



Avance Final 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 'Create a virtual machine' wizard in Microsoft Azure. The current step is 'Detalles del proyecto' (Project details). The user has selected 'Azure for Students' as the subscription and '(Nuevo) BlueTeam_group' as the resource group. Under 'Detalles de instancia' (Instance details), the name is set to 'BlueTeam', region to '(US) West US', and availability option to 'Conjunto de disponibilidad' (Availability set). A note indicates that creating an availability set allows for managing, configuring, and scaling virtual machines with load balancing. At the bottom, there are buttons for '< Anterior' (Previous), 'Siguiente: Discos' (Next: Disks), 'Revisar y crear' (Review + Create), and 'Enviar comentarios' (Send feedback).

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The current step is 'Configuración de la máquina virtual' (Virtual machine configuration). The user has selected 'No hay conjuntos de disponibilidad en la ubicación y el grupo de recursos a...' (No availability sets in the location and resource group) for the availability set. Other settings include 'Máquinas virtuales de inicio seguro' (Secure boot virtual machines) for security type, 'Ubuntu Server 24.04 LTS - x64 gen. 2' for the image, 'x64' for architecture, and 'Standard_D2s_v3 - 2 vcpu, 8 GiB de memoria (\$85.41/mes)' for the size. Under 'Cuenta de administrador' (Administrator account), 'Clave pública SSH' (SSH public key) is selected for authentication type. At the bottom, there are buttons for '< Anterior' (Previous), 'Siguiente: Discos' (Next: Disks), 'Revisar y crear' (Review + Create), and 'Enviar comentarios' (Send feedback).

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

Supervisión

Configure las opciones de supervisión de la máquina virtual.

Alertas

Habilitar reglas de alerta recomendadas

Reglas de alerta no configuradas

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

Total mensual estimado: 0.00 USD

< Anterior | Siguiente: Opciones avanzadas > | 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

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](#)

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](#)

Apagado automático

Habilitar apagado automático

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

Zona horaria: (UTC-06:00) Centroamérica

Notificación antes del apagado

< Anterior | Siguiente: Supervisión > | Revisar y crear | Enviar comentarios

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

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

Red virtual * (nuevo) BlueTeam-vnet | Crear nuevo

Subred * (nuevo) default (10.0.0.0/24) | Crear nuevo

IP pública (nuevo) BlueTeam-ip | Crear nuevo

Grupo de seguridad de red de NIC Ninguno | Básico | Opciones avanzadas

Configurar el grupo de seguridad de red (nuevo) BlueTeam-nsg | Crear nuevo

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 | Enviar comentarios

Crear una máquina virtual

Cuenta de administrador

Tipo de autenticación: Contraseña

Nombre de usuario: admin_blue

Contraseña: redacted

Confirmar contraseña: redacted

Reglas de puerto de entrada

Selección de 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: Permitir los puertos seleccionados

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

< Anterior | Siguiente: Discos > | Revisar y crear | Enviar comentarios

CreateVm-canonical.ubuntu-24_04-lts-server-20251013222217 | Información general

Se completó la implementación

Nombre de implementación: CreateVm-canonical.ubuntu-24_04-lts...
Suscripción: Azure for Students
Grupo de recursos: BlueTeam_group

Hora de inicio: 13/10/2025, 11:03:21 p.m.
Id. de correlación: 0c744483-3d4d-421a-9bfb-40391832cbc1

Detalles de implementación

Pasos siguientes

- Configurar el apagado automático Recomendado
- Supervisar el estado, el rendimiento y las dependencias de red de la máquina virtual Recomendado
- Ejecutar un script dentro de la máquina virtual Recomendado

Ir al recurso | Crear otra VM | Enviar comentarios | Cuéntenos su experiencia con la implementación

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%
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
        ether fe80::20d:3aff:fe30:d7df  txqueuelen 1000  (Ethernet)
            RX packets 35457  bytes 47793311 (47.7 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 6667  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
        ether 00:0d:3a:30:d7:df  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 7.94SVN ( 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 (0.0001s 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.

