

# EJERCICIOS SEGURIDAD INFORMÁTICA

Universidad Nacional Autónoma de México



UNAM  
CUAUTEMOCIN

## INTEGRANTES

- Bautista Becerra Erika Monserrat
- Mejía Vargas Marco Antonio
- Mendoza Vázquez Jimmy Ross
- Grande Rincón José Jair
- Zamorano Rodríguez Luis Francisco

Prof. Rosalba Nancy Rosas Fonseca

## Indice

<b>Seguridad Informática - Ejercicio 1</b>	3
Objetivo.....	3
Requerimientos.....	3
Resultado esperado.....	4
<b>Seguridad Informática - Ejercicio 2</b>	5
Objetivo.....	5
Requerimientos.....	5
Resultado esperado.....	9
<b>Seguridad Informática - Ejercicio 3</b>	11
Objetivo.....	11
Requerimientos.....	11
Resultado esperado.....	13
<b>Seguridad Informática - Ejercicio 4</b>	14
Objetivo.....	14
Requerimientos.....	14
Resultado esperado.....	19
<b>Seguridad Informática - Ejercicio 5</b>	20
Objetivo.....	20
Requerimientos.....	20
Resultado esperado.....	23
<b>Seguridad Informática - Ejercicio 6</b>	24
Objetivo.....	24
Requerimientos.....	24
Resultado esperado.....	28

## Seguridad Informática - Ejercicio 1

Tema	5. Código Malicioso	Subtema	5.1.1 Dos y DDos (Negación de Servicio)
No. De Practica	1	Profesora	Rosalba Nancy Rosas Fonseca

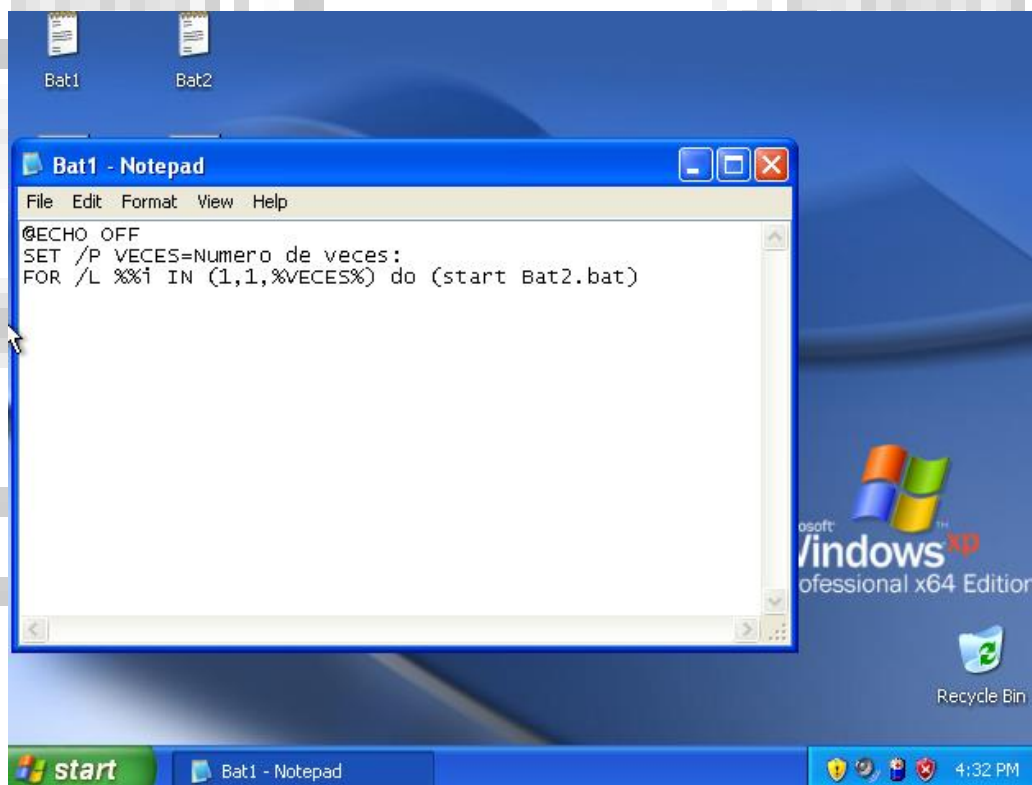
### Objetivo

En este ejercicio se demostrará la teoría básica detrás de un ataque DoS y DDoS generando peticiones excesivas a una sola IP, lo que puede saturarla.

