LAB-13

Secure Coding

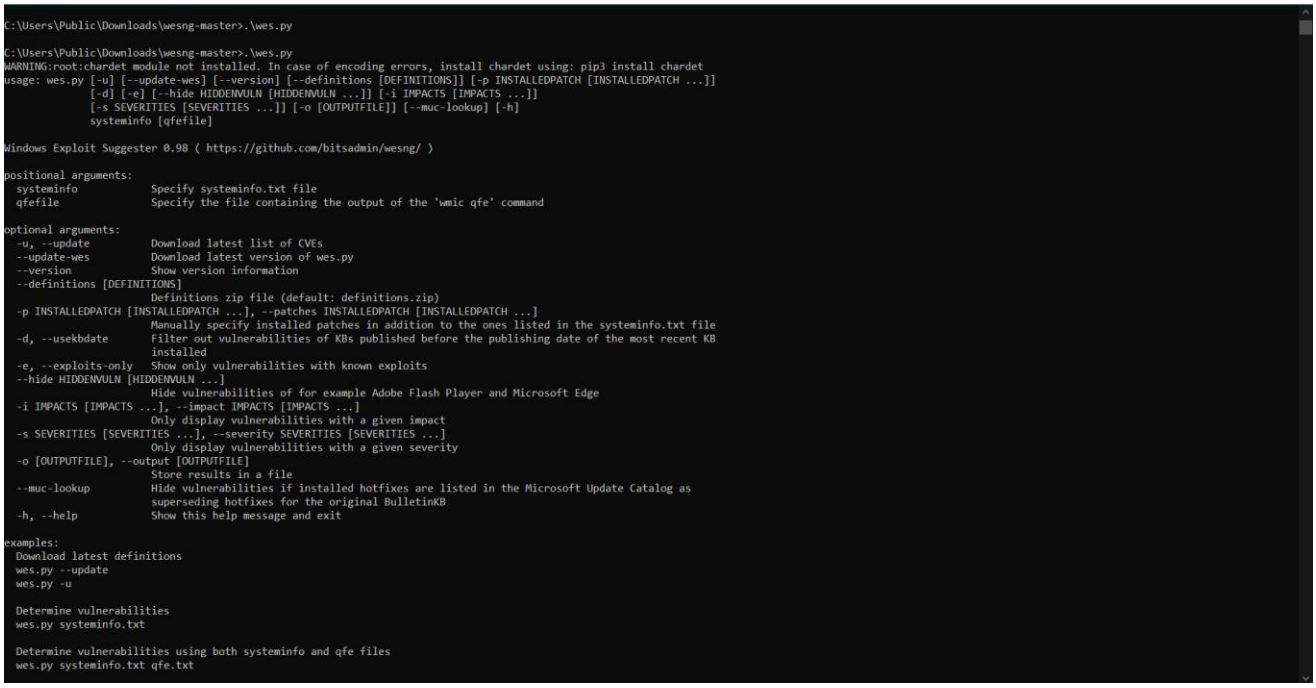
Lab experiment – Automated Vulnerability Analysis and Patch ManagementExperiment and Analysis

D.V.S MOHITH GUPTA

18BCN7072

- **Deploy Windows Exploit Suggester - Next Generation (WES-NG)**
- **Obtain the system information and check for any reported vulnerabilities.**
- **If any vulnerabilities are reported, apply patches and make your systemsafe.**

1) Clone the Windows Exploit Suggester repo and run the wes.py
2) Output your system info with this command
3) Now look for vulnerabilities using your last txt file output
4) All vulnerabilities in your system are shown in vul.csv



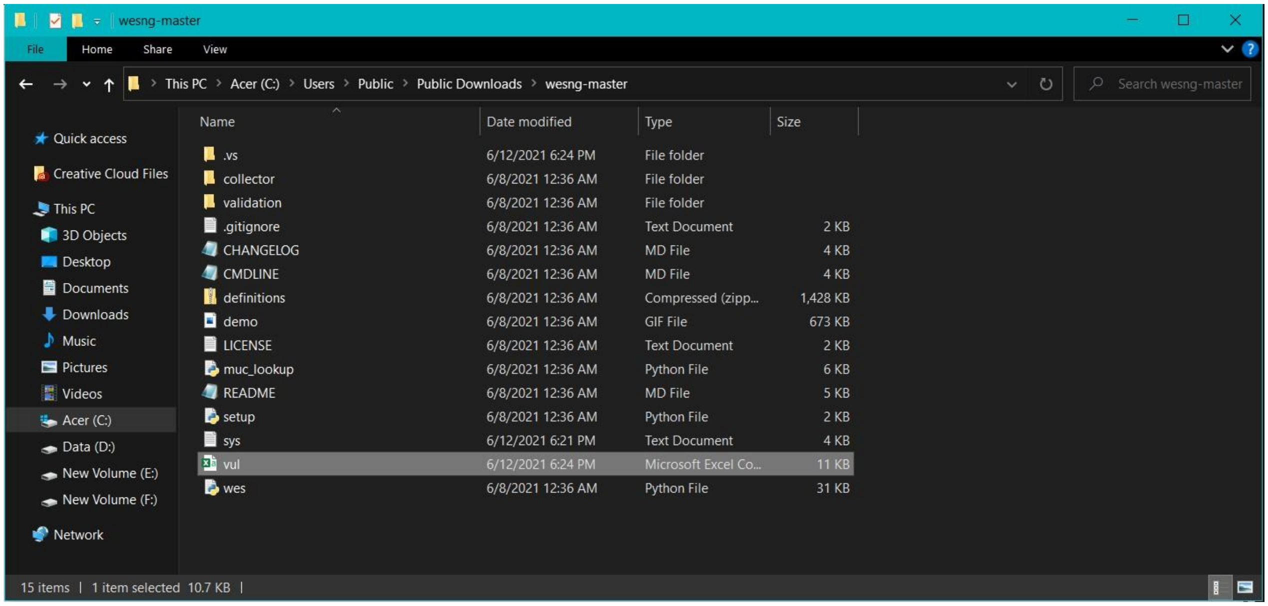
```
  wes.py systeminfo.txt -d

  Determine vulnerabilities explicitly specifying definitions file
  wes.py systeminfo.txt --definitions C:\tmp\mydefs.zip

  List only vulnerabilities with exploits, excluding IE, Edge and Flash
  wes.py systeminfo.txt --exploits-only --hide "Internet Explorer" Edge Flash
  wes.py systeminfo.txt -e --hide "Internet Explorer" Edge Flash

  Only show vulnerabilities of a certain impact
  wes.py systeminfo.txt --impact "Remote Code Execution"
  wes.py systeminfo.txt -i "Remote Code Execution"

  Only show vulnerabilities of a certain severity
  wes.py systeminfo.txt --severity critical
  wes.py systeminfo.txt -s critical

  Validate supersedence against Microsoft's online Update Catalog
  wes.py systeminfo.txt --muc-lookup

  Download latest version of WES-NG
  wes.py --update-wes

C:\Users\Public\Downloads\wesng-master>systeminfo>sys.txt

C:\Users\Public\Downloads\wesng-master>python wes.py sys.txt --output vul.csv
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
[+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19042
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (7): KB5003254, KB4562830, KB4577586, KB4580325, KB4589212, KB5003637, 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.

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

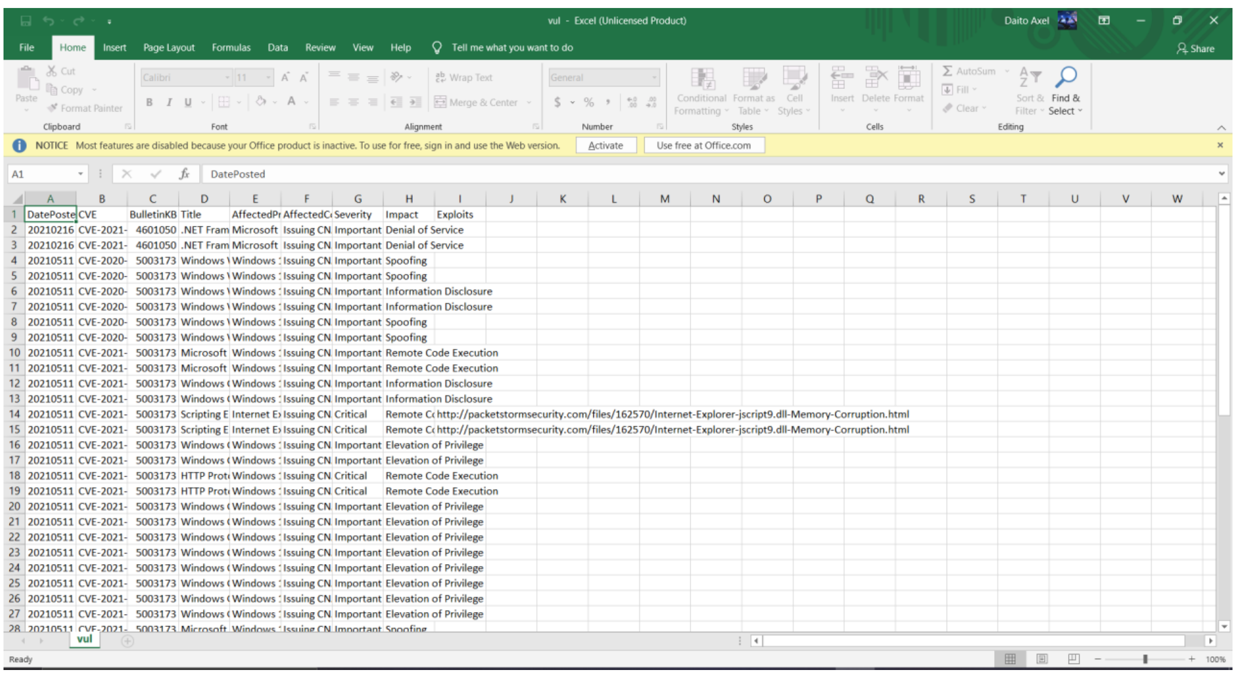
sys - Notepad

File Edit Format View Help

```
Host Name:                 LAPTOP-9GPA2HP1
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:          N/A
Registered Organization:   N/A
Product ID:                00327-35870-75472-AAOEM
Original Install Date:     3/15/2021, 3:25:18 PM
System Boot Time:          6/11/2021, 6:24:44 PM
System Manufacturer:       Acer
System Model:              Nitro AN515-43
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 24 Stepping 1 AuthenticAMD ~1400 Mhz
BIOS Version:              Insyde Corp. V1.08, 12/24/2019
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             in;Indonesian
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     6,083 MB
Available Physical Memory: 804 MB
Virtual Memory: Max Size:  17,859 MB
Virtual Memory: Available: 8,171 MB
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8


wesng-master
File
Home
Share
View
This PC > Acer (C:) > Users > Public > Public Downloads > wesng-master
Search wesng-master
Quick access
Creative Cloud Files
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Acer (C:)
Data (D:)
New Volume (E:)
New Volume (F:)
Network
Name
Date modified
Type
Size
.vs 6/12/2021 6:24 PM File folder
collector 6/8/2021 12:36 AM File folder
validation 6/8/2021 12:36 AM File folder
.gitignore 6/8/2021 12:36 AM Text Document 2 KB
CHANGELOG 6/8/2021 12:36 AM MD File 4 KB
CMDLINE 6/8/2021 12:36 AM MD File 4 KB
definitions 6/8/2021 12:36 AM Compressed (zipp... 1,428 KB
demo 6/8/2021 12:36 AM GIF File 673 KB
LICENSE 6/8/2021 12:36 AM Text Document 2 KB
muc_lookup 6/8/2021 12:36 AM Python File 6 KB
README 6/8/2021 12:36 AM MD File 5 KB
setup 6/8/2021 12:36 AM Python File 2 KB
sys 6/12/2021 6:21 PM Text Document 4 KB
vul 6/12/2021 6:24 PM Microsoft Excel Co... 11 KB
wes 6/8/2021 12:36 AM Python File 31 KB
15 items | 1 item selected 10.7 KB |


vul - Excel (Unlicensed Product)
Daito Axel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me what you want to do
Share
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
A1
DatePosted
DatePoste CVE BulletinKB Title AffectedPr AffectedC Severity Impact Exploits
20210216 CVE-2021- 4601050 .NET Fram Microsoft Issuing CN Important Denial of Service
20210216 CVE-2021- 4601050 .NET Fram Microsoft Issuing CN Important Denial of Service
20210511 CVE-2020- 5003173 Windows Windows Issuing CN Important Spoofing
20210511 CVE-2020- 5003173 Windows Windows Issuing CN Important Information Disclosure
20210511 CVE-2021- 5003173 Microsoft Windows Issuing CN Important Remote Code Execution
20210511 CVE-2021- 5003173 Scripting E Internet E Issuing CN Critical Remote C http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.html
20210511 CVE-2021- 5003173 Windows Windows Issuing CN Important Elevation of Privilege
20210511 CVE-2021- 5003173 HTTP Prot Windows Issuing CN Critical Remote Code Execution
vul
Ready