INFORME EJECUTIVO DE AUDITORIA

VULNERABILIDADES

WEBGOAT

Vulnerabilidades WebGoat

Información Gathering

PRUEBAS FOOTPRINTING

Primera técnica aplicada WHOIS, no dio resultados porque es una pagina privada

Respuestas ejecución DIG

- status: NXDOMAIN me dice que la pagina no esta registrada y no tiene DNS
- QUESTION SECTION consulta de tipo A (Cual es la direccion ip de esta pagina) Dominio 127.0.0.1:8080/WebGoatr pero no muestra IP
- Servidor IP 192.168.0.1.

El dominio no existe en la zona de nombres y no tiene DNS asociada

Dig mx no responde por lo que no tiene mails asociados

Dig txt no responde, no tiene servicios contratados

Dnsenum no devuelve host, tampoco nombre de servidor.

Geolocalizando la dirección retorna: The IP address '127.0.0.1' is a reserved IP address (private, multicast, etc.) por lo que dirección IP no se puede localizar.

TECNICAS FOOTPRINTING INEFICACES

PRUEBAS FINGERPRINTING

WAPPALYZER:

LAS TECNOLOGIAS UTILIZADAS PARA WEBGOAT SON:

- **PARA CODIFICAR LA PAGINA UTILIZARON UN FRAMEWORK DE JAVASCRIPT, BACKBONE.JS Y REQUIREJS**
- **BIBLIOTECAS UTILIZADAS PARA SU FUNCIONABILIDAD JQUERY, JQUERY UI Y UNDESCORE.JS**
- **PARA LA FUENTE DE LAS LETRAS UTILIZARON FONT AWESOME**
- **PARA EL FRONTEND UTILIZARO BOOTSTRAP**
- **EL LENGUAJE SOBRE EL QUE SE PROGRAMO ES JAVA**

Conclucion Wappalyzer:
Hemos conseguido un objetivo, logramos ver sobre que tecnologias de programacion fue creado WebGoat

NMAP: network mapper

Ejecute nmap en http://127.0.0.1:8080/WebGoat pero me dice que no hay un host ni direccion IP, agrego probarlo con el comando –Pn y aun asi no encuentra.

Tambien lo ejecute poniendo direccion del comando ifconfig en etho: inet y inet6 IP 192.168.0.255 o lo fe80::a00:27ff:fec2:63e9

Lo ejecute en mi propia direccion ip 192.168.1.1 y me dice lo mismo, pero es obvio que lo que devolveria seria mi propia direccion ip

Ejecutandolo con la IP de mi pc 127.0.0.1 (Fray me dijo que esa es mi verdadera direccion IP) dio un resultado distinto:

Starting Nmap 7.94 (https://nmap.org) at 2023-06-27 09:00 EDT

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000064s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE

8080/tcp open http-proxy

9090/tcp open zeus-admin

- **Host is up nos confirma que el host esta activo, dio una respuesta muy rapida**
- **Los puertos son 998 TCP y estan todos cerrados porque rechasaron (refused) la conexión**
- **El puerto 8080 esta abierto con el servicio http-proxy, esta disponible para recibir conexiones**
- **El puerto 9090 tambien esta abierto a recibir conexiones y utiliza el servicio zeus-admin**

Cuando le agrego a nmap 127.0.0.1 -O (-O busca el sistema operativo o OS) se agrega esta info:

DEVICE TYPE: GENERAL PURPOSE

RUNNING: LINUX 2.6.X

OS CPE: CPE:/O:LINUX:LINUX_KERNEL:2.6.32

OS DETAILS: LINUX 2.6.32

NETWORK DISTANCE: 0 HOPS

PUERTOS ABIERTOS: 8080 Y 9090

SISTEMA OPERATIVO: LINUX VERSION 2.6.32

LENGUAJE DE PROGRAMACION: JAVA Y JAVASCRIPT