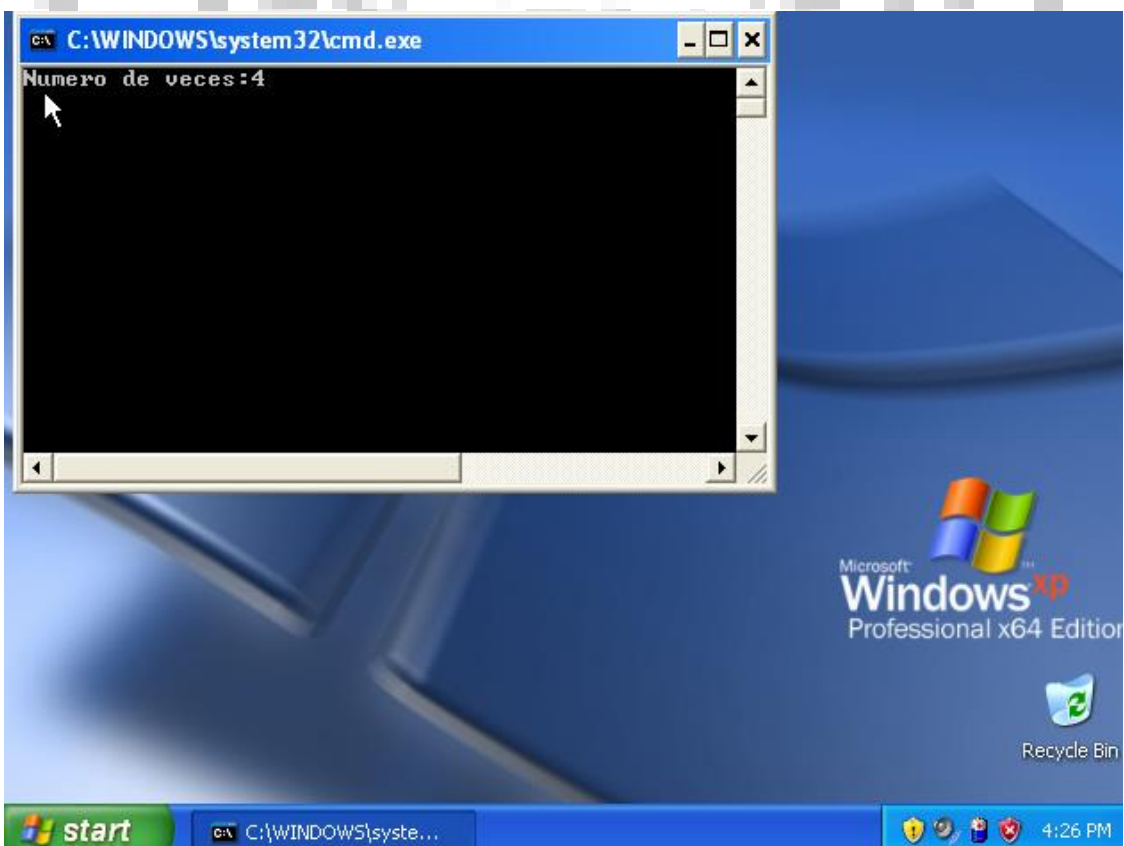
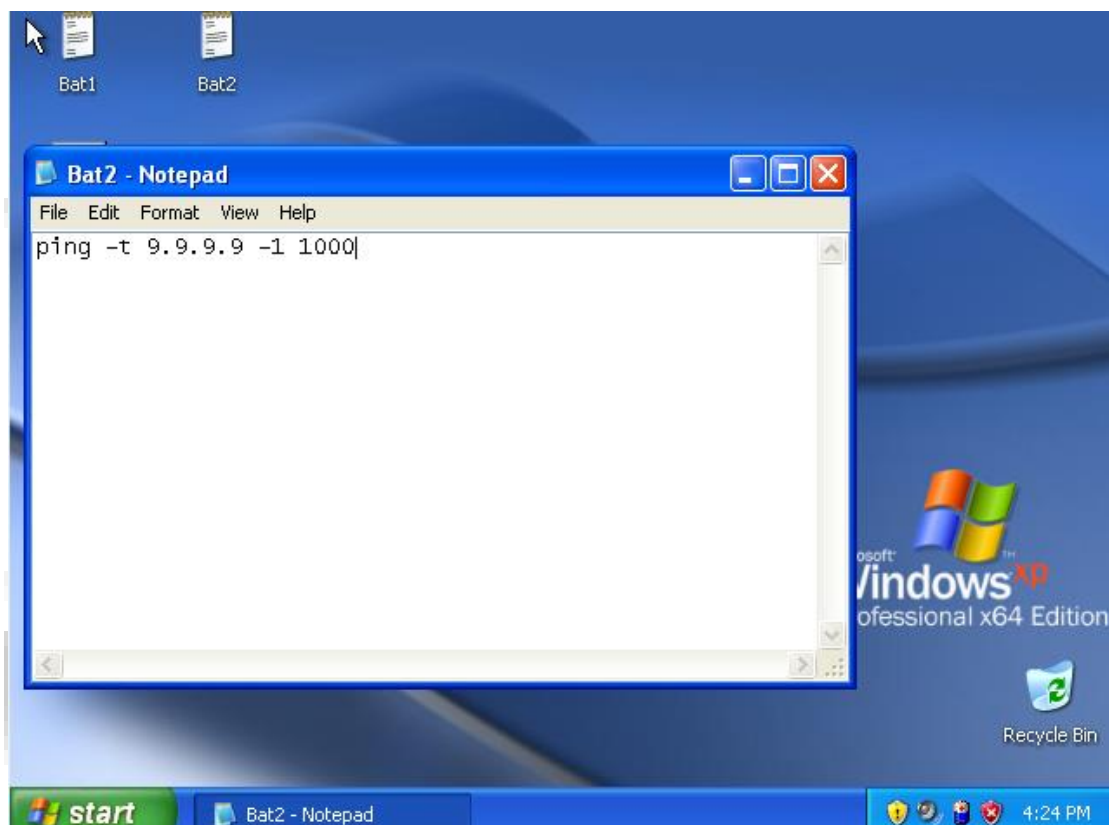
### Requerimientos

- Sistema Operativo Windows

### Procedimiento



UNAM  
CUAUTITLÁN

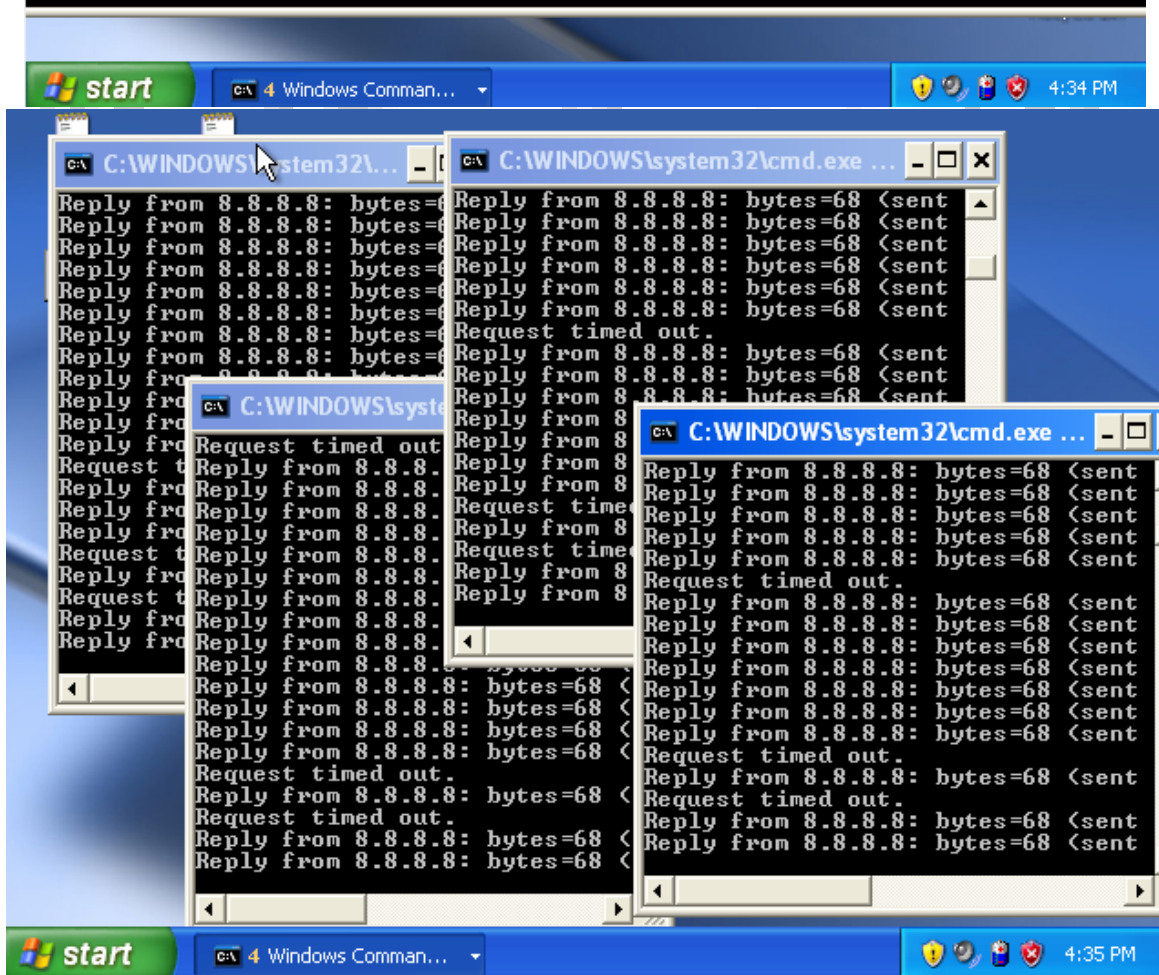


```
C:\WINDOWS\system32\cmd.exe - Bat2.bat
C:\WINDOWS\system32\cmd.exe - Bat2.bat
C:\WINDOWS\system32\cmd.exe - Bat2.bat

C:\Documents and Settings\Administrator\MARCO-LSJQ3Z9MC\Desktop>ping -t 8.8.8.8 -l 1000

Pinging 8.8.8.8 with 1000 bytes of data:

Reply from 8.8.8.8: bytes=68 <sent 1000> time=120ms TTL=54
Reply from 8.8.8.8: bytes=68 <sent 1000> time=64ms TTL=54
Reply from 8.8.8.8: bytes=68 <sent 1000> time=60ms TTL=54
Reply from 8.8.8.8: bytes=68 <sent 1000> time=69ms TTL=54
Reply from 8.8.8.8: bytes=68 <sent 1000> time=75ms TTL=54
Reply from 8.8.8.8: bytes=68 <sent 1000> time=71ms TTL=54
```



