconocimiento de red
- Reconocimiento vía ingeniería social
- Herramientas
- Reconocimiento pentesting
- Laboratorio Information Gathering

8. ESCANEO

Comprobación de existencia de sistemas

- Técnicas de escaneo
- Técnicas de evasión
- Mapeo de Sistemas Activos
- Mapeo de Puertos TCP/UDP
- Mapeo de Sistemas Operativos
- Mapeo de Versiones de Software
- Banner Grabbing
- Rastreo de eMails
- Enumeración
- Laboratorio de escaneo

9. ESCANEO DE VULNERABILIDADES

Introducción al escaneo de vulnerabilidades

- Funcionamiento de escaneo de vulnerabilidades
- OpenVas
- Nessus
- Nikto
- NSE nmap
- Acunetix
- Otras herramientas
- Laboratorio de vulnerabilidades

10. EXPLOTACIÓN

- Ataques lado servidor
- Arquitectura de Metasploit
- Módulos
- msfconsole / msfcli / msfgui / msfweb
- Meterpreter

- El Framework Dradis
- Plugins Auxiliares
- Análisis de Vulnerabilidades
- Verificación de Login SMB
- Autentificación VNC
- Ejecución de Exploits
- Msfvenom / Msfpayload / Msfrop
- Egghunter-Mixin
- Escalada de Privilegios
- Pivoting
- Scripting en Meterpreter
- Keylogging
- Meterpreter “Backdoor”
- Ataques del lado cliente
- Buffer Overflows
- Laboratorio de Explotacion

11. POST EXPLOTACIÓN

Introducción POST-Explotación

- Backdoors
- CookieBackdoor
- Not Found
- Rootkits
- Laboratorio Post-Explotación

12. PENTESTING WEB (Introducción)

- Information Gathering
- Sql injetions
- XSS
- Sesión Hijacking
- Shellcodes
- Laboratorio Pentesting Web

13. PENTESTING WIFI (Modos inalámbricos)

- Habilitación de modo monitor
- Utilización de airodump-ng
- Ataque de autenticación
- Creación de access points fake (Honeypot)

- Métodos de acceso WEP/WPA
- Laboratorio Pentesting Wifi

14. ATAQUES DE INGENIERIA SOCIAL (Introducción a la ingeniería social)

- Ingeniería social en practica
- Email spoofing
- Social Network Spoofing
- Set tool
- Laboratorio ingeniería social

15. PROYECTO REAL DE PENTESTING (Planeamiento)

- Alcance del proyecto
- Etapas posibles
- Ejecución
- Reunión inicial
- Personal involucrado
- Gestión de las expectativas y Gestión de los problemas
- Reportes técnico y gerencial
- Elaboración de los documentos
- Seguimiento
- Reuniones post proyecto
- Selección de contramedidas
- Implementación de contramedidas

16. CONCLUSIONES Y CIERRE OFICIAL

MODO DE EVALUACIÓN

La evaluación se realizará con una puntuación sobre 100 puntos y se debe obtener mínimo el 80% para obtener la certificación.

Se distribuirá de la siguiente manera:

- A lo largo del curso se realizarán ejercicios teórico-prácticos, con una puntuación de 30 puntos.
- Asistencia mínima de 18 horas con una puntuación de 20 puntos.
- El CTF se realizará el ultimo día y tiene un puntaje de 50 puntos para obtener el 100% total de la calificación.

CERTIFICACIÓN

Se entregará un certificado de asistencia con una duración de 20 horas cursadas en el Bootcamp Hacker Girls.