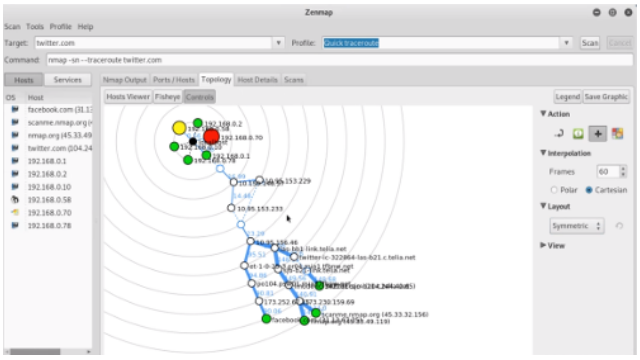
Nmap

Curso Virtual - 2020



Único Curso del Año 2020

Fechas:

Sábados 21 y 28 de Marzo del 2020

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

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

1. Presentación:

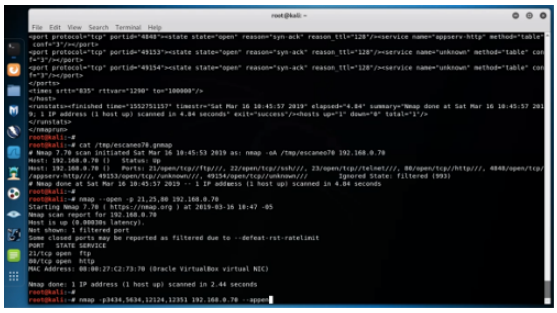
Nmap (Network Mapper) o por su traducción al español “Mapeador de Red”, es una herramienta libre y open source especializada en la exploración de redes y auditorías de seguridad. También es útil para tareas como realizar un inventario de la red, gestionar horarios para la actualización de servicios,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

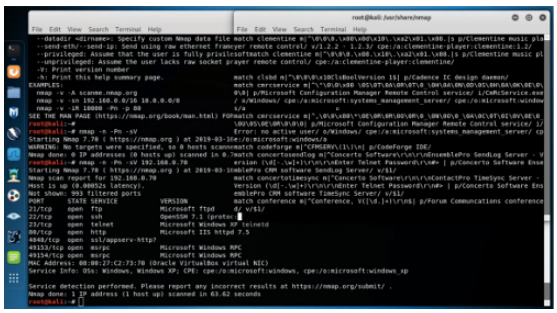
Nmap utiliza paquetes IP en bruto para determinar cuales hosts están disponibles en la red, cuales servicios (nombre y versión de la aplicación) ofrecen estos hosts, cuales sistemas operativos (y versiones del sistema operativo) están ejecutando, cual tipo de filtro de paquetes o firewall están utilizando,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

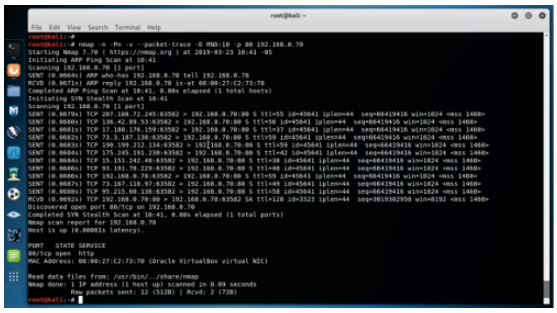
Este curso totalmente práctico proporciona una excelente guía para utilizar todas las funcionalidades y características incluidas en Nmap. Así mismo este curso es una excelente fuente de conocimiento tanto para quienes recién se inician con la utilización de esta herramienta, como para los profesionales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

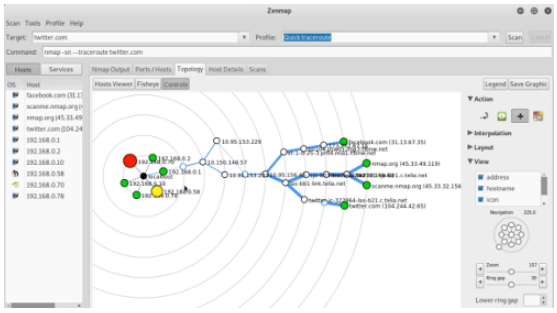
2. Temario:

- 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:

Todos los participantes al Curso Virtual de Nmap tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

Adicionalmente el participante tiene la opción de adquirir por S/. 50 Soles adicionales, Un (1) DVD conteniendo las máquinas virtuales utilizadas durante el desarrollo del curso. Este costo incluye los gastos de envío a cualquier lugar del Perú.

En caso el participante no adquiera los DVDs, se le sugiere descargar y configurar las siguientes máquinas virtuales.

Kali Linux:

Link de Descarga: https://www.kali.org/downloads/

Metasploitable 2

Link de Descarga: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Metasploitable 3

Link de Descarga: https://github.com/rapid7/metasploitable3

4. Día y Horario:

El Curso Virtual de Nmap tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**
  Sábados 21 y 28 de mazo del 2020
- **Horario:**
  De 9:00 am a 12:15 pm (UTC -05:00). 6 horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

5. Inversión y Forma de Pago:

El Curso Virtual de Nmap tiene un costo de:

S/. 165 Soles o $ 50 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito Bancario en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada También puede realizar el depósito en un Agente Scotiabank. Encuentre el más cercano utilizando la siguiente página: https://intl.scotiabank.com/es-pe/locator/Default.aspx Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**	Transferencia o pago mediante Western Union o Moneygram, También mediante Paypal. MoneyGram. WESTERN UNION WU moving money for better Paypal: PayPal Escríbame por favor un mensaje de correo electrónico para detallarle los datos necesarios para realizar la transferencia o el pago. Una vez realizada la transferencia o el pago, enviar por favor el documento escaneado al siguiente correo: **caballero.alonso@gmail.com**

Confirmado el depósito o la transferencia se le enviará al correo electrónico del participante los datos necesarios para conectarse al sistema, además del material utilizado durante el desarrollo del curso.

El curso se realiza utilizando el sistema de video conferencias Anymeeting. El cual proporciona la transmisión de audio y video en tiempo real de alta calidad, tanto para el instructor como también para los participantes, entre otras características ideales para impartir cursos de manera virtual.

INTERMEDIA ANYMEETING

http://www.anymeeting.com

6. Más Información:

Si requiere más 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: +51 949 304 030

7. Instructor:

Alonso 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, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y Pen Testing. 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 dieciséis años de experiencia en el área y desde hace doce 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.