Pentest Web

Entornos de laboratorio

Pentest Web – Entorno de laboratorio

- Conceptos y necesidades
- Tipologías
- Instalación de Dojo Web Security
  - Configuración
- Laboratorios por niveles
- Ley Hacker (curiosidad)

Pentest Web – Entorno de laboratorio

Conceptos y necesidades

- Actualmente, y según la normativa nacional e internacional, **queda totalmente prohibido cualquier intento intrusivo contra una infraestructura la cual no es de nuestra propiedad**, y queda reflejado en la famosa "Ley Hacker" del Código Penal en su artículo 197, con penas de prisión

Pentest Web – Entorno de laboratorio

Conceptos y necesidades – Reseña Ley Hacker

- El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión **de seis meses a dos años**.
- Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se **le impondrá la pena de multa de seis meses a dos años**. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.
- Número 3 del artículo 197 introducido en su actual redacción por el apartado quincuagésimo tercero del artículo único de la L.O. 5/2010, de 22 de junio, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 23 junio).Vigencia: 23 diciembre 2010

Pentest Web – Entorno de laboratorio

Conceptos y necesidades

Ante este escenario quedan dos opciones:

1. Realizar **nuestro propio entorno de pruebas**, diseñando un site web con los contenidos estáticos y dinámicos, y la programación del lado servidor, e incluir bugs para poder realizar pruebas posteriormente.
2. **Utilizar entornos de pruebas especialmente diseñados** con los principales ataques y bugs, que en un entorno controlado por nosotros nos permita desarrollar en su plenitud toda la potencia de inspecciones y validaciones, sin miedo a repercusiones

Pentest Web – Entorno de laboratorio

Conceptos y necesidades

- El primero de los casos, en este punto del curso, es inviable, **nos encontramos aprendiendo a identificar los errores en plataformas web**.
- En el segundo de los casos vamos a centrar el módulo actual. Será nuestro cometido realizar un completo laboratorio de test para poder realizar pruebas, para ello identificaremos dos posibles escenarios:
  - Acceso a escenario laboratorio **remoto**
  - Acceso a escenario laboratorio **local**

Pentest Web – Entorno de laboratorio

Conceptos y necesidades

- El primero de los casos, en este punto del curso, es inviable, **nos encontramos aprendiendo a identificar los errores en plataformas web**.
- En el segundo de los casos vamos a centrar el módulo actual. Será nuestro cometido realizar un completo laboratorio de test para poder realizar pruebas, para ello identificaremos un único escenario:
  - Acceso a escenario laboratorio **local**
- **Es muy habitual el uso de laboratorios remotos pero en esta caso no contaremos con uno (Caso OffSec)**

Pentest Web – Entorno de laboratorio

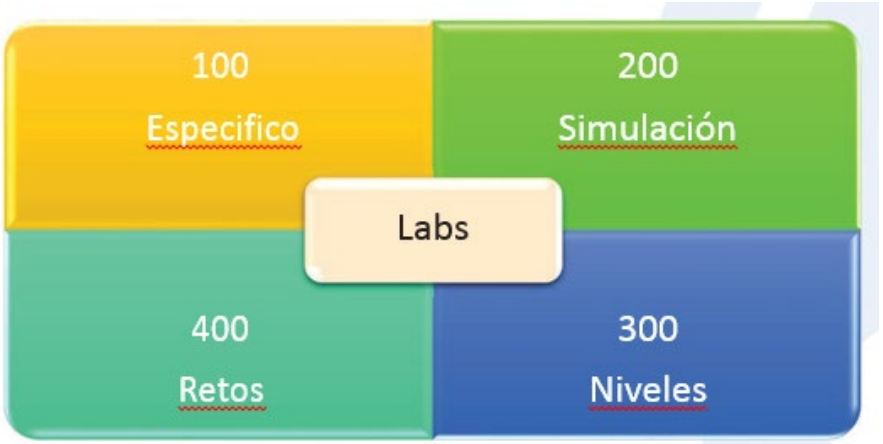
Conceptos y necesidades

- Ventajas del laboratorio local:
  - Disponibilidad de código: se podrá revisar el código o configuración que provoca la posibilidad de ataque y vulnerabilidad origen.
  - Posibilidad de realizar configuraciones propias
- Desventajas:
  - Escenario directo: la accesibilidad es directa, y no se verá afectada por las diferentes configuraciones de enrutamiento y configuración de filtros de los prestadores de servicios, los cuales en muchas ocasiones, son parte determinante.
  - Configuración estándar

