VIT-AP
UNIVERSITY

Name : Ratna Rajiv Mulpuri
Reg.No : 18BCN7089

LAB 13

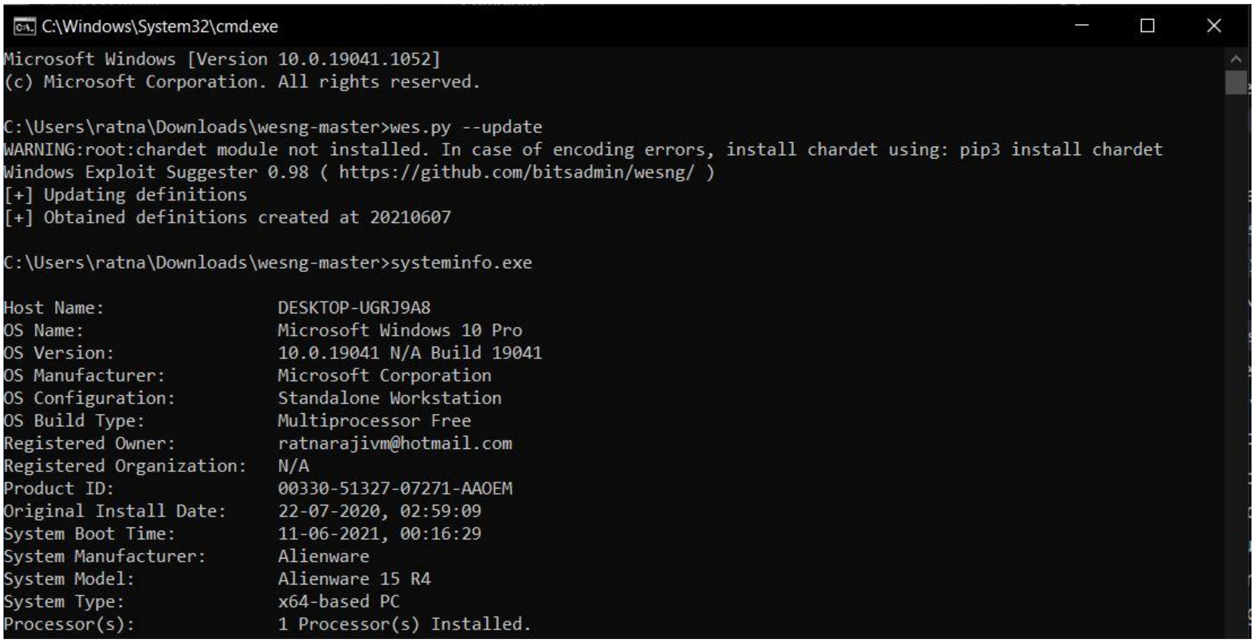
Windows exploit suggester

WES-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 Windows XP and Windows 10, including their Windows Server counterparts, is supported.

Usage :

1.Obtain the latest database of vulnerabilities by executing the command wes.py --update.
2.Use Windows' built-in systeminfo.exe tool to obtain the system information of the local system, or from a remote system using systeminfo.exe /S MyRemoteHost, and redirect this to a file: systeminfo > systeminfo.txt
3.Execute WES-NG with the systeminfo.txt output file as the parameter: wes.py systeminfo.txt. WES-NG then uses the database to determine which patches are applicable to the system and to which vulnerabilities are currently exposed, including exploits if available.

Double click on the setup.py to setup windows exploit suggester:

