Experto Universitario en Ethical Hacking

Unidad 2:

Métodos de control de Vulnerabilidades

Ejercicio Número 1 Unidad 2:

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.

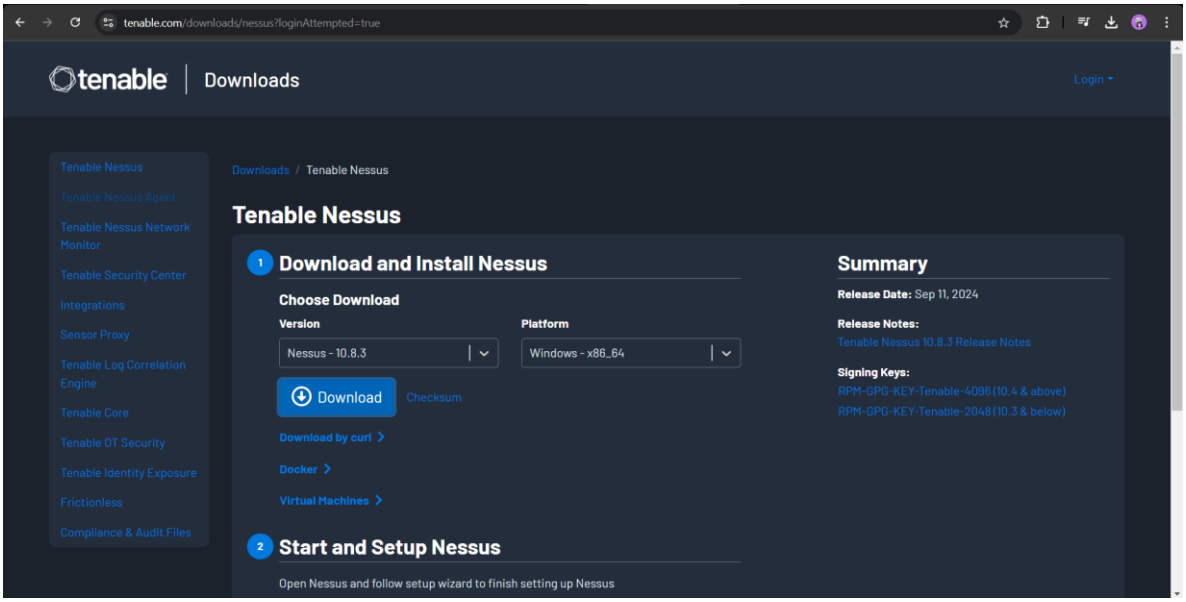
Ponerlo en el foro por favor, únicamente nombre de la aplicación, alguna captura y sitio web de descarga.

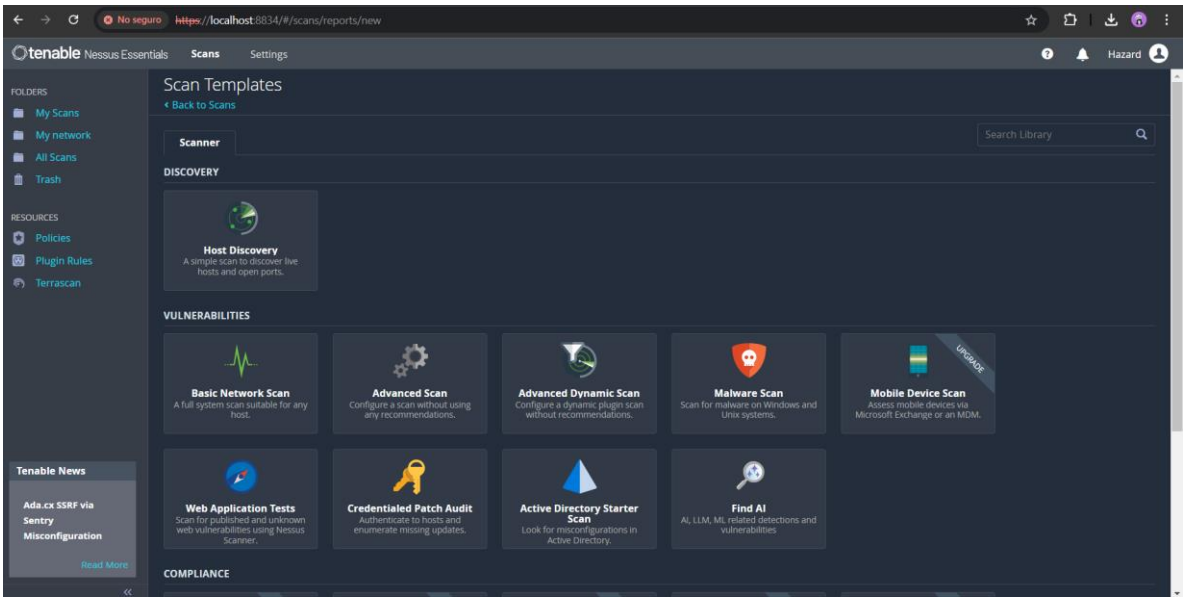
1. **Nessus**

Descripción: Un escáner de vulnerabilidades ampliamente utilizado para detectar vulnerabilidades, configuraciones incorrectas y malware en una variedad de sistemas.

