



Universidad del  
**Rosario**



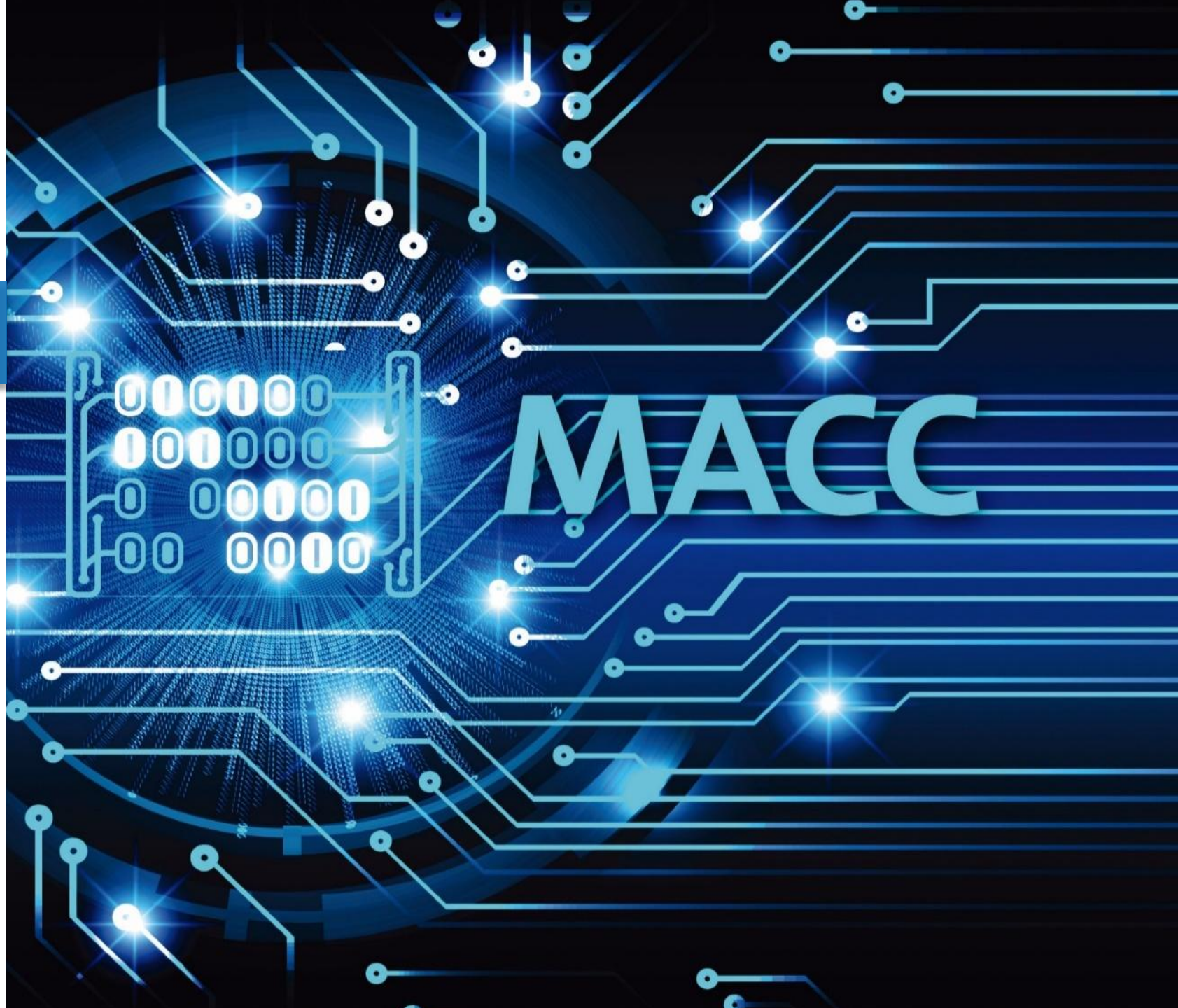
**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

## Análisis de vulnerabilidades

Hacking Ético

**Daniel Orlando Díaz López, PhD**

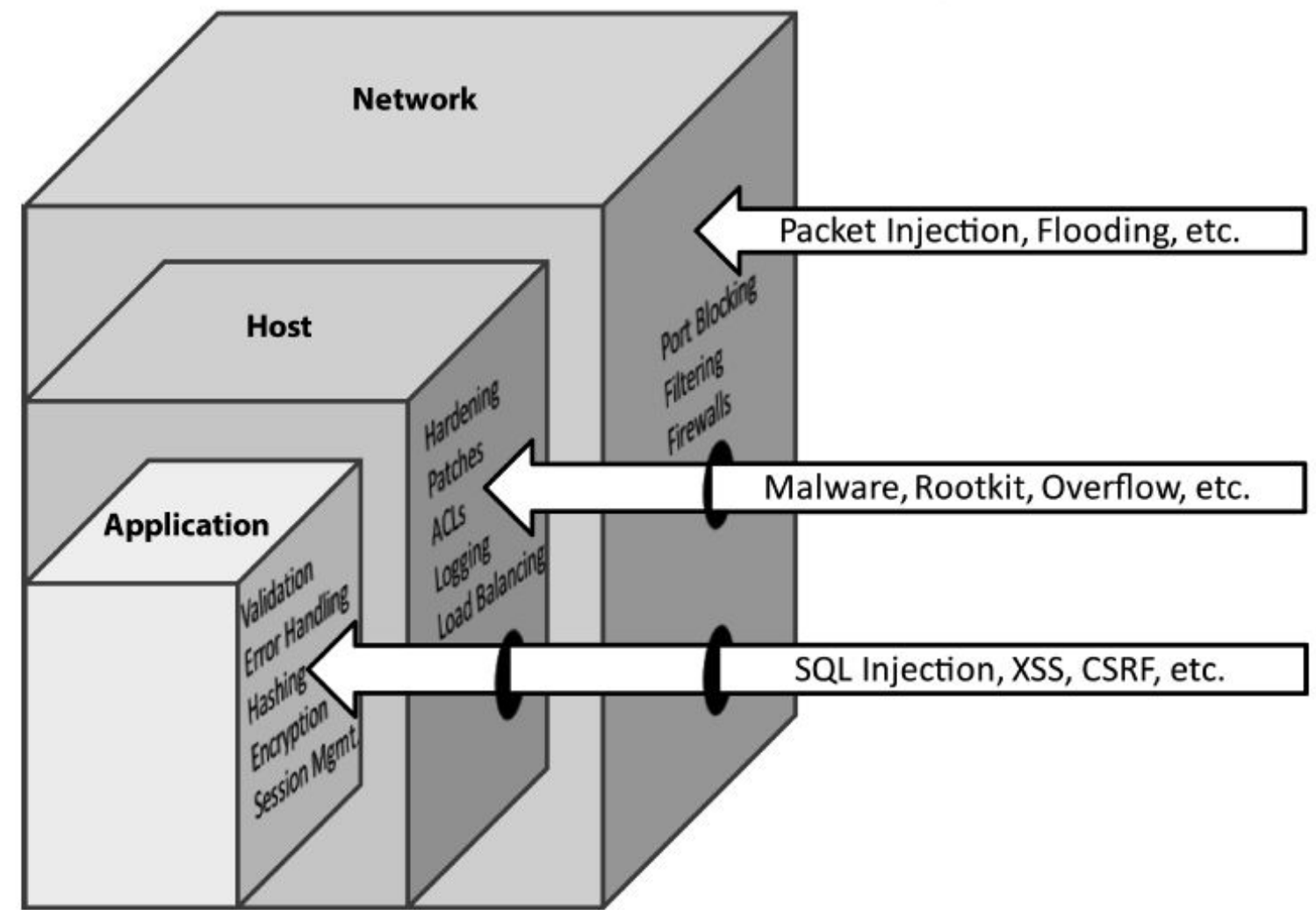
Profesor principal  
Departamento MACC  
Universidad del Rosario  
[danielo.diaz@urosario.edu.co](mailto:danielo.diaz@urosario.edu.co)

