Secure Coding Lab - 13

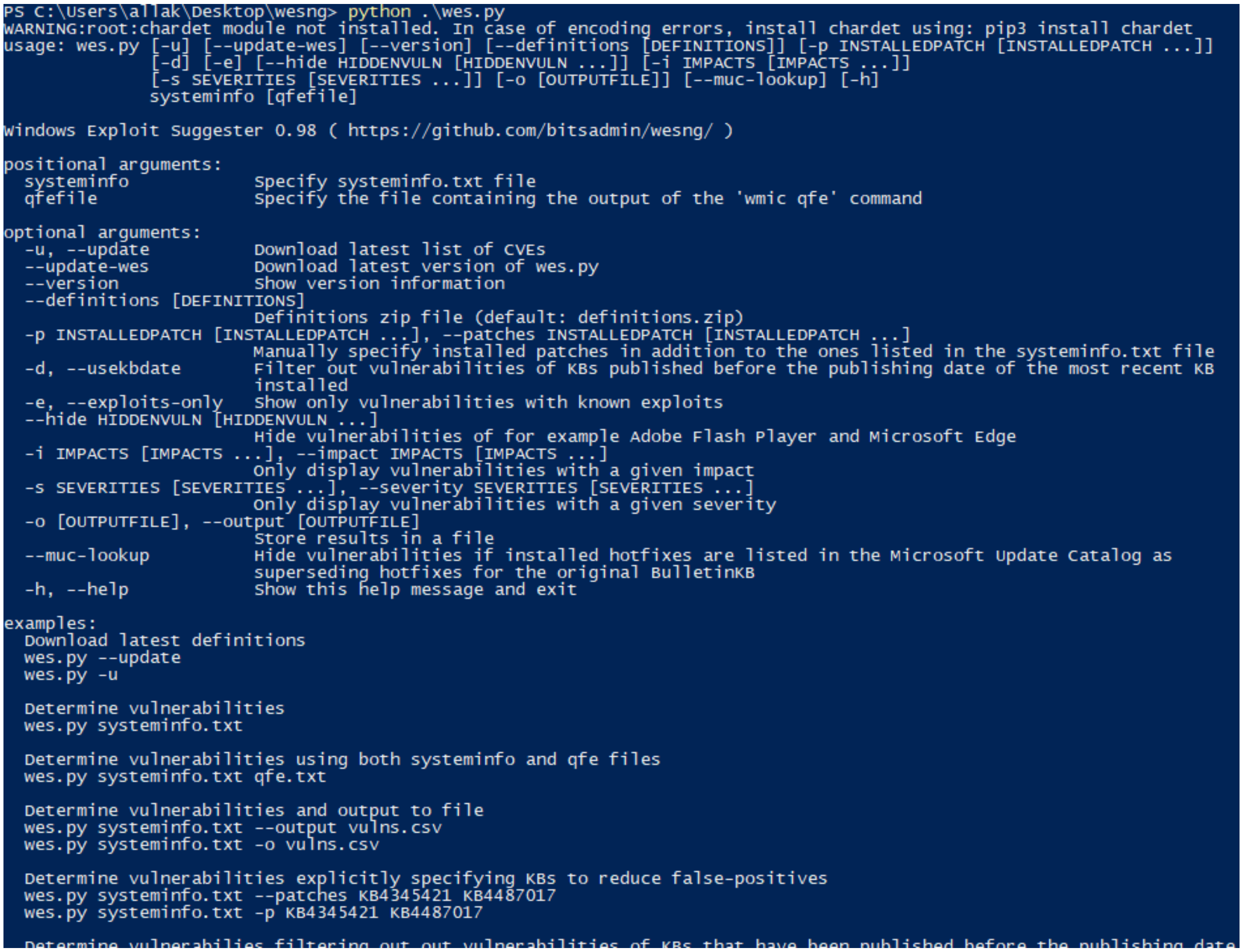
Name: Tejeswar Allaka

Reg No: 18BCN7033

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.**

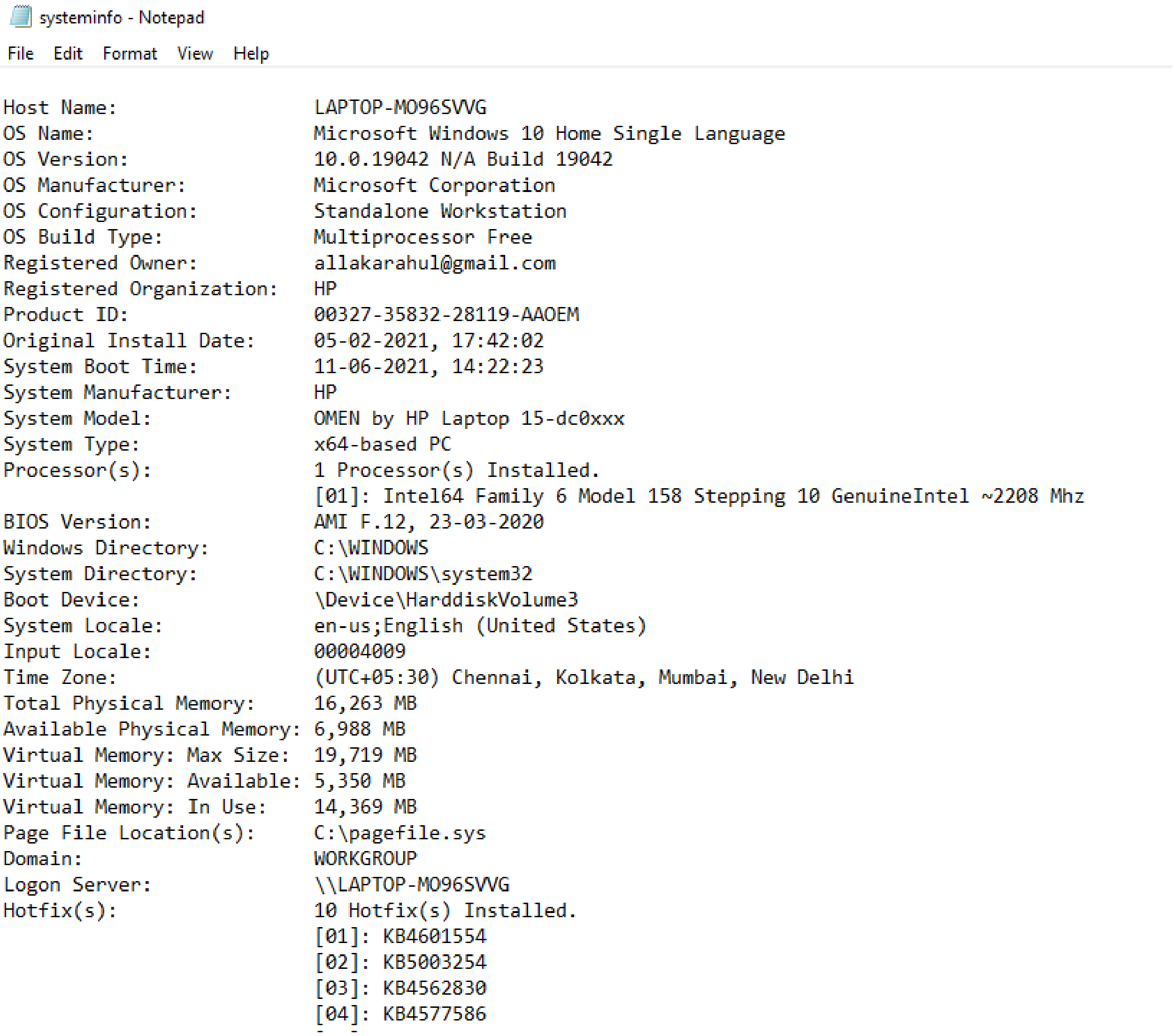
1) Clone the Windows Exploit Suggester repo and run the wes.py



```
PS C:\Users\allak\Desktop\wesng> python .\wes.py
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
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:
  -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

  Determine vulnerabilities
  wes.py systeminfo.txt

  Determine vulnerabilities using both systeminfo and qfe files
  wes.py systeminfo.txt qfe.txt

  Determine vulnerabilities and output to file
  wes.py systeminfo.txt --output vulns.csv
  wes.py systeminfo.txt -o vulns.csv

  Determine vulnerabilities explicitly specifying KBs to reduce false-positives
  wes.py systeminfo.txt --patches KB4345421 KB4487017
  wes.py systeminfo.txt -p KB4345421 KB4487017

  Determine vulnerabilies filtering out out vulnerabilities of KBs that have been published before the publishing date
```

2) Output your system info with this command

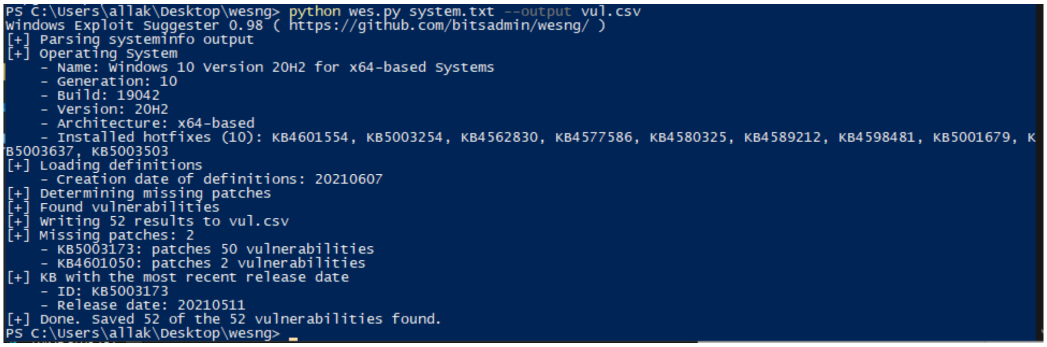
“systeminfo> systeminfo.txt “



```
Host Name:                 LAPTOP-MO96SVVG
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:          allakarahul@gmail.com
Registered Organization:   HP
Product ID:                00327-35832-28119-AAOEM
Original Install Date:     05-02-2021, 17:42:02
System Boot Time:          11-06-2021, 14:22:23
System Manufacturer:       HP
System Model:              OMEN by HP Laptop 15-dc0xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2208 Mhz
BIOS Version:              AMI F.12, 23-03-2020
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,263 MB
Available Physical Memory: 6,988 MB
Virtual Memory: Max Size:  19,719 MB
Virtual Memory: Available: 5,350 MB
Virtual Memory: In Use:    14,369 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-MO96SVVG
Hotfix(s):                 10 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB5003254
                           [03]: KB4562830
                           [04]: KB4577586
```

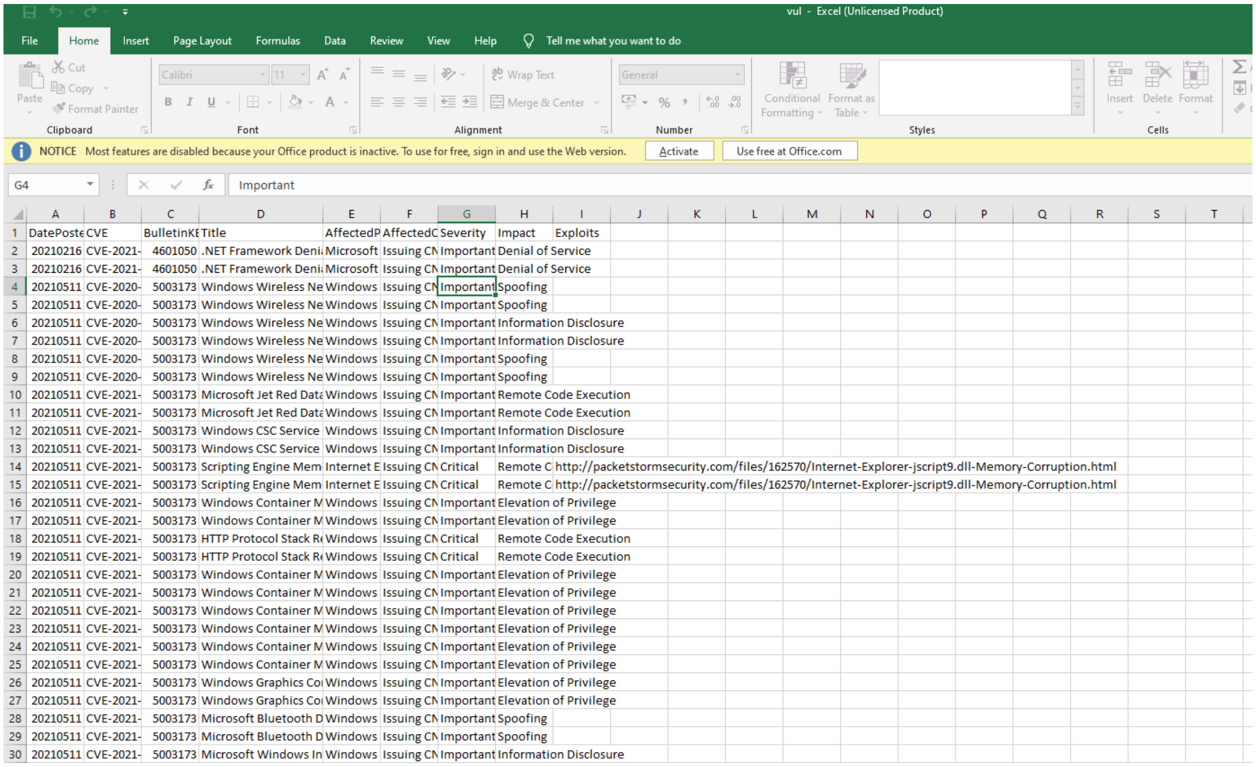
3) Now look for vulnerabilities using your last txt file output

“ wes.py systeminfo.txt --output vul.csv”



```
PS C:\Users\allak\Desktop\wesng> python wes.py system.txt --output vul.csv
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 (10): KB4601554, KB5003254, KB4562830, KB4577586, KB4580325, KB4589212, KB4598481, KB5001679, K
B5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
[+] Writing 52 results to vul.csv
[+] Missing patches: 2
    - KB5003173: patches 50 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511
[+] Done. Saved 52 of the 52 vulnerabilities found.
PS C:\Users\allak\Desktop\wesng> _
```

4) All vulnerabilities in your system are shown in vul.csv



NOTICE Most features are disabled because your Office product is inactive. To use for free, sign in and use the Web version. Activate Use free at Office.com

G4 Important

	A	B	C	D	E	F	G	H	I
1	DatePoste	CVE	BulletinKE	Title	AffectedP	AffectedC	Severity	Impact	Exploits
2	20210216	CVE-2021-	4601050	.NET Framework Deni	Microsoft	Issuing CN	Important	Denial of Service	
3	20210216	CVE-2021-	4601050	.NET Framework Deni	Microsoft	Issuing CN	Important	Denial of Service	
4	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Spoofing	
5	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Spoofing	
6	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Information Disclosure	
7	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Information Disclosure	
8	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Spoofing	
9	20210511	CVE-2020-	5003173	Windows Wireless Ne	Windows	Issuing CN	Important	Spoofing	
10	20210511	CVE-2021-	5003173	Microsoft Jet Red Data	Windows	Issuing CN	Important	Remote Code Execution	
11	20210511	CVE-2021-	5003173	Microsoft Jet Red Data	Windows	Issuing CN	Important	Remote Code Execution	
12	20210511	CVE-2021-	5003173	Windows CSC Service	Windows	Issuing CN	Important	Information Disclosure	
13	20210511	CVE-2021-	5003173	Windows CSC Service	Windows	Issuing CN	Important	Information Disclosure	
14	20210511	CVE-2021-	5003173	Scripting Engine Mem	Internet E	Issuing CN	Critical	Remote C	http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.html
15	20210511	CVE-2021-	5003173	Scripting Engine Mem	Internet E	Issuing CN	Critical	Remote C	http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.html
16	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
17	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
18	20210511	CVE-2021-	5003173	HTTP Protocol Stack R	Windows	Issuing CN	Critical	Remote Code Execution	
19	20210511	CVE-2021-	5003173	HTTP Protocol Stack R	Windows	Issuing CN	Critical	Remote Code Execution	
20	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
21	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
22	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
23	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
24	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
25	20210511	CVE-2021-	5003173	Windows Container M	Windows	Issuing CN	Important	Elevation of Privilege	
26	20210511	CVE-2021-	5003173	Windows Graphics Co	Windows	Issuing CN	Important	Elevation of Privilege	
27	20210511	CVE-2021-	5003173	Windows Graphics Co	Windows	Issuing CN	Important	Elevation of Privilege	
28	20210511	CVE-2021-	5003173	Microsoft Bluetooth D	Windows	Issuing CN	Important	Spoofing	
29	20210511	CVE-2021-	5003173	Microsoft Bluetooth D	Windows	Issuing CN	Important	Spoofing	
30	20210511	CVE-2021-	5003173	Microsoft Windows In	Windows	Issuing CN	Important	Information Disclosure	