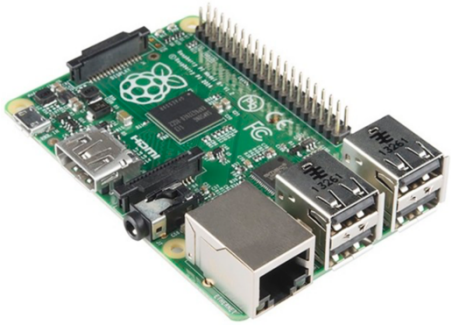
Seguridad informática empleando Rasberry Pi y Kali

7 Nov 2019 11:30 - 12:30 - Dr. Alejandro Corletti Estrada (*acorletti@darFe.es*)

Índice

Desarrollo

1. ¿Qué es Raspberry PI?



Raspberry Pi es un ordenador de placa simple de bajo coste desarrollado en el Reino Unido por la **Raspberry Pi Foundation**, con el objetivo de estimular la enseñanza de informática en las escuelas.

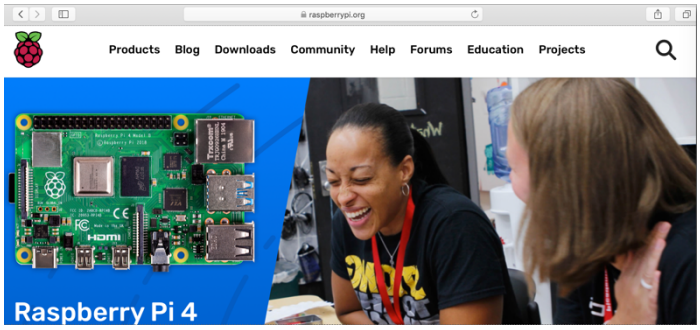
Su página Web de referencia es: https://www.raspberrypi.org

En español: https://www.raspberrypi.org/forums/viewforum.php?f=76

RISC (*Reduced Instruction Set Computer - Ordenador con Conjunto Reducido de Instrucciones)* de 32 bits y, con la llegada de su versión V8-A, también de 64 Bits.

Raspberry, se basa en la arquitectura **ARM** (*Advanced **RISC** Machine*) se trata de un conjunto de instrucciones de 32 y 64 bits. Fue concebida originalmente por **Acorn Computers** para su uso en ordenadores personales, los primeros productos basados en ARM eran los Acorn Archimedes, lanzados en 1987. La relativa simplicidad de los procesadores ARM los hace ideales para aplicaciones de baja potencia. La arquitectura ARM es licenciable. Esto significa que el negocio principal de **ARM Holdings** es la venta de núcleos IP (propiedad intelectual), estas licencias se utilizan para crear microcontroladores y CPUs basados en este núcleo.

El diseño del ARM se ha convertido en uno de los más usados del mundo, desde discos duros hasta juguetes y móviles. Hoy en día, cerca del 75% de los procesadores de 32 bits poseen este chip en su núcleo.



En febrero de 2015 salió al mercado otra placa **Raspberry Pi 2**. Hemos tomado la misma como punto de partida de esta ponencia pues añade dos importantes novedades: una CPU de cuatro núcleos (quad core) ARMv7 a 900 MHz y 1 GB de memoria RAM. Estos aspectos ya nos facilitan poder trabajar adecuadamente en los temas que veremos hoy. hoy en día ya está disponible la versión 4.

2. Kali Linux

Web: https://www.kali.org

En español: https://kali-linux.net

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de **BackTrack,** que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

(Párrafo tomado de Wikipedia: https://es.wikipedia.org/wiki/Kali_Linux)

En nuestro caso, reuniremos los dos conceptos anteriores y trabajaremos con una instalación de "**Kali**" sobre una "**Rasberry Pi 2**".

3. Cómo instalar kali linux en Raspberry pi

Vamos a seguir la guía de: https://www.linuxenespañol.com/tutoriales/como-instalar-kali-linux-en-raspberry-pi/

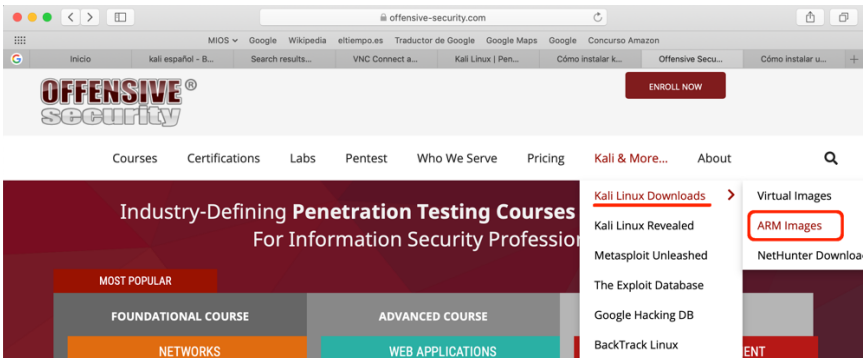
¿Qué necesitamos?

