PRÁCTICA : E2 - Herramientas de auditoría de seguridad Web OWASP, Acunetix, Dirb **MF0487_3 : Auditoría de seguridad informática**			**Fecha** 08 / 04 / 2022 Página 1 de 3
Curso	**SEGURIDAD INFORMÁTICA**	**Código del curso**	FC-2021.1/II.000/1914256

Nombre y Apellidos:		**Firma del Alumno:**	
DNI:		**Firma del Profesor:**	

Apto: ☐ **No Apto:** ☐ **Calificación:** ☐

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 1860 minutos
(Temporalizados durante el módulo)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0487_E2**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- Pendrive.

Instrucciones específicas

El objetivo de esta práctica guiada es realizar una auditoría con Nessus a la versión DVWA (Damn Vulnerable Web App) e identificar las vulnerabilidades más importantes que trae dicha distribución y tratar de reducir la gran cantidad de vulnerabilidades web que esta distribución trae.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 1860 minutos para realizar la práctica.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs :

Configuración DVWA en DVL en FEDORA.

http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson1/

Como instalar DVWA (Damn Vulnerable Web App) en Kali linux
https://aprendizdesysadmin.com/como-instalar-dvwa-damn-vulnerable-web-app-en-kali-linux/

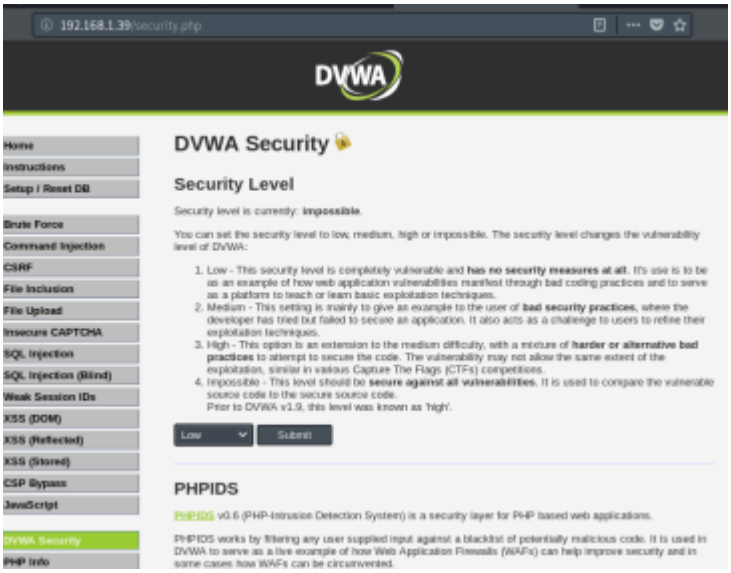
Pentesting de vulnerabilidades web con Damn Vulnerable Web App
http://www.solvetic.com/tutoriales/article/2332-pentesting-de-vulnerabilidades-web-con-damn-vulnerable-web-app/
http://aegis.pe/vega-nueva-solucion-open-source-para-analisis-de-vulnerabilidades-en-webapps