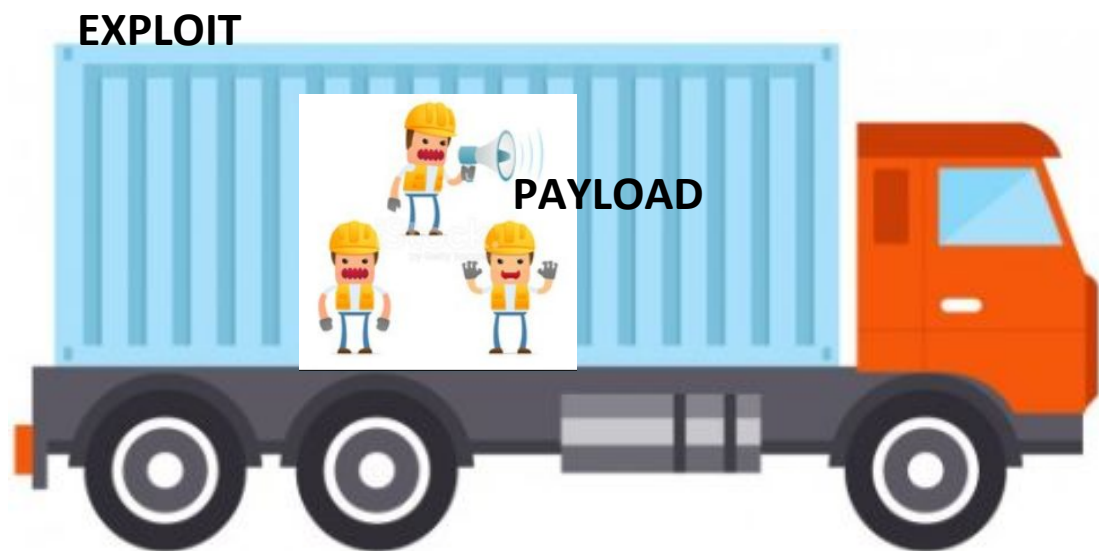




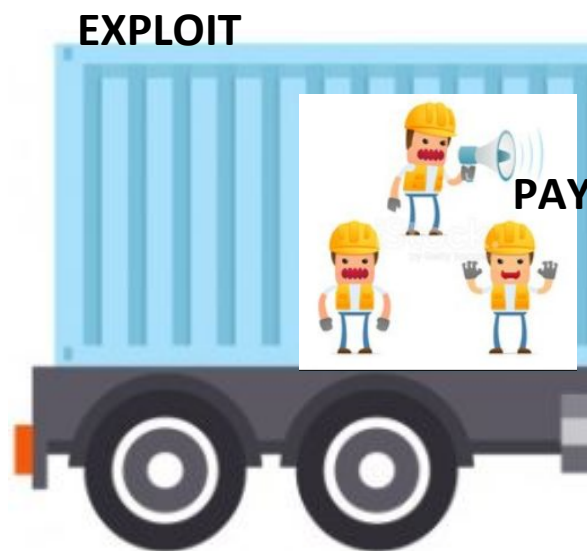
## ¿Que es el análisis de vulnerabilidades?

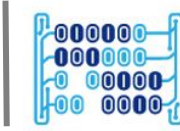
Es la identificación de loopholes [vacíos, rendijas, brechas, etc.] en las **redes** de comunicaciones, los **sistemas operativos** o los **aplicativos** de una empresa objetivo, con el fin de poder realizar una explotación posterior











## ¿Porque realizar análisis de vulnerabilidades en una empresa?

Para identificar **nuevas** tendencias en amenazas y/o ataques

Para obtener información que me ayude a **prevenir** problemas de seguridad

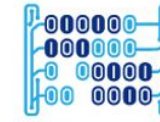
Para identificar **debilidades actuales** en mi red, sistemas operativos o software

Para saber como **recuperarme** en caso de un ataque



## Tipos de vulnerabilidades

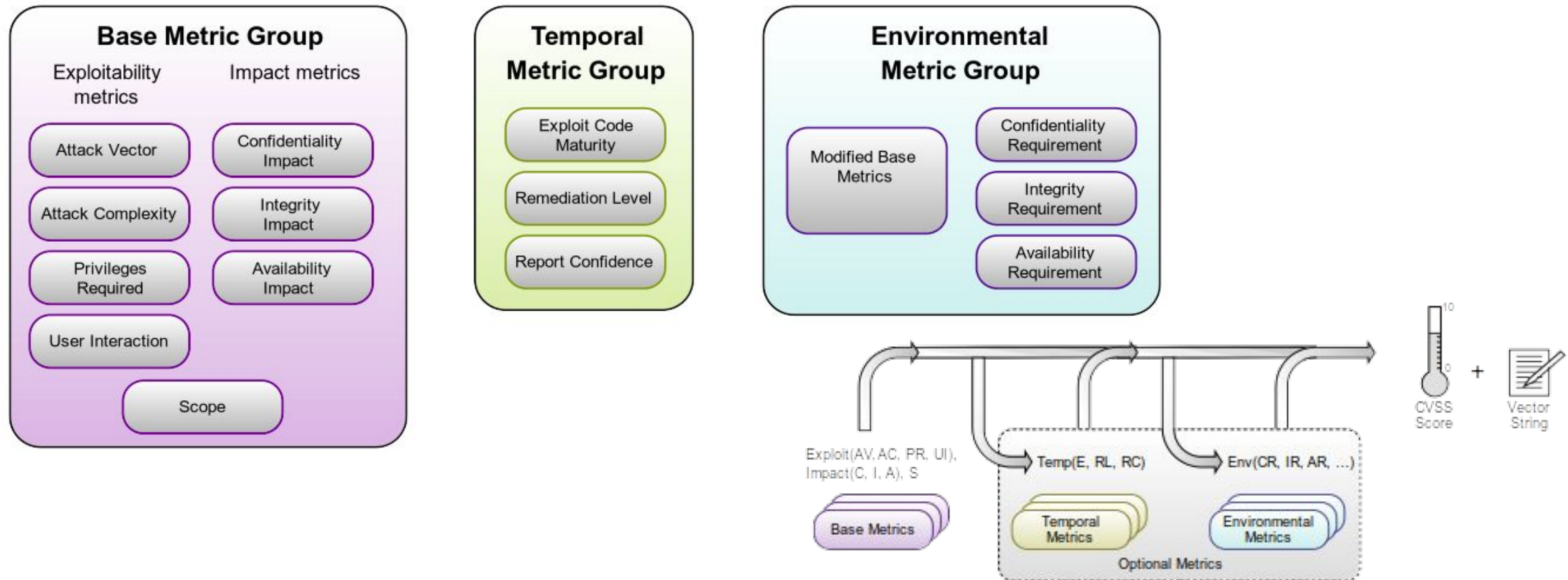
1. Malas configuraciones
  2. Instalaciones por defecto
  3. Buffer overflow
  4. Servidores sin [parches, actualizaciones] de seguridad
  5. Errores de diseño
  6. Errores en sistemas operativos
  7. Errores en aplicativos
  8. Servicios abiertos
  9. Passwords por defecto
1. Un webserver que permita transferencia de datos sensibles por protocolos no seguros (mejor https que http)
  2. Aplicativos con módulos innecesarios (instalados por default)
  3. Entradas de datos que superan el tamaño de las variables en el código
  4. Servidores sin *service packs* o *security updates*
  5. Aplicativos que utilizan esquemas de cifrado débiles
  6. Sistemas operativos sin software antimalware
  7. Aplicativos con vulnerabilidades de inyección de código
  8. Un webserver con puertos abiertos sin necesidad (ssh, telnet)
  9. Uso de passwords posibles de encontrar en un diccionario o repetidos



