



## **Avance 1 del proyecto (Red Team vs Blue Team en Azure)**

### **Integrantes:**

**Betzabeth Araya Abarca**

**Jose Arias Rodríguez**

**Carlos Garreta Quesada**

**Luis Ugalde Álvarez**

**Jose Ugalde Moreno**

**Fiorella Ureña Jaubert**

### **Curso: Programación Avanzada**

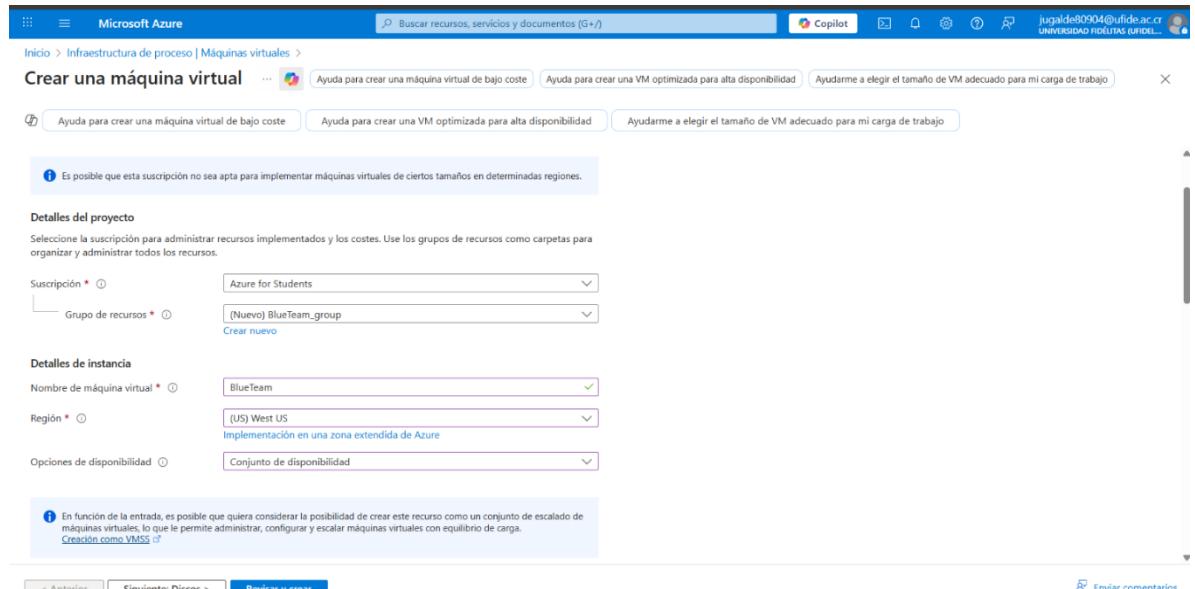
**Profesor. Andrés Felipe Vargas Rivera**