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

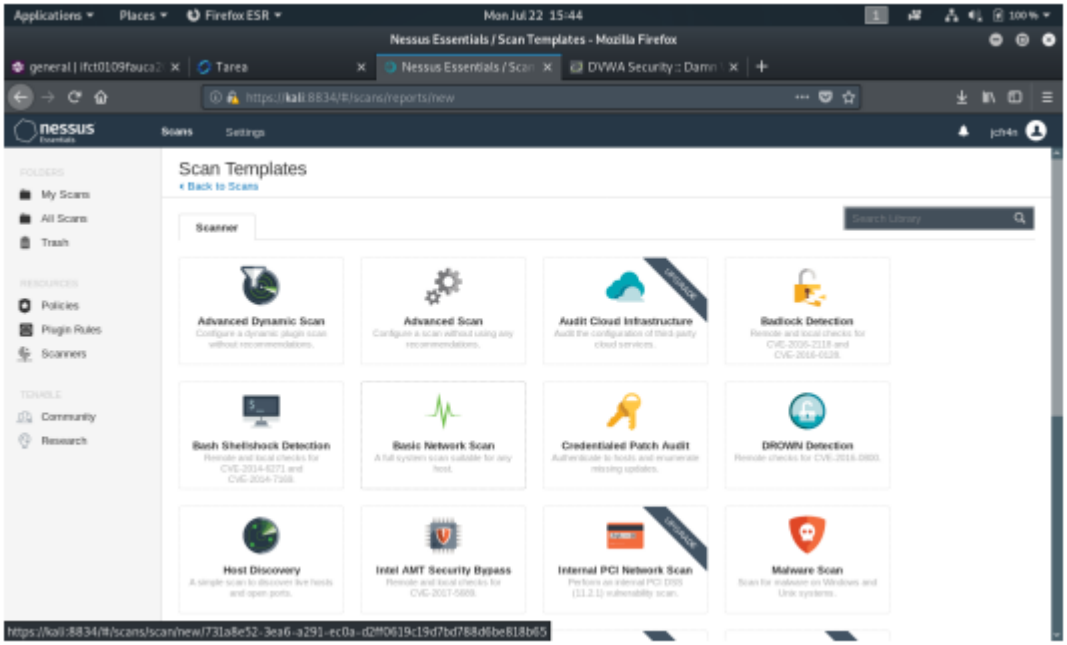
Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

