

## LAB-13

# Secure Coding

## Lab experiment – Automated Vulnerability Analysis and Patch Management

### Experiment and Analysis

Name: A.Shreejay

Reg.No: 18BCN7040

- 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 [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
```

```
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 supersedece against Microsoft's online Update Catalog
wes.py systeminfo.txt --muc-lookup

Download latest version of WES-MG
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
Virtual Memory: In Use:    9,688 MB

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

