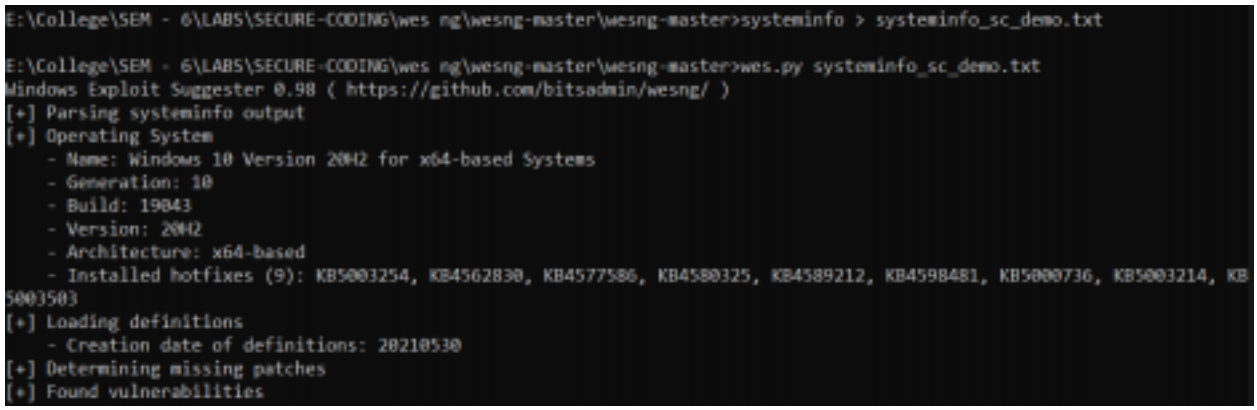
Name : Jayanth Chennupati
Regn No : 18BCN7084
Lab : 12

Windows exploit suggester:

This is a tool that helps you to identify the vulnerability in your naïve windows system. Follow the link in github to download the files required…..

https://github.com/bitsadmin/wesng Double click on the **setup.py** to setup windows exploit suggester.

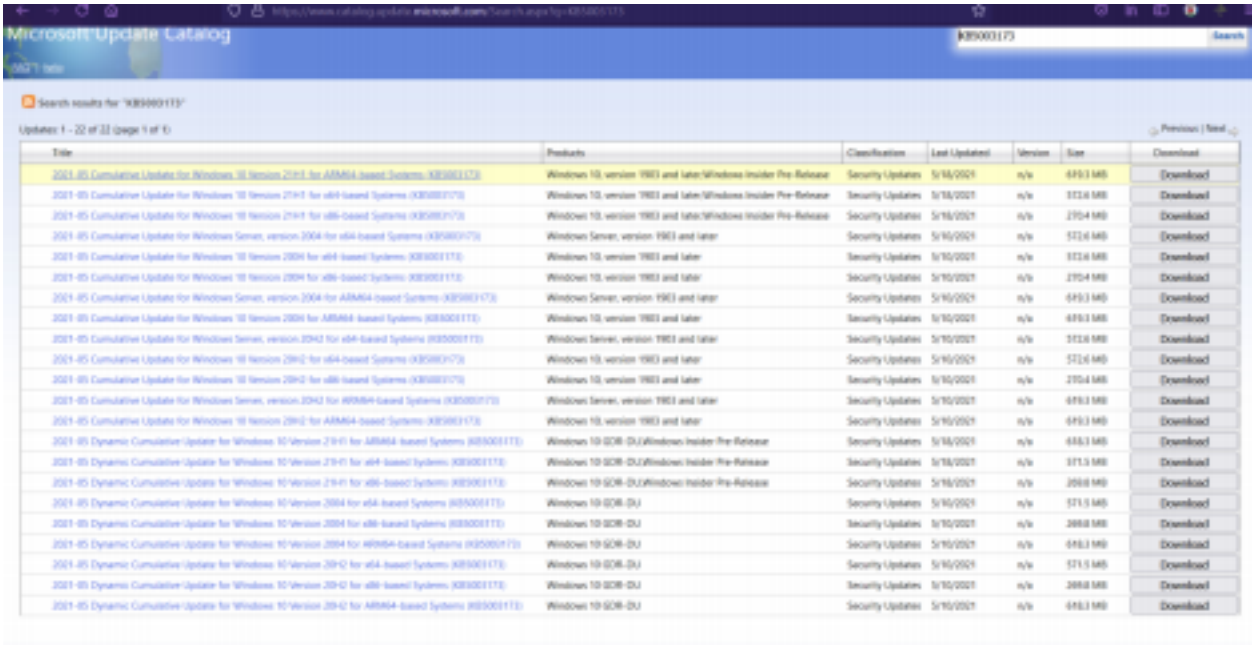
Now open command prompt do as follows



Pipe the systeminfo as a txt file to the wes.py and it will list all the vulnerabilities in the system. At last it will give you all the patches that are required to patch the vulnerabilities as below.

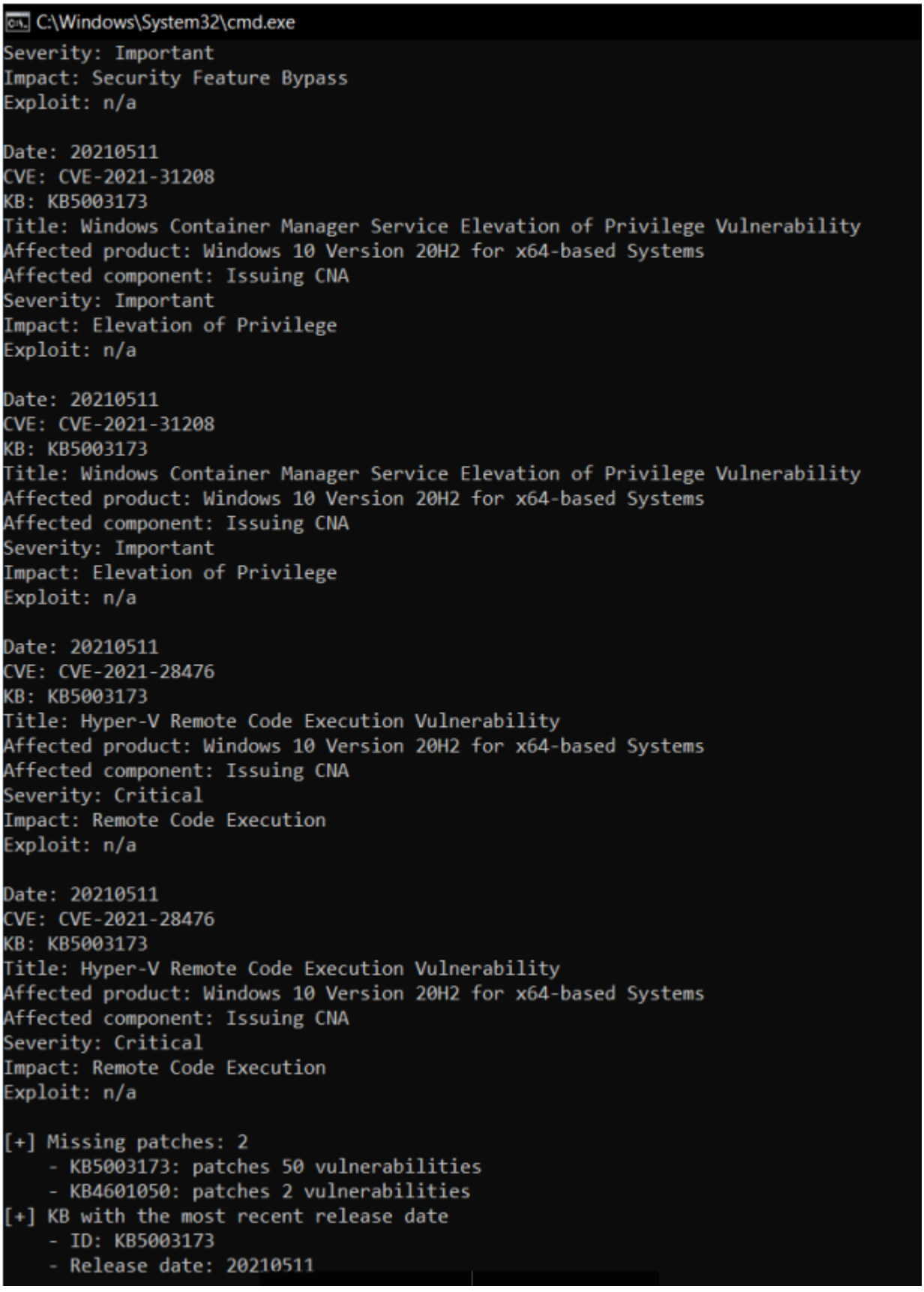
```
[+] Missing patches: 2
    - KB5003173: patches 50 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 52 of the 52 vulnerabilities found.
```

