UNIVERSITI TEKNOLOGI MARA

CSP760

PREDICTING VULNERABILITY SUSCEPTIBILITY IN MALAYSIAN BANK USING SUPERVISED MACHINE LEARNING

STUDENT NOR ADANI BINTI KAMAL MOHAMAD NASIR (2024782087)

SUPERVISOR DR SITI ARPAH BINTI AHMAD

Date: 7 December 2025

UNIVERSITI TEKNOLOGI MARA

TABLE OF CONTENT

Cybersecurity

CURRENT APPROACH (REACTIVE)

VA TOOLS → DETECT TODAY'S VULNERABILITIES

FUTURE APPROACH (PROACTIVE)

ML MODEL → PREDICT TOMORROW'S VULNERABILITIES

OWASP
Zed Attack Proxy

OPENVAS
by Greenbone

Qualys.

nessus
Professional

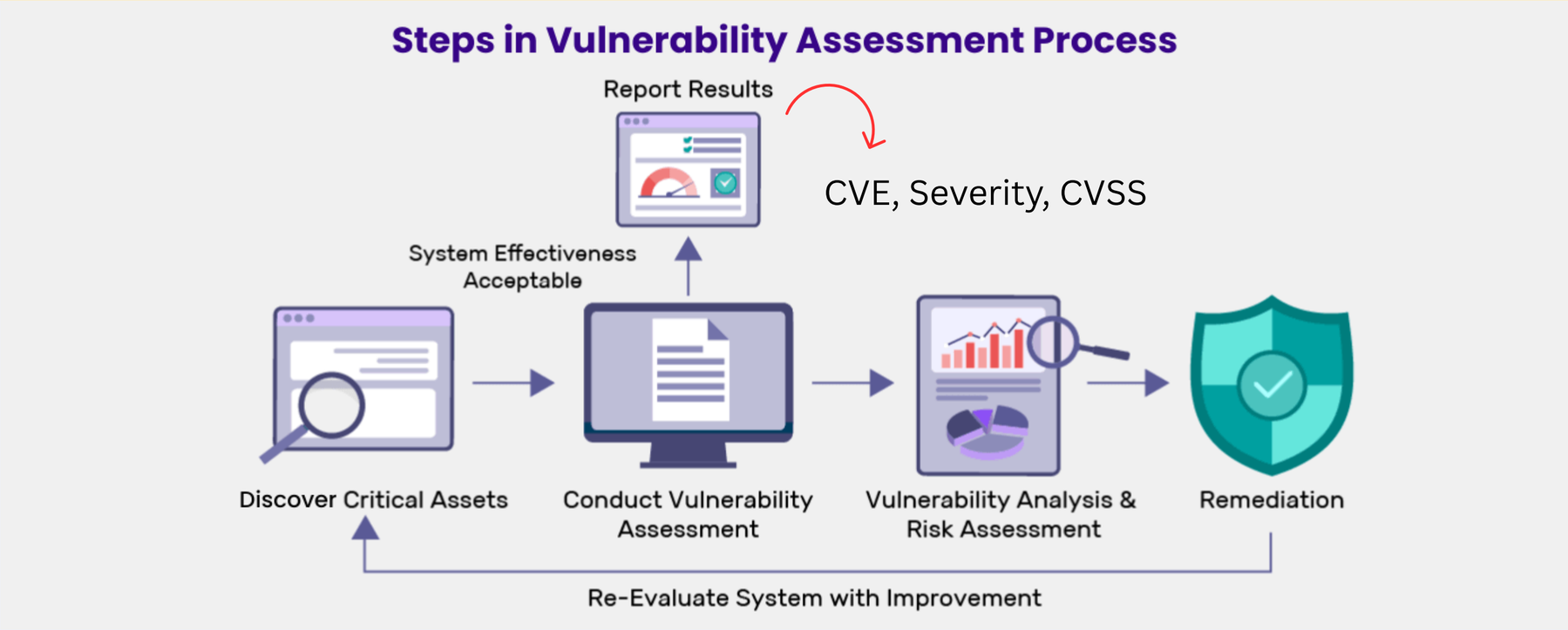
What is Vulnerability Assessment (VA)?

