# Tema 3b: Análisis dinámico

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática

# Índice

# Introducción

- El análisis dinámico implica ejecutar un binario en un entorno controlado para comprobar su comportamiento
  - Simular servicios
- Es un análisis que consiste en monitorizar…:
  - Actividades (los procesos o hilos),
  - Interacciones, y
  - Efectos sobre el sistema

# Índice

# Monitorización del sistema

- Monitorización de procesos
  - Su actividad y ejecución
- Monitorización del sistema de ficheros
  - Durante la ejecución del malware
- Monitorización de registros
  - Acceso/modificación, datos, ...
- Monitorización de red
  - Tráfico en tiempo real

# Índice

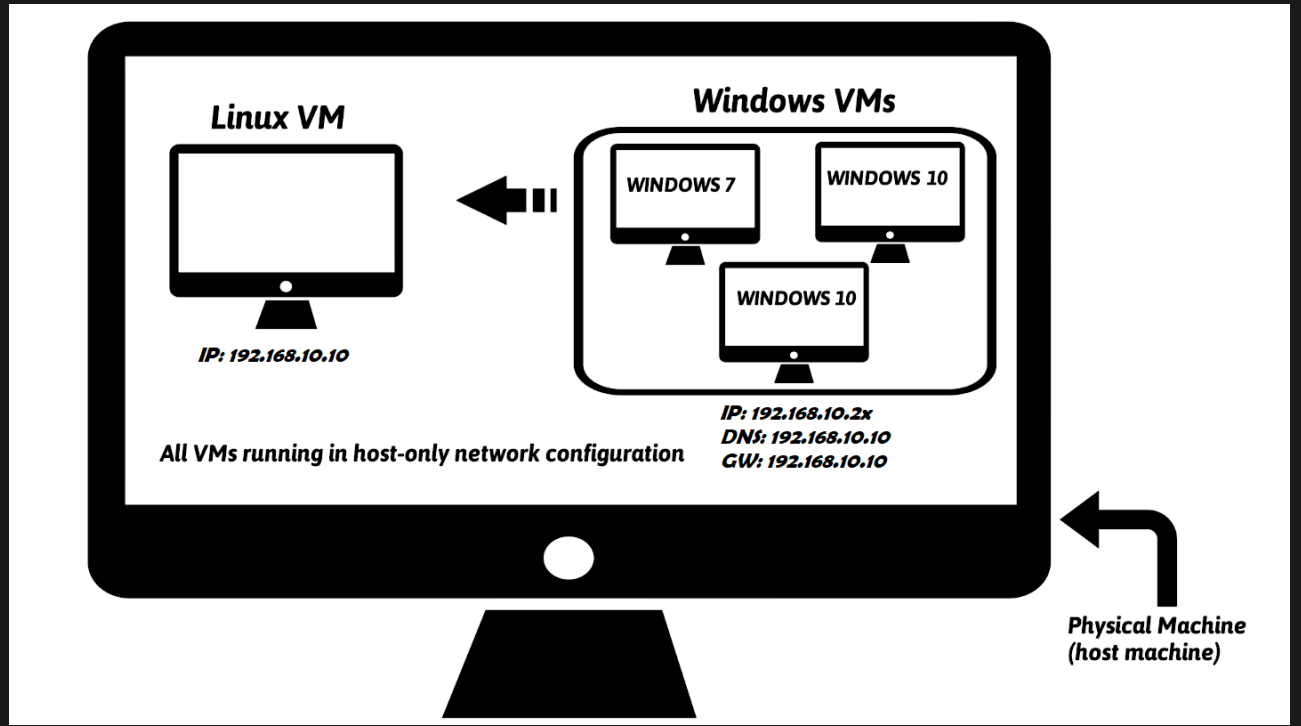
# Herramientas de análisis dinámico

- Process Hacker – Procesos ejecutándose en el sistema
- Process Monitor – Comprobar la interacción de los procesos con el sistema de ficheros, registros, y otros procesos e hilos
- Noriben – Incluye filtros sobre la actividad llevada a cabo en el sistema
- Wireshark – Captura el tráfico de red
- InetSim – Simulación de servicios