- Lector de tarjetas microSD.
- Monitor con HDMI
- Ordenador con conexión a internet.
- Teclado y ratón.
- Raspberry Pi.
  - Conector de red o wifi.
  - Tarjeta micro SD de mínimo 16Gb.

Descargar imagen Kali Linux

La imagen de kali ha sido creada en base a un script programado por el equipo de offensive security. La imagen es estable y cuenta con los paquetes básicos del SO Kali.

Buscar la última versión https://www.offensive-security.com



Instalación de kali en Raspberry empleando NOOBS:

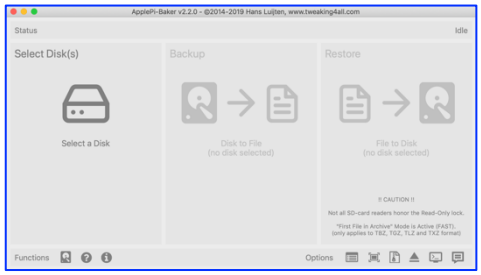
https://www.linuxenespañol.com/tutoriales/como-instalar-kali-linux-en-raspberry-pi/

Instalación de kali en Raspberry empleando MAC:

http://www.domoticadomestica.com/manual-para-instalar-un-sistema-operativo-en-tu-raspberry-pi/

Instalación en la Raspberry Pi a través de un Mac:

- **Paso 1** : Inserta la MicroSD en tu ordenador utilizando para ello un Adaptador a SD.
- **Paso 2** : Descarga el programa ApplePi-Baker.
- **Paso 3** : Abre el programa ApplePi-Baker.
- **Paso 4** : Introduce tu contraseña de administrador.
- **Paso 5** : En la parte de la izquierda, selecciona la memoria MicroSD que acabamos de conectar.
- **Paso 6** : En la derecha, en «IMG file» seleccionamos el lugar donde hayamos descargado nuestra imagen de Raspbian y pinchamos en "Restore Backup».



- **Paso 7** : (opcional) Comprobamos nuestro correo electrónico mientras el progreso de instalación se completa.
- **Paso 8** : Cuando haya terminado, nos saldrá un pop-up indicándonos que el proceso ha terminado y podemos extraer (con cuidado) la tarjeta.
- **Paso 9** : Extraemos con seguridad la memoria para evitar dañar la información que acabamos de cargarle.

4. Acceso a Kali.

4.1. Primer acceso.

El primer acceso lo podemos hacer por medio de un teclado , ratón y monitor HDMI, o en el caso que contemos con un router o dispositivo cableado con asignación de IP dinámica vía DHCP, también podemos conectarlo por cable y desde nuestro ordenador escaneamos la red para identificar qué dirección IP le ha asignado y conectarnos vía **SSH**, pues por defecto Kali trae abierto el puerto 22.

```
sh-3.2# nmap -n -sV 192.168.1.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2019-11-05 13:35 CET
Nmap scan report for 192.168.1.220
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.0p1 Debian 4 (protocol 2.0)
MAC Address: B8:27:EB:4D:38:4C (Raspberry Pi Foundation)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En cualquier caso, la cuenta de usuario y contraseña que viene preconfigurada en Kali es:

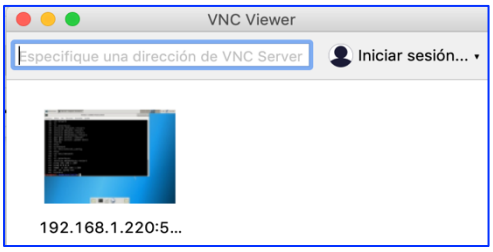
Usuario: **root**

Contraseña: **toor**

4.2. Presentación de VNC.

En el caso de esta presentación, emplearemos la conexión desde un portátil a la Raspberry por medio de **VNC**.

VNC son las siglas en inglés de (*Virtual Network Computing - Computación Virtual en Red*). **VNC** es un programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente.



En el caso de mi portátil, emplearemos el cliente **VNC Viewer**, que puede descargarse en:

https://www.realvnc.com/es/connect/download/viewer/ y es útil para casi todos los sistemas operativos.

Para poder conectarnos a la Raspberry, es necesario que la misma ejecute algún software como **VNC** Server.

El servicio de VNC es considerado como inseguro pues nos habilita un acceso con un importante grado de control del host, debido a ello, en general la cuente "root" no suele emplearse para este tipo de accesos. Para cumplir esta medida, es conveniente crear una cuenta que no posea tantos privilegios, en nuestro caso, nos conectaremos a la Raspberry como root:

```
#ssh  root@192.168.1.220
```

4.3. Creación de un usuario sin privilegios.

Una vez conectados, crearemos un nuevo usuario, en mi caso será "acorletti":

```
root@kali#adduser acorletti
```

4.4. Configuración estática y permanente de una interfaz de red.

En nuestro caso, como emplearemos esta Raspberry para esta exposición y conectada de forma directa a mi portátil, le podemos dejar configurada de forma estática y permanente esta dirección IP. En el sistema operativo "Debian" sobre el que está montado Kali, toda la configuración de la red ser realiza desde el directorio "/etc/network", y la configuración de las interfaces, en el archivo homónimo "interfaces". A continuación presentamos esta configuración:

```
root@kali:/etc/network# cat interfaces
        auto lo
        iface lo inet loopback
        auto eth0
        #iface eth0 inet dhcp
        iface eth0 inet static
        address 192.168.1.220
        netmask 255.255.255.0
        gateway 192.168.1.200
        dns-nameservers 8.8.8.8
```

Como se puede apreciar, se encuentra comentada ("#") la línea: #iface eth0 inet dhcp, la misma es tal cual viene la configuración inicial de Kali para que se asigne de forma automática vía DHCP (*Dynamic Host Contiguration Protocol*) una dirección IP si conectamos la interfaz física Ethernet vía conector RJ45.

En nuestro caso hemos configurado la de forma estática (static) la interfaz eth0 (iface eth0) con la dirección IP 192.168.1.220. La máscara de red hemos decidido colocar 255.255.255.0 (es decir "/24") y el Gateway es la IP que tengo configurada en mi portátil para la interfaz Ethernet, por último también configuramos el DNS de Google.

Si se desea dejar activa esta configuración, se puede ejecutar el comando:

```
root@kali:/etc/network# service networking restart
```

4.5. Análisis del hardware de la Raspberry.

Para analizar el hardware de nuestra Raspberry hay un comando de debían que es muy útil "**lshw**", el mismo no viene instalado en Kali. Para instalarlo descargamos el paquete "**lshw_02.18.85-0.1_armhf.deb**" desde: https://packages.debian.org/buster/lshw, lo subimos hasta nuestra Kali y lo ejecutamos con: **sudo dpkg -i lshw_02.18.85-0.1_arm64.deb**

Una vez instalado nos es muy útil para analizar el hardware de la Raspberry que tenemos:

```
acorletti@kali:~$ sudo lshw
[sudo] password for acorletti:
kali
    description: ARMv7 Processor rev 5 (v7l)
    product: Raspberry Pi 2 Model B Rev 1.1
    serial: 00000000374d384c
    width: 32 bits
    capabilities: smp
  *-core
       description: Motherboard
       physical id: 0
     *-cpu:0
          description: CPU
          product: cpu
          physical id: 0
          bus info: cpu@0
          size: 900MHz
          capacity: 900MHz
          capabilities: half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm
cpufreq
     *-cpu:1
          description: CPU
          product: cpu
          physical id: 1
          bus info: cpu@1
          size: 900MHz
          capacity: 900MHz
```