## Seguridad Informática - Ejercicio 2

Tema	5. Código Malicioso	Subtema	5.1.1 Dos y DDos (Negación de Servicio)
No. De Ejercicio	2	Profesora	Rosalba Nancy Rosas Fonseca

### Objetivo

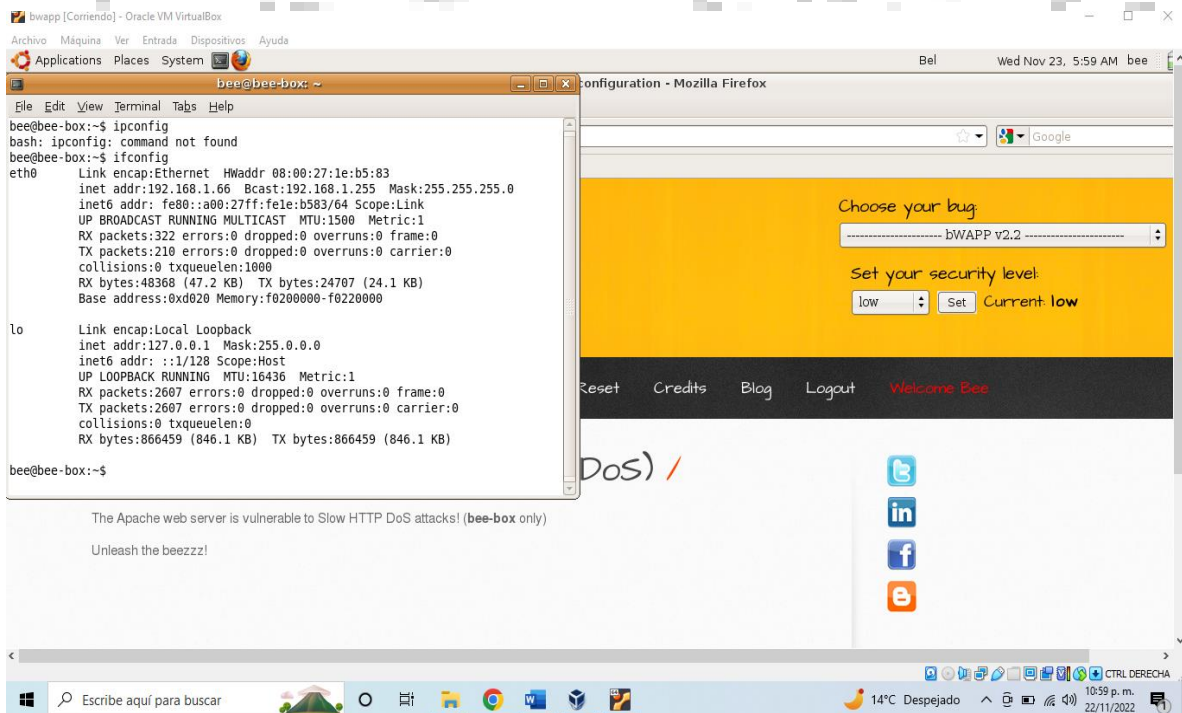
Realizar un ataque DDOS que deniegue un servicio web utilizando la herramienta bWapp, una distribución de Linux enfocada en la práctica de explotación y prevención de vulnerabilidades

### Requerimientos

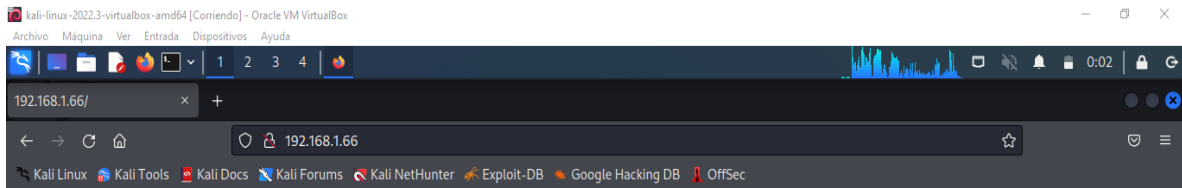
- Una Máquina virtual de bee-box (bWAPP), si tienes dudas de como instalarla, puedes seguir este tutorial.
- Una Máquina virtual de Kali Linux, si tienes dudas de como instalarla, puedes seguir este tutorial.

