SECURE CODING LAB-13
07-06-2021

SLOT-L39+L40
18BCN7134
NIHARIKA VISWANADHUNI

Lab experiment - Automated Vulnerability Analysis and Patch Management

QUESTION

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.**

OUTPUT

Download Next Generation from https://github.com/bitsadmin/wesng.Now run wes.py
Command:python wes.py

```
Command Prompt
C:\Users\nihar\Downloads\wesng-master>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]
                        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
```

Update wes.py

```
Command Prompt
C:\Users\nihar\Downloads\wesng-master>python wes.py --update
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210607
```

Now,create a text file to store the vulnerabilities

```
Command Prompt
C:\Users\nihar\Downloads\wesng-master>systeminfo > system_demo.txt
```

Now enter the vulnerabilities to the text file created.

```
Command Prompt
C:\Users\nihar\Downloads\wesng-master>python wes.py system_demo.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 (10): KB5003254, KB4577266, KB4577586, KB4580325, KB4586864, KB4589212, KB4593175, KB4598481, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] 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
```

```
[+] Missing patches: 4
    - KB5003173: patches 50 vulnerabilities
    - KB4569745: patches 2 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
    - KB4566785: patches 1 vulnerability
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 55 of the 55 vulnerabilities found.
```

Now open the text file to see the vulnerabilities

Command Prompt

```
C:\Users\nihar\Downloads\wesng-master>system_demo.txt
```

system_demo.txt - Notepad

File Edit Format View Help

```
Host Name:                 LAPTOP-O4KU1R81
OS Name:                   Microsoft Windows 10 Home Single Language
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          niharikaviswanadhuni@gmail.com
Registered Organization:
Product ID:                00327-35831-27946-AAOEM
Original Install Date:     27-10-2020, 18:23:20
System Boot Time:          12-06-2021, 1:34:33
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 ~16
BIOS Version:              LENOVO 8TCN51WW, 08-12-2018
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:     8,101 MB
Available Physical Memory: 3,148 MB
Virtual Memory: Max Size:  15,525 MB
Virtual Memory: Available: 6,439 MB
Virtual Memory: In Use:    9,086 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-O4KU1R81
Hotfix(s):                 10 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4577266
                           [03]: KB4577586
                           [04]: KB4580325
                           [05]: KB4586864
                           [06]: KB4589212
                           [07]: KB4593175
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8