Definition

Vulnerability Assessment (VA) is a cybersecurity process used to identify security weaknesses in systems, servers, applications, and networks.

Why Banks Use VA?

- Detect outdated software
- Identify misconfigurations
- Find exploitable services



RMIT Revised - 28/11/2025

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology (RMiT)

Applicable to:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers including professional reinsurers
5. Licensed takaful operators including professional retakaful operators
6. Prescribed development financial institutions
7. Approved issuers of electronic money
8. Operator of a designated payment system
9. Registered merchant acquirers
10. Intermediary remittance institutions

Issued on: 28 November 2025

BNM/RH/PD 028-98

(a) conducting continuous review to ensure that CIB does not occur in the IT environments of the financial institution, its intermediaries, or third party service providers. The financial institution shall also incorporate scanning or screening of customer information into the scope of periodic security assessments (e.g. penetration testing, red teaming, or other security validation exercises) to detect accidental exposure of customer information on financial institution's systems;

(b) enhancing cybersecurity operations to promptly detect and strengthen the safeguards against CIB;

(c) ensure that the scope of financial institutions' internal audit reviews encompasses the management and security controls pertaining to CIB; and

(d) conduct a thorough investigation to identify the technical root cause(s) of all CIBs with appropriate action and consequence management to mitigate recurrence.

CIB - customer information breach

CVE, CVSS & Severity

These fields are core features used by my ML model to learn vulnerability patterns.

CVE Common Vulnerabilities & Exposures

- Unique ID for each known vulnerability
- Example: CVE-2024-12345
- Used globally by scanners (Nessus, Qualys, OpenVAS)

CVSS (Common Vulnerability Scoring System)

- Standard scoring system (0.0–10.0)
- Measures exploitability + impact
- Higher score = higher risk

CVSS Security Levels

Base Score Range	Security Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10	Critical

SEVERITY

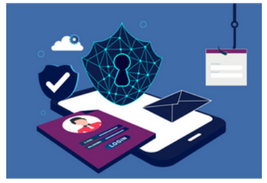
Common Threats in Financial Instituition

Type of threats that need to be remediate as fast before attacker explot it.