### Procedimiento



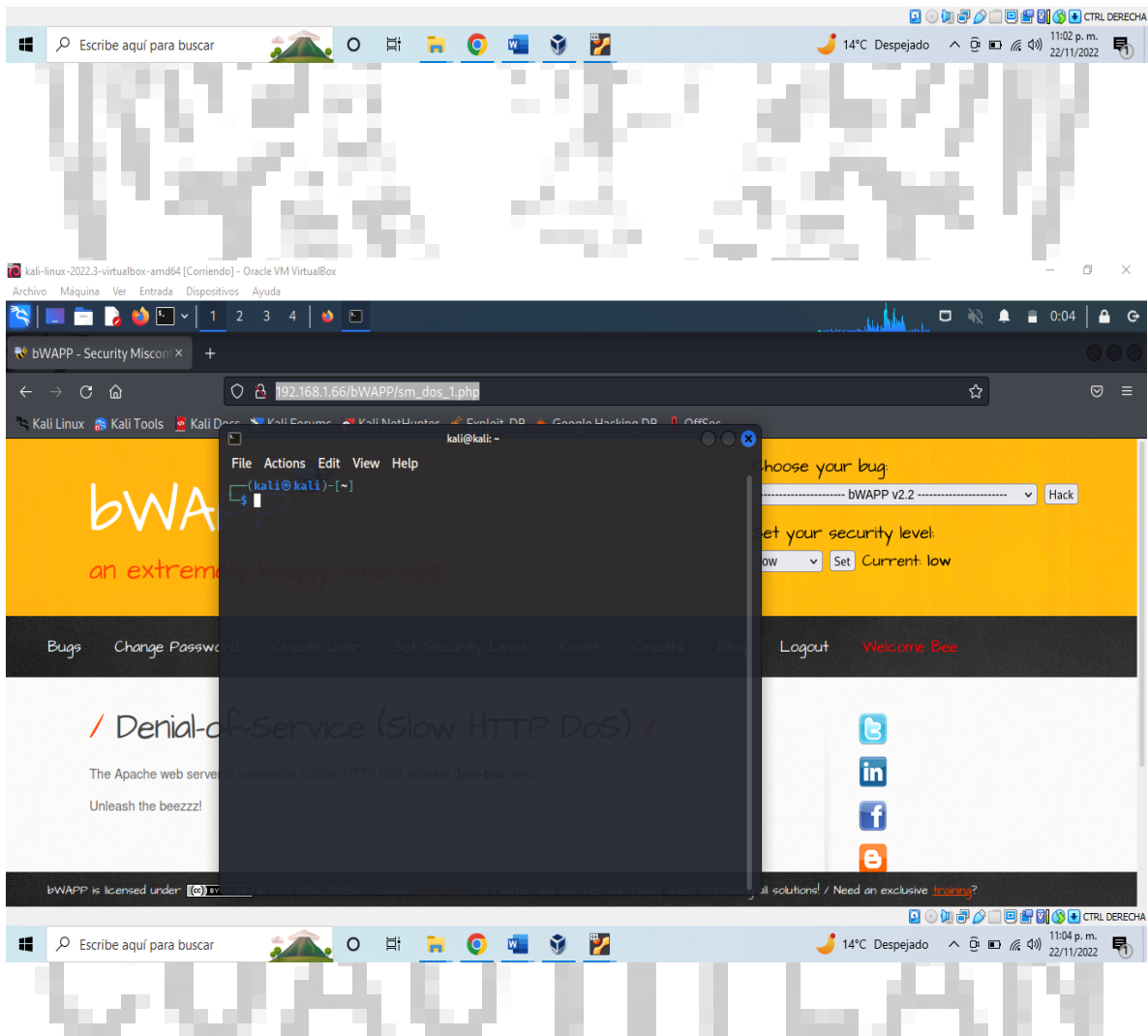




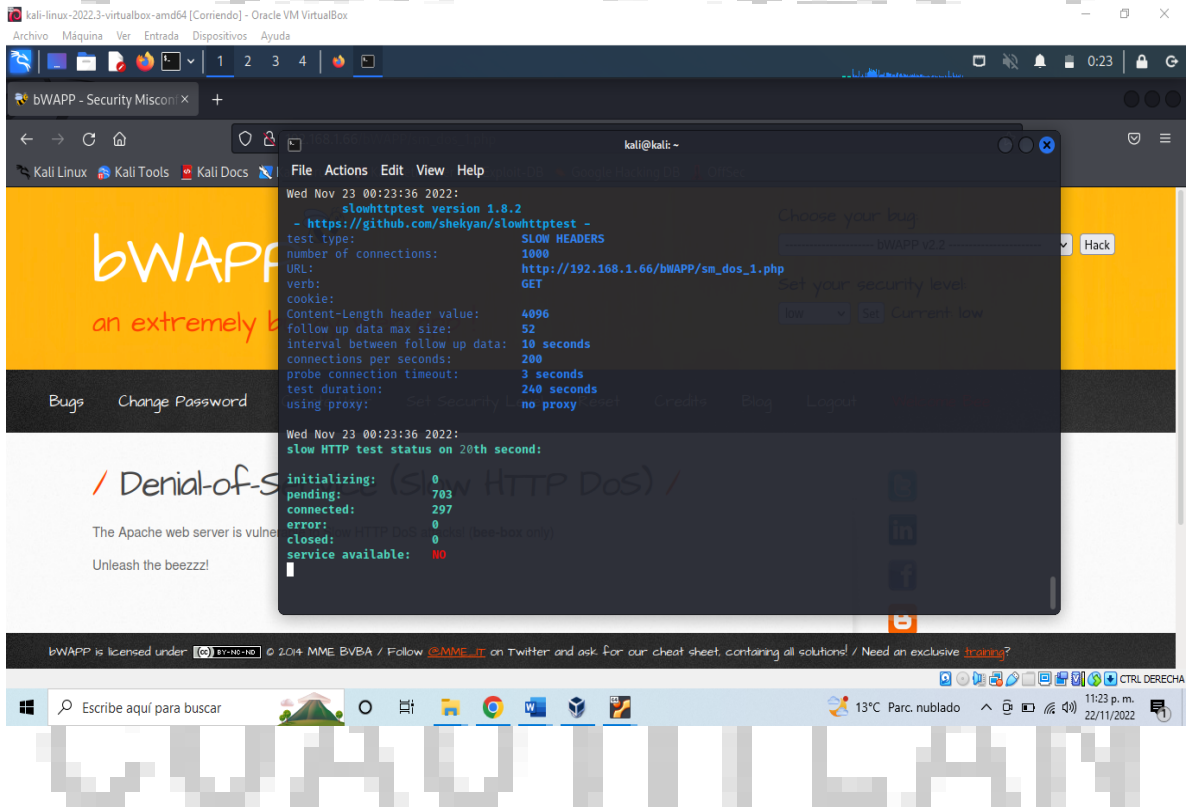
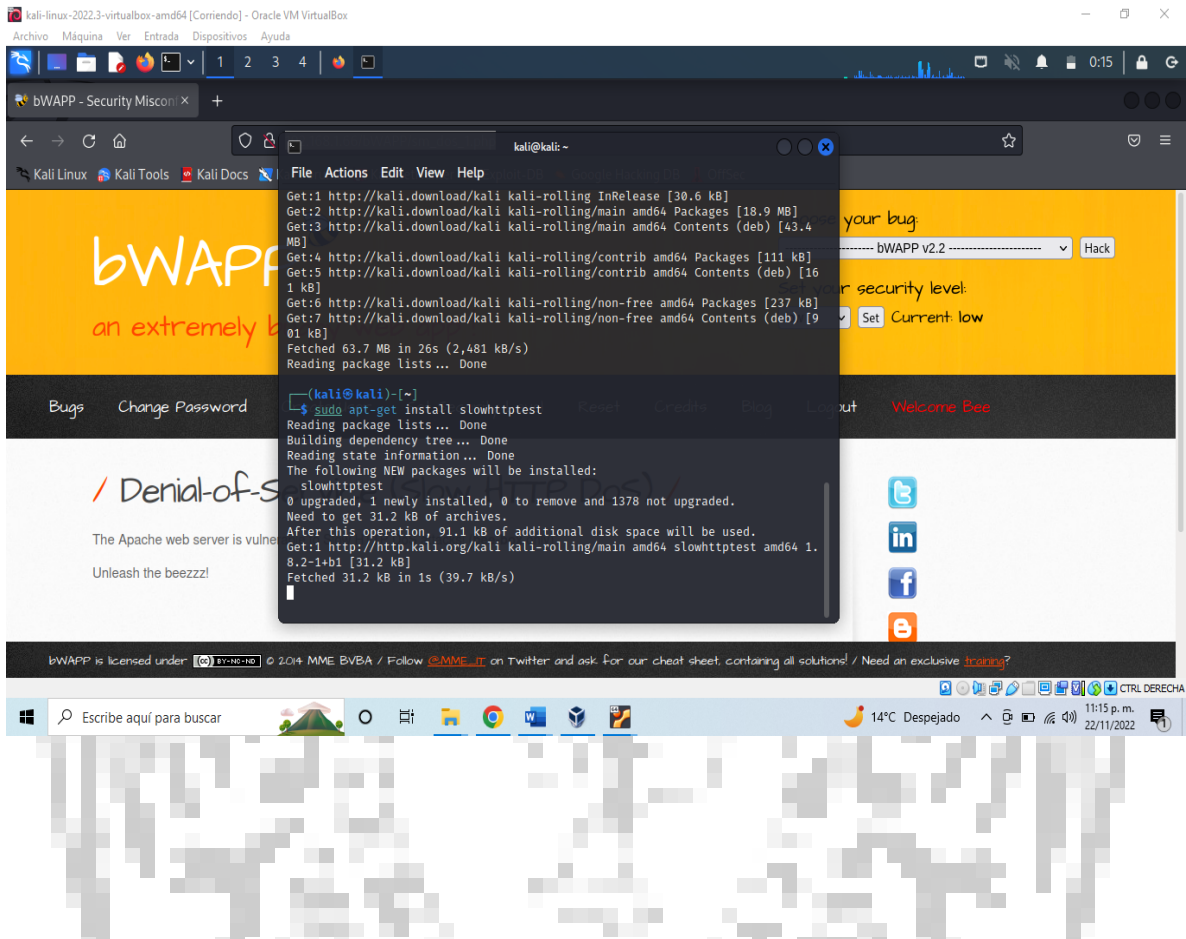


