

Curso introductorio de Ethical Hacking

Semana 02

Profesor: Randall Barnett Villalobos

Aplicación de la etapa de Escaneo

Sesión 05

Configuración de Targets

Uso de un escáner de vulnerabilidades.

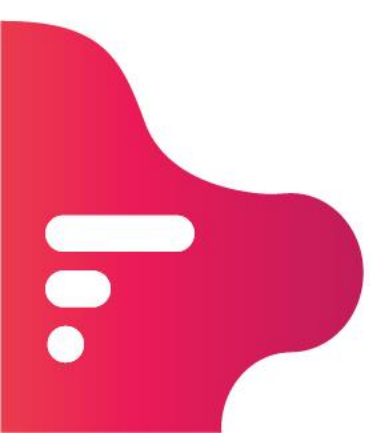
OpenVAS (Open Vulnerability Assessment System)

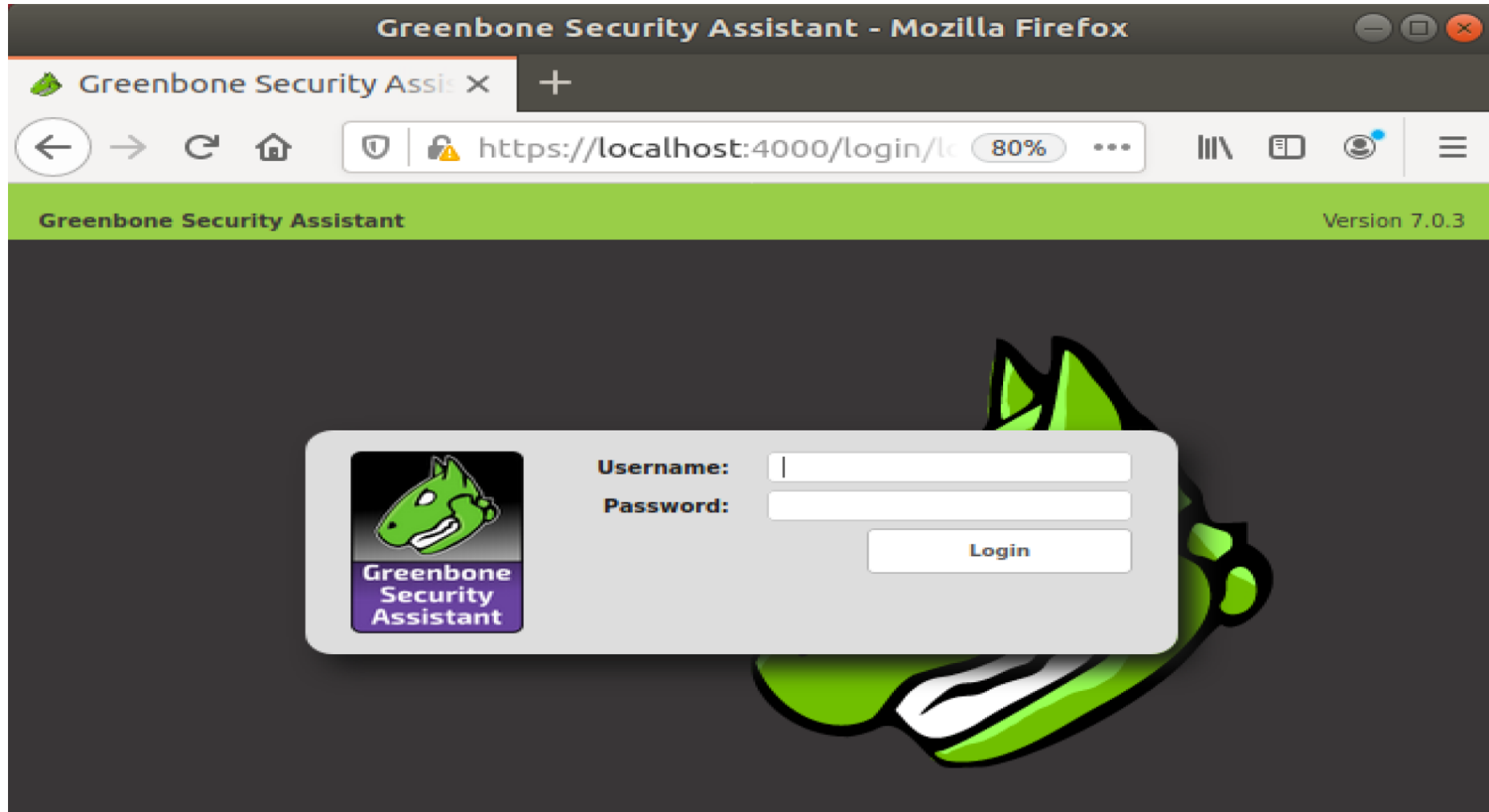
- Se trata de un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management).



Uso de OpenVas

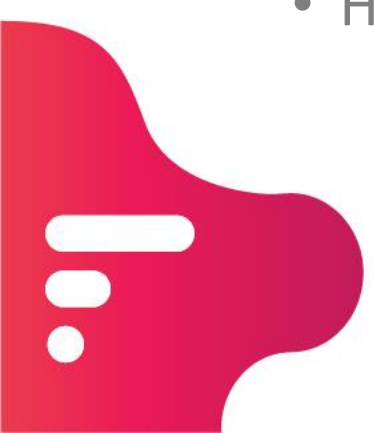
- En la sesión 04 de la semana anterior, se vió cómo instalar OpenVas.
- Una vez que el script ha concluido con éxito la instalación, se comienza a utilizar el escáner desde la siguiente URL:
 - <https://localhost:4000>
- En este momento, solo existe la cuenta de acceso inicial con el usuario admin y la contraseña admin:





Inicio de la configuración

- Luego de iniciar la sesión de trabajo, se tienen las siguientes opciones para configurar e iniciar el gestor y escáner de OpenVAS:
 - Scan management
 - Asset management
 - Configuration
 - Extras
 - Administration
 - Help



Nuevo objetivo

- El inicio rápido se realiza desde la pestaña Configuration, a través de configurar un objetivo o un conjunto de sistemas (hosts) a analizar.
- Los sistemas se pueden identificar a través de sus direcciones IP, nombres de host o por su notación de red CIDR (Classless Inter-Domain Routing).




**Greenbone**
Security Assistant



No auto-refresh

Logged in as Admin **admin** | Logout
Fri Aug 7 01:44:54 2020 UTC

DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp



Filter:
rows=10 first=1 sort=name





**Targets**

Name	Hosts
------	-------

New Target

Name

Metasploitable_AV

Comment

Analisis de prueba

Hosts

☒ Manual

☐ From file

☐ From host assets (0 hosts)

10.0.2.129

Examinar...

No se ha seleccionado ningún archivo.

Exclude Hosts

Reverse Lookup Only

☐ Yes ☒ No

Reverse Lookup Unify

☐ Yes ☒ No

Port List

All IANA assigned TCP 20... 

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

-- on port 22 

SMB

-- 

ESXi

-- 

SNMP

-- 

Mira el video

Configurar un target.