```
        capabilities: half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm
cpufreq
     *-cpu:2
          description: CPU
          product: cpu
          physical id: 2
          bus info: cpu@2
          size: 900MHz
          capacity: 900MHz
          capabilities: half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm
cpufreq
     *-cpu:3
          description: CPU
          product: cpu
          physical id: 3
          bus info: cpu@3
          size: 900MHz
          capacity: 900MHz
          capabilities: half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm
cpufreq
     *-memory
          description: System memory
          physical id: 4
          size: 926MiB
   *-usbhost
        product: DWC OTG Controller
        vendor: Linux 4.19.66-Re4son-v7+ dwc_otg_hcd
        physical id: 1
        bus info: usb@1
        logical name: usb1
        version: 4.19
        capabilities: usb-2.00
        configuration: driver=hub slots=1 speed=480Mbit/s
     *-usb
          description: USB hub
          product: SMC9514 Hub
          vendor: Standard Microsystems Corp.
          physical id: 1
          bus info: usb@1:1
          version: 2.00
          capabilities: usb-2.00
          configuration: driver=hub maxpower=2mA slots=5 speed=480Mbit/s
        *-usb
             description: Ethernet interface
             product: SMSC9512/9514 Fast Ethernet Adapter
             vendor: Standard Microsystems Corp.
             physical id: 1
             bus info: usb@1:1.1
             logical name: eth0
             version: 2.00
             serial: b8:27:eb:4d:38:4c
             size: 100Mbit/s
```

```
        capacity: 100Mbit/s
        capabilities: usb-2.00 ethernet physical tp mii 10bt 10bt-fd 100bt 100bt-fd autonegotiation
        configuration: autonegotiation=on broadcast=yes driver=smsc95xx driverversion=22-Aug-
2005 duplex=full firmware=smsc95xx USB 2.0 Ethernet ip=192.168.1.220 link=yes maxpower=2mA
multicast=yes port=MII speed=100Mbit/s
```

Para analizar el estado de los discos duros y particiones, tenemos las siguientes opciones.

```
root@kali:/etc/network# lsblk -fm
NAME      FSTYPE LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINT   SIZE OWNER GROUP MODE
mmcblk0                                                                    125G root  disk  brw-rw----
 ├─mmcblk0p1 vfat   FBEF-2553                              54,9M    55% /boot        122,1M root  disk  brw-rw----
 └─mmcblk0p2 ext4   66f0b950-b5c0-42c9-a7e1-1c60  113,7G     3% /   124,6G root  disk  brw-rw----

root@kali:/etc/network# df -h
S.ficheros    Tamaño Usados  Disp Uso% Montado en
/dev/root       123G   3,9G  114G   4% /
devtmpfs        459M     0  459M   0% /dev
tmpfs           464M     0  464M   0% /dev/shm
tmpfs           464M   624K  463M   1% /run
tmpfs           5,0M     0  5,0M   0% /run/lock
tmpfs           464M     0  464M   0% /sys/fs/cgroup
/dev/mmcblk0p1  122M    67M   55M  55% /boot
tmpfs            93M   4,0K   93M   1% /run/user/113
tmpfs            93M     0   93M   0% /run/user/1000
```

En ambos casos, podemos observar que se trata de un disco duro (en nuestro caso memoria microSD) de 12X GB (*en concreto es una microSD de **128 GB***). Tenemos una partición vfat de 122,1M donde está montado el arranque (/boot) y otra ext4 de 124,6G

Por último nos falta verificar sus interfaces, que lo haremos con el comando "**ifconfig**".

```
root@kali:/etc/network# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.220  netmask 255.255.255.0  broadcast 192.168.1.255
      inet6 fe80::ba27:ebff:fe4d:384c  prefixlen 64  scopeid 0x20<link>
      ether b8:27:eb:4d:38:4c  txqueuelen 1000  (Ethernet)
      RX packets 1293  bytes 92053 (89.8 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 1893  bytes 234410 (228.9 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1000  (Local Loopback)
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 0  bytes 0 (0.0 B)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Podemos verificar que ya tenemos nuestra interfaz Ethernet (Eth0) tal cual la configuramos de forma estática y permanente y también su local loop (lo).

4.6. Acceso al entorno gráfico.

En nuestro caso, para poder aprovechar al máximo las herramientas que incorpora Kali, nos interesa poder hacer uso del entorno gráfico, por lo que también como "root" habilitamos para que permita el empleo de X11 en las conexiones SSH:

En **/etc/ssh**, abrimos el fichero "**sshd_config**" y colocamos en "**yes**" el parámetro "**X11Forwarding**" y reiniciamos el servicio:

```
root@kali#service ssh restart
```

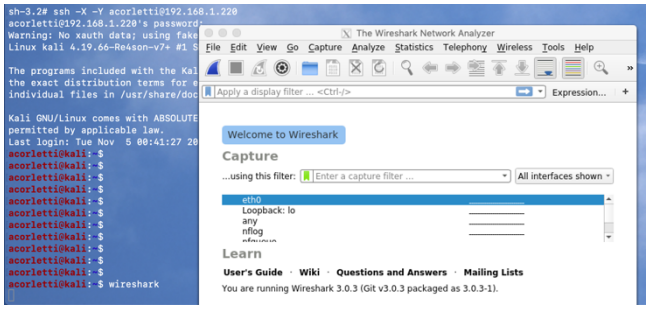
Luego salimos para emplear este nuevo usuario.

```
root@kali#exit
```

Ahora sí nos conectamos con el mismo aprovechando la posibilidad de emplear X11 (la opción **"-X"** es para que emplee X11 y la **"-Y"** para indicar que es una conexión confiable):

```
#ssh -X -Y acorletti@192.168.1.220
```

Con esta conexión, por ejemplo ya podemos ejecutar aplicaciones que empleen entorno gráfico (en el ejemplo vemos como abre la herramienta "Wireshark").

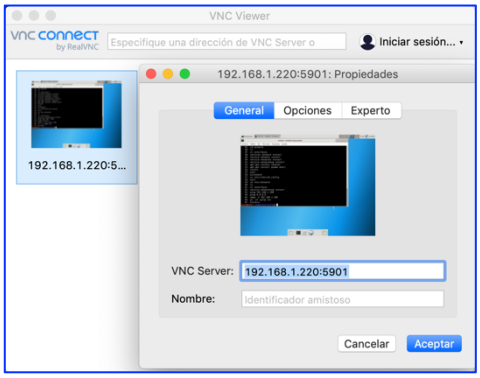


Si queremos tener un escritorio completo, tal cual usa el entorno gráfico de "Kali", debemos entonces recurrir al mencionado VNCServer, que como dijimos ya viene instalado en Kali. Con lo cual ejecutamos el comando:

```
acorletti@kali:~$ vncserver
        New 'X' desktop is kali:2
        Starting applications specified in /home/acorletti/.vnc/xstartup
        Log file is /home/acorletti/.vnc/kali:2.log
```

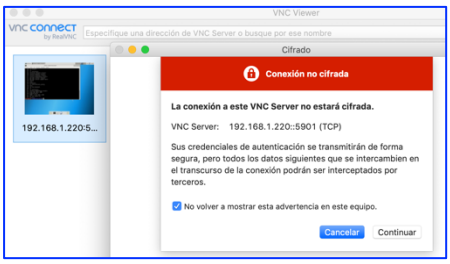
Nos interesa conocer el puerto que ha abierto, para poder conectarnos desde nuestro VNC cliente, para lo cual podemos ejecutar:

```
acorletti@kali:~$ ps -ef |grep vnc
        acorlet+ 19098     1  0 nov04 ?        00:00:15 Xtightvnc :1 -desktop X -auth
        /home/acorletti/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth
        /home/acorletti/.vnc/passwd -rfbport 5901 -fp
        /usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr
        /share/fonts/X11/100dpi/ -co /etc/X11/rgb
```



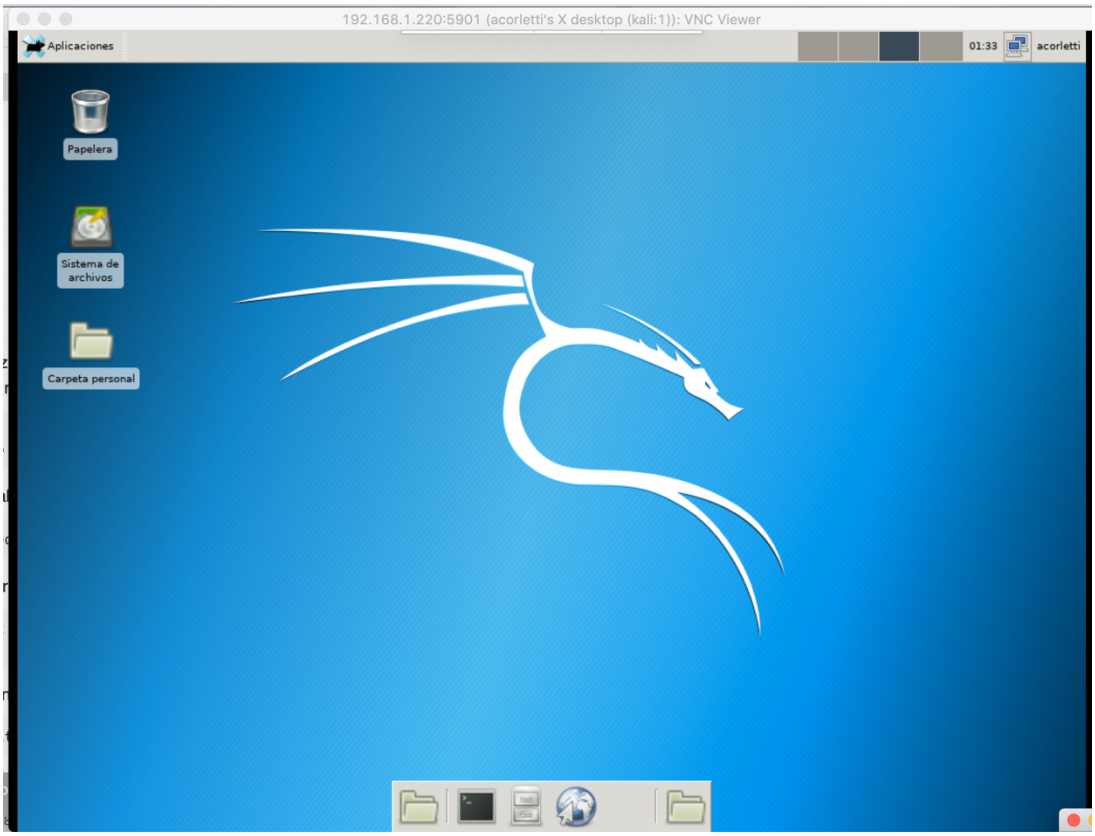
Podemos ver que se trata del puerto "**5901**", así que será esta al que apuntaremos nuestro cliente VNCViewer:

Una vez que ejecutamos la aplicación, nos muestra claramente esto de la "inseguridad de emplear VNC:



NOTA: También podemos usar como cliente un navegador como **Safari,** colocando en su ventana: vnc://192.168.1.220:5901 (*nos abrirá una nueva ventana pidiendo la contraseña del usuario dado de alta en vncerver*).

Al confirmar en cualquiera de los casos que aceptamos este riesgo, ya se nos despliega el escritorio de Kali:



5. ¿Qué nos ofrece el trabajo de Rasberry con Kali?

Tengamos en cuenta que se trata de una versión muy optimizada, por lo que su entorno gráfico dista bastante de la versión original de esta distribución. A pesar de esta limitación veremos algunas de los inmensos beneficios que nos ofrece esta metodología de trabajo.

5.1. Paquetes instalados.

Lo primero que nos interesa para comenzar a trabajar es conocer los paquetes que trae instalado por defecto esta distribución de Kali para Raspberry. El comando que podemos emplear es:

```
acorletti@kali:~$ sudo apt-cache pkgnames
```

A continuación, presentamos los mismos (*los hemos ordenado alfabéticamente para simplificar su búsqueda, con el comando "**sort**"):*

abootimg	cpp-8	ethtool	gcc-8-base	gtk2-engines-pixbuf	kali-desktop-core
adduser	crda	exfat-fuse	gcc-9-base	gtk2-engines-xfce	kali-desktop-xfce
adwaita-icon-theme	cron	exfat-utils	gcr	gtk3-engines-xfce	kali-menu
aircrack-ng	crunch	exo-utils	gdbm-l10n	gtk-update-icon-cache	kalipi-bootloader
apache2	curl	exploitdb	gdisk	gvfs	kalipi-kernel
apache2-bin	dash	fake-hwclock	geoip-database	gvfs-common	kalipi-kernel-headers
apache2-data	dbus	fakeroot	gir1.2-glib-2.0	gvfs-daemons	kalipi-re4son-firmware
apache2-utils	dbus-user-session	fdisk	git	gvfs-libs	kali-root-login
apt	dbus-x11	file	git-man	gzip	kbd
apt-transport-https	dconf-cli	findutils	glib-networking	haveged	keyboard-configuration
apt-utils	dconf-gsettings-backend	firebird3.0-common	glib-networking-common	hicolor-icon-theme	klibc-utils
atftpd	dconf-service	firebird3.0-common-doc	glib-networking-services	hostname	kmod
at-spi2-core	debconf	firefox-esr	gnome-accessibility-themes	hunspell-en-us	krb5-locales
base-files	debconf-i18n	firmware-amd-graphics	gnome-keyring	hwloc	less
base-passwd	debian-archive-keyring	firmware-atheros	gnome-keyring-pkcs11	hydra	libaacs0
bash	debianutils	firmware-libertas	gnome-theme-kali	hyperion	libacl1
bind9-host	debtags	firmware-linux	gnