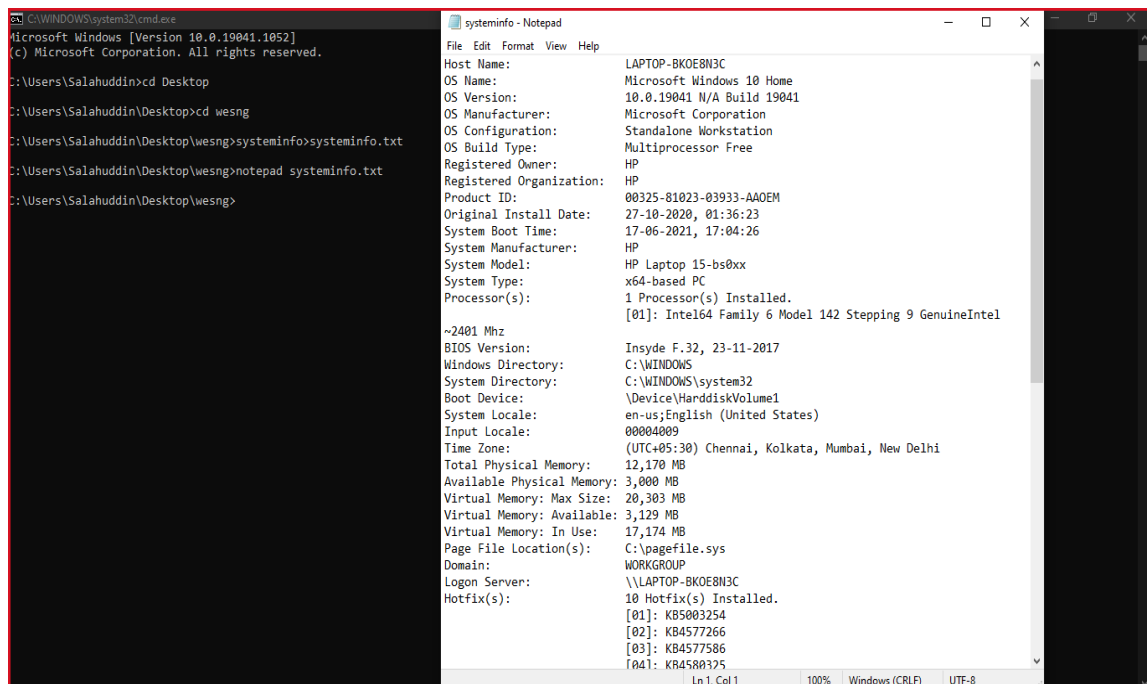


SECURE CODING LAB ASSIGNMENT 13

Mohammad Abraar
19BCN7024

Creating systeminfo.txt file



The screenshot shows a Windows command prompt window on the left and a Notepad window on the right. The command prompt displays the following commands and their outputs:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Salahuddin>cd Desktop
C:\Users\Salahuddin\Desktop>cd wesng
C:\Users\Salahuddin\Desktop\wesng>systeminfo>systeminfo.txt
C:\Users\Salahuddin\Desktop\wesng>notepad systeminfo.txt
C:\Users\Salahuddin\Desktop\wesng>
```

The Notepad window, titled "systeminfo - Notepad", displays the output of the systeminfo command:

```
File Edit Format View Help
Host Name: LAPTOP-BKOE8N3C
OS Name: Microsoft Windows 10 Home
OS Version: 10.0.19041 N/A Build 19041
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: HP
Registered Organization: HP
Product ID: 00325-81023-03933-AAOEM
Original Install Date: 27-10-2020, 01:36:23
System Boot Time: 17-06-2021, 17:04:26
System Manufacturer: HP
System Model: HP Laptop 15-bs0xx
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 142 Stepping 9 GenuineIntel
~2401 Mhz
BIOS Version: Insyde F.32, 23-11-2017
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: 00004009
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 12,170 MB
Available Physical Memory: 3,000 MB
Virtual Memory: Max Size: 20,303 MB
Virtual Memory: Available: 3,129 MB
Virtual Memory: In Use: 17,174 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\LAPTOP-BKOE8N3C
Hotfix(s): 10 Hotfix(s) Installed.
[01]: KB5003254
[02]: KB4577266
[03]: KB4577586
[04]: KB4580325
```

Wes

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Salahuddin>cd Desktop

C:\Users\Salahuddin\Desktop>cd wesng

C:\Users\Salahuddin\Desktop\wesng>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
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 of the most recent KB installed
wes.py systeminfo.txt --usekbdate
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
```

Finding vulnerabilities:

```

C:\WINDOWS\system32\cmd.exe
C:\Users\Salahuddin\Desktop>wesng>wes.py systeminfo.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: 19041
  - Version: 20H2
  - Architecture: x64-based
  - Installed hotfixes (10): KB5003254, KB4577266, KB4577586, KB4580325, KB4586864, KB4593175, KB4598481, KB5001679, KB5003637, KB5003503
[+] Loading definitions
  - Creation date of definitions: 20210621
[+] Determining missing patches
[+] Found vulnerabilities
[+] Writing 5 results to vul.csv
[+] Missing patches: 3
  - KB4569745: patches 2 vulnerabilities
  - KB4601050: patches 2 vulnerabilities
  - KB4566785: patches 1 vulnerability
[+] KB with the most recent release date
  - ID: KB4601050
  - Release date: 20210216
[+] Done. Saved 5 of the 5 vulnerabilities found.

```

Patching:

```
C:\Users\Salahuddin\Desktop>wesng>wes.py -e systeminfo.txt --hide "Internet Explorer" Edge
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 2004 for x64-based Systems
    - Generation: 10
    - Build: 19041
    - Version: 2004
    - Architecture: x64-based
    - Installed hotfixes (10): KB5003254, KB4577266, KB4577586, KB4580325, KB4586864, KB4593175, KB4598481, KB5001679, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210621
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found
```

All the vulnerabilities are stored in vul.csv:

[illegible]