



Avance 1 del proyecto

Integrantes:

Alexandra Mora Brenes

Isaac David Robles Meza

Jurgen Brenes Arce

Kennan Joved Sánchez Garro

Santiago Murillo Campos

Curso: Programación avanzada

Profesor: Andres Felipe Vargas Rivera

III Cuatrimestre 2025

1. Roles del grupo

Nombre	Rol de cada uno	Pequeña descripción
Alexandra Mora Brenes	Es la coordinadora del proyecto y de toda la documentación	Se encarga de reunir toda la información, de la elaboración del documento y organiza la entrega del proyecto
Isaac David Robles Meza	Es el encargado de la parte del repositorio	Se encarga de crear la estructura del repositorio, también el README.md y de mantener el orden de archivos
Jurgen Brenes Arce	Es el encargado de la parte del firewall	Se encarga de desarrollar el script y de verificar que funcione correctamente
Kennan Joved Sánchez Garro	Es el administrador de la VM	Se encarga de configurar la maquina virtual, de ejecutar el script y de tomar evidencias
Santiago Murillo Campos	Es el encargado de la verificación y las pruebas	Se encarga de realizar el escaneo Nmap desde otra VM y de tomar evidencias

2. IP de la VM y puertos permitidos

- Sistema operativo utilizado: Ubuntu
- La IP asignada: 158.23.162.91
- Los puertos permitidos:
 - 22 → SSH
 - 80 → HTTP
 - 443 → HTTPS

3. Pasos rápidos de creación de la VM en Azure

1. Ingresar a Microsoft Azure (portal.azure.com).
2. Ingresar al servicio de creación de recursos.
3. Seleccionar la opción de "Crear" Máquina Virtual.
4. Anotar los datos básicos solicitados (Ejemplo: Grupo de recursos, Nombre de Máquina Virtual, Región (la más cercana a CR), nivel de seguridad, la imagen del sistema operativo a instalar, la arquitectura de la VM, tamaño, usuario, contraseña, puertos accesibles desde la red pública) etc.
5. Escoger el tamaño de Disco del OS, el tipo de disco (SSD o HDD), y también si se desea eliminar cuando se elimine la VM.
6. Rellenar los datos de las redes, Ejemplo: seleccionar red, ip pública, puertos de entrada públicos y si se desea equilibrio de carga.
7. Administrar todo lo que tiene que ver con: Microsoft Defender Cloud, Identidad, Apagado Automático, copia de seguridad, recuperación ante desastres y actualizaciones del OS.8.
8. Realizar la supervisión: Diagnósticos de arranque.
9. Etiquetas, si se desea.
10. Revisar y crear.

Datos de la creación:

Nombre de la VM> PrograAvanzadaG5

Region> Mexico Central

Zona de disponibilidad > Zona 2

Tipo de seguridad> Estandar

Imagen Ubuntu Server 22.04 LTS - x64 gen 2

Arquitectura > x64

Tamano> Standard_D2ls_v5 - 2 vcpu, 4 GiB de memoria (\$68.26/mes)

Usuario> Progra_G5

Contrasena> Grupo5_Progra

Discos

Reglas de puerto de entrada> Puertos de entrada publicos > 80, 443, 22

Disco del SO> 30GB

Tipo de disco> SSD Estandar

Redes

Red Virtual> Grupo5_Progra

Subred> (nuevo) default (10.0.0.0/24)

Grupo de seguridad de red de NIC> Basico

Puertos de entrada publicos> 80,443,22

Equilibrio de carga> Ninguno

Administración

Microsoft Defender for Cloud> Habilitar el plan básico de forma gratuita

Diagnostico> Todo se deja por defecto

Contraseña y Usuario:

Usuario: Progra_G5

Contraseña: Grupo5_Progra

4. Buenas prácticas

Asegurarse de apagar la VM cuando no esté en uso.

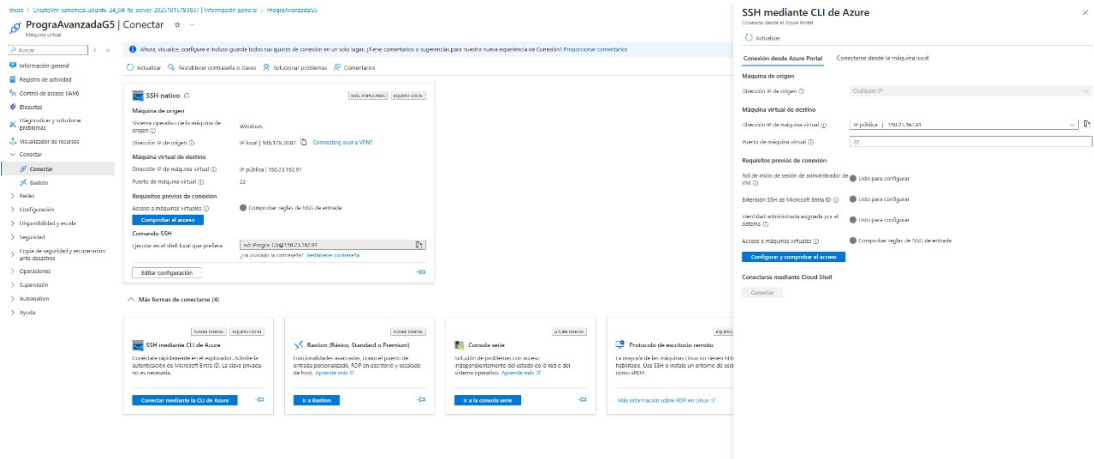
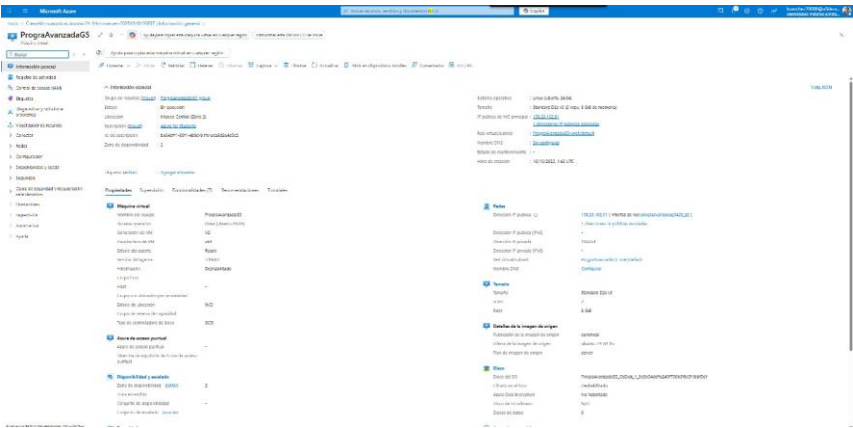
Del todo no exponer puertos innecesarios.

Siempre mantener el firewall activo y sobre todo revisado.

Solamente subir solo los archivos requeridos al repositorio.

Siempre documentar todo con capturas claras y evidencias.

5. Evidencias del avance



SSH mediante CLI de Azure

Conexión desde el Azure Portal

Actualizar

Conexión desde Azure Portal

Conectarse desde la máquina local

Máquina de origen

Dirección IP de origen

Máquina virtual de destino

Dirección IP de máquina virtual

Puerto de máquina virtual

Requisitos previos de conexión

Rol de inicio de sesión de administrador de VM ☐ Listo para configurar

Extensión SSH de Microsoft Entra ID ☐ Listo para configurar

Identidad administrada asignada por el sistema ☐ Listo para configurar

Acceso a máquinas virtuales ☐ Comprobar reglas de NSG de entrada

Configurar y comprobar el acceso

Conectarse mediante Cloud Shell

Conectar

```
Progra_G5@PrograAvanzada:~$ ssh -o StrictHostKeyChecking=no 158.23.162.91
Warning: Permanently added '158.23.162.91' (ED25519) to the list of known hosts.
Progra_G5@158.23.162.91's password:
Permission denied, please try again.
Progra_G5@158.23.162.91's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1012-azure x86_64)

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

System information as of Thu Oct 16 01:59:25 UTC 2025

System load:  0.0          Processes:      117
Usage of /:   6.4% of 28.02GB Users logged in:    0
Memory usage: 4%          IPv4 address for eth0: 10.0.0.4
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

26 updates can be applied immediately.
13 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Progra_G5@PrograAvanzadaG5:~$
```

```
santimur@ubuntuserver:~/blue_team$ chmod +x firewall.basic.sh
santimur@ubuntuserver:~/blue_team$ sudo ./firewall.basic.sh
Guardando una copia de las reglas actuales por seguridad
Limpiando todas las reglas existentes
Estableciendo políticas predeterminadas
Permitidos el tráfico local (loopback)
Permitiendo conexiones ya establecidas o relacionadas
Permitiendo conexión por SSH (puerto 22)
Permitiendo tráfico por web HTTP (puerto 80)
Permitiendo tráfico web seguro HTTPS (puerto 443)
santimur@ubuntuserver:~/blue_team$
```

6. Conclusiones

-Todo el entorno del trabajo fue configurado de la manera correcta, con la estructura del proyecto que fue establecida por el profesor y además realizamos el firewall 100% funcional.

-Se reviso que la conectividad a través de los puertos 22, 80 y 443 de manera correcta.

-Se cumplio con la organización del equipo de trabajo y se cumplieron los requerimientos de seguridad que se pedían.