

Name : Debavi Banerjee

Registration Number : 19BCN7014

Subject Code : CSE2010

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

```
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 [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

  Determine vulnerabilities
  wes.py systeminfo.txt

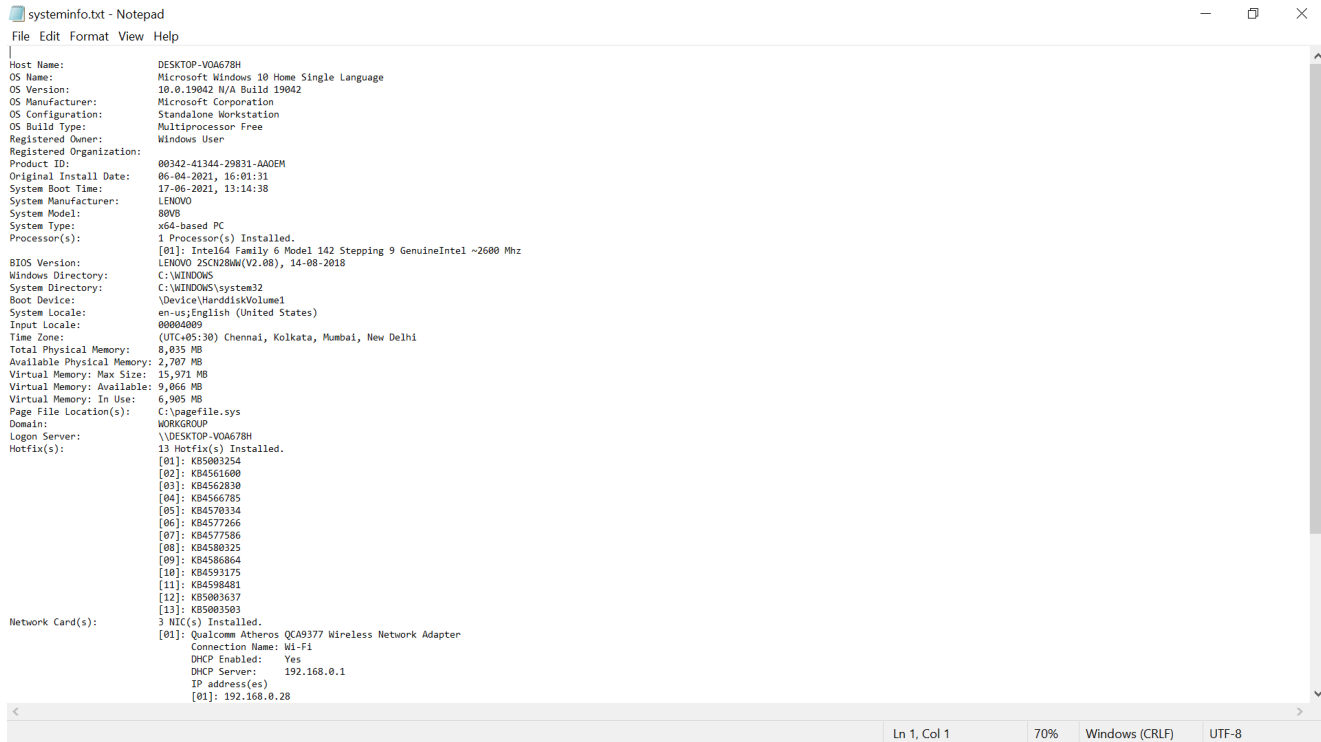
  Determine vulnerabilities using both systeminfo and qfe files
  wes.py systeminfo.txt qfe.txt

  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 vulnerabilities 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 “



```
systeminfo.txt - Notepad
File Edit Format View Help

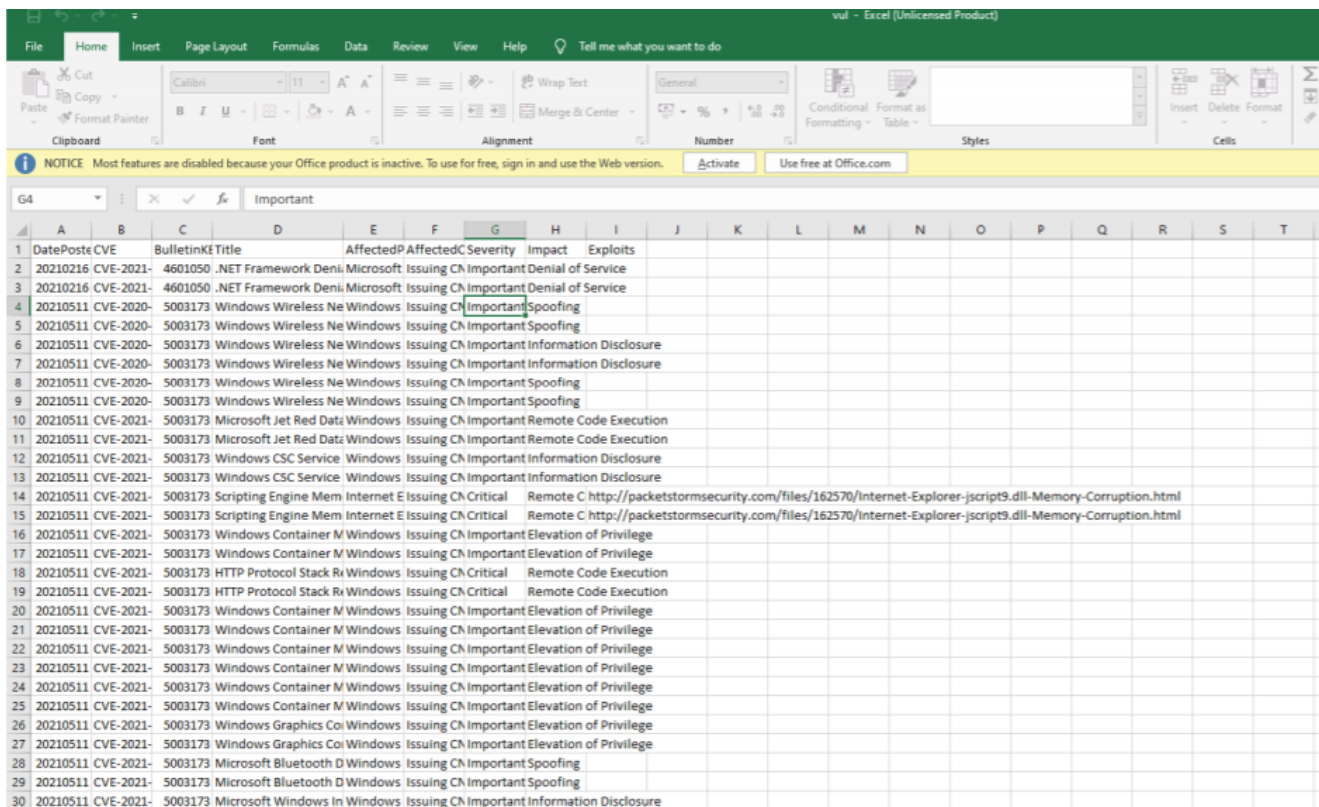
Host Name:                DESKTOP-V04678H
OS Name:                  Microsoft Windows 10 Home Single Language
OS Version:               10.0.19042 N/A Build 19042
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00342-41344-29831-AA0EM
Original Install Date:     06-04-2021, 16:01:31
System Boot Time:          17-06-2021, 13:14:38
System Manufacturer:      LENOVO
System Model:              80V8
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 9 GenuineIntel ~2600 Mhz
BIOS Version:              LENOVO 25CN28MM(V2.08), 14-08-2018
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              08040009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,035 MB
Available Physical Memory: 2,707 MB
Virtual Memory: Max Size:  15,971 MB
Virtual Memory: Available: 9,066 MB
Virtual Memory: In Use:    6,905 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \DESKTOP-V04678H
Hotfix(s):                 13 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4561600
                           [03]: KB4562838
                           [04]: KB4566785
                           [05]: KB4570334
                           [06]: KB4577266
                           [07]: KB4577586
                           [08]: KB4580325
                           [09]: KB4586864
                           [10]: KB4593175
                           [11]: KB4598481
                           [12]: KB5003637
                           [13]: KB5003903
Network Card(s):           3 NIC(s) Installed.
                           [01]: Qualcomm Atheros QCA9377 Wireless Network Adapter
                               Connection Name: Wi-Fi
                               DHCP Enabled:   Yes
                               DHCP Server:    192.168.0.1
                               IP Address(es)  [01]: 192.168.0.28
```

Ln 1, Col 1 70% Windows (CRLF) UTF-8

3) Now look for vulnerabilities using your last txt file output “ wes.py systeminfo.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, 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.
```

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



Date	CVE	Bulletin	Title	Affected Product	Affected Severity	Impact	Exploits
20210216	CVE-2021-4601050	.NET Framework Deni	Microsoft	Issuing CN Important	Denial of Service		
20210216	CVE-2021-4601050	.NET Framework Deni	Microsoft	Issuing CN Important	Denial of Service		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Information Disclosure		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Information Disclosure		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2020-5003173	Windows Wireless Ne	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2020-5003173	Microsoft Jet Red Dat	Windows	Issuing CN Important	Remote Code Execution		
20210511	CVE-2021-5003173	Microsoft Jet Red Dat	Windows	Issuing CN Important	Remote Code Execution		
20210511	CVE-2021-5003173	Windows CSC Service	Windows	Issuing CN Important	Information Disclosure		
20210511	CVE-2021-5003173	Windows CSC Service	Windows	Issuing CN Important	Information Disclosure		
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	
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	
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	HTTP Protocol Stack R	Windows	Issuing CN Critical	Remote Code Execution		
20210511	CVE-2021-5003173	HTTP Protocol Stack R	Windows	Issuing CN Critical	Remote Code Execution		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Container M	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Graphics Coi	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Windows Graphics Coi	Windows	Issuing CN Important	Elevation of Privilege		
20210511	CVE-2021-5003173	Microsoft Bluetooth D	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2021-5003173	Microsoft Bluetooth D	Windows	Issuing CN Important	Spoofing		
20210511	CVE-2021-5003173	Microsoft Windows In	Windows	Issuing CN Important	Information Disclosure		