

## **SECURE CODING LAB-13(L23+L24)**

M.Hruthik

19BCN7092

### **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 [qfile]

Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )

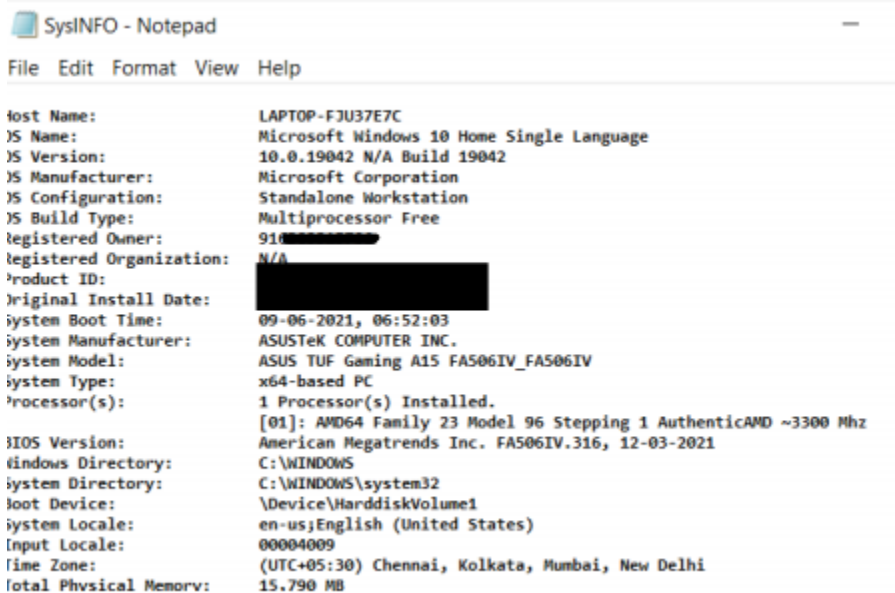
positional arguments:
  systeminfo            Specify systeminfo.txt file
  qfile                 Specify the file containing the output of the 'wmic
                        qfe' command

optional arguments:
  -u, --update          Download latest list of CVEs
  --update-wes          Download latest version of wes.py
  --version             Show version information
  --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
  wes.py -u

```

- Generating system info into a text file



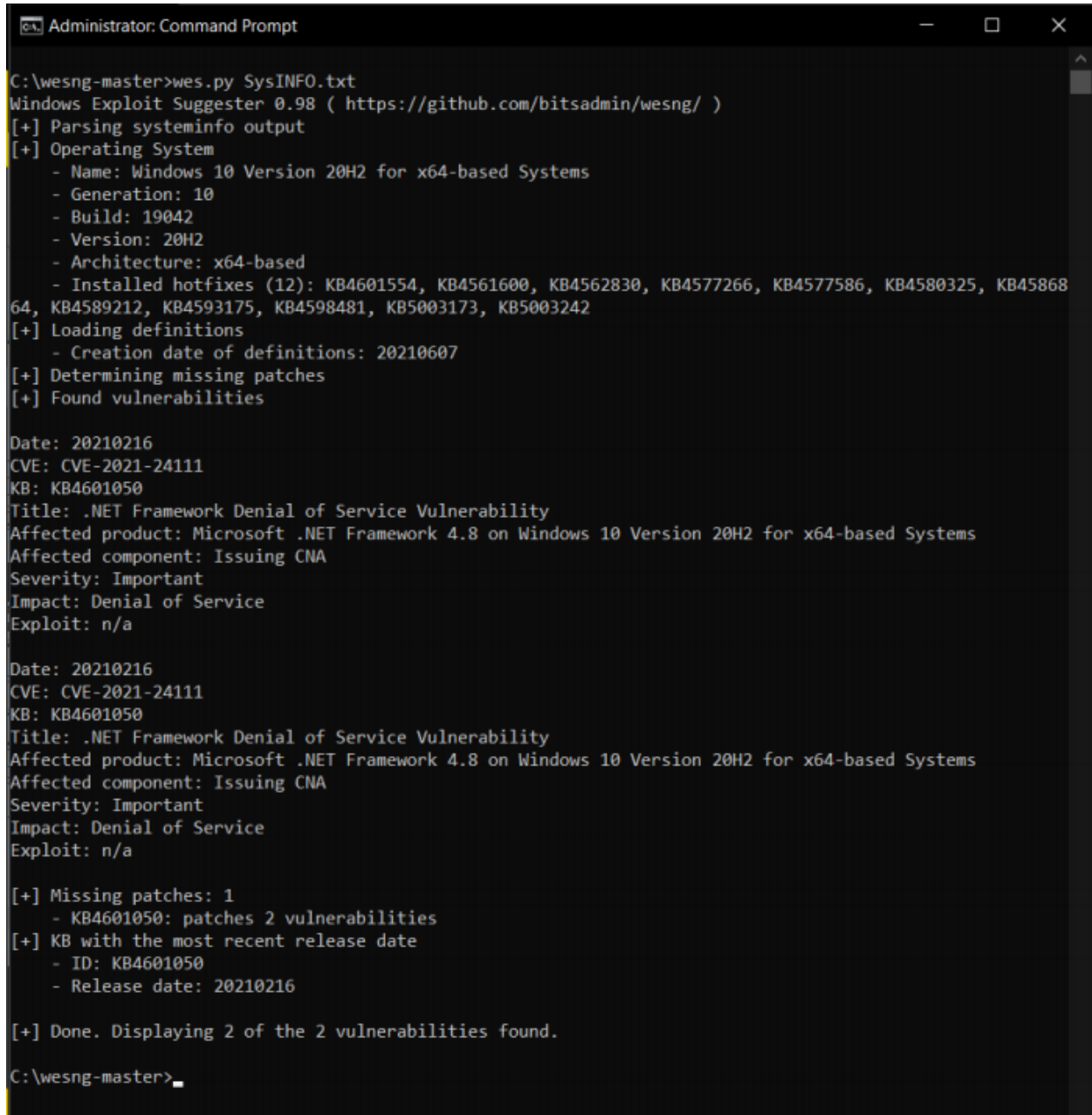
The screenshot shows a Notepad window titled "SysINFO - Notepad" with a menu bar (File, Edit, Format, View, Help). The text content displays system information in two columns:

Host Name:	LAPTOP-FJU37E7C
OS Name:	Microsoft Windows 10 Home Single Language
OS Version:	10.0.19042 N/A Build 19042
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
Registered Owner:	91630
Registered Organization:	N/A
Product ID:	[REDACTED]
Original Install Date:	[REDACTED]
System Boot Time:	09-06-2021, 06:52:03
System Manufacturer:	ASUSTeK COMPUTER INC.
System Model:	ASUS TUF Gaming A15 FA506IV_FA506IV
System Type:	x64-based PC
Processor(s):	1 Processor(s) Installed. [01]: AMD64 Family 23 Model 96 Stepping 1 AuthenticAMD ~3300 Mhz
BIOS Version:	American Megatrends Inc. FA506IV.316, 12-03-2021
Windows Directory:	C:\WINDOWS
System Directory:	C:\WINDOWS\system32
Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)
Input Locale:	00004009
Time Zone:	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:	15.790 MB

- Updating WES-NG with latest package

```
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.
```

- 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>
```

- . The vulnerabilities can be addressed by installing patches for the hotfix: KB4601050 from Microsoft update catlog: According to Microsoft support

Microsoft Update Catalog

[FAQ](#) | [help](#)

Search results for "KB4601050"

Updates: 1 - 10 of 10 (page 1 of 1)
 |

Title	Products	Classification	Last Updated	Version	Size	Download
2021-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server, version 20H2 for x64 (KB4601050)	Windows Server, version 1903 and later	Security Updates	2/8/2021	n/a	65.0 MB	<input type="button" value="Download"/>

# Windows Update

Restart required
Your device will restart outside of active hours.

2021-06 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 (KB5003637)
**Status:** Pending restart

2021-06 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003637)
**Status:** Downloading - 79%