OPEN SOURCE HYPERVISOR ASSESSMENT

Afnan Albokhari

Jesse Hembree

C&A IA Capstone 4580- 001

Mathhew Hale

AGENDA

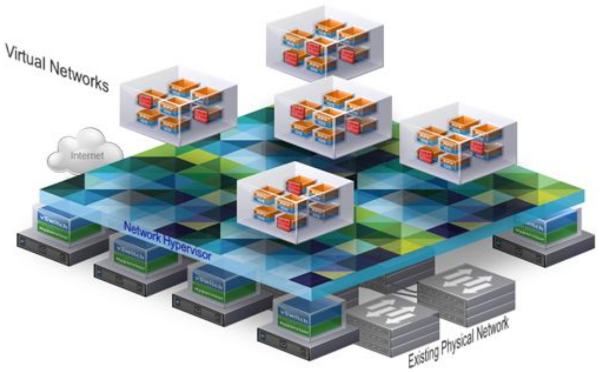
- ❑ Introduction
- ❑ Project goals
- ❑ A Hypervisor overview
- ❑ Hypervisor and cloud computing
- ❑ Xen hypervisor project
- ❑ User stories realization
- ❑ results

PROJECT GOALS

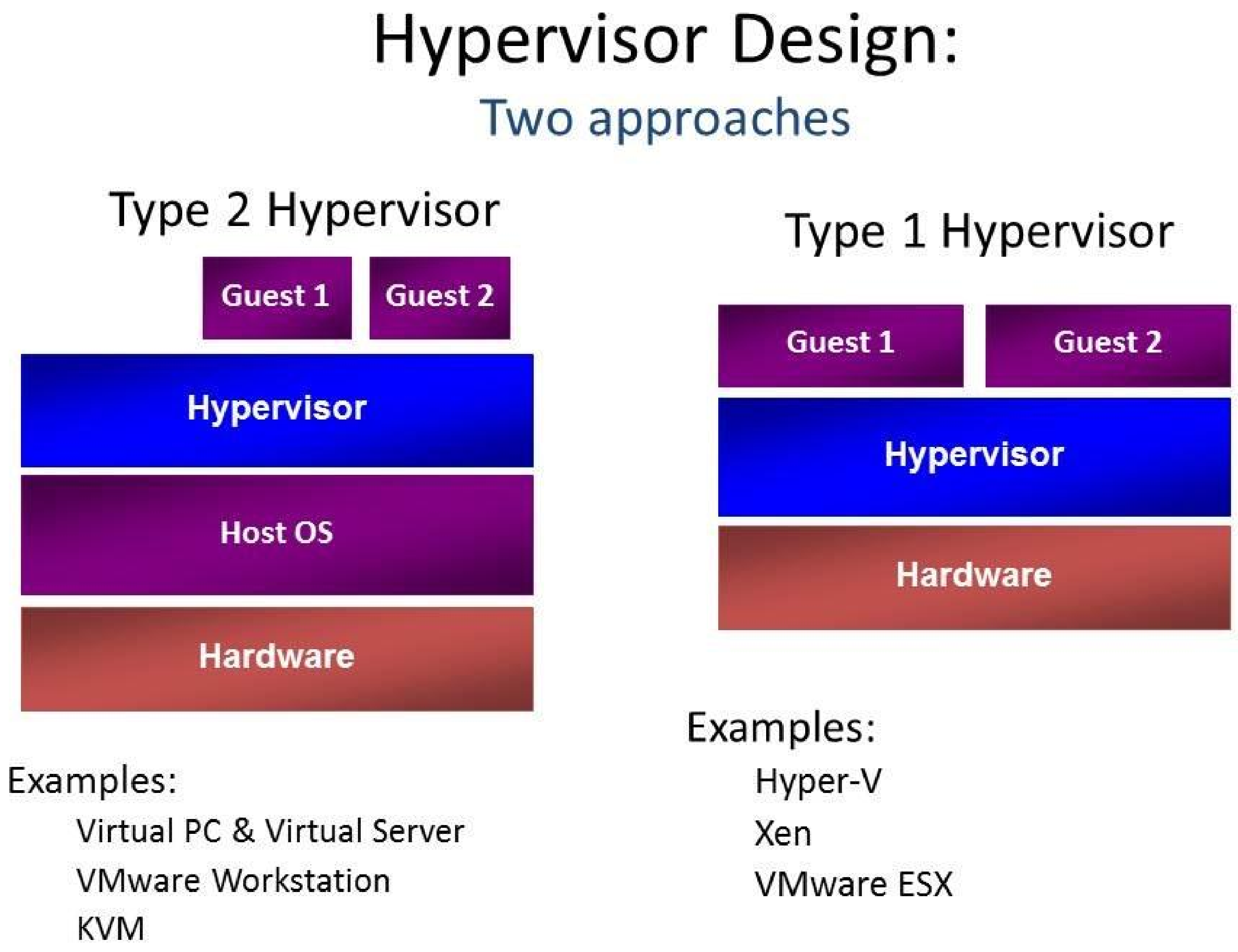
- ❑ Create repeatable framework utilizing the Xen Hypervisor for vulnerability assessment and testing
- ❑ Conduct analysis of the Vulnerability Assessment Toolkit (VASTO)
- ❑ Perform review of the current vulnerability space for the Xen Hypervisor
- ❑ Replicate findings in of vulnerabilities in test environment

