A.Harshita

19bce7033

L39+L40

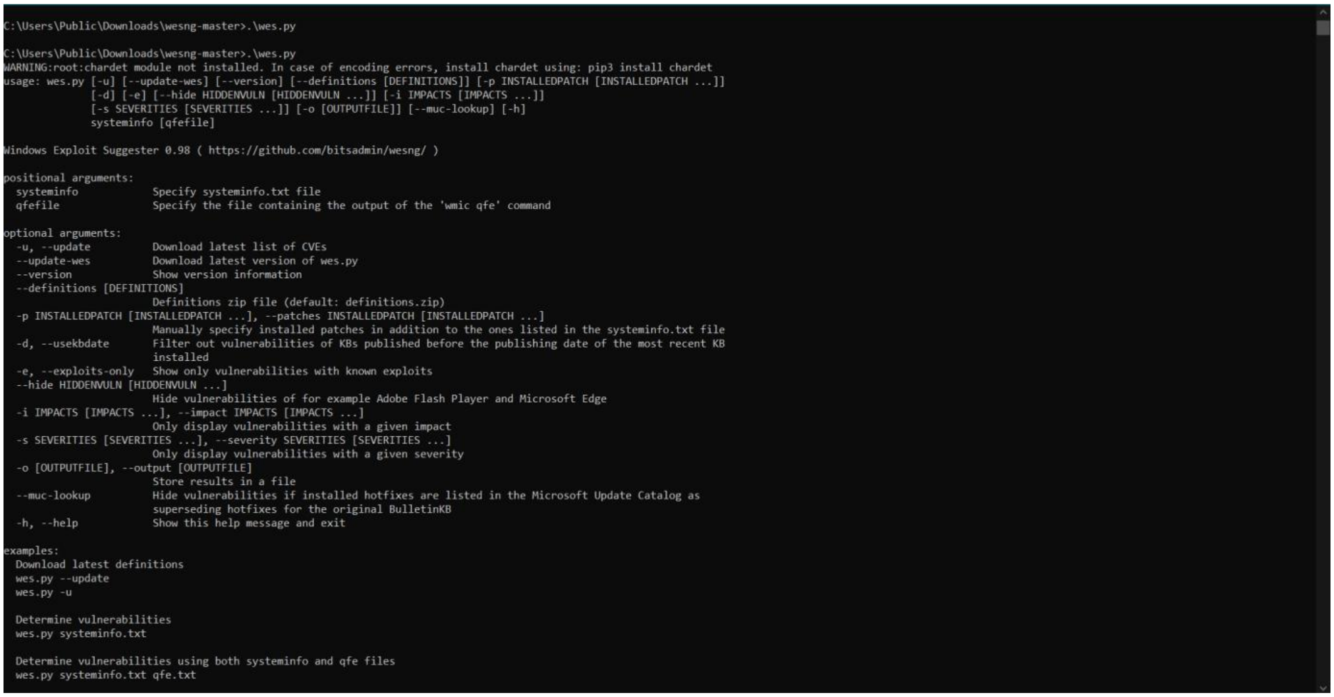
LAB 13

Lab experiment – Automated Vulnerability Analysis and Patch Management

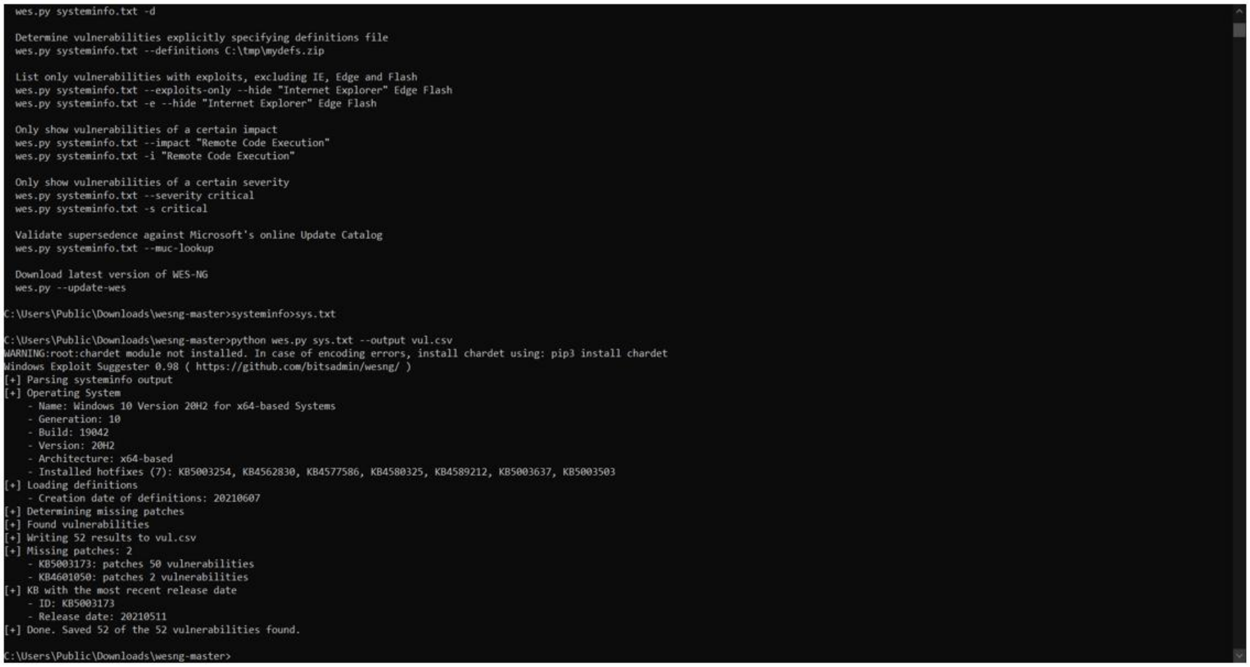
Experiment and Analysis

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

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

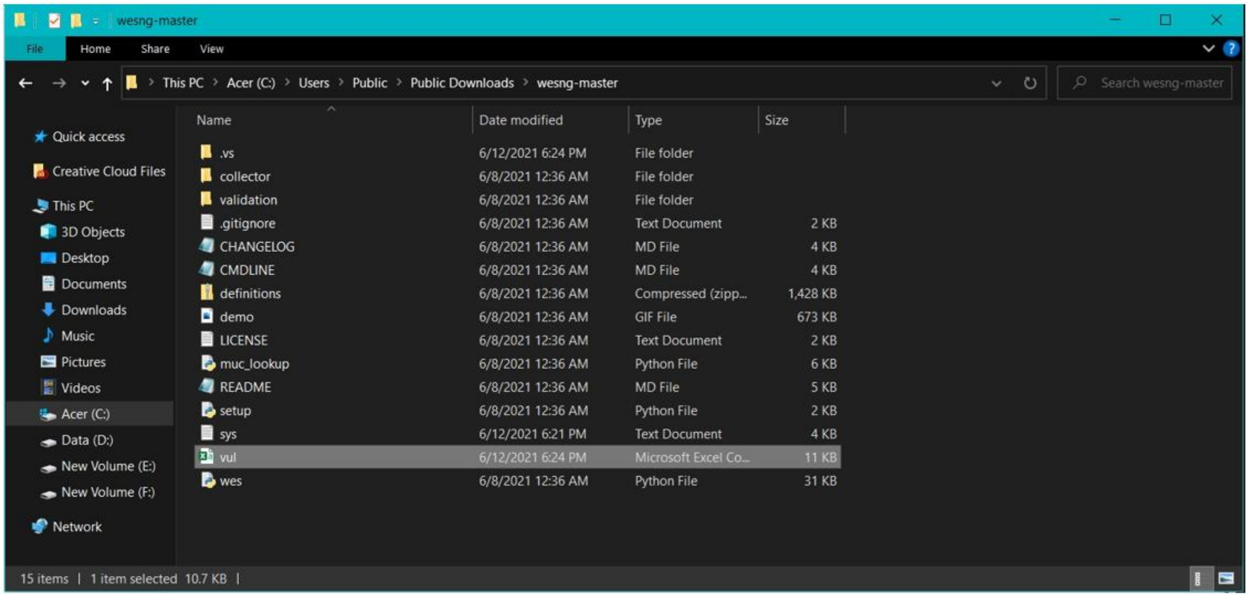


```
C:\Users\Public\Downloads\wesng-master>.\wes.py

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



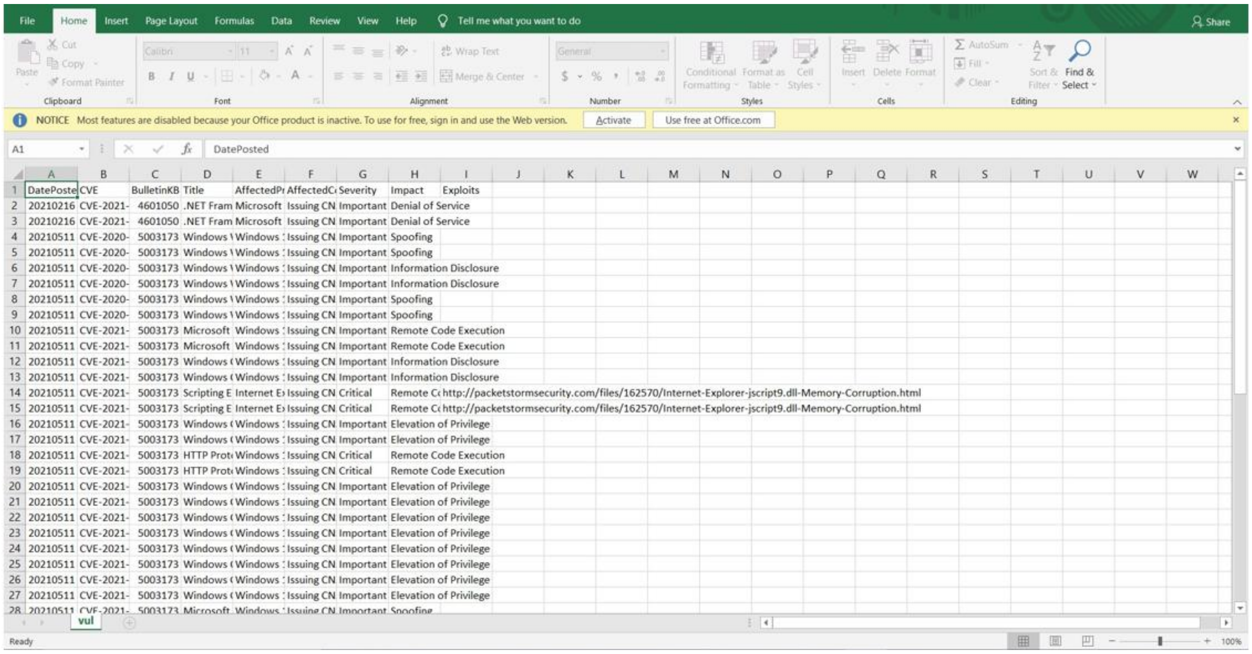
```
  wes.py systeminfo.txt -d