## Soluciones de evaluación de vulnerabilidades

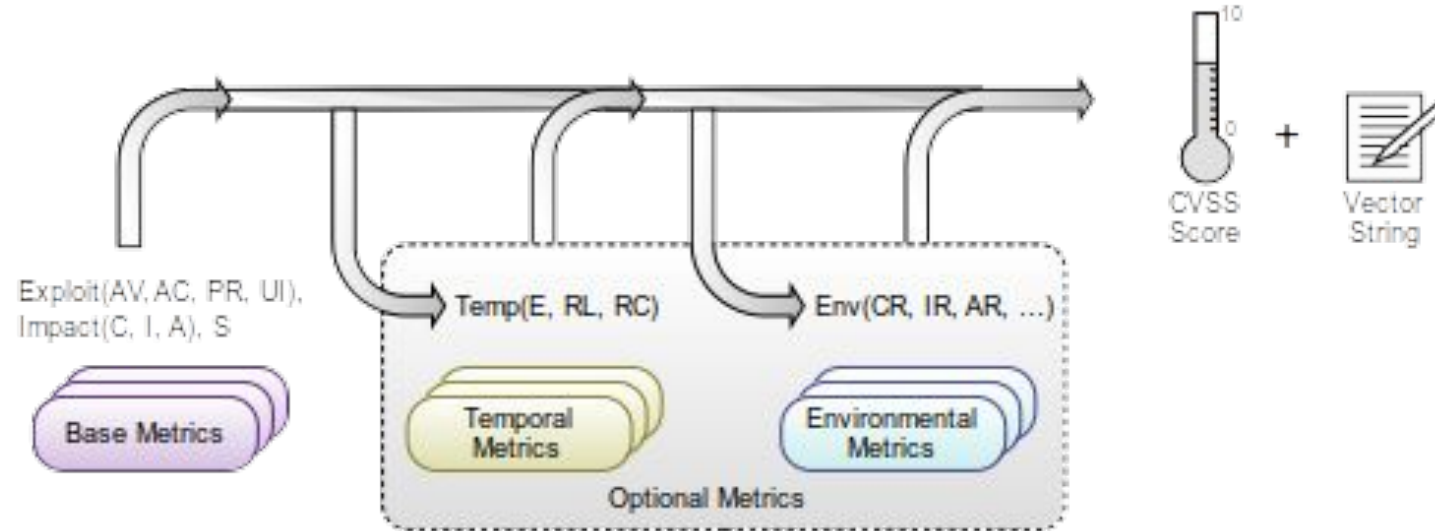
## Sistemas de *scoring* de vulnerabilidades

- Los sistemas de *scoring* nos permiten evaluar la **severidad** y el **riesgo** asociado de cada vulnerabilidad.
- CVSS (Common Vulnerability Scoring System) es el sistema de scoring mas común
- El NVD (National Vulnerability Database) calcula los valores de CVSS para cada vulnerabilidad. <https://nvd.nist.gov/>





## Sistemas de *scoring* de vulnerabilidades



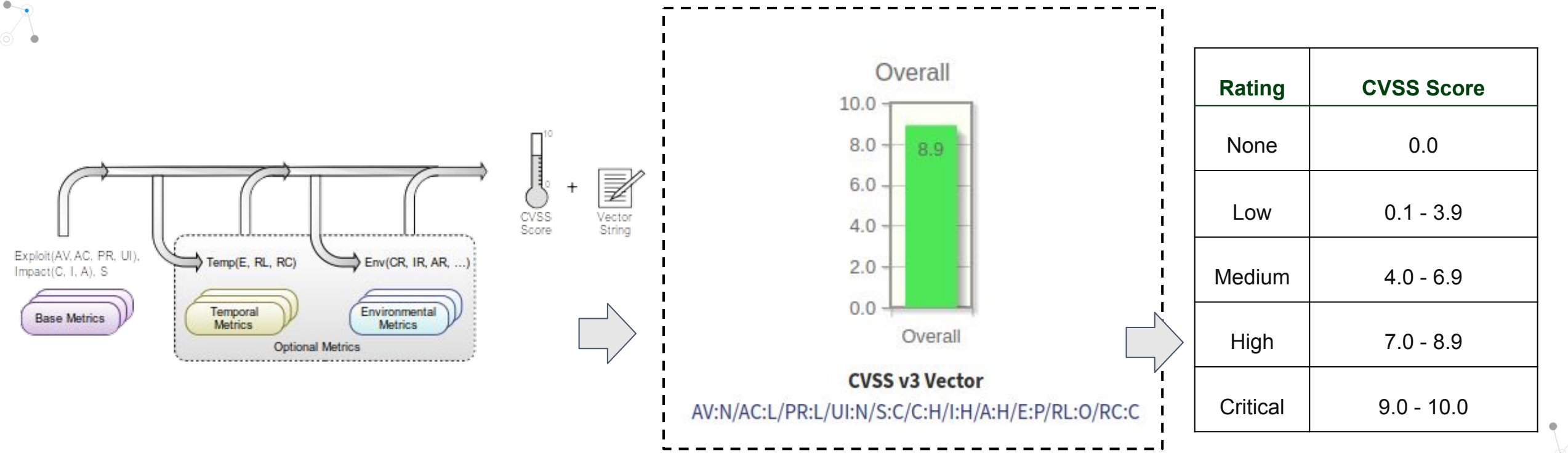
$$\text{Impact Sub-Score (ISS)} = 1 - [ (1 - \text{Confidentiality}) \times (1 - \text{Integrity}) \times (1 - \text{Availability}) ]$$

$$\text{TemporalScore} = \text{Roundup} (\text{BaseScore} \times \text{ExploitCodeMaturity} \times \text{RemediationLevel} \times \text{ReportConfidence})$$

$$\text{Modified Impact Sub-Score (MISS)} = \text{Minimum} ( 1 - [ (1 - \text{ConfidentialityRequirement} \times \text{ModifiedConfidentiality}) \times (1 - \text{IntegrityRequirement} \times \text{ModifiedIntegrity}) \times (1 - \text{AvailabilityRequirement} \times \text{ModifiedAvailability}) ], 0.915)$$



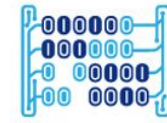
## Sistemas de *scoring* de vulnerabilidades



Conectarse a la siguiente URL para probar la calculadora de CVSS de NIST:

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C>





## Sistemas de *scoring* de vulnerabilidades

CVSS (Common Vulnerability Scoring System): El NVD (National Vulnerability Database) calcula los valores de CVSS para cada vulnerabilidad. <https://nvd.nist.gov/>

**Vector de Acceso (AV):** Métrica asociada al tipo de acceso por medio del cual la vulnerabilidad puede ser explotada.

Valor	Descripción
<b>Local (L)</b>	La vulnerabilidad puede ser explotada teniendo acceso físico al sistema objetivo o una cuenta local.
<b>Red Adyacente (A)</b>	La vulnerabilidad puede ser explotada accediendo al dominio de colisión o dominio de broadcast del sistema objetivo.
<b>Red (N)</b>	La vulnerabilidad se encuentra en un nivel de capa de red, o uno superior en el modelo OSI. Corresponde a vulnerabilidades explotadas remotamente.

**Complejidad de explotación (AC):** Métrica asociada a la facilidad de explotación de la vulnerabilidad.

Valor	Descripción
<b>Alto (H)</b>	Se requiere una ventana de tiempo específica para la explotación, y/o el uso de técnicas complementarias como ingeniería social.
<b>Medio (M)</b>	Se requiere cumplir algunos requisitos para la explotación como características técnicas específicas del origen del ataque o del sistema objetivo.
<b>Bajo (B)</b>	No se requiere el cumplimiento de condiciones especiales para la explotación y la vulnerabilidad podría ser explotada desde diferentes orígenes.





## Sistemas de *scoring* de vulnerabilidades

CVSS (Common Vulnerability Scoring System): El NVD (National Vulnerability Database) calcula los valores de CVSS para cada vulnerabilidad. <https://nvd.nist.gov/>

**Autenticación (Au):** Describe el número de veces que se requiere un proceso de autenticación para lograr explotar la vulnerabilidad.

