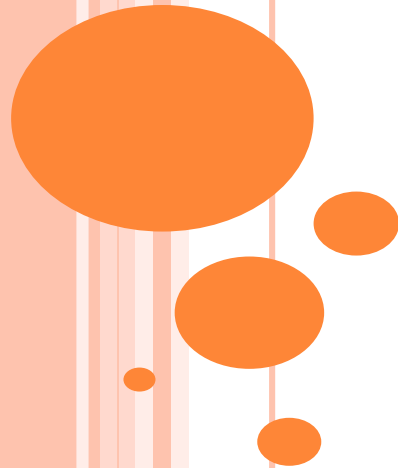# 48730, 32548 - Cyber Security Essentials

Lab 1: Introduction, Information Gather, and SQL Injection

Tutor: Ngoc LE

Tutor: **Ngoc Le**, PhD

You can call me **NGOC**

Research interest: Cyber security, Mobile

Security, Cloud computing security

Email: **Thuy.Le@uts.edu.au**

Outline:

1 Instructions, Objectives

2 VMware, and Ubuntu

3 The overview of Lab 1

1. Instruction for cyber security

CyberCrime Advisement

1. The tutorials will cover various types of attacks by conducting them in a safe and controlled environment.

2. These are for learning purposes and should not be conducted outside the controlled environment. We are not, in any way, advising/suggesting/endorsing its use in the real world.

3. Doing so in the real world is a criminal offense(CyberCrime) with a penalty of 2-10 years imprisonment. More info here: https://www.cdpp.gov.au/crimes-we-prosecute/cybercrime

1. Instruction for cyber security

Regarding the Lab setup

1. The labs are based on 2 setups, the VM Images (Tutorial 1-6) and Juniper Network Devices(Tutorial 7-9).

2. The VM Images can be downloaded, extracted and run without any additional setup required.

3. It is recommended to use an external storage device with at least 64GB space and UBS3.0 standard.

4. Using external storage avoids downloading the VM every session as the IT department cleans the system every week.

5. The VM can be run directly off the USB stick/External HDD.

6. Only the Server VM can access the internet, the Client and Attacker can not in order to isolate any attacks.

7. If your VM crashes/doesn't boot-up, you can just get a fresh set. It is advised to keep the downloaded compressed file handy for this purpose.

1. Instruction for cyber security

Regarding Marks

1. The Skill-Based Assessment (SBA) will take place in **week 12** and is worth 30% weightage. It is held in the tutorial session with the submission on UTS Online.

2. Only for **32548(Post-Grad**) - The **Research project** is worth **10%** and will be introduced in week 5.

3. **Quiz 1 (Takes place in week 5) and Quiz 2 (Takes place in week 9) are worth 10% each** and will be held in the tutorial session on UTS Online (questions based on lecture content).

4. **Bonus marks** can be obtained by submitting the **weekly tasks (Provided in the Lab Manuals) on UTS Online**. (This is not mandatory but highly recommended)

5. **Each successful submission will get a 0.5 bonus. This will be added to your score in the SBA at the end of the semester**.

6. A submission is considered successful if the student has attempted all the tasks and has provided screenshots and explanations for each task.

7. No extension will be given for the weekly submissions, no email submissions will be accepted.
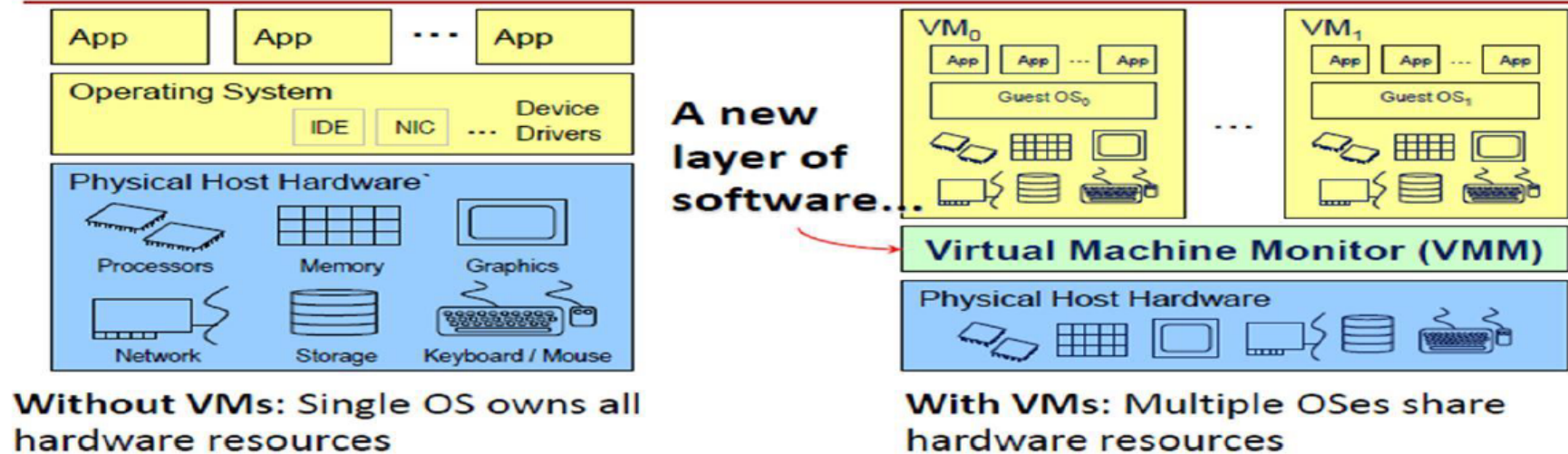
1. Objectives of the lab 1

