LAB 2: CVSS	Name: Luthfil Hadi Bin Zul Hisham Student ID: CS01083180	Name: Mal Syazani Bin Mal Soefian Student ID: CS01083151

Example 1: CVE-2023-21989

Vulnerability: Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attackers with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data.

Metric	**Value**	**Comments**
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have administrative control over a virtual machine within the virtual machine host.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	None	There is no impact to the vulnerable system confidentiality.
Vulnerable System Integrity	None	There is no impact to the vulnerable system integrity.
Vulnerable System Availability	None	There is no impact to the vulnerable system availability.
Subsequent System Confidentiality	High	An attacker could exploit this vulnerability to access confidential information stored within the VM host hypervisor system.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.

By using CVSS Calculator, what is the Base metric score? **[2 marks]**
Answer: **5.9**

Example 2: CVE-2020-3947

VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine.

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	High	An attacker must have administrative control over a virtual machine within the virtual machine host.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	An attacker could execute arbitrary code on the vulnerable system.
Vulnerable System Integrity	High	An attacker could execute arbitrary code on the vulnerable system.
Vulnerable System Availability	High	An attacker could execute arbitrary code on the vulnerable system.
Subsequent System Confidentiality	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Subsequent System Integrity	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Subsequent System Availability	High	An attacker could take actions on other systems hosted within the virtual hypervisor.
Exploit Maturity	Proof-of-Concept (P)	A proof of concept is available

By using CVSS Calculator, what is the Base metric score? **[2 marks]**
Answer: **9.4**

Scenario 1: OpenSSL Heartbleed Vulnerability (CVE-2014-0160)
Vulnerability: The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Attack: A successful attack requires only sending a specially crafted message to a web server running OpenSSL. The attacker constructs a malformed "heartbeat request" with a large field length and small payload size. The vulnerable server does not validate the length of the payload against the provided field length and will return up to 64 kB of server memory to the attacker. It is likely that this memory was previously utilized by OpenSSL. Data returned may contain sensitive information such as encryption keys or user names and passwords that could be used by the attacker to launch further attacks

Metric	**Value**	**Comments**
Attack Vector	Network (N)	Performed over the network, remote exploitation enables
Attack Complexity	Low (L)	No additional knowledge required
Attack Requirements	None	No attack requirement
Privileges Required	None (N)	No privilege required
User Interaction	None (N)	No interaction required
Vulnerable System Confidentiality	High	Can obtain data from the system
Vulnerable System Integrity	None	No impact on integrity
Vulnerable System Availability	None	No impact on availability
Subsequent System Confidentiality	None	No impact on confidentiality
Subsequent System Integrity	None	No impact on integrity
Subsequent System Availability	None	No impact on availability
Exploit Maturity	None	Not defined
By using CVSS Calculator, what is the Base metric score? Give your reason in the comments **[14 marks]** Answer: 8.7 / High		

Scenario 2: **CVE-2023-30560**

Vulnerability: There are two known configurations of a product known as the Becton Dickinson PCU which can be modified without authentication using physical connection to the PCU. A PCU is commonly used for infusion delivery in a healthcare provider environment. With that context in mind, it could be inferred that an exploit of this vulnerability might have Safety impact. The below is only an example of how this, or a similar vulnerability, *could* be scored.

v3.1	**v4.0 Base**
6.8	8.3
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:H/SA:N/S:P/V:D

Question 1: Based on table above, what is the main reason for the different version **CVSS** give different scoring for the vulnerabilities?

[2 marks]

Answer: v4.0 Base add new metrics that are more detailed. It adds new measure like availability and safely impacts that affect the risks assessment for higher scores.

REFERENCES

https://www.first.org/cvss/