INFORMATION SECURITY NEWSPAPER

FIND HACKED EMAIL ADDRESSES

Share this...

Data breaching in these days have been common. Many of the popular websites are targeted in data breach. This process of data breaching is still continue as many anonymous attackers are using open source tools. There is a popular tool called h8mail which is used to check breach mails.

According ethical hacking researcher of International Institute of Cyber Security h8mail is used in initial phase of penetration testing.

H8mail is an OSINT tool used to search emails and passwords. This tool find breached emails through different sites. This tool uses data breached emails. For showing you we have tested this tool on Kali Linux 2018.4

Before installing tool you must install nodejs and update python in Kali Linux. This tool only works with python3, according to ethical hacking courses.

- For installing python type **sudo apt-get update**

- Then type **sudo apt-get install python3**
- For checking python version type **python –version**
- Then type **sudo apt-get install nodejs**
- After installing all the above pre-requisites clone h8mail.
- For cloning type **git clone https://github.com/khast3x/h8mail.git**
- Type **cd h8mail**
- pe **pip install -r requirements.txt**

```
root@kali:/home/iicybersecurity/Downloads/h8mail# pip install -r requirements.txt
 Requirement already satisfied: requests in /usr/lib/python2.7/dist-packages (from -r requirements.txt (line 1)) (2.18.4)
 Collecting python-cli-ui (from -r requirements.txt (line 2))
   Downloading https://files.pythonhosted.org/packages/71/76/4772ff1c2c982c3e5cd75f5e01ae575adb979afc3473d267915de39813f4/python-cli-ui-0.7.4.tar.gz
     Complete output from command python setup.py egg_info:
     Error: Please upgrade to Python3
Command "python setup.py egg_info" failed with error code 1 in /tmp/pip-install-oC2WCX/python-cli-ui/
```

- While installing pip if it shows the above error that means you have to upgrade pip in your Linux Distros.
- For that type **sudo apt-get update python3-pip**

```
root@kali:/home/iicybersecurity/Downloads/h8mail# sudo apt-get install python3-pip
 Reading package lists… Done
 Building dependency tree
 Reading state information… Done
 python3-pip is already the newest version (18.1-4).
 The following packages were automatically installed and are no longer required:
   golang-1.10 golang-1.10-doc golang-1.10-go golang-1.10-src golang-src
 Use 'apt autoremove' to remove them.
 0 upgraded, 0 newly installed, 0 to remove and 1554 not upgraded.
```

- After upgrading pip, type **pip install -r requirements.txt**

```
root@kali:/home/iicybersecurity/Downloads/h8mail# pip3 install -r requirements.txt
 Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (2.18.4)
 Collecting python-cli-ui (from -r requirements.txt (line 2))
   Downloading https://files.pythonhosted.org/packages/fc/32/e63370450c69ccc06aefb8e55926011a7eeb3824787fed8d3d12149b4e
09/python_cli_ui-0.7.4-py3-none-any.whl
 Collecting cfscrape (from -r requirements.txt (line 3))
   Downloading https://files.pythonhosted.org/packages/ee/5e/6f36d5305b4c5abe793a7a057003f342300e9b853384a11fee8dc58e68
16/cfscrape-1.9.5.tar.gz
 Collecting unidecode (from python-cli-ui->-r requirements.txt (line 2))
   Downloading https://files.pythonhosted.org/packages/31/39/53096f9217b057cb049fe872b7fc7ce799a1a89b76cf917d9639e7a558
b5/Unidecode-1.0.23-py2.py3-none-any.whl (237kB)
     100% |████████████████████████████████| 245kB 576kB/s
 Requirement already satisfied: tabulate in /usr/lib/python3/dist-packages (from python-cli-ui->-r requirements.txt (li
ne 2)) (0.8.2)
 Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from python-cli-ui->-r requirements.txt (li
ne 2)) (0.3.7)
 Building wheels for collected packages: cfscrape
   Running setup.py bdist_wheel for cfscrape … done
   Stored in directory: /root/.cache/pip/wheels/4b/7d/70/32db6ba6ac95be8d24d5563436fc4ffe52f271adb2da153531
 Successfully built cfscrape
 Installing collected packages: unidecode, python-cli-ui, cfscrape
 Successfully installed cfscrape-1.9.5 python-cli-ui-0.7.4 unidecode-1.0.23
```

