

Universidad Tecnológica de Panamá
Facultad de Sistemas Computacionales
Asignatura: Desarrollo de Software IV
Laboratorio Práctico2

Profesor: Napoleón Ibarra

Valor: 100 puntos

Estudiante: Jorge Jiménez

Cédula: 4-826-874

Fecha de Inicio: 18/09/2025 → Hora: 3:20 PM

Fecha de Entrega: 18/09/2025 → Hora: 4:55 PM

Procedimiento:

1. De manera Individual / Grupal, realizar la asignación.
2. Entregar el trabajo en formato digital en la plataforma utilizada. Sustente su desarrollo en clase.

Criterios de Evaluación:

Criterios	Puntos (Mínimo=1, Máximo=5)	Porcentaje
Puntualidad Sustentación	1 - 5	15 %
Responsabilidad Entrega	1 - 5	15 %
Desarrollo Simulación	1 - 5	70 %

I PARTE. Caso de Estudio. *Valor 35 Puntos.*

SITUACIÓN ACTUAL. La empresa estatal JC de Las Lomas requiere realizar un Desarrollo Web que contenga todos los elementos necesarios de un prototipo desarrollado. Queda a criterio la elección HTML nativo / ASP.

II PARTE. Simulación Ataque / Mitigación Servicios. *Valor 35 Puntos.*

Procedimiento:

1. En un escenario local controlado (RED LAN SIN ACCESO A INTERNET) cada grupo de trabajo debe cambiar / editar <http://127.0.0.1:5000/> del sitio web desarrollado en el Laboratorio Práctico1, veamos un ejemplo: <http://192.168.11.50:5000>. Conforme a la RED LAN Inalámbrica desarrollada para el laboratorio.

2. Habilite la máquina virtual, configure su SO (PARROT, KALI LINUX, Otro) elegido para su laboratorio.
3. Lanzar / Iniciar el escaneo de puerto con NMAP en la Red LAN / Sitio Web (WEB) detectado.
4. Verifique tráficos de entrada / salida de equipo (Wireshark).
5. Lanzar / Iniciar el ataque de Ataque DDoS (SO Elegido) sobre el Sitio Web (WEB) detectado con la herramienta elegida.
6. Verificar funcionamiento del Sitio Web (Ping infinito/intermitente). Durante la simulación.
7. Capture evidencias correspondientes (Escenarios)en base a los puntos solicitados.

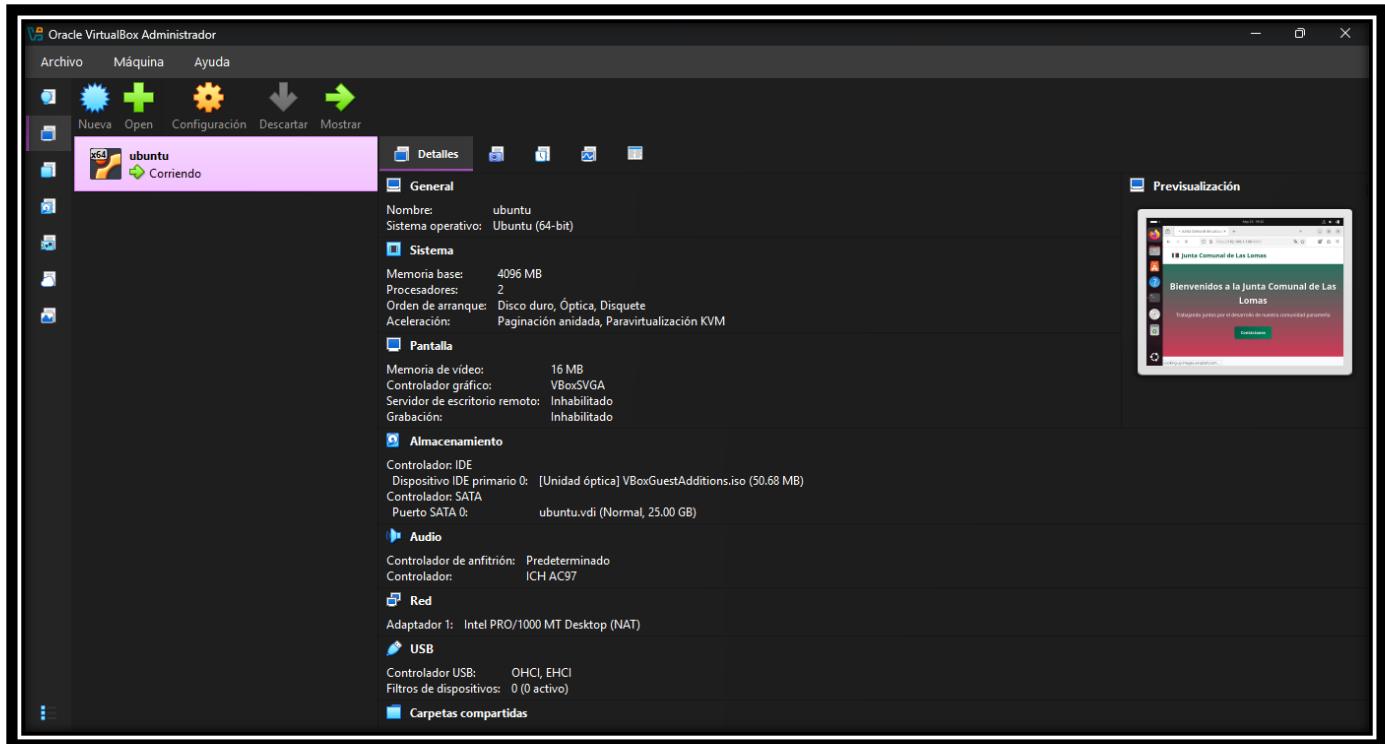
Objetivo:

