GDSSecurity / Windows-Exploit-Suggester

Watch 61 Star 236 Fork 74

Code Issues 0 Pull requests 0 Pulse Graphs

This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target. It also notifies the user if there are public exploits and Metasploit modules available for the missing bulletins.

24 commits 1 branch 0 releases 1 contributor

Branch: master New pull request New file Find file HTTPS https://github.com/GDSSec Download ZIP

sammbertram Adding new exploits to db Latest commit 24010c9 Jan 4, 2016

LICENSE.md	Adding support for windows 10	Sep 16, 2015
README.md	Adding support for windows 10	Sep 16, 2015
windows-exploit-suggester.py	Adding new exploits to db	Jan 4, 2016

README.md

DESCRIPTION

This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

on the target. It also notifies the user if there are public exploits and Metasploit modules available for the missing bulletins.

It requires the 'systeminfo' command output from a Windows host in order to compare that the Microsoft security bulletin database and determine the patch level of the host.

It has the ability to automatically download the security bulletin database from Microsoft with the --update flag, and saves it as an Excel spreadsheet.

When looking at the command output, it is important to note that it assumes all vulnerabilities and then selectively removes them based upon the hotfix data. This can result in many false-positives, and it is key to know what software is actually running on the target host. For example, if there are known IIS exploits it will flag them even if IIS is not running on the target host.

The output shows either public exploits (E), or Metasploit modules (M) as indicated by the character value.

It was heavily inspired by Linux_Exploit_Suggester by Pentura.

Blog Post: "Introducing Windows Exploit Suggester", https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit-suggester.html

USAGE

update the database

```
 $ ./windows-exploit-suggester.py --update
[*] initiating...
[*] successfully requested base url
[*] scraped ms download url
[+] writing to file 2014-06-06-mssb.xlsx
[*] done
```

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

install dependencies

(install python-xlrd, $ pip install xlrd --upgrade)

feed it "systeminfo" input, and point it to the microsoft database

```
 $ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --systeminfo win7sp1-systeminfo.txt
[*] initiating...
[*] database file detected as xls or xlsx based on extension
[*] reading from the systeminfo input file
[*] querying database file for potential vulnerabilities
[*] comparing the 15 hotfix(es) against the 173 potential bulletins(s)
[*] there are now 168 remaining vulns
[+] windows version identified as 'Windows 7 SP1 32-bit'
[*]
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - I
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Cr
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Impo
[*] done
```

possible exploits for an operating system can be used without hotfix data

```
 $ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --ostext 'windows server 2008 r2'
```

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

```
[*] initiating...
[*] database file detected as xls or xlsx based on extension
[*] getting OS information from command line text
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 196 potential bulletins(s)
[*] there are now 196 remaining vulns
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Impo
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Im
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
```

LIMITATIONS

Currently, if the 'systeminfo' command reveals 'File 1' as the output for the hotfixes, it will not be able to determine which are installed on the target. If this occurs, the list of hotfixes will need to be retrieved from the target host and passed in using the --hotfixes flag

It currently does not seperate 'editions' of the Windows OS such as 'Tablet' or 'Media Center' for example, or different architectures, such as Itanium-based only

False positives also occur where it assumes EVERYTHING is installed on the target Windows operating system. If you receive the 'File 1' output, try executing 'wmic qfe list full' and feed that as input with the --hotfixes flag, along with the 'systeminfo'

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com

LICENSE

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/.

open in browser PRO version Are you a developer? Try out the HTML to PDF API pdfcrowd.com