**LAB14 Vulnerability assessment**

1. Design scenario

|  |  |  |
| --- | --- | --- |
| No | Steps | Remarks |
| 1 | Determine inspection area | Network vul.  Web vul. |
| 2 | Choose target | Your own VM IP  CTU IP  CICT IP |
| 3 | Choose scanning program/tool | [Under Linux]  Nikto  Nmap vulners  Nmap vulscan |
| [Under Windows]  Window Nmap vulners |
| 4 | Run the program |  |
| 5 | Display running result | List up the vulnerability checking items |
| 6 | Find vulnerability type | Find vulnerability type |
| 7 | Grade the vulnerability level | Grade the vulnerability level |
| 8 | Analyze the result | Analyze the result based on your idea |

2. Exercise model [Under Linux]

[STEP1] vulners.nse script

1. Download “Nmap-vulners” from github.

git clone https://github.com/vulnersCom/nmap-vulners.git

cd nmap-vulners

1. Check network information

ifconfig

1. Shows all related CVEs, vulnerability details and reference that related to target IP address.

sudo nmap -sV --script vulners.nse [target IP address]

1. Copy link <https://vulners.com/cve/CVE-2021-39275> and paste into browser to invest the vulnerability.

[STEP2] vulscan

1. Install vulscan on terminal of ubuntu from github.
2. Run the command

$ sudo nmap -Sv –script=vulscan/vulscan.nse 111.111.1.1

.

References:

<https://www.hackingloops.com/nmap-for-vulnerability-scanning/>

<https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/>

<https://github.com/vulnersCom/nmap-vulners>

How to search CVSS Score

[CVSS Score Distribution Reports and Trends Over Time (cvedetails.com)](https://www.cvedetails.com/cvss-score-charts.php)

# Vulnerabilities By Type

[Vulnerability distribution of cve security vulnerabilities by types (cvedetails.com)](https://www.cvedetails.com/vulnerabilities-by-types.php)