Curso Virtual de Nmap

Único Curso del Año 2018

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Sábados 20 y 27 de Enero del 2018

De 9:00 am a 12:15 pm (UTC -05:00) - 6 horas en Total

1. Presentación:

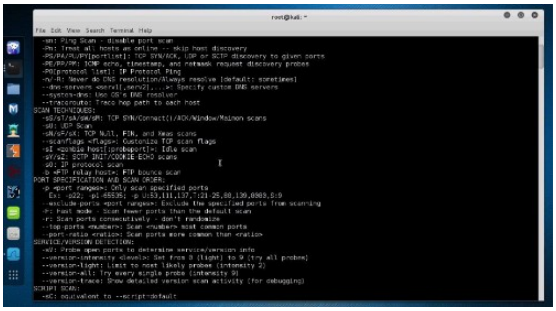
Nmap (Network Mapper) o por su traducción al español “Mapeador de Red”, es una herramienta libre y open source especializada en la exploración de redes y auditorías de seguridad. También es útil para tareas como realizar un inventario de la red, gestionar horarios para la actualización de servicios, además de vigilancia de hosts o tiempo de funcionamiento de un servicio.

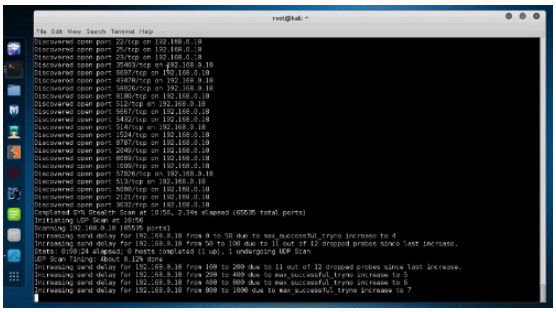
Nmap utiliza paquetes IP en bruto para determinar cuales son los hosts disponibles en la red, cuales servicios (nombre y versión de la aplicación) ofrecen estos hosts, cuales sistemas operativos (y versiones del Sistema Operativo) están ejecutando, cual tipo de filtro de paquetes o firewall están utilizando, y docenas de otras características. Está diseñado para escanear rápidamente grandes redes, pero trabaja también muy bien con algunos hosts. Nmap puede ser ejecutado y utilizado en los principales sistemas operativos.

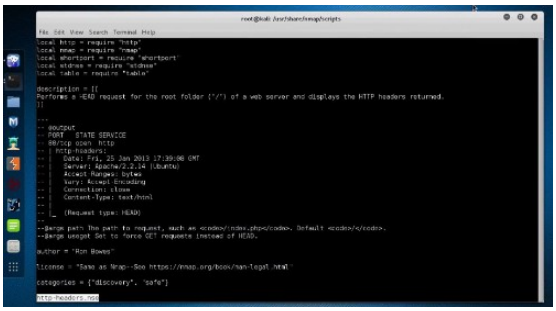
Este curso totalmente práctico proporciona una excelente guía para utilizar todas las funcionalidades y características incluidas en Nmap. Así mismo este curso es una excelente fuente de conocimiento tanto para aquellos quienes recién se inician con esta herramienta, como para los profesionales quienes lo utilizan constantemente.

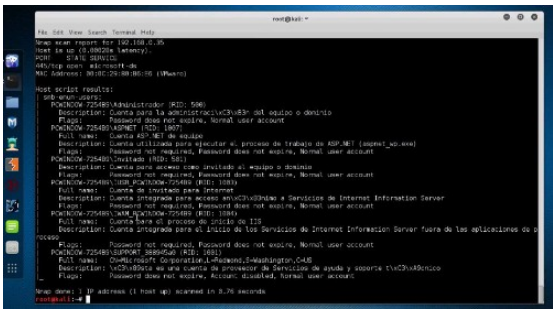
2. Temario:

- Introducción a Nmap
- Descubrimiento de Hosts
- Especificar Hosts y Redes Objetivos
- Encontrar la Dirección IP de una Organización
- Controles para Descubrimiento del Host
- Técnicas para el Descubrimiento del Host
- Introducción al Escaneo de Puertos
- Opciones en Línea de Comandos
- Técnicas para el Escaneo de Puertos
- Tipos de Escaneo TCP SYN, TCP Connect, UDP. TCP FIN, NULL, Xmas, ACK
- Optimizar el Desempeño de Nmap
- Técnicas para la Reducción del Tiempo de Escaneo
- Datos y Estrategias para la Selección de Puertos
- Controles de Tiempo a Bajo Nivel
- Plantillas de Tiempo
- Detección de Servicios y Versión de Aplicación
- Procesadores Posteriores
- Formato del archivo nmap-services-probes
- Detección Remota del Sistema Operativo
- Métodos soportados por Nmap de Reconocimiento TCP/IP
- Métodos Evitados por Nmap para el Reconocimiento de la Huella
- Algoritmos de Coincidencia del Sistema Operativo
- Enfrentando Hosts no Identificados
- Nmap Scripting Engine (NSE)
- Formato del Script
- Lenguaje del Script
- Scripts NSE
- Detección de Firewalls e IDS
- Determinar Reglas del Firewall
- Evadir Reglas del Firewall
- Transtornar y Evitar IDS
- Interfaz Gráfica (Zenmap)
- Interpretar los Resultados del Escaneo
- Explorar la Topología de Reducción
- Editor de Perfiles
- Buscar y Comparar Resultados









3. Material:

Se sugiere al participante instalar la versión estable más reciente de Nmap, ya sea en Windows o GNU/Linux. Nmap puede ser descargado desde los siguientes enlaces.

Nmap: http://nmap.org/download.html

Enlace de Descarga (Windows): https://nmap.org/dist/nmap-7.60-setup.exe
Enlace de Descarga (GNU/Linux): https://nmap.org/dist/nmap-7.60.tar.bz2

También se sugiere tener instalada y configurada la siguiente máquina virtual:

Metasploitable 2.

Link de Descarga: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Nombre del Archivo: metasploitable-linux-2.0.0.zip

[*] Si el participante lo requiere se le puede enviar 1 DVD con las máquinas virtuales; Kali Linux 2.0 y Metasploitable 2, añadiendo S/. 50 soles por el concepto de gastos de envío hacia cualquier lugar del Perú.

4. Día y Horario:

La duración total del curso es de 6 (seis) horas. El curso se dictará en los siguientes días y horarios.

Sábados 20 y 27 de Enero del 2018
De 9:00 am a 12:15 pm (UTC -05:00) - 6 Horas en total.

[*] No habrá reprogramaciones. El curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 130 Soles o $ 40 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

ScotiaBank
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

Una vez realizado el depósito, enviar por favor el comprobante escaneado a la siguiente dirección de correo electrónico: **caballero.alonso@gmail.com**.

Otros Países

Para residentes en otros países el pago se realiza mediante una transferencia de dinero utilizando Western Union o MoneyGram. Por favor escribir un mensaje de correo electrónico a **caballero.alonso@gmail.com**. para coordinarlos datos para realizar la transferencia.

Confirmado el depósito o transferencia, se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia el sistema y poder participar en el curso.

6. Más Información:

Si desea mayor información sobre el Curso Virtual de Nmap, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: +51 949304030

7. Instructor:

A**lonso Eduardo Caballero Quezada** es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.