

FIND ANY EXPLOIT WITH ONE COMMAND

Share this...



There are many tools available which can find exploits. These tools are more often works on automated way. As they show results in very short period of time. Nowdays most security researchers/ pentesters rely on these tools, ethical hacking teachers assure. Today we will show you a tool which find exploits in automated search.

According to [ethical hacking](#) researcher of International Institute of Cyber Security, pompem is very useful tool which are capable of finding exploits. The tool comes handy in initial phase of pentesting.

Pompem is a tool design to search for exploits & vulnerability in automated way. Pompem uses some popular databases to search for exploits. It uses databases like National Vulnerability Database, WPScan Vulnerability Database, PacketStorm security, CXSecurity, ZeroDay, Vulners. These are the standard repositories where all the vulnerabilities are present, as per an ethical hacking investigation.

- The tool has been tested on Kali Linux 2018.4

- For cloning tool : <https://github.com/rfunix/Pompem.git>

```
root@kali:/home/iicybersecurity# git clone https://github.com/rfunix/Pompem.git
Cloning into 'Pompem'...
remote: Enumerating objects: 749, done.
remote: Total 749 (delta 0), reused 0 (delta 0), pack-reused 749
Receiving objects: 100% (749/749), 377.13 KiB | 353.00 KiB/s, done.
Resolving deltas: 100% (421/421), done.
```

- Type **cd Pompem**
- Type **chmod u+x pompem.py**

```
root@kali:/home/iicybersecurity/Pompem# chmod u+x pompem.py
```

- Type **pip install -r requirements.txt**

```
root@kali:/home/iicybersecurity/Pompem# pip install -r requirements.txt
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7
won't be maintained after that date. A future version of pip will drop support for Python 2.7.
Collecting requests==2.9.1 (from -r requirements.txt (line 1))
  Downloading https://files.pythonhosted.org/packages/b8/f7/3bb4d18c234a8ce7044d5ee2e1082b7d72bf6c550afb8d51ae266dea56
f1/requests-2.9.1-py2.py3-none-any.whl (501kB)
    100% |████████████████████████████████| 501kB 668kB/s
dropbox 9.3.0 has requirement requests>=2.16.2, but you'll have requests 2.9.1 which is incompatible.
Installing collected packages: requests
  Found existing installation: requests 2.18.4
  Uninstalling requests-2.18.4:
```

Successfully uninstalled requests-2.18.4

Successfully installed requests-2.9.1

- Type **python pompem.py**
 - Now e will run pompem

```
bt@kali:/home/iicybersecurity/Pompem# python pompem.py
```

Rafael Francischini (Programmer and Ethical Hacker) - @rfunix

Bruno Fraga (Security Researcher) - @brunofraga.net

```
Usage: pompem.py [-s/--search <keyword, keyword, keyword, ...>]
                  [--txt Write txt file]
                  [--html Write html file]
Get basic options and Help, use: -h\--help
```

- Type `python pompem.py -s wordpress`

- **-s** is used for search keyword. **wordpress** is the keyword to search.

```
root@kali:/home/iicybersecurity/Pompem# python pompem.py -s wordpress
+Results wordpress
+-----+
+-----+-----+
| Date | Description | Url |
+-----+-----+
| 2019-02-15 | WordPress Booking Calendar 8.4.3 SQL Injection | https://packetstormsecurity.com/files/151692/WordPress-Booking-Calendar-8.4.3-SQL-Injection.html |
+-----+
+-----+-----+
| 2019-02-14 | WordPress WP-JS-External-Link-Info 2.2.0 Open Redi | https://packetstormsecurity.com/files/151679/WordPress-WP-JS-External-Link-Info-2.2.0-Open-Redirection.html |
+-----+
+-----+-----+
| 2019-02-14 | WordPress Jssor-Slider 3.1.24 Cross Site Request F | https://packetstormsecurity.com/files/151678/WordPress-Jssor-Slider-3.1.24-Cross-Site-Request-Forgery-File-Upload.html |
+-----+
+-----+-----+
| 2019-02-12 | Joomla WordPress Blog 4.8.0 SQL Injection | https://packetstormsecurity.com/files/151626/Joomla-WordPress-Blog-4.8.0-SQL-Injection.html |
+-----+
+-----+-----+
| 2019-02-06 | WordPress YOP Poll 6.0.2 Cross Site Scripting | https://packetstormsecurity.com/files/151559/WordPress-YOP-Poll-6.0.2-Cross-Site-Scripting.html |
+-----+
```

-----+
2019-02-06 | WordPress WP Live Chat 8.0.18 Cross Site Scripting | <https://packetstormsecurity.com/files/151557/WordPress-WP-Live-Chat-8.0.18-Cross-Site-Scripting.html>
-----+
-----+
2019-02-06 | WordPress wpGoogleMaps 7.10.41 Cross Site Scripting | <https://packetstormsecurity.com/files/151556/WordPress-wpGoogleMaps-7.10.41-Cross-Site-Scripting.html>
-----+
-----+
2019-02-06 | WordPress Social Networks Auto-Poster 4.2.7 Cross | <https://packetstormsecurity.com/files/151554/WordPress-Social-Networks-Auto-Poster-4.2.7-Cross-Site-Scripting.html>
-----+
-----+
2019-02-06 | WordPress KingComposer 2.7.6 Cross Site Scripting | <https://packetstormsecurity.com/files/151552/WordPress-KingComposer-2.7.6-Cross-Site-Scripting.html>

