Tema 1: Introducción al análisis de Malware

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática

Índice

Introducción (I)

- El malware se define como el código informático, en cualquiera de sus posibles formas, que realiza acciones maliciosas sobre un sistema.
- Los canales de acceso son muy variados (e-mail, web, USBs…)
- Algunas acciones realizadas por malware:
  - Interrupción de operaciones
  - Robo de información
  - Acceso no autorizado a recursos
  - Espionaje
  - Envío de Spam
  - Ataques distribuidos de denegación de servicio (DDOS)
  - Bloqueo de archivos y petición de rescate (Ransomware)

Introducción (II)

- Tipos de malware:
  - Virus o gusanos: Basados en la autocopia, el virus requiere la intervención del usuario, el gusano no.
  - Troyanos: Malware disimulado como un programa normal para ser instalado.
  - *Remote Access Trojan (RAT)*: También conocidos como *backdoor trojans*, permite el acceso y ejecución de comandos en el equipo comprometido.
  - *Adware*: Usualmente transmitidos mediante descargas gratuitas, ofrece publicidad no deseada al usuario.
  - *Botnet*: Grupo de ordenadores infectados con el mismo malware para realizar acciones conjuntas (por ejemplo, DDOS).
  - Ladrón de información: Malware como *key loggers*, *spyware* o *sniffers* especialmente diseñado para el robo de información (tarjetas bancarias, contraseñas, etc.).
  - *Ransomware*: Bloquea usuarios o encripta archivos del ordenador infectado para pedir un rescate por ellos a continuación.
  - *Rootkit*: Permite acceso privilegiado y oculto a otros programas en el ordenador infectado.
  - *Downloader / Dropper*: Permite descargas o instalaciones no deseadas de componentes malware.

Análisis de Malware (I)

- **Definición:**
  - El análisis de malware se basa fundamentalmente en el estudio del comportamiento de programas clasificados como malware, con el objetivo de entender su funcionamiento, y desarrollar técnicas de detección y eliminación. Implica el análisis de archivos binarios sospechosos en entornos seguros de forma que se puedan identificar características y patrones para construir mejores defensas

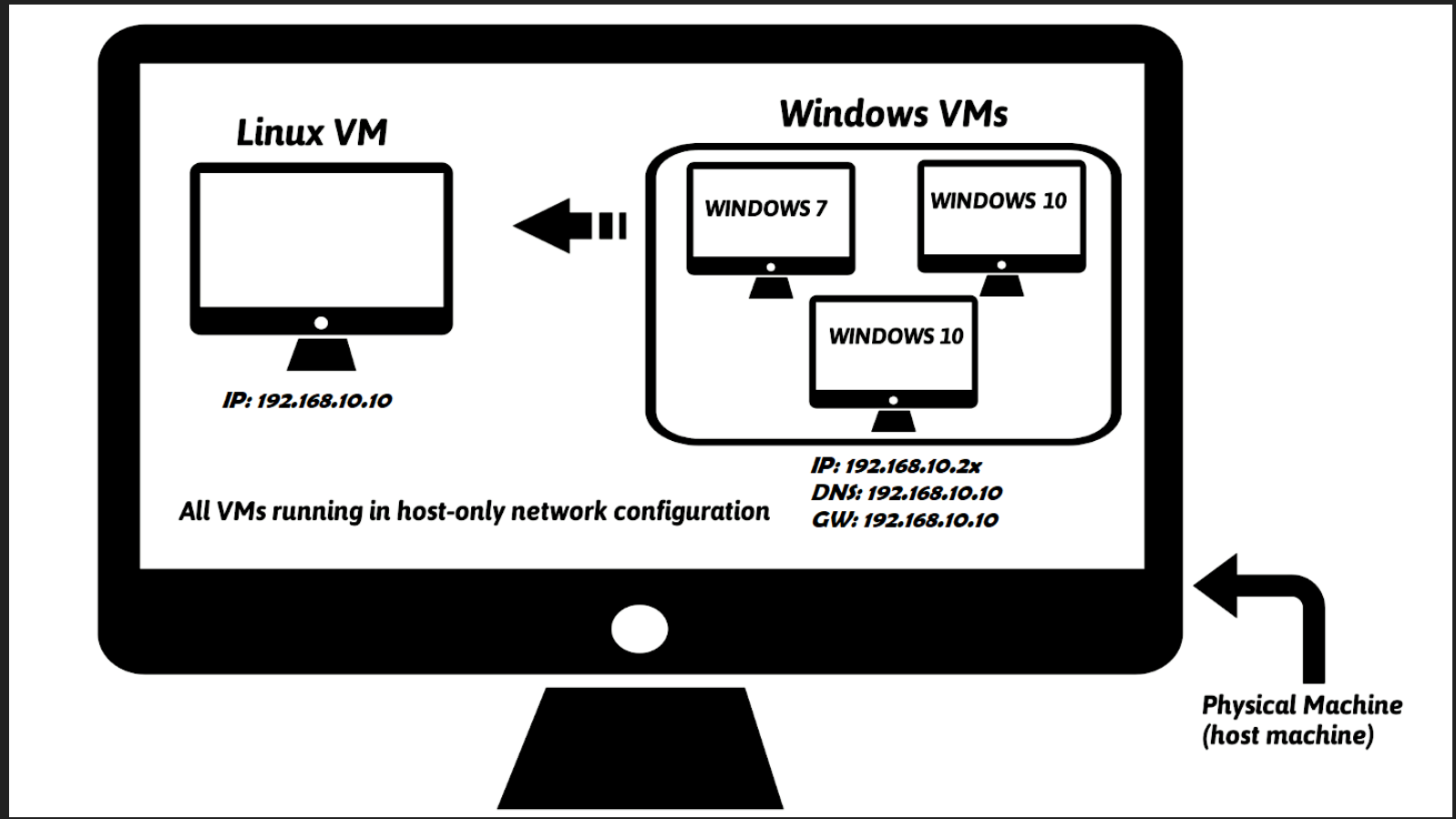
Análisis de Malware (II)

