KITPLOIT THE HACKER'S TOOLS

Contact Affiliate Blackploit Sumit a Tool

Home Windows GNU/Linux OS X Android iPhone Categories ▼

WideOrbit is driving transformation in advertising globally. In our data centers. Be Limitless The New Digital Realty

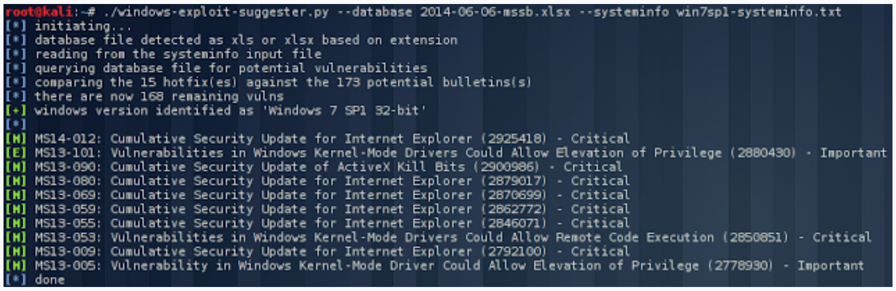
Labels ▼ Search

SCAN YOUR WEBSITE FOR SQLi, XSS & OTHER VULNERABILITIES WITH acunetix WVS 10

Home » Database » GNU » Metasploit » Remote Code Execution » vulnerabilities » Windows » Windows-Exploit-Suggester » Windows-Exploit-Suggester - Tool To Compares A Targets Patch Levels Against The Microsoft Vulnerability Database

Windows-Exploit-Suggester - Tool To Compares A Targets Patch Levels Against The Microsoft Vulnerability Database

Lydecker Black on 5:43 PM



```
root@kali:~# ./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) - Important
[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) - Critical
[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) - Important
[*] done
```

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.

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

Subscribe via e-mail

Subscribe via e-mail

Subscribe

Python for Offensive Penetration Testing Learn how to hack using Python One Time Offer 15$

Submit a Tool

Elasticsearch Conference

Elastic{ON} Feb 17-19 in SF. 40+ Talks, Deep Dives, Ask Me Anything

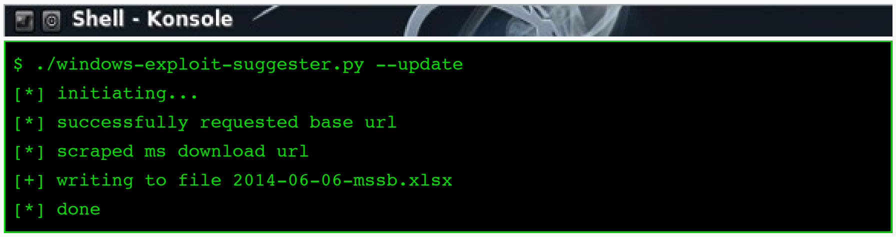
www.elastic.co/elasticon

Follow us!

Easy, Automated and Scalable Web Application Security
netsparkercloud
Register For a Free Trial