Subscription *

Resource group *

Azur

(New

Create

Size *

Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$70.08/month)

[See all sizes](#)



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

Instance details

Virtual machine name *

Redf

Administrator account

(US)

Deploy

Region *

Authentication type

SSH public key

Password

Username *

red_team

Password *

.....

Confirm password *

.....

Availability options

Security type

Trust

Config

Image *

See all

VM architecture

A

X

Run with Azure Spot discount

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

None

Allow selected ports

Select inbound ports *

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

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

< Previous

Next : Disks >

[Review + create](#)

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](#)

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%

Basics

Subscription

Azure for Students

Resource group

(new) RedTeam_group

Virtual machine name

RedTeam

Region

West US 3

Availability options

No infrastructure redundancy required

Zone options

Self-selected zone

Security type

Trusted launch virtual machines

Enable secure boot

Yes

Enable vTPM

Yes

Integrity monitoring

No

Image

Ubuntu Server 24.04 LTS - Gen2

x64

VM architecture

Standard D2s v3 (2 vcpus, 8 GiB memor

Size

No

Enable Hibernation

Password

Authentication type

red_team

Username

SSH, HTTPS, HTTP

Public inbound ports

No

Azure Spot

Disks

OS disk size

Image default

OS disk type

Standard HDD LRS

Use managed disks

Yes

Delete OS disk with VM

Enabled

Ephemeral OS disk

No

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
Boot diagnostics	On
Enable OS guest diagnostics	Off
Enable application health monitoring	Off
Advanced	
Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

[< Previous](#)
[Next >](#)
Create

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.

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 ... ↑
BlueTeam	Azure for Stud...	BlueTeam_group	West US	Detenido (desa...)	Linux	Standard_D2s_v3	172.184.103.17

3. Puertos Permitidos (NSG):

HTTP: 80

HTTPS: 443

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

red_team/scann.py

Corre un script importando las librerías nmap (para escaneo de red) y os (para detectar la carpeta actual) y se realiza un scan con diferentes flags.

Se especifican los diferentes tipos de escaneo que vamos a realizar en la variable “options”:

- -sS: escaneo TCP SYN
- -sV: detecta la versión del servicio
- -Pn: tratar a todos los hosts como online (se salta el ping)
- -p 1-1000: puertos a escanear

README.md – Red Team: Ataque y Evaluación de Seguridad

Propósito

Este módulo documenta las herramientas, técnicas y procedimientos utilizados por el Red Team para identificar vulnerabilidades, ejecutar ataques controlados y evaluar la postura de seguridad de la máquina virtual del Blue Team en Azure.

Roles y Responsabilidades

- Simular ataques reales de ciberseguridad.
- Identificar debilidades en la configuración de la VM.
- Documentar hallazgos y proponer mejoras.
- Utilizar scripts en Python para automatizar escaneos y ataques.

Requisitos Técnicos

- Python 3.x
- Módulos: nmap, scapy, paramiko, os, subprocess, logging
- Acceso a una VM en la misma red que el Blue Team
- Azure CLI (opcional para gestión de recursos)

Scripts Ofensivos

Script	Descripción
scanner.py	Escaneo de puertos y servicios usando Nmap desde Python.
packet_attack.py	Ataques de red como sniffing y ARP Spoofing con Scapy.
ssh_brute.py	Ataque de diccionario al servicio SSH usando Paramiko.
report.md	Documentación detallada del ataque, hallazgos y recomendaciones.

Instrucciones de Ejecución

1. scanner.py

```
sudo python3 scanner.py
```

- Realiza escaneo básico y avanzado.
- Genera reporte de puertos abiertos y servicios activos.

2. packet_attack.py

```
sudo python3 packet_attack.py
```

- Ejecuta sniffing de paquetes TCP.
- Simula ataques ARP/DNS spoofing.