Pentest Web – Entorno de laboratorio

Tipologías

- Se indicará cómo montar nuestro laboratorio de **dos de las categorías** disponibles, debido a la necesidad de establecer los requerimientos base de formación. Estas pruebas proveerán de los recursos necesarios para prácticas y poner a prueba todo lo aprendido, y poder realizar auditorías completas.



Pentest Web – Entorno de laboratorio

Tipologías

- 100 - Laboratorio Especifico
  - Estos laboratorios se identifican por ser un gran compendio de **pruebas segmentadas,** es decir, se podrá seleccionar la vulnerabilidad específica que se desea evaluar, e iniciar el ataque contra la misma.
  - Ideales para entrenar las capacidades adquiridas en un módulo concreto.
- 200 - Laboratorio de Simulación
  - Nos encontramos con escenarios que **intentan emular la realidad**, con sites completos de diferentes temáticas, juego, banca, red social, etc. en los cuales tendremos que volcar todo nuestro arsenal y capacidades para obtener el control o la base de datos

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Creado por el laboratorio de seguridad de Maven, **no es una plataforma unificada de test, por el contrario es el conjunto de múltiples laboratorios libres**, configurados en un mismo entorno, pero preservando la unicidad de cada uno de los mismos.
- Podemos **encontrar tanto herramientas para ser atacadas**, como herramientas para realizar los test, es decir, **aplicaciones para atacar los objetivos**, por lo que tiene doble visión, como plataforma y batería de pruebas, o como herramienta para gestionar y automatizar los ataques dirigidos

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Laboratorios:
  - OWASP's WebGoat
  - Google's Gruyere
  - Damn Vulnerable Web App
  - Hacme Casino
  - OWASP InsecureWebApp
  - w3af's test website

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Herramientas:
  - Burp Suite (free version}
  - w3af
  - sqlmap
  - arachni
  - metasploit
  - Zed Attack Proxy
  - OWASP Skavenger
  - OWASP Dirbuster
  - Paros
  - Webscarab
  - Etc.

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- https://sourceforge.net/projects/websecuritydojo/files/

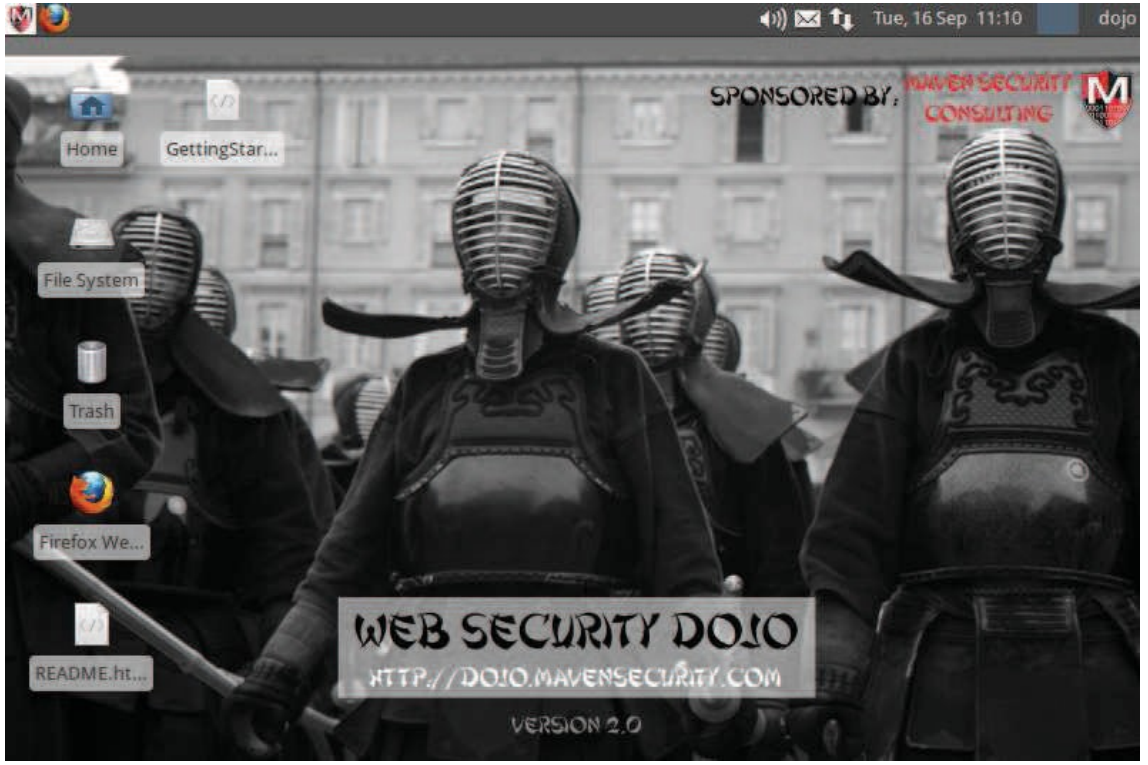
Para esta máquina usaremos VirtualBox en caso de que VMWare no funcione.