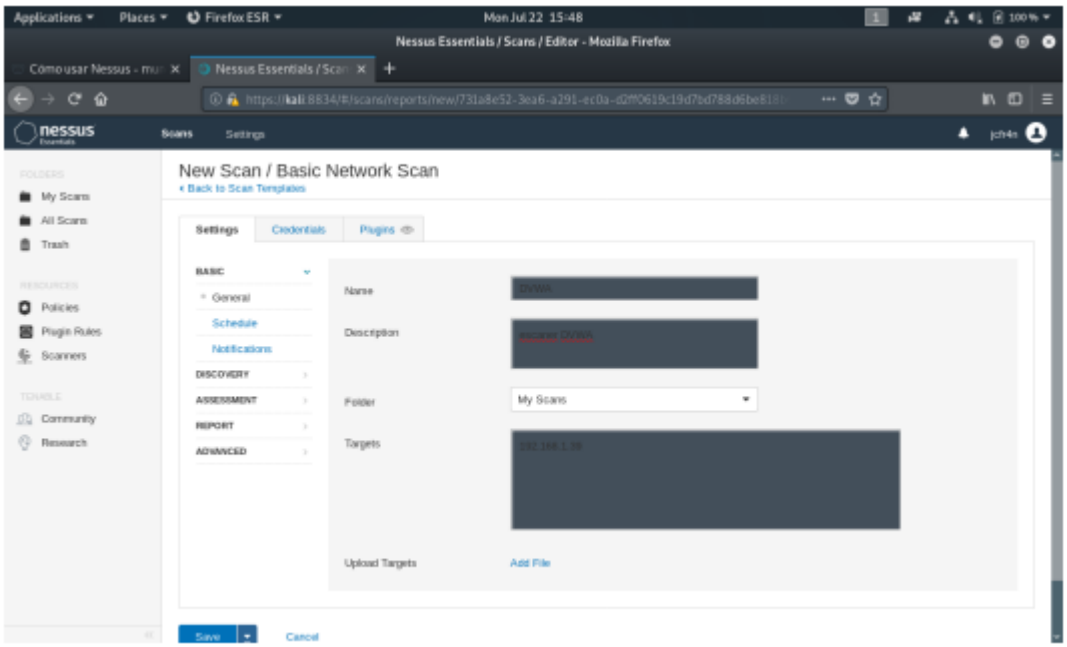
Descripción de la práctica

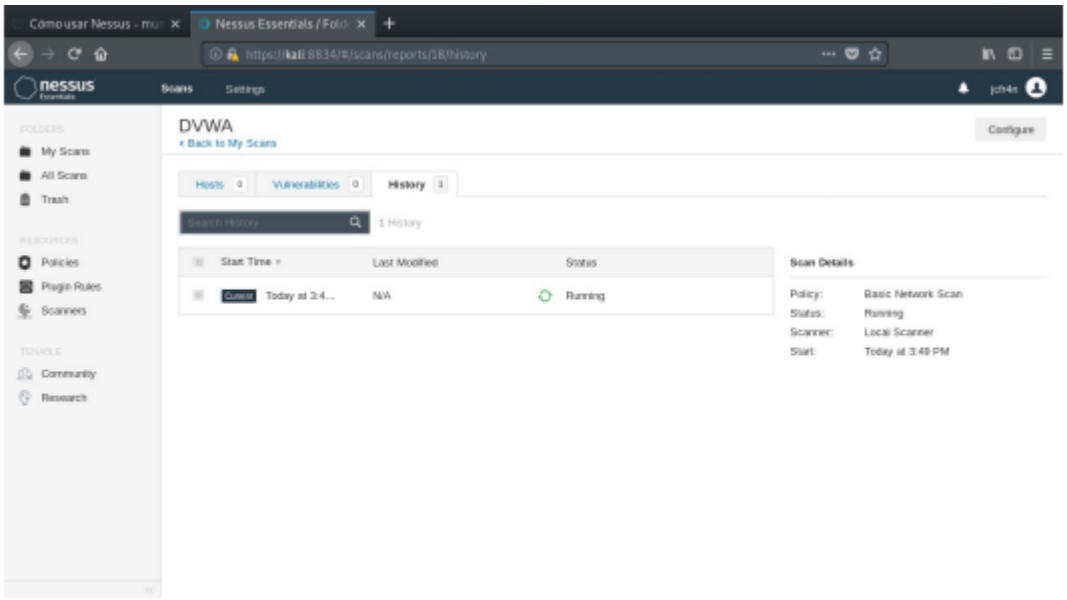
1. Instalación de DVWA : https://dvwa.co.uk/

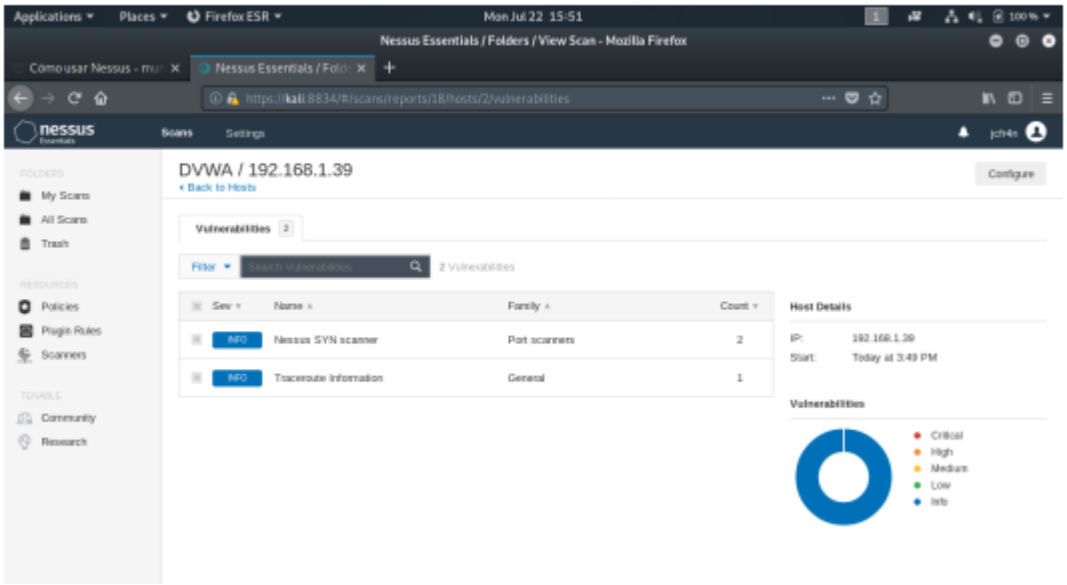


2. Realizar un escaneo con el programa NESSUS






Nessus Essentials / Folders
nessus
Scans
Settings
DVWA
Back to My Scans
Configure
Hosts
Vulnerabilities
History
Start Time
Last Modified
Status
Running
Scan Details
Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 3:49 PM
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
Community
Research