**III Cuatrimestre 2025**

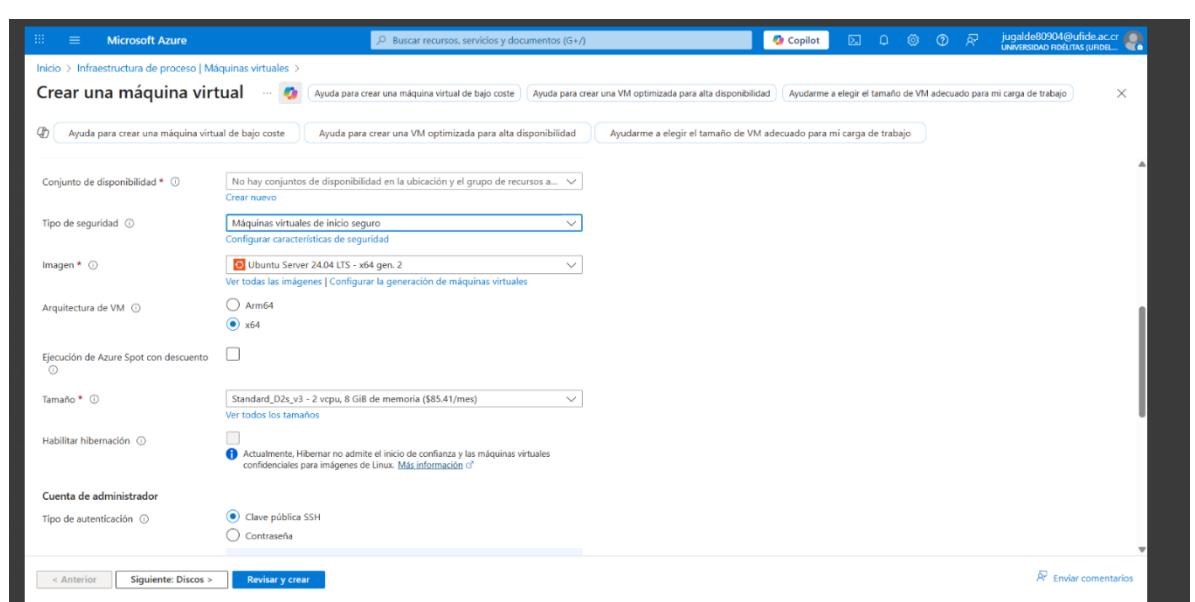
## 1.Roles del Equipo:

-Blue Team: Su rol es la de protector de ciberataques necesita conocer las formas y métodos de ataque para poder defenderse de los mismos. También hay medidas de que reducen la probabilidad de ataques.

### Crear y configurar la VM en Azure



The screenshot shows the first step of the 'Create a virtual machine' wizard in the Microsoft Azure portal. The title bar says 'Microsoft Azure'. The top navigation bar includes 'Buscar recursos, servicios y documentos (G+)', 'Copilot', and user information 'jugalde80904@ufide.ac.cr UNIVERSIDAD FEDERAS (UFIDE...)'. The main content area is titled 'Crear una máquina virtual' and shows the 'Detalles del proyecto' section. It asks to select a subscription and resource group. The 'Suscripción' dropdown is set to 'Azure for Students' and the 'Grupo de recursos' dropdown is set to '(Nuevo) BlueTeam\_group'. A note indicates that the current subscription might not be suitable for certain VM sizes in specific regions. The 'Detalles de instancia' section includes fields for 'Nombre de máquina virtual' (set to 'BlueTeam'), 'Región' (set to '(US) West US'), and 'Opciones de disponibilidad' (set to 'Conjunto de disponibilidad'). A note about creating a VMSS is present. At the bottom are buttons for '< Anterior', 'Siguiente: Discos >', and 'Revisar y crear'.

The screenshot shows the second step of the 'Create a virtual machine' wizard, continuing from the previous step. The title bar and top navigation bar are identical. The main content area shows the 'Configurar características de seguridad' section under 'Tipo de seguridad'. Other settings include 'Imagen' (Ubuntu Server 24.04 LTS - x64 gen. 2), 'Arquitectura de VM' (x64 selected), and 'Tamaño' (Standard\_D2s\_v3 - 2 vcpus, 8 GiB de memoria (\$85.41/mes)). A note about hibernation is present. At the bottom are buttons for '< Anterior', 'Siguiente: Discos >', and 'Revisar y crear'.

**Microsoft Azure** | **Inicio > Infraestructura de proceso | Máquinas virtuales >** Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste | Ayuda para crear una VM optimizada para alta disponibilidad | Ayuda para elegir el tamaño de VM adecuado para mi carga de trabajo

**Supervisión**

Configuración de reglas de alertas recomendadas

Seleccionar reglas de alertas

- > Percentage CPU es mayor que 80 %
- > es menor que Available Memory Bytes 1 GB
- > Data Disk IOPS Consumed Percentage es mayor que 95 %
- > OS Disk IOPS Consumed Percentage es mayor que 95 %
- > Network In Total es mayor que 500 GB
- > Network Out Total es mayor que 200 GB
- > es menor que VmAvailabilityMetric 1

