Dirigido a:

Todos los cursos previos al DurivaCON están orientado a profesionales de informática, estudiantes o entusiastas que desean aprender de la mano de expertos distintas herramientas de hacking, ciberseguridad y hardering.

Para aprovechar el curso es importante contar con conocimientos básicos de redes y sistemas operativos.

Objetivo:

Al finalizar el curso los alumnos tendrán los conocimientos generales necesarios para poder llevar desde auditorías informáticas, creación de exploits, así como pruebas de pentesting o implementación de seguridad a redes empresariales.

Los talleres son 100% prácticos, por lo que habrá mucho tiempo para enfocarse en prácticas con ambientes reales.

Ventaja competitiva

Nunca antes en México se había juntado para un congreso y para la impartición de los mismos talleres tanto talento de expertos en seguridad que cuentas con certificaciones internacionales que avalan su nivel profesional.

Adquiere las habilidades que el mundo está buscando

Requerimientos de equipo de cómputo:

- 10 Gb de espacio en disco duro
- 4 GB en RAM
- Procesador Intel i3 o superior

Precios: Los costos de los talleres dependen de la duración, en todos los casos ya incluye el acceso al DurivaCON 2018 y playera de participación.

Duración del taller	Inversión
1 día (24 agosto)	$2,800
2 días (23 y 24 agosto)	$4,600
3 días (22, 23 y 24 agosto)	$6,300

Facilidades: Internet, conexiones eléctricas y servicio de coffe break incluido.

Horario: Todos los talleres tienen el mismo horario por día, de 09:00 – 18:00 horas.

Talleres:

Nombre del taller	Días
Introducción a Cobalt Strike	1 día
Web Penetration Testing	2 días
Ensamblador, reversa y desarrollo de exploits para Linux	2 días
Hacking Data Network and hardering	3 días

Taller de 1 día

Introducción a Cobalt Strike (Gonzalo Sánchez – RedTech)

Temario:

Introducción a Cobalt Strike

- Estructura de Cobalt Strike
- Conociendo Cobalt Strike
- El primer Listener

Recolección de información

- Descubrimiento e identificación de puertos y servicios
- Personalizando un escaneo

Análisis de vulnerabilidades

- Análisis de vulnerabilidades con nmap
- Importando escaneos con Nessus

Obteniendo el acceso

- Explotación de vulnerabilidades en sistema operativo
  - Windows
  - Linux
- Explotación de vulnerabilidades en aplicaciones
  - JAVA-RMI
  - MYSQL
  - POSTGRESQL
  - VNC
  - IRC
  - TOMCAT
- Explotación de vulnerabilidades en servicios
  - SMB
  - Servicios “r”
  - NFS (Network File System)

Ingeniería social

- Ejecutables maliciosos
- USB auto ejecutable
- Generando acceso por medio de macros en Excel

Post explotación (60 minutos)

- Elevar privilegios
- Persistencia
- Obtención de información del sistema operativo
- Obtención de información de las aplicaciones
- Obtención de información en servicios
- Obtención de información de hardware
- Obtención de passwords y cracking
- Generando scripts propios
- Pivoteo

Taller de 2 días

Web Penetration Testing – Rafael Bucio (ponente del congreso)

Temario:

Día 01 + TEORICO

1. Introducción y recopilación de información ▸ Vista general de la web desde la perspectiva de Web Pentester ▸ Explorando los diferentes servidores y clientes ▸ Discusión de los diferentes tipos de vulnerabilidades y su medición. ▸ Definición de un alcance y proceso de prueba de aplicación web ▸ Definición y metodologías de pruebas de penetración ▸ Definición del uso de proxy en un pentest ▸ Tipos de reportes

2. Recolección de información e identidad ▸ Descubriendo la infraestructura dentro de la aplicación ▸ Identificación de las máquinas y sistemas operativos ▸ Métodos de aprendizaje para identificar nodos ▸ Descubrimiento de configuración de software ▸ Explorando fuentes de información externas ▸ definición de un spider hacia web. ▸ Introducción a shell scripting enfocado a auditorias web. ▸ Creación de secuencias de comandos para automatizar las solicitudes web y spidering.