Web de descarga: https://www.tenable.com/downloads/nessus?loginAttempted=true

Screenshots:



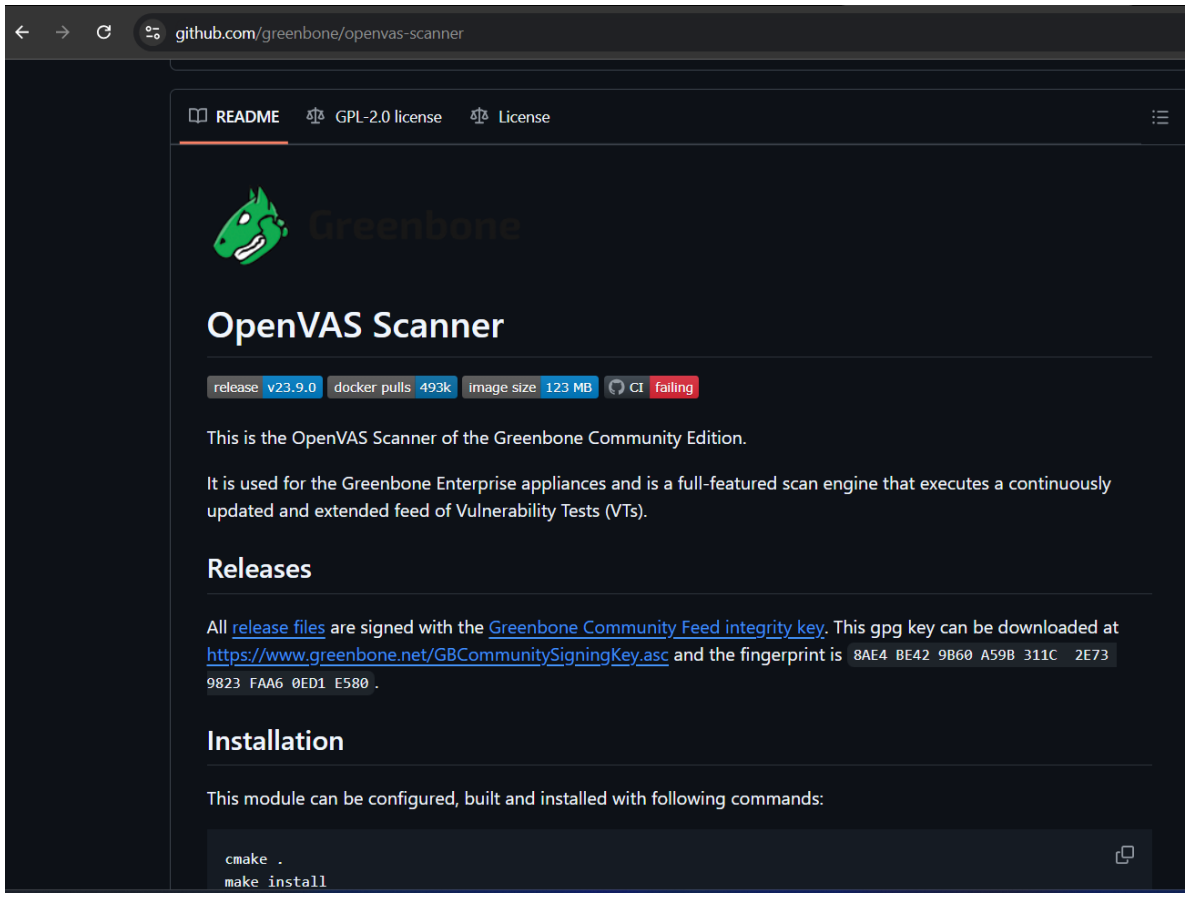


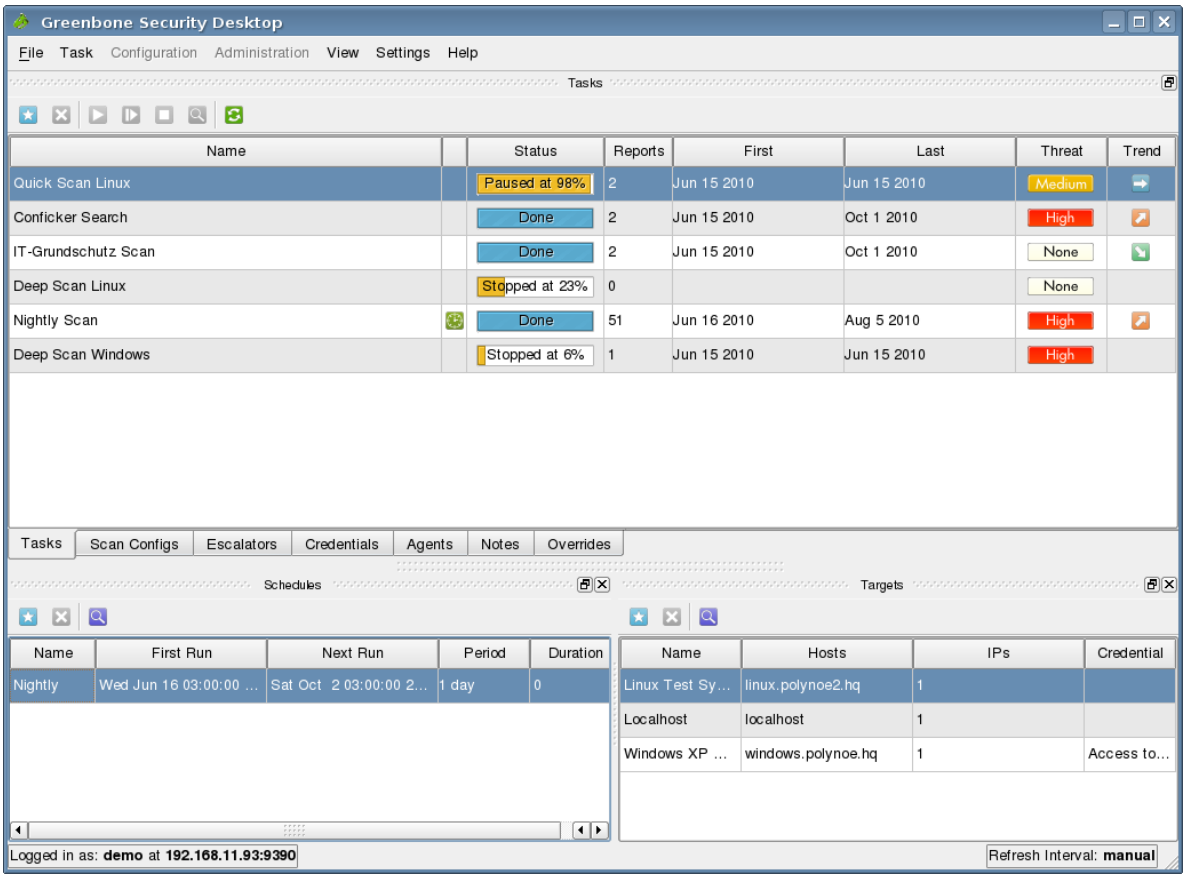
2. OpenVAS

Descripción: Un escáner de vulnerabilidades de código abierto que es parte del proyecto Greenbone. Ofrece análisis de redes, sistemas y aplicaciones, y es considerado una buena opción gratuita.

Web de descarga: https://github.com/greenbone/openvas-scanner

Screenshots:


github.com/greenbone/openvas-scanner
README
GPL-2.0 license
License
Greenbone
OpenVAS Scanner
release v23.9.0
docker pulls 493k
image size 123 MB
CI failing
This is the OpenVAS Scanner of the Greenbone Community Edition.
It is used for the Greenbone Enterprise appliances and is a full-featured scan engine that executes a continuously updated and extended feed of Vulnerability Tests (VTs).
Releases
All release files are signed with the Greenbone Community Feed integrity key. This gpg key can be downloaded at https://www.greenbone.net/GBCommunitySigningKey.asc and the fingerprint is 8AE4 BE42 9B60 A59B 311C 2E73 9823 FAA6 0ED1 E580 .
Installation
This module can be configured, built and installed with following commands:
cmake .
make install

