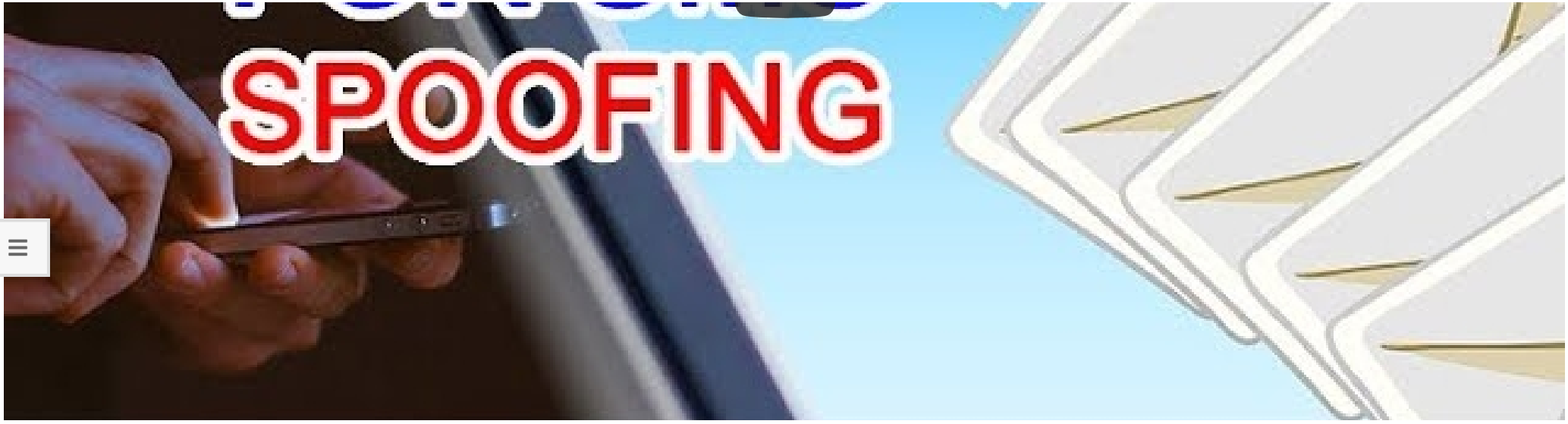
CRACK WINDOWS PASSWORD WITH JOHN THE RIPPER



JOHN THE RIPPER:- John the ripper is a password cracker tool, which try to detect weak passwords. John the ripper can run on wide variety of passwords and hashes. This tool is also helpful in recovery of the password, in care you forget your password, mention ethical hacking professionals.

John the ripper is popular because of the dictionary attacks & is mainly is used in bruteforce attacks. Ethical hacking researcher of iicybersecurity said this method is useful because many old firms still uses the windows old versions which is not good in terms of cybersecurity.