(probar con VMWare File→Open → fichero. Si nos deja abrirlo pulsar Retry cuando pregunte)

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Una vez arrancada la máquina:
  - Credenciales: dojo/dojo



Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- El entorno, de forma predefinida, viene configurado **con accesibilidad limitada de forma intencionada**, esto quiere decir que solamente podremos acceder a los aplicativos de test desde el sistema de Dojo, no desde cualquier otro ordenador de la red.

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Activar DVWA:
- Editamos el fichero /var/www/dvwa/.htaccess sudo nano /var/www/dvwa/.htaccess
- Las últimas líneas deberán quedar como la imagen inferior, y una vez reiniciemos el servidor web, apache:
  - sudo invoke-rc.d apache2 restart
- Podremos acceder al servicio desde cualquier Sistema desde el link que indicamos:
  - http://<ip_maquina_dojo/dvwa/login.php admin/password

Pentest Web – Entorno de laboratorio

Instalación de Dojo Web Security

- Activar Hackme Casino - Simulación
  - Hackme Casino no necesita ninguna configuración especial para poder acceder desde direcciones externas, solamente iniciarlo, y se realizará desde el menú Targets -> Hacme Casino Start.
- http://<ip_maquina_dojo>:3000
- Este entorno es uno de los más reales, aunque esta aplicación este orientada para usuarios noveles, y por lo tanto el nivel de dificultad es muy bajo, nos posiciona en lo que sería un test de penetración real, y las fases que debemos cubrir.

Pentest Web – Entorno de laboratorio

Laboratorios por niveles

- El laboratorio por niveles tiene como **objetivo realizar pruebas en base a un perfil de destreza y habilidad**, lo que nos obliga a mejorar la perfección de los conocimientos, tanto en profundidad como en el desarrollo de la técnica.
- Para diseñar el entorno utilizaremos **laboratorios que ya hemos configurado y que nos proveen de la posibilidad de desarrollarlos bajo niveles de perfiles de seguridad**. Estas propiedades nos posibilitan a realizar los test en modo básico o fácil, y volver a repetir la explotación pero en niveles superiores, donde tendremos que mejorar nuestras capacidades, y mejoraremos de forma secuencial conforme avancemos en dificultad

Pentest Web – Entorno de laboratorio

Laboratorios por niveles

- DVWA
  - Nos posicionamos en la sección **DVWA Security (menu izquierda)**, donde podremos seleccionar el **nivel de seguridad, bajo, medio y alto** Mediante esta configuración realizaremos nuestras pruebas, elevando la dificultad conforme completemos en su totalidad la explotación de la vulnerabilidad.
  - PRO: para poder afianzar y desarrollar nuestros conocimientos, nos permite configurar una herramienta de detección de **ataques en PHP, PHPIDS**. Si habilitamos **PHPIDS podremos simular un site con una protección para la detección de atacantes**, por lo que podremos evaluar la capacidad de ocultar los ataques, con métodos de ofuscación y evasión de defensas, teniendo que crear secuencias de ataque especialmente diseñadas.