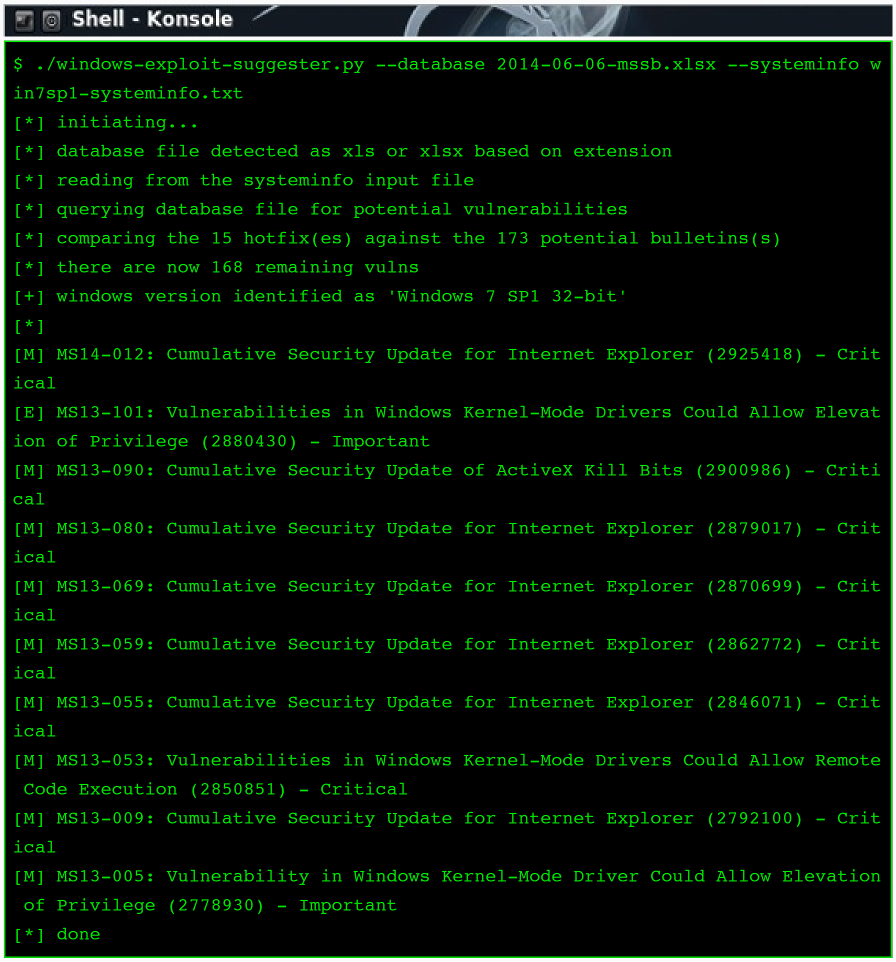
USAGE

update the database


Shell - Konsole

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

install dependencies
(install python-xlrd, $ pip install xlrd --upgrade)
feed it "systeminfo" input, and point it to the microsoft database


Shell - Konsole

```
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --systeminfo w
in7sp1-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) - Crit
ical
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevat
ion of Privilege (2880430) - Important
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Criti
cal
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Crit
ical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Crit
ical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Crit
ical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Crit
ical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote
 Code Execution (2850851) - Critical
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Crit
ical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation
 of Privilege (2778930) - Important
[*] done
```

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

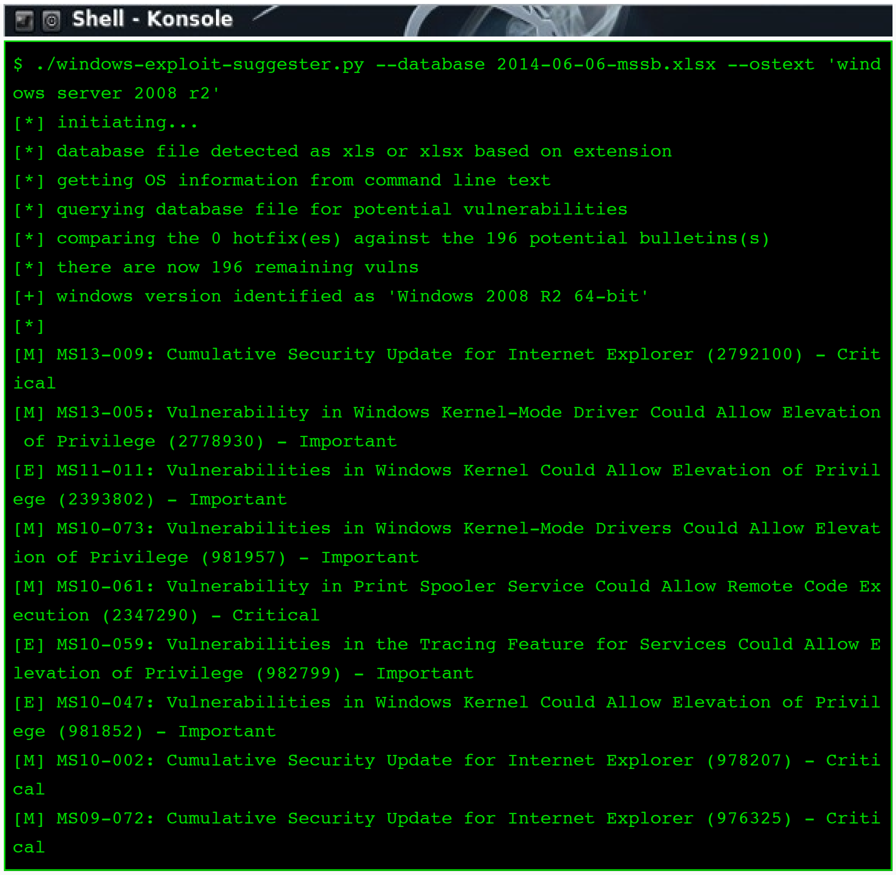
PenTest Tools
Like Page 14k likes
Follow @KitPloit 51.9K followers
KitPloit
Follow +1
+ 4,689
listeners BY FEEDBURNER
DedicatedSolutions.com
www.dedicatedsolutions.com
Best Quality
24/7 Live Support!
30-Day Money Back!
100% Uptime SLA!
100% Redundant Network!