- Then type **python3 h8mail.py –help**

```
root@kali:/home/iicybersecurity/Downloads/h8mail# python3 h8mail.py --help
 usage: h8mail.py [-h] -t TARGET_EMAILS [-c CONFIG_FILE] [-o OUTPUT_FILE]
                  [-bc BC_PATH] [-v] [-l] [-k CLI_APIKEYS]


Email information and password finding tool

optional arguments:
   -h, --help            show this help message and exit
   -t TARGET_EMAILS, --targets TARGET_EMAILS
                         Either single email, or file (one email per line).
                         REGEXP
   -c CONFIG_FILE, --config CONFIG_FILE
                         Configuration file for API keys
   -o OUTPUT_FILE, --output OUTPUT_FILE
                         File to write output
   -bc BC_PATH, --breachcomp BC_PATH
                         Path to the breachcompilation Torrent.

https://ghostbin.com/paste/2cbdn
   -v, --verbose         Show debug information
   -l, --local           Run local actions only
   -k CLI_APIKEYS, --apikey CLI_APIKEYS
                         Pass config options. Format is "K:V,K:V"
```

- The above queries are used to gather breached email addresses and passwords.

H8MAIL USES VARIOUS APIS TO SEARCH FOR BREACHED EMAIL ADDRESSES :-

- HaveIBeenPwned (**https://haveibeenpwned.com/)** : This website checks if the email id has been pwned or not. This website collects large no, of databases dumps and paste containing information about all billions of leak accounts.
- Shodan **(https://www.shodan.io/)** : Shodan is an search engine for web. This website pings all the available IP address that are currently using the internet.
- Hunter.io **(https://hunter.io/)** : Hunter is an source of h8mail. In hunter is used to find and verify professional email address. For using these services you have to y some of the amount in hunter.io
- eleakinfo **(https://weleakinfo.com/api/public)** : Weleakinfo is another breached database search engine.
- Snusbase **(https://snusbase.com/)** : Snusbase is a database search engine which collects data of sites that have been hacked. And provide those data to their users. For using these services you have to pay some of the amount in snusbase.

FINDING BREACHED EMAIL ADDRESS :-

- Type **python3 h8mail.py -t puti@reddcoin2.com**
- **-t** is used to enter target email address.

```
root@kali:/home/iicybersecurity/Downloads/h8mail# python3 h8mail.py -t puti@reddcoin2.com

.. ..      ;;
     | .. | | .. |     ; h8mail.py ;     | !| |||! |     ;------------;     !| |_!  Heartfelt Email OSINT
     .||| |.   Use responsibly etc
     | .| |. | ;____________;
     | !! | | !! | ; github.com/khast3x ;
     !! !! ;--------------------;

Targets

=> puti@reddcoin2.com

```

```
Lookup Status

Result puti@reddcoin2.com

=> not breached ✗
 Target hostname: reddcoin2.com

✔ Done
```

- The above query shows, email which has been scanned is not breached of any databases mentioned above.
- It shows that HIBP (HaveIBeenPwned) could not find email address in any database. Nor its password is available in HIBP database.

FIND BULK EMAIL IDS FOR TESTING:-

- For getting bulk email addresses. You can use TheHarvester is a popular tool to find mail addresses or details of the employees.

```
root@kali:/home/iicybersecurity/Downloads# theharvester -d testsites.com -b pgp


Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's d
ocumentation for more information.


*
|  ||  |_    _    /\  /__ _ _ _      |  |_  _ __   *
|  |  '_ \ / _ \  / // / ` | '\ \ / / _ \/ | / _ \ '__| *
|  ||  | | |  / /   / (| | |   \ V /  /__ \ ||  / |     *
__|| ||___| \/ // _,||    _/ ___||/__|_|     *
```

```
*
TheHarvester Ver. 2.7.2                                          *
Coded by Christian Martorella                                    *
Edge-Security Research                                           *
cmartorella@edge-security.com                                    *


[-] Starting harvesting process for domain: testsites.com

[-] Searching in PGP key server..

Harvesting results

[+] Emails found:
mariot.chauvin@testsites.com
 lauren.emms@testsites.com
 danny.daly@testsites.com
 amy.hughes@testsites.com
 jon.norman@testsites.com
 tom.forbes@testsites.com
 niko.kommenda@testsites.com
 sam.jones@testsites.com
 regis.kuckaertz@testsites.com
 hannah.devlin@testsites.com
 joseph.smith@testsites.com
 calum.campbell@testsites.com
 jacob.riggs@testsites.com
 michael.barton@testsites.com
```

```
akash.askoolum@testsites.com
peter.colley.freelance@testsites.com
nicolas.long@testsites.com
alex.hern@testsites.com
thomas.bonnin@testsites.com
richard.tynan@testsites.com
at.heywood@testsites.com
nathaniel.bennett@testsites.com
sally.goble@testsites.com
jennifer.sivapalan@testsites.com
michael.safi@testsites.com
justin.pinner@testsites.com
jonathan.soul@testsites.com
jasper.jackson@testsites.com
oliver.holmes@testsites.com
hilary.osborne@testsites.com
rupert.bates@testsites.com
caelainn.barr@testsites.com
christopher.lloyd@testsites.com
susie.coleman@testsites.com
chris.whitworth@testsites.com
andi.elsner@testsites.com
calla.wahlquist@testsites.com
paul.farrell@testsites.com
james.gorrie@testsites.com
simon.bowers@testsites.com
```

- The above is the list of the email addresses which can be used in scanning if the above email addresses are breached or not.

- Save the above list. Type **nano emaillist.txt**
- Then copy paste whole email addresses. Then save the list.
- Type **python3 h8mail.py -t /home/iicybersecurity/Downloads/testsites.txt -bc /Downloads/breachcompilation/ -k “snusbase_url: http://snusbase.com ,snusbase_token: 5sxxxxxxxxxxxxxxxxxxxxBuXQ”**
- **-t** is used to enter tartgets.
- **-bc** is used to give path for pwned targets.
- is used to enter snusbase API key.

```
root@kali:/home/iicybersecurity/Downloads/h8mail# python3 h8mail.py -t /home/iicybersecurity/Downloads/testsites.txt -b
c /Downloads/breachcompilation/ -k "snusbase_url: http://snusbase.com ,snusbase_token: 5sxxxxxxxxxxxxxxxxxxxxBuXQ"

.. ..     ;;
     | .. | | .. |     ; h8mail.py ;     | !| |||! |     ;------------;     !| |_!  Heartfelt Email OSINT
     .||| |.   Use responsibly etc
     | .| |. | ;____________;
     | !! | | !! | ; github.com/khast3x ;
     !! !! ;--------------------;

Targets
mariot.chauvin@testsites.com
  lauren.emms@testsites.com
  danny.daly@testsites.com
  amy.hughes@testsites.com
  jon.norman@testsites.com
  tom.forbes@testsites.com
  niko.kommenda@testsites.com
  sam.jones@testsites.com
  regis.kuckaertz@testsites.com
```

```
hannah.devlin@testsites.com
joseph.smith@testsites.com
calum.campbell@testsites.com
jacob.riggs@testsites.com
michael.barton@testsites.com
akash.askoolum@testsites.com
peter.colley.freelance@testsites.com
nicolas.long@testsites.com
alex.hern@testsites.com
thomas.bonnin@testsites.com
richard.tynan@testsites.com
mat.heywood@testsites.com
nathaniel.bennett@testsites.com
sally.goble@testsites.com
jennifer.sivapalan@testsites.com
michael.safi@testsites.com
justin.pinner@testsites.com
jonathan.soul@testsites.com
jasper.jackson@testsites.com
oliver.holmes@testsites.com
hilary.osborne@testsites.com
rupert.bates@testsites.com
caelainn.barr@testsites.com
christopher.lloyd@testsites.com
susie.coleman@testsites.com
chris.whitworth@testsites.com
andi.elsner@testsites.com
calla.wahlquist@testsites.com
```

```
paul.farrell@testsites.com
james.gorrie@testsites.com
simon.bowers@testsites.commariot.chauvin@testsites.com
lauren.emms@testsites.com
danny.daly@testsites.com
amy.hughes@testsites.com
jon.norman@testsites.com
tom.forbes@testsites.com
niko.kommenda@testsites.com
sam.jones@testsites.com
regis.kuckaertz@testsites.com
hannah.devlin@testsites.com
joseph.smith@testsites.com
calum.campbell@testsites.com
jacob.riggs@testsites.com
michael.barton@testsites.com
akash.askoolum@testsites.com
peter.colley.freelance@testsites.com
nicolas.long@testsites.com
alex.hern@testsites.com
thomas.bonnin@testsites.com
richard.tynan@testsites.com
mat.heywood@testsites.com
nathaniel.bennett@testsites.com
sally.goble@testsites.com
jennifer.sivapalan@testsites.com
michael.safi@testsites.com
justin.pinner@testsites.com
```

```
   jonathan.soul@testsites.com
   jasper.jackson@testsites.com
   oliver.holmes@testsites.com
   hilary.osborne@testsites.com
   rupert.bates@testsites.com
   caelainn.barr@testsites.com
   christopher.lloyd@testsites.com
   susie.coleman@testsites.com
   chris.whitworth@testsites.com
   andi.elsner@testsites.com
   calla.wahlquist@testsites.com
   paul.farrell@testsites.com
   james.gorrie@testsites.com
   simon.bowers@testsites.com

=========== SNIPPED =================
```

- The above query shows that above email addresses has not been in data breach in HIBP.
- If you see snusbase error, it means you have to purchase their services to search in their database.

USING SINGLE QUERY :-

- Type **python3 h8mail.py -t targets.txt -c config.ini -o pwned_targets.csv**
- **-t** is used to select target file. You have to create target.txt file.
- **-c** is used to select config file where APIs has been entered.
- **-o** is used where data will be saved in .csv form.

```
root@kali:/home/iicybersecurity/Downloads/h8mail#
python3 h8mail.py -t targets.txt -c config.ini -o pwned_targets.csv
 tuckerkaren2000@yahoo.com
 tuckersadie@yahoo.com
 tucko100@yahoo.com
 tucktunes@yahoo.com
  ucsonclint2008@yahoo.com
 tucu.ionut@yahoo.com

 Lookup Status
 ======== SNIPPED ===============
```

- If the email addresses has been pwned data breach.
- This information can be used in other hacking activities, mention ethical hacking teachers.

(Visited 1,999 1 times)

Share this...

BY: JIM GILL / ON: JANUARY 16, 2019 / IN: RECONNAISSANCE, SCANNING, TUTORIALS / TAGGED: DATA BREACH, EMAIL ADDRESSES AND PASSWORDS, EMAIL SCANNING, H8MAIL, SCANNING

FOLLOW & LIKE US

Follow Like

LATEST VIDEOS

POPULAR NEWS VIDEO 10 JULY

POPULAR NEWS VIDEO 9 JULY

VIEW ALL

POPULAR POSTS

HOW TO EXPLOIT NEW FACEBOOK FEATURE TO ACCESS...

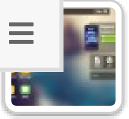
HOW TO HACK WI-FI: CRACKING WPA2-PSK PASSWORDS USING...

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

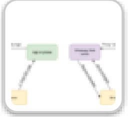


HOW TO CONNECT ANDROID TO PC/MAC WITHOUT WIFI

CRACK WINDOWS PASSWORD WITH JOHN THE RIPPER

CREATE YOUR OWN WORDLIST WITH CRUNCH

HOW TO EXPLOIT SUDO VIA LINUX PRIVILEGE ESCALATION



HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB

FIND WEBCAMS, DATABASES, BOATS IN THE SEA USING SHODAN

DO HACKING WITH SIMPLE PYTHON SCRIPT

EXTRACTING HASHES & PLAINTEXT PASSWORDS FROM WINDOWS 10

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

HOW TO HACK ANY CAR WITH THIS TOOL

BEST HACKING TOOLS OF 2017 FOR WINDOWS, LINUX, AND OS X

FAKE ANY WEBSITE IN SECONDS FACEBOOK, SNAPCHAT, INSTAGRAM :-

HACK WINDOWS, ANDROID, MAC USING THEFATRAT (STEP BY…

HACKSPY TROJAN EXPLOIT

PIRATED SMASH BROS. ULTIMATE COPY FOR SALE IN MEXICO…

PORNHUB AND ITS METHOD TO BYPASS INDIA’S PORN SITES BAN

BYPASS ANTIVIRUS DETECTION WITH PHANTOM PAYLOADS

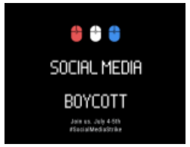
EXPLOITING PYTHON CODE INJECTION IN WEB APPLICATIONS

HACK ANY WEBSITE WITH ALL IN ONE TOOL

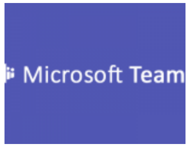
VULNERABILITIES

INTEL DATA CENTER SSD DRIVES ALLOW HACKERS TO TAKE COMPLETE CONTROL OF SERVERS

APPLE WATCH VULNERABILITY ALLOWS YOU TO SPY ON YOUR FRIENDS’ IPHONE



THIS PGP BUG COULD ALLOW HACKERS TO CONTROL YOUR EMAIL SERVERS



VULNERABILITY IN MICROSOFT TEAMS COULD ALLOW HACKER TO GAIN COMPLETE CONTROL OF YOUR INFRASTRUCTURE

ORIGIN, AN EA PLATFORM, EXPOSES DATA OF 300 MILLION USERS

FAKE EMERGENCY ALERTS ARE LAUNCHED VIA VULNERABILITY IN LTE

A HACKER PUBLISHED A NEW IOS JAILBREAK13 WITH TFP0 EXPLOIT

DELL LAPTOPS ARE NOT SECURE; ANOTHER VULNERABILITY IN DELL SOFTWARE

CISCO DNA ALLOWED UNAUTHORIZED USERS ACCESS TO ENTERPRISE NETWORKS FOR A LONG TIME

ANOTHER ZERO DAY FOUND IN MOZILLA FIREFOX IT’S CAUSING UNREST AMONG TOR USERS

CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

CRITICAL FIREFOX VULNERABILITY, UPDATE MOZILLA IMMEDIATELY

NEW VULNERABILITIES FOUND ON LINUX AND FREEBSD DEVICES

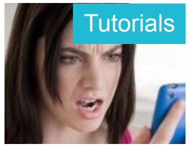
HACKERS EXPLOIT VULNERABILITY TO MALICIOUSLY ALTER MEDICAL DEVICES

EVERNOTE EXTENSION FOR CHROME VULNERABILITY ALLOWS CONFIDENTIAL INFORMATION THEFT

NEW ZERO-DAY CRYPTOGRAPHIC VULNERABILITY FOUND IN WINDOWS 10

VIEW ALL

TUTORIALS



HOW TO CHECK IF YOUR MOBILE PHONE IS HACKED OR NOT?

CHECK IF YOUR WHATSAPP IS HACKED OR NOT ?

HOW TO ANALYZE USB TRAFFIC

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

Configuring update for Windows 10
5% complete
Do not turn off your computer
ble Windows 10 Updates & Defen

HAVING PROBLEM WITH WINDOWS 10 UPDATES? DISABLE IN 2 MINUTES

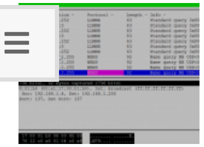
CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

HOW TO OPEN UNKNOWN FILES THAT HAVE MALWARE IN WINDOWS 10 WITH SANDBOX

KILLSHOT TO HACK ANY WEBSITE

TALK SECRETLY WITH YOUR FRIENDS – EVERYTHING ABOUT STEGANOGRAPHY

SOLUTION TO SPAMMING, CHECK ANY UNKNOWN EMAIL ID EXISTENCE

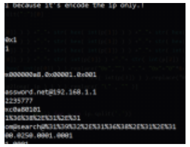


LIGHT WEIGHT PACKETS ANALYZER IS HERE!

SMART WAY OF DISCOVERING COMPUTER ON NETWORK USING ARPING

TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY

FIND DETAILS OF ANY MOBILE NUMBER, EMAIL ID, IP ADDRESS IN THE WORLD (STEP BY STEP)



CONVERT ANY MALICIOUS IP INTO URL TO HACK YOUR FRIEND

SEND FAKE MAIL TO HACK YOUR FRIENDS

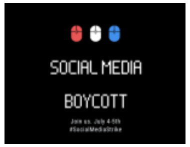
TOP 6 HACKING MOBILE APPS – MUST HAVE

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

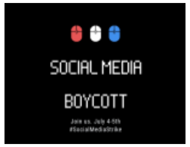
VIEW ALL

MALWARE

MORE THAN 25 MILLION SMARTPHONES INFECTED WITH NEW MALWARE HIDDEN IN WHATSAPP



NEW RANSOMWARE INFECTS WINDOWS MACHINES EVEN WITHOUT CLICKING OR OPENING AN EMAIL

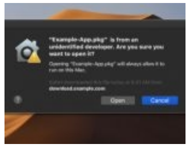


HACKERS EARN MILLIONS WITH THIS ATM CASHOUT MALWARE

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

FACEBOOK PAGES INFECTING THOUSANDS OF USER WITH VIRUS

YOU CAN HACK BANKS WITH THIS MICROSOFT EXCEL ATTACK



"Example-App.pkg" is from an unidentified developer. Are you sure you want to open it?

Opening "Example-App.pkg" will always allow it to run on this Mac.

[illegible]
download.example.com

NEW VULNERABILITY ON MAC IS EXPLOITED WITH MALWARE

PLUROX, THE ALL-IN-ONE MALWARE INFECTING COMPUTERS AROUND THE WORLD

NEW TOOL TO REMOVE GANDCRAB RANSOMWARE ENCRYPTION

YOUR IOT DEVICES, SUCH AS CAMERAS, WASHING MACHINES, NAS STORAGE WILL BE AFFECTED BY THIS NEW MALWARE

CYBERATTACKS AGAINST GAMER COMMUNITY KEEP GROWING

COMPANIES WITH ORACLE WEBLOGIC MUST BE CAREFUL; CRYPTOMINING MALWARE AFFECTS SERVERS

FIRST IT WAS BALTIMORE, NOW PHILADELPHIA IS UNDER MALWARE ATTACK

TWENTY YEARS IN PRISON FOR HACKERS/FOUNDERS OF MARIPOSA BOTNET AND BITCOIN PLATFORM NICEHASH

A HACKER TRICK GOOGLE TO INSTALL A BACKDOOR ON ANDROID PHONES AROUND THE WORLD; HOW DID HE DO IT?

SPECIALISTS DETECT NEW AND DANGEROUS CRYPTOCURRENCY MINING MALWARE IN ASIA AND U.S.

SOURCE CODE OF TOOLS USED BY MALICIOUS HACKERS FROM IRAN IS EXPOSED

VIEW ALL

CYBER SECURITY CHANNEL

≡

POPULAR NEWS VIDEO 9 JULY

POPULAR NEWS VIDEO 7 JULY

≡

POPULAR NEWS VIDEO 5 JULY

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY

How to hack WhatsApp
There is an app which allows to Hack upto 10 WhatsApp Account
3:39 PM
WHATSAPP
HACK

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

WIPRO IS HACKED!

CONTACT US