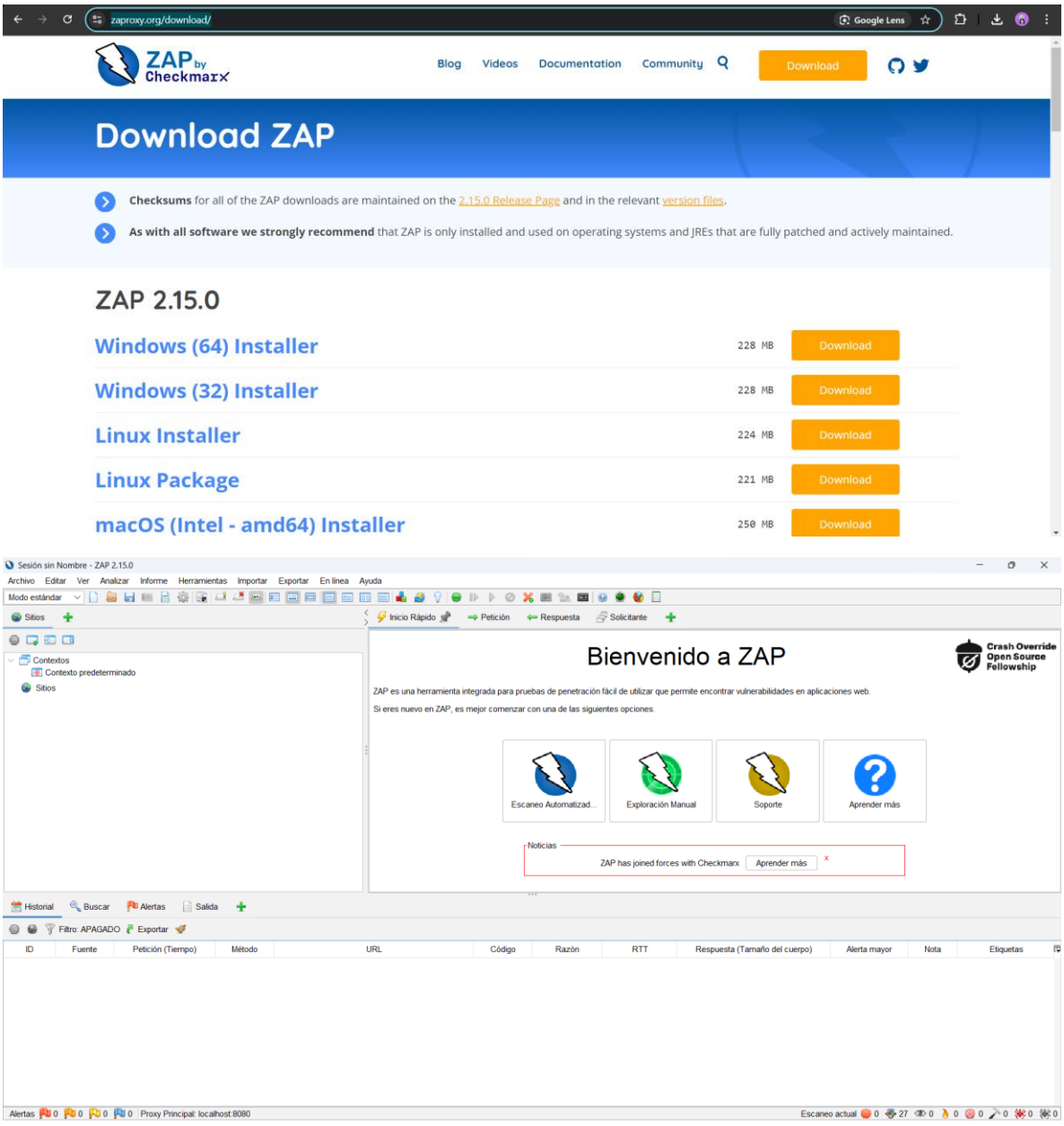


3. OWASP ZAP

Descripción: Un proyecto de código abierto mantenido por OWASP para pruebas de seguridad de aplicaciones web. Ofrece un escáner de vulnerabilidades automatizado y herramientas para pruebas manuales.

Web de descarga: https://www.zaproxy.org/download/

Screenshots:



También destaco entre los mas conocidos y utilizados para servidores web: Burp Suite y Nikto.

Ejercicio Número 2 Unidad 2:

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

Ponerlo en el foro, SER BREVE por favor, no más de 15 renglones.

Buscando en internet lo que puedo encontrar de pentesting a primera vista es:

- Conceptos/Definiciones
- Cursos
- Tutoriales
- Tools: Kali Linux, Burp Suite, Wireshark, John the Ripper, Hashcat, Nmap, Invicti, entre otras.
- Tipos de pentesting: Port Scanner, Vulnerability scanners, Network sniffer, Web proxy, Password cracker, etc.
- Eventos: Ekoparty

Rodrigo Vila.-