- 1) Elegir un posible equipo, inhabilitar el Sitio Web. Sustente como se hará esto.
- 2) Proteger el Sitio Web de su desarrollo.
- 3) Documentar / Sustentar su trabajo.

BUENA SUERTE

Desarrollo - Imágenes de Prueba

Máquina Virtual (*por fin tengo*): es un Ubuntu.



Sitio web:

A screenshot of the website for 'Municipio JC de Las Lomas'. The header features a blue navigation bar with links for Inicio, Visión & Misión, Servicios, Ciudadanos, Historia, Departamentos, and Contáctanos. On the left side, there's a large graphic element featuring a stylized 'L' logo composed of red and blue geometric shapes. The main banner area has a blurred background image of a city skyline at sunset. Overlaid on the banner is the text 'Municipio Lomas de Zamora JC de Las Lomas' and the tagline 'Comprometidos con la comunidad: servicios eficientes y desarrollo sostenible.' Below the banner, a white box contains the word 'Bienvenidos' and a paragraph of text: 'JC de Las Lomas atiende las necesidades de la población, promoviendo proyectos y facilitando trámites municipales con eficiencia y transparencia.' At the bottom of the page is a blue footer bar with the copyright notice '© 2025 JC de Las Lomas. Todos los derechos reservados.'

Escaneo con NMAP: utilizando comandos como “nmap sn” para buscar las IPs conectadas al router y “nmap sV” para buscar su sitio en apache2.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

