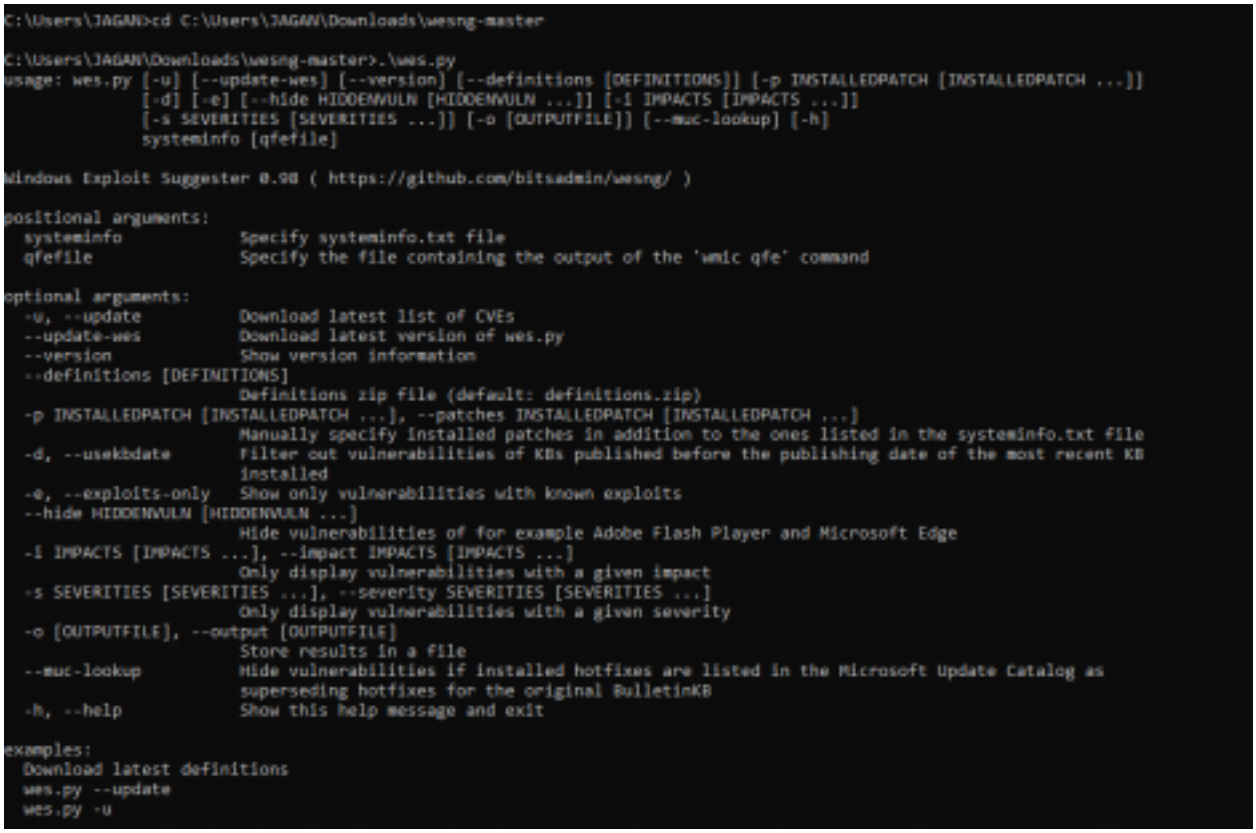
Secure Coding Cse 2010
Lab 13

K. Charan teja
18BCN7141



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

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

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 vulnerabilies 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
```

C:\Users\JAGAN\Downloads\wesng-master>systeminfo > systeminfo.txt

systeminfo.txt [C:\] - Notepad2-mod (Administrator)

File Edit View Settings ?

```
Host Name:                 DESKTOP-RUBIUJ4
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.16299 N/A Build 16299
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00328-90000-00000-AAOEM
Original Install Date:     24/10/2017, 14:59:36
System Boot Time:          02/03/2019, 11:00:57
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping 3 GenuineIntel ~2496 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.9694812.B64.1808210100, 21/08/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
```