Día 02 + PRACTICO

3. Inyección. ▸ Vulnerabilidades de aplicaciones web y técnicas de verificación manual ▸ Proxies de intercepción (Burp Suite) ▸ Fuga de información y exploración de directorios ▸ Recolección del Usuarios. ▸ Inyección de comando. ▸ path traversal ▸ Inclusión de archivos locales (LFI) ▸ Inclusión remota de archivos (RFI) ▸ inyección SQL ▸ Inyección SQL a ciegas ▸ Automatización en inyecciones sql ▸ JavaScript para el atacante

4. JavaScript y XSS ▸ Vectores de ataques en XSS ▸ Session flaws ▸ Session fixation ▸ Comparación de XML y JSON en vectores de ataque. ▸ Ataques de lógica ▸ Herramientas de automatización de aplicaciones web. 5. CSRF and Logic Flaws ▸ Metasploit para Web Pentesters ▸ Aprovechando los ataques para obtener acceso al sistema ▸ Cómo pivotar nuestros ataques a través de una aplicación web ▸ Comprender los métodos de interacción con un servidor mediante inyección SQL ▸ Explotar aplicaciones para robar cookies ▸ Ejecutando comandos a través de vulnerabilidades de aplicaciones web ▸ Caminando a través de un escenario de ataque completo.

Taller de 2 días

Ensamblador, reversa y desarrollo de exploits para Linux – Rodolfo Cecena (ponente del congreso)

Temario:

1- ¿Qué es ensamblador?

2-Assembler y linker

3-Syscalls y nuestro primer programa en ensamblador

4-Instrucciones básicas de ensamblador

5-Analisis de un binario

6-Intrucciones aritméticas en ensamblador

7-Cadenas de texto en ensamblador (Strings)