A HYPERVISOR OVERVIEW

- A hypervisor allows multiple virtual machines to run is a single hardware
- Called as VMM
- A hypervisor is “software layer that provides abstraction of hardware to the operating system by allowing multiple operating system or multiple instances of the same operating system, turned as a guest, to run on a host computer” (Desai, Oza, Sharma, and Patel, 2013, p. 222)
- “Is strongly protected against software running in VMs, and enforces isolation of VMs and resources” (Sailer, Jaeger, Valdez, Caceres, Perez, Berger, Griffin, and Vandoorn, 2005)
- Two types of hypervisor:
  - Type-1 hypervisor (bare-metal)
  - Type-2 hypervisor (hosted)



A HYPERVISOR



Hypervisor Design:

Two approaches

Type 2 Hypervisor

Guest 1

Guest 2

Hypervisor

Host OS

Hardware

Examples:

Virtual PC & Virtual Server
VMware Workstation
KVM

Type 1 Hypervisor

Guest 1

Guest 2

Hypervisor

Hardware

Examples:

Hyper-V
Xen
VMware ESX

- Xen hypervisor is “software system that allows the execution of multiple virtual guest operating systems simultaneously on a single physical machine” (Xen project.org)

HYPERVIOSR IN CLOUD COMPUTING

- Each cloud different is their function and strategies which is a changing to the digital forensics analyst.
- Eight major area could help to get a clear image about any criminal :
    - Architecture – diversity, data segregation
    - Data collection – location , data recovery
    - Analysis – time sync, metadata
    - anti-forensics- data hiding, malware
    - Incident first responders- response time
    - Role management – owner, user
    - legal - contracts
    - Standard – testing, validating
    - Training – forensics investigator, cloud providers

