Introducción a DevSecOps

INT_DEVSECOPS

En este curso tendrá laboratorios prácticos con pruebas y software de código abierto.

Nos concentraremos en cómo puede agregar una DAST (herramienta de prueba de seguridad de aplicaciones dinámicas) en su CI/CD (canalización de DevOps) con éxito. Agregar una herramienta que no está ajustada, la herramienta incorrecta, una herramienta con un alcance infinito, etc., puede hacer que una canalización se ejecute durante mucho tiempo, crear toneladas de falsos positivos o incluso romper su servidor de aplicaciones. Queremos que tenga éxito.

Cubriremos varias formas en que puede usar una herramienta DAST (también conocida como escáner de aplicaciones web, proxy web, escáner dinámico, herramienta de piratería ética o incluso "escáner pew pew"). No necesita poner todo en un CI/CD solo porque puede hacerlo. ¡Cubriremos todas las formas en que se puede usar una herramienta como esta!

Configuraremos todo para un escaneo exitoso, le presentaremos Nexploit (el escáner DAST que usaremos), GitHub Actions (el CI/CD que usaremos) y Broken Crystals (la aplicación vulnerable que usaremos).

¡Escanearemos todas las cosas! Configuraremos 3 tipos de escaneos (aplicación web regular, escaneo API y escaneo de archivos HAR), registraremos un archivo HAR y exploraremos cada tipo de prueba que podamos hacer. También cubriremos qué pruebas debe hacer para varios tipos de aplicaciones, para que pueda hacer el escaneo lo más rápido posible, mientras se asegura de cubrir todas sus bases.

Revisaremos todos los resultados de nuestro(s) escaneo(s) y hablaremos sobre cómo remediar los resultados. Habrá muchos resultados para que los revisemos.

Haremos un resumen rápido y le ofreceremos los recursos para que continúe con su aprendizaje.

Objetivos del curso

Puede estar pensando: "¿Por qué estoy aquí? Soy un desarrollador, no necesito saber cómo usar herramientas de seguridad".

El mundo está cambiando y la seguridad se está volviendo más importante que nunca. Un desarrollador de software, un miembro del equipo de control de calidad, un profesional de seguridad de TI o un administrador de sistemas que sepa cómo escanear una aplicación web en busca de vulnerabilidades, es un gran activo para cualquier organización centrada en la tecnología.

	Si está creando software usted mismo, este conjunto de habilidades puede ayudarlo a garantizar que sus aplicaciones sean seguras de usar, y sus clientes no se sorprenderán con un informe de un probador de penetración que encuentra cien cosas mal, porque tendrá ya solucionados todos los problemas obvios antes de tiempo. Además, las aplicaciones de escaneo son simplemente divertidas, como verá a medida que avanza en este curso.
Prerrequisitos	Conocer los fundamentos de la Nube, haber participado en algún proyecto de Nube en cualquier arquitectura tanto Pública como Privada e Híbrida; deseos de superación y hambre de colaborar con los compañeros para participar en laboratorios y retos.

Temario

Capítulo 1. Introducción a DevOps

- Objetivos
- Introduccion
- 1.1 La necesidad de DevOps.
- 1.1.1 El Objetivo (El Libro).
- 1.1.2 El Objetivo (Entrega de Aplicaciones).
- 1.2 Cuellos de Botella en la Entrega de Aplicaciones.
- 1.2.1 El Modelo de Cascada.
- 1.2.2 Dev vs Ops.
- Resumen
- Bibliografia
- Práctica

Capítulo 2. Toolchain DevOps

- Objetivos
- Introduccion
- 2.1 Como construtir una cadena de Herramientas DevOps
- 2.1.1 Solucion todo en uno
- 2.1.2 Solucion codigo abierto
- 2.2 Porque necesitamos una cadela de herramientas Devops
- 2.3 Beneficios de desarrollar una aplicación usando Devops
- 2.4 Herramientas populares para crear una cadena de herramientas devops

- 2.4.1 Planificacion
- 2.4.2 Construir
- 2.4.3 Integracion continue y entrega continua
- 2.4.4 Funcionar / Operar
- 2.5 Desarrolle una aplicación usuando Devops Toolchain
- Resumen
- Bibliografia
- Quiz
- Practica

Capítulo 3. Camino a DevSecOps

- Objetvos
- Introduccion
- Procesos de Desarrollo Ágil
- 3.1 Git y su papel en DevOps Moderno.
- 3.2 Infrastructure as Code.
- 3.3 Nube
- 3.4 Monolitos
- 3.5 Microservicios
- 3.6 Funciones “as Service”.
- 3.7 Integración (continua), implementación y Despliegue
- Resumen
- Bibliografia
- Quiz
- Practica

Capítulo 4. S-SDLC integrado con CI/CD

- Objetivos
- Introduccion
- 4.1 ¿Qué es S-SDLC?
- 4.2 Tendencia actual
- 4.3 ¿Por qué S-SDLC?
- 4.4 Breve explicación de S-SDLC

- 4.5 Partes interesadas (Stakeholders)
- 4.6 Desarrollo de políticas y procedimientos de apoyo
- 4.7 Midiendo el éxito
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 5. Static Application Security Testing (SAST)

- Objetvos
- Introduccion
- 5.1 Riesgos de seguridad de la aplicación
- 5.2 ¿Qué es el Top 10 de OWASP?
- 5.3 Fundamentos de SAST
- 5.4 Pros y contras de SAST
- 5.5 ¿Por qué es importante SAST?
- 5.6 ¿Cómo funciona SAST?
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 6. Software Composition Analysis (SCA)

- Objetvos
- Introduccion
- 6.1 ¿Qué es SCA (Software Composition Analysis)?
- 6.2 ¿Por qué utilizar una herramienta de Software Composition Analysis)?
- 6.3 ¿Cómo elegir una herramienta de Software Composition Analysis)?
- 6.3.1 Motor de políticas
- 6.3.2 Apto para desarrolladores
- 6.3.3 Calidad y procedencia del código
- 6.3.4 Informes de última generación
- 6.3.5 Soporte e integraciones del ecosistema

- 6.3.6 Análisis de dependencia
- 6.3.7 Detección de vulnerabilidades
- 6.3.8 Priorización
- 6.3.9 Remediación
- 6.3.10 Automatización y extensibilidad
- 6.3.11 Seguridad de aplicaciones nativas en la nube
- 6.4 ¿Cómo es que el Software Composition Analysis ayuda a reducir riesgos en OSS?
- 6.4.1 SCA ayuda a identificar y analizar vulnerabilidades de OSS
- 6.4.2 SCA hace que la gestión de vulnerabilidades sea más eficiente
- 6.4.3 Desplazamiento hacia la izquierda Mitigación de riesgos
- 6.4.4 Aplicación de políticas a escala
- 6.5 Código abierto en 2022
- 6.6 Desafíos del análisis de composición de software
- 6.6.1 Visibilidad oscurecida
- 6.6.2 Comprender la lógica de dependencia
- 6.6.3 Crecientes vulnerabilidades
- 6.6.4 Bases de datos de vulnerabilidad limitada
- 6.7 Mejores prácticas de análisis de composición de software
- 6.7.1 Habilitar
- 6.7.2 Desplazamiento a la izquierda
- 6.7.3 Automatizar
- 6.7.4 Priorizar
- 6.8 El futuro del Software Composition Analysis
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 7. Dynamic Application Security Testing (DAST)

- Objetvos
- Introduccion
- 7.1 Pros y Contras de DAST

- 7.2 ¿Por qué DAST es importante?
- 7.3 ¿Cómo funciona DAST?
- 7.4 ¿Qué es una herramienta DAST adecuada para los desarrolladores?
- 7.5 ¿Cuál es la diferencia entre SAST y DAST?
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 8. Seguridad en Infrastructure as Code

- Objetvos
- Introduccion
- 8.1 Beneficios de la infraestructura como código
- 8.2 Infraestructura como enfoques de código
- 8.3 Las 5 principales herramientas de infraestructura como código
- 8.4 Infraestructura como mejores prácticas de código
- 8.4.1 ¿Escaneo de seguridad IaC?
- 8.4.2 Reglas de escaneo de seguridad de IaC
- 8.5 Dos escáneres IaC de código abierto para comenzar
- 8.6 Beneficios de usar la infraestructura como código en DevOps
- 8.7 Integrar con una canalización de CI/CD
- 8.8 Desafíos comunes para IaC en DevOps
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 9. Seguridad en Contenedores

- Objetvos
- Introduccion
- 9.1 Construir seguridad en la tubería del contenedor
- 9.1.1 Reunir imágenes
- 9.1.2 Anticipar y remediar vulnerabilidades

- 9.1.3 Administrar acceso
- 9.2 Integre las pruebas de seguridad y automatice la implementación
- 9.3 Defiende tu infraestructura
- 9.4 Desafíos de seguridad de contenedores
- 9.5 Integre con CI/CD Pipeline y proteja su entorno de host
- 9.6 Componentes clave de las herramientas de seguridad de contenedores
- Resumen
- Bibliografia
- Quiz
- Practica

Capitulo 10. Cumplimiento como Código

- Objetvos
- Introduccion
- 10.1 La implementación requiere colaboración y transparencia
- 10.1.1 Mejorando la tecnología a través de la cultura
- 10.1.2 El cumplimiento como código ofrece ventajas para toda la organización
- Resumen
- Bibliografia
- Quiz
- Practica

Debido a las constantes actualizaciones de los contenidos de los cursos por parte del fabricante, el contenido de este temario puede variar con respecto al publicado en el sitio oficial, sin embargo, Netec siempre entregará la versión actualizada de éste