Ex.No: 13
Date: 07-05-2021

Name: Ganga Suresh Kumar Nair
Reg.No: 18BCN7014

Secure Coding

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.**
- **Submit the auto-generated report using pwndoc.**

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

```
C:\Users\ganga>cd C:\Users\ganga\Downloads\wesng-master\wesng-master

C:\Users\ganga\Downloads\wesng-master\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]
```

```
C:\Users\ganga>cd C:\Users\ganga\Downloads\wesng-master\wesng-master

C:\Users\ganga\Downloads\wesng-master\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
```

2) Output your system info with this command

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

sys - Notepad

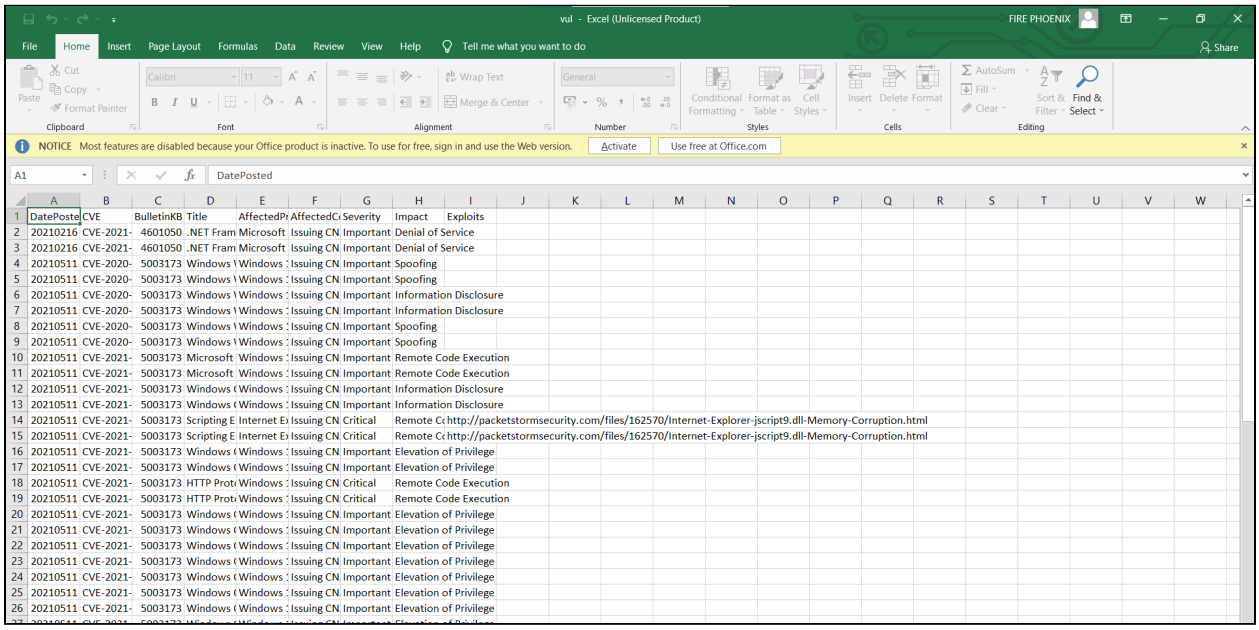
File Edit Format View Help

```
Host Name:                 LAPTOP-VMTQ6TRH
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          gangasuresh2000@gmail.com
Registered Organization:   HP
Product ID:                00325-81260-68063-AAOEM
Original Install Date:     23-04-2021, 22:32:43
System Boot Time:          11-06-2021, 09:19:05
System Manufacturer:       HP
System Model:              HP Pavilion Gaming Laptop 15-cx0xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2208 Mhz
BIOS Version:              Insyde F.12, 11-10-2018
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-gb;English (United Kingdom)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,272 MB
Available Physical Memory: 8,046 MB
Virtual Memory: Max Size:  18,704 MB
Virtual Memory: Available: 6,887 MB
Virtual Memory: In Use:    11,817 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-VMTQ6TRH
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB5003254
```

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

```
C:\Users\ganga\Downloads\wesng-master\wesng-master>python wes.py sys.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 (7): KB5003254, KB4562830, KB4577586, KB4580325, KB5001679, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
[+] Writing 52 results to vul.csv
```

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



vul - Excel (Unlicensed Product) — FIRE PHOENIX

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do — Share

Paste Cut Copy Format Painter | Calibri 11 | Wrap Text Merge & Center | General | Conditional Formatting Format as Table Cell Styles | Insert Delete Format | AutoSum Fill Clear | Sort & Filter Find & Select

Clipboard Font Alignment Number Styles Cells Editing

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	DatePoste	CVE	BulletinKB	Title	AffectedPr	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 1	Issuing CN	Important	Spoofing															
5	20210511	CVE-2020-	5003173	Windows \	Windows 1	Issuing CN	Important	Spoofing															
6	20210511	CVE-2020-	5003173	Windows \	Windows 1	Issuing CN	Important	Information Disclosure															
7	20210511	CVE-2020-	5003173	Windows \	Windows 1	Issuing CN	Important	Information Disclosure															
8	20210511	CVE-2020-	5003173	Windows \	Windows 1	Issuing CN	Important	Spoofing															
9	20210511	CVE-2020-	5003173	Windows \	Windows 1	Issuing CN	Important	Spoofing															
10	20210511	CVE-2021-	5003173	Microsoft	Windows 1	Issuing CN	Important	Remote Code Execution															
11	20210511	CVE-2021-	5003173	Microsoft	Windows 1	Issuing CN	Important	Remote Code Execution															
12	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Information Disclosure															
13	20210511	CVE-2021-	5003173	Windows (	Windows 1	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 1	Issuing CN	Important	Elevation of Privilege															
17	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
18	20210511	CVE-2021-	5003173	HTTP Prot	Windows 1	Issuing CN	Critical	Remote Code Execution															
19	20210511	CVE-2021-	5003173	HTTP Prot	Windows 1	Issuing CN	Critical	Remote Code Execution															
20	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
21	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
22	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
23	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
24	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
25	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															
26	20210511	CVE-2021-	5003173	Windows (	Windows 1	Issuing CN	Important	Elevation of Privilege															