Notificarme antes del

- Correo electrónico jugalde80904@ufide.ac.cr
- Rol de Azure Resource Manager de correo electrónico Seleccionar un rol de Azure Resource Manager
- notificación de Azure Mobile App jugalde80904@ufide.ac.cr

Total mensual estimado: 0.00 USD

**Alertas**

Habilitar reglas de alerta recomendadas

**Reglas de alerta**

**Reglas de alerta no configuradas**

**Configurar**

**Diagnóstico**

**Diagnósticos de arranque**

- Habilitar con la cuenta de almacenamiento administrada (recomendado)
- Habilitar con la cuenta de almacenamiento personalizada
- Deshabilitar

Habilitar diagnósticos del SO invitado

**Estado**

Habilitar supervisión de estado de la aplicación

**Revisar y crear**

**Guardar** **Cancelar**

**Microsoft Azure** | **Inicio > Infraestructura de proceso | Máquinas virtuales >** Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste | Ayuda para crear una VM optimizada para alta disponibilidad | Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

Habilitar el plan básico de forma gratuita

Esto se aplicará a todas las máquinas virtuales de la suscripción seleccionada

**Identidad**

Habilitar identidad administrada asignada por el sistema

**Microsoft Entra ID**

Inicio de sesión con Microsoft Entra ID

El inicio de sesión de id. de Microsoft Entra utiliza ahora autenticación basada en certificados SSH. Tendrá que utilizar un cliente SSH compatible con los certificados OpenSSH. Puede usar la CLI de Azure o Cloud Shell desde Azure Portal. [Más información](#)

La asignación de rol RBAC de Inicio de sesión de administrador de máquina virtual o Inicio de sesión de usuario de máquina virtual es necesaria cuando se utiliza el inicio de sesión de id. de Microsoft Entra. [Más información](#)

**Apagado automático**

Habilitar apagado automático

Hora de apagado 7:00:00 p.m.

Zona horaria (UTC-06:00) Centroamérica

Notificación antes del apagado

**Revisar y crear**

**Enviar comentarios**

Microsoft Azure Buscar recursos, servicios y documentos (G+) Copilot

Inicio > Infraestructura de proceso | Máquinas virtuales > Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste Ayuda para crear una VM optimizada para alta disponibilidad Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

Al crear una máquina virtual, se crea una interfaz de red automáticamente.

Red virtual \* (nuevo) BlueTeam-vnet

Subred \* (nuevo) default (10.0.0.0/24)

IP pública (nuevo) BlueTeam-ip

Grupo de seguridad de red de NIC  Ninguno  Básico  Opciones avanzadas

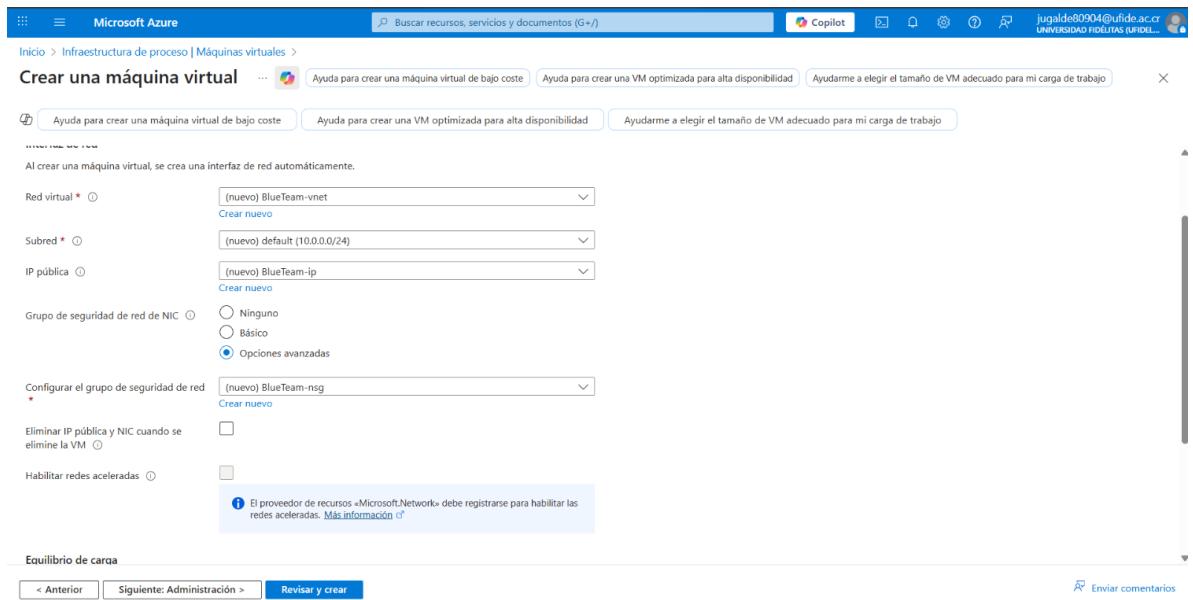
Configurar el grupo de seguridad de red \* (nuevo) BlueTeam-nsg