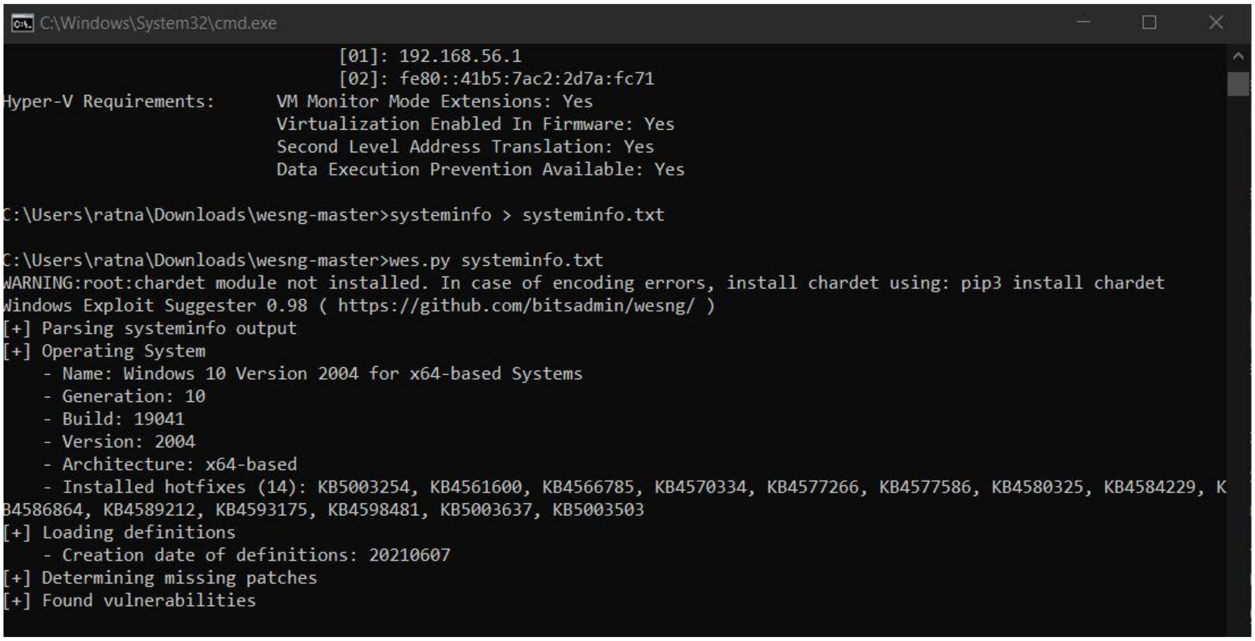


```
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ratna\Downloads\wesng-master>wes.py --update
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/ )
[+] Updating definitions
[+] Obtained definitions created at 20210607

C:\Users\ratna\Downloads\wesng-master>systeminfo.exe

Host Name:                 DESKTOP-UGRJ9A8
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          ratnarajivm@hotmail.com
Registered Organization:   N/A
Product ID:                00330-51327-07271-AAOEM
Original Install Date:     22-07-2020, 02:59:09
System Boot Time:          11-06-2021, 00:16:29
System Manufacturer:       Alienware
System Model:              Alienware 15 R4
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
```

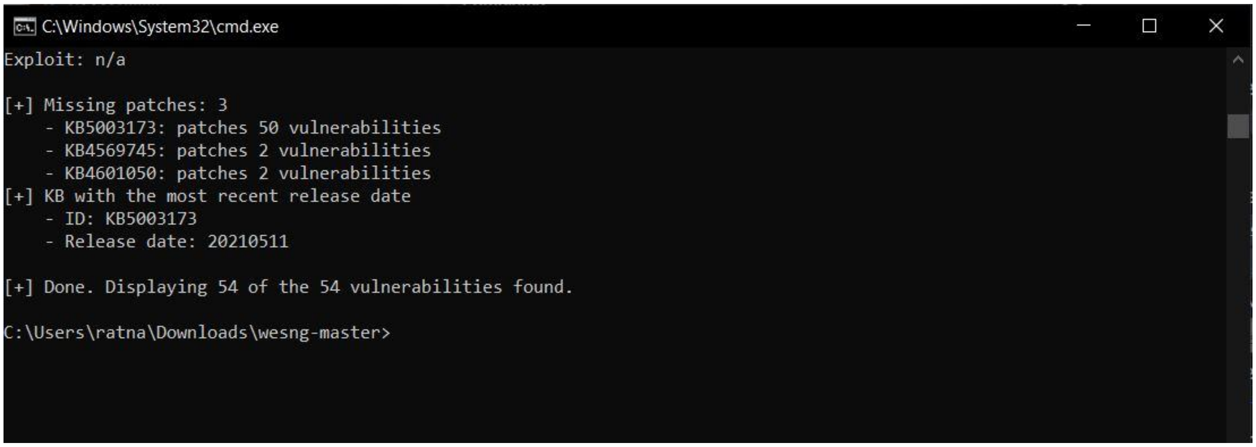


```
                                 [01]: 192.168.56.1
                                 [02]: fe80::41b5:7ac2:2d7a:fc71
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes

:\Users\ratna\Downloads\wesng-master>systeminfo > systeminfo.txt

:\Users\ratna\Downloads\wesng-master>wes.py systeminfo.txt
ARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
indows 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 (14): KB5003254, KB4561600, KB4566785, KB4570334, KB4577266, KB4577586, KB4580325, KB4584229, K
B4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
```