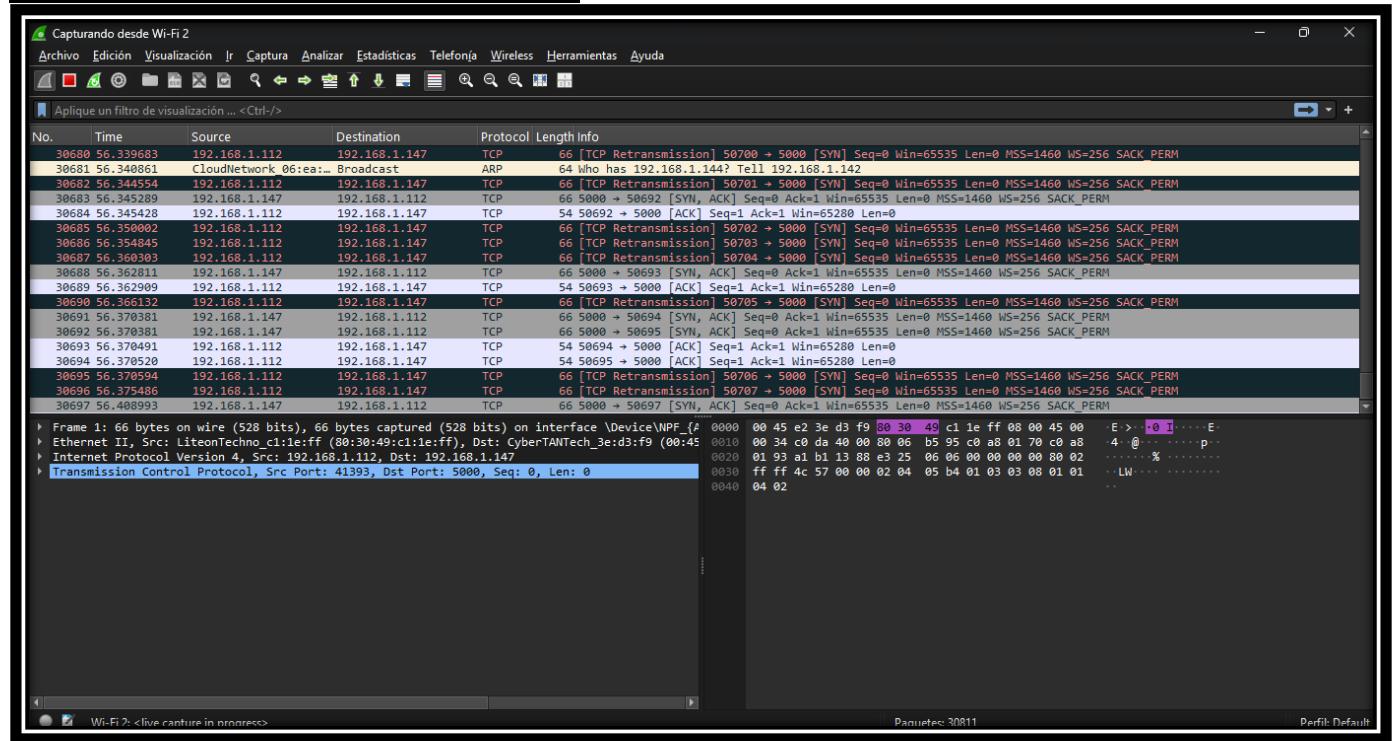
PS C:\Users\jorge> nmap -sn 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-23 14:25 -0500
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 57.25% done; ETC: 14:25 (0:00:07 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.26s latency).
MAC Address: 14:91:82:74:38:50 (Belkin International)
Nmap scan report for 192.168.1.100
Host is up (0.26s latency).
MAC Address: A8:41:F4:5D:24:43 (AzureWave Technology)
Nmap scan report for 192.168.1.108
Host is up (0.18s latency).
MAC Address: 74:48:BB:43:C9:C5 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.114
Host is up (0.11s latency).
MAC Address: 50:5B:C2:D6:BB:BF (Liteon Technology)
Nmap scan report for 192.168.1.115
Host is up (0.085s latency).
MAC Address: 50:5B:C2:D6:BB:BF (Liteon Technology)
Nmap scan report for 192.168.1.116
Host is up (0.41s latency).
MAC Address: 80:45:DD:03:63:17 (Intel Corporate)
Nmap scan report for 192.168.1.139
Host is up (3.4s latency).