Eliminar IP pública y NIC cuando se elimine la VM

Habilitar redes aceleradas   
El proveedor de recursos «Microsoft.Network» debe registrarse para habilitar las redes aceleradas. [Más información](#)

Equilibrio de carga

< Anterior Siguiente: Administración > Revisar y crear Envíar comentarios



Microsoft Azure Buscar recursos, servicios y documentos (G+) Copilot

Inicio > Infraestructura de proceso | Máquinas virtuales > Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste Ayuda para crear una VM optimizada para alta disponibilidad Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

CONTRASEÑAS para imágenes de Linux: [https://docs.microsoft.com/.../Linux](#)

Cuenta de administrador

Tipo de autenticación  Clave pública SSH  Contraseña

Nombre de usuario \* admin\_blue

Contraseña \*

Confirmar contraseña \*

Reglas de puerto de entrada

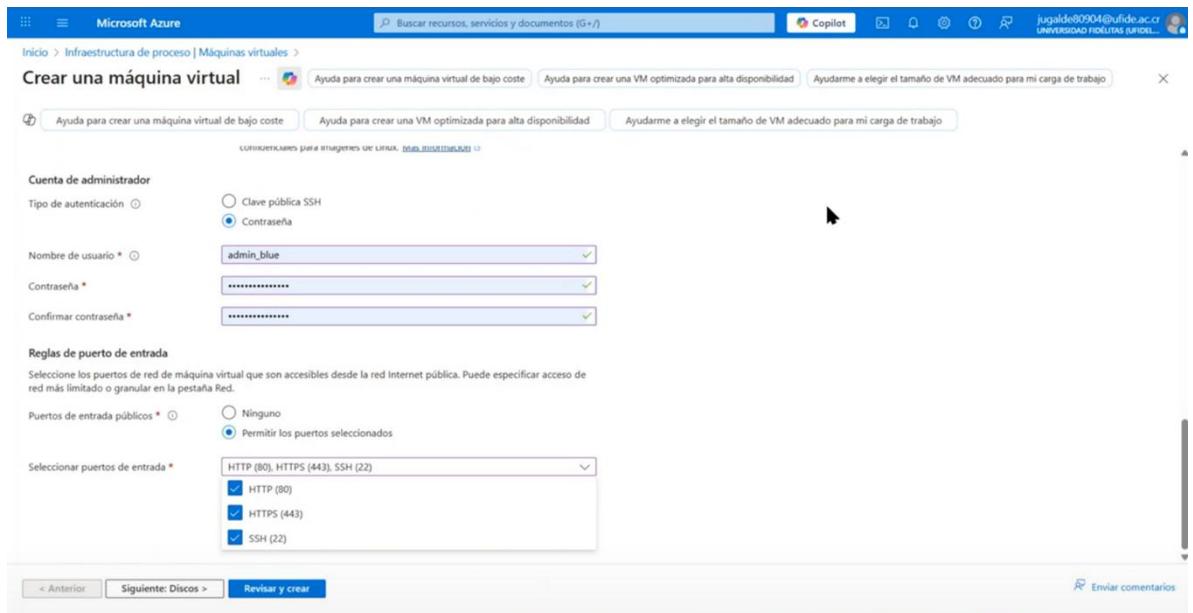
Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.