Pipe the systeminfo as a txt file to the wes.py and it will list all the vulnerabilities in the system. At last it will give you all the patches that are required to patch the vulnerabilities as below:



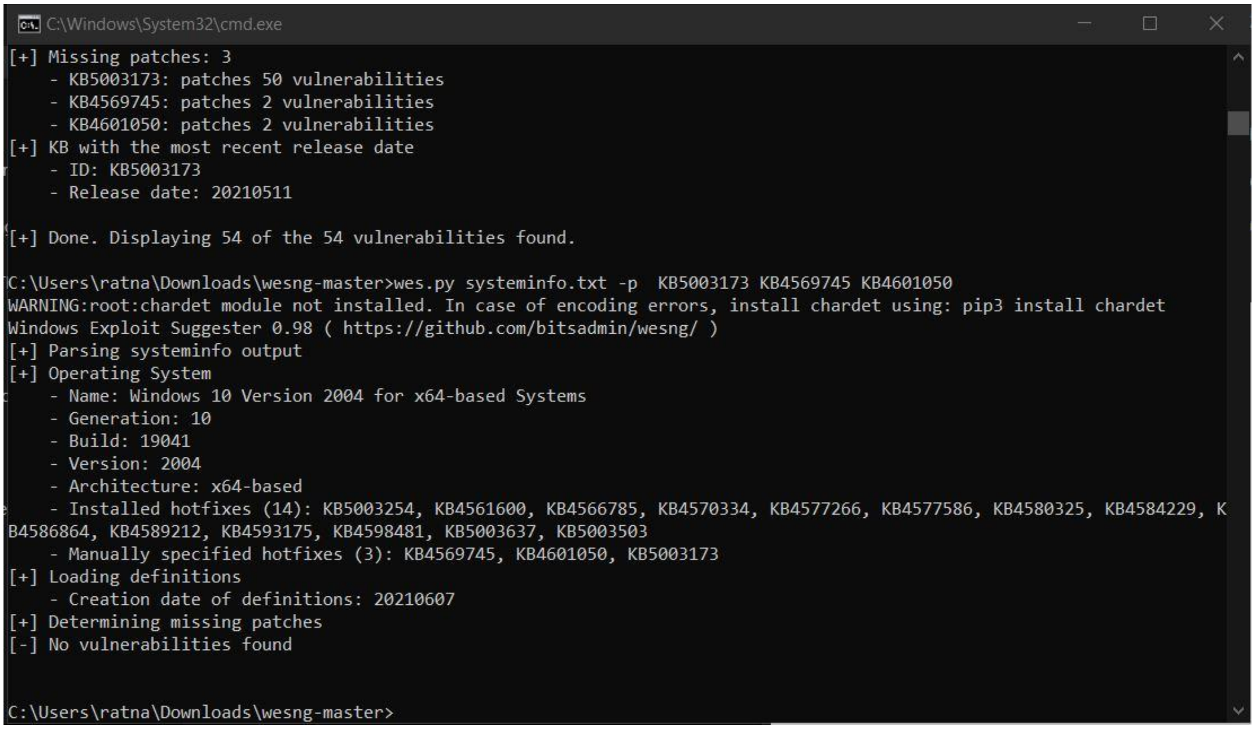
```
Exploit: n/a

[+] Missing patches: 3
    - KB5003173: patches 50 vulnerabilities
    - KB4569745: patches 2 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 54 of the 54 vulnerabilities found.

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

Fixing Vulnerabilities:



```
[+] Missing patches: 3
    - KB5003173: patches 50 vulnerabilities
    - KB4569745: patches 2 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 54 of the 54 vulnerabilities found.

C:\Users\ratna\Downloads\wesng-master>wes.py systeminfo.txt -p  KB5003173 KB4569745 KB4601050
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 (14): KB5003254, KB4561600, KB4566785, KB4570334, KB4577266, KB4577586, KB4580325, KB4584229, K
B4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
    - Manually specified hotfixes (3): KB4569745, KB4601050, KB5003173
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[-] No vulnerabilities found


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