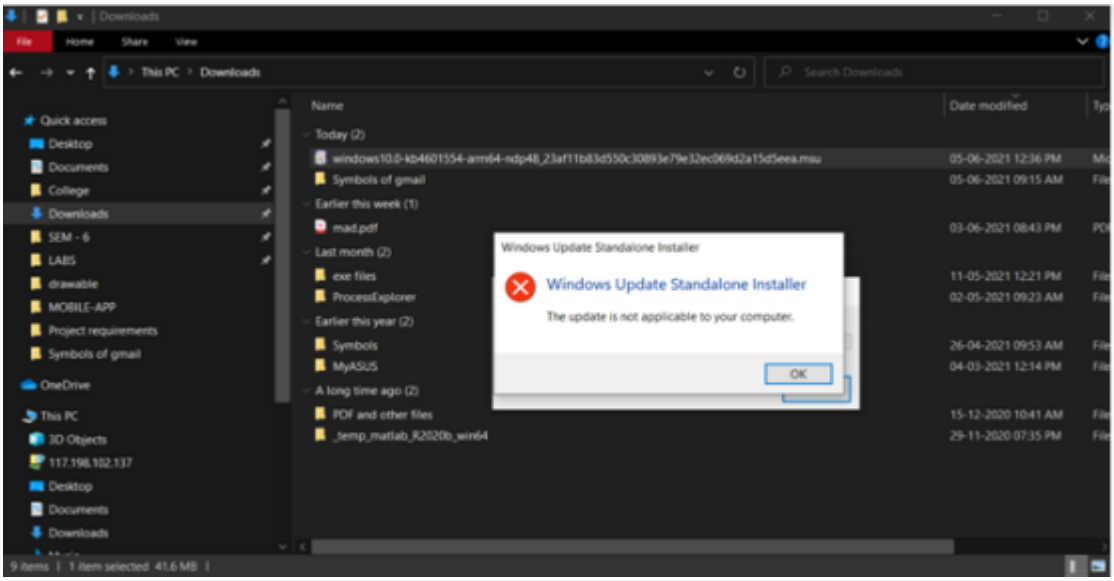
Now go to the Microsoft catalog to download the required hotfixes I will be like below.



Download the appropriate hotfixes for your pc type **winver** in start to get the version of the pc you are using. Download your hotfixes and fix your vulnerabilities.

About Windows
Windows 10
Microsoft Windows
Version 21H1 (OS Build 19043.1023)
© Microsoft Corporation. All rights reserved.
The Windows 10 Home Single Language operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software License Terms to:
user name
org name
OK


C:\Windows\System32\cmd.exe
Severity: Important
Impact: Security Feature Bypass
Exploit: n/a
Date: 20210511
CVE: CVE-2021-31208
KB: KB5003173
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20210511
CVE: CVE-2021-31208
KB: KB5003173
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a
Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a
[+] Missing patches: 2
- KB5003173: patches 50 vulnerabilities
- KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
- ID: KB5003173
- Release date: 20210511


Downloads
File
Home
Share
View
This PC
Downloads
Search Downloads
Quick access
Desktop
Documents
College
Downloads
SEM - 6
LABS
drawable
MOBILE-APP
Project requirements
Symbols of gmail
OneDrive
This PC
3D Objects
117.198.102.137
Desktop
Documents
Downloads
Name
Date modified
Today (2)
windows10.0-kb4601554-armé4-ndp48_23af11b83d550c30893e79e32ec069d2a15d5eea.msu
05-06-2021 12:36 PM
Symbols of gmail
05-06-2021 09:15 AM
Earlier this week (1)
mad.pdf
03-06-2021 08:43 PM
Last month (2)
exe files
11-05-2021 12:21 PM
ProcessExplorer
02-05-2021 09:23 AM
Earlier this year (2)
Symbols
26-04-2021 09:53 AM
MyASUS
04-03-2021 12:14 PM
A long time ago (2)
PDF and other files
15-12-2020 10:41 AM
_temp_matlab_R2020b_win64
29-11-2020 07:35 PM
Windows Update Standalone Installer
Windows Update Standalone Installer
The update is not applicable to your computer.
OK
9 items | 1 item selected 41.6 MB