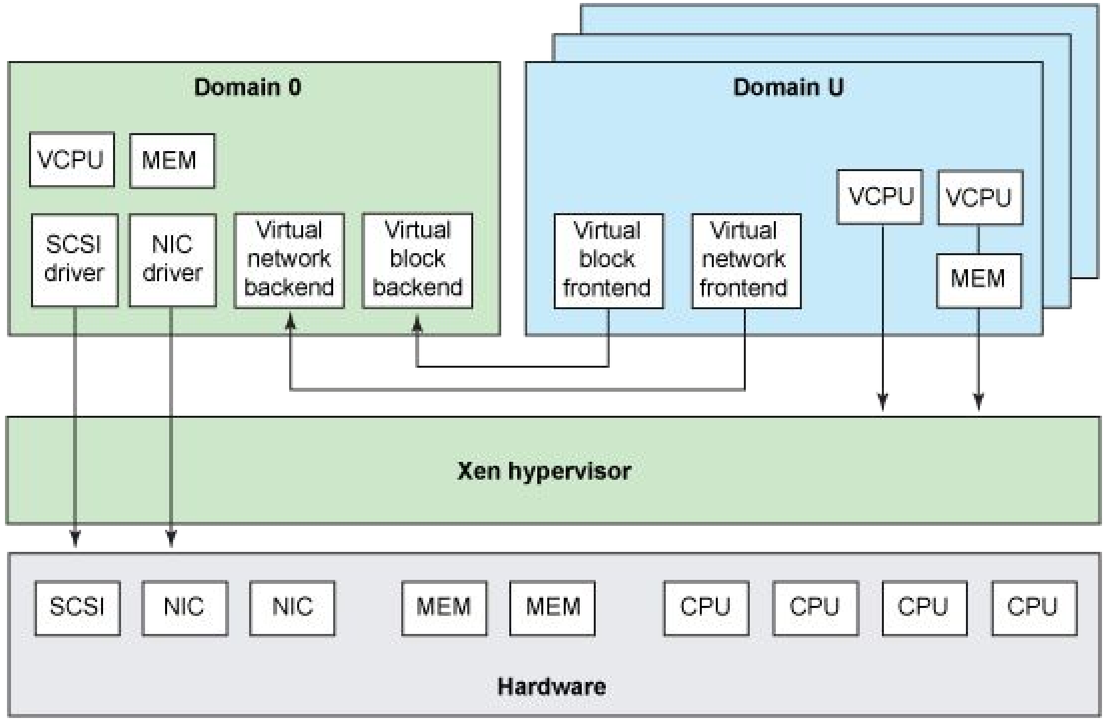
CLOUD COMPUTING

- Hypervisor based intrusion detection system used to defend attack on hypervisor in the cloud computing
- “analysis the system matrices through cloud requests from the hypervisor and detect any possible misuse tends” (Dildar, Khan, et al)
- Tracking a virtual machines, hypervisor, virtual network.

XEN HYPERVISOR PROJECT

- The Xen hypervisor requires:
  - 64 bit x86 computer and 1 GB of Ram
  - Sufficient storage space
  - CD burner
  - Install/download Debian

- The project is supporting two different types of virtualization:
  - Paravirtulization
  - Hardware virtual machine (full virtualization)

