**LAB14 Vulnerability assessment**

Class: M04 Name: Truong Dang Truc Lam Students ID: B2111933

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 |

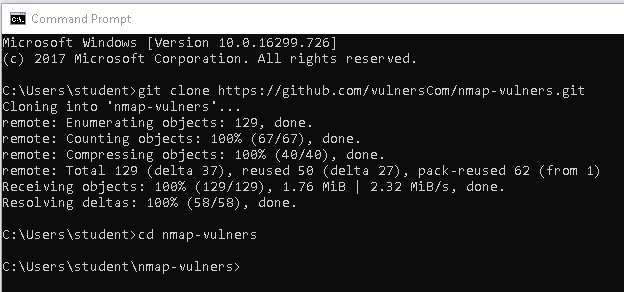
2. Exercise model [Under Linux]

[STEP1] vulners.nse script

1. Download “Nmap-vulners” from github.

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

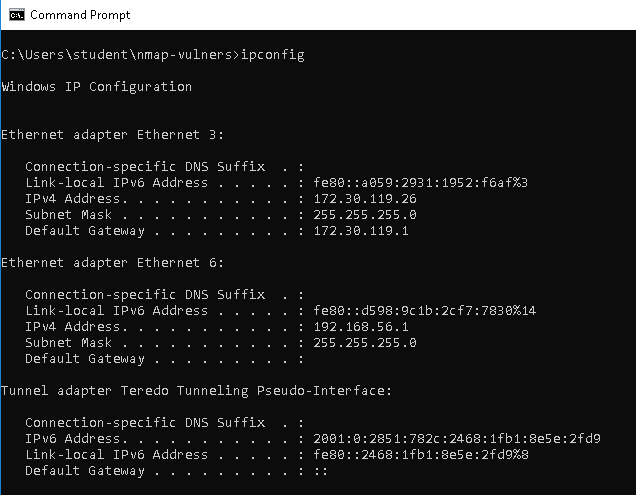
cd nmap-vulners



Download “Nmap-vulners” from github.