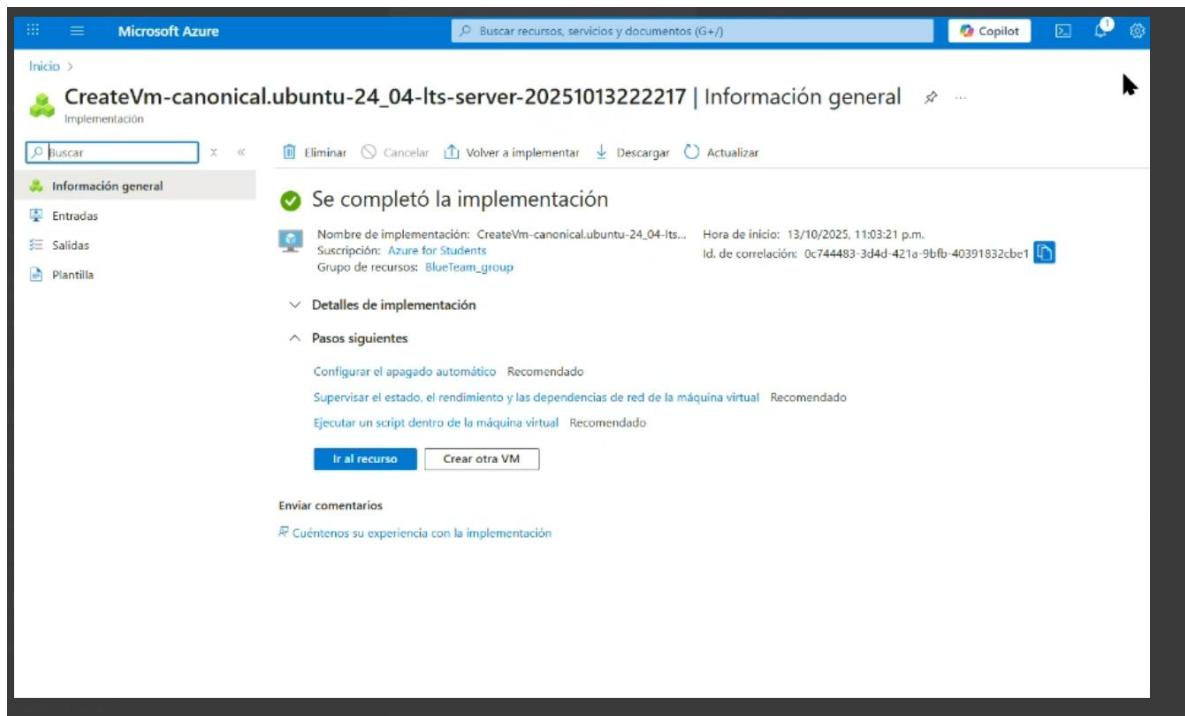
Puertos de entrada públicos \*  Ninguno  Permitir los puertos seleccionados

Seleccionar puertos de entrada \* HTTP (80), HTTPS (443), SSH (22)

HTTP (80)  
 HTTPS (443)  
 SSH (22)

< Anterior Siguiente: Discos > Revisar y crear Envíar comentarios





Pasos a seguir:

Desde el navegador con Azure Bastion (sin abrir puertos)

En el portal de la VM → botón Conectar → pestaña Bastion.

Si no está creado, haz Crear Bastion (sigue el asistente).

Rellena usuario y contraseña/clave → Conectar.

