MALWARE ANALYSIS

MALWAREANALYSISIN VIRTUALMACHINES

Dr. Zeyad Safaa Younus Saffawi

Dynamic Analysis

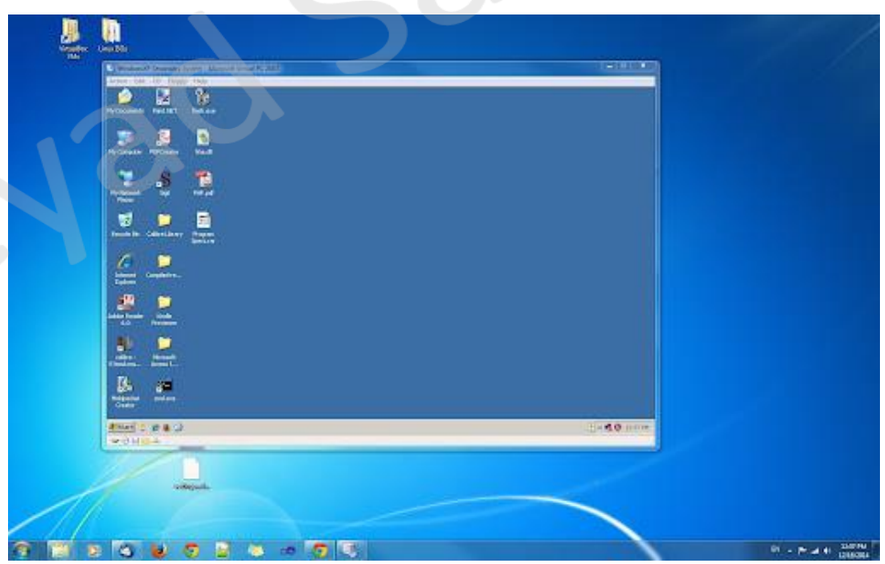
- **Dynamic analysis** refers to the process of executing malware in a controlled and isolated environment in order to observe its behavior in real time.
- This analysis allows researchers to monitor system changes, network activity, file operations, and process behavior caused by the malware.
- To prevent the malware from spreading or causing damage to other systems or networks, dynamic analysis must be performed in a **secure environment** such as a sandbox or a virtual machine.

Real Machines

- **Real machines** can be **airgapped (isolated) from the** network – no connection to the Internet or to other machines
- Advantage
- Useful if malware detects virtual machines (Some malware can detect VMs and change behavior)
- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary ((most people who test malware on physical machines use a tool such as Norton Ghost to manage backup images of their operating systems (OSs), which they restore on their machines after they've completed their analysis)).

Virtual Machines

- A **Virtual Machine (VM)** is a software-based emulation of a physical computer that runs an operating system and applications in an isolated environment. VMs provide a safe and controlled platform for conducting malware analysis, as any malicious activity is confined within the virtual environment and does not affect the host system.
- A **virtual machine (VM)** acts like a **computer inside another computer**.



Virtual Machines

- A guest OS runs inside the host OS through virtualization software.
- The guest OS is isolated from the host system.
- The most common method for analysis
- Easy to create, reset, and isolate.
- If the VM is damaged by malware, it can be: Reinstalled quickly.
- Restored to a previous clean state using snapshots.
- Easy to clone or copy virtual machines for repeated testing.
- This protects the host machine from the malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

Virtualization Features

- **Snapshots**: Allow the current state of a virtual machine to be saved and restored later. This enables analysts to revert the system to a known clean state after malware execution.
- **Cloning**: Involves duplicating the virtual machine to perform parallel or repeated analyses without affecting the original environment.
- **Isolation**: Ensures that malware remains contained within the virtual or sandboxed environment, preventing it from escaping to the host system or network.
- These techniques are essential for conducting dynamic malware analysis safely and effectively, minimizing the risk of accidental infection.

Virtualization Tools

- **VMware** (most commonly used for malware analysis).
  - VMware Player (free, limited features, and cannot take snapshots).
  - VMware Workstation is a better choice, but it costs money (paid, full features).
- Other alternatives:
  - VirtualBox
  - Parallels
  - Microsoft Virtual PC
  - Microsoft Hyper-V
  - Xen

Creating a Malware Analysis VM

- To conduct malware analysis safely, a **virtual machine (VM)** can be created using platforms such as **VMware Workstation** or **VirtualBox**, with the default hardware settings recommended by the software.
- VMware utilizes **dynamic disk allocation**, meaning that if a virtual disk of 20 GB is created but only 4 GB is used, the system will occupy only the 4 GB of physical storage. A disk size of **20 GB** is generally sufficient to accommodate:
- The guest operating system.
- Malware analysis tools and sample files.
- The **guest operating system** should be installed first. **Windows** is commonly chosen, as a large portion of malware targets this platform. Once the OS is installed, all required analysis tools can be added, including **Wireshark** for network monitoring, **PEview** for examining executable structures, **Regshot** for registry changes, and **Resource Hacker** for resource inspection, among others.
- This configuration ensures a controlled, safe environment for both static and dynamic malware analysis.