8-Ciclos en ensamblador

9-Condicionales en ensamblador

10-Ingenieria inversa, conceptos básicos

11-Radare framework para la ingeniería inversa

12-Ingenieria inversa en routers

13-Ingenieria inversa en forense

14-Parchando un binario vulnerable con ingeniería inversa

15-Desarrollo de exploits, conceptos básicos

16-Fallos de segmentación

17-Bit setuid

18-Shellcodes de conexión directa

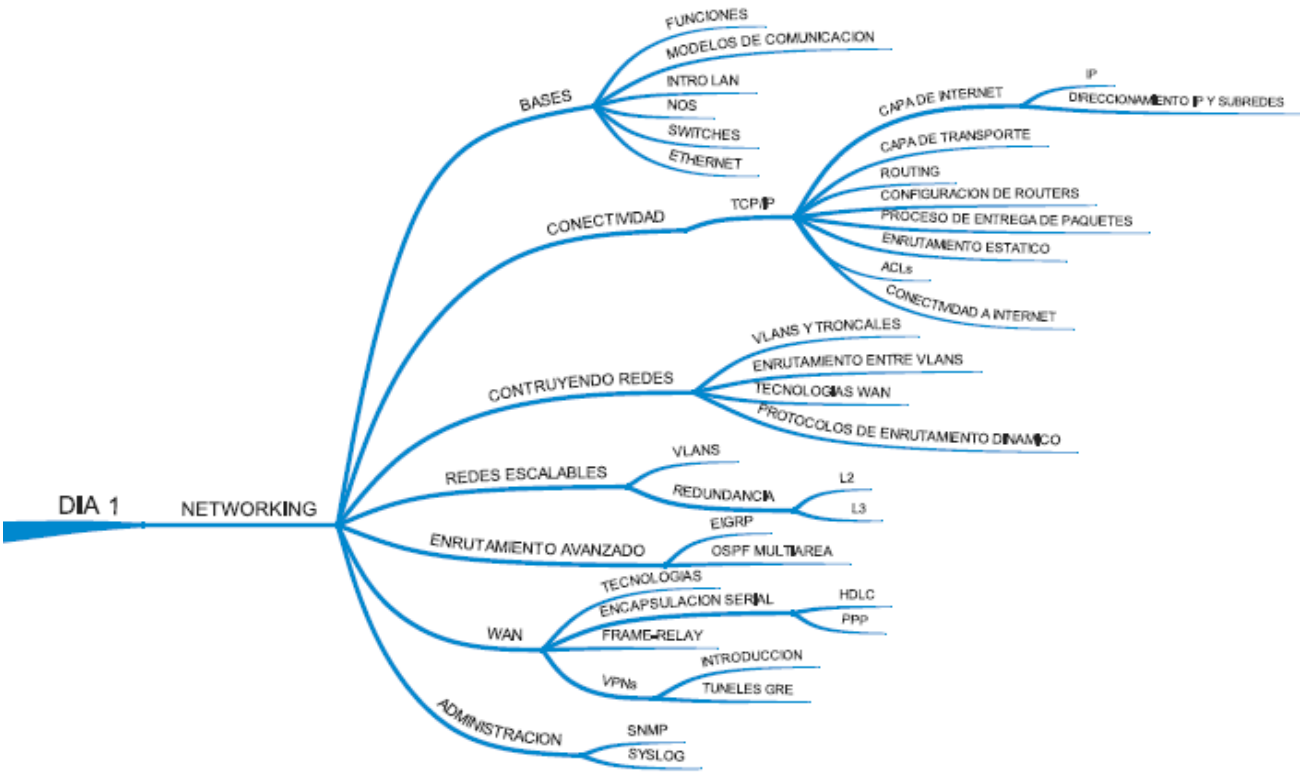
19-Shellcodes de conexión inversa

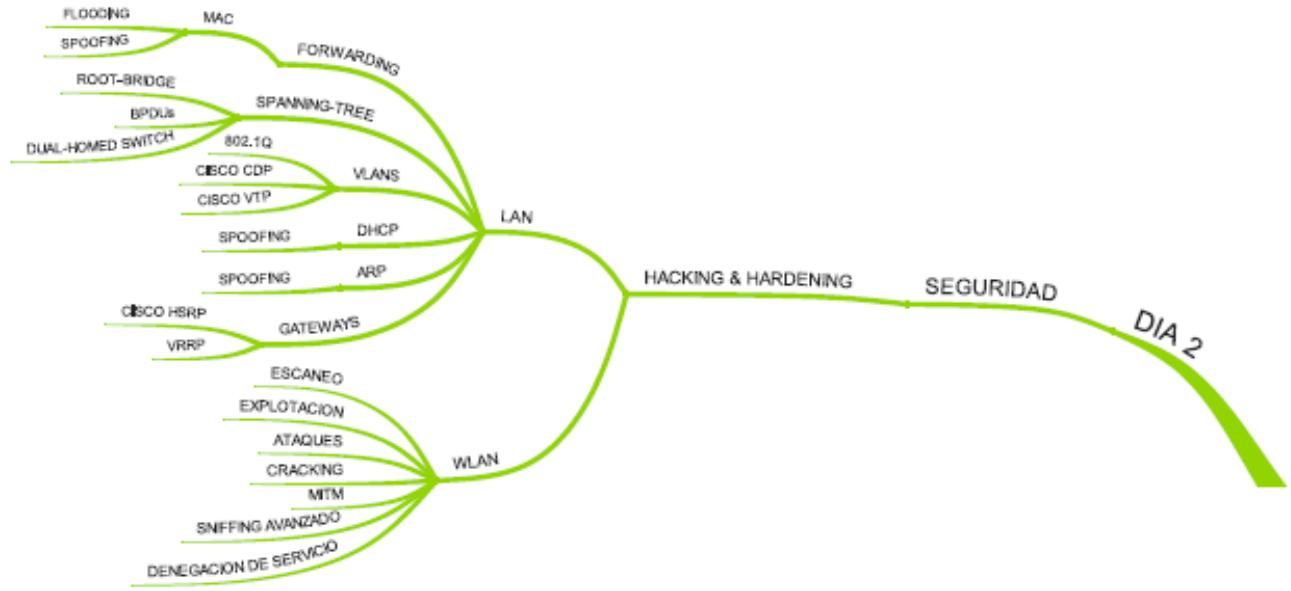
20-Tecnicas para evadir protecciones y mecanismos de defensa

Taller de 3 días

Hacking Data Network and hardering – Ricardo Quintana Toscano (CCDP)

Temario:




DIA 2
SEGURIDAD
HACKING & HARDENING
LAN
MAC
FLOODING
SPOOFING
FORWARDING
SPANNING-TREE
ROOT-BRIDGE
BPDUs
DUAL-HOMED SWITCH
802.1Q
VLANS
CISCO CDP
CISCO VTP
DHCP
SPOOFING
ARP
SPOOFING
GATEWAYS
CISCO HSRP
VRRP
WLAN
ESCANEO
EXPLOTACION
ATAQUES
CRACKING
MITM
SNIFFING AVANZADO
DENEGACION DE SERVICIO


DIA 3
FORENCIA
ANALISIS DE TRAFICO
PAQUETES DE DATOS
FLUJOS DE DATOS
WLAN
IDS/IPS
BASES
DISPOSITIVOS DE RED Y SERVIDORES
LOG DE EVENTOS
SWITCHES
ROUTERS
FIREWALLS
PROXYWEB
VPNS
MALWARE

- Todos los talleres ya incluyen el acceso al DurivaCON 2018

- Reconocimiento firmado y sellado de participación en el congreso.

- Constancia de participación en el taller

- Playera conmemorativa al DurivaCON 2018.

- Acceso exclusivo a los retos del evento