Resultado: consola SSH en el navegador.

```
• Documentation: https://help.ubuntu.com
• Management: https://landscape.canonical.com
• Support: https://ubuntu.com/pro

System information as of Tue Oct 14 05:16:41 UTC 2025

System load: 0.11 Processes: 127
Usage of /: 5.3% of 29.95GB Users logged in: 0
Memory usage: 3% IPv4 address for eth0: 10.0.0.4
Swap usage: 0%

xpanded Security Maintenance for Applications is not enabled.

updates can be applied immediately.

nable ESM Apps to receive additional future security updates.
ee https://ubuntu.com/esm or run: sudo pro status

he list of available updates is more than a week old.
o check for new updates run: sudo apt update

he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*copyright*.

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.

dmin_blue@BlueTeam:~$ ifconfig
ommand 'ifconfig' not found, but can be installed with:
udo apt install net-tools
dmin_blue@BlueTeam:~$ sudo apt in
```

```
dmin_blue@BlueTeam:~$ ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.4 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::20d:3aff:fe30:d7df prefixlen 64 scopeid 0x20<link>
            ether 00:0d:3a:30:07:0f txqueuelen 1000 (Ethernet)
            RX packets 35457 bytes 47793311 (47.7 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 6067 bytes 1552806 (1.5 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

o: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 392 bytes 27507 (27.5 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 392 bytes 27507 (27.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dmin_blue@BlueTeam:~$
```

```
admin blue@BlueTeam:~$ nmap
admin_blue@BlueTeam:~$ sudo nmap -p 22,80,443,3389 10.0.0.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-14 05:42 UTC
Nmap scan report for blueteam.internal.cloudapp.net (10.0.0.4)
Host is up (0.00011s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    closed http
443/tcp   closed https
3389/tcp  closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
admin_blue@BlueTeam:~$
```

-Red Team: Su rol es el de agresor virtual identifica y utiliza las vulnerabilidades del sistema o de los usuarios del sistema. Para modificar leer o ver datos confidenciales.

## Creación y Configuración de la VM en Azure

ⓘ This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Size \***  ⓘ Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$70.08/month)  ⓘ See all sizes

**Enable Hibernation**  ⓘ   ⓘ Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#)  ⓘ

**Administrator account**

Authentication type  ⓘ  SSH public key  Password

User	Basics	Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create
Passw	Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. <a href="#">Learn more</a> <span> ⓘ</span>							
Confir	<b>VM disk encryption</b>							
Inbou	Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.							
Select netw	Encryption at host <span> ⓘ</span> <input type="checkbox"/>							<span> ⓘ</span> Encryption at host is not registered for the selected subscription. <a href="#">Learn more</a> <span> ⓘ</span>
Public								

Select **OS disk**

OS disk size  ⓘ Image default (30 GiB)  ⓘ

OS disk type \*  ⓘ Standard HDD (locally-redundant storage)  ⓘ The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

ⓘ Delete with VM  ⓘ

Key management  ⓘ Platform-managed key  ⓘ

ⓘ Enable Ultra Disk compatibility  ⓘ Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_D2s\_v3.

**Data disks for RedTeam**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM <span> ⓘ</span>
<a href="#">Create and attach a new disk</a> <a href="#">Attach an existing disk</a>					

ⓘ Advanced

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

#### Basics

Subscription	Azure for Students
Resource group	(new) RedTeam_group
Virtual machine name	RedTeam
Region	West US 3

#### Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	Image Default

#### Monitoring

Alerts	Off	Pasos a seguir:
Boot diagnostics	On	Desde el
Enable OS guest diagnostics	Off	navegador con
Enable application health monitoring	Off	

#### Advanced

Extensions	None	Azure Bastion
VM applications	None	
Cloud init	No	
User data	No	(sin abrir
Disk controller type	SCSI	
Proximity placement group	None	
Capacity reservation group	None	puertos)

< Previous

Next >

Create

En el portal de

la VM → botón Conectar → pestaña Bastion.

Si no está creado, haz Crear Bastion (sigue el asistente).

Rellena usuario y contraseña/clave → Conectar.