MAC Address: 80:45:DD:03:63:17 (Intel Corporate)
Nmap scan report for 192.168.1.142
Host is up (0.14s latency).
MAC Address: 60:E9:AA:06:EA:25 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.145
Host is up (0.26s latency).
```

Escaneo con NMAP (Especifico): Para ver la IP seleccionada con el “nmap sV”

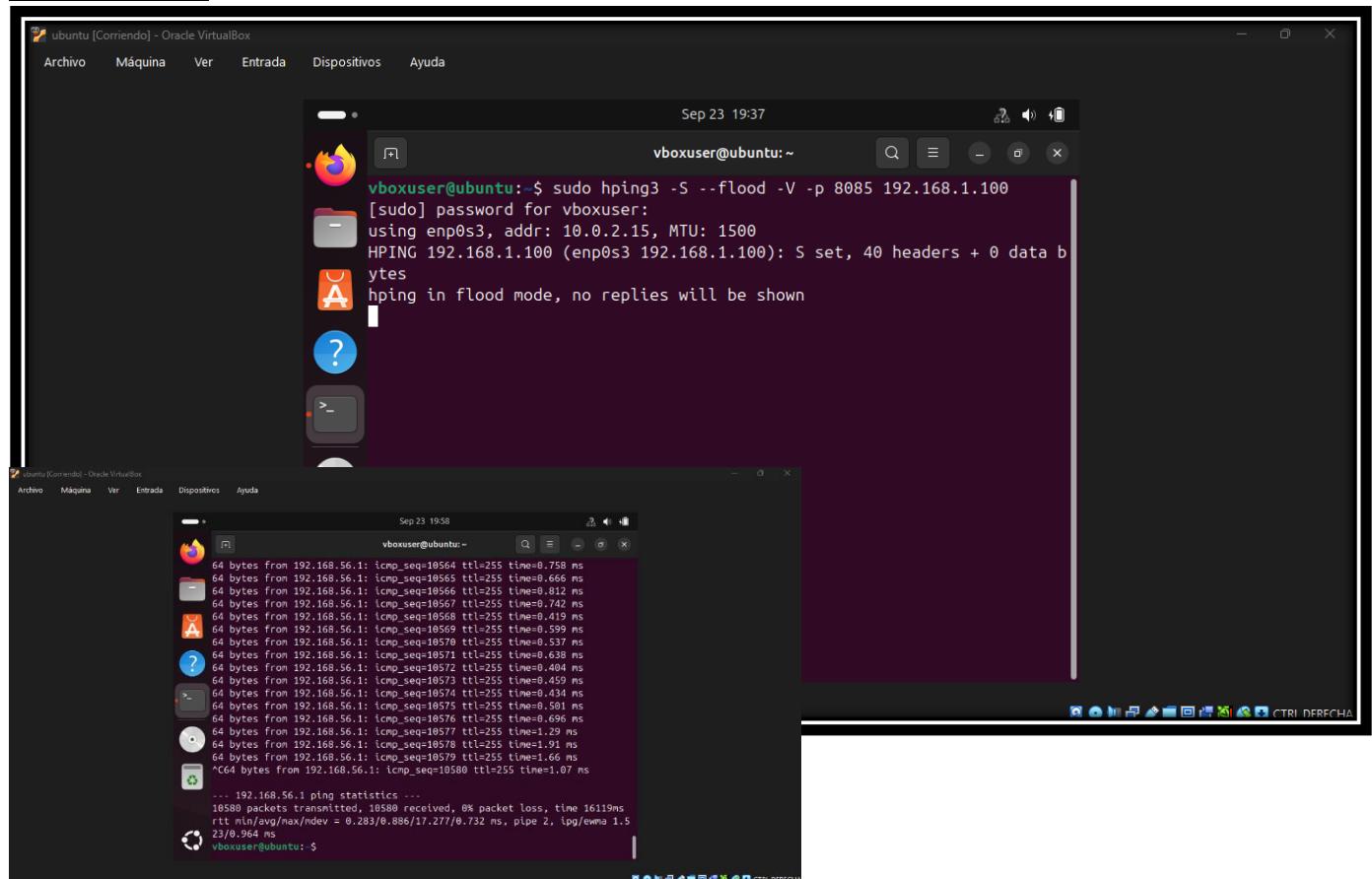
```
C:\Users\jorge>nmap -sV 192.168.1.101
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-23 14:12 -0500
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.45% done; ETC: 14:12 (0:00:29 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 34.80% done; ETC: 14:12 (0:00:11 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.60% done; ETC: 14:12 (0:00:08 remaining)
Nmap scan report for 192.168.1.101
Host is up (0.065s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  tcpwrapped
139/tcp    open  tcpwrapped
445/tcp    open  tcpwrapped
3306/tcp   open  tcpwrapped
5357/tcp   open  tcpwrapped