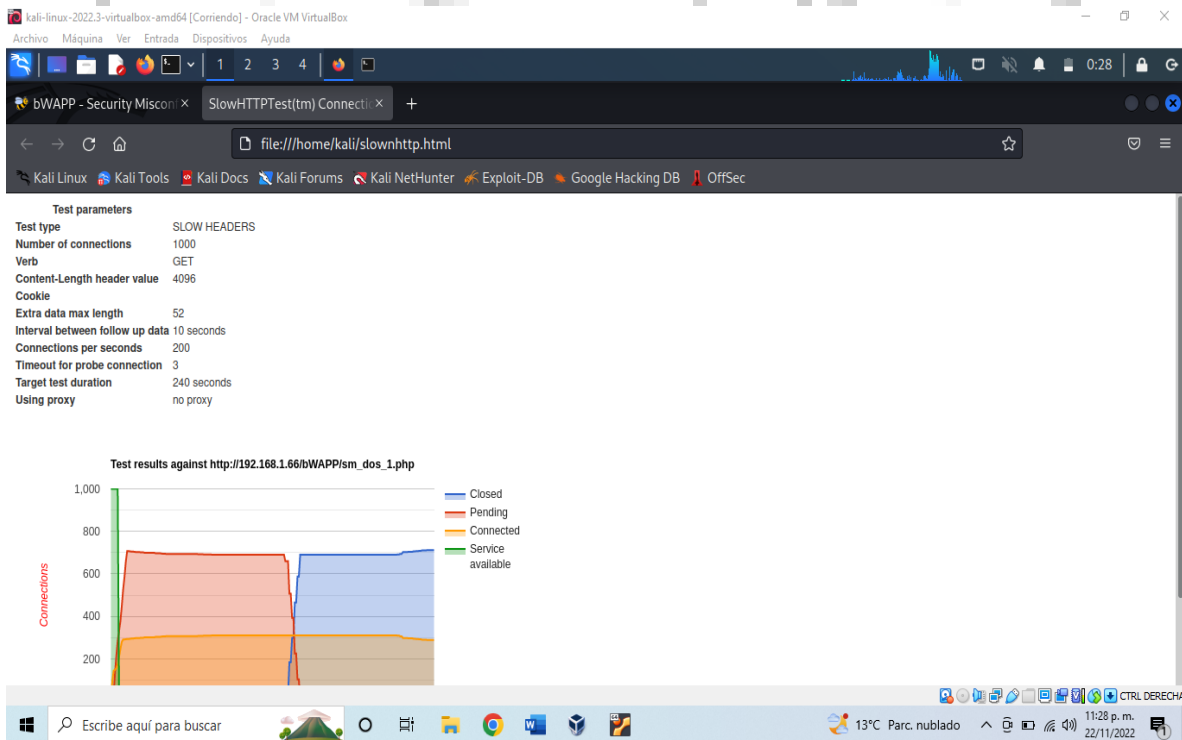
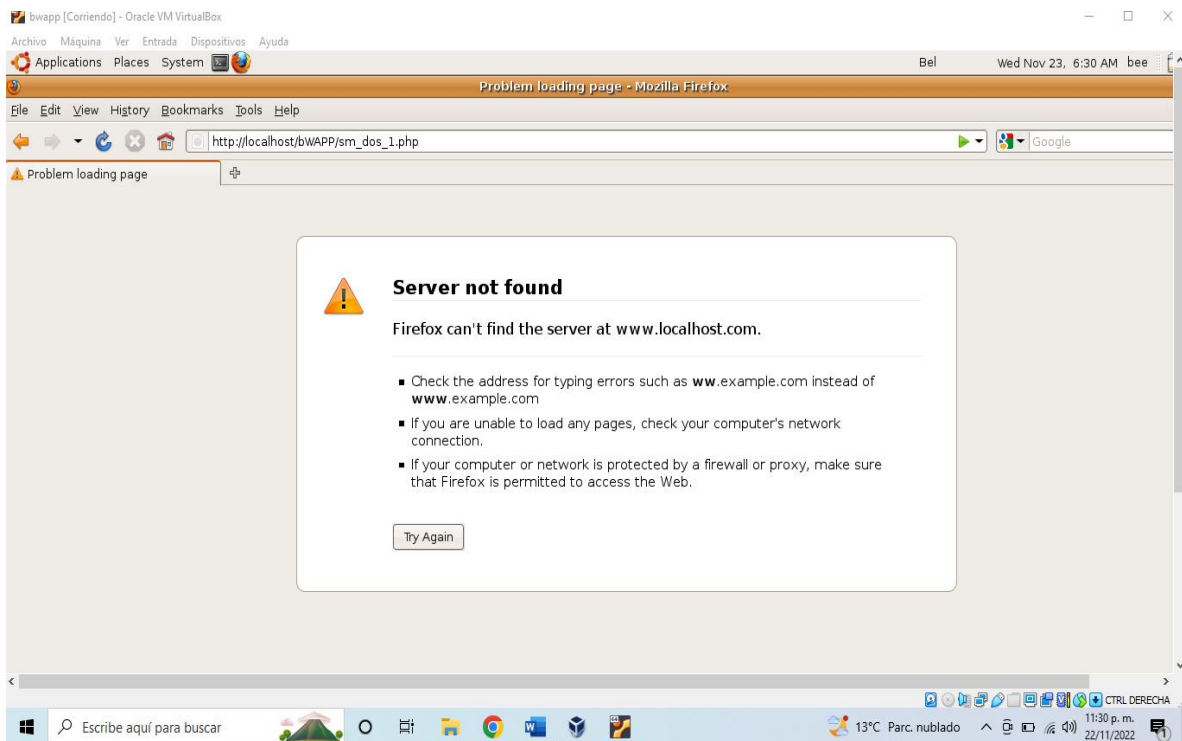
## bWAPP, an extremely buggy web app !

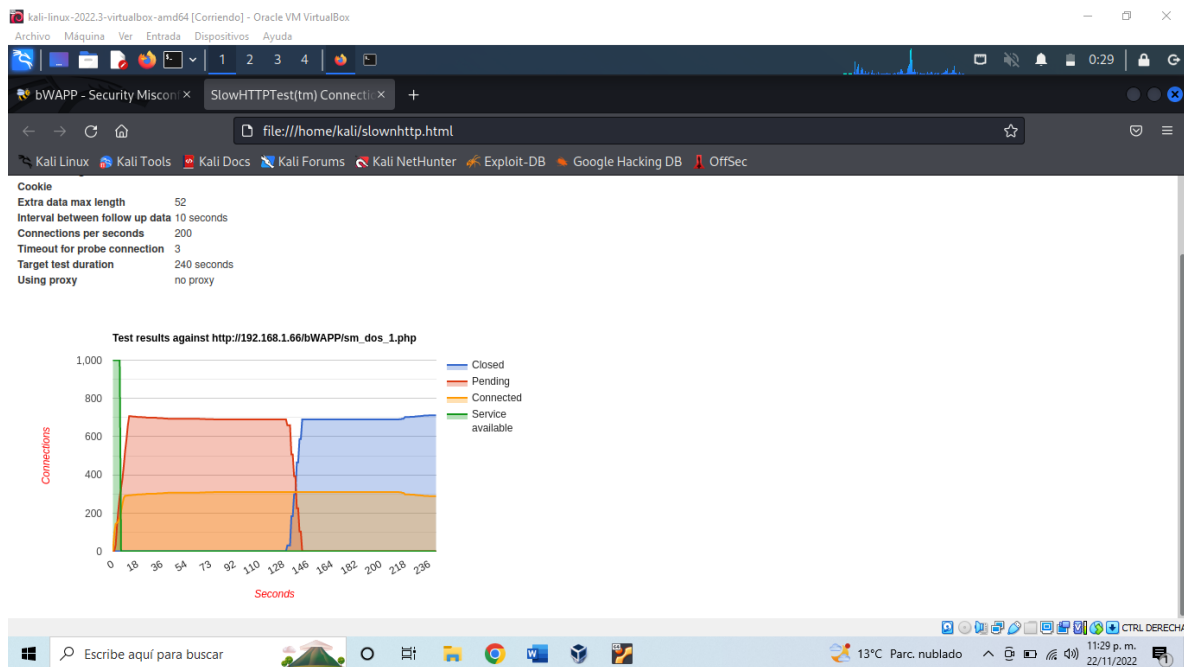
[bWAPP](#)  
[Drupageddon](#)  
[Evil folder](#)  
[phpMyAdmin](#)  
[SQLiteManager](#)











## Seguridad Informática - Ejercicio 3

Tema	5. Código Malicioso	Subtema	5.1.2 Troyanos
No. De Ejercicio	3	Profesora	Rosalba Nancy Rosas Fonseca

