

Secure Coding Lab - 13

Name: Rushik kumar Avula

Reg. No: 18BCN7008

Note : this is done in virtual machine.

After installing the wesng from github.

```
C:\Users\IEUser\Downloads\wesng-master\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 20210607

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

```
C:\Users\IEUser\Downloads\wesng-master\wesng-master>python wes.py 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 1809 for x64-based Systems
- Generation: 10
- Build: 17763
- Version: 1809
- Architecture: x64-based
- Installed hotfixes (13): KB4580979, KB4462930, KB4465065, KB4470788, KB4480056, KB4486153, KB4489907, KB4561600, KB4566424, KB4580325, KB4587735, KB5003243, KB4592440
[+] Loading definitions
- Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities

Date: 20181113
CVE: CVE-2018-8566
KB: KB4465664
Title: BitLocker Security Feature Bypass Vulnerability
Affected product: Windows 10 Version 1809 for x64-based Systems
Affected component: BitLocker
Severity: Important
Impact: Security Feature Bypass
Exploit: n/a

Date: 20181129
CVE: ADV180030
KB: KB4477029
Title: November 20, 2018 Flash Updates
Affected product: Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems
Affected component: Adobe Flash Player
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a
```

```
[+] Missing patches: 17
- KB4512578: patches 112 vulnerabilities
- KB5003171: patches 36 vulnerabilities
- KB4507419: patches 6 vulnerabilities
- KB4483452: patches 4 vulnerabilities
- KB4556441: patches 4 vulnerabilities
- KB4535101: patches 4 vulnerabilities
- KB4578973: patches 4 vulnerabilities
- KB4570505: patches 4 vulnerabilities
- KB4514601: patches 2 vulnerabilities
- KB4535680: patches 2 vulnerabilities
- KB4601887: patches 2 vulnerabilities
- KB4465664: patches 1 vulnerability
- KB4477029: patches 1 vulnerability
- KB4487038: patches 1 vulnerability
- KB4516115: patches 1 vulnerability
- KB4519337: patches 1 vulnerability
- KB4558997: patches 1 vulnerability
[+] KB with the most recent release date
- ID: KB5003171
- Release date: 20210511

[+] Done. Displaying 186 of the 186 vulnerabilities found.

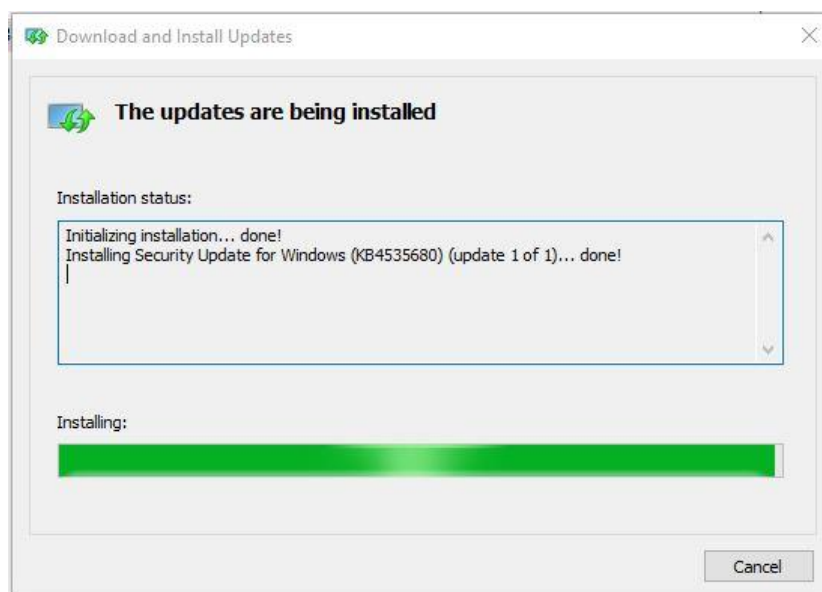
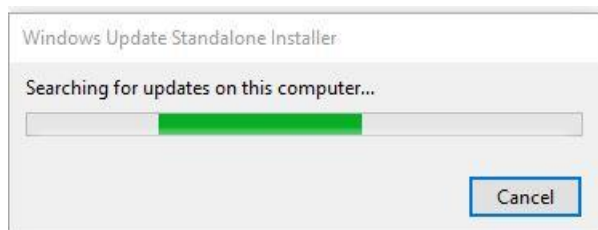
C:\Users\IEUser\Downloads\wesng-master\wesng-master>
```

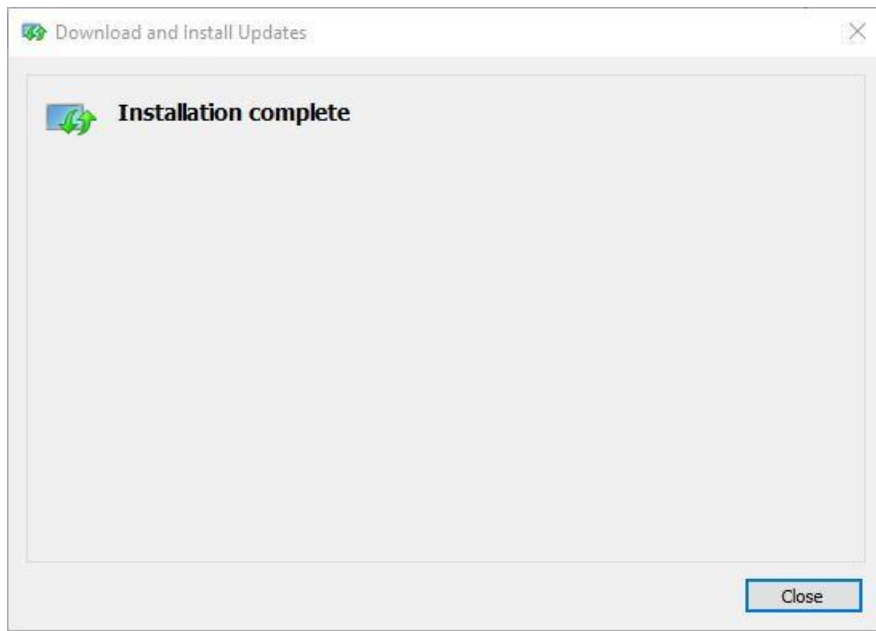
These are the vulnerabilities found in the machine. And the above-mentioned vulnerabilities are patched in this report.

The screenshot shows the Microsoft Update Catalog website with search results for KB4535680. The search bar at the top contains 'KB4535680'. Below the search bar, there is a table of results. The table has columns for Title, Products, Classification, Last Updated, Version, Size, and Download. There are 12 results listed, all for Security Updates. The first result is 'Security Update for Windows Server, version 1909 for x64-based Systems (KB4535680)' for Windows Server, version 1903 and later. The last result is '2021-01 Security Update for Windows 10 Version 1507 for x64-based Systems (KB4535680)' for Windows 10 LTSB. At the bottom of the page, there is a taskbar showing a file named 'windows10.0-kb4...msu'.

Title	Products	Classification	Last Updated	Version	Size	Download
Security Update for Windows Server, version 1909 for x64-based Systems (KB4535680)	Windows Server, version 1903 and later	Security Updates	1/11/2021	n/a	206 KB	Download
Security Update for Windows Server 2019 for x64-based Systems (KB4535680)	Windows Server 2019	Security Updates	1/11/2021	n/a	205 KB	Download
Security Update for Windows Server 2016 for x64-based Systems (KB4535680)	Windows Server 2016	Security Updates	1/11/2021	n/a	227 KB	Download
Security Update for Windows 10 Version 1909 for x64-based Systems (KB4535680)	Windows 10, version 1903 and later	Security Updates	1/11/2021	n/a	206 KB	Download
Security Update for Windows 10 Version 1809 for x64-based Systems (KB4535680)	Windows 10	Security Updates	1/11/2021	n/a	205 KB	Download
Security Update for Windows 10 Version 1803 for x64-based Systems (KB4535680)	Windows 10	Security Updates	1/11/2021	n/a	222 KB	Download
Security Update for Windows 10 Version 1607 for x64-based Systems (KB4535680)	Windows 10	Security Updates	1/11/2021	n/a	227 KB	Download
2021-01 Security Update for Windows Server 2012 R2 for x64-based Systems (KB4535680)	Windows Server 2012 R2	Security Updates	1/11/2021	n/a	251 KB	Download
2021-01 Security Update for Windows 8.1 for x64-based Systems (KB4535680)	Windows 8.1	Security Updates	1/11/2021	n/a	251 KB	Download
2021-01 Security Update for Windows Embedded 8 Standard for x64-based Systems (KB4535680)	Windows 8 Embedded	Security Updates	1/11/2021	n/a	239 KB	Download
2021-01 Security Update for Windows Server 2012 for x64-based Systems (KB4535680)	Windows Server 2012	Security Updates	1/11/2021	n/a	239 KB	Download