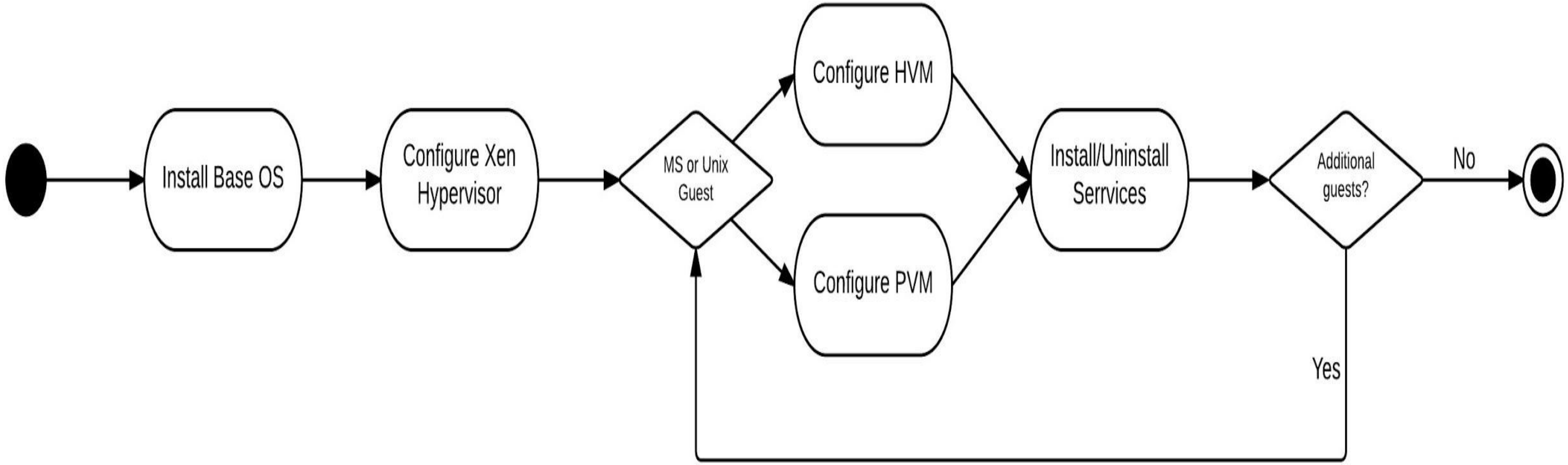


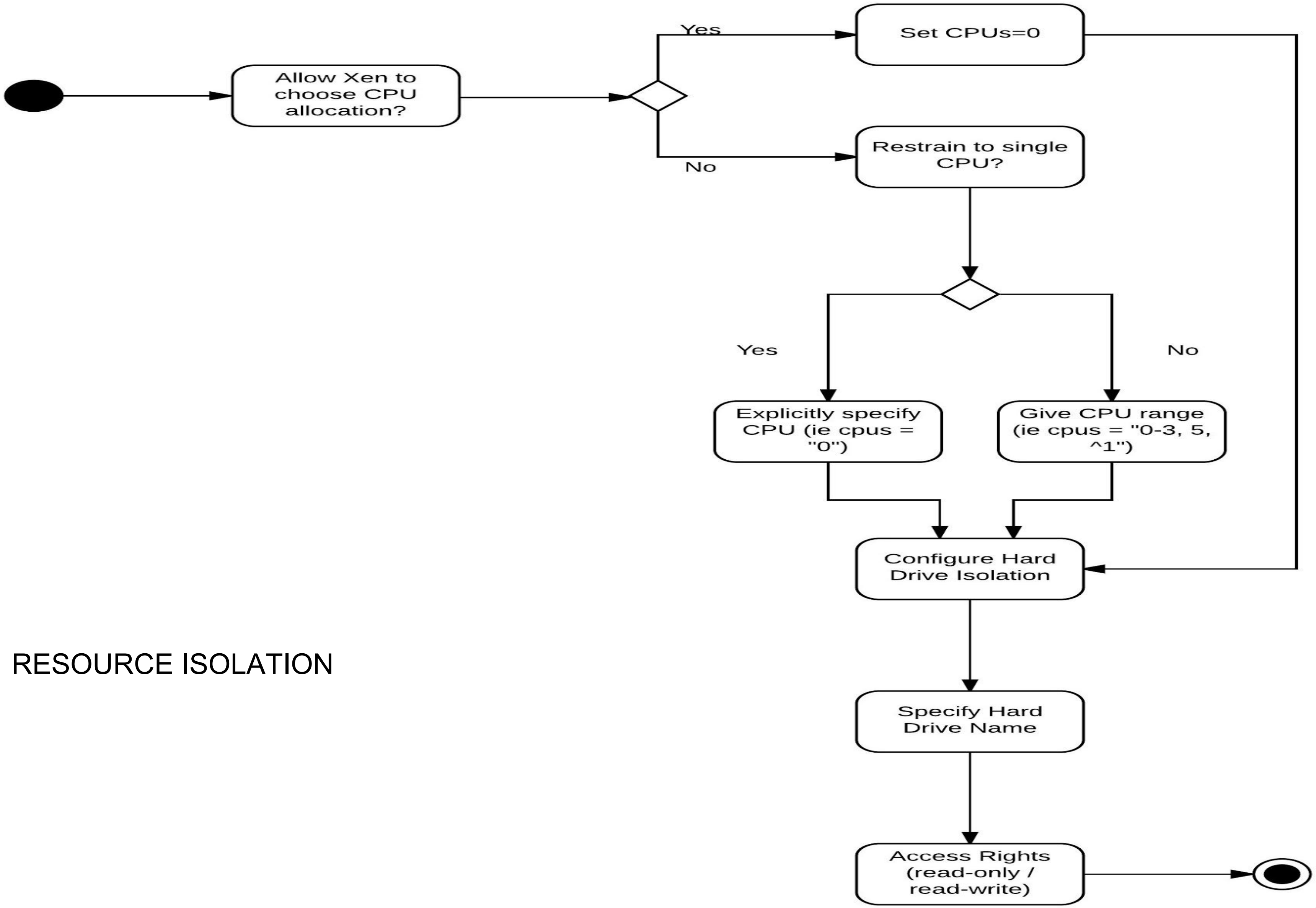
https://www.ibm.com/developerworks/library/l-multipath-xen/Figure01.gif

