SECURE CODINGLAB REPORT

Lab : WINDOWS EXPLOIT SUGGESTER

Devi Jagannadh Kotha

28-04-2021

18BCN7079

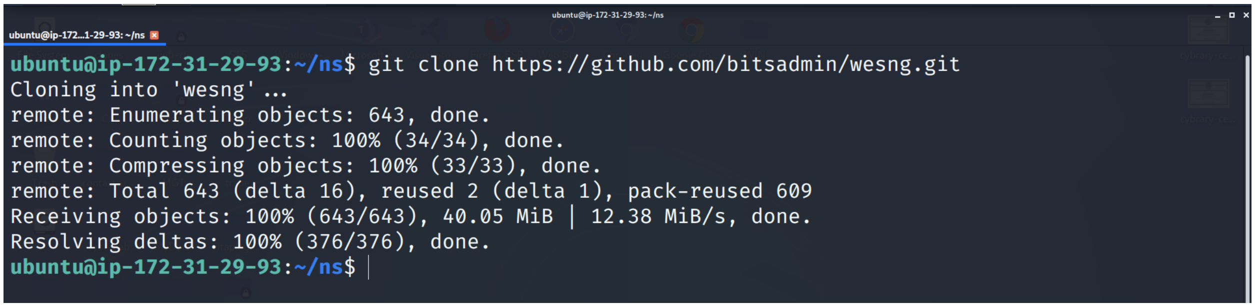
INTRODUCTION

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.

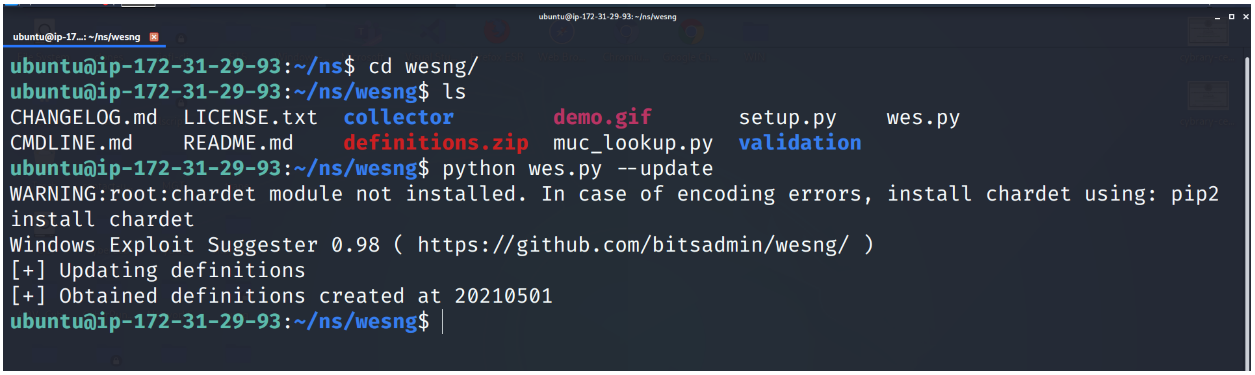
INSTALLATION

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.
4. As the data provided by Microsoft's MSRC feed is frequently incomplete and false positives are reported by wes.py, @DominicBreuker contributed the --muc-lookup parameter to validate identified missing patches against Microsoft's Update Catalog. Additionally, make sure to check the Eliminating false positives page at the Wiki on how to interpret the results. For an overview of all available parameters, check CMDLINE.md.

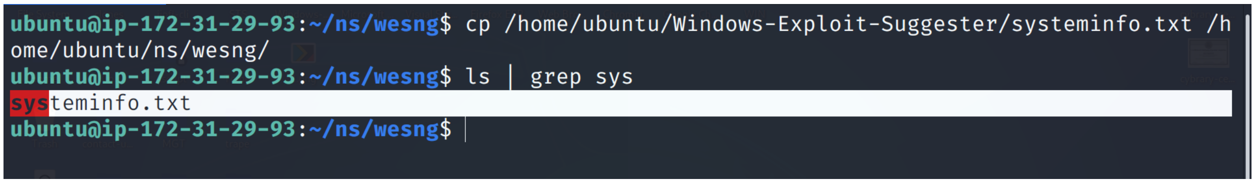
EXECUTION



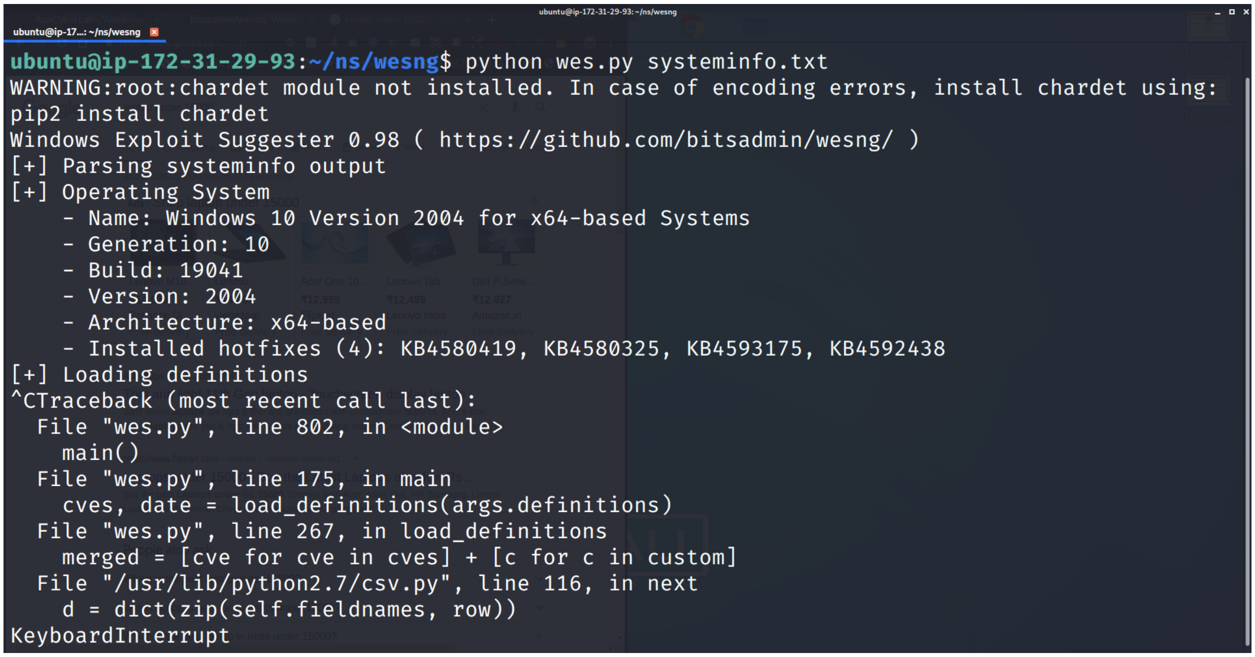
```
ubuntu@ip-172-31-29-93:~/ns$ git clone https://github.com/bitsadmin/wesng.git
Cloning into 'wesng'...
remote: Enumerating objects: 643, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 643 (delta 16), reused 2 (delta 1), pack-reused 609
Receiving objects: 100% (643/643), 40.05 MiB | 12.38 MiB/s, done.
Resolving deltas: 100% (376/376), done.
ubuntu@ip-172-31-29-93:~/ns$
```


ubuntu@ip-172-31-29-93: ~/ns/wesng
ubuntu@ip-17...: ~/ns/wesng

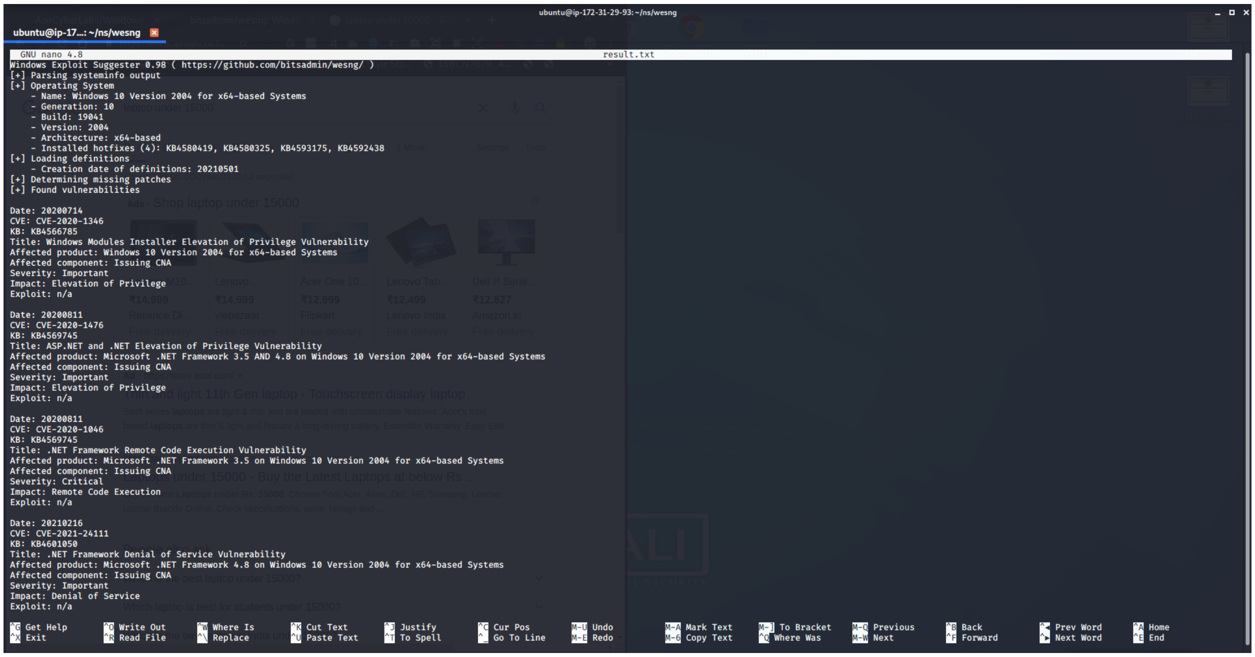
```
ubuntu@ip-172-31-29-93:~/ns$ cd wesng/
ubuntu@ip-172-31-29-93:~/ns/wesng$ ls
CHANGELOG.md  LICENSE.txt  collector        demo.gif       setup.py    wes.py
CMDLINE.md    README.md    definitions.zip  muc_lookup.py  validation
ubuntu@ip-172-31-29-93:~/ns/wesng$ python wes.py --update
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip2
install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210501
ubuntu@ip-172-31-29-93:~/ns/wesng$
```



```
ubuntu@ip-172-31-29-93:~/ns/wesng$ cp /home/ubuntu/Windows-Exploit-Suggester/systeminfo.txt /h
ome/ubuntu/ns/wesng/
ubuntu@ip-172-31-29-93:~/ns/wesng$ ls | grep sys
systeminfo.txt
ubuntu@ip-172-31-29-93:~/ns/wesng$
```


ubuntu@ip-172-31-29-93: ~/ns/wesng
ubuntu@ip-17...: ~/ns/wesng

```
ubuntu@ip-172-31-29-93:~/ns/wesng$ python wes.py systeminfo.txt
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using:
pip2 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 (4): KB4580419, KB4580325, KB4593175, KB4592438
[+] Loading definitions
^CTraceback (most recent call last):
  File "wes.py", line 802, in <module>
    main()
  File "wes.py", line 175, in main
    cves, date = load_definitions(args.definitions)
  File "wes.py", line 267, in load_definitions
    merged = [cve for cve in cves] + [c for c in custom]
  File "/usr/lib/python2.7/csv.py", line 116, in next
    d = dict(zip(self.fieldnames, row))
KeyboardInterrupt
```


ubuntu@ip-172-31-29-93: ~/ns/wesng
ubuntu@ip-17...: ~/ns/wesng
GNU nano 4.8
result.txt

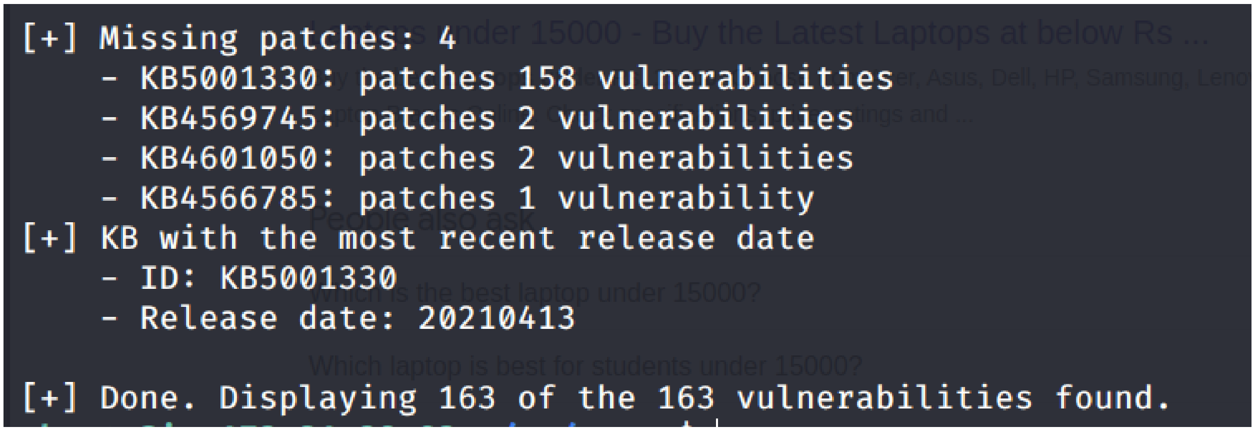
```
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 2004 for x64-based Systems
    - Generation: 10
    - Build: 19041
    - Version: 2004
    - Architecture: x64-based
    - Installed hotfixes (4): KB4580419, KB4580325, KB4593175, KB4592438
[+] Loading definitions
    - Creation date of definitions: 20210501
[+] Determining missing patches
[+] Found vulnerabilities

Date: 20200714
CVE: CVE-2020-1346
KB: KB4566785
Title: Windows Modules Installer Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20200811
CVE: CVE-2020-1476
KB: KB4569745
Title: ASP.NET and .NET Elevation of Privilege Vulnerability
Affected product: Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20200811
CVE: CVE-2020-1046
KB: KB4569745
Title: .NET Framework Remote Code Execution Vulnerability
Affected product: Microsoft .NET Framework 3.5 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

Date: 20210216
CVE: CVE-2021-24111
KB: KB4601050
Title: .NET Framework Denial of Service Vulnerability
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 2004 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a
```



```
[+] Missing patches: 4
    - KB5001330: patches 158 vulnerabilities
    - KB4569745: patches 2 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
    - KB4566785: patches 1 vulnerability
[+] KB with the most recent release date
    - ID: KB5001330
    - Release date: 20210413

[+] Done. Displaying 163 of the 163 vulnerabilities found.
```

REFERENCES

1. https://github.com/bitsadmin/wesng