- After executing the above query, pompem has used above list databases to find exploits & vulnerabilities in target running wordpress.
- When we open the first URL which is found by pompem in wordpress. It shows :

WordPress Booking Calendar 8.4 x

https://packetstormsecurity.com/files/151692/WordPress-Booking-Calendar-8.4.3-SQL-Injection.html

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Wordpress Booking Calendar v8.4.3 - Authenticated SQL Injection Vulnerability
# Date: 2018-12-28
# Exploit Author: B0UG
# Vendor Homepage: https://wpbookingcalendar.com/
# Software Link: https://wordpress.org/plugins/booking/
# Version: Tested on version 8.4.3 (older versions may also be affected)
# Tested on: WordPress
# Category : Webapps
# CVE: CVE-2018-20556

#I. VULNERABILITY

Authenticated SQL Injection

#II. BACKGROUND
'Booking Calendar' WordPress plugin developed by oplugins is a booking system which allows website visitors to check the availability of services and make reservations.

#III. DESCRIPTION
An authenticated SQL Injection vulnerability in the 'Booking Calendar' WordPress plugin allows an attacker to read arbitrary data from the database.

#IV. PROOF OF CONCEPT
1) Access WordPress control panel.
2) Navigate to the Booking Calendar plugin page.
3) Set up Burp Suite to capture the traffic.
4) Select one of the booking entries and click on the 'Trash Can' button to delete the entry.
5) Within Burp Suite, analyse the POST request and identify the parameter 'booking_id'.
6) The 'booking_id' parameter is vulnerable to the following different types of SQL injection:
   a) Boolean based blind injection
```

File Archive: February 2019 <

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

Top Authors In Last 30 Days

KingSkrupeLlos 95 files

Ubuntu 40 files

Red Hat 38 files

Ihsan Sencan 27 files

Debian 24 files

Google Security Research 17 files

Rafael Pedrero 15 files

- As you can see the above listed link shows that vulnerability is in the wordpress plugin. This vulnerability can cause sql injection. If the target is using wordpress booking calendar in wordpress site. The attack can be done.
- As mentioned above pompem uses different security databases where all the vulnerabilities are listed which can be done easily.
- These vulnerabilities can be extended to further hacking activities.
- Type **python pompem.py -s windows**
- s** is the search keyword. **windows** is the keyword to search for.