3. ssh_brute.py

```
python3 ssh_brute.py
```

- Requiere diccionario de contraseñas.
- Intenta acceso por fuerza bruta al puerto 22.

Evaluación del Éxito

- Acceso no autorizado a la VM del Blue Team.
- Identificación de puertos inseguros o servicios expuestos.
- Captura de tráfico sensible.
- Documentación clara de vulnerabilidades y recomendaciones.

Estructura del Directorio

```
red_team/
```



Buenas Prácticas

- No ejecutar ataques fuera del entorno controlado.
- Documentar cada paso y resultado.
- Validar que las herramientas estén correctamente instaladas.
- Apagar la VM cuando no esté en uso para conservar créditos de Azure.

README – Blue Team: Defensa y Monitoreo en Azure

Propósito

Este módulo documenta las herramientas, técnicas y procedimientos utilizados por el Blue Team para proteger, monitorear y mantener la seguridad de la máquina virtual en Azure.

Roles y Responsabilidades

- Implementar medidas de defensa y mitigación.
- Monitorear eventos y alertas de seguridad.
- Responder a incidentes y realizar análisis forense.
- Utilizar scripts en Python para automatización y auditoría.

Requisitos Técnicos

- Python 3.x
- Módulos: psutil, os, subprocess, logging, paramiko
- Acceso a la VM en Azure
- Azure CLI para gestión y monitoreo

Scripts Defensivos

Script	Descripción
<u>monitor.py</u>	Monitoreo de procesos, uso de CPU y memoria en tiempo real.
<u>log_audit.py</u>	Auditoría y análisis de logs del sistema para detectar anomalías.
<u>alert.py</u>	Envío de alertas por correo o mensajes ante eventos sospechosos.

Instrucciones de Ejecución

1. monitor.py

```
python3 monitor.py
```

- Monitorea recursos del sistema y genera reportes.

2. log_audit.py

```
python3 log_audit.py
```

- Analiza logs para detectar patrones inusuales.

3. alert.py

```
python3 alert.py
```

- Configura y envía alertas en tiempo real.

4. response.py

```
python3 response.py
```

- Ejecuta acciones automáticas para mitigar amenazas.

Evaluación del Éxito

- Detección temprana de ataques o anomalías.
- Respuesta rápida y efectiva a incidentes.
- Mantenimiento de la integridad y disponibilidad de la VM.
- Documentación clara de eventos y acciones tomadas.

Estructura del Directorio

blue_team/

```
├── monitor.py
├── log_audit.py
└── alert.py
└── response.py
```

Buenas Prácticas

- Mantener actualizadas las herramientas y scripts.
- Revisar periódicamente los logs y alertas.
- Documentar todas las acciones y hallazgos.
- No ejecutar scripts en producción sin pruebas previas.
- Asegurar la comunicación segura entre componentes.Azure.

Evidencias de ejecución:

BlueTeam (defensa)

sudo ./firewall_basic.sh

```
BlueTeam@BlueTeam:~$ sudo ./firewall_basic.sh
Reseteando UFW a estado por defecto (si está instalado)...
Backing up 'user.rules' to '/etc/ufw/user.rules.20251217_032402'
Backing up 'before.rules' to '/etc/ufw/before.rules.20251217_032402'
Backing up 'after.rules' to '/etc/ufw/after.rules.20251217_032402'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20251217_032402'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20251217_032402'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20251217_032402'

Estableciendo políticas por defecto: deny incoming, allow outgoing
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
Habilitando logging (low) y habilitando UFW
```

sudo python3 ./os_audit.py

```
new profiles. skip
BlueTeam@BlueTeam:~$ sudo python3 os_audit.py
Auditoria básica del sistema

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

--- Puertos abiertos ---
Netid State Recv-Q Local Address:Port Peer Address:PortProcess
udp  UNCONN 0      127.0.0.54:53      0.0.0.0:*
udp  UNCONN 0      127.0.0.53%lo:53    0.0.0.0:*
udp  UNCONN 0      10.0.0.4%eth0:68   0.0.0.0:*
udp  UNCONN 0      127.0.0.1:323     0.0.0.0:*
udp  UNCONN 0      [::1]:323        [::]:*
```

sudo python3 ./alert_logger.py

```
BlueTeam@BlueTeam:~$ sudo python3 alert_logger.py
== Alert Logger del Blue Team ==
Esperando alertas desde otros módulos...

Realizando pruebas locales del logger:

/home/BlueTeam/alert_logger.py:34: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetime.
  "timestamp": datetime.utcnow().isoformat(),
[INFO] selftest: Inicio del módulo de alertas.
[WARN] selftest: Actividad sospechosa detectada.
[AUTO] Advertencia registrada. No se requiere acción inmediata.
[CRIT] selftest: Posible intrusión detectada.
[AUTO] ALERTA CRÍTICA. Requiere intervención manual.
[AUTO] Detalle: Posible intrusión detectada.

[OK] alert_logger.py está funcionando correctamente.
```

sudo python3 ./sniffer_defence.py

```
Solo se mostrarán alertas CRÍTICAS (port scans)
Las alertas de puertos sensibles se guardan en log
Ejecutando... (Ctrl+C para detener)
=====

/home/BlueTeam/sniffer_defense.py:68: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use time
now = datetime.utcnow()
[WARNING] sniffer_defense: Trafico a puerto sensible 22 (TCP) desde 177.93.10.96 hacia 10.0.0.4
[WARNING] sniffer_defense: Trafico a puerto sensible 80 (TCP) desde 10.0.0.4 hacia 168.63.129.16
[WARNING] sniffer_defense: Trafico a puerto sensible 22 (TCP) desde 52.225.31.164 hacia 10.0.0.4
[CRITICAL] sniffer_defense: POSIBLE PORT SCAN desde 168.63.129.16. Contacto 20 puertos en 60 segundos.
[AUTO] ALERTA CRÍTICA. Requiere intervención manual.
[AUTO] Detalle: POSIBLE PORT SCAN desde 168.63.129.16. Contacto 20 puertos en 60 segundos.
[WARNING] sniffer_defense: Trafico a puerto sensible 80 (TCP) desde 52.225.31.164 hacia 10.0.0.4
[WARNING] sniffer_defense: Trafico a puerto sensible 443 (TCP) desde 52.225.31.164 hacia 10.0.0.4
```

RedTeam (ataque)

```
sudo python3 ./scanner.py
```

```
RedTeam@RedTeam:~$ sudo python3 scanner.py
Host: 20.228.97.25
State: up
Protocol: tcp
Port: 22 State: open
Port: 80 State: closed
Port: 443 State: closed
RedTeam@RedTeam:~$ cat report.txt
Host: 20.228.97.25
State: up
Protocol: tcp
Port: 22 State: open
Port: 80 State: closed
Port: 443 State: closed
```

```
sudo python3 ./packet_attack.py
```

```
RedTeam@RedTeam:~$ sudo python3 packet_attack.py
--- Envío seguro de paquetes Scapy (Azure Lab) ---

[~] Enviando ping (ICMP Echo)...
[X] Sin respuesta al ping

[~] Enviando packet TCP SYN seguro...
[X] No hubo respuesta TCP

[~] Enviando paquete UDP de laboratorio...
[OK] Paquete UDP enviado (no disruptivo)

[OK] Simulación completada. Revisa packet_lab.log para ver los registros.
```

```
sudo python3 ./ssh_brute.py
```

```
RedTeam@RedTeam:~$ sudo python3 ssh_brute.py
[X] Falló: BlueTeam:1234
[X] Falló: BlueTeam:password
[X] Falló: BlueTeam:admin
[OK] Acceso logrado: BlueTeam:Jb8QHdBy@LDtA8y
```