

CN LAB - 13

G. Srineha
19BCN7244

TOPIC-Automated Vulnerability Analysis and Patch Management Experiment and Analysis

- **Deploy Windows Exploit Suggester - Next Generation (WES-NG)**
- **Obtain the system information and check for any reported**
- **vulnerabilities. If any vulnerabilities reported, apply patch and make your system**
- **safe. Submit the auto-generated report using pwndoc.**
- **At first copy all system info into text file.**

Windows exploit suggester:

This is a tool that helps you to identify the vulnerability in your naïve windows system.

Follow the link in github to download the files required.....

<https://github.com/bitsadmin/wesng>

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

Now open command prompt do as follows

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

C:\Users\SRINEHA\Downloads\wesng-master>python wes.py --update
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210530

C:\Users\SRINEHA\Downloads\wesng-master>python wes.py systeminfo_sc_demo.txt
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
```

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.

```
[+] 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. Displaying 5 of the 5 vulnerabilities found.
```

Fix your vulnerabilities.

```
C:\Users\SRINEHA\Downloads\wesng-master>python wes.py systeminfo_sc_demo.txt -p KB4569745 KB4566785 KB4601050
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 (16): KB4601554, KB4534170, KB4537759, KB4542335, KB4545706, KB4570334, KB4577266, KB4577586,
KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5001679, KB5003173, KB5003242
  - Manually specified hotfixes (3): KB4566785, KB4601050, KB4569745
[+] Loading definitions
  - Creation date of definitions: 20210530
[+] Determining missing patches
[-] No vulnerabilities found
```

```
C:\Users\SRINEHA\Downloads\wesng-master>python
Windows Exploit Suggester 0.98 ( https://github
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 10 Version 2004 for x64-ba
  - Generation: 10
  - Build: 19041
  - Version: 2004
  - Architecture: x64-based
  - Installed hotfixes (16): KB4601554, KB45
B4580325, KB4586864, KB4589212, KB4593175, KB4
  - Manually specified hotfixes (3): KB45667
[+] Loading definitions
  - Creation date of definitions: 20210530
[+] Determining missing patches
[-] No vulnerabilities found
```