```
root@kali:/home/iicybersecurity/Pompem# python pompem.py -s windows
+Results windows
+-----
```

+Date	Description	Url
+		
2019-02-02	SolarWinds Serv-U FTP 15.1.6 Privilege Escalation	https://packetstormsecurity.com/files/151473/SolarWinds-Serv-U-FTP-15.1.6-Privilege-Escalation.html
+		
2019-01-30	Microsoft Windows/x86 msiexec.exe Download And Exe	https://packetstormsecurity.com/files/151404/Microsoft-Windows-x86-msiexec.exe-Download-And-Execute-Shellcode.html
+		
2019-01-27	R 3.4.4 Local Buffer Overflow	https://packetstormsecurity.com/files/151344/R-3.4.4-Local-Buffer-Overflow.html
+		
2019-01-22	Microsoft Windows VCF Arbitrary Code Execution	https://packetstormsecurity.com/files/151267/Microsoft-Windows-VCF-Arbitrary-Code-Execution.html
+		
2019-01-17	Windows Debugging 101	https://packetstormsecurity.com/files/151215/Windows-Debugging-101.html
+		
2019-01-16	Microsoft Windows .contact Arbitrary Code Execution	https://packetstormsecurity.com/files/151194/Microsoft-Windows-.contact-Arbitrary-Code-Execution.html
+		

- After executing the above query, pompem has find many vulnerabilities regarding windows operating system. As told above pompem uses security databases to find exploits.
- The above vulnerabilities can be used in other hacking activities.
- When we open first URL. It shows :



SolarWinds Serv-U FTP 15.1.6 Privilege Escalation

Authored by Chris Moberly

Posted Feb 2, 2019

SolarWinds Serv-U FTP Server version 15.1.6 is vulnerable to privilege escalation from remote authenticated users by leveraging the CSV user import function. This leads to obtaining remote code execution under the context of the Windows SYSTEM account in a default installation.

tags | exploit, remote, code execution
systems | windows
advisories | CVE-2018-15906
MD5 | 2d9d1dea8fb44a6520cc80fea10a1f40

Download | Favorite | Comments (0)

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

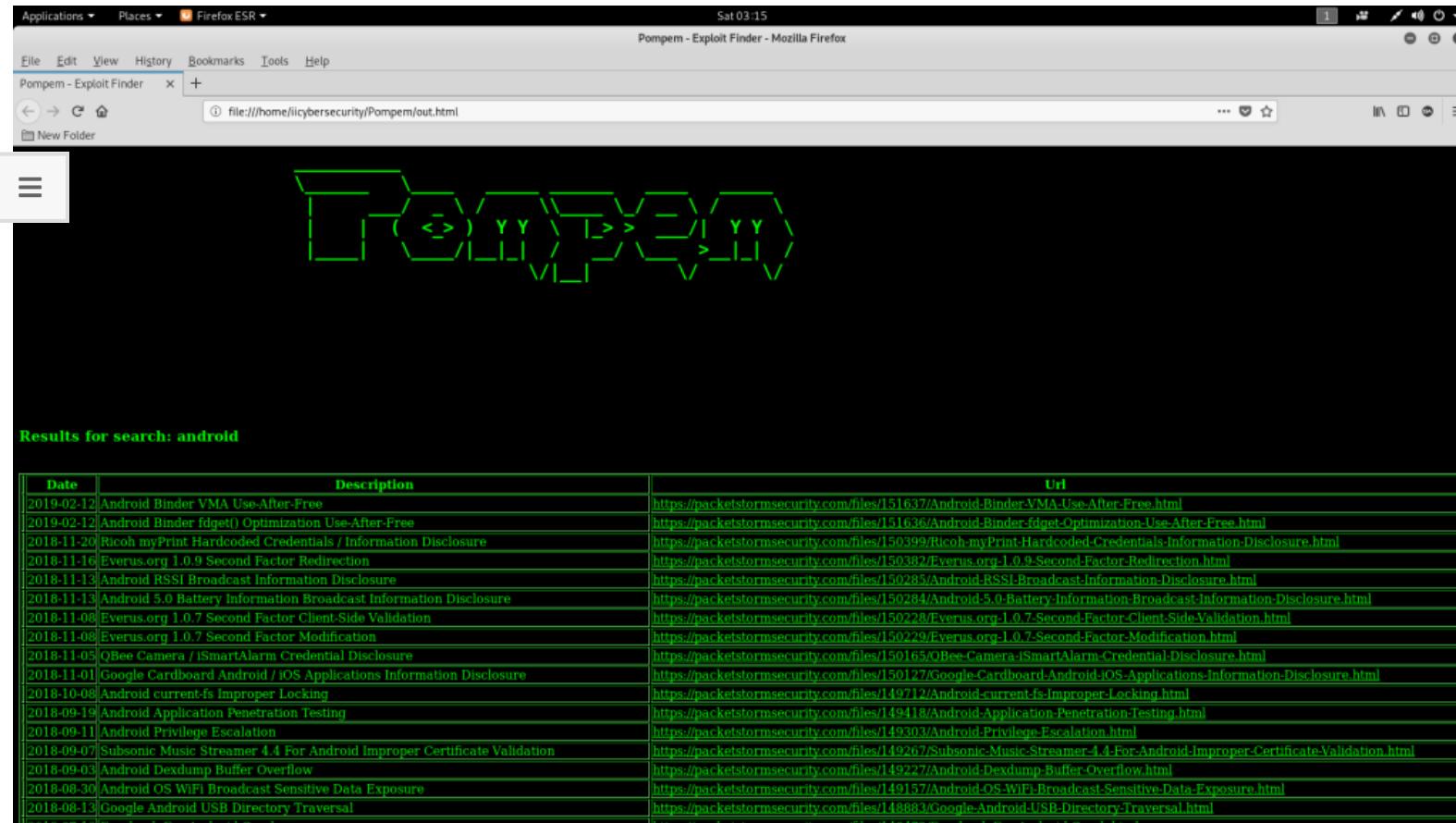
File Archive: February 2019 <

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

- The above vulnerability shows privilege escalation attack could be done on windows operating system.
- Type **python pompem.py -s android –html**
- **-s** is used to search for keyword. Here **android** is keyword to search for.
- **–html** is used to save file in html.