Applications
Places
Firefox ESR
Mon Jul 22 15:51
Nessus Essentials / Folders / View Scan - Mozilla Firefox
nessus
Scans
Settings
DVWA / 192.168.1.39
Back to Hosts
Configure
Vulnerabilities
Filter
Sev
Name
Family
Count
Nessus SYN scanner
Port scanners
Traceroute Information
General
Host Details
IP: 192.168.1.39
Start: Today at 3:49 PM
Vulnerabilities
Critical
High
Medium
Low
Info
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
Community
Research

3. Hacer uso de la herramienta Dirb para conocer parte del arbol de directorios.
4. Hacer uso del software NIKTO (Scaner de vulnerabilidades Open Source, escrito en Perl)

Nota :

Nikto proporciona la capacidad de escanear servidores web en busca de vulnerabilidades. Realiza más de 6,400 verificaciones por archivos o scripts potencialmente peligrosos, realiza 1,200 pruebas para versiones desactualizadas de servidores, y verifica cerca de 300 problemas específicos a versiones de servidores web.

La manera de ejecutar Nikto es a través de una línea de comando en la terminal.

nikto -host IP

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.39
+ Target Hostname:    192.168.1.39
+ Target Port:        80
+ Start Time:         2019-07-23 16:30:11 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 7915 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:          2019-07-23 16:31:20 (GMT-4) (69 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

5. Hacer uso de la herramienta SPARTA.

SPARTA es una aplicación GUI (Interfaz Gráfica de Usuario) escrita en Python, con la cual nos simplifica las pruebas de penetración en una determinada infraestructura de red y nos permite realizar diversas pruebas de penetración en la fase de escaneo y enumeración. Estas cualidades permite al pentester ahorrar tiempo en el momento de realizar una auditoria. SPARTA equivale a tener acceso a su caja de herramientas en la cual nos muestra toda la producción de las herramientas de una manera conveniente y ordenada.

Características de SPARTA

• Ejecutar Nmap desde SPARTA con el fin de poder obtener resultados rápidamente y lograr una cobertura completa, permite importar y exportar los resultados en XML. • Menú contextual configurable para cada servicio. Cualquier herramienta que se pueda ejecutar desde la terminal, se puede ejecutar desde SPARTA.

• Definir tareas automatizadas para los servicios (por ejemplo ejecutar Nikto en cada servicio HTTP, o SSLSCAN en cada servicio SSL.).

• Credenciales predeterminadas de verificación para los servicios más comunes. Por supuesto, esto también se puede configurar para ejecutarse automáticamente.

• Identifica la reutilización de contraseñas en la infraestructura de la prueba. Si alguno de los nombres de usuario/contraseñas se encuentran gracias a Hydra se almacenan en listas de palabras internas que luego pueden ser utilizados en otros objetivos que compartan la misma red.

Instalación de SPARTA

Para instalar SPARTA, es necesario tener instalado en el sistema al menos:

– Nmap (para agregar hosts)

– Hydra (para fuerza bruta)

– Cutycapt (para captura de pantalla)

– Nikto (para pruebas de vulnerabilidad)

Es recomendado utilizar SPARTA en Kali Linux, pues esta distribución ya posee preinstaladas todas las herramientas necesarias para su correcto funcionamiento, podemos utilizar cualquier distribución basada en Debian e instalarlo.

1) Actualizamos repositorios:

```
sudo apt-get update && apt-get upgrade
```

2) Instalamos Nmap, Nikto Hydra y Cutycapt:

```
apt-get install nmap nikto hydra cutycapt
```

3) Si no tenemos Python instalado en el sistema, ejecutaremos lo siguiente:

```
apt-get install python-elixir python-qt4
```

4) Clonamos el proyecto desde GitHub:

```
git clone https://github.com/secforce/sparta.git
```

6) Y por último lo ejecutamos.

```
python sparta.py
```

Ya podemos empezar a trabajar con SPARTA, la primera vez que se ejecuta crea dos archivos txt donde irá almacenando los usuarios y contraseñas válidos para futuros ataques poder reutilizarlos.

