ARQUITECTURA GENERAL

RED TEAM PC Local, Python

BLUE TEAM VM en Azure, Linux

INICIO

FIREWALL_BASIC.SH
Configura iptables
Política DROP
Abre 22, 80, 443

SNIFFER_DEFENSE.PY
(Modo Escucha)

SETUP

ENTRADA
Ingresar IP objetivo

SCANNER.PY
nmap -sS -sV -Pn
Guarda resultados

ATAQUE

ENTRADA
Puerto objetivo
Cantidad de SYN
Delay

PACKET_ATTACK.PY
Envía paquetes SYN a la VM
Emula intento de intrusión

SNIFFER_DEFENSE.PY
¿El paquete es TCP?
¿Flag == SYN?
¿Puerto inusua?
defense_log.txt

OS_AUDIT.PY
Puertos abiertos
Procesos y estado del sistema

FIN