TÉRMINOS Y CONDICIONES
Entrenamiento HackerGirls Team Colombia

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.

Para ello, se ha diseñado un programa de entrenamiento que parte del uso de herramientas de hacking, metodologías y técnicas que amplían las competencias de las 'Hackers Girls', desde el conocimiento y la habilidad. El propósito, es que las participantes puedan ser entrenadas para mejorar sus capacidades en pruebas tipo Capture The Flag-CTF y en labores de Hacking ético. Estos son conocimientos necesarios para generar capacidades que permitan contrarrestar cualquier vector de ataque contra sistemas informáticos de instituciones o empresas.

Este programa de entrenamiento se plantea como una inmersión de 60 horas con un entrenamiento de alto rendimiento, que estará bajo la conducción de un equipo de tres Hackers internacionales permitiendo obtener un grupo calificado de mujeres hacker de primer nivel y constituyendo a Colombia como pionero en este perfil de Hacker Girls Team.

Se espera que este programa sea el punto de partida para el grupo que constituiría las "Colombian Hacker Girls Team", que a futuro será la Selección Femenina de Hackers Colombianas, que tendrían un protagonismo y liderazgo relevante en esta materia.

QUIÉNES PARTICIPAN

20 estudiantes o profesionales de carreras afines con Ingenierías de Sistemas/Electrónica/Telecomunicaciones, quienes hicieron parte del primer grupo de las 50 mujeres HackerGirls, que participaron en un espacio de formación bajo la metodología participativa y práctica, a través de un workshop en "Ethical hacking", realizado en septiembre del 2017 en Colombia 4.0. Estas estudiantes o profesionales obtuvieron la mejor calificación y el mejor desempeño e interés en este ejercicio.

ALCANCE TÉCNICO

El entrenamiento del Hacker Girls Team Colombia se realizará bajo las siguientes características:

- ✓ **Tipo de actividad:** Presencial.
- ✓ **Modalidad:** Talleres de trabajo y entrenamiento.
- ✓ **Intensidad:** 60 horas, en dos semanas intensivas de entrenamiento del **2 a 14 de abril** de 2018.
- ✓ **Número de participantes:** Hasta 20 participantes locales.
- ✓ **Contenidos:** CYBER-WARFARE para las COLOMBIAN HACKER GIRLS TEAM

PROGRAMA ACADÉMICO

Temario Curso: Hacking e intrusión no autorizada a sistemas informáticos y redes de ordenadores

MÓDULO: HACKING E INTRUSIÓN A SISTEMAS INFORMÁTICOS Y REDES DE ORDENADORES.

Duración 60 horas

Ítem 1. CONCEPTOS IMPRESCINDIBLES Y EL PROTOCOLO TCP/IP

- Capas de red.
- Dirección IP.
- Mascara de subred.
- Protocolos IP, ICMP.
- Encaminamiento.
- Protocolo UDP, Protocolo TCP.
- Puertos y dominios.
- Sitios Web indispensables para trabajar en inseguridad informática.
- Sitios Web indispensables para trabajar en seguridad informática.

Ítem 2. TÉCNICAS DE RASTREOS Y EXPLORACIÓN

- ¿Qué es seguir el rastro a una organización?
- Seguir el rastro en Internet.
- Determinación del ámbito de actividades de la víctima (empresa).
- Enumeración de la red.
- Interrogaciones DNS.
- Reconocimiento de la red y su topología previo al ataque.
- Obtención de información en la red con Maltego.
- Interpretación de resultados y fisuras.
- Técnicas de gathering information
- Contramedidas a adoptar ante las fisuras.
- *DESAFIOS PRÁCTICOS*.

Ítem 3. EXPLORACIÓN DEL OBJETIVO

- Consultas ICMP.
- Exploración de puertos.
- Tipos de escaneos a realizar sobre el objetivo.
- Evasión de dispositivos de filtrado y detección de port scanning.
- Detección del sistema operativo, versiones y servicios en ejecución.
- Ejercicios prácticos y de análisis.
- Interpretación de resultados y fisuras.
- Medidas a adoptar ante las fisuras.
- Herramientas automáticas de descubrimiento y contramedidas.
- *DESAFIOS PRÁCTICOS*

Ítem 4. METODOLOGÍA DE LA INTRUSIÓN: TÉCNICAS DE HACKING CONTRA LOS SISTEMAS

- Firewalls y routers.
- Técnicas de firewalking (atravesar cortafuegos).
- Cómo los intrusos se hacen invisibles en Internet (el anonimato en la operación).
- Métodos para engañar a los ficheros .log en la ofensiva.
- Técnicas de suplantación de IP atacantes en Internet (looping spoffing ip)
- Obtención de exploits
- Ataques distribuidos desde Internet.
- Establecimiento de puertas traseras (backdoors).
- Metodología para la detección de puertas traseras.

- Entrando en los sistemas: enumeración y la escalada de privilegios.
- Métodos de descarga de herramientas de prospección en el sistema comprometido
- Anulando la efectividad de los antivirus (generación de herramientas indetectables)
- Cómo se recaba información una vez en los sistemas.
- Medidas de seguridad a implementar.
- Alteración, falsificación e intoxicación de ficheros .log.
- *DESAFIOS PRÁCTICOS*

Ítem 5. DETECCIÓN DE VULNERABILIDADES Y PENETRATIONS TEST

- Introducción.
- Vulnerabilidades básicas tras la instalación del sistema.
- Vulnerabilidades en los servicios del sistema.
- Uso de los scaneadores de vulnerabilidades (vulnerability scanners: Nessus, Retina).
- Configuración de las plantillas de auditoria.
- Práctica realización de auditorías sobre sistemas internos.
- Práctica realización de auditorías sobre sistemas cara a Internet.
- Herramientas para test de penetración (Metasploit framework).
- *DESAFIOS PRÁCTICOS*.

Ítem 6. AUDITORÍA SOBRE POLÍTICAS DE USUARIOS Y CONTRASEÑAS

- Análisis del problema en la organización.
- Métodos de descifrado y ruptura de contraseñas.
- Herramientas para la auditoria de contraseñas.
- Herramientas para ruptura de contraseñas y métodos de cracking de contraseñas.
- Implementación de políticas confiables.
- *DESAFIOS PRÁCTICOS*.

Ítem 7 INTRODUCCIÓN A INYECCIÓN DE CÓDIGO SQL Y VULNERABILIDADES EN SITIOS WEB

- Introducción a TSQL
- Aprendiendo SQL orientado a la inyección de código.
- Entendiendo porque la aplicación es vulnerable a la inyección de código.
- Localización y análisis de la fisura.
- Explotación del bug.
- Inyecciones de código básicas.
- Analizando y comprendiendo inyecciones avanzadas.
- Recomendaciones a seguir para minimizar riesgos.
- Introducción a técnicas XSS.
- *DESAFIOS PRÁCTICOS de inyección SQL.*
- Herramientas de auditoría y detección de vulnerabilidades de inyección de código.
- Herramientas para inyectar sentencias SQL
- Prácticas con las herramientas e interpretación de resultados.
- Trabajos sobre aplicaciones vulnerables.
- *DESAFIOS PRÁCTICOS.*

Ítem 8 ANÁLISIS FORENSE INFORMÁTICO

- Aprendiendo sobre el problema forense sobre dispositivos comprometidos.
- Estructura de sistemas de ficheros.
- La recuperación de datos en los dispositivos.
- Herramientas de recuperación y análisis.
- Búsqueda de evidencias, sustracción de las pruebas.
- Forensica en redes.
- Monitorización y análisis de tráfico legitimo e ilegitimo.
- Análisis de procesos sospechosos.
- *DESAFIOS PRÁCTICOS.*

Ítem 9 SISTEMAS SIEM Y MONITORIZACIÓN DE EVENTOS/LOGS

- ¿Qué es un SIEM?
- La importancia de sistemas SIEM en CSIRTS y CERTS.
- La plataforma de monitoreo y su configuración.
- Las fuentes de eventos y conectores.
- Enganchando fuentes de eventos a ser monitorizadas.