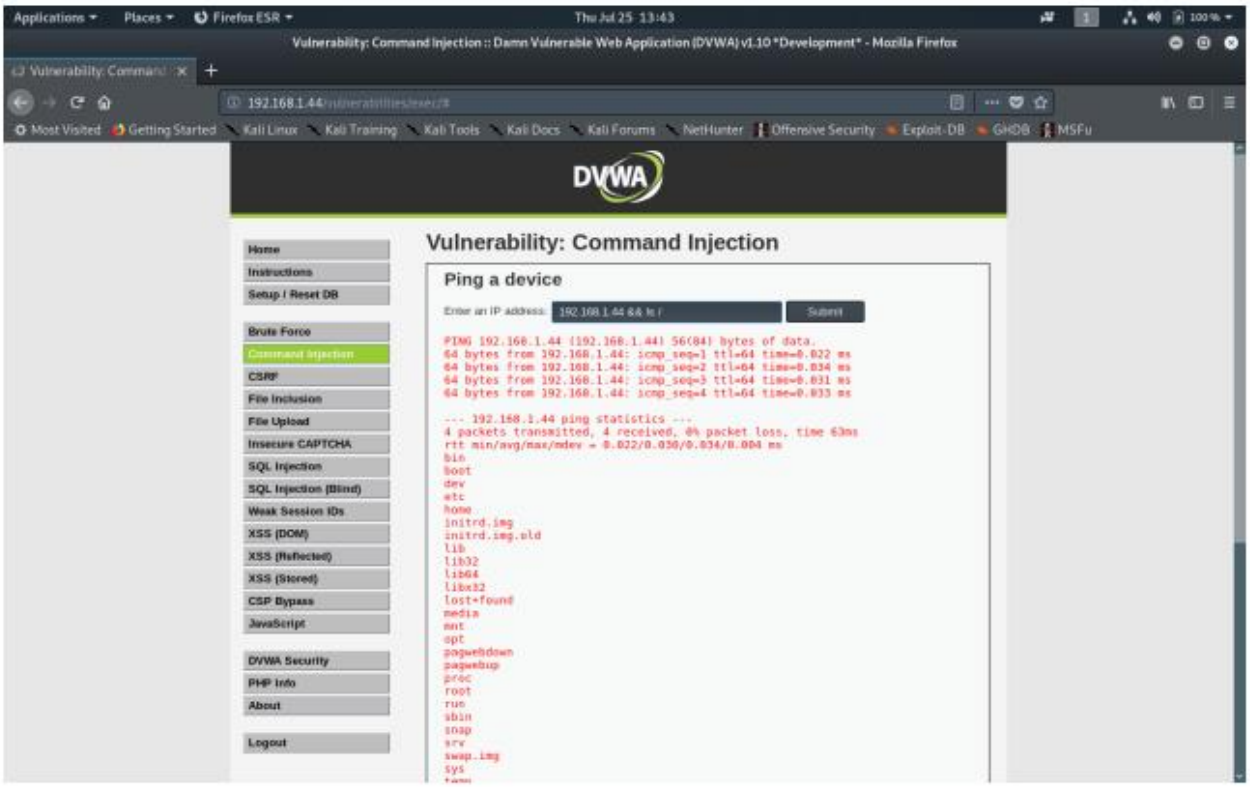
Explotando vulnerabilidades

BRUTE FORCE

La primera de las vulnerabilidades se explotó en modo fácil, partiendo del supuesto que conocemos el usuario y la clave la tenemos toda en mayúsculas por lo que debemos hacer que haga los cambios pertinentes, usamos la aplicación BURP y después le indicamos que haga las pruebas para entender el concepto, una vez descifrada la contraseña se le dice al programa que se valide en la página web y nos de acceso.

INYECCIÓN DE COMANDOS

En esta vulnerabilidad lo que buscamos es que en aquellas páginas desde las que nos permitan hacer ping a otras para comprobar la conexión, si no están debidamente protegidas se pueden inyectar comandos como ls, dir, strings, etc, que nos permiten hacer un reconocimiento del objetivo.



Arriba tenemos un ejemplo de la inyección del comando **ls /**