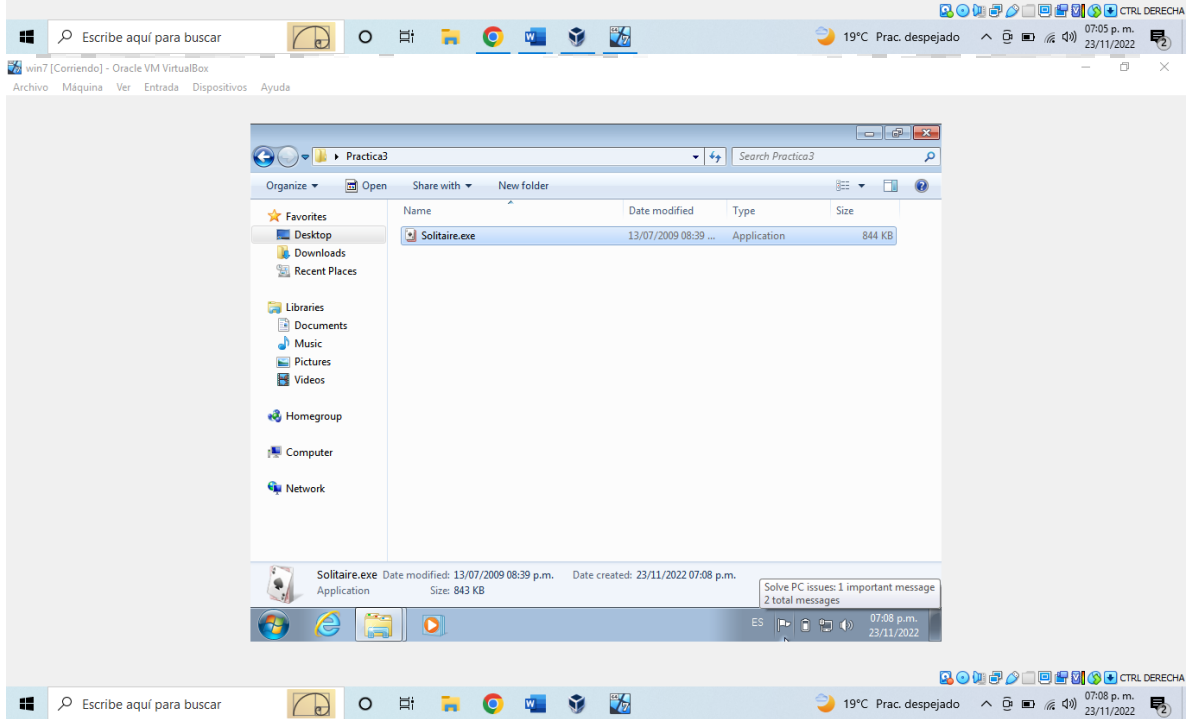
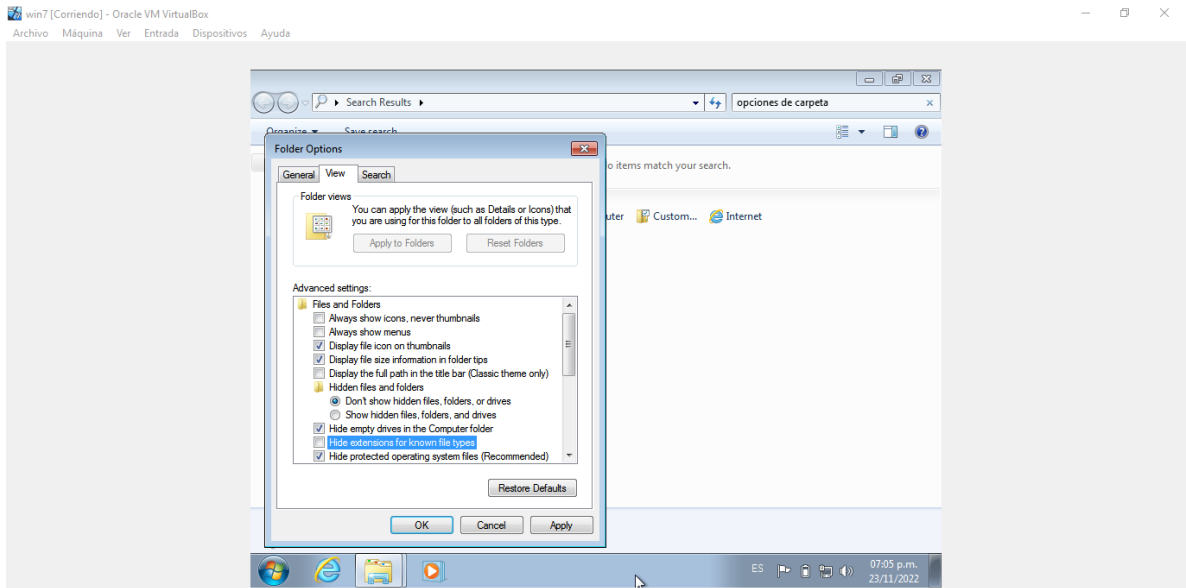
### Objetivo

Los troyanos son un tipo de Malware que se hace pasar por una aplicación o archivo legítimo, pero ejecutan un código malicioso capaz de robar información de un equipo o incluirlo en una botnet. En esta práctica se alterará de manera básica un archivo .exe y mostrar una forma en que se puede ocultar que se trata de un ejecutable.

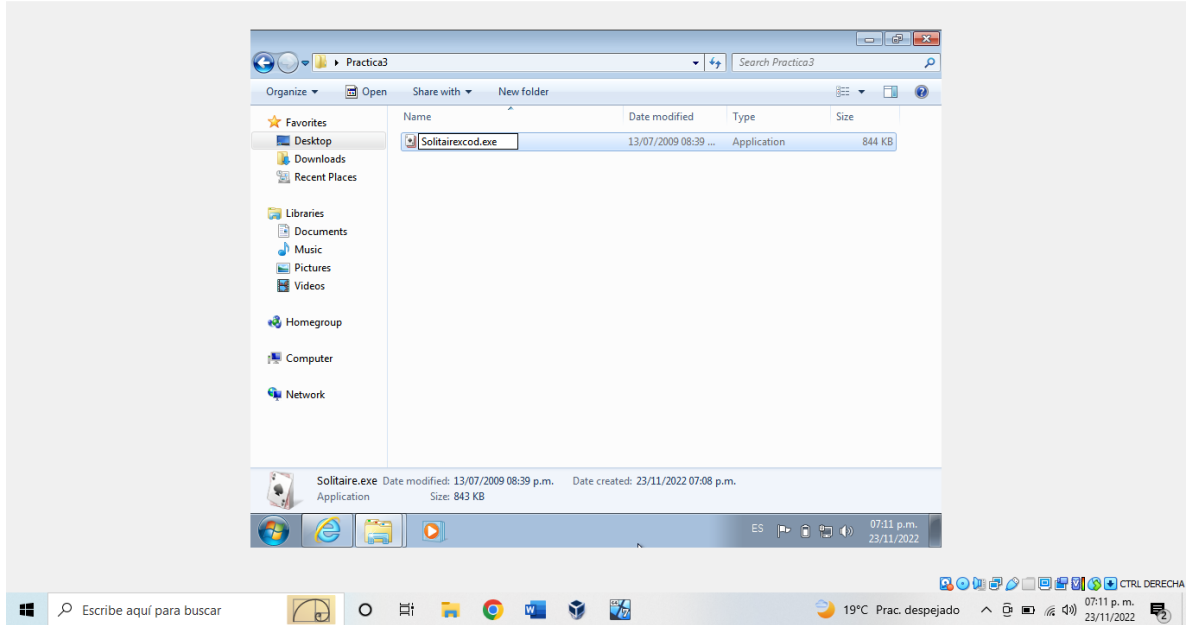
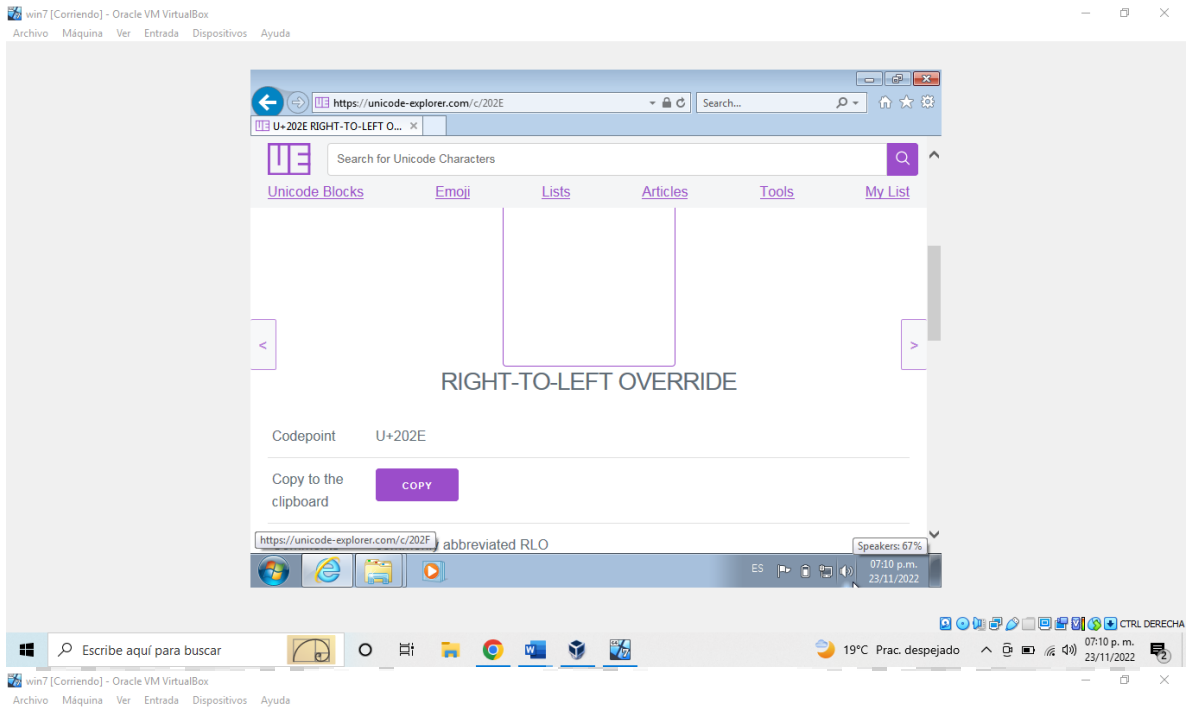
### Requerimientos

- Sistema Operativo Windows

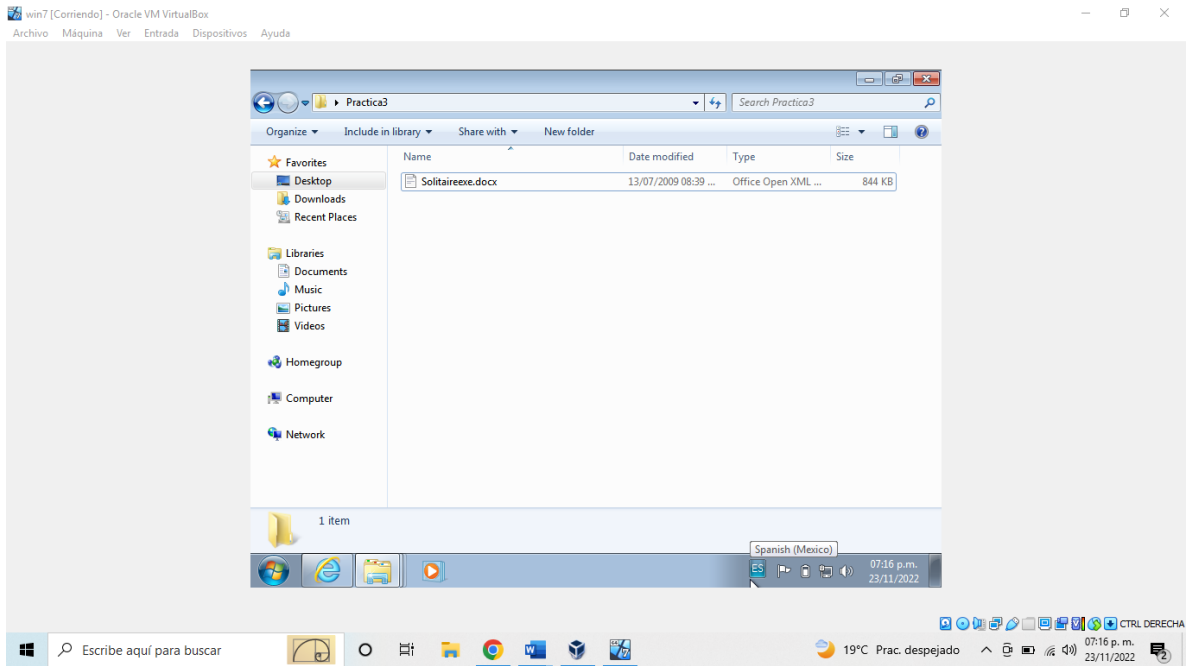
### Procedimiento



UNAM  
CUAUTITLÁN



UNAM  
CUAUTITLÁN



UNAM  
CUAUTITLÁN