MAC Address: A8:41:F4:8D:3C:0D (AzureWave Technology)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.37 seconds
```

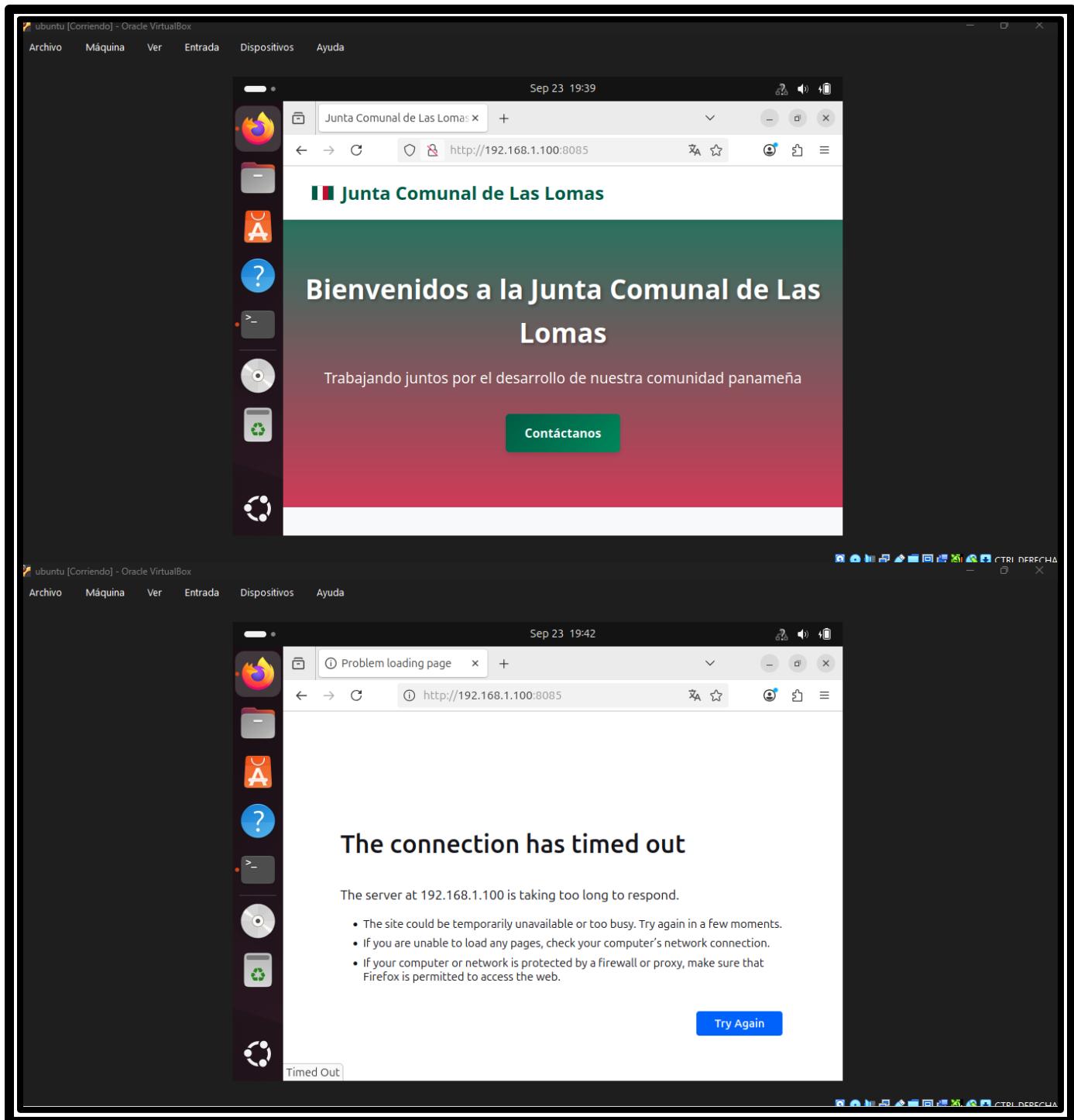
Verificación de tráfico con Wireshark:



Ataque DDoS: Utilizando “hping3” para derrumbar una página que encontré con nmap.



Funcionamiento de la página (antes y después del ataque):



En cuanto a la defensa:

Mi sitio no se pudo defender, apenas el compañero lanza los pings el sitio se cayó, aunque tuviera en el firewall una opción para bloquear pings...

A screenshot of the Windows Defender Firewall settings. On the left, there are navigation links: 'Reglas de entrada', 'Reglas de salida', 'Reglas de seguridad de conexión', and 'Supervisión'. The 'Reglas de entrada' link is selected, and its details pane is shown on the right. The title of this pane is 'Reglas de entrada'. The table lists four rules:

Nombre	Grupo	Perfil	Habilitado	Acción
Rede [redacted]	Todo	Sí	Permitir	
Rede [redacted]	Todo	Sí	Permitir	
BLOQUEAR PING	Todo	Sí	Bloquear	