```
root@kali:/home/iicybersecurity/Pompem# python pompem.py -s android --html
+Results android
+-----
+-----+-----+-----+
| Date | Description | Url |
+-----+-----+-----+
| 2019-02-12 | Android Binder VMA Use-After-Free | https://packetstormsecurity.com/files/151637/Android-Binder-VMA-Use-After-Free.html |
+-----+-----+-----+
| 2019-02-12 | Android Binder fdget() Optimization Use-After-Free | https://packetstormsecurity.com/files/151636/Android-Binder-fdget-Optimization-Use-After-Free.html |
+-----+-----+-----+
| 2018-11-20 | Ricoh myPrint Hardcoded Credentials / Information | https://packetstormsecurity.com/files/150399/Ricoh-myPrint-Hardcoded-Credentials-Information-Disclosure.html |
+-----+-----+-----+
| 2018-11-16 | Everus.org 1.0.9 Second Factor Redirection | https://packetstormsecurity.com/files/150382/Everus.org-1.0.9-Second-Factor-Redirection.html |
+-----+-----+-----+
| 2018-11-13 | Android RSSI Broadcast Information Disclosure | https://packetstormsecurity.com/files/150285/Android-RSSI-Broadcast-Information-Disclosure.html |
+-----+-----+-----+
```

- After executing the above query pompem has find vulnerabilities which can be used to exploit android users.
- Sometimes if the html file is not opened. Go to **Pompem** directory and open **out.html**. Opening its html file.



Results for search: android

Date	Description	Url
2019-02-12	Android Binder VMA Use-After-Free	https://packetstormsecurity.com/files/151637/Android-Binder-VMA-Use-After-Free.html
2019-02-12	Android Binder fdget() Optimization Use-After-Free	https://packetstormsecurity.com/files/151636/Android-Binder-fdget-Optimization-Use-After-Free.html
2018-11-20	Ricoh myPrint Hardcoded Credentials / Information Disclosure	https://packetstormsecurity.com/files/150399/Ricoh-myPrint-Hardcoded-Credentials-Information-Disclosure.html
2018-11-16	Everus.org 1.0.9 Second Factor Redirection	https://packetstormsecurity.com/files/150382/Everus.org-1.0.9-Second-Factor-Redirection.html
2018-11-13	Android RSSI Broadcast Information Disclosure	https://packetstormsecurity.com/files/150285/Android-RSSI-Broadcast-Information-Disclosure.html
2018-11-13	Android 5.0 Battery Information Broadcast Information Disclosure	https://packetstormsecurity.com/files/150284/Android-5.0-Battery-Information-Broadcast-Information-Disclosure.html
2018-11-08	Everus.org 1.0.7 Second Factor Client-Side Validation	https://packetstormsecurity.com/files/150228/Everus.org-1.0.7-Second-Factor-Client-Side-Validation.html
2018-11-08	Everus.org 1.0.7 Second Factor Modification	https://packetstormsecurity.com/files/150229/Everus.org-1.0.7-Second-Factor-Modification.html
