CSE-2010

Secure Coding(L23 + L24)

Lab - 13

Name :- MD Shafiq Ahmed

Reg no :- 18BCN7122

- **Deploy Windows Exploit Suggester - Next Generation (WES-NG)**

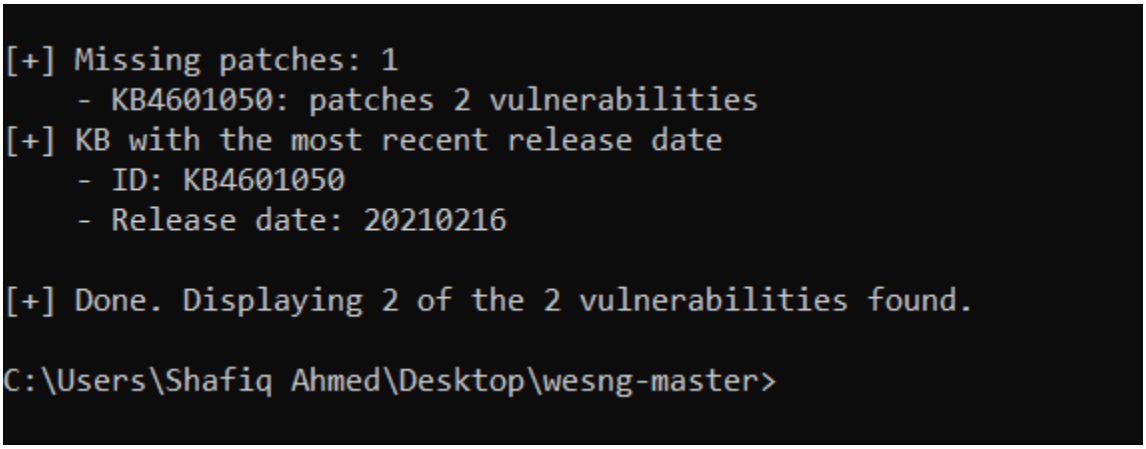
```
C:\Users\Shafiq Ahmed>cd Desktop

C:\Users\Shafiq Ahmed\Desktop>cd wesng-master

C:\Users\Shafiq Ahmed\Desktop\wesng-master>systeminfo > 18BCN7122_sysinfo.txt

C:\Users\Shafiq Ahmed\Desktop\wesng-master>python wes.py
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
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
```

- **Obtain the system information and check for any reported vulnerabilities.**

```
C:\Users\Shafiq Ahmed\Desktop\wesng-master>python 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 20210530
```

```
C:\Users\Shafiq Ahmed\Desktop\wesng-master>python wes.py 18BCN7122_sysinfo.txt
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 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19042
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (16): KB4601554, KB4560366, KB4561600, KB4562830, KB4566785, KB4570334, KB4577266, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5001679, KB5003173, KB5003242
[+] Loading definitions
    - Creation date of definitions: 20210530
[+] Determining missing patches
[+] Found vulnerabilities

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 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
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 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Denial of Service
Exploit: n/a

[+] Missing patches: 1
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB4601050
    - Release date: 20210216

[+] Done. Displaying 2 of the 2 vulnerabilities found.

C:\Users\Shafiq Ahmed\Desktop\wesng-master>
```

- **If any vulnerabilities are reported, apply patches and make your system safe.**



- **For CVE 2021-2411 no patch is available for my windows 10 version 21H1**

Feb 9, 2021	Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2	Windows Server 2016 (Server Core installation)	Denial of Service	Important	4601318	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2	Windows 10 Version 1607 for 32-bit Systems	Denial of Service	Important	4601318	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 20H2 for x64-based Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 2004 for 32-bit Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 2004 for ARM64-based Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 20H2 for ARM64-based Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows Server, version 20H2 (Server Core Installation)	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 2004 for x64-based Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows Server, version 2004 (Server Core installation)	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.8	Windows 10 Version 20H2 for 32-bit Systems	Denial of Service	Important	4601050	Security Update	CVE-2021-24111
Feb 9, 2021	Microsoft .NET Framework 4.6	Windows Server 2008 for x64-based Systems Service Pack 2	Denial of Service	Important	4603005 4602961	Monthly Rollup Security Only	CVE-2021-24111