Phishing & Social Engineering

01

Attackers steal login credentials or trick staff/customers



Ransomware

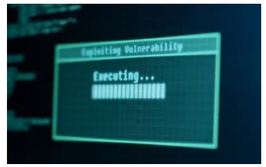
02

Encrypt data, demand payment

Exploitation of Unpatched Systems

03

Outdated RHEL, Windows, SSL/TLS vulnerabilities



Misconfiguration Attacks

04

Weak firewall rules, exposed services, default credentials

Zero-Day Vulnerabilities

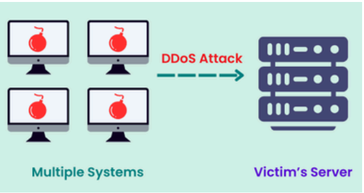
05

Attackers exploit before patches exist

DDOS

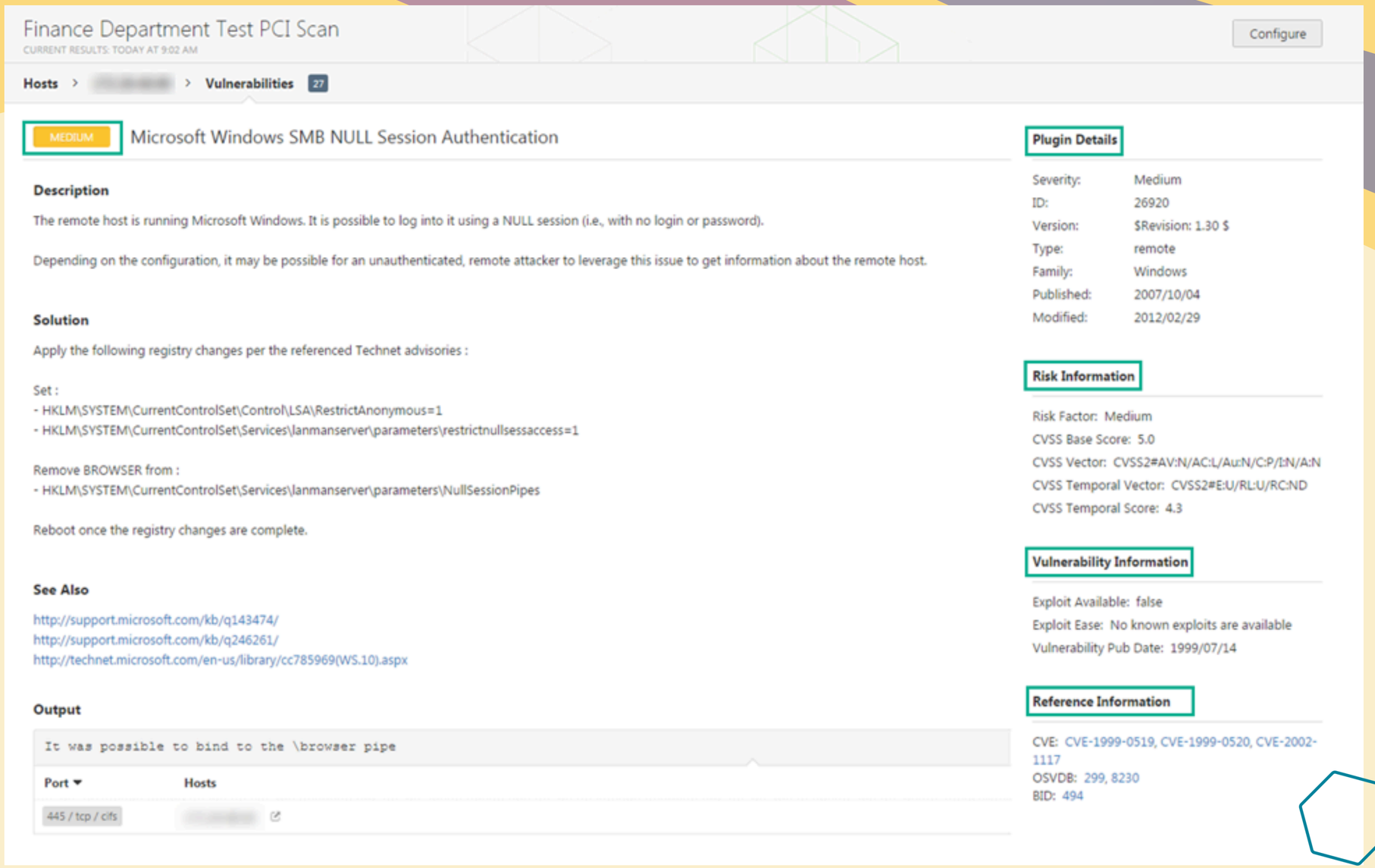
06

Floods a server, website, or network with massive amounts of fake internet traffic



Cybersecurity Attributes in Tenable/Nessus Data

Nessus generates structured vulnerability data that includes



ExploitDB & Real-World Exploitability

A public database containing actual exploit codes used by attackers to exploit vulnerabilities.

Why it important?

- Shows whether a vulnerability can be actively weaponized
- Helps FI prioritize for urgent patching
- A CVE with an available exploit = high risk

How I use ExploitDB info?

- Extracted CVE-related exploit information
- Added “exploit availability” into dataset
- Strengthens ML prediction of high-risk vulnerabilities

Vulnerabilities with public exploits tend to escalate faster and are more dangerous.

CSP760

THANK YOU