A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 6**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

REFLECTION QUESTIONS

1. In your own words, explain about Common Vulnerability Scanning System (CVSS) and Common Vulnerability Enumeration (CVE).

* CVSS - It's a system for evaluating and rating the seriousness of security vulnerabilities in software. It helps organizations prioritize responses to threats by quantifying the risk of each vulnerability.
* CVE - This is a database of known information security vulnerabilities. Each entry has a unique identifier, allowing for standardized referencing and discussion of vulnerabilities across different security tools.

1. Explain the difference(s) between CVSS and CVE.

|  |  |  |
| --- | --- | --- |
| **Aspect** | **CVSS** | **CVE** |
| Purpose and Function | Framework for assessing and rating vulnerability severity. | Database of unique identifiers for known vulnerabilities. |
| Nature | Scoring system for assigning severity scores. | Identifier system for uniquely referencing vulnerabilities. |
| Output | Numerical score (Base Score) indicating severity. | Unique identifier (CVE ID) for each vulnerability. |
| Usage | Prioritizing responses based on severity scores. | Uniquely identifying and tracking vulnerabilities. |

1. How many severity levels are there in the CVSS version 3.0?

Low, Medium, High, Critical

1. Draw a table of CVSS3.0 severity levels and their base score range.

|  |  |
| --- | --- |
| **Severity Level** | **Base Score Range** |
| Low | 0.0 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 1. - 10.0 |

1. Observe the information provided at vuldb.com and answer the questions below:
2. List three (3) most recent vulnerabilities and their severities.

* CVE-2020-1472 (ZeroLogon)
* CVE-2021-44228 (Log4Shell)
* CVE-2022-22536 (ICMAD)

1. List three (3) latest available exploits.

* Improper Input Validation in Apache Log4j Logging Library: In 2022, this vulnerability was exploited to allow remote code execution. Organizations and individuals using this library were at risk of potential attacks.
* Vulnerability in Fortinet SSL VPNs (CVE-2018-13379): This particular vulnerability affected Fortinet SSL VPNs and was routinely exploited. It was mentioned as one of the top routinely exploited vulnerabilities in 2020.
* Various Vulnerabilities in Confluence Server (CVEs): Atlassian Confluence Server had multiple vulnerabilities in 2022 that were exploited. The specific CVEs were not mentioned, but it highlights the importance of regularly patching and updating software to protect against potential exploits.

1. List three (3) vulnerabilities in current CVSS Top 5.

* Unitronics Vision Series PLC all insecure default initialization of resource
* Zyxel NAS326/NAS542 WSGI Server os command injection
* Zyxel NAS326/NAS542 HTTP POST Request show\_zysync\_server\_contents os command  
  injection

Task 1

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a green screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Task 2

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

16.a

|  |  |
| --- | --- |
| Severity | Total |
| High | 24 |
| Medium | 39 |
| Low | 6 |
| Log | 91 |
| Grand Total | 168 |

b. What are the vulnerabilities that have the highest severities? List them.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

c. What is the vulnerability for port 513/tcp?

rlogin Passwordless Login, The rlogin service is running

d. List 3 vulnerabilities with medium severity.

A screenshot of a computer

Description automatically generated

e. Based on the given information by GSM, how do we solve the “VNC Brute Force” vulnerability?

A white background with black text

Description automatically generated