- **Motivaciones:**
  - Determinar la naturaleza y el propósito del malware.
  - Entender cómo se ha comprometido un sistema y cuál es el impacto.
  - Identificar indicadores de red relacionados con el malware (por ejemplo, dominios o direcciones IP específicas).
  - Extraer indicadores basados en el *host*, como determinados archivos, claves de registro, etc.
  - Determinar las intenciones y motivaciones de los atacantes.

Tipología del análisis de malware

- **Análisis estático**: análisis de un binario sin ejecutarlo. Permite la extracción de metadatos y otra información inicial interesante, aunque no se revela toda la información clave sobre el malware.
- **Análisis dinámico (o comportamental)**: ejecución de un binario en un entorno controlado para ver sus efectos. Igualmente, no tiene por qué revelar todas las funcionalidades hostiles.
- **Análisis de código**: técnica avanzada para revelar información oculta al análisis estático y dinámico. Se divide en:
  - Análisis de código estático: desensamblado del código binario para su estudio.
  - Análisis de código dinámico: depuración controlada de la ejecución para entender la funcionalidad.
- **Análisis de memoria (*memory forensics*)**: análisis de la memoria RAM del ordenador infectado para estudiar el comportamiento del malware tras la infección (sus capacidades de pasar desapercibido y evadir controles y desinfecciones).

Entorno de trabajo (I)



Entorno de trabajo (II)

- *Host* físico, virtualización con *VMWare* o *VirtualBox*
- Software para simulación: *InetSim*
- Máquina virtual (MV) Ubuntu 18: Servidor de red (simulación de los servicios de internet, DNS, HTTP…)
- Máquina(s) virtual(es) (MV) Windows 10/7: Ejecución del malware. La puerta de enlace y la dirección DNS serán la IP del servidor.
- Ejecución en modo *host-only*: Sin conexión a internet para asegurar un entorno aislado y seguro. Uso de NAT para configuración, ha de ser desactivado tras realizar las instalaciones de software oportunas.

Entorno de trabajo (III)

- Realizar la práctica 0 para la configuración del entorno de trabajo.

Entorno de trabajo (IV)

- **Descarga de ejemplos de malware:**
  - *Hybrid análisis*
  - *KernelMode.info*
  - *VirusBay*
  - *Contagio malware dump*
  - *AVCaesar*
  - *Malwr*
  - *VirusShare*
  - *theZoo*

Tema 1: Introducción al análisis de Malware

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática