

Actividad práctica número 6:

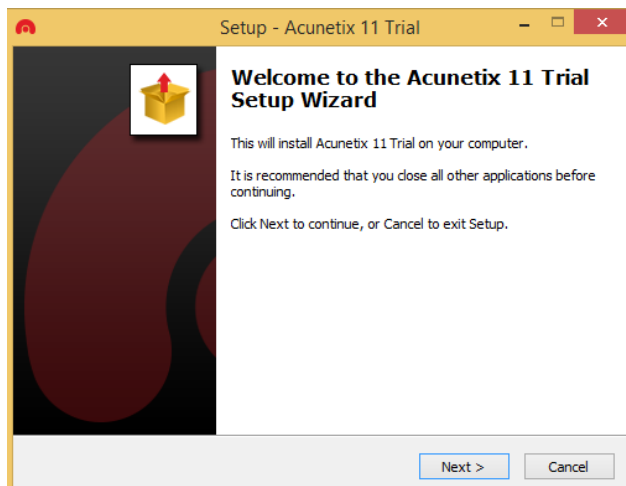
Formato: Individual.

Asignatura: Seguridad de Sistemas

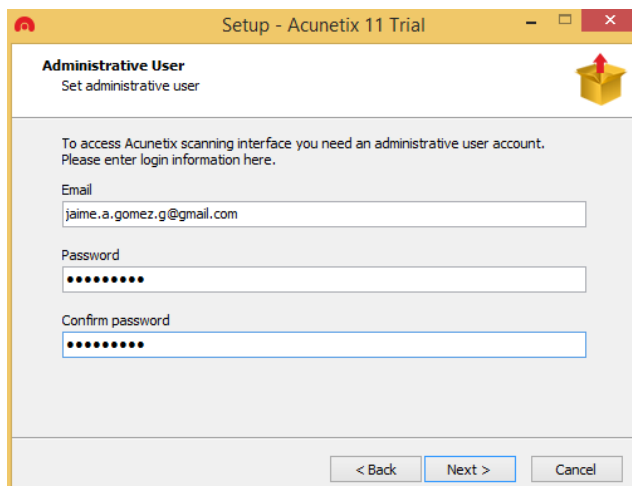
Título: Análisis de aplicaciones web

A.- Análisis con Acunetix

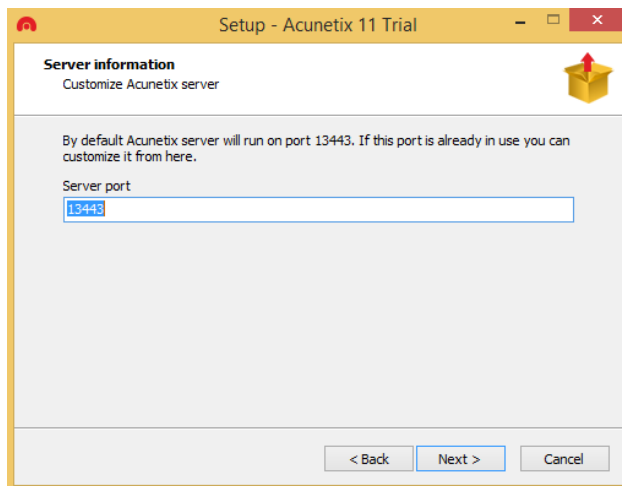
- 1.- Inicie su computador en Windows 10.
- 2.- Realice la instalación de la aplicación Acunetix provista por su profesor



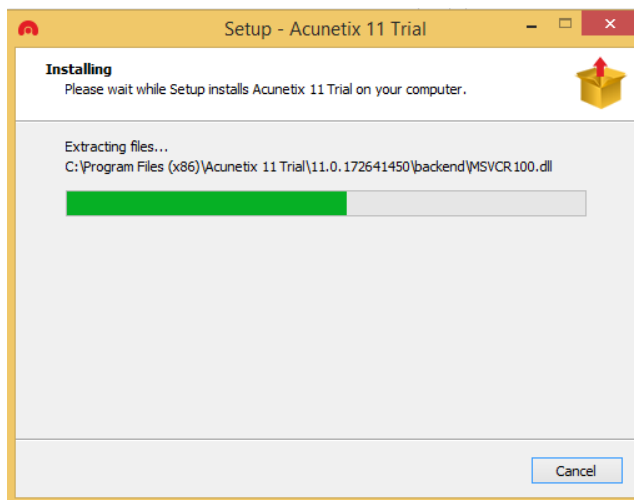
- 3.- Ingrese los parámetros para la administración



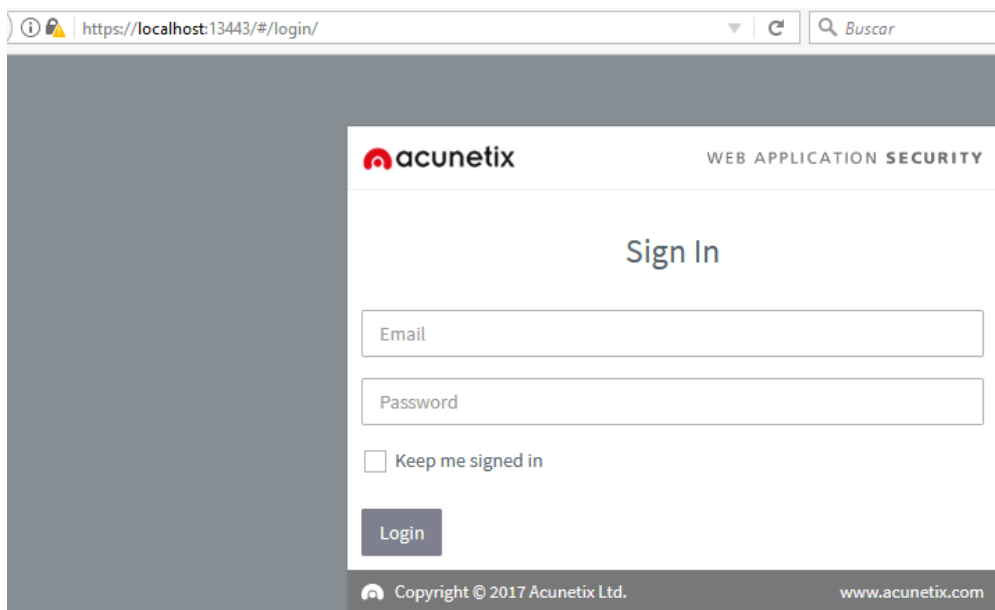
4.- Confirme el puerto de administración



5.- Realice la instalación por defecto



6.- Conéctese a través del browser a la interfaz de administración



7.- Cree la configuración del servidor a analizar

Add Target

×

Address

http://10.0.2.4

Description

Servidor de prueba

Add Target

Close

8.- Haga clic en “Scan” para iniciar el análisis

Back

Scan

Save

General

Crawl

HTTP

Advanced

Target Info

http://10.0.2.4

Description

Servidor de prueba

Business Criticality

Critical

Scan Speed

Slower

Slow

Moderate

Fast

9.- Configure las opciones de Scan

Choose Scanning Options

×

Scan Type

Full Scan

Report

Affected Items

×

Schedule

Instant

1 scan will be created

Create Scan

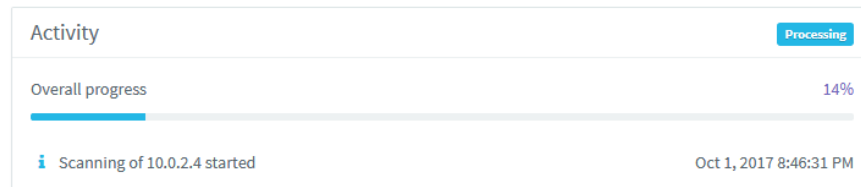
Close

10.- Espere a que finalice el análisis



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.



