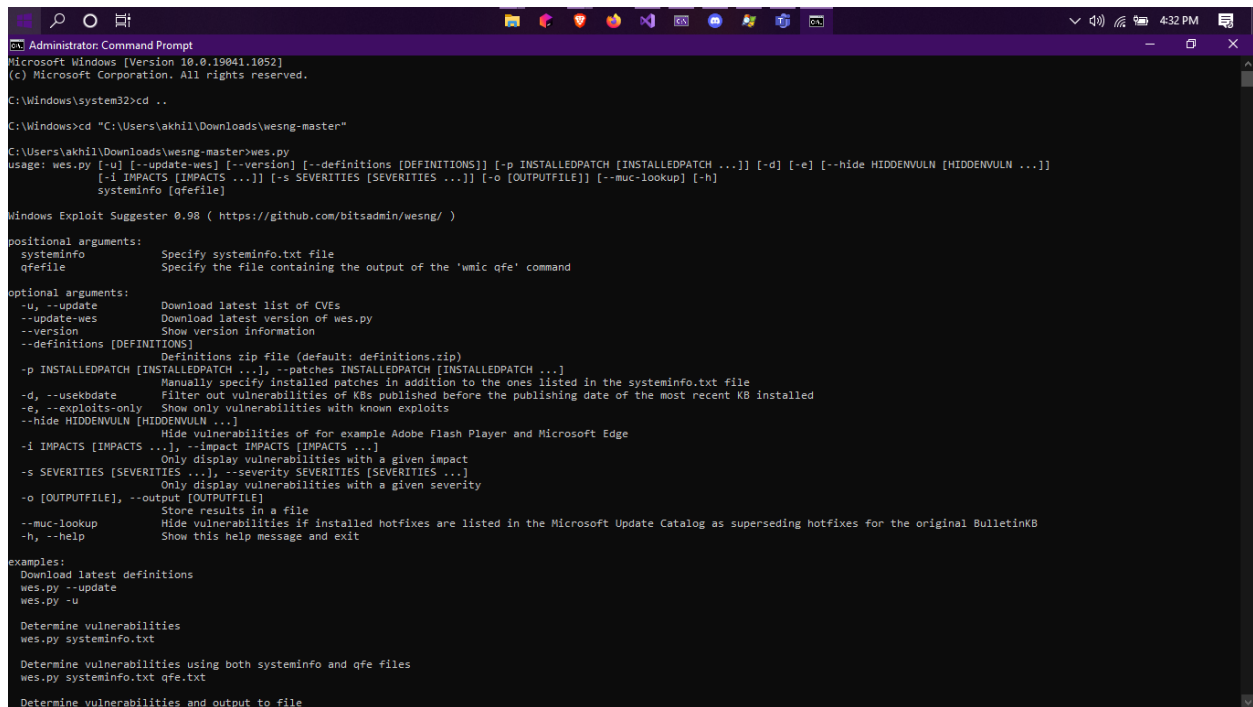


NAME: A KRISHNA AKHIL  
REG NO: 18BCE7076  
SECURE CODING LAB L39+L40  
*Guided By: Prof. Sibi Chakravarthy*  
**[LAB 13]**

## Windows Exploit Suggester-Next Generation (WES-NG)

ES-NG is a tool based on the output of Windows systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between XP and 10, including the Windows Server counterparts is supported.

→ **wes.py**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
C:\Windows>cd "C:\Users\akhil\Downloads\wesng-master"
C:\Users\akhil\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

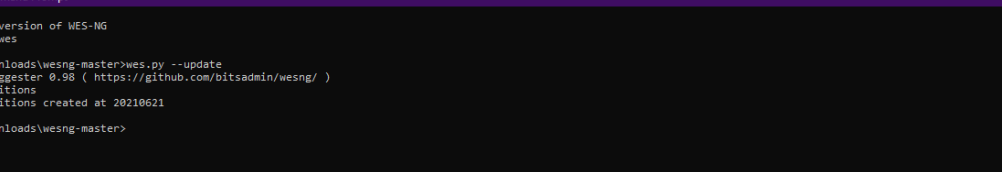
examples:
  Download latest definitions
  wes.py --update
  wes.py -u

  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 --update**



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command prompt displays the following text:

```
Download latest version of WES-NG  
wes.py --update-wes  
  
C:\Users\akhill\Downloads\wesng-master>wes.py --update  
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )  
[*] Updating definitions  
[*] Obtained definitions created at 20210621  
  
C:\Users\akhill\Downloads\wesng-master>
```

## Export SystemInfo into a txt file

→ **systeminfo > systeminfo.txt**

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

systeminfo - Notepad

File Edit Format View Help

```

Host Name:                DESKTOP-5HT6BMD
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:         akhilsproject@gmail.com
Registered Organization:
Product ID:               [REDACTED]
Original Install Date:    10/8/2020, 4:24:59 AM
System Boot Time:         6/23/2021, 11:55:03 PM
System Manufacturer:      TOSHIBA
System Model:              Satellite L55-B
System Type:              x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~1700 Mhz
BIOS Version:              INSYDE Corp. 2.00, 12/11/2014
Windows Directory:        C:\Windows
System Directory:         C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,112 MB
Available Physical Memory: 1,353 MB
Virtual Memory: Max Size: 13,744 MB
Virtual Memory: Available: 4,794 MB
Virtual Memory: In Use:    8,950 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-5HT6BMD
Hotfix(s):                 13 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4561600
                           [03]: KB4570334

```

Ln1 Col1 100% Windows (CRLF) UTF-8

```
→wes.py systeminfo.txt --output vulns.cvs
```

```
Administrator: Command Prompt

C:\Users\akhil\Downloads\wesng-master>wes.py systeminfo.txt --output vulns.csv
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 (13): KB5003254, KB4561600, KB4570334, KB4576754, KB4577266, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
+ Loading definitions
  - Creation date of definitions: 20210621
+ Determining missing patches
+ Found vulnerabilities
+ Writing 5 results to vulns.csv
+ Missing patches: 3
  - KB4589745: 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.

C:\Users\akhil\Downloads\wesng-master>
```

vulns.csv - LibreOffice Calc

File Edit View Insert Format Styles Sheet Data Tools Window Help

LibreOffice Calc

fx Σ = DatePosted

A	B	C	D	E	F	G	H	I	J	K
1	DatePosted	CVE	BulletinKB Title	AffectedProduct	AffectedComponent	Severity	Impact	Exploits		
2	20200714	CVE-2020-1346	4566785 Windows Modules Installer Elevation of Privilege Vulnerability	Windows 10 Version 2004 for x64-based Systems	Issuing CNA	Important	Elevation of Privilege			
3	20200811	CVE-2020-1476	4569745 ASP.NET and .NET Elevation of Privilege Vulnerability	Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 2004 for x64-based Systems	Issuing CNA	Important	Elevation of Privilege			
4	20200811	CVE-2020-1046	4569745 .NET Framework Remote Code Execution Vulnerability	Microsoft .NET Framework 3.5 on Windows 10 Version 2004 for x64-based Systems	Issuing CNA	Critical	Remote Code Execution			
5	20210216	CVE-2021-2411	4601050 .NET Framework Denial of Service Vulnerability	Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems	Issuing CNA	Important	Denial of Service			
6	20210216	CVE-2021-2411	4601050 .NET Framework Denial of Service Vulnerability	Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems	Issuing CNA	Important	Denial of Service			
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
35										
36										
37										
38										
39										

Sheet 1 of 1 | Default | English (USA) | Average: Sum: 0 | 75%