unidad2_aliaga.md

Unidad 2

Ejercicio 1

Buscar en Internet o en el uso habitual en nuestros trabajos, para realizar una lista de lo que podremos encontrar respecto a nombres de scanners de vulnerabilidades.

Recientemente empecé a trabajar para una empresa local que da servicios a una empresa muy grande de supermercados. Me llamó MUCHO la atención la falta de medidas de seguridad; muchas aplicaciones están abiertas a internet y como única medida para llegar a ciertas páginas usan una VPN. No implementan un NHIS ni encriptado obligatorio del disco. Simplemente alguna que otra política con respecto a las contraseñas y esas otras aplicaciones accesibles desde una VPN.

En otras empresas tenía políticas generales de Windows (GOP), además de doble VPN en algunos casos. En otra empresa usaban Carbon Black y encriptado de disco con Sophos.

En esta nueva empresa, sí aplican medidas de seguridad en cuando al código

- Dependency-check: comprueba si las dependencias del código tienen vulnerabilidades conocidas
- sonarqube
- trivy: escanea contenedores y artefactos
- ZAP: escanea endpoints
- archery: concentra reportes

Ejercicio 2

Buscar en Internet o en el uso habitual, y hacer una lista de lo que podremos encontrar respecto a pentesting (eventos, tools, etc)

Se conoce como equipo rojo o red team al equipo de ethical hacking a cargo de realizar tareas identificación y explotación de vulnerabilidades de un sistema. Su contraparte es el equipo azul (blue team), encargado de monitorear el estado de la seguridad de la infraestructura de la empresa. Estos dos equipos si bien pareciera que están enfrentados, en realidad tienen el mismo objetivo: hacer que el equipo azul gane.

Las pruebas de pentesting sirven para que el equipo azul vea dónde tiene vulnerabilidades que desconocía y corregirlas de manera preventiva. Como se expuso durante la unidad, existen distintos tipos de pentesting:

- Caja negra: más parecido a un ataque real - los pentesters no tienen conocimiento específico de la infraestructura de la empresa y deben obtener toda la información en base al reconocimiento (OSINT).
- Caja blanca: el atacante, normalmente una persona dentro de la empresa, conoce toda la infraestructura de la empresa.
- Caja gris: el atacante tiene un conocimiento parcial previo a la infraestructura objetivo.

Todas estas modalidades de ataque se deben realizar previo contrato con el empleador para definir tanto un contrato de confidencialidad como onjetivos del ataque. Algunas herramientas que se usan para el reconocimiento previo al ataque son:

- Shodan: información sobre activos conectados a internet.
- Spyse: información técnica sobre puntos de entrada y explotación.
- Google Dorks: facilita la búsqueda para extraer información a través de la búsqueda con indexación.
- Maltego: se usa para rastrear las huellas digitales de usuarios.

- TheHarvester: herramienta para encontrar correos electrónicos, subdominios, direcciones IP entre otros a partir de varios datos públicos.
- Recon-ng: herramienta OSINT modular que permite apuntar a sitios específicos en busca de cierta información.