11.- Una vez finalizado el proceso de revisión, genere el reporte

Generate Report

Template

Affected Items

About Report Templates

Generate Report

Close

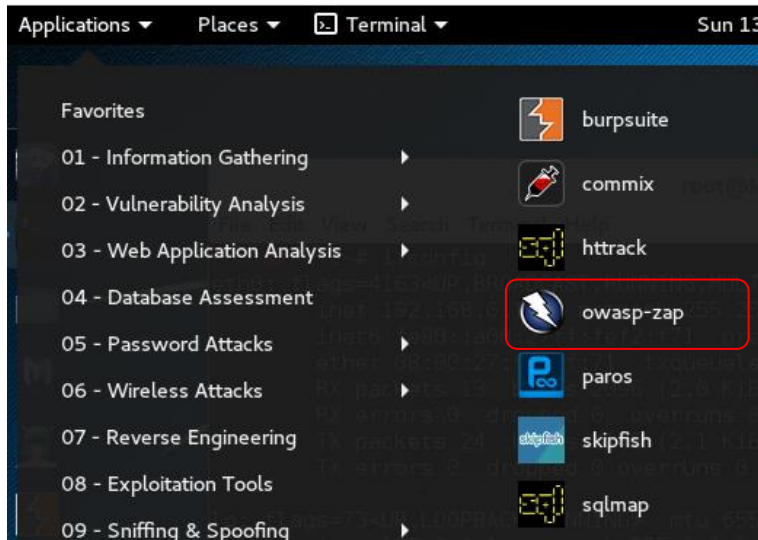
Affected items

| | |
|---------------------------------|---|
| Web Server | |
| Alert group | Blind SQL Injection |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

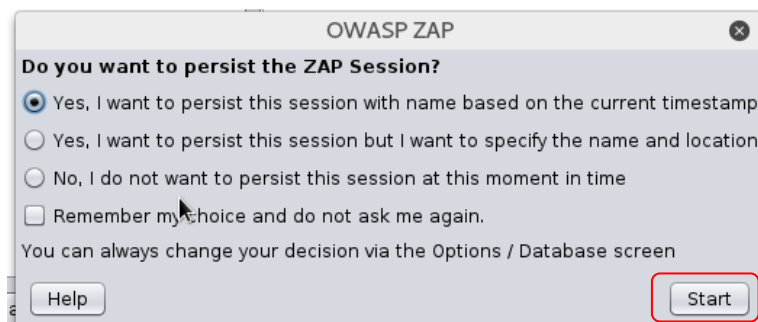
| | |
|-----------------|---|
| Web Server | |
| Alert group | Blind SQL Injection |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |

B.- Análisis web con ZAP de OWASP

- 1.- Inicie su máquina Kali con la interfaz de red en modo Red NAT
- 2.- Inicie la aplicación OWAS ZAP siguiendo el menú de la figura



- 3.- Seleccione la primera opción y haga click en start

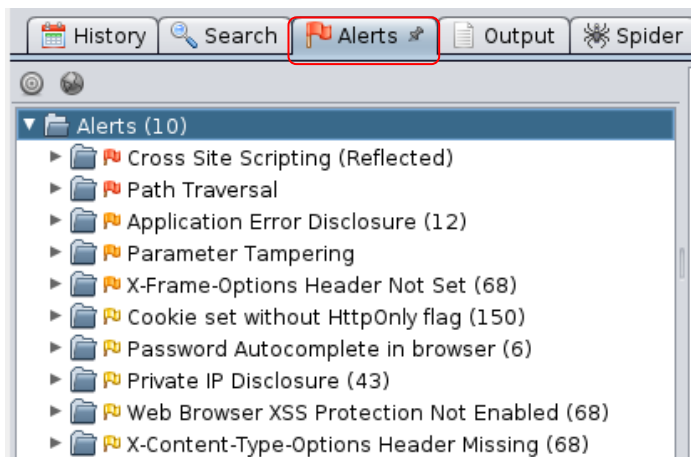


- 4.- Ingrese la URL mostrada en la figura utilizando la dirección IP de su servidor Metasploitable



A continuación, haga click en “Attack”

5.- Una vez finalizado el análisis revise las alertas en el menú “Alerts”



6.- Realice un reporte con las dos vulnerabilidades de más alto riesgo indicando:

- URL afectada: _____
- nivel de riesgo: _____
- Descripción: _____
- Solución: _____