Kali Linux

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

hostname: kali
username: root
p: toor (default)
IP addr: <kaliip>

- 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*
- root, with full privileges, is the default Kali user account
- Kali Linux installed service that would listen on a public network interface are disabled by default, such as HTTP and SSH. You can still manually handle them with
- *kali $ systemctl <enable|disable|start|restart|stop|status> <service>*
  or
- *kali $ /etc/init.d/<service> <enable|disable|start|restart|stop|status>*
  Example
- *kali $ /etc/init.d/apache2 start/status/restart/stop*
- To connect from external host
  host $ ssh root@<kaliip>

Creating bootable USB Live ISO

- The best for a corporate environment is to use a encrypted bootable USB drive loaded with Kali Linux
- Suggested 64GB USB stick

On you host 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 $ wget http://cdimage.kali.ork/current/SHA256SUMS
host $ wget http://cdimage.kali.ork/current/SHA256SUMS.gpg
host $ grep kali-linux-2019.2-amd64.iso SHA256SUMS | sha256sum -c
Plug the USB Drive stick and check the peripheral node (be /dev/sdb)
make sure it is unmounted
copy ISO image over the USB stick
host $ 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
host $ sudo parted /dev/sdb print
Ceate a start variable with the actual size of the kali imagekali ISOo
host $ sudo start=$(du --block-size=1MB kali-linux-2019.2-amd64.iso | awk '{print $1}')
host $ 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
host $ sudo parted -a optimal /dev/sdb mkpart primary "${start}MB" 100%
Check the new configuration
host $ sudo parted /dev/sdb print
Format sdb3
host $ sudo mkfs.ext4 -L persistence /dev/sdb3
Mount sdb3 and creating the pesistence.conf file
host $ sudo mount /dev/sdb3 /mnt
host $ sudo touch /mnt/pesistence.conf
host $ sudo vim /mnt/pesistence.conf
Add "/ union", save and quit
Note: such avspecial value will enable full persistence for all directories
WARNING: when rebooting with the USB plugged, always 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 kali (it takes 2 days!!)

kali $ apt update
kali $ apt do dist-upgrade
kali $ reboot
They suggest to do this once a week

Change password

kali $ passwd
To make this change persistent, copy the new hash read from */etc/shadow*
"root:<password hash>:etc."
into */lib/live/config/0031-root-password*
"usermod -p '<password hash>' root"

Tips

To open the Activities screen: move cursor to the top-left corner
Keyboard shortcut to open a new terminal: Ctrl+Alt+F*n*
To disable lockscreen timeout: Settings > Privacy > turn off lockscreen
To disable automatic suspend:
$ gnome-control-center power
in *Suspend & Power Button* set *Automatic suspend* to *Off*

Apache2 web server

To enable server
kali $ /etc/init.d/apache2 start
From remote station browse home page
host $ open -a safari http://<kaliip>:80
Note: the root website is /var/www. So when you use the server, just drop your website pages/folders into /var/www/

Postgresql server

kali $ systemctl start postgresql
kali $ su - postgres
kali $ createuser -P kevin_mitnick
kali $ createdb -T template0 -E UTF-8 -0 kevin_mitnick kevin_mitnick
From remote station
host $ psql -h <kaliip> -U kevin_mitnick kevin_mitnick
psql: could not connect to server: Connection refused
Is the server running on host "192.168.0.18" and accepting
TCP/IP connections on port 5432?

Netfilter

The linux firewall

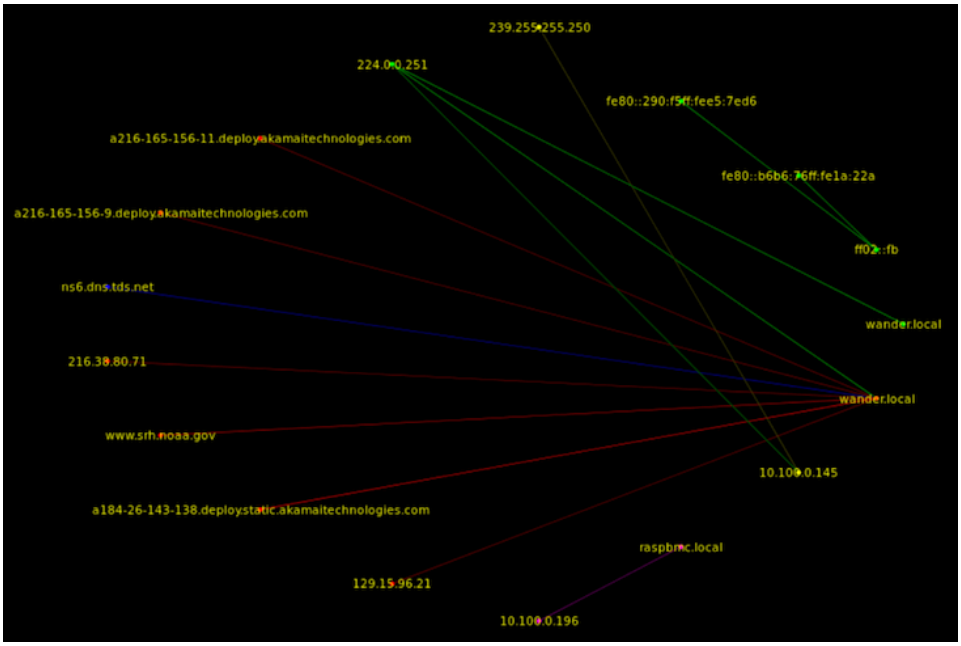
- List input rules: *$ iptables -n -L INPUT —line-numbers*
- Delete an input rule: *$ iptables -D INPUT <linenum>*
- Add a dropping rule: *$ iptables -A INPUT-s <src-ip> -j DROP*

Terminator

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