SECURE CODING

CSE-2010

LAB ASSIGNMENT – 13

Name : Nishit Verma

Reg.No : 19BCN7050

Slot : L25+26

Lab experiment – Automated Vulnerability Analysis and Patch Management

Experiment and Analysis

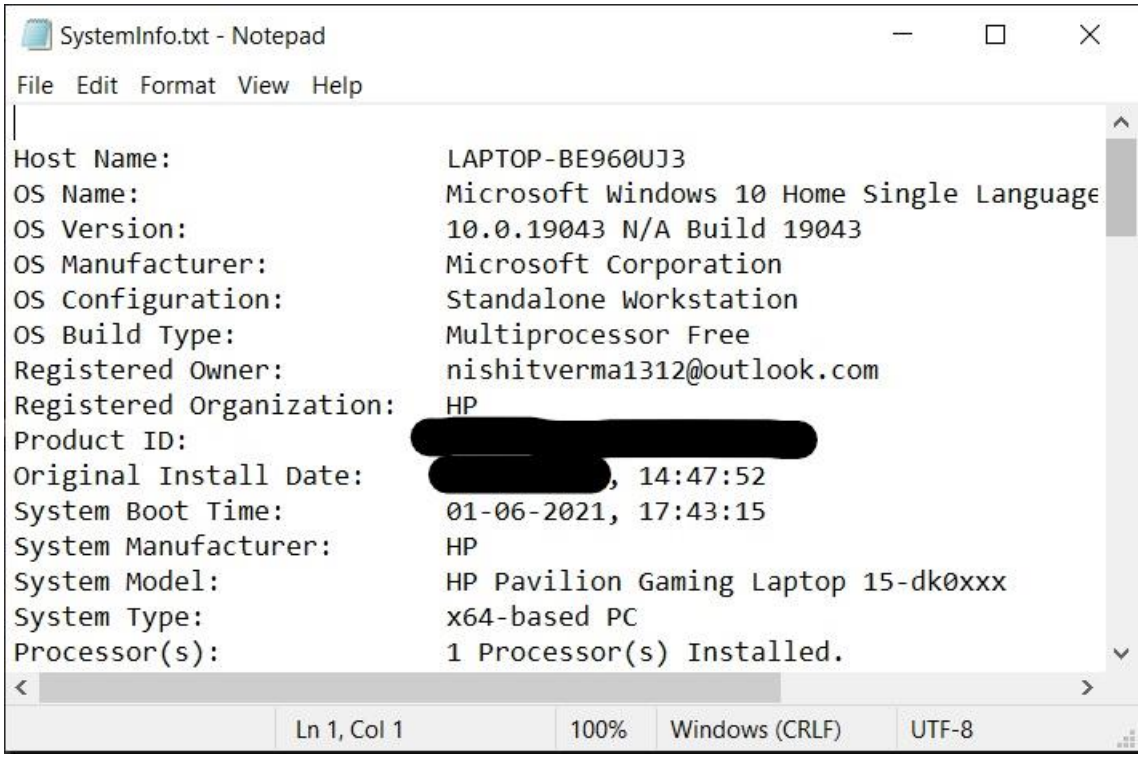
- **Deploy Windows Exploit Suggester - Next Generation (WES-NG)**
- **Obtain the system information and check for any reported vulnerabilities.**
- **If any vulnerabilities reported, apply patch and make your system safe.**
- **Submit the auto-generated report using pwndoc.**

Happy Learning!!!

1. Generating System Information in the SystemInfo.txt file

```
D:\wesng>systeminfo > SystemInfo.txt
```

The SystemInfo.txt file

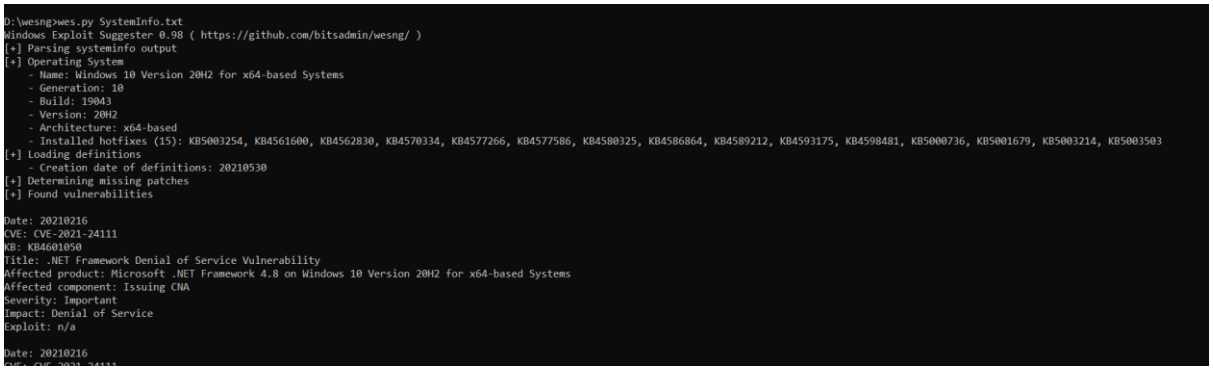


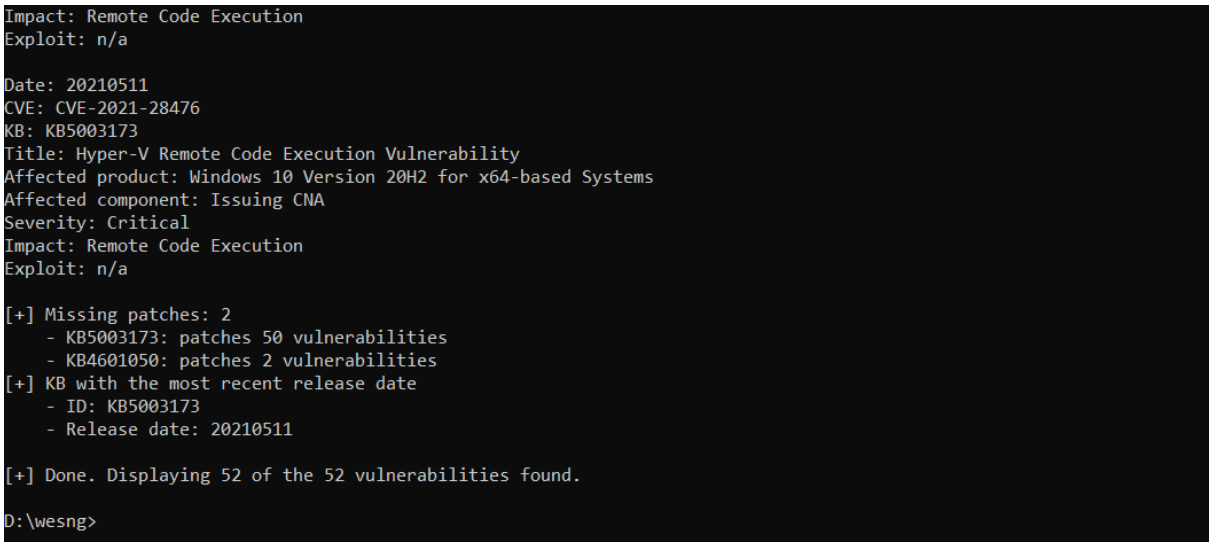
2. Updating WES-NG with the latest database

```
D:\wesng>pip3 install chardet
Collecting chardet
  Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
     |████████████████████████████████| 178 kB 1.1 MB/s
Installing collected packages: chardet
Successfully installed chardet-4.0.0

D:\wesng>wes.py --update
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210530
```

3. Checking for Vulnerabilities



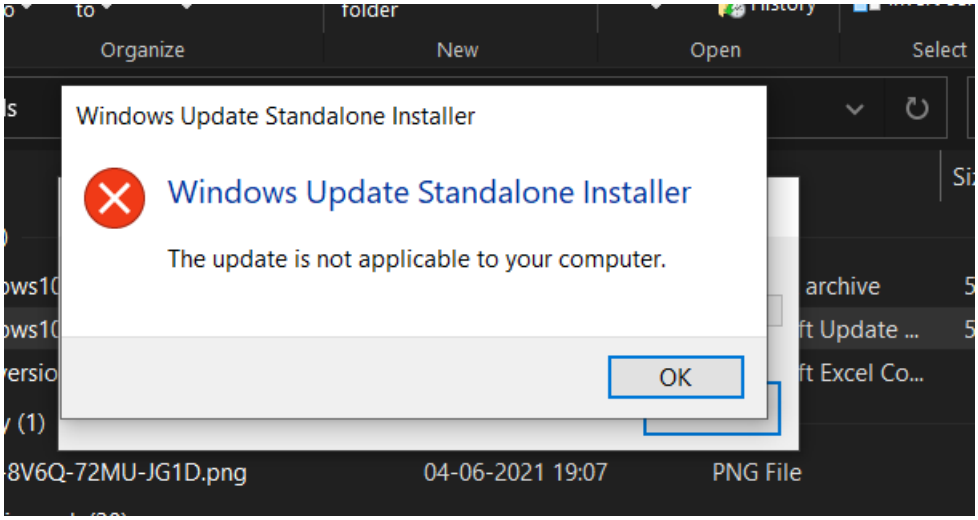


The vulnerabilities can be prevented by downloading the KB5003173 and KB4601050 patches.

4. Patching

The patches are installed in our PC but due to some errors the tool WES-NG couldn't recognise it.

So when we try to reinstall the same patches, we are not able to install them due to some errors from the OEM or simply Microsoft.



Hence we cannot install the patches to make the found vulnerability count '0'.

5. Another Way of finding dangerous vulnerabilities

We can also filter out the output in the tool WES-NG by adding display filters before scanning for vulnerabilities.

Hence we get 0 vulnerabilities if we apply display filters.

```
D:\wesng>wes.py -e SystemInfo.txt --hide "Internet Explorer" Edge
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19043
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (15): KB5003254, KB4561600, KB4562830, KB4570334, KB4577266, KB4577586, KB4580325, KB4586864, K
B4589212, KB4593175, KB4598481, KB5000736, KB5001679, KB5003214, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210530
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found


D:\wesng>
```

This shows that there aren’t any major vulnerabilities that cannot be patched from updates.