USER STORIES REALIZATION

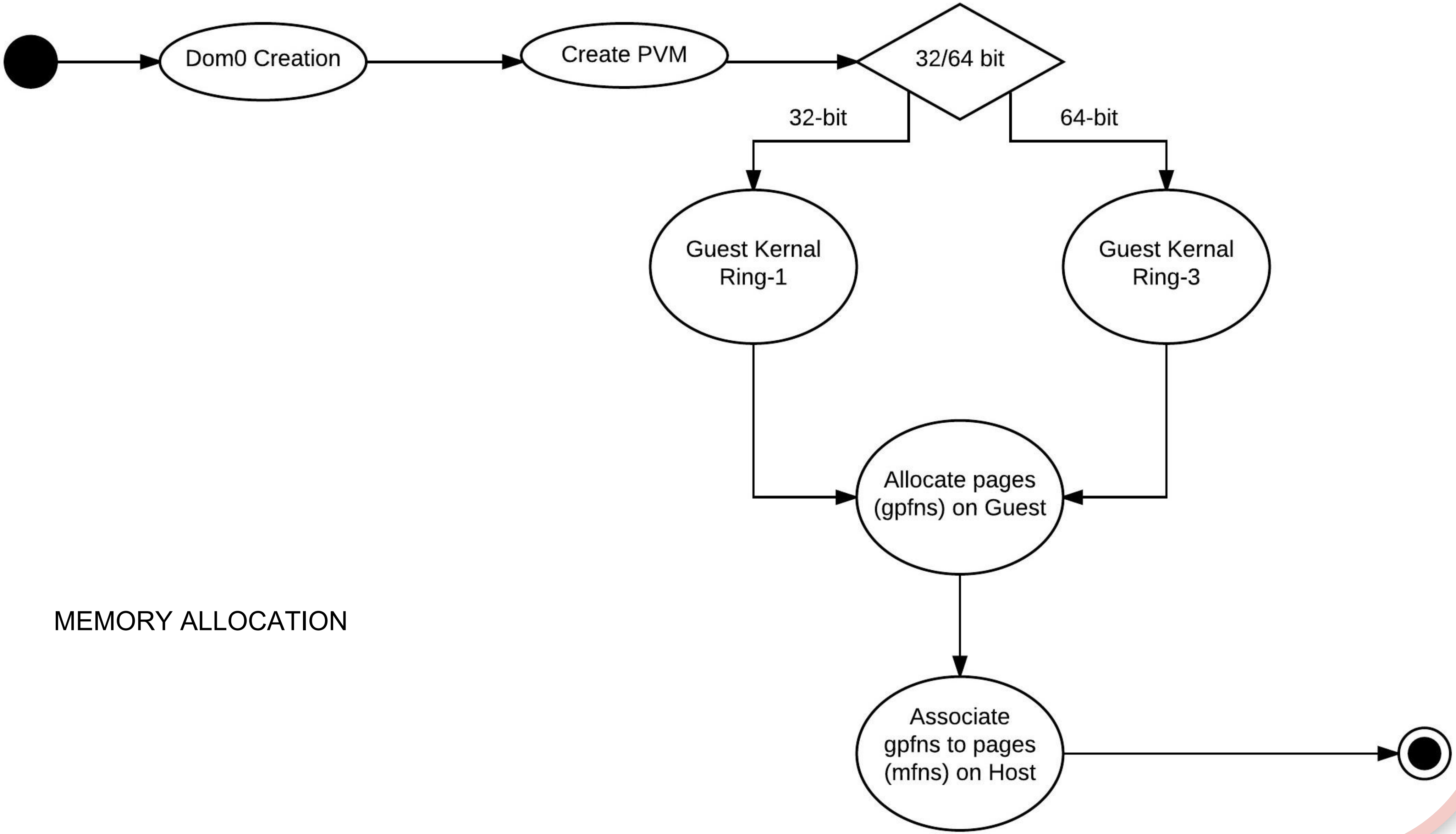
ACTIVITY DIAGRAMS :

