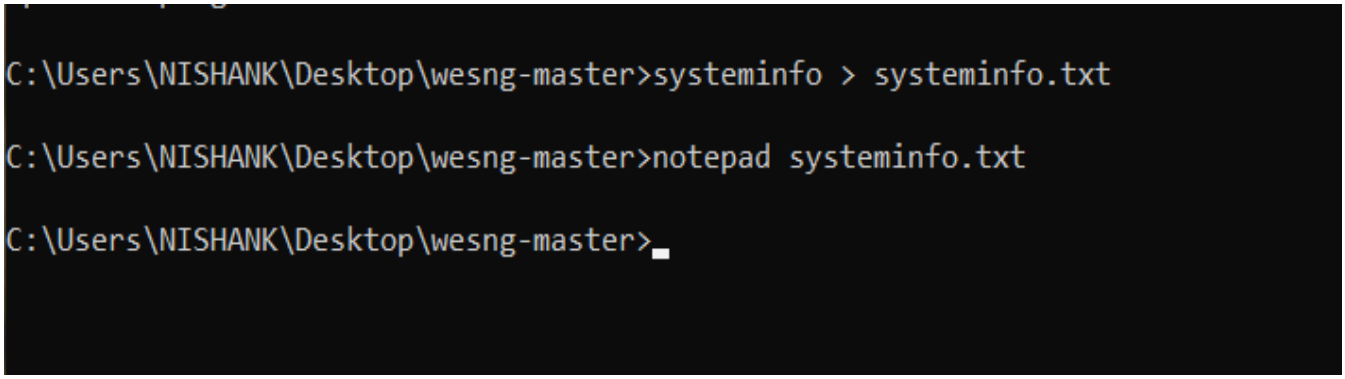
SECURE CODING LAB-13

By-Nishank Verma

19BCN7131

Creating systeminfo.txt file



Host Name: LAPTOP-G637AG3U

OS Name: Microsoft Windows 10 Home Single Language

OS Version: 10.0.19042 N/A Build 19042

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation

OS Build Type: Multiprocessor Free

Registered Owner: HP

Registered Organization: HP

Product ID: xxxx-xxxx-xxxx-xxxx

Original Install Date: 24-07-2020, 20:22:46

System Boot Time: 13-06-2021, 01:10:51

System Manufacturer: HP

System Model: HP Pavilion Laptop 15-cc1xx

System Type: x64-based PC

Processor(s): 1 Processor(s) Installed.

[01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1792 Mhz

BIOS Version: Insyde F.35, 08-12-2020

Windows Directory: C:\WINDOWS

System Directory: C:\WINDOWS\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: 00004009

Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Total Physical Memory: 8,078 MB

Available Physical Memory: 1,778 MB

Virtual Memory: Max Size: 12,942 MB

Virtual Memory: Available: 5,267 MB

Virtual Memory: In Use: 7,675 MB

Page File Location(s): C:\pagefile.sys

Domain: WORKGROUP

Logon Server: \\LAPTOP-G637AG3U

Hotfix(s): 15 Hotfix(s) Installed.

[01]: KB5003254

[02]: KB4561600

[03]: KB4562830

[04]: KB4566785

[05]: KB4570334

[06]: KB4577266

[07]: KB4577586

[08]: KB4580325

[09]: KB4586864

[10]: KB4589212

[11]: KB4593175

[12]: KB4598481

[13]: KB5001679

[14]: KB5004476

[15]: KB5003503

Network Card(s): 4 NIC(s) Installed.

[01]: Realtek PCIe GBE Family Controller

Connection Name: Ethernet 2

Status: Media disconnected

[02]: Intel(R) Dual Band Wireless-AC 7265

Connection Name: Wi-Fi

DHCP Enabled: Yes

DHCP Server: 192.168.1.1

IP address(es)

[01]: 192.168.1.7

[02]: fe80::49c8:728e:e6c1:54e4

[03]: VirtualBox Host-Only Ethernet Adapter

Connection Name: Ethernet

DHCP Enabled: No

IP address(es)

[01]: 192.168.56.1

[02]: fe80::84b7:924e:f036:b859

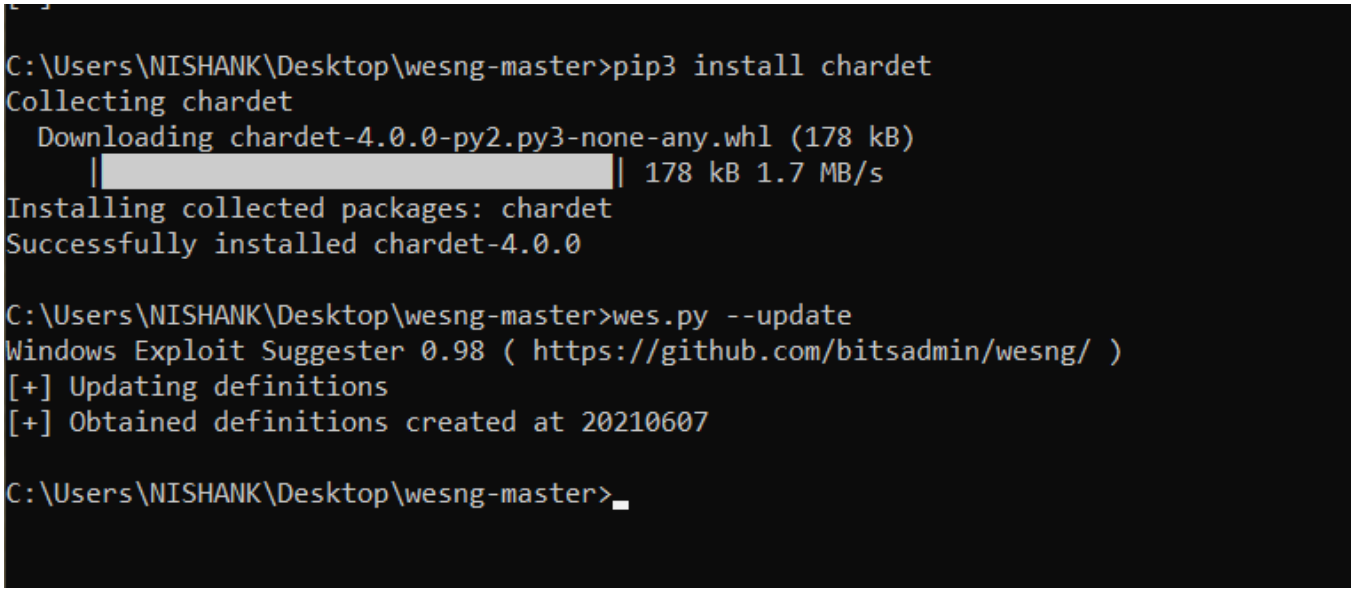
[04]: Kaspersky Security Data Escort Adapter

Connection Name: Ethernet 3

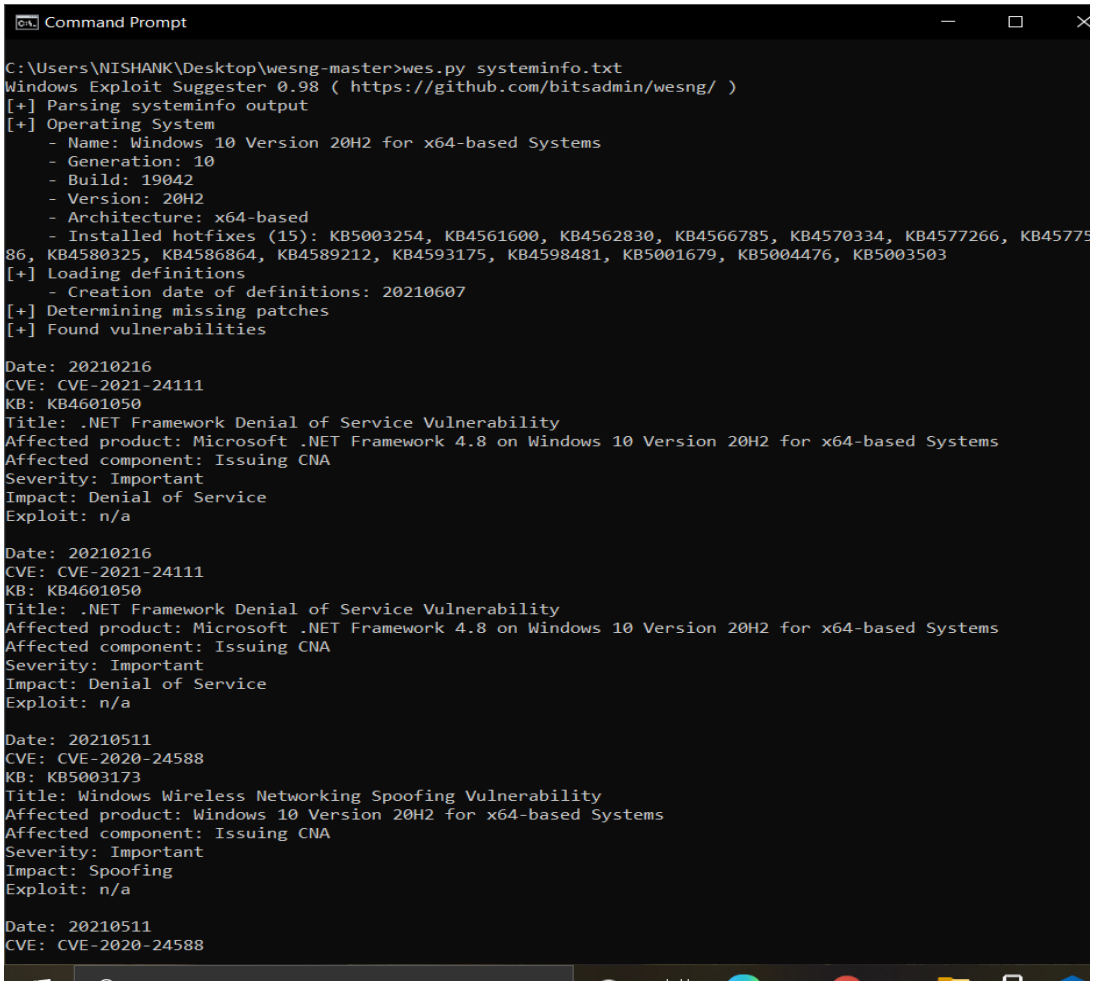
Status: Media disconnected

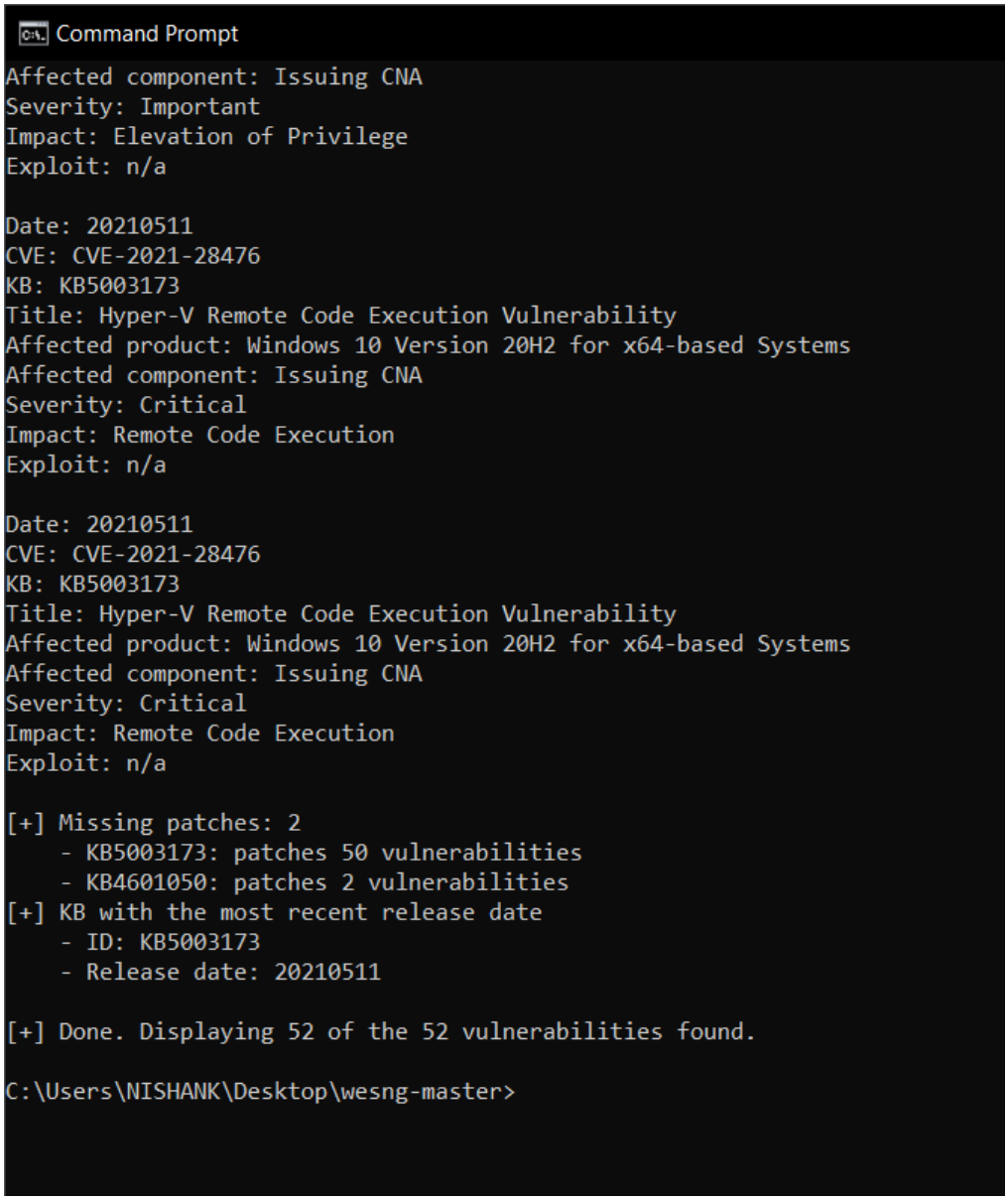
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

Updating WES-NG with the latest database



Checking vulnerabilities




Command Prompt
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a
Date: 20210511
CVE: CVE-2021-28476
KB: KB5003173
Title: Hyper-V Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a
[+] Missing patches: 2
- KB5003173: patches 50 vulnerabilities
- KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
- ID: KB5003173
- Release date: 20210511
[+] Done. Displaying 52 of the 52 vulnerabilities found.
C:\Users\NISHANK\Desktop\wesng-master>

Patching

```
[+] Done. Displaying 50 of the 52 vulnerabilities found.

C:\Users\NISHANK\Desktop\wesng-master>
C:\Users\NISHANK\Desktop\wesng-master>wes.py -e systeminfo.txt --hide "Internet Explorer" Edge
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 (15): KB5003254, KB4561600, KB4562830, KB4566785, KB4570334, KB4577266, KB45775
86, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5001679, KB5004476, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found


C:\Users\NISHANK\Desktop\wesng-master>
```