Kali Linux

G. Filosofi 2019
https://www.kali.org

khost: kalisabu
kp: l0pht69

- Kali Linux is a Debian GNU/Linux distribution enabling security professionals and IT administrators to conduct advanced penetration testing, forensic analysis, security auditing, reverse engineering
- Kali Linux is a rolling distribution, which means that *you will receive updates every single day*
- Since many tools included in Kali Linux can only be executed with root privileges, this is the default Kali user account
- Kali Linux disables any installed service that would listen on a public network interface by default, such as HTTP and SSH. You can still manually enable any services with
  host $ systemctl enable <service>
  or
  host $ /etc/init.d/<service> start
  Example
  host $ /etc/init.d/apache2 start
  host $ /etc/init.d/apache2 status
  host $ /etc/init.d/apache2 restart
  host $ /etc/init.d/apache2 stop
- The best for a corporate environment is to use a encrypted bootable USB drive loaded with Kali Linux
- Persistence: changes will be retained across reboots. look at https://docs.kali.org/downloading/kali-linux-live-usb-persistence to add persistency
- Suggested 64GB USB stick

Creating bootable USB Live ISO

download ISO image from https://www.kali.org/downloads/
kali-linux-2019.2-amd64.iso
cd into directory hosting the ISO image
host $ cd <kaliiso>
check the hash is correct
host $ sha256sum kali-linux-2019.2-amd64.iso
Plug the USB Drive stick and check the peripheral node (be /dev/sdb)
make sure sdb is unmounted
copy ISO image over the USB stick
$ sudo dd if=kali-linux-2019.2-amd64.iso of=/dev/sdb
Note: this command will take more than half an hour.
Note: for a macOS host you need to add the parameter bs=1M
Now the USB stick is recognized as /dev/sdb and contains partitions sdb1 and sdb2. sdb2 contains the ISO image which takes about 3.2GB.

Add Persistency:

To add persistency we need to create a new partition to store our persistent data into, starting right above the second Kali Live partition, put an ext4 file system onto it, and create a persistence.conf file on the new partition
Check the starting configuration
$ sudo parted /dev/sdb print
Ceate a start variable with the actual size of the kali image
$ sudo start=$(du --block-size=1MB kali-linux-2019.2-amd64.iso | awk '{print $1}')

$ sudo echo ”Size of image is $start MB”
Size of image is 3354 MB
Resize sdb2 just to store the ISO image and create the new partition
$ sudo parted -a optimal /dev/sdb mkpart primary ”${start}MB” 100%
Check the new configuration
$ sudo parted /dev/sdb print
Format sdb3
$ sudo mkfs.ext4 -L persistence /dev/sdb3
Mount sdb3 and creating the pesistence.conf file
$ sudo mount /dev/sdb3 /mnt
$ sudo touch /mnt/pesistence.conf
$ sudo vim /mnt/pesistence.conf
Add ”/ union”, save and quit
Note: such avspecial value will enable full persistence for all directories
When rebooting, select Live USB Persistance

Reboot

Check machine info
kali $ uname -a
Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64 GNU/Linux
Change screen timeout and keyboard layout

Upgrade the system (it takes 2 days!!)

kali $ apt update
kali $ apt upgrade

Change password

To change a password
kali $ passwd
when prompted enter your old password (toor) and then a new password

A DVD with burned Kali
host: an Internet-connected computer, DVD player, and USB bootable, 8 GB of RAM. Ubuntu

or Debian OS is recommended.
The Kali Linux ISO that matches your workstation architecture (32 or 64 bit)

- Steps
  - Pick the Graphic Install from the menu
  - Set hostname, domain name (filosofi.net), root password
  - Pick Guided – Use entire disk and set up encrypted LVM
  - Pick the USB disk and click on Continue to start partitioning
  - Set the passphrase (long and plain)
  - reboot the live USB (with persistance) and login