Valor	Descripción
<b>Múltiple (M)</b>	Se requiere que el atacante se autentique dos o más veces
<b>Simple (S)</b>	Se requiere que el atacante se autentique una vez
<b>Ninguna (N)</b>	No se requiere autenticación del atacante

**Confidencialidad (C):** Describe el impacto causado al activo de información en términos de confidencialidad.

Valor	Descripción
<b>Ninguna (N)</b>	No hay impacto sobre la confidencialidad del sistema
<b>Parcial (P)</b>	La confidencialidad del activo se ve afectada de forma parcial. La visualización no autorizada se da sobre un conjunto de los datos.







## Sistemas de *scoring* de vulnerabilidades

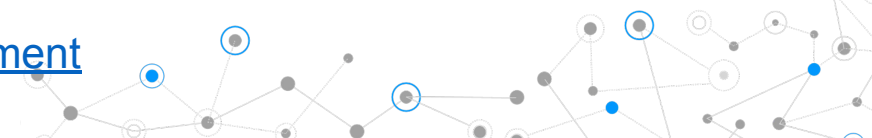
CVSS (Common Vulnerability Scoring System): El NVD (National Vulnerability Database) calcula los valores de CVSS para cada vulnerabilidad. <https://nvd.nist.gov/>

**Integridad (I):** Describe el impacto causado al activo de información en términos de integridad.

**Disponibilidad (A):** Cuantifica el impacto sobre la disponibilidad de los recursos del activo de información objetivo, tales como capacidad de procesador, almacenamiento, ancho de banda, etc.

Valor	Descripción
<b>Ninguna (N)</b>	No hay impacto sobre la integridad del sistema
<b>Parcial (P)</b>	La integridad del activo se ve afectada de forma parcial. La modificación de los activos se puede dar pero con ciertas limitaciones.
<b>Completo (C)</b>	La integridad del activo se ve afectada de forma total, bien sea porque se desencadena alguna modificación o eliminación no autorizada.

Valor	Descripción
<b>Ninguna (N)</b>	No hay impacto sobre la disponibilidad del sistema
<b>Parcial (P)</b>	La disponibilidad del activo se ve afectada de forma parcial, impactado algún aspecto del desempeño del activo.
<b>Completo (C)</b>	La disponibilidad del activo se ve afectada de forma total



## Sistemas de *scoring* de vulnerabilidades

**Ejemplo: Vulnerabilidad CVE-2004-0492 ocasionada por Apache Tomcat 1.3.26 -1.3.32**

**Descripción:** Versión de apache vulnerable a bufferoverflow en proxy\_útil.c para servidores con mod\_proxy habilitado y configurado.

**Impacto:** Generación de denegación de servicio y posible ejecución de código malicioso en el servidor

**Fecha de publicación de la vulnerabilidad:** 2004/06/10

CVE: CVE-2004-0492

OSVDB: 6839

RHSA: 2004:245

SECUNIA: 11841, 11854, 11859, 11866, 11917,  
11946, 11957, 11968, 12971, 13115

BID: 10508

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVSS Temporal Score: 8.3

Detalles de la vulnerabilidad:

- <https://nvd.nist.gov/vuln/detail/CVE-2004-0492>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0492>
- <https://www.securityfocus.com/bid/10508/info>

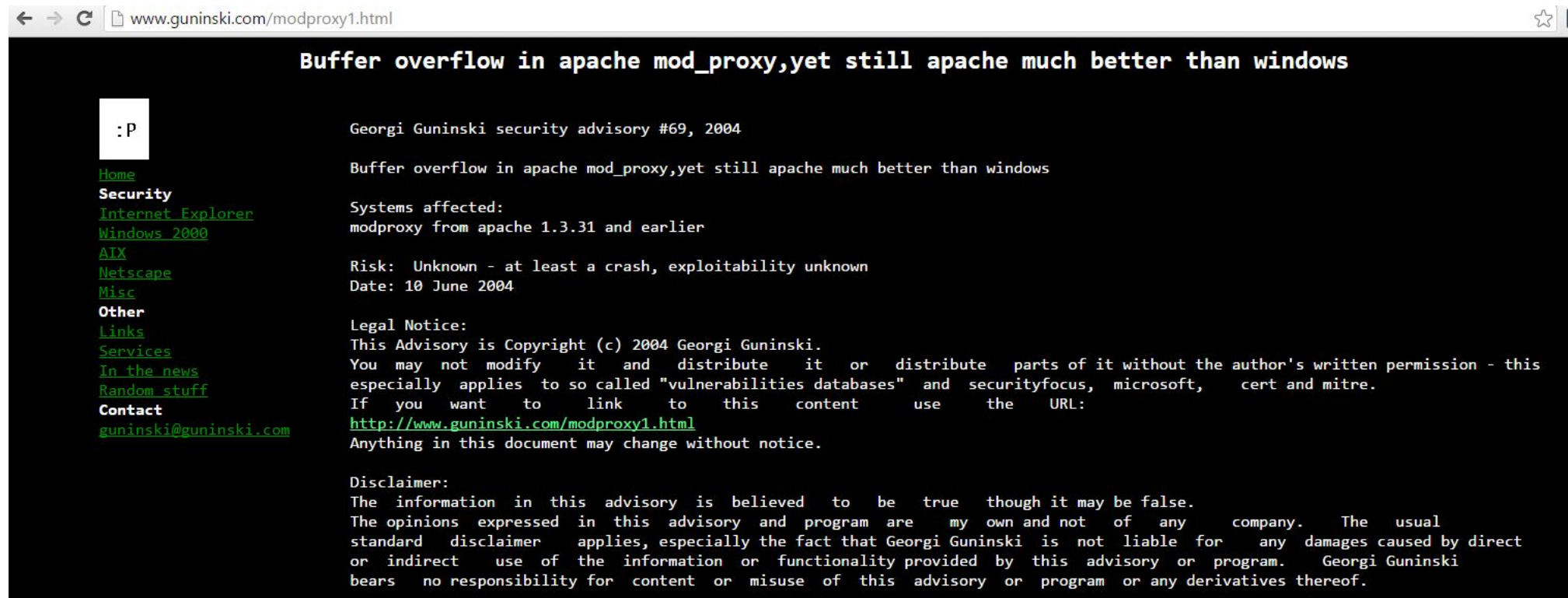
-> ¿Exploit disponible?

## Sistemas de *scoring* de vulnerabilidades

**Ejemplo: Vulnerabilidad CVE-2004-0492 ocasionada por Apache Tomcat 1.3.26 -1.3.32**

**Causa:** Un servidor remoto retorna un valor de tamaño de contenido negativo, el cual puede ser utilizado en una operación de copiado, generando una corrupción de memoria.

**Exploit:**



The screenshot shows a web browser window with the address bar displaying "www.guninski.com/modproxy1.html". The page content is a security advisory titled "Buffer overflow in apache mod\_proxy,yet still apache much better than windows". On the left side, there is a navigation menu with links: Home, Security, Internet Explorer, Windows 2000, AIX, Netscape, Misc, Other, Links, Services, In the news, Random stuff, and Contact. The main content area contains the following text:

```
Georgi Guninski security advisory #69, 2004

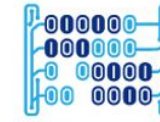
Buffer overflow in apache mod_proxy,yet still apache much better than windows

Systems affected:
modproxy from apache 1.3.31 and earlier

Risk: Unknown - at least a crash, exploitability unknown
Date: 10 June 2004

Legal Notice:
This Advisory is Copyright (c) 2004 Georgi Guninski.
You may not modify it and distribute it or distribute parts of it without the author's written permission - this
especially applies to so called "vulnerabilities databases" and securityfocus, microsoft, cert and mitre.
If you want to link to this content use the URL:
http://www.guninski.com/modproxy1.html
Anything in this document may change without notice.

Disclaimer:
The information in this advisory is believed to be true though it may be false.
The opinions expressed in this advisory and program are my own and not of any company. The usual
standard disclaimer applies, especially the fact that Georgi Guninski is not liable for any damages caused by direct
or indirect use of the information or functionality provided by this advisory or program. Georgi Guninski
bears no responsibility for content or misuse of this advisory or program or any derivatives thereof.
```



## Herramientas de análisis de vulnerabilidades

- Qualys
- Nessus Professional
- GFI LanGuard
- Qualys freescan
- Nikto
- OpenVAS
- Retinca CS
- SAINT
- MBSA (Microsoft Baseline Security Analyzer)



## Reporte de análisis de vulnerabilidades

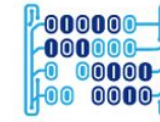
### Laboratorio

- Acceda a la página <https://www.securityfocus.com/> e identifique 3 vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad. Para cada una de ellas especificar
  - CVE
  - Interpretación completa del Score y Vector CVSS
  - Identificar si existe algún exploit para cada vulnerabilidad
- Utilice la herramienta Nessus Essentials para realizar un análisis de vulnerabilidades de ZICO
- Por cada vulnerabilidad de prioridad alta identificada por Nessus, defina un plan de remediación (Los planes de remediación son las acciones que se deben aplicar para cerrar las vulnerabilidades)

# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

## 1. Regístrese para obtener un código de activación

→ ↻ es-la.tenable.com/products/nessus/nessus-essentials?tns\_redirect=true ☆ 1

Descargas Blog Contacto Inicio de sesión Español (América Latina)

 Cyber Exposure Productos Soluciones Investigación Servicios Compañía Socios [Prueba gratuita](#) [Compre ahora](#)



Como parte de la familia Nessus, Nessus® Essentials (anteriormente, Nessus Home) le permite escanear su entorno (hasta 16 direcciones IP por escáner) con la misma alta velocidad, evaluaciones a profundidad y comodidad de escaneo sin agente que disfrutaron los suscriptores de Nessus. Nessus Essentials elimina la restricción anterior de usar Nessus Home únicamente para uso personal no comercial.

### Regístrese para obtener un código de activación

Nombre \* Apellido \*

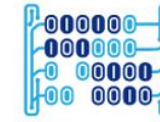
Daniel Díaz

Correo electrónico \*

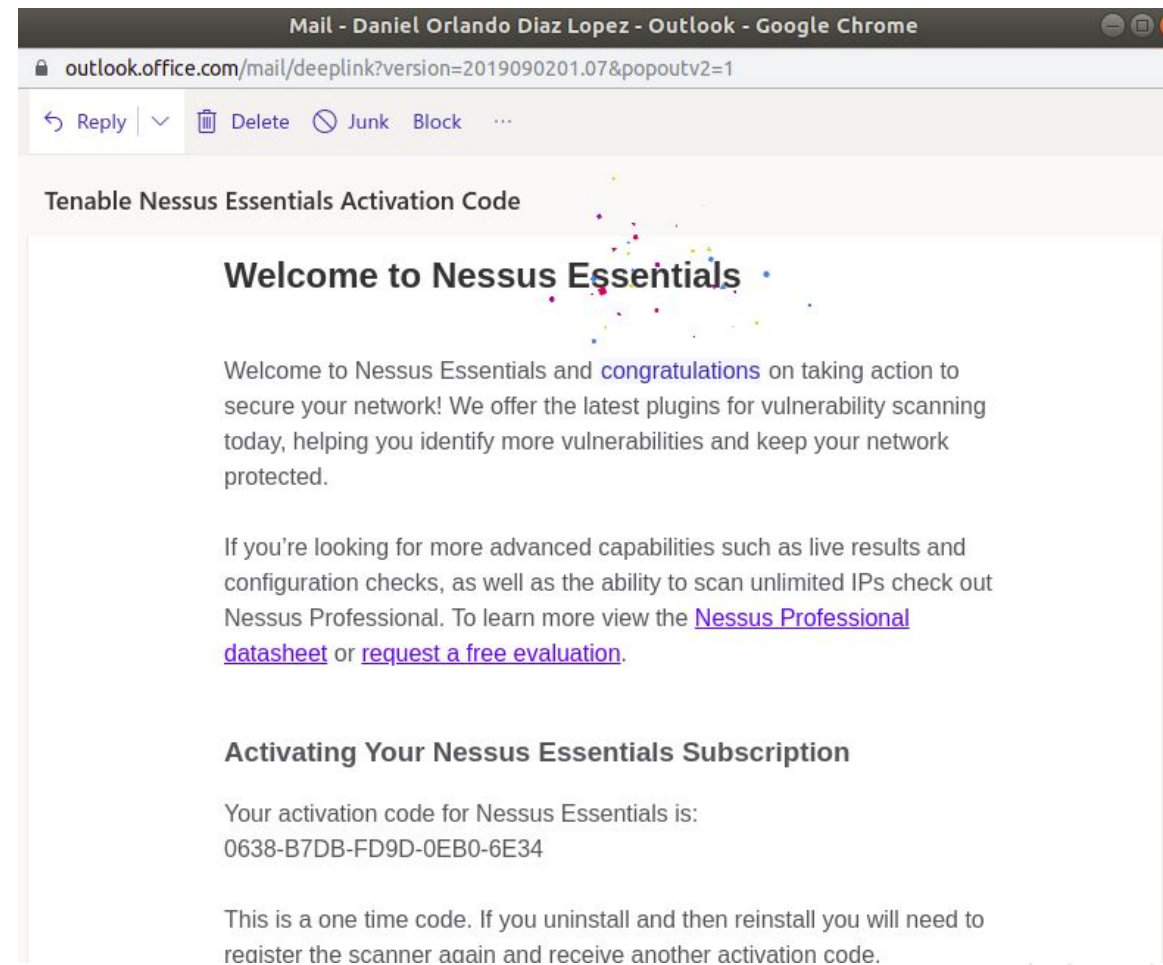
danielo.diaz@urosario.edu.co

☐ Marque para recibir actualizaciones de Tenable

[Registrarse](#)



## 2. El código de activación llegará al email registrado





## 3. Instalar Nessus en Kali Linux (Validar que tenga conectividad a Internet)

- Descargar **Nessus-8.6.0-debian6\_amd64.deb** desde la siguiente página <https://www.tenable.com/downloads/nessus>
- Instalar Nessus con el siguiente comando:  
**sudo dpkg -i Nessus-8.3.2-debian6\_amd64.deb**
- Iniciar Nessus con el siguiente comando:
  - `/etc/init.d/nessusd start`
- Abrir un navegador y acceder a la siguiente URL: **https://kali:8834**
- Crear una cuenta y e ingresar el código de activación que se obtuvo por correo en el paso previo



## Instalación del paquete .deb e inicio del Nessusd

```
root@kali:~# pwd
/root
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls
Nessus-8.6.0-debian6_amd64.deb  VBoxLinuxAdditions.run
root@kali:~/Downloads# dpkg -i Nessus-8.6.0-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 357989 files and directories currently installed.)
Preparing to unpack Nessus-8.6.0-debian6_amd64.deb ...
Unpacking nessus (8.6.0) ...
Setting up nessus (8.6.0) ...
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (239-10) ...
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~/Downloads#
```

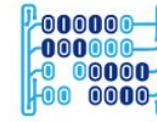
Firefox can't establish a connection to the server at https://localhost:8834/

- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

# Uso de Nessus para escaneo de vulnerab.

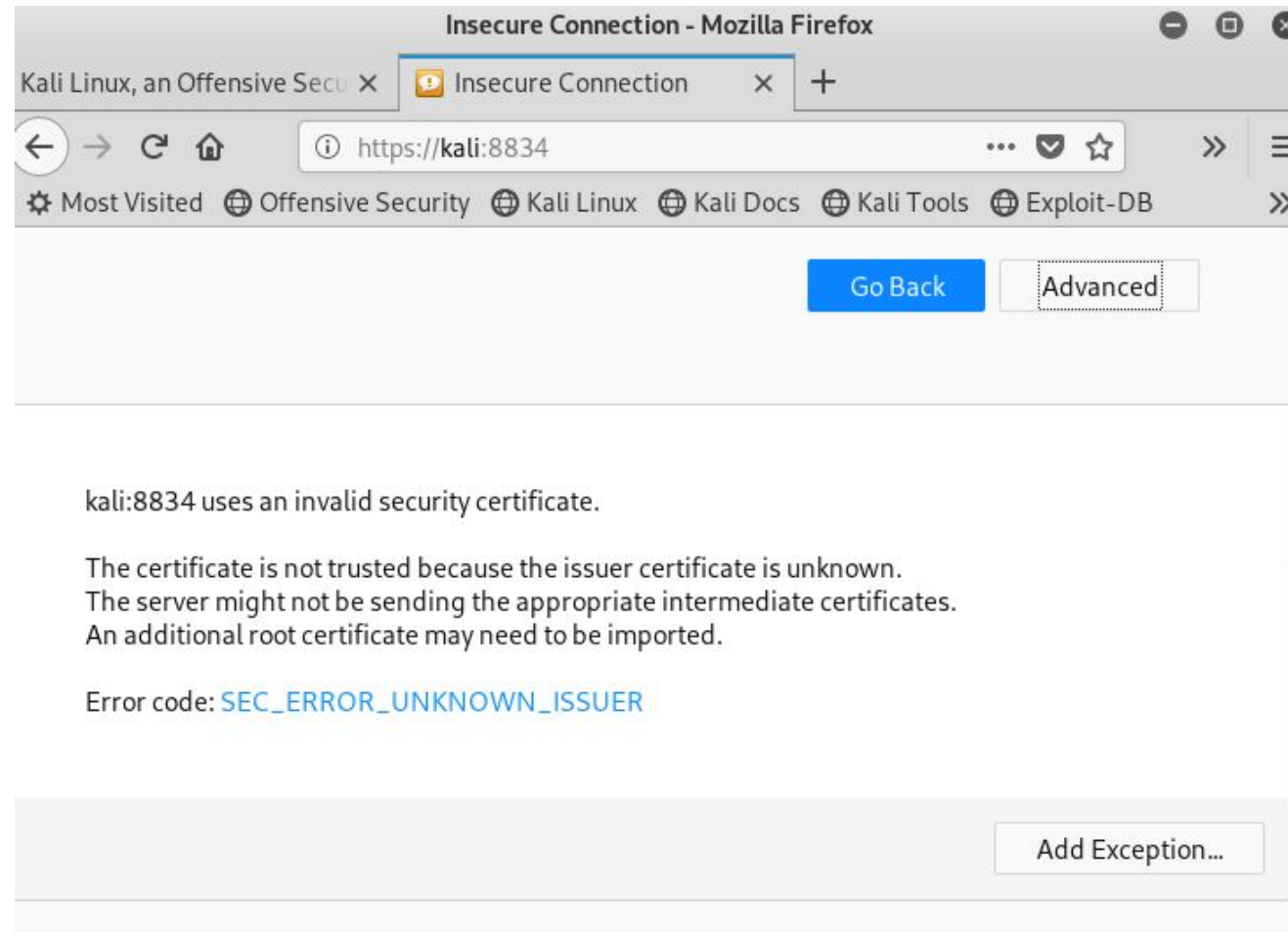


Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

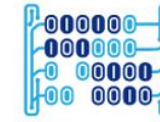
Acceso a la URL de Nessus <https://kali:8834>



# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

Agregar excepción de seguridad para permitir la conexión hacia Nessus por el protocolo https

**Add Security Exception**

You are about to override how Firefox identifies this site.  
Legitimate banks, stores, and other public sites will not ask you to do this.

**Server**

Location:

**Certificate Status**

This site attempts to identify itself with invalid information.

**Unknown Identity**

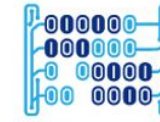
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☒ Permanently store this exception

# Uso de Nessus para escaneo de vulnerab.

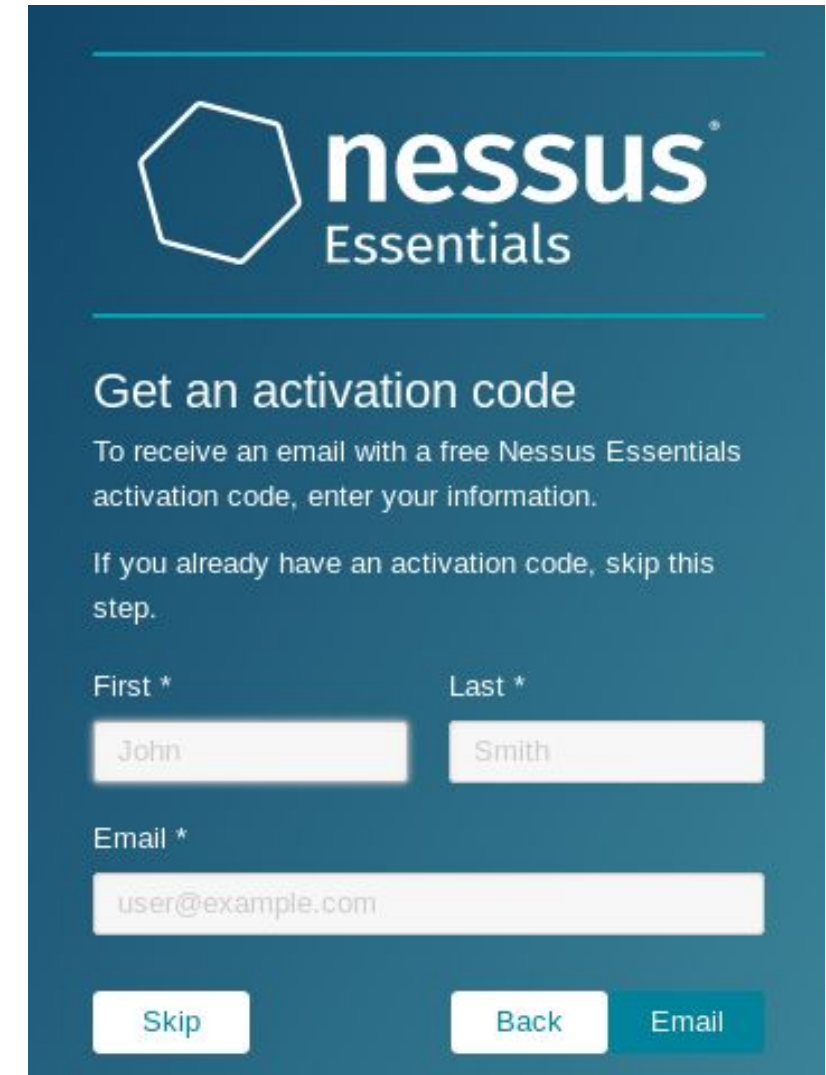
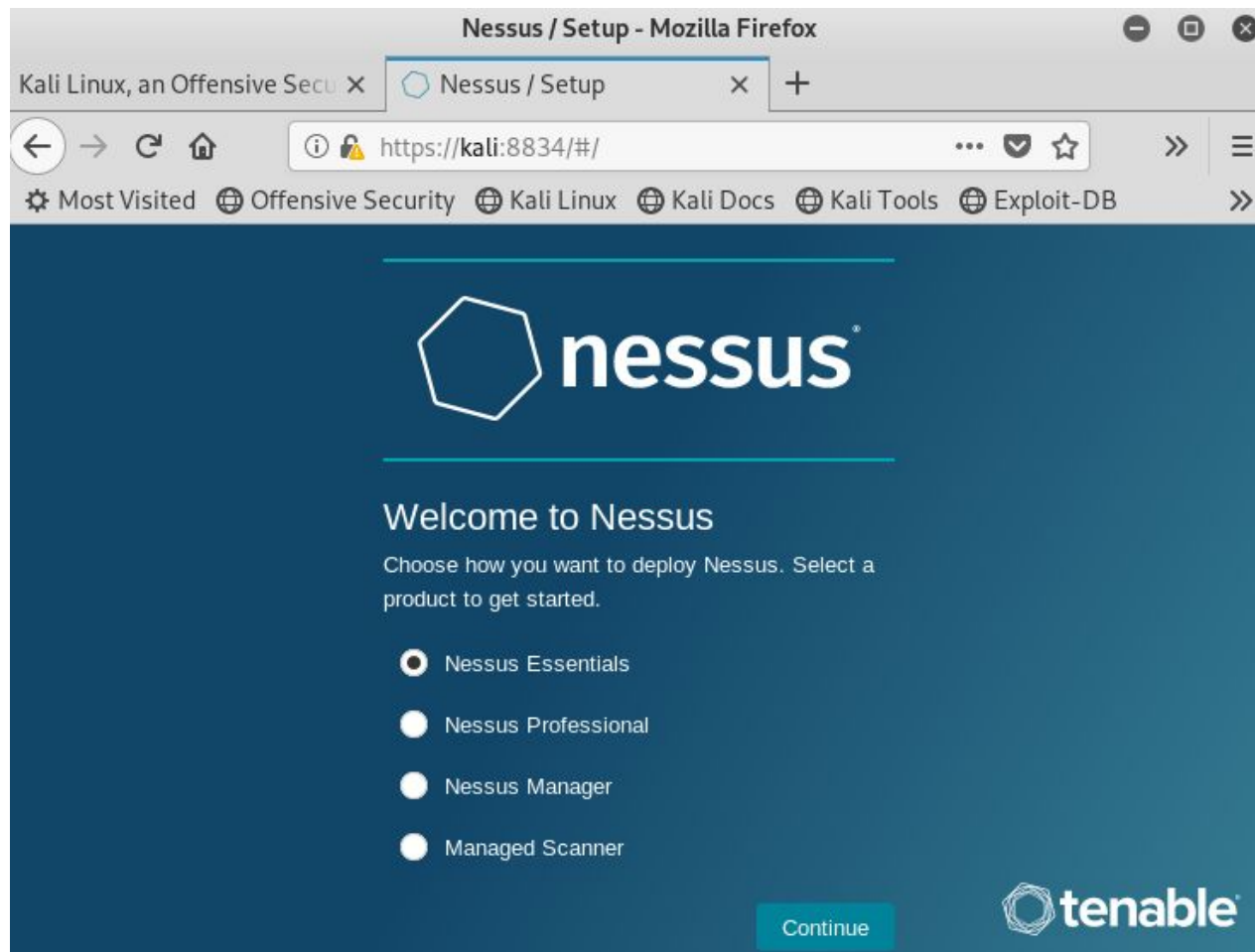


Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

Selección de la versión de Nessus a instalar (Nessus Essentials) e ingreso del código de activación

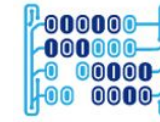




# Uso de Nessus para escaneo de vulnerab.

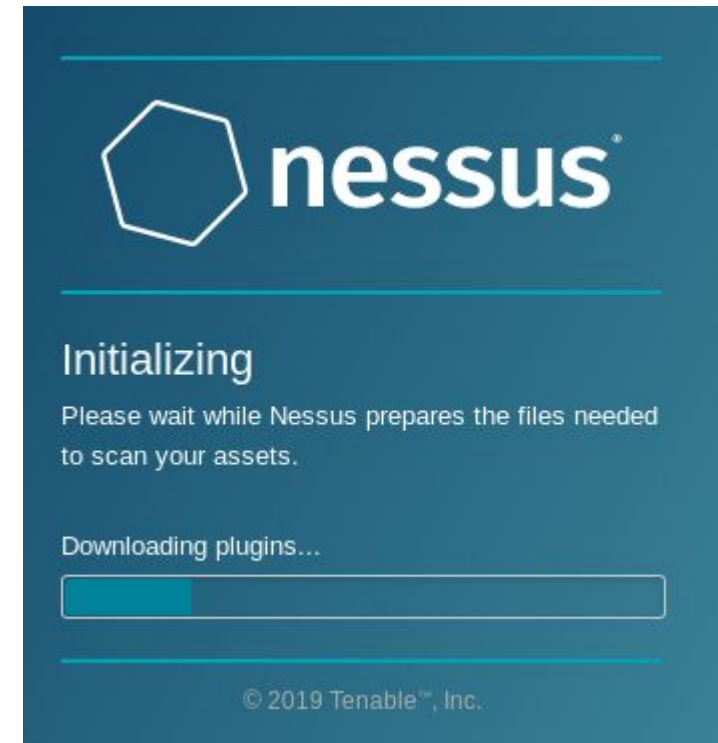
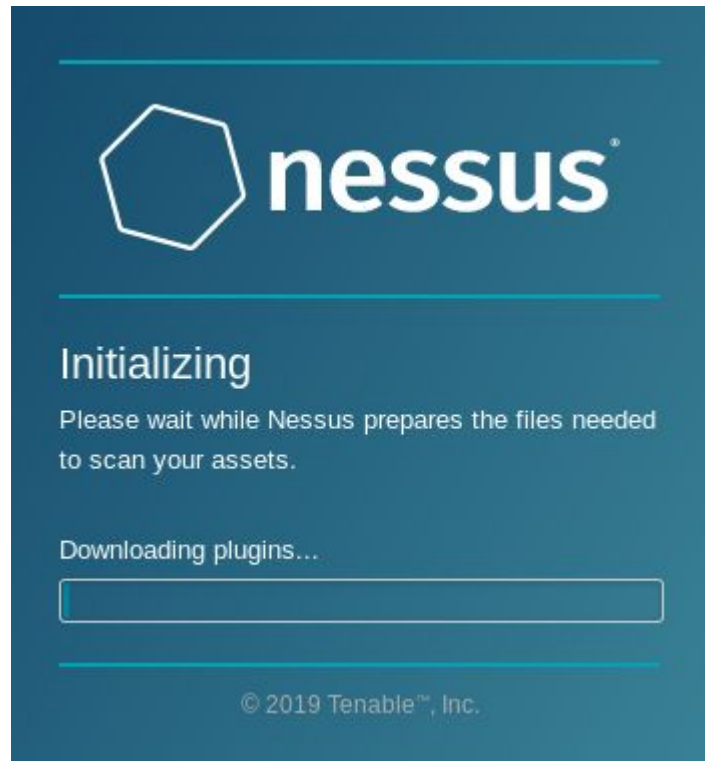


Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

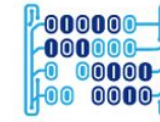
Descarga de todos los plugins de Nessus



# Uso de Nessus para escaneo de vulnerab.

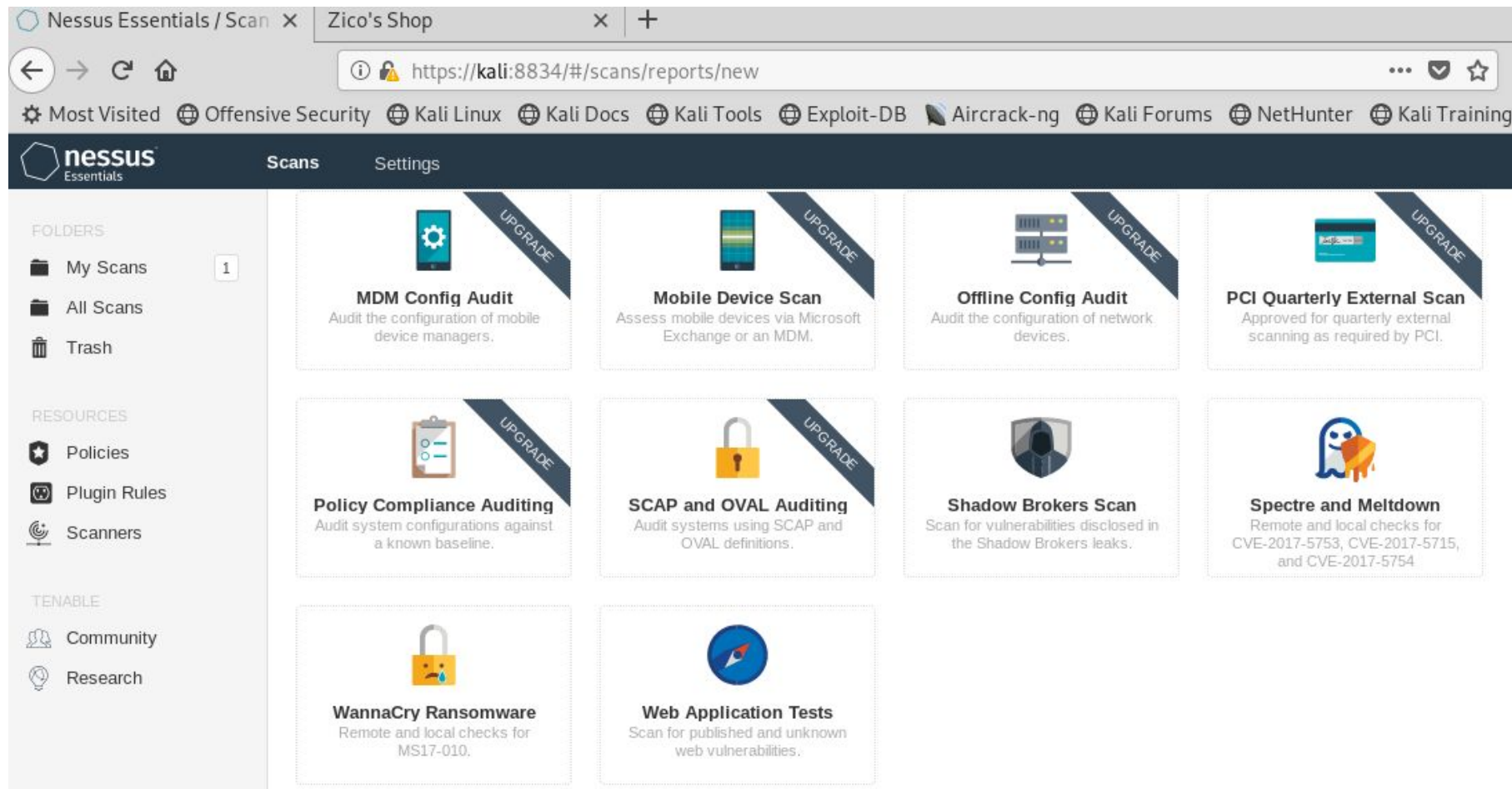


Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

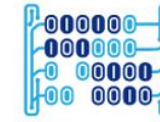
Despues de la descarga ya puede acceder a Nessus por medio de la <https://kali:8834> y explorar todas sus funcionalidades



# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**

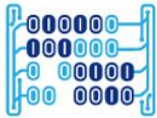
Matemáticas Aplicadas y  
Ciencias de la Computación

En este punto ya debe colocar la máquina Kali Linux en configuración “Host Only” y levantar la máquina de Zico para poder hacerle el análisis de vulnerabilidades

The screenshot shows the Nessus Essentials web interface in a browser window. The address bar displays the URL: `https://kali:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65`. The browser's bookmark bar includes links to 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', 'Kali Forums', and 'NetHunte'. The Nessus Essentials header is visible, with 'Scans' and 'Settings' tabs. A left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Scanners). The main content area shows the 'Settings' tab for a new scan named 'zico'. The 'BASIC' section is expanded, showing 'General' settings. The 'Name' field is 'zico', the 'Description' field is empty, the 'Folder' is 'My Scans', and the 'Targets' field contains the IP address '192.168.56.102'. Other sections like 'Schedule', 'Notifications', 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED' are collapsed.



# Uso de Nessus para escaneo de vulnerab.



Configure un escaneo de tipo “Basic Network” y uno de tipo “Web Application Test” sobre la IP de Zico, ejecútelo y espere hasta que Nessus termine indicándole las vulnerabilidades encontradas

My Scans

More

Import

New Folder

New Scan

Search Scans

1 Scan (1 Selected) Clear Selected Item

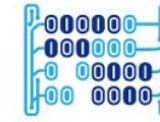
<input checked="" type="checkbox"/>	Name	Schedule	Last Modified
<input checked="" type="checkbox"/>	zico	On Demand	N/A



# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

Por cada vulnerabilidad de prioridad crítica y alta identificada por Nessus, defina un plan de remediación (Los planes de remediación son las acciones que se deben aplicar para cerrar las vulnerabilidades)

The screenshot displays the Nessus Essentials web interface. The browser address bar shows the URL `https://kali:8834/#/scans/reports/5/vulnerabilities`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Scanners', 'Community', and 'Research'. The main content area shows the scan results for 'Zico's Shop'. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (24), and 'History' (1). Below these is a search bar and a table of vulnerabilities.

Sev	Name	Family	Count
CRITICAL	Unix Operating System Unsupported Versi...	General	1
MIXED	SSH (Multiple Issues)	Misc.	4
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	RPC Services Enumeration	Service detection	4
INFO	HTTP (Multiple Issues)	Web Servers	3
INFO	Nessus SYN scanner	Port scanners	2

On the right side, the 'Scan Details' section shows: Policy: Basic Network Scan, Status: Running, Scanner: Local Scanner, and Start: Today at 8:13 AM. Below this is a 'Vulnerabilities' section with a donut chart and a legend indicating the severity levels: Critical (red), High (orange), Medium (yellow), and Low (green).

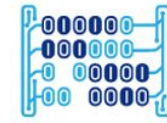




# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación



CRITICAL

Unix Operating System Unsupported Version Detection

>

Plugin Details

### Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

### Solution

Upgrade to a version of the Unix operating system that is currently supported.

### Output

```
Ubuntu 12.04 support ended on 2017-04-30.  
Upgrade to Ubuntu 18.10.  
  
For more information, see : https://wiki.ubuntu.com/Releases
```

Port ▲	Hosts
--------	-------

Severity:	Critical
ID:	33850
Version:	1.250
Type:	combined
Family:	General
Published:	August 8, 2008
Modified:	July 19, 2019

### Risk Information

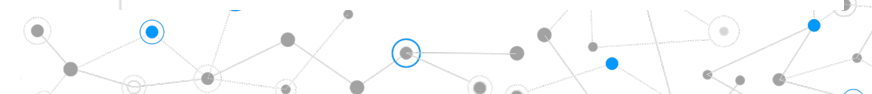
Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N  
/UI:N/S:C/C:H/I:H/A:H

CVSS Base Score: 10.0

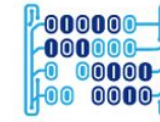
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
/I:C/A:C



# Uso de Nessus para escaneo de vulnerab.



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

Seleccionar todas las vulnerabilidades y exportar un reporte como PDF

**zico**  
[← Back to My Scans](#)

Snooze

Modify

Configure

Audit Trail

Launch

Report

- PDF
- HTML
- CSV

Hosts 1

Vulnerabilities 25

History 1

Filter

Search Vulnerabilities

25 Vulnerabilities (25 Selected) [Clear Selected Items](#)

<input checked="" type="checkbox"/>	Sev	Name	Family	Count		
<input checked="" type="checkbox"/>	CRITICAL	Unix Operating System U...	General	1		
<input checked="" type="checkbox"/>	MIXED	4 SSH (Multiple Issues)	Misc.	4		
<input checked="" type="checkbox"/>	MIXED	2 Apache HTTP Serve...	Web Servers	2		
<input checked="" type="checkbox"/>	INFO	RPC Services Enumeration	Service detection	4		
<input checked="" type="checkbox"/>	INFO	3 HTTP (Multiple Issues)	Web Servers	3		
<input checked="" type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	3		

**Scan Details**  
Policy: Basic Network Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 8:13 AM  
End: Today at 8:18 AM  
Elapsed: 5 minutes

**Vulnerabilities**  

- Critical
- High



Universidad del  
**Rosario**



**MACC**



**HINNT**

# ¡Gracias!