# Índice

# Pasos a seguir

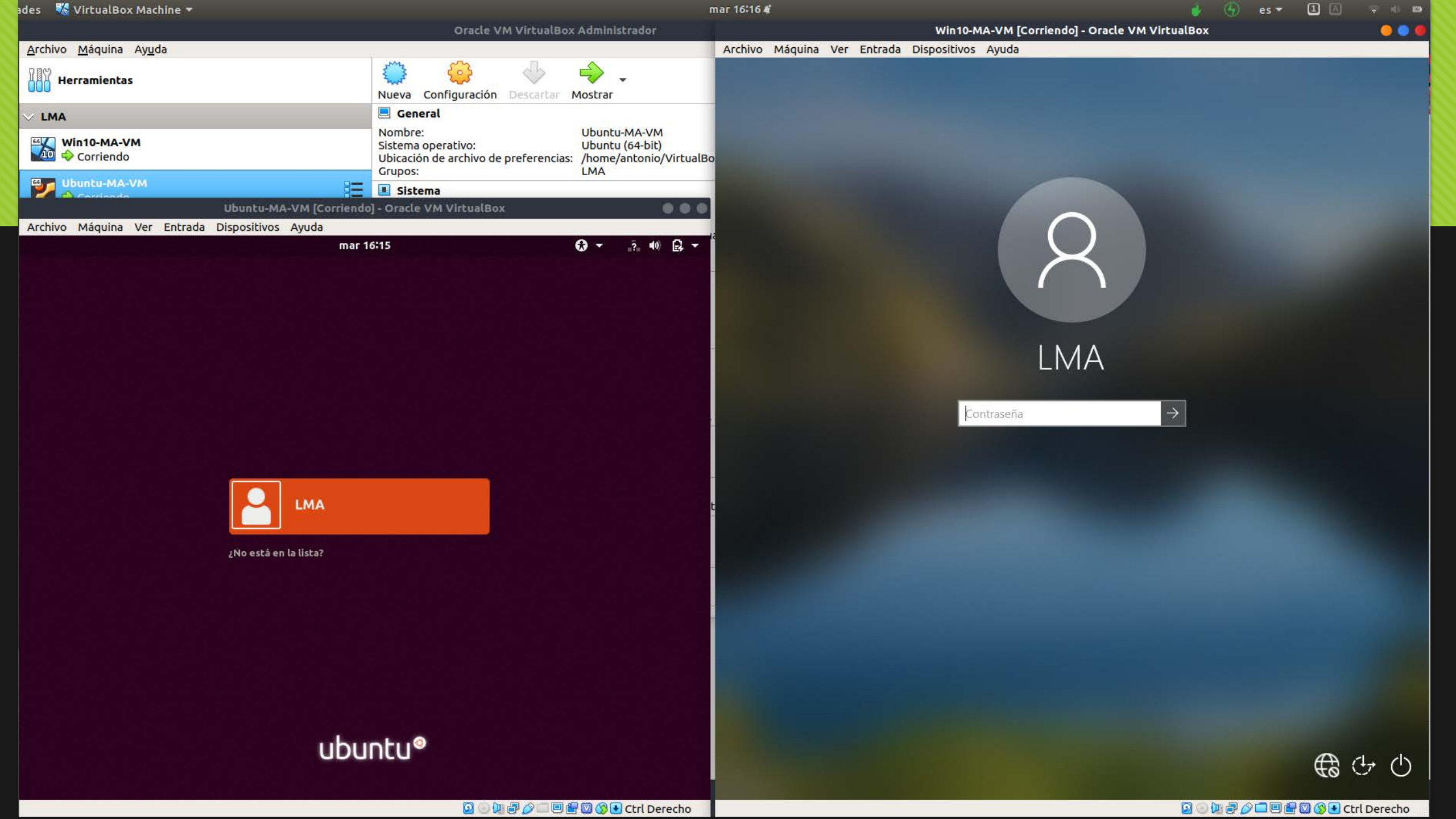
- Pasos para llevar a cabo un análisis de malware dinámico:
  - Volver a un estado seguro en el entorno controlado
  - Ejecutar las herramientas de análisis y monitorización dinámica
  - Ejecutar el malware (o posible malware)
  - Parar las herramientas de monitorización
  - Analizar los resultados obtenidos



# Índice

# Análisis estático y dinámico conjunto (I)

- Realizar primero un análisis estático para obtener información relacionada con el binario sin estar en ejecución (metadatos, ...)
  - Análisis exploratorio
- Ejemplo de uso en un entorno virtual controlado:
  - MV Linux, que simulará los servicios de red y hará de enlace entre la red virtual y la red física
  - MV Windows, donde se ejecutará el binario


VirtualBox Machine
mar 16:16
es
Oracle VM VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nueva Configuración Descartar Mostrar
LMA
Win10-MA-VM
Corriendo
Ubuntu-MA-VM
General
Nombre: Ubuntu-MA-VM
Sistema operativo: Ubuntu (64-bit)
Ubicación de archivo de preferencias: /home/antonio/VirtualBo
Grupos: LMA
Sistema
Ubuntu-MA-VM [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
mar 16:15
LMA
¿No está en la lista?
ubuntu
Ctrl Derecho
Win10-MA-VM [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
LMA
Contraseña
Ctrl Derecho

# Análisis estático y dinámico conjunto (III)

- MV Linux, que simulará los servicios de red y hará de enlace entre la red virtual y la red física
  - *Process Hacker*, para examinar los atributos de los procesos
  - *Noriben Python (*y *Process Monitor)*, para inspeccionar la interacción del malware con el sistema
- MV Windows, donde se ejecutará el binario
  - *InetSim*, para simular los servicios de red
  - Wiresharck, para capturar el tráfico de red
- Ejecutar durante 40 segundos, y parar todos los programas y servicios simulados
- Examinar el comportamiento del malware

# Índice

# Análisis de librerías DLL (I)

- El malware podría ser capaz de utilizar funciones, llamadas *exported functions*, en las Dynamic-Link Libraries (DLLs)
  - Windows contiene varias DLLs que exportan APIs
  - Interacción con el sistema de archivos, procesos, registros, redes e interfaces gráficas
- Herramienta de ejemplo: CFF Explorer

# Análisis de librerías DLL (II)

- Razones de implementar malware como una DLL:
  - No se pueden ejecutar haciendo doble click
  - Necesitan un proceso anfitrión (capacidad de esconder acciones)
  - Capacidad de persistencia
  - Acceso a toda la memoria y funcionalidad del proceso anfitrión
  - Una DLL no se puede analizar directamente
- Ejemplo: rundll32.exe (puede ser utilizado para ejecutar una DLL)

# Tema 3b: Análisis dinámico

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática