CY-302 Programación Avanzada

Entrega 1: Base del proyecto y entorno

Proyecto: Red Team vs Blue Team en Azure

Docente: Andrés Vargas

Estudiantes:

- Eduardo Jiménez Bonilla
- Andrés Alonso Obando Fallas
- Daniel Vargas
- Victoria Arguedas
- Fabricio Calderon
- Jose Castillo

Fecha: 15 de octubre de 2025

Repositorio: https://github.com/fxbricm/proyecto_ciberseguridad/tree/main

Roles por equipo (Blue / Red)

Distribución por equipos

Integrante	Rol
Eduardo Jiménez	Blue Team
Jose Castillo	Blue Team
Daniel Vargas	Blue Team
Victoria Arguedas	Red Team
Fabricio Calderon	Red Team
Andrés Obando	Red Team

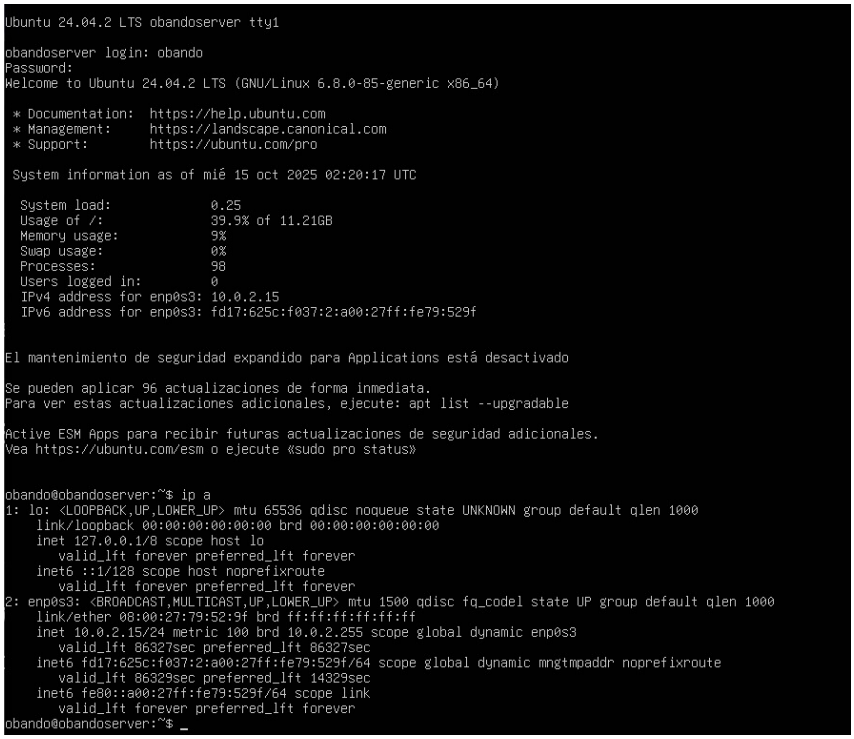
Roles del equipo

- **Blue Team (Defensa):** Encargado de hardening de la VM, configuración de firewall, detección y bloqueo básico.
- **Red Team (Ataque):** Encargado de pruebas controladas de escaneo y ataques en el entorno de laboratorio.

IP de la VM objetivo

Parámetro	Valor

Nombre del host (VM)	obandoserver
Sistema operativo	Ubuntu Server 24.04.2 LTS
Versión del kernel	6.8.0-85-generic (x86_64)
Usuario actual	obando
Interfaz de red	enp0s3
Dirección IPv4 interna	**10.0.2.15**
Dirección IPv6	**fd17:625c:f037:2:a00:27ff:fe79:529f**
Estado del sistema	Activa (login exitoso)



Puertos permitidos (NSG)

Nombre regla	Puerto	Protocolo	Acción	Notas
SSH	22	TCP	Allow	Recomendar restringir origen a IPs conocidas
HTTP	80	TCP	Allow	Solo si se hospeda servicio web
HTTPS	443	TCP	Allow	Solo si se hospeda servicio seguro
Default Inbound	*	*	Deny	Bloquear todo lo demás

Pasos rápidos de creación de la VM

Desde el Portal de Azure:

1. Iniciar sesión en https://portal.azure.com.
2. Seleccionar **“Crear un recurso”** → **“Máquina virtual”**.
3. Escoger la **suscripción** y crear un nuevo **grupo de recursos** (por ejemplo, RG_PROYECTO).
4. Asignar un **nombre** a la máquina virtual, como vm-blue.
5. Seleccionar la **imagen** del sistema operativo: *Ubuntu Server 24.04.2 LTS*.
6. Elegir el **tamaño Standard_B1s**, recomendado por su bajo costo y rendimiento adecuado.
7. En el apartado **Autenticación**, seleccionar **SSH public key** para mayor seguridad.

8. En la pestaña **Redes (Networking)**, crear o seleccionar un **Network Security Group (NSG)** y permitir únicamente los puertos 22, 80 y 443.
9. Revisar la configuración general y hacer clic en **“Crear”**.
10. Esperar el despliegue y copiar la **dirección IP pública** asignada.
11. Probar la conexión desde la terminal mediante SSH:

Buenas prácticas (apagar VM y seguridad)

El entorno de pruebas del proyecto fue diseñado siguiendo lineamientos de eficiencia, seguridad y ética en el uso de recursos de nube.

A continuación, se detallan las **buenas prácticas aplicadas** para garantizar el control de costos y la protección del sistema:

Ahorro de costos

- **Apagar la VM cuando no esté en uso:**

  Se recomienda detener la máquina virtual al finalizar las prácticas diarias para evitar el consumo del crédito disponible.

  - Desde el Portal de Azure:

    → Opción **“Stop (deallocate)”**.

“az vm deallocate --resource-group RG_PROYECTO --name vm-blue"

- **Usar tamaños pequeños:**

  Se seleccionó el tamaño **Standard_B1s**, ya que ofrece un equilibrio entre rendimiento y costo dentro del crédito gratuito de Azure for Students.

- **Programar apagado automático:**

  En el portal se configuró la opción **Auto-shutdown** para que la máquina virtual se apague automáticamente en horarios no laborales.

- **Supervisión del crédito:**

  Se recomienda revisar el panel de costos de Azure periódicamente para evitar un consumo innecesario de recursos.

Seguridad del entorno

- **Principio de mínima exposición:**

  Solo se habilitaron los puertos estrictamente necesarios (22, 80 y 443) y se bloqueó todo el tráfico no autorizado mediante el grupo de seguridad de red (NSG).
- **Autenticación por clave SSH:**

  Se implementó acceso mediante clave pública SSH, evitando contraseñas para reducir el riesgo de acceso no autorizado.
- **Restricción de acceso remoto:**

  Se recomienda limitar el puerto SSH (22) únicamente a direcciones IP específicas del equipo de trabajo.
- **Actualización del sistema:**

  Se ejecuta periódicamente el siguiente comando para mantener la VM actualizada y libre de vulnerabilidades:

```
sudo apt update && sudo apt upgrade -y
```

- **Backups y snapshots:**

  Se crearán instantáneas (snapshots) solo cuando sea necesario y se eliminarán al concluir las pruebas para optimizar el espacio en disco.

- **Monitoreo de actividad:**

  El Blue Team mantendrá registros de acceso y logs básicos del sistema para auditoría y control.

Ética y uso responsable

- Todas las pruebas ofensivas y defensivas se realizarán **exclusivamente dentro del entorno autorizado del curso**.
- No se ejecutarán escaneos, ataques ni accesos hacia infraestructuras externas o terceros.
- Los datos empleados no contendrán información personal ni sensible (PII).