NAME-SLVN YASWANTH

REGNO-19BCN7114

LAB EXPERIMENT 13

Lab experiment – Automated Vulnerability Analysis and Patch Management

Experiment and Analysis

- Deploy Windows Exploit Suggester - Next Generation (WES-NG)
- Obtain the system information and check for any reported vulnerabilities.
- If any vulnerabilities reported, apply patch and make your system safe.
- Submit the auto-generated report using pwndoc.

Happy Learning!!!

EXPERIMENT

Step 1: Clone the following repository link to desktop

Link: https://github.com/bitsadmin/wesng

While cloning we can choose the destination folder to save this zip file.

Step 2: Get the System info by running the Systeminfo.exe and store the data in systeminfo.txt

Use the following commands and them in command prompt to get system info

```
C:\Users\yaswanth>cd C:\Users\yaswanth\Downloads\wesng-master\wesng-master

C:\Users\yaswanth\Downloads\wesng-master\wesng-master>systeminfo >systeminfo_19bce7450

C:\Users\yaswanth\Downloads\wesng-master\wesng-master>python wes.py systeminfo_19bce7450
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
```

systeminfo > systeminfo_19bce7450.txt

notepad systeminfo.txt

The systeminfo.txt file contains the data related to system specifications, Hotfix, network cards and etc.

BEFORE PATCHING

Step 3:

Run the setup.py

Then see update the wes.py to the latest version

And then run the wes.py file for the systeminfo_19bce7450.txt file

We will get the details of the vulnerabilities along with the appropriate patch.

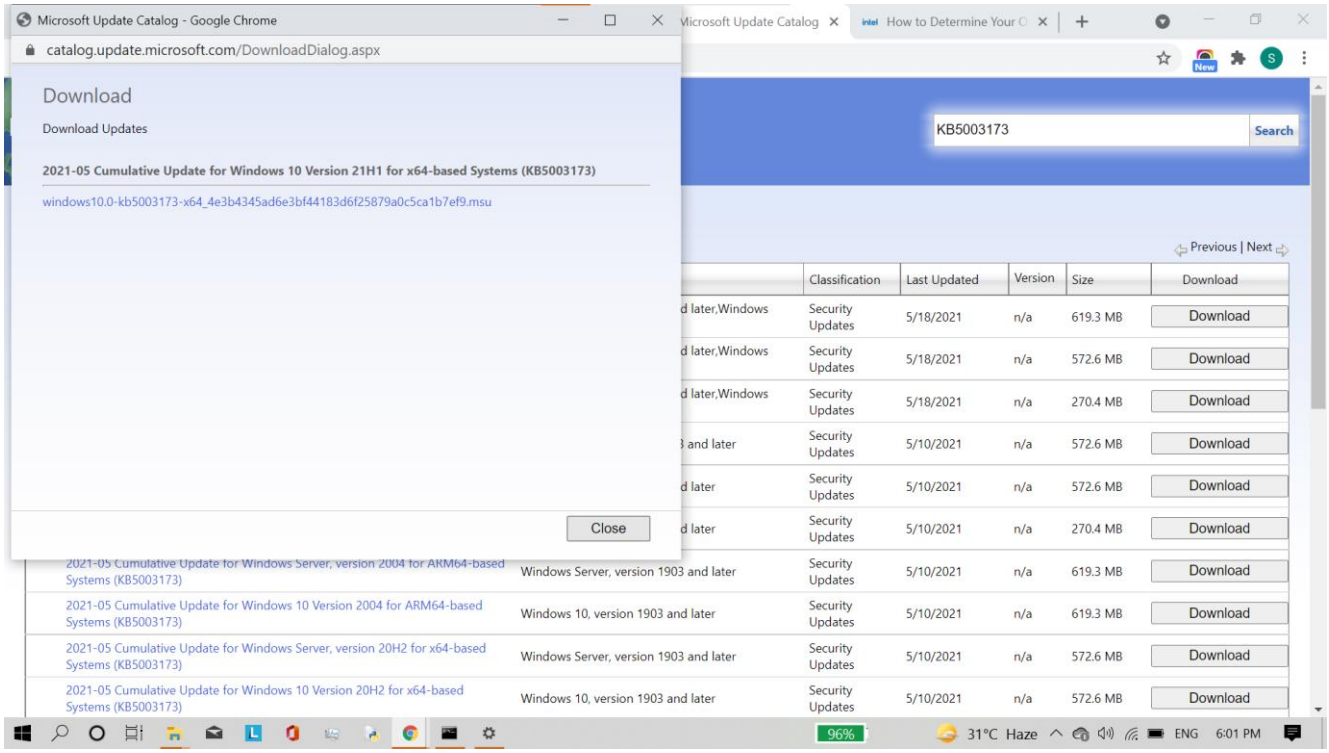
```
Date: 20210511
CVE: CVE-2021-31208
KB: KB5003173
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

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

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

C:\Users\yaswanth\Downloads\wesng-master\wesng-master>
```

AFTER PATCH

Find the missing patch from the windows catalogue and install it.

Select the appropriate patch which is suitable for the system version and download it.

While clicking download we get a dialog box like this



We can also patch it by the searching on basis of vulnerability.

If the missing patch is already downloaded then it gets updated and doesn't appear while running the test again.

While running the test we noticed there is a missing patch

But in the update history the patch is successfully installed and updated to the latest version

This might be an OEM error and Microsoft hasn't resolved it yet.

We can use this command to find any major vulnerabilities and the system doesn't have any major vulnerability.