Populars Comments Archive

FastIR Collector - Windows Incident Response Tool
This tool collects different artefacts on live Windows and records the results in csv files. With the analyses of this artefacts, an ear...

GDB-Dashboard - Modular Visual Interface For Gdb In Python
Modular visual interface for GDB in Python. This comes as a standalone single-file .gdbinit which, among the ot...

Windows-Exploit-Suggester - Tool To Compares A Targets Patch Levels Against The Microsoft Vulnerability Database
This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on ...



```
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --ostext 'wind
ows server 2008 r2'
[*] 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) - Crit
ical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation
 of Privilege (2778930) - Important
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privil
ege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevat
ion of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Ex
ecution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow E
levation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privil
ege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Criti
cal
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Criti
cal
```

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'

Download Windows-Exploit-Suggester

Is your website vulnerable to SQL INJECTION and XSS Vulnerabilities?
netsparker®
Web Application Security Scanner
DOWNLOAD NOW

Subscribe via e-mail for updates! Subscribe

Like 95 Tweet G+1 2 Share 1

V3n0M-Scanner - Popular SQLi and Pentesting Scanner

V3n0M runs on Python3 [Live Project - Readding old features back in and improved for Python3] v3n0m is a free and open source sca...

Viper - Cracking Unix Passwords Brute Force

Viper is a prute force UNIX-style password cracker for passwords encrypt with crypt. It has been developed from Hale's viper 1.4 Pe...

Metabrik - Perl Brik Platform

Smartphones have their apps, Web browsers have their apps, shells don't. With Metabrik , we tried to merge the power of shells with the p...

XXEinjector - Tool For Automatic Exploitation Of XXE Vulnerability

XXEinjector automates retrieving files using direct and out of band methods. Directory listing only works in Java applications. Brutefor...

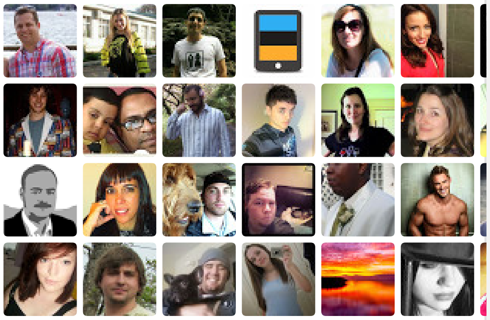
Labels

Linux Windows Mac Scanner Android Wireless Malware Analysis Malware SQLi Facebook iPhone Cheat Sheet Keylogger RAT

Google+ Followers

KitPloit

Follow

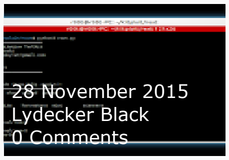


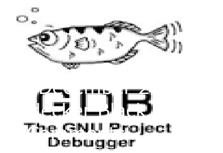
3,638 have us in circles

Next
V3n0M-Scanner - Popular SQLi and Pentesting Scanner

Previous
p0wnedShell - PowerShell Runspace Post Exploitation Toolkit

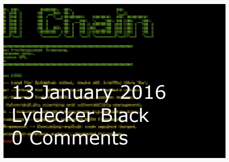
Related Posts

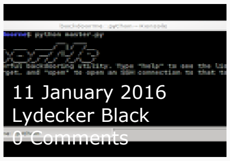

28 November 2015
Lydecker Black
0 Comments



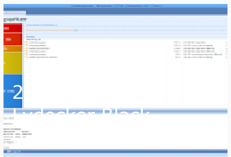
23 December 2015
Lydecker Black
0 Comments

25 January 2016
Lydecker Black
0 Comments


13 January 2016
Lydecker Black
0 Comments


11 January 2016
Lydecker Black
0 Comments

27 August 2015
Lydecker Black
0 Comments



Sponsored
FXOPEN

外汇交易平台|炒外汇|外汇理财|模拟外汇|MT4平台-FXOPEN中文官网

Fxopen是全球顶级在线外汇交易商,位列2010全球金融100强,fxopen提供MT4 ECN外汇交易平台,比特币等虚拟货币账户，PAMM账户,免费的外汇经纪,在线外汇培训,外汇交易,模拟外汇交易平台,迷你外汇等外汇相关服务.

Learn More

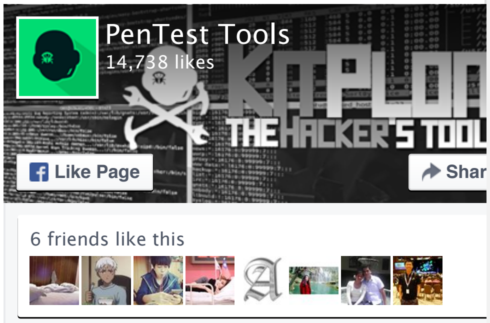
0 Comments KitPloit - Tools for your PenTest Arsenal! 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Add Disqus Add Privacy DISQUS



Tweets Follow

Hacker Tools ☣ @KitPloit 10h
SEE - Sandboxed Execution Environment goo.gl/97TJqL #Framework #Python #Sandbox pic.twitter.com/GPUDtS8mvK

Expand

Hacker Tools ☣ @KitPloit 10h

Tweet to @KitPloit

Sponsored

1. 10 Most Luxurious Hotels in the World 11 months ago happylifestylejournal.com Happy Lifestyle Journal HappyLifestyleJournal.com (sponsored) luxury

2. 14 Bathroom Inventions You Didn't Realize You Needed 7 months ago huffingtonpost.com Huffington Post HuffingtonPost.com (AOL) The Huffington Post News Team The Huffington Post News Team (sponsored) Most

Contact Form

Name

Email *

Message *

Send

Recommended:

- Blackploit [Pentest]
- DedicatedSolutions (Private Cloud)
- DedicatedSolutions (Server Products)
- DigitalOcean
- ExoClick
- Funeek!
- Th3 R4v3n
- TraffBoost
- 7PRO
- Underc0de
- Sunploit

Site Info
kitploit.com
Jan 31, 2016

Traffic Rank:	Links in:
297,908	54

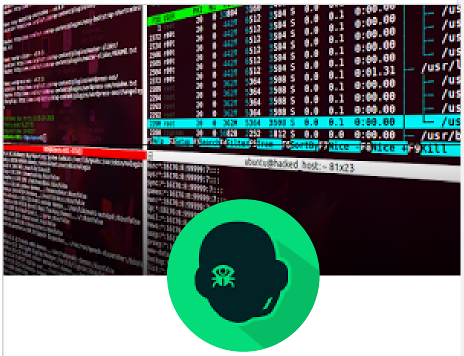
Powered by Alexa

14online

Follow us!

PenTest ...
Like Page

Follow @KitPloit 51.9K followers



KitPloit

google.com/+KitploitWeb

Hacking and PenTest Tools for your Security Arsenal!

Follow +1

+ 4,689

1089 listeners
BY FEEDBURNER

Copyright © 2012 KitPloit - PenTest Tools for your Security Arsenal! All Right Reserved
Designed by IVYthemes | MKR Site