- El registro consolidado de logs de distintas fuentes.
- Reglas y políticas de ciberseguridad para detectar patrones de ataque.
- Reconstrucción de ataques sobres sistemas bajo monitoreo.
- Análisis de la incidencia (tipo de ataque, tiempo, lugar, servicio).
- Trazabilidad de los logs recopilados en la fuente.
- Trazabilidad y alcance del compromiso.
- *CASOS PRÁCTICOS.*

Ítem 10 SEGURIDAD EN REDES WIFI

- Parámetros de estudio, Estructura y Topología de redes inalámbrica.
- Cobertura, Alcance, Propagación, Interferencia, ganancia.
- Banda de uso civil. Canales. Potencia de transmisión.
- Sistemas de codificación.
- Canales disponibles de uso sin solapamiento.
- Legalidad e ilegalidad.
- Implementación y cobertura.
- BSSID, ESSID, Células, IBSS.

Equipos inalámbricos Wifi a utilizar en auditorías de redes inalámbricas

- NIC, Adaptadores (tipos según interface, chipsets, amplificación).
- Equipos todo en uno, Adaptador o Router monopuesto, Hotspots.
- Antenas direccionales, medida, polarización.
- Amplificadores, Cables, Conectores, Adaptadores y Pigtails. Adaptadores PoE.
- Routers avanzados y su configuración de seguridad.
- Contramedidas a adoptar ante las fisuras inicialmente detectadas.
- *CASOS PRÁCTICOS.*

Ítem 11 HACKING A REDES WIFI

Realización de rastreos sobre las posibles víctimas

- Utilizando equipos de medida y diagnóstico.
- Medidores de potencia.
- Inhibidores de frecuencia.
- Correcta configuración de las tarjetas inalámbrica a utilizar en el ataque.
- Utilizaron de los scanners e interpretación de resultados.
- Autenticación y Asociación.

- El tipo de encriptación de canal un factor determinante en el momento del ataque.

Fase de ataque

- Objetivo fijado, estudio pasivo del objetivo.
- Búsqueda de la mejor situación de cobertura, estudio de la señal.
- Estudio activo de la infraestructura (APS, clientes, SSIDs, MACs, Encriptación, Marcas, Canales, Relación entre equipos, velocidades de trabajo, autenticación, Rangos IP).
- Tipos de ataques a realizar.
- Elección del mejor ataque.
- Realización del ataque. Ruptura de la seguridad.
- Conectándonos a red comprometida. Dentro de la red.
- *CASOS PRÁCTICOS*

HERRAMIENTAS DE CONTRAMEDIDAS Y HACKING QUE SE UTILIZAN DURANTE EL CURSO

- Versión de sistema para auditorías informáticas y pentest Kali Linux 2017.02
- Herramientas de exploración.
- Herramientas de enumeración.
- Herramientas de footprinting (rastreado).
- Herramientas para conseguir accesos.
- Herramientas de penetración y puertas traseras, Ocultación de huellas.
- Herramientas de auditoría de redes y ordenadores.

MÓDULO 2: DESARROLLO DE DESAFÍOS DE HACKING PASO A PASO - DESAFÍOS DE COMPETICIONES CTF (CAPTURE THE FLAG)

- Se desarrollarán juegos de guerra desde el inicio de la operación hasta su fin, con objetivos de logros de información en distintos escenarios.

- Se realizarán pruebas de competición en plataforma CTF para manejo de estrés, resolución de desafíos y desarrollo de las competencias en equipo. Estos ejercicios se basan en pruebas de hacking utilizadas en todas las competiciones de hackers en lo que se denominan CTF (Competiciones Capture The Flag).

MODO DE EVALUACIÓN

La evaluación se realizará con una puntuación sobre 100 puntos, y se debe obtener mínimo el 70% para obtener la certificación.

Se distribuirá de la siguiente manera:

- ✓ A lo largo del curso se realizarán 8 ejercicios teórico-prácticos, cada uno con una puntuación de 10 puntos.
- ✓ El CTF se realizará el ultimo día y tiene un puntaje de 20 putos para obtener el 100% total de la calificación.

CERTIFICACIÓN

Además de aprobar como mínimo el 70% en la calificación, es necesario que las estudiantes realicen seis (6) horas de actividades como charlas y talleres de sensibilización en temas relacionados con recomendaciones del buen uso de internet, a entidades privadas y públicas, se deben enviar videos y listas de asistencia como evidencia de esta actividad al correo dmontanez@mintic.gov.co Para esta actividad se tiene tres semanas a partir de la fecha de terminación del entrenamiento.

Una vez cumplido con lo anterior se recibirá una certificación de conocimiento y habilidades en Seguridad Digital, con una duración de 60 horas cursadas, al mes de terminada esta actividad.