CRACKING THE WINDOWS:-

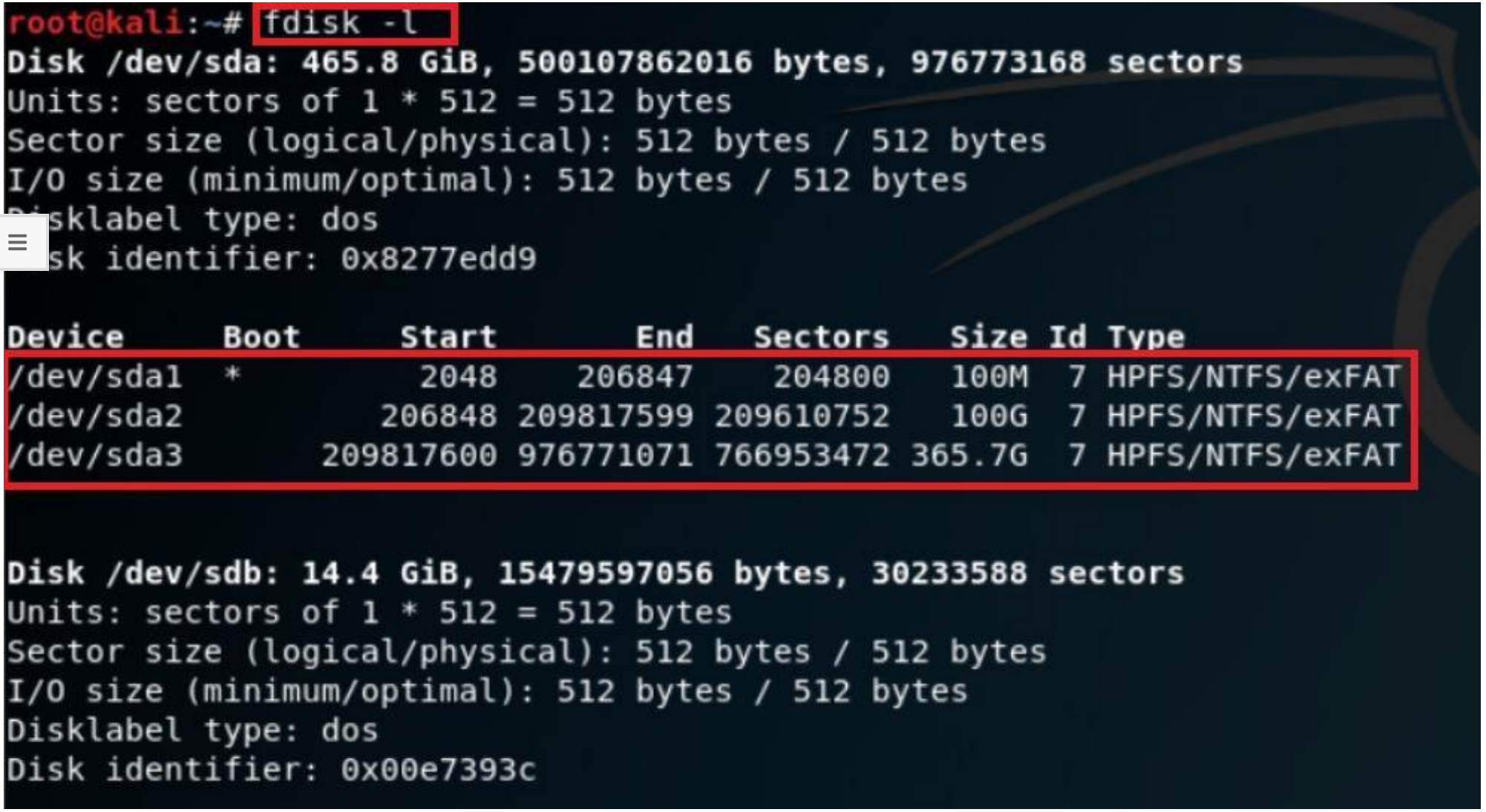
In windows, password is typically stored in **SAM** file in **%SystemRoot%\system32\config.** Windows uses the **NTLM hash**. During the boot time the hashes from the SAM file gets decrypted using SYSKEY and hashes is loaded in registry which is then used for authentication purpose, according to ethical hacking courses.

Windows does not allow users to copy the **SAM** file in another location so you have to use another OS to mount windows over it and copy the **SAM** file. Once the file is copied we will decrypt the SAM file with SYSKEY and get the hashes for breaking the password.

In below case we are using **Kali Linux OS** to mount the windows partition over it.

- For making the bootable disk you can use **rufus** freeware which is available here: https://rufus.ie/en_IE.html
- This freeware is very easy to use. You simply have to select Kali linux iso image for making bootable disk.
- After creating the boot disk. Simply boot with bootable disk and follow steps as mentioned below:
- First you have to check the hard disk partition that where is the windows is installed. For that type **fdisk -l.**

CHECKING THE HARD DISK PARTITIONS:-



- In the above screen shot, after executing the query the command has shown 3 partitions of the target hard disk. By looking at size of partition you can know that where the target OS (Windows) in installed.

MOUNT:-

- Type **mkdir /mnt/CDrive** for creating the directory.
- For mounting the hard disk partition **/dev/sda2** to **CDrive** directory, type **mount /dev/sda2 /mnt/tmp/CDrive**
- Then for checking the mount point. Type **ls -ltr /mnt/tmp/CDrive**
- Type **mount** to check the mounted drive

```
root@kali:~/temp# mount

sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)

proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)

udev on /dev type devtmpfs (rw,nosuid,relatime,size=2042548k,nr_inodes=201161,mode=755)

devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)

tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=412292k,mode=755)

/dev/sdb1 on /run/live/medium type vfat (ro,noatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,
utf8,errors=remount-ro)

/dev/loop0 on /run/live/rootfs/filesystem.squashfs type squashfs (ro,noatime)

tmpfs on /run/live/overlay type tmpfs (rw,noatime,size=2061444k,mode=755)

overlay on / type overlay (rw,noatime,lowerdir=/run/live/rootfs/filesystem.squashfs/,upperdir=/run/live/overlay/rw,work
dir=/run/live/overlay/work)

tmpfs on /usr/lib/live/mount type tmpfs (rw,nosuid,noexec,relatime,size=412292k,mode=755)
```

```
/dev/sdb1 on /usr/lib/live/mount/medium type vfat (ro,noatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro)

/dev/loop0 on /usr/lib/live/mount/rootfs/filesystem.squashfs type squashfs (ro,noatime)

pfs on /usr/lib/live/mount/overlay type tmpfs (rw,noatime,size=2061444k,mode=755)

securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)

tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)

tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)

cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)

cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)

pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)

bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)

cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)

cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
```

```
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)

cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)

cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)

roup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)

cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)

cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)

cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)

systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=34,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe
_ino=16732)

hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)

mqueue on /dev/mqueue type mqueue (rw,relatime)

debugfs on /sys/kernel/debug type debugfs (rw,relatime)

tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)

binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)

tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=412288k,mode=700)
```

```
gvfsd-fuse on /run/user/0/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=0,group_id=0)

fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
```

```
/dev/sda2 on /mnt/CDrive type fuseblk (rw,relatime,user_id=0,group_id=0,allow_other,blksize=4096)
```

- In the above output, last line shows that target hard disk partition has been mounted to **CDrive** directory.

COPYING THE SAM FILE:-

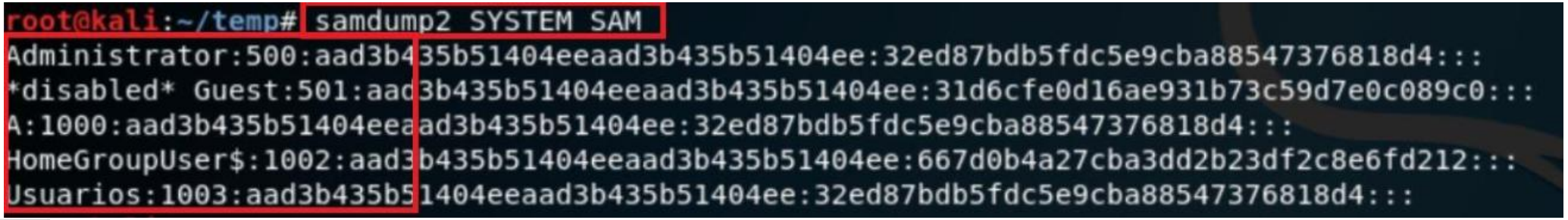
- Type **mkdir /tmp/temp**
- Type **cp /mnt/CDrive/Windows/System32/config/SAM /tmp/temp**

SAM FILE:-

- **Samdump2** fetches the SYSKEY and extract hashes from windows SAM file.
- For installing the **samdump2** type **sudo apt-get update** after then type **sudo apt-get install samdump2.**

COPYING THE SYSTEM FILE:-

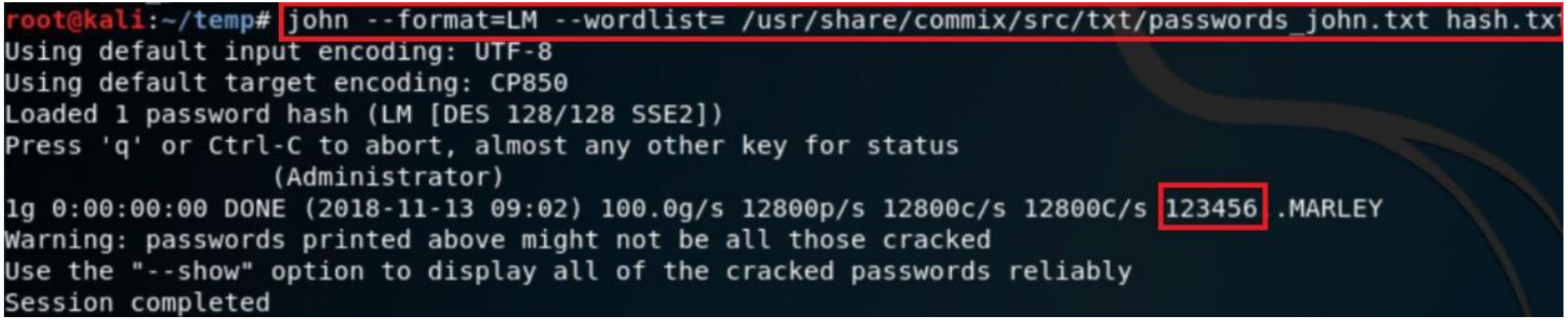
- Now copy the SYSKEY file, type **cp /mnt/CDrive/Windows/System32/config/SYSTEM /tmp/temp**
- Type **samdump2 SYSTEM SAM**



- In the above screen shot, after executing samdump2. The **samdump2** will show the hashes in **SAM** files. In the next red marked there are 4 users on the target system.
- Now type **samdump2 SYSTEM SAM > hash.txt** for redirect the hash output to a file named **hash.txt**.

CRACKING PASSWORD USING JOHN THE RIPPER:-

- Type **john –format=LM –wordlist=/root/usr/share/john/password_john.txt hash.txt**



- In the above screen shot after executing above query. The wordlist will be used to crack the password. As shown above the current password for the target **OS** is **123456.**
- Attacker can also use his own **wordlist** for cracking the password. In kali linux many wordlists are available that can be used in cracking. For using the kali linux wordlist go to -> /**usr/share/wordlists/**

NOTE:- The above method will work till WINDOWS 7 Operating system. It will not work on WINDOWS 8/8.1/10

BY: JIM GILL / ON: NOVEMBER 27, 2018 / IN: NETWORK TOOLS, TUTORIALS / TAGGED: CRACK WINDOWS PASSWORD, JOHN THE RIPPER

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?

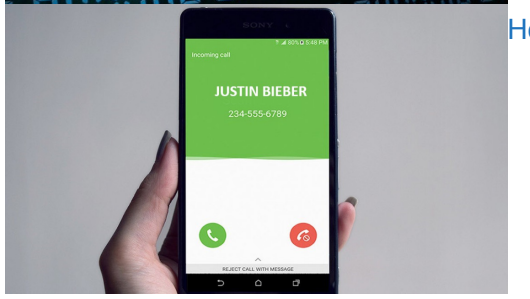
WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

VIEW ALL

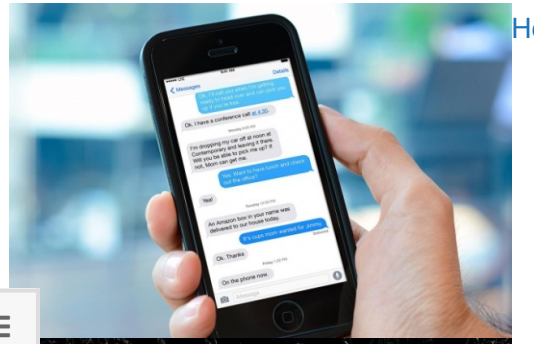
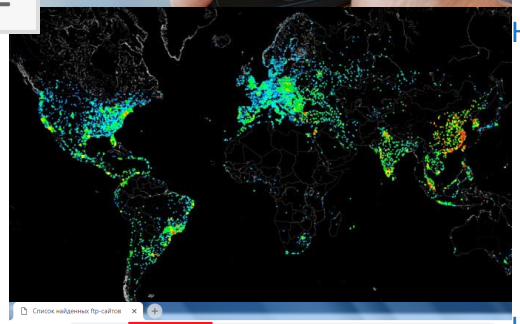
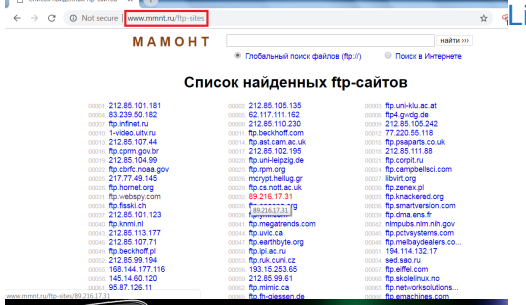
POPULAR POSTS:

- 

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…
- 

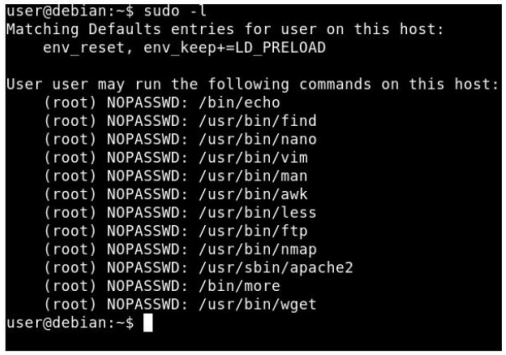
  List of all Open FTP Servers in the World
- 

  Hack Whatsapp account of your friend

- 

CREATE YOUR OWN WORDLIST WITH CRUNCH

Crack Windows password with john the ripper

- 

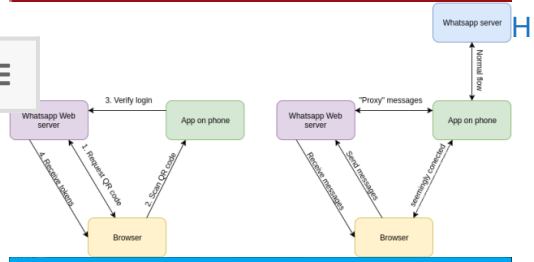
How to exploit SUDO via Linux Privilege Escalation

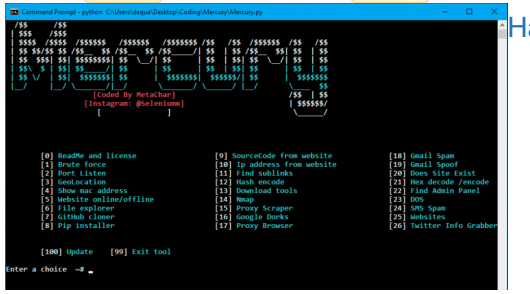
- 
  How to Connect Android to PC/Mac Without WiFi
- 

  Do Hacking with Simple Python Script
- 

  Fake any website in seconds Facebook, Snapchat, Instagram :-
- 
  Find Webcams, Databases, Boats in the sea using Shodan

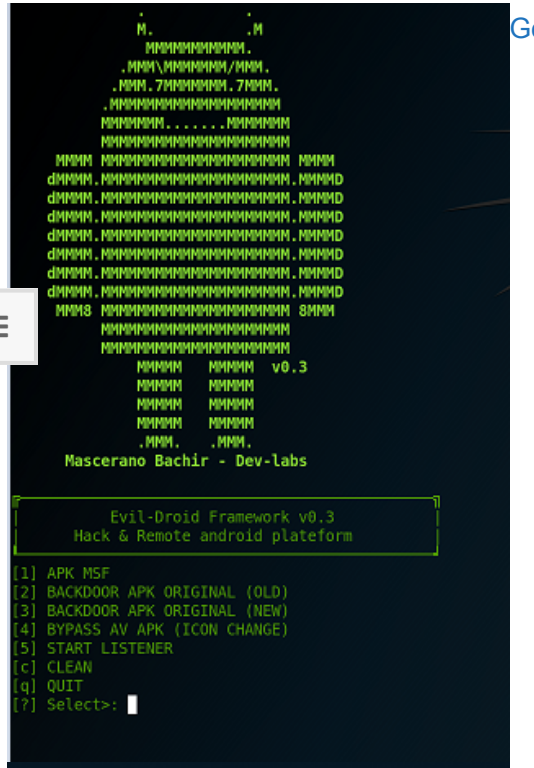
- 

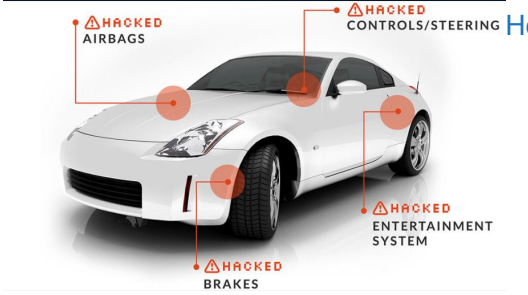
Hack Windows, Android, Mac using TheFatRat (Step by…
- 

HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB
- 

Hack any website with All in One Tool
- 

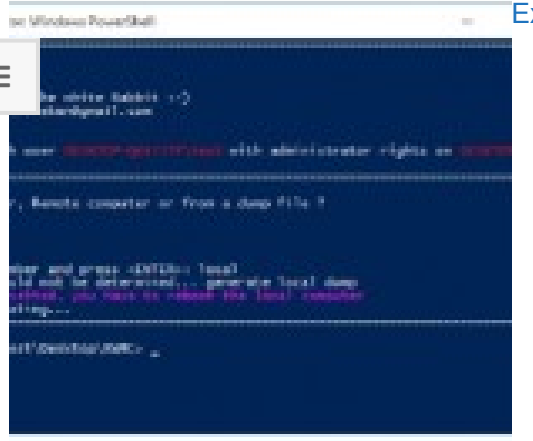
Create your own BotNet (Step By Step tutorial)

- 

Generate Android App in 2 mins and hack any android mobile
- 
Bypass antivirus detection With Phantom Payloads
- 

How to hack any car with this tool

- 

List of credit cards, proxies on Deep Web
- 
Extracting Hashes & Plaintext Passwords from Windows 10
- 

recon-ng – Good tool for Information Gathering
- 

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

VULNERABILITIES

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 VBULLETIN EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED

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

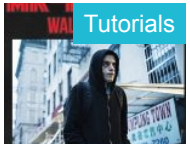
ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH

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

EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS

VIEW ALL

TUTORIALS



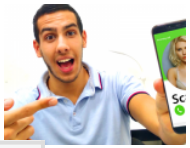
MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH

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

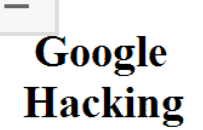
HACK WIFI WITHOUT ROOTING ANDROID DEVICES

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



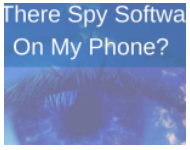
SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I

CRACK ANY WIFI PASSWORD WITH WIFIBROOT

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 HIDDENEYE

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

MALWARE

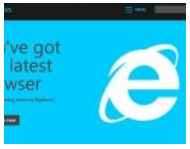
PAYING THE RANSOM OF A CYBERATTACK IS NOW LEGAL: FBI

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

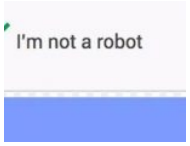


CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !

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

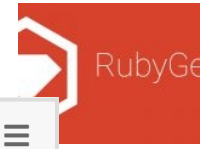
JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS

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