Resultado: consola SSH en el navegador.

## **2. IP de la Máquina Virtual Objetivo (BlueTeam):**

### **Máquina Virtual Blue Team:**

**IP: 172.184.103.17**

Nombre ↑	Suscripción	Grupo de recu...	Ubicación	Estado	Sistema operat...	Cambiar el ta...	Dirección IP p...	Discos
BlueTeam	Azure for Stud...	VM_P_PA	West US	Detenido (desa...)	Linux	Standard_E2s_v3	20.253.181.111	1

## **3. Puertos Permitidos (NSG):**

- SSH: 22

## **4. Buenas Prácticas de Seguridad:**

- Mantener actualizado el sistema con `sudo apt update && sudo apt upgrade -y`.
- Apagar la VM cuando no esté en uso.
- Evitar exponer servicios innecesarios.
- Utilizar contraseñas y claves seguras.
- Supervisar accesos SSH desde direcciones IP conocidas

BlueTeam:

Usuarios, Puertos Abiertos, Servicios Activos.

```
BlueTeam@BlueTeam:~/Entrega2$ sudo ./os_audit.py
Auditoría básica del sistema

--- Usuarios del sistema ---
Usuario: BlueTeam, Shell: /bin/bash

--- Puertos abiertos ---
Netid State Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp  UNCONN 0      0        127.0.0.54:53      0.0.0.0:*
udp  UNCONN 0      0        127.0.0.53%lo:53    0.0.0.0:*
udp  UNCONN 0      0        10.0.0.4%eth0:68    0.0.0.0:*
udp  UNCONN 0      0        127.0.0.1:323     0.0.0.0:*
udp  UNCONN 0      0        [::]:323          [::]:*
tcp   LISTEN 0     4096    127.0.0.53%lo:53    0.0.0.0:*
tcp   LISTEN 0     4096    0.0.0.0:22         0.0.0.0:*
tcp   LISTEN 0     4096    127.0.0.54:53     0.0.0.0:*
tcp   LISTEN 0     4096    [::]:22           [::]:*

--- Servicios activos ---
UNIT            LOAD  ACTIVE SUB      DESCRIPTION
chrony.service  loaded active running chrony, an NTP client/server
cron.service    loaded active running Regular background program processing daemon
dbus.service    loaded active running D-Bus System Message Bus
fwupd.service   loaded active running Firmware update daemon
getty@tty1.service loaded active running Getty on tty1
hv-kvp-daemon.service loaded active running Hyper-V KVP Protocol Daemon
ModemManager.service loaded active running Modem Manager
multipathd.service loaded active running Device-Mapper Multipath Device Controller
networkd-dispatcher.service loaded active running Dispatcher daemon for systemd-networkd
polkit.service   loaded active running Authorization Manager
rsyslog.service  loaded active running System Logging Service
serial-getty@ttyS0.service loaded active running Serial Getty on ttyS0
ssh.service     loaded active running OpenBSD Secure Shell server
systemd-journald.service loaded active running Journal Service
systemd-logind.service loaded active running User Login Management
systemd-networkd.service loaded active running Network Configuration
systemd-resolved.service loaded active running Network Name Resolution
systemd-udevd.service loaded active running Rule-based Manager for Device Events and Files
udisks2.service  loaded active running Disk Manager
unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
user@1000.service loaded active running User Manager for UID 1000
walinuxagent.service loaded active running Azure Linux Agent

Legend: LOAD  → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB   → The low-level unit activation state, values depend on unit type.

22 loaded units listed.

BlueTeam@BlueTeam:~/Entrega2$ |
```

RedTeam:

No funciona Nmap en la maquina

```
RedTeam@RedTeam:~/Entrega2$ sudo ./scanner.py
Traceback (most recent call last):
  File "/home/RedTeam/Entrega2./scanner.py", line 2, in <module>
    import nmap
ModuleNotFoundError: No module named 'nmap'
RedTeam@RedTeam:~/Entrega2$ |
```