1. Check network information

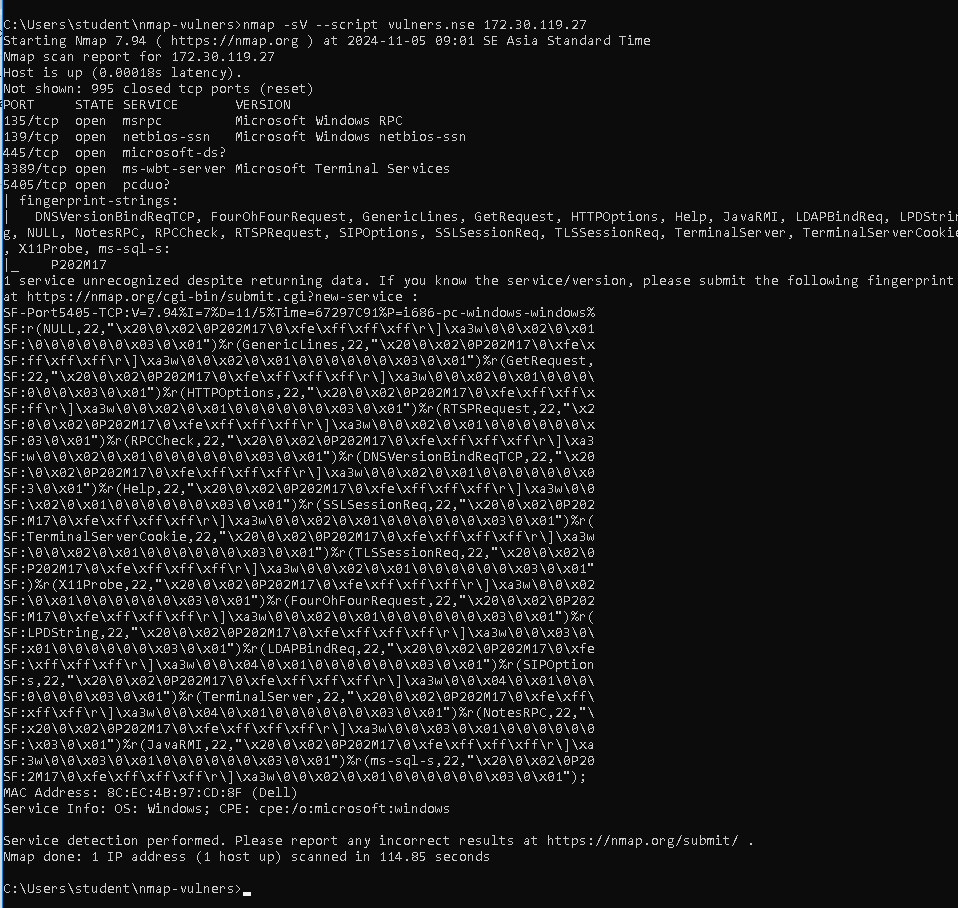
ipconfig



Check network info

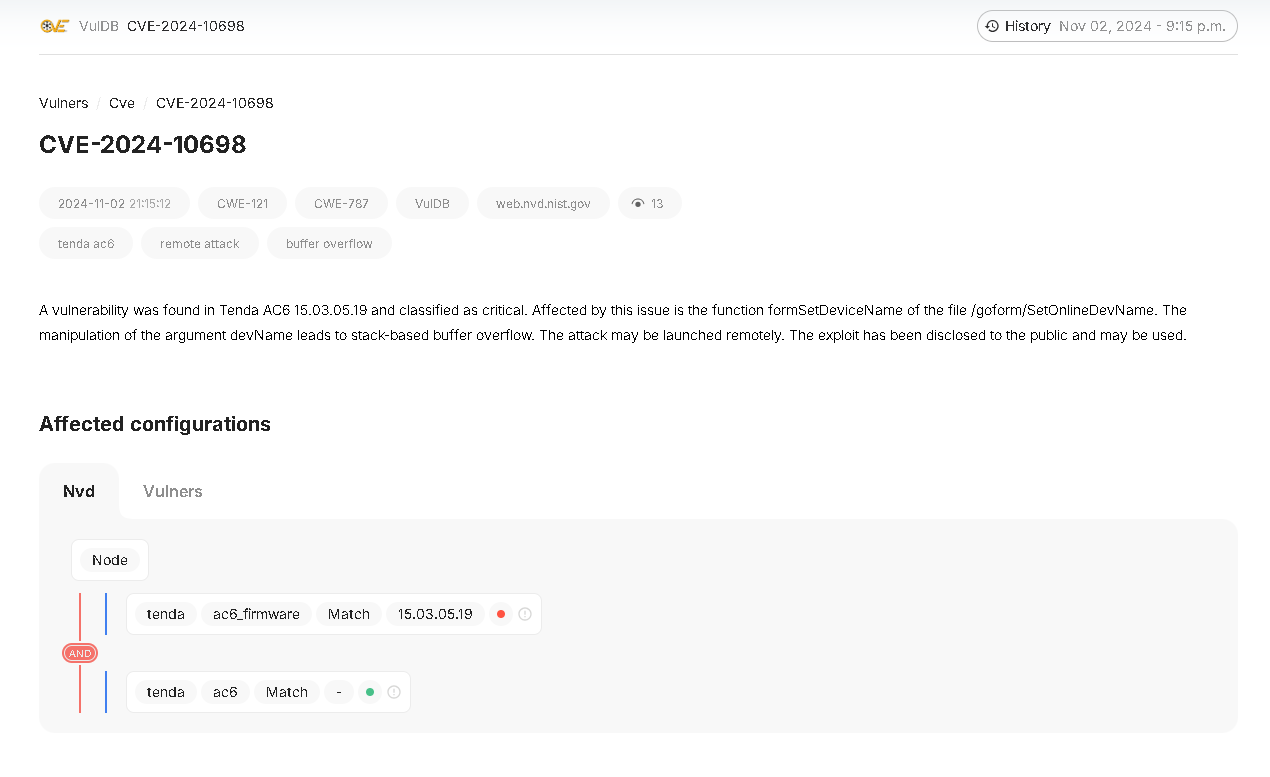
1. Shows all related CVEs, vulnerability details and references that are related to target IP address.

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



The provided Nmap scan reveals an open port on a Windows system. Ports 135, 139, and 445, associated with Microsoft services, are open, indicating potential vulnerabilities. Port 5405 is also open, but its service is unidentified. The system has a Dell MAC address and is running a Microsoft Windows operating system.

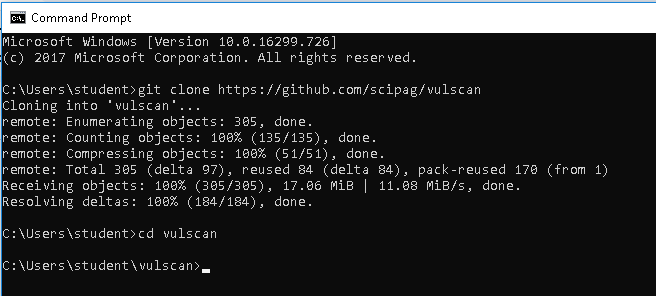
1. Copy link <https://vulners.com/cve/CVE-2021-39275> and paste into browser to investigate the vulnerability.



A kind of vulnerability

[STEP2] vulscan

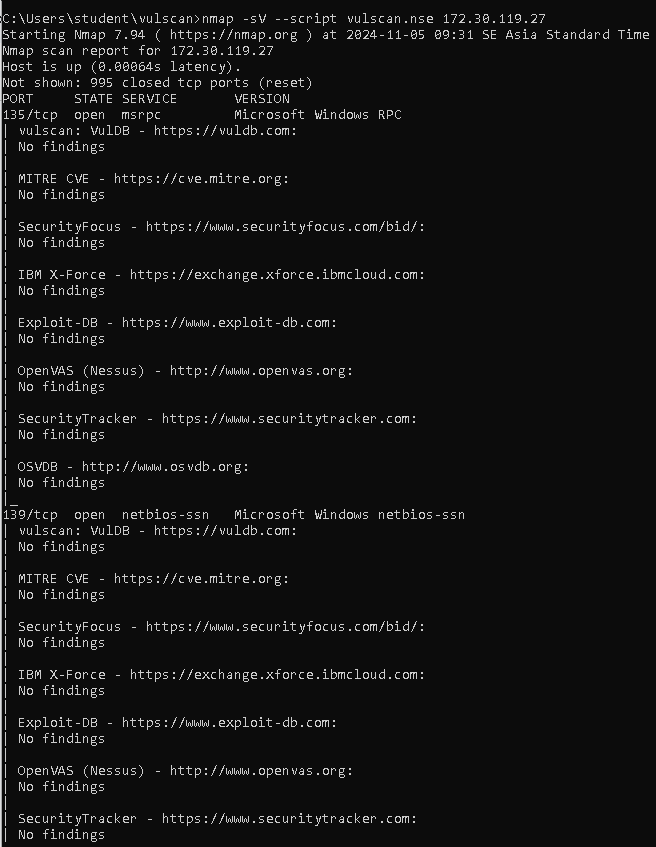
1. Install vulscan on terminal of windows from github.

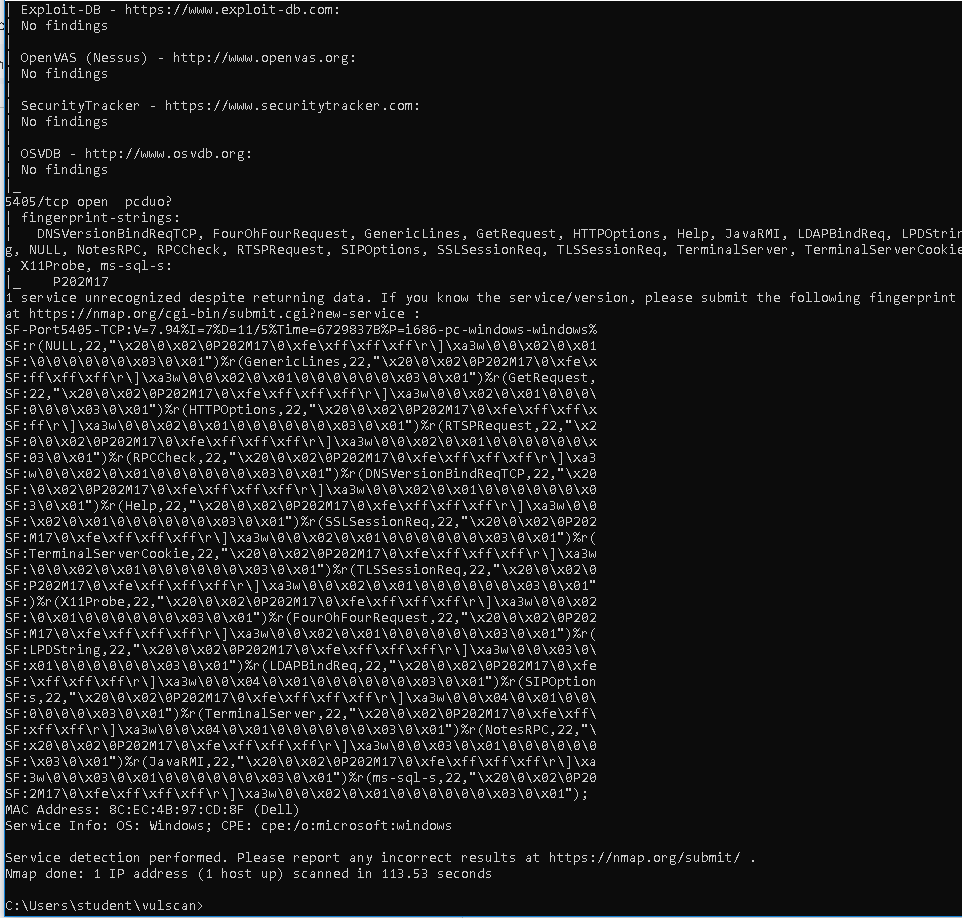


Install vulscan on terminal of windows from github.

1. Run the command

$ nmap -sV --script vulscan.nse 172.30.119.27





The scan found that the target system is running Windows with a service on port 5485/tcp that is unrecognized. The service fingerprint suggests it might be related to Microsoft but the exact service and version remain unknown. No known vulnerabilities or exploits were found for this service. It's recommended to investigate further to identify the service and assess potential risks.

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)