DGTIC Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Implementación automatizada de entornos de pruebas de seguridad

Baruch Guerra Rodolfo

Portillo Castro Karina Ximena

Valverde Martínez Alberto

Descripción

- La herramienta **Sandbox Generator** sirve para **automatizar la creación y configuración de entornos virtuales**

- Funciona con un **archivo de entrada** en formato JSON, el cual contiene la configuración para las máquinas virtuales (VMs) a implementar

- Desarrollado para trabajar en Windows Server 2019, con el hipervisor de Windows (**Hyper-V**)

SO	Servicios/Funcionalidades disponibles
Windows Server 2019	● Windows Defender ● Active Directory (AD) ● Certificate Services ● IIS ● DHCP ● DNS
Linux/Unix **(**Debian 10, Kali Linux 2020.04, CentOS 8/Stream, RHEL 8, Familia Ubuntu**)**	● Servidor Web (Apache/Nginx) ● RDBMS (MariaDB, MySQL, PostgreSQL, SQL Server*) ● DHCP ● Bind DNS ● Iptables ***:** disponible sólo en la familia Ubuntu (Xenial 16.04, Bionic 18.04 y Focal 20.04)
Clientes Windows 10	● Instalación de paquetes MSI
FortiOS	● Restaurar desde un backup

Objetivo

Reducir la interacción humana y el tiempo utilizado en la creación y configuración de entornos virtuales de prueba mediante la especificación de los requerimientos en un archivo único que:

- Genere infraestructuras virtuales replicables
- Instale y configure servicios requeridos
- Evite errores de lógica y/o de recursos

Herramientas utilizadas

Windows Server 2019

- Hyper-V
- Powershell
- **DISM:** generar archivos de disco duro virtual (.vhd,vhdx) válidos

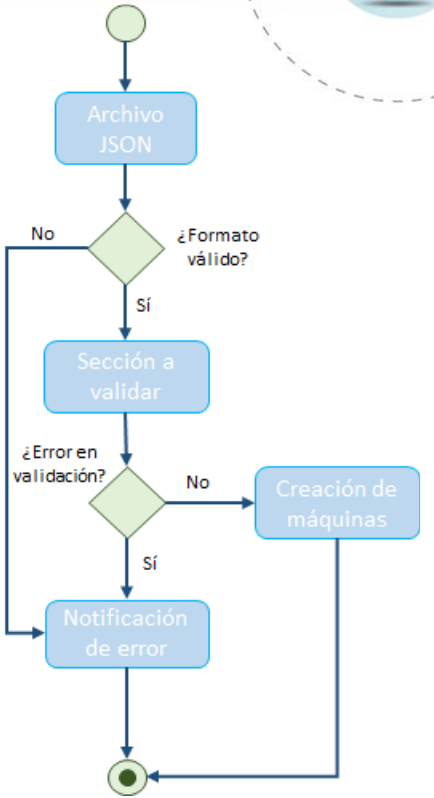
Herramientas utilizadas

WLS: Subsistema de Linux para Windows

- **whois**: generar estructuras válidas para el archivo /etc/passwd con la herramienta mkpasswd la cual es parte del paquete
- **dos2unix**: evitar errores de EoL al hacer la transición Windows --> Linux
- **mkisofs**: generar archivos de imagen .iso válidos para Linux/FortiOS

Metodología de desarrollo

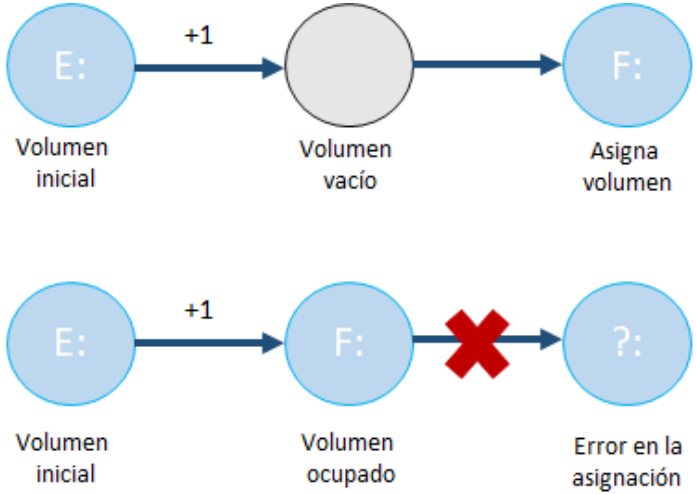
1. Validación del archivo de entrada
2. Revisión de secciones del archivo de entrada
    1. Datos generales de la VM
    2. Datos dependientes de la VM
    3. Datos de los servicios por SO
3. Creación de máquinas
    1. Presentación de los datos ingresados
    2. Confirmación
    3. Creación de ruta raíz, folders necesarios, etc.
    4. Creación de VM dentro de Hyper-V
    5. Creación de vhdx o iso
    6. Instalación y configuración de servicios



Demostración

Problemas y retos presentados

- Conflictos con el manejo de discos durante la creación de las imágenes de los sistemas operativos creados



Problemas y retos presentados

- Es necesario ejecutar un script para finalizar la configuración estipulada en los siguientes sistemas operativos:
  - Debian 10 Buster
  - Kali Linux 20.04
  - Ubuntu Family
  - Windows Server 2019 únicamente si el servicio IIS es configurado

Oportunidades de mejora

- Ampliar el alcance de la herramienta para otros hipervisores como VirtualBox o VMWare
- Implementación de un administrador web que permita generar archivos de entrada válidos de manera más intuitiva
- Agregar nuevos valores a los ya existentes:
  - Sistemas Operativos/Versiones
  - Servicios
  - Configuraciones y validaciones más robustas para los servicios
- Ejecución de procesos simultáneos para optimizar los recursos del equipo host

Conclusiones

La herramienta cumple con su objetivo, ya que minimiza los tiempos requeridos por los usuarios para creación y replicación de entornos de prueba específicos, además de proporcionar validaciones que disminuyen la presencia de errores durante el proceso.

Documentación

- Repositorio del proyecto: https://github.com/barvch/generador-de-sandbox
- Creación de archivo de entrada válido: https://drive.google.com/file/d/1F-kv7awZ0BfdEEHCnjH5ICOtm8Yp7JoA/view
- Interacción y flujo de la herramienta: https://drive.google.com/file/d/1rf91jSrD6FEsrO-s-RIStoBLzxlkfeel/view

¡Gracias por su atención!

¿Preguntas?