  - Go to Applications > Accessories > Terminal

host $ apt-get update && apt-get -y upgrade

  - Press *Alt+F2*. Type “terminal” in the field, and click OK

Gedit

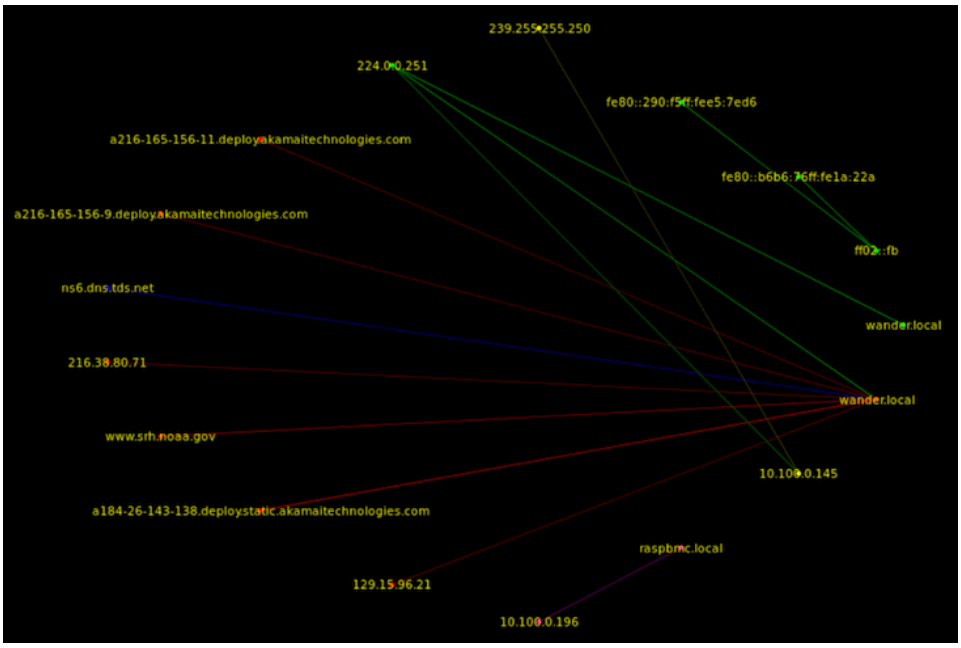
host $ apt-get -y install gedit

Terminator

Terminator is a terminal emulator with multiple windows and broadcast command functionality
host $ apt-get -y install terminator

EtherApe

It is a tool to display in graphical mode the network nodes and traffic.
In the images below, 10.0.0.4 is the Kali hackbox. All of the other endpoints are internal and external hosts



OpenVAS

OpenVAS is the utility to assess vulnerabilities

- Setting up and configuring OpenVAS

Application > openvas initial setup

Riunning this script will set up the self-signed certificates for SSL and download the latest vulnerability files and related data. It will also generate a password for the admin account on the system.

- Check the setup is ok

Applications > Kali Linux > System Services > OpenVas > openvas check setup

- Open the browser and go to https://localhost:9392
- Login with “admin” user, change the radio button for Use existing value to the blank field and add your new password and click the Save button

KeepNote

This is the standalone document organizer

Applications > Kali Linux > Recording tools > Documentation > KeepNote

Dradis

This is the web-based document organizer

Dradis is a web application, and can be used to share documentation with a team

The default URL for Dradis is https://127.0.0.1:3004. The application can be hosted on a remote secure server, and that is the best feature about Dradis.

nmap
Zenmap
OpenVAS
Maltego
KeepNote
unicorn-scan is an alternative to nmap

Top ten Kali security tools

- Aircrack-ng: Encryption-cracking tool for cracking 802.11 WPA-PSA and WEP keys
- Burpsuite: An integrated tool for testing web applications
- Hydra: A parallelised login cracker
- John the Ripper: A password-cracking tool
- Maltego: An intelligence and forensics application

- Metasploit Framework: An extremely flexible security testing suite
- nmap: The pre-eminent network mapping tool
- Owasp-ZAP: Another web application testing tool
- SqlMap: An SQL injection and database takeover tool
- Wireshark: The premier network protocol analysis tool

Fingerprinting the network: discover the network nodes and the traffic in between, and assess the vulnerabilities on the network

John the Ripper

It is a open source password cracker (*http://www.openwall.com/john/*) used to obtain the password from a password hash
host $ ./john capturedhash.txt

dsniff

- It is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI
- download and extract package from *http://monkey.org/~dugsong/dsniff/*

host $ tar zxf dsniff-<v>.tar
host $ cd dsniff-<v>
host $ brew install berkeley-db
host $ ./configure
configure: error: libpcap not found
non trova pace.h in /usr/include
Riuscito a installare su Linux host.

theHarvester

- It is a tool that of a given company's domain gathers emails, names, subdomains, IPs, and URLs using multiple public data sources. It can also perform active DNS searches (dictionary enumeration, reverse lookup of IP in order to find hostnames, TDL expansion)
- To find email addresses belonging to example.com using Google

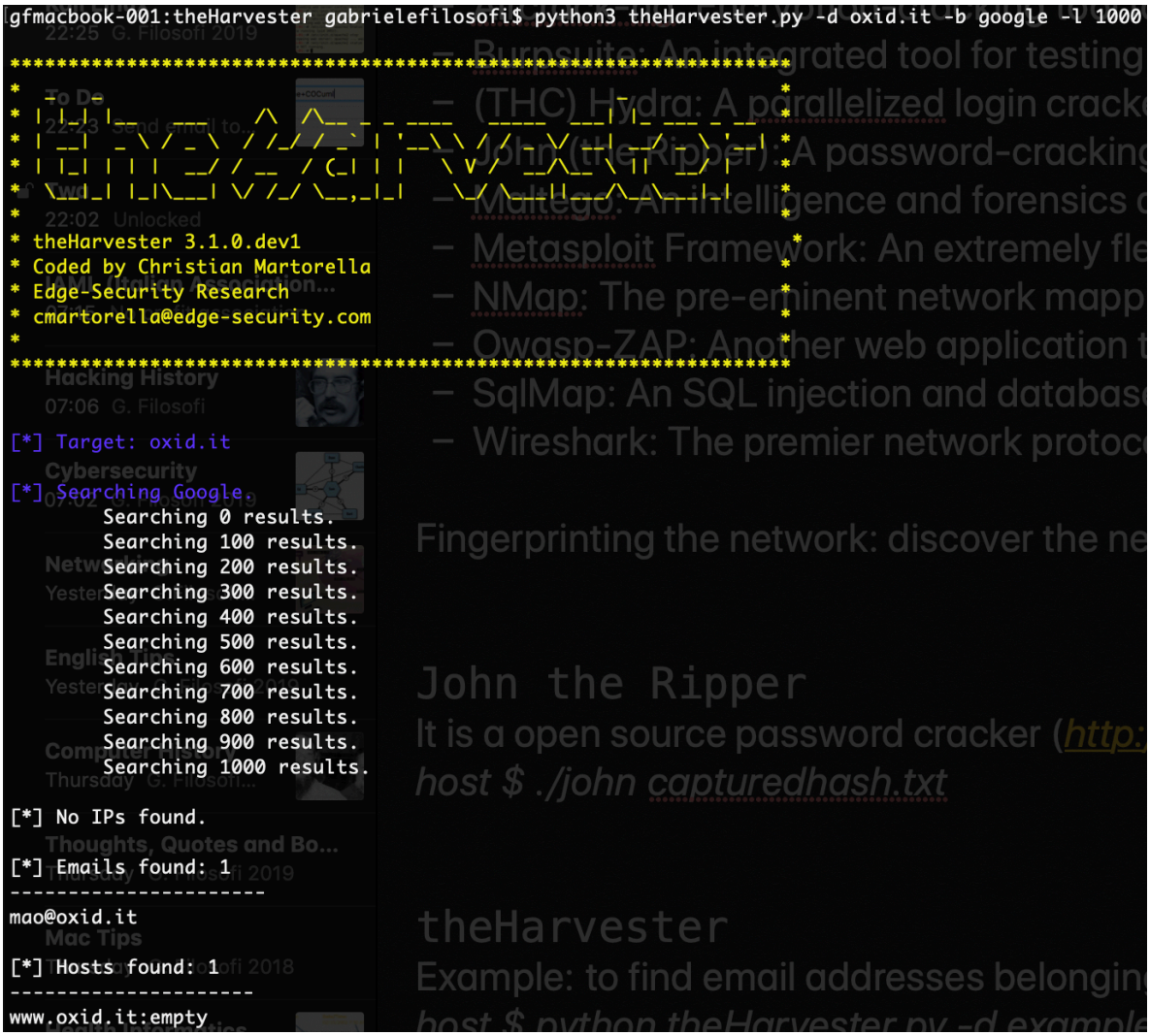
host $ python theHarvester.py -d example.com -b google -l 1000

- Install

ensure you have python 3.6+ ($ python3 -V)
host $ git clone https://github.com/laramies/theHarvester.git
host $ cd theHarvester/
host $ python3 -m install -r requirements.txt

- Example: to find email addresses belonging to example.com using Google

host $ python3 theHarvester.py -d oxid.it -b google -l 1000


gfmacbook-001:theHarvester gabrielefilosofi$ python3 theHarvester.py -d oxid.it -b google -l 1000
* theHarvester 3.1.0.dev1
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: oxid.it
[*] Searching Google.
Searching 0 results.
Searching 100 results.
Searching 200 results.
Searching 300 results.
Searching 400 results.
Searching 500 results.
Searching 600 results.
Searching 700 results.
Searching 800 results.
Searching 900 results.
Searching 1000 results.
[*] No IPs found.
[*] Emails found: 1
mao@oxid.it
[*] Hosts found: 1
www.oxid.it:empty
– Burpsuite: An integrated tool for testing
– (THC) Hydra: A parallelized login crack
– John (the Ripper): A password-cracking
– Maltego: An intelligence and forensics
– Metasploit Framework: An extremely fle
– NMap: The pre-eminent network mapp
– Owasp-ZAP: Another web application
– SqlMap: An SQL injection and databas
– Wireshark: The premier network protoc
Fingerprinting the network: discover the ne
John the Ripper
It is a open source password cracker (http:
host $ ./john capturedhash.txt
theHarvester
Example: to find email addresses belongin
host $ python theHarvester.py -d exampl

TrustedSec