2018-11-05	QBee Camera / iSmartAlarm Credential Disclosure	https://packetstormsecurity.com/files/150165/QBee-Camera-iSmartAlarm-Credential-Disclosure.html
2018-11-01	Google Cardboard Android / iOS Applications Information Disclosure	https://packetstormsecurity.com/files/150127/Google-Cardboard-Android-iOS-Applications-Information-Disclosure.html
2018-10-08	Android current-fs Improper Locking	https://packetstormsecurity.com/files/149712/Android-current-fs-Improper-Locking.html
2018-09-19	Android Application Penetration Testing	https://packetstormsecurity.com/files/149418/Android-Application-Penetration-Testing.html
2018-09-11	Android Privilege Escalation	https://packetstormsecurity.com/files/149303/Android-Privilege-Escalation.html
2018-09-07	Subsonic Music Streamer 4.4 For Android Improper Certificate Validation	https://packetstormsecurity.com/files/149267/Subsonic-Music-Streamer-4.4-For-Android-Improper-Certificate-Validation.html
2018-09-03	Android Dxdump Buffer Overflow	https://packetstormsecurity.com/files/149227/Android-Dxdump-Buffer-Overflow.html
2018-08-30	Android OS WiFi Broadcast Sensitive Data Exposure	https://packetstormsecurity.com/files/149157/Android-OS-WiFi-Broadcast-Sensitive-Data-Exposure.html
2018-08-13	Google Android USB Directory Traversal	https://packetstormsecurity.com/files/148883/Google-Android-USB-Directory-Traversal.html
2018-07-10	QBee Camera 1.0.9 Android Crash	https://packetstormsecurity.com/files/148177/QBee-Camera-1.0.9-Android-Crash.html

- Opening one of the scanned URL from output :

Android Binder fdget() Optimization Use-After-Free x

https://packetstormsecurity.com/files/151636/Android-Binder-fdget-Optimization-Use-After-Free.html

Register | Login

packet storm

exploit the possibilities

Home Files News About Contact Add New

Android Binder fdget() Optimization Use-After-Free

Authored by Jann Horn, Google Security Research Posted Feb 12, 2019

Android binder suffers from a use-after-free vulnerability via fdget() optimization.

tags | exploit
advisories | CVE-2019-2000
MD5 | bc3a95911082f54f5d3a2b398792bb8b

Download | Favorite | Comments (0)

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Comments

No comments yet, be the first!

Follow us on Twitter
Follow us on Facebook
Subscribe to an RSS Feed

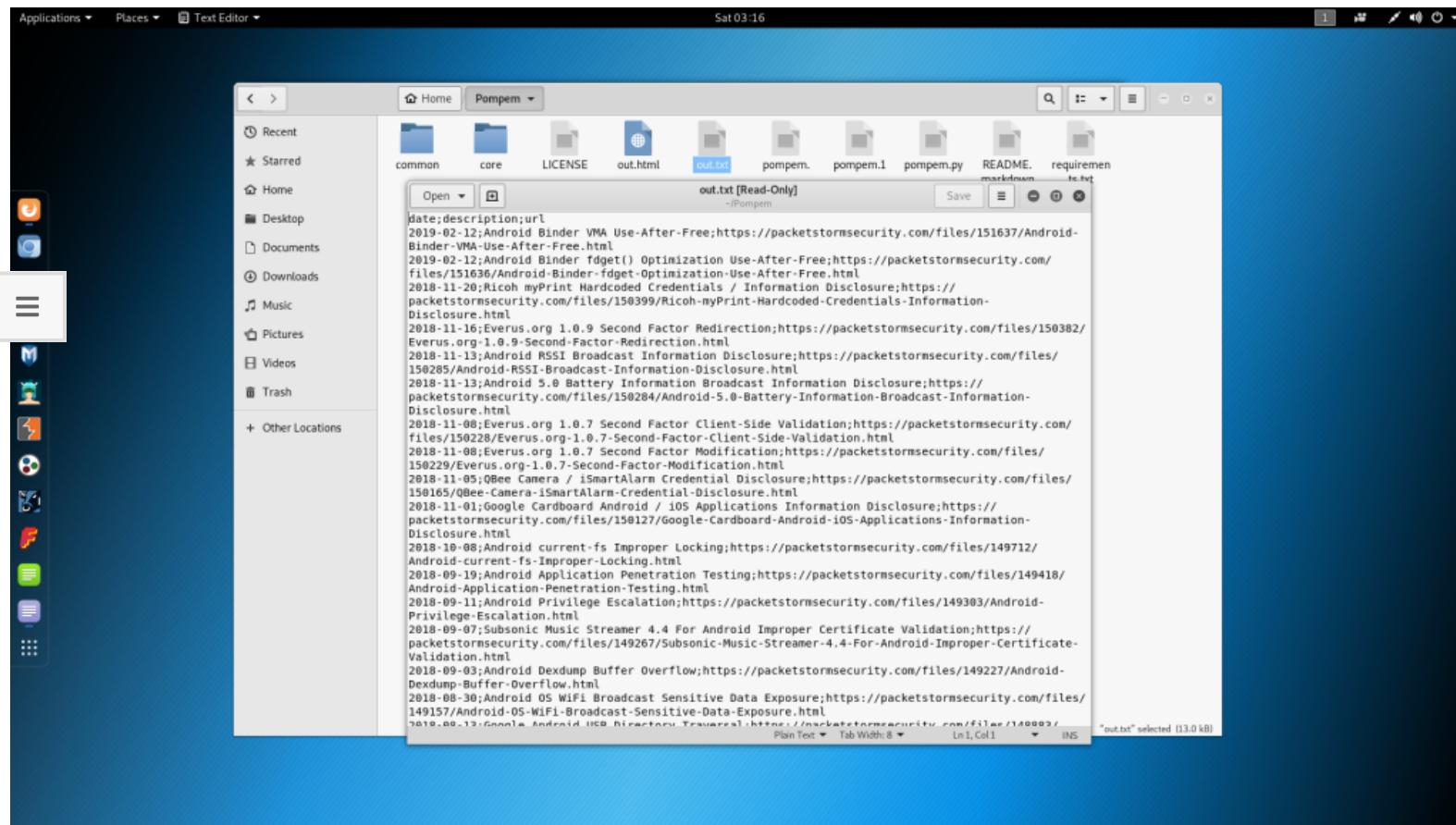
File Archive: February 2019

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

- The above shows the android binder vulnerability which can cause many other possibility of hacking attacks.
- You can also get an txt file. For that type **python pompem.py -s android --txt**
- **-s** is used to search for keyword. **android** is the keyword to search for.
- **--txt** is used to save file in **txt** form.

```
root@kali:/home/iicybersecurity/Pompem# python pompem.py -s android --txt
```

- For opening the txt file go to **pompem** directory. open **out.txt**



- The above is the list of URL which can be used in other hacking activities.
- Searching on different keywords type **python pompem.py -s fortinet**
- **-s** is used to search for keyword. **fortinet** is the firewall to search for. Fortinet is network firewall used in networks.

```
root@kali:/home/iicybersecurity/Pompem# python pompem.py -s fortinet
+Results fortinet
+-----+
+Date          Description          Url
+-----+
```

```
+-----+
-----+
2018-08-05 | Fortinet FortiClient 5.2.3 Local Privilege Escalat | https://packetstormsecurity.com/files/148811/Fortinet-FortiClient-5.2.3-Local-Privilege-Escalation.html
+-----+
-----+
018-01-03 | Fortinet Installer Client 5.6 DLL Hijacking | https://packetstormsecurity.com/files/145625/Fortinet-Installer-Client-5.6-DLL-Hijacking.html
+-----+
-----+
2018-01-02 | Fortinet FortiClient Windows Privilege Escalation | https://packetstormsecurity.com/files/145611/Fortinet-FortiClient-Windows-Privilege-Escalation.html
+-----+
-----+
2017-12-13 | Fortinet FortiClient VPN Credential Disclosure | https://packetstormsecurity.com/files/145397/Fortinet-FortiClient-VPN-Credential-Disclosure.html
+-----+
```

- The above query shows some serious vulnerabilities regarding firewall. Opening one of output links :

Fortinet FortiClient 5.2.3 Local Pri x https://packetstormsecurity.com/files/148811/Fortinet-FortiClient-5.2.3-Local-Privilege-Escalation.html

Home Files News About Contact Add New

Fortinet FortiClient 5.2.3 Local Privilege Escalation

Authored by [sickness](#), [mschenk](#) Posted Aug 5, 2018

Fortinet FortiClient version 5.2.3 (Windows 10 x64 Creators) suffers from a local privilege escalation vulnerability.

tags | exploit, local
systems | windows
advisories | [CVE-2015-4077](#), [CVE-2015-5736](#)
MD5 | [c481ba1c8cfdb5ac306d51bfefbf9590](#)

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

[Related Files](#)

Share This

[Like 0](#) [Tweet](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

Change Mirror [Download](#)

```
#include "stdafx.h"
#include <stdio.h>
#include <Windows.h>
#include <Psapi.h>
#include <Shlobj.h>

#pragma comment (lib,"psapi")

PULONGLONG leak_buffer = (PULONGLONG)VirtualAlloc((LPVOID)0x00000001a00000, 0x2000, MEM_RESERVE | MEM_COMMIT,
```

Follow us on Twitter [Follow us on Facebook](#) [Subscribe to an RSS Feed](#)

File Archive: February 2019 <

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

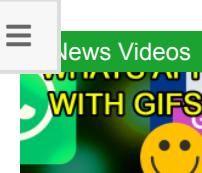
- Opening the links shows vulnerability of local privilege escalation. There are many vulnerabilities which can be used in further hacking activities.
- This tool can be used after Reconnaissance phase. For list of [Reconnaissance](#) tools & techniques please refer link over it.

(Visited 1,047 times, 1 visits today)

Share this...



LATEST VIDEOS



WHATSAPP HACKED USING JUST A GIF. UPDATE YOUR APP AS SOON AS POSSIBLE



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

[VIEW ALL](#)

POPULAR POSTS:



How to exploit new Facebook feature to access...



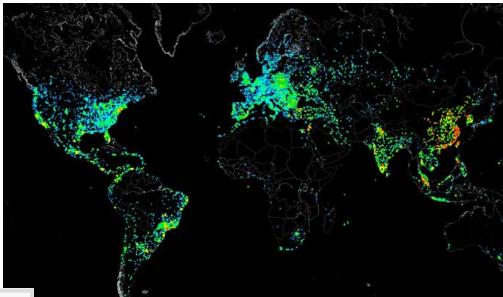
How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using...



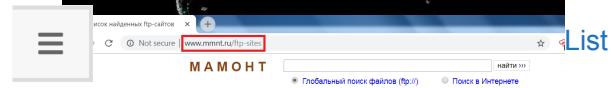
How to fake your phone number: Make it look like...



How to intercept mobile communications (calls and...



How to scan whole Internet 3.7 billion IP addresses...



List of all Open FTP Servers in the World

Список найденных ftp-сайтов



Hack Whatsapp account of your friend



CREATE YOUR OWN WORDLIST WITH CRUNCH

CRUNCH

- **PASSWORD CRACKING** Crack Windows password with john the ripper



```
r@debian:~$ sudo -l
List of user Defaults entries for user on this host:
env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
(root) NOPASSWD: /bin/echo
(root) NOPASSWD: /usr/bin/find
(root) NOPASSWD: /usr/bin/nano
(root) NOPASSWD: /usr/bin/vim
(root) NOPASSWD: /usr/bin/man
(root) NOPASSWD: /usr/bin/awk
(root) NOPASSWD: /usr/bin/less
(root) NOPASSWD: /usr/bin/ftp
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/sbin/apache2
(root) NOPASSWD: /bin/more
(root) NOPASSWD: /usr/bin/wget
user@debian:~$
```

How to exploit SUDO via Linux Privilege Escalation



How to Connect Android to PC/Mac Without WiFi



Do Hacking with Simple Python Script

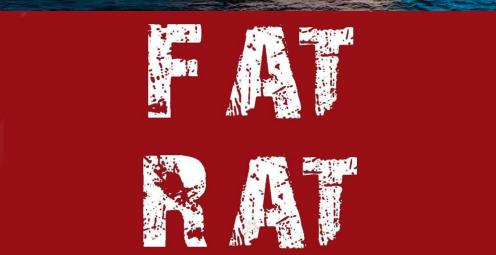
- Fake any website in seconds Facebook, Snapchat, Instagram :-



- Find Webcams, Databases, Boats in the sea using Shodan

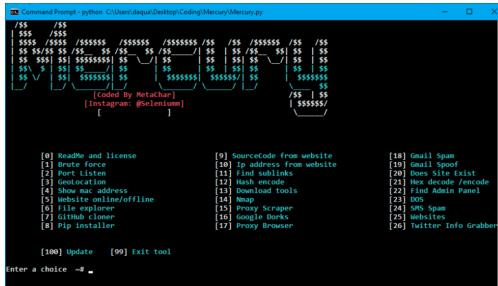


- Hack Windows, Android, Mac using TheFatRat (Step by...



- HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB



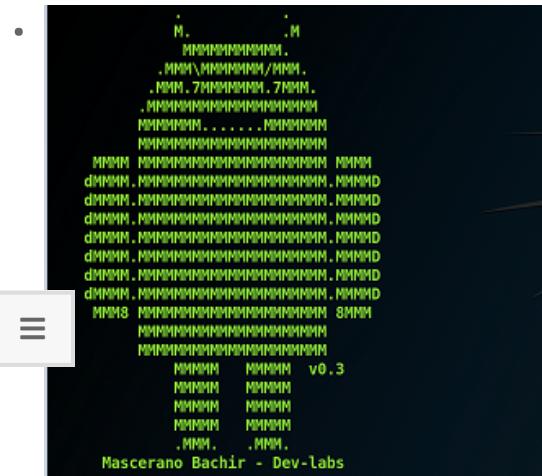


Hack any website with All in One Tool

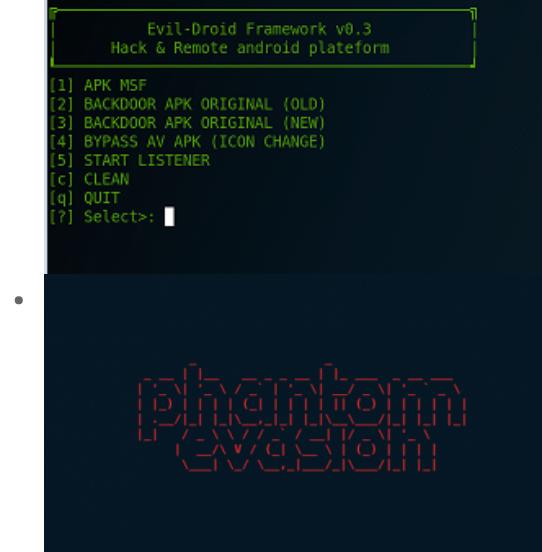
3

Create your own BotNet (Step By Step tutorial)





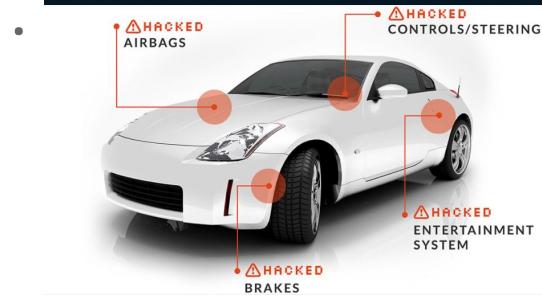
Generate Android App in 2 mins and hack any android mobile



Evil-Droid Framework v0.3
Hack & Remote android platform

[1] APK MSF
[2] BACKDOOR APK ORIGINAL (OLD)
[3] BACKDOOR APK ORIGINAL (NEW)
[4] BYPASS AV APK (ICON CHANGE)
[5] START LISTENER
[c] CLEAN
[q] QUIT
[?] Select>: █

Bypass antivirus detection With Phantom Payloads



How to hack any car with this tool



List of credit cards, proxies on Deep Web

• on Windows PowerShell

Extracting Hashes & Plaintext Passwords from Windows 10

```
PS C:\Windows\system32> .\Windows-Hash-Extractor.ps1 -ComputerName 192.168.1.10 -Administrator
```

The screenshot shows a Windows PowerShell window with the following text:

```
PS C:\Windows\system32> .\Windows-Hash-Extractor.ps1 -ComputerName 192.168.1.10 -Administrator
```

Administrator: The command is run with administrative rights on the computer.

PS C:\Windows\system32> Remote computer or local a dump file? 1

Administrator: The user and group (Administrator) has been added to the local users and groups for the specified computer. The local users and groups file has been added to the local computer settings.

PS C:\Windows\system32> 1

RECON-NG



recon-ng – Good tool for Information Gathering

• 2017 Edition



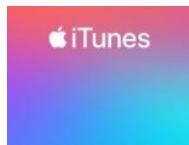
Best Hacking Tools Of 2017 For Windows, Linux, And OS X



CRITICAL VULNERABILITY IN CYBEROAM FIREWALL, BY SOPHOS: PATCH NOW AVAILABLE



MILLIONS OF HP LAPTOPS AND DESKTOPS ARE EASY TARGETS FOR HACKERS: NEW VULNERABILITIES ARE REPORTED



CRITICAL ITUNES VULNERABILITY EXPLOITED BY RANSOMWARE. UPDATE NOW



CRITICAL VULNERABILITY FOUND IN JOOMLA! UPDATE AS SOON AS POSSIBLE



PALO ALTO, FORTINET AND PULSE SECURE VPNS ARE VULNERABLE TO ATTACKS: NSA



CRITICAL FOXIT PDF READER VULNERABILITIES: UPDATE AS SOON AS POSSIBLE



PIXEL, HUAWEI, XIAOMI, OPPO, MOTOROLA AND SAMSUNG SMARTPHONES ARE EASILY HACKABLE; UPDATE ASAP. FULL LIST HERE



EXPERTS FOUND CRITICAL VULNERABILITY IN AIRCRAFT OPERATING SYSTEMS



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



CRITICAL VULNERABILITY AFFECTING CLOUD SERVERS: THOUSANDS OF SERVERS INFECTED



CRITICAL ROOT ACCESS VULNERABILITY ON CISCO DEVICES ALERT! PATCH IMMEDIATELY



ZERO-DAY VULNERABILITY IN VBUCKET EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED



XSRF VULNERABILITY IN PHPMYADMIN; THERE IS NO PATCH TO FIX THIS FLAW SO FAR



ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH



SECURE YOUR D-LINK & COMBA ROUTERS' PASSWORDS; CRITICAL VULNERABILITY FOUND



EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS



VIEW ALL

TUTORIALS



MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH



CYBERCRIMES SEXTORTION & REVENGEPORN, WHAT TO DO IF IT HAPPENS TO YOU?



HACK WIFI WITHOUT ROOTING ANDROID DEVICES



20 WAYS OF DOING SOCIAL PROTEST WITHOUT EXPOSING YOUR IDENTITY, JUST LIKE IN CHINA



FAKE TEXT MESSAGE ATTACK. HOW PRANK OR HACK YOUR FRIENDS WITH FAKE SMS BOMBER



SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



Google Hacking

HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I



CRACK ANY WIFI PASSWORD WITH WIFIBOOT



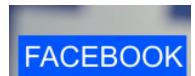
4 BROWSERS FOR SAFE ANONYMOUS SURFING



HOW TO CHECK IF SOMEONE IS SPYING ON YOUR MOBILE



BEST ANDROID APPS TO HACK WIFI NETWORKS



HACK YOUR FRIENDS FACEBOOK ACCOUNT USING HIDDEN EYE



ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART II

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART I

ALL-NEW WINDOWS EXPLOIT SUGGESTER IS HERE, WES-NG

ALL-NEW APP STORE FOR HACKERS, KALI NETHUNTER

TURN ANY ANDROID DEVICE INTO AN PENTESTING DEVICE

8 METHODS FOR BYPASSING SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

[VIEW ALL](#)



PAYING THE RANSOM OF A CYBERATTACK IS NOW LEGAL: FBI



ONTARIO GOVERNMENT HAD TO PAY HACKERS A \$75K USD RANSOM



DOWNLOAD THE FREE DECRYPTOR FOR YATRON, FORTUNECRYPT AND WANNACRYFAKE RANSOMWARE VARIANTS



MICROSOFT BANNED CCLEANER



A CALIFORNIA CITY SHUTS DOWN ALL OPERATIONS DUE TO VIRUS ATTACKS ON ITS GOVERNMENT SYSTEMS



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



FACEBOOK SUSPENDED THOUSAND OF APPS



UNINSTALL THESE ANDROID BEAUTY APPS RIGHT NOW !



MASSACHUSETTS TO PAY \$400K USD TO HACKERS DUE TO RANSOMWARE ATTACK



HOW CAPTCHA IS BEING USED TO BYPASS ANTI MALWARE SECURITY SCANS AND FIREWALLS



JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP



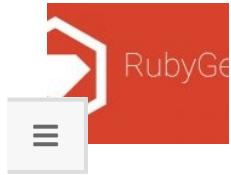
LILU, THE RECENTLY DISCOVERED AND DANGEROUS RANSOMWARE VARIANT



THE SCHOOL KID WHO HACKED OVER A MILLION IOT DEVICES



IDAHO SCHOOLS UNDER RANSOMWARE ATTACK. WILL RANSOMWARE MAKE AMERICA GREAT AGAIN?



STOP PROGRAMMING IN RUBY, APPLICATIONS USING RUBY LIBRARIES HAVE A BACKDOOR



YOU WANT TO MAKE MILLIONS IN FORTNITE? THIS VIDEOGAME HACKING TOOL IS A RANSOMWARE

[VIEW ALL](#)

CYBER SECURITY CHANNEL



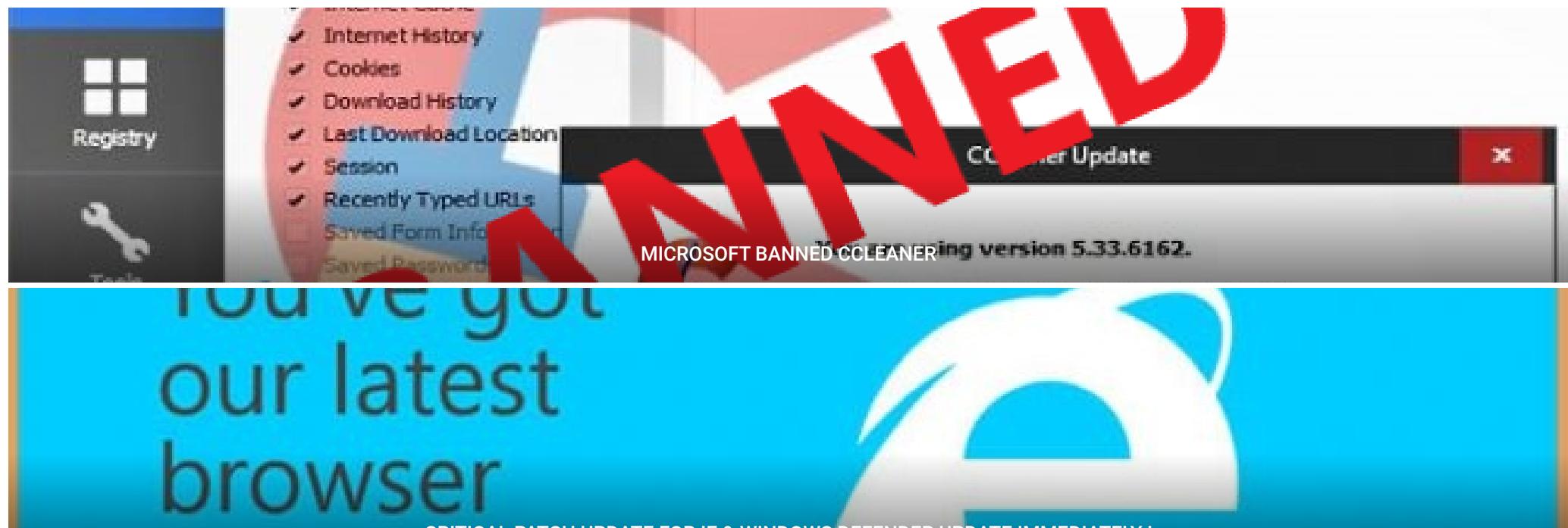
VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS



GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



FACEBOOK SUSPENDED THOUSAND OF APPS



SMS CRITICAL VULNERABILITY TO HACK ANY MOBILE



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP