SECURE CODING CSE2010

LAB-13

CH.SAI SUMEDH

REG NO:-18BCN7092

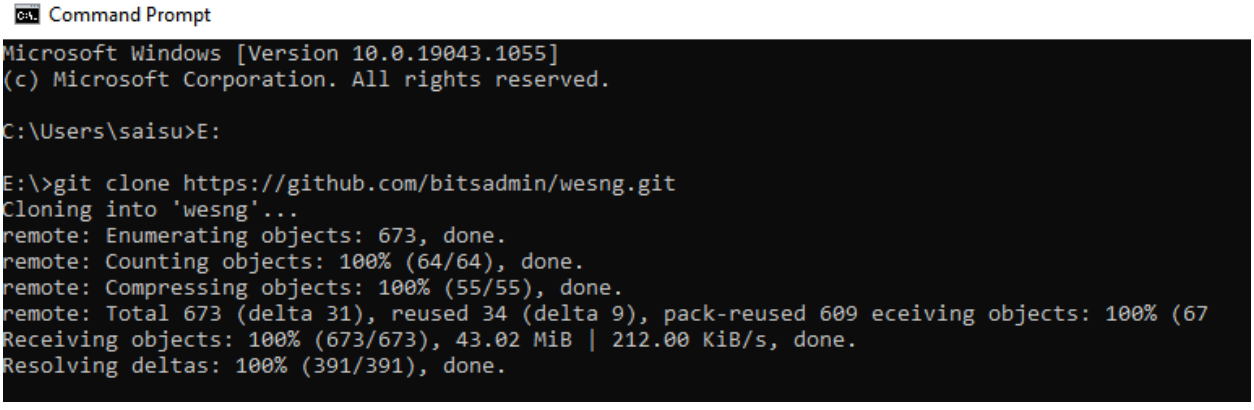
SLOT:-L39+L40

Lab experiment – 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.**

Download and install WES-NG in your system.



```
E:\>cd wesng

E:\wesng>wes.py

E:\wesng>python wes.py
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]
```

Now get the systeminfo and write it into a text document.

```
E:\wesng>systeminfo > systeminfo.txt

E:\wesng>notepad systeminfo.txt
```

systeminfo.txt - Notepad

File Edit Format View Help

```
Host Name:                 DESKTOP-FJE40NV
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19043 N/A Build 19043
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          saisumedh16@gmail.com
Registered Organization:
Product ID:                00331-10000-00001-AA182
Original Install Date:     3/9/2021, 9:39:34 PM
System Boot Time:          6/14/2021, 2:05:28 AM
System Manufacturer:       LENOVO
System Model:              81DE
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1600 Mhz
BIOS Version:              LENOVO 8TCN60WW, 11/26/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,101 MB
Available Physical Memory: 982 MB
Virtual Memory: Max Size:  15,781 MB
Virtual Memory: Available: 4,396 MB
Virtual Memory: In Use:    11,385 MB
Page File Location(s):     C:\pagefile.sys
```

Now check whether vulnerabilities exists or not

```
E:\wesng>python wes.py systeminfo.txt
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: 19043
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (11): KB5003254, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212, KB4598481, KB5000736,
 KB5004476, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210614
[+] 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
```

There are no vulnerabilities in my pc.