RL4Eng

Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Dr. Omar H. Kombo

Software Security: Buffer overflow

Co-funded by the Erasmus+ Programme of the European Union

Introduction

Software security is the process of ensuring that software can withstand malicious attacks while remaining functioning. This includes preventing and mitigating vulnerabilities caused by incorrect memory management during program development.

Key Concepts Covered in this presentation:

1. Introduction to Software Vulnerabilities
2. Setup Four VM/Docker with Buffer Overflow Vulnerability
3. Attempt to Escalate Privilege to Root Privilege within the VM/Docker
4. Mitigating Buffer Overflow Vulnerabilities

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Software Vulnerabilities

- **Software vulnerabilities** are those defects or weaknesses in software systems that attackers can exploit to ruin the system's integrity, availability, or confidentiality.
- **Common vulnerabilities:**
  - Buffer overflows
  - Insecure setups
  - Cross-site scripting (XSS), and
  - SQL injections
- It is therefore, very important to develop understanding these vulnerabilities in order to keep systems safe.

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Buffer Overflows

- **Buffer overflow** is a well-known software security vulnerability or code flaw that hackers can use to gain unauthorized access to systems.

  Conditions for buffer overflows: When code depends on data attributes that are enforced beyond their immediate scope, when depending on external data to regulate behavior of the code, or when the complexity of code does not allow for its prediction.

- **Types of Buffer Overflows**
  1. **Heap-Based Buffer Overflows:** Occurs in heap memory and may allow attackers to modify data structures or introduce malicious payloads into a program.
  2. **Stack-Based Buffer Overflows:** Occurs on the stack and can overwrite return addresses or change the execution path, allowing attackers to run arbitrary code in the program.
  3. **Format string attack:** Occurs when an application treats input data as a command or fails to validate it appropriately, which allows the attacker to execute code, access data from the stack, and create segmentation faults in the application.

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

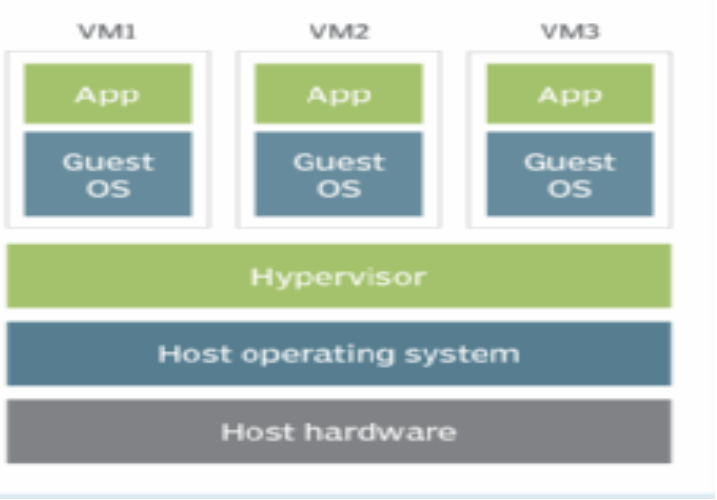
Virtual Machine (VM) and Docker Vulnerability Environment

- The difference in Vulnerability between VM and Docker:
  - Vulnerability in virtual machine vulnerability is mainly due to insecure guest systems, misconfigurations, or weaknesses in hypervisor
  - Vulnerability in Docker is characterized by the shared host kernel between containers.
- Configuring Vulnerable Systems: A controlled environment should be used when testing vulnerability.
- Tools for testing:
  - Metasploitable
  - Damn Vulnerable Linux
  - Custom Docker containers

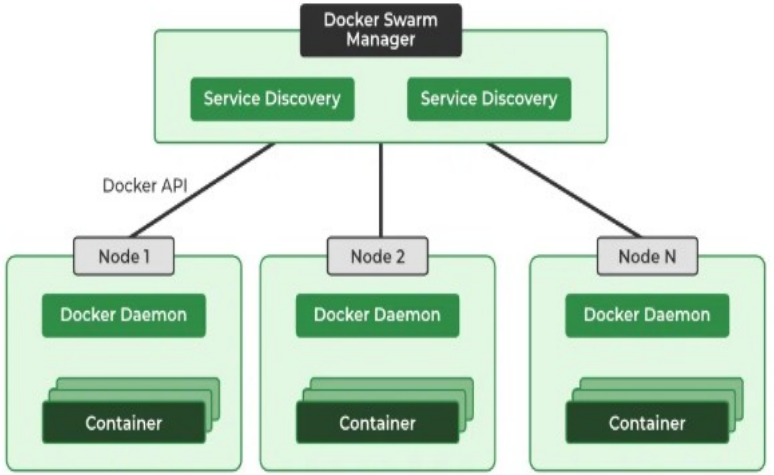
RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Setup VM/Docker with Buffer Overflow Vulnerability

- Install VM or Docker.
- Configure the VM/Docker for certain buffer overflow. vulnerabilities
- Validate the vulnerabilities with multiple test inputs.



Architecture of virtualization using VMs.



Docker Swarm

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Attempt to Escalate Privilege to Root Privilege within the VM/Docker

- Privilege escalation attempts are used to get unlawful root access within a virtual machine or Docker container. This access gives attackers complete control over the system, the ability to modify crucial configurations and access sensitive data.

Common techniques:

- Privilege escalation scripts
- Kernel Exploits, and
- misconfigured Docker images.

Steps for exploitation:

- Identify a Vulnerability
- Exploit the Vulnerability
- Bypass Security Mechanisms
- Gain Shell Access as Root

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Measures to Prevent Escalation of Privilege within the VM/Docker

- Measures to combat these attempts are:
  - Restricting the capability of Docker containers.
  - Use of updated software.
  - Only essential applications should be installed.
  - Enable crucial security features.
  - Identify buffer overflow vulnerabilities.
  - Recurrent security audit.

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Mitigating Buffer Overflow Vulnerabilities

- There are six (6) common methods for preventing programs from writing **excessive** data to the memory than the memory can accommodate:
  - Run-time protection
  - Secure coding
  - Regular testing and auditing
  - Compiler-level shield
  - Memory protection at OS level
  - Employing modern frameworks and libraries

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Mitigating Buffer Overflow Vulnerabilities

- Additional mitigation methods for eliminating buffer overflow threats are built into the operating system. These include:
- **Address space layout randomization (ASLR):** Moves at random through data areas to randomize address spaces so that attackers can not know the exact location of executable code, making overflow attacks difficult.
- **Data execution prevention:** Prevents an attacker from running code in non-executable locations by classifying memory sections as executable or non-executable.
- **Structured exception handling overwrite protection (SEHOP):** Prohibits attackers' malicious code from attacking the structured exception handling (SHE) by preventing attempts aimed at rewriting the SHE.

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Q&A

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union