  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>
```

```
Host Name:                 DESKTOP-CE46344
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-10000-00001-AA328
Original Install Date:     10/12/2020, 13:54:00
System Boot Time:          13/06/2021, 10:15:58
System Manufacturer:       Dell Inc.
System Model:              Inspiron 5559
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping 3
GenuineIntel ~1800 Mhz
BIOS Version:              Dell Inc. 1.2.1, 08/06/2016
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-gb;English (United Kingdom)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,084 MB
Available Physical Memory: 3,643 MB
Virtual Memory: Max Size:  9,364 MB
Virtual Memory: Available: 3,186 MB
Virtual Memory: In Use:    6,178 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-CE46344
Hotfix(s):                 9 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4577586
                           [03]: KB4580325
                           [04]: KB4586864
                           [05]: KB4589212
                           [06]: KB4593175
                           [07]: KB4598481
                           [08]: KB5003637
                           [09]: KB5003503
Network Card(s):           4 NIC(s) Installed.
                           [01]: Realtek PCIe FE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
                           [02]: Intel(R) Dual Band Wireless-AC 3160
                                 Connection Name: WiFi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.87.199
                                 IP address(es)
                                 [01]: 192.168.87.57
                                 [02]: fe80::11be:4096:cc23:28cd
                                 [03]:
2409:4070:2e88:86e4:e915:a18a:9cda:ee42
                                 [04]:
2409:4070:2e88:86e4:11be:4096:cc23:28cd
                           [03]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: VirtualBox Host-Only
Network
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::6108:c060:73fd:9792
                           [04]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network
Connection 2
                                 Status:          Media disconnected
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```



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 |



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

A1 DatePosted

	A	B	C	D	E	F	G	H	I
1	DatePoste	CVE	BulletinKB	Title	AffectedP	AffectedC	Severity	Impact	Exploits
2	20210216	CVE-2021-	4601050	.NET Fram	Microsoft	Issuing CN	Important	Denial of Service	
3	20210216	CVE-2021-	4601050	.NET Fram	Microsoft	Issuing CN	Important	Denial of Service	
4	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Spoofing	
5	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Spoofing	
6	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Information Disclosure	
7	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Information Disclosure	
8	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Spoofing	
9	20210511	CVE-2020-	5003173	Windows	Windows	Issuing CN	Important	Spoofing	
10	20210511	CVE-2021-	5003173	Microsoft	Windows	Issuing CN	Important	Remote Code Execution	
11	20210511	CVE-2021-	5003173	Microsoft	Windows	Issuing CN	Important	Remote Code Execution	
12	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Information Disclosure	
13	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Information Disclosure	
14	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
15	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
16	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
17	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
18	20210511	CVE-2021-	5003173	HTTP Prot	Windows	Issuing CN	Critical	Remote Code Execution	
19	20210511	CVE-2021-	5003173	HTTP Prot	Windows	Issuing CN	Critical	Remote Code Execution	
20	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
21	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
22	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
23	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
24	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
25	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
26	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
27	20210511	CVE-2021-	5003173	Windows	Windows	Issuing CN	Important	Elevation of Privilege	
28	20210511	CVE-2021-	5003173	Microsoft	Windows	Issuing CN	Important	Spoofing	