RUNNING MULTIPLE HOST

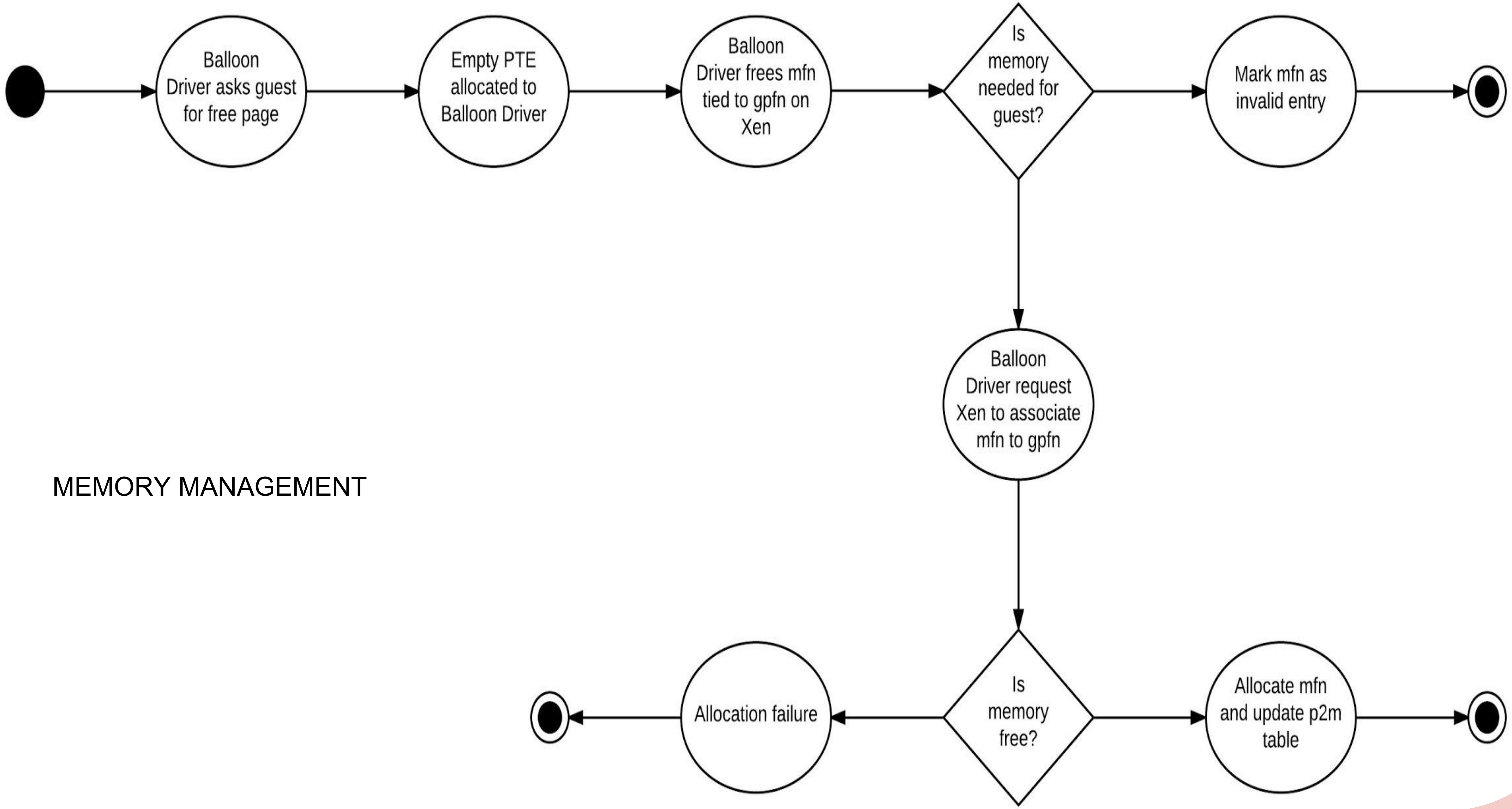



Allow Xen to choose CPU allocation?
Yes
Set CPUs=0
No
Restrain to single CPU?
Yes
No
Explicitly specify CPU (ie cpus = "0")
Give CPU range (ie cpus = "0-3, 5, ^1")
Configure Hard Drive Isolation
Specify Hard Drive Name
Access Rights (read-only / read-write)

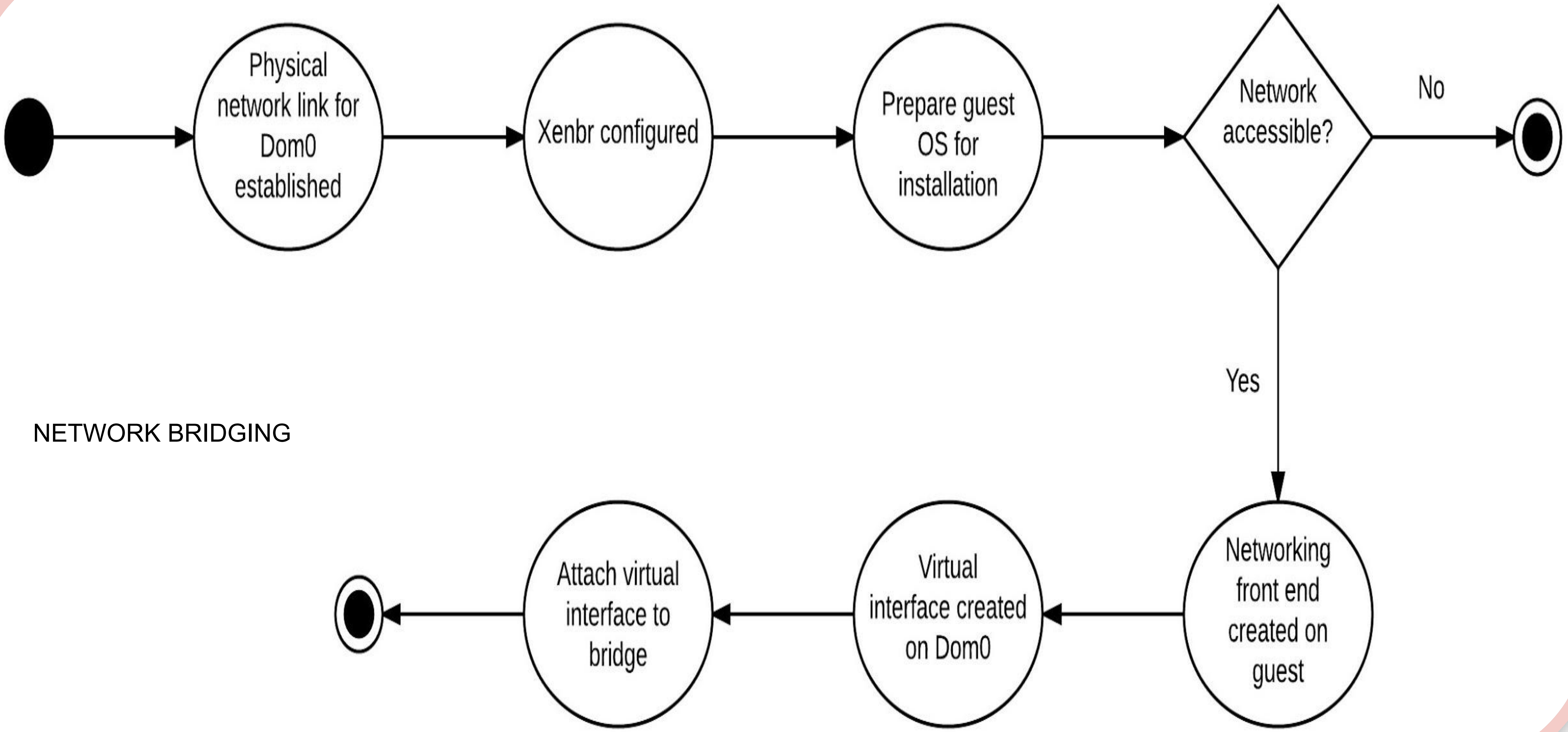
RESOURCE ISOLATION



MEMORY ALLOCATION


Balloon Driver asks guest for free page
Empty PTE allocated to Balloon Driver
Balloon Driver frees mfn tied to gpfn on Xen
Is memory needed for guest?
Mark mfn as invalid entry
Balloon Driver request Xen to associate mfn to gpfn
Is memory free?
Allocate mfn and update p2m table
Allocation failure

MEMORY MANAGEMENT


Physical network link for Dom0 established
Xenbr configured
Prepare guest OS for installation
Network accessible?
No
Yes
Networking front end created on guest
Virtual interface created on Dom0
Attach virtual interface to bridge

NETWORK BRIDGING

RESULTS

- ❑ Successfully installed Xen Hypervisor running on Debian Linux with two PVM hosts and one HVM host installed
- ❑ VASTO, while a good tool, is not very useful for testing Xen.
  - ❑ Of the 18 modules available in VASTO only 1 was for Xen
- ❑ The Xen platform is widely tested and supported by it’s community
  - ❑ Most recently published vulnerabilities from 5/2
  - ❑ Largely related to weaknesses in the memory allocation and memory management processes
- ❑ Unsuccessful in replicating results from previously released vulnerabilities
  - ❑ Source code not very accessible
  - ❑ Differences in environments

Questions