Creating a Malware Analysis VM

- Install VM tools:
  - Go to VM → Install VMware Tools.
  - VMware Tools improve:Mouse and keyboard responsiveness.
  - File sharing and drag-and-drop.
  - General performance of the VM.
- Network: Host-only / Internal (no Internet) — enable Internet only when absolutely required.
- Security: Disable shared folders, clipboard, drag-and-drop between host and guest.
- Snapshot: Take a clean snapshot named Before_Run.
- Workflow: Start monitors → run sample inside VM → collect logs/screenshots/IOCs → revert to snapshot.

Virtual Machine Network Configuration for Malware Analysis (Network modes)

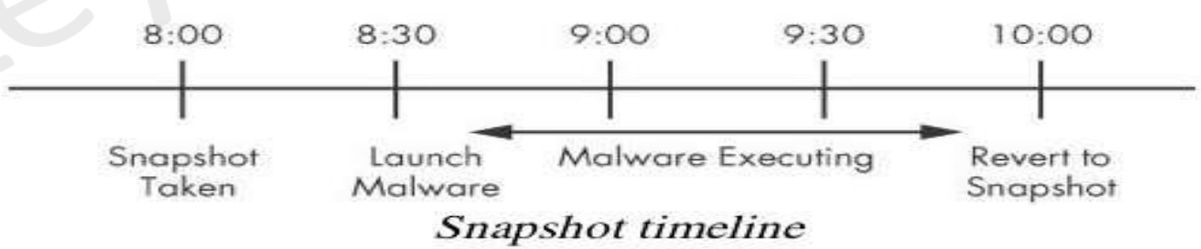
- Proper network configuration is a critical aspect of creating a safe environment for malware analysis. Different **virtual network modes** provide varying levels of connectivity and risk:
- **Host-only / Internal Network (Recommended):** In this mode, virtual machines can communicate only with each other and the host system, without access to the external Internet. This configuration is considered the safest default option for malware analysis, as it allows controlled interaction while preventing the malware from reaching external networks.
- **NAT (Network Address Translation):** NAT allows the virtual machine to access the Internet through the host system's network connection. This mode may be used temporarily, for example, to download analysis tools or updates. However, it is recommended to switch back to a more restrictive mode after completing such tasks to reduce risk.

Virtual Machine Network Configuration for Malware Analysis (*Network modes*)

- **Bridged Network:** In bridged mode, the virtual machine becomes part of the physical network. This configuration poses a **high security risk** in malware analysis environments, as it may allow malware to spread to other systems, send spam, or participate in distributed denial-of-service (DDoS) attacks. Bridged networking should only be used in fully isolated laboratory environments.
- **Disconnected Network:** This mode completely disables network access, providing maximum isolation. While it ensures strong containment, it also prevents observation of network-based malware behaviors such as command-and-control communication.
- Selecting the appropriate network mode helps balance **safety** and **analysis visibility**, making it a crucial decision in dynamic malware analysis setups.

Snapshots

- A *snapshot* is a saved state of a virtual machine at a specific point in time.
- It allows you to **return to that exact state later**, similar to Windows Restore Points.
- Very useful for testing and analysis without reinstalling the OS.
- Example:
  - At 8:00 → Take snapshot.
  - Run malware.
  - At 10:00 → Revert snapshot → machine returns to 8:00 state (malware effects erased).



Snapshot timeline

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM, and it may **change behavior or stop executing** to avoid analysis.
- VMware has Vulnerabilities: malware may crash or exploit it.
- Vulnerabilities have been found in:
  - Shared folders
  - Drag-and-drop functionality
- Malware may spread or affect the host
  - Never analyze malware on sensitive or critical machines.
  - Use isolated and controlled environments.

References

- Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press.
- Bowne, S. (n.d.). *CNIT 126 Ch 2: Malware Analysis in Virtual Machines & 3: Basic Dynamic Analysis* [PowerPoint slides]. SlideShare. https://www.slideshare.net/slideshow/cnit-126-2-malware-analysis-in-virtual-machines-3-basic-dynamic-analysis/71069826
- Bowne, S. (n.d.). *CNIT 126: Ch 2-3 Basic Dynamic Analysis* [Video]. YouTube. https://www.youtube.com/watch?v=Nsy8U8UAbHk