Objectives:

1. **Understand the importance of information gathering**

2. **Clarify between active and passive information gathering**

3. **Understand how SQL injection work**

4. **Exploit the SQL injection by yourself**

5. **Anti SQL injection**
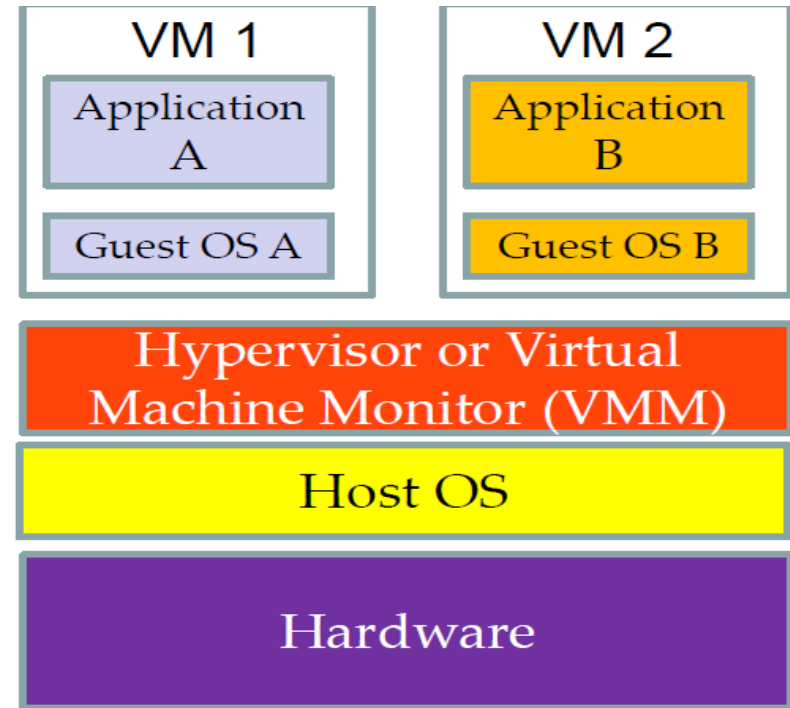
2. Virtualization [1]

System Virtual Machines (VMs)

Without VMs: Single OS owns all hardware resources

With VMs: Multiple OSes share hardware resources

Virtualization is a conversion process that translates unique IT hardware into Emulated and Standardized software-based copies.

15

[1] Cloud Computing Structure – Standford Electrical Engineering

2. Virtualisation and Hypervisor [1]
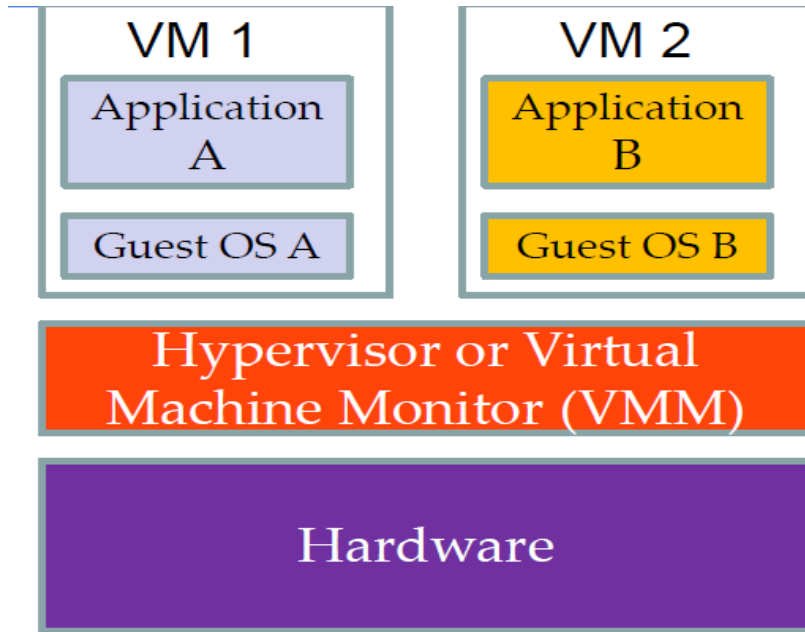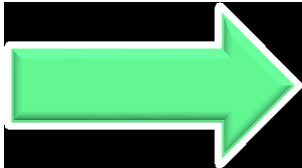
Hardware-based Virtualization

Operating System-based Virtualization

[1] Cloud Computing Structure – Standford Electrical Engineering

2. Vmware: moved or copied using for your laptop

	"I Moved It" (change?)	"I Copied It" (change?)
uuid.bios	✗	✓
uuid.location	✓	✓
ethernet.generatedaddress	✗	✓
guestCPUID.x	✓	✓
hostCPUID.x	✓	✓
userCPUID.x	✓	✓

[...] https://techhead.co/vmware-esx-i-moved-it-or-i-copied-it-whats-the-difference/
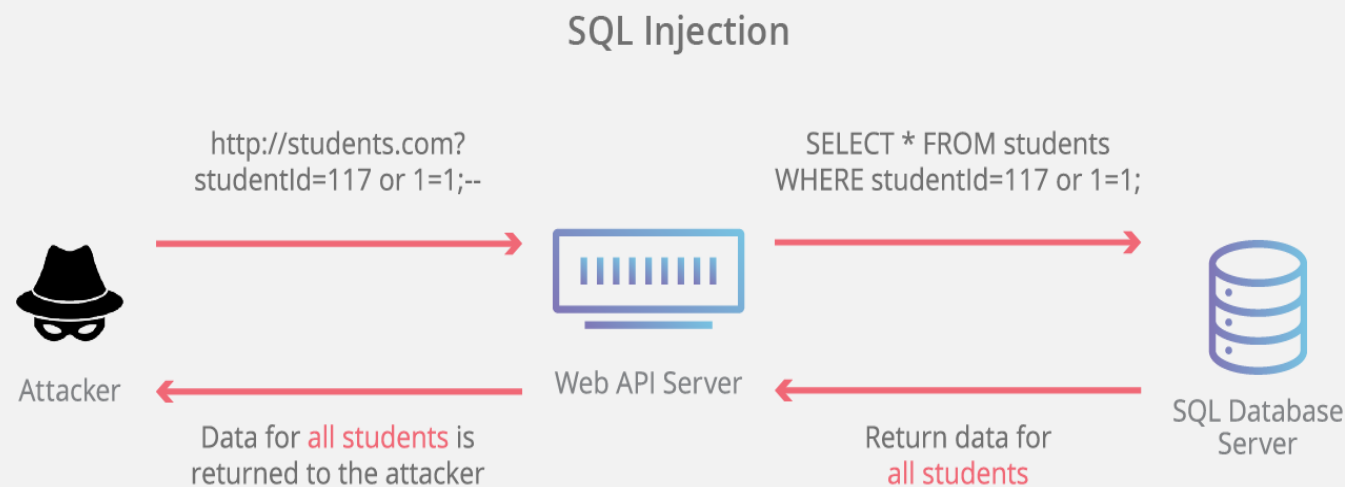
2. Using Ubuntu [2]

[2] https://online.uts.edu.au/bbcswebdav/pid-3658248-dt-content-rid-51678070_1/courses/32548-48730-2019-SPRING-CITY/Ubuntu-Commands.pdf

3. Over view of Lab 1

✓ **Task 1:** Information gathering

    ✓ Active (netcraft)

    ✓ Passive (zenmap)

✓ **Task 2:** SQL injection

    ✓ What kind of SQL

    ✓ The reason makes SQL vulnerable

    ✓ How to exploit SQL injection

3. SQL injection [3]

[3] https://www.cloudflare.com/learning/security/threats/sql-injection/

THANK YOU!

Question & Answer