Lab experiment – Automated Vulnerability Analysis and Patch Management

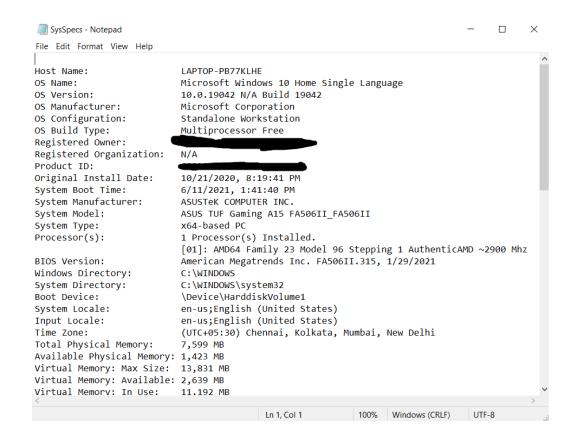
## **Experiment and Analysis**

- 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.

```
C:\Users\91630\Downloads\wesng-master\wesng-master>wes.py
usage: wes.py [-u] [--update-wes] [--version] [--definitions [DEFINITIONS]]
              [-p INSTALLEDPATCH [INSTALLEDPATCH ...]] [-d] [-e]
              [--hide HIDDENVULN [HIDDENVULN ...]] [-i IMPACTS [IMPACTS ...]]
              [-s SEVERITIES [SEVERITIES ...]] [-o [OUTPUTFILE]]
              [--muc-lookup] [-h]
              systeminfo [qfefile]
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
positional arguments:
  systeminfo
                        Specify systeminfo.txt file
  qfefile
                        Specify the file containing the output of the 'wmic
                        qfe' command
optional arguments:
                        Download latest list of CVEs
  -u, --update
  --update-wes
                        Download latest version of wes.py
                        Show version information
  --version
  --definitions [DEFINITIONS]
                        Definitions zip file (default: definitions.zip)
  -p INSTALLEDPATCH [INSTALLEDPATCH ...], --patches INSTALLEDPATCH [INSTALLEDPATCH ...]
                        Manually specify installed patches in addition to the
                        ones listed in the systeminfo.txt file
  -d, --usekbdate
                        Filter out vulnerabilities of KBs published before the
                        publishing date of the most recent KB installed
  -e, --exploits-only
                        Show only vulnerabilities with known exploits
  --hide HIDDENVULN [HIDDENVULN ...]
                        Hide vulnerabilities of for example Adobe Flash Player
                        and Microsoft Edge
  -i IMPACTS [IMPACTS ...], --impact IMPACTS [IMPACTS ...]
                        Only display vulnerabilities with a given impact
  -s SEVERITIES [SEVERITIES ...], --severity SEVERITIES [SEVERITIES ...]
                        Only display vulnerabilities with a given severity
  -o [OUTPUTFILE], --output [OUTPUTFILE]
                        Store results in a file
  --muc-lookup
                        Hide vulnerabilities if installed hotfixes are listed
                        in the Microsoft Update Catalog as superseding
                        hotfixes for the original BulletinKB
  -h, --help
                        Show this help message and exit
examples:
  Download latest definitions
  wes.py --update
```

## 1) Generate system Info into text file.

Go to cmd and enter "%userprofile%\Desktop\SysSpecs.txt & notepad %userprofile%\Desktop\SysSpecs.txt"



## 2) Updating WES-NG with latest packages

```
C:\wesng-master>pip install chardet
Requirement already satisfied: chardet in c:\python\lib\site-packages (4.0.0)
WARNING: You are using pip version 21.0.1; however, version 21.1.2 is available.
You should consider upgrading via the 'c:\python\python.exe -m pip install --upgrade pip' command.
```

## 3) Checking for Vulnerabilities

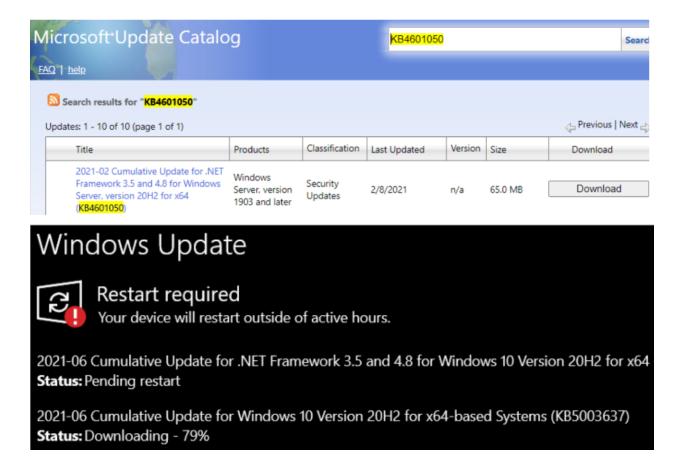
```
Administrator: Command Prompt
C:\wesng-master>wes.py SysINFO.txt
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
   - Build: 19042
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (12): KB4601554, KB4561600, KB4562830, KB4577266, KB4577586, KB4580325, KB45868
64, KB4589212, KB4593175, KB4598481, KB5003173, KB5003242
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a
Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a
[+] Missing patches: 1
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB4601050
    - Release date: 20210216
[+] Done. Displaying 2 of the 2 vulnerabilities found.
C:\wesng-master>_
```

4) The Vulnerabilities can be addressed by installing patches for the hotfix:KB4601050 from Microsoft update catlog:

According to Microsoft support:

| Windows Update<br>and Microsoft<br>Update | Yes | None. This update will be downloaded and installed automatically from Windows Update.      |
|---|-----|--|
| Microsoft Update<br>Catalog               | Yes | To get the standalone package for this update, go to the Microsoft Update Catalog website. |

Standalone package from MS update catlog:



Standalone package was available. Patch along with few other patches was installed directly via Windows Update not displayed i system info txt file.