2021-01 Security Update for Windows 10 Version 1507 for x64-based Systems (KB4535680)	Windows 10 LTSB	Security Updates	1/11/2021	n/a	203 KB	Download

Downloaded the respective msu file and started installing it.





Similarly, Install the updates for last vulnerability also.

A screenshot of the Microsoft Update Catalog website. The browser address bar shows "catalog.update.microsoft.com/Search.aspx?q=KB4558997". The page title is "Microsoft Update Catalog". A search bar contains "KB4558997" and a "Search" button. Below the search bar, it says "Search results for 'KB4558997'". There are navigation links "Previous" and "Next". Below that, it says "Updates: 1 - 4 of 4 (page 1 of 1)". A table lists the updates with columns: Title, Products, Classification, Last Updated, Version, Size, and Download. The table contains four rows of update information. At the bottom, there is a footer with copyright information: "© 2021 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | help".

Title	Products	Classification	Last Updated	Version	Size	Download
2020-07 Servicing Stack Update for Windows 10 Version 1809 for x86-based Systems (KB4558997)	Windows 10, Windows 10 LTSB	Security Updates	7/13/2020	n/a	6.1 MB	Download
2020-07 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4558997)	Windows Server 2019	Security Updates	7/13/2020	n/a	13.6 MB	Download
2020-07 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB4558997)	Windows 10, Windows 10 LTSB	Security Updates	7/13/2020	n/a	13.6 MB	Download
2020-07 Servicing Stack Update for Windows 10 Version 1809 for ARM64-based Systems (KB4558997)	Windows 10, Windows 10 LTSB	Security Updates	7/13/2020	n/a	16.8 MB	Download

Now running again the systeminfo and wes.py:

```
C:\Windows\System32\cmd.exe
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 1809 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

[+] Missing patches: 15
- KB4512578: patches 112 vulnerabilities
- KB5003171: patches 36 vulnerabilities
- KB4507419: patches 6 vulnerabilities
- KB4483452: patches 4 vulnerabilities
- KB4556441: patches 4 vulnerabilities
- KB4535101: patches 4 vulnerabilities
- KB4578973: patches 4 vulnerabilities
- KB4570505: patches 4 vulnerabilities
- KB4514601: patches 2 vulnerabilities
- KB4601887: patches 2 vulnerabilities
- KB4465664: patches 1 vulnerability
- KB4477029: patches 1 vulnerability
- KB4487038: patches 1 vulnerability
- KB4516115: patches 1 vulnerability
- KB4519337: patches 1 vulnerability
[+] KB with the most recent release date
- ID: KB5003171
- Release date: 20210511

[+] Done. Displaying 183 of the 183 vulnerabilities found.
C:\Users\IEUser\Downloads\wesng-master\wesng-master>
```

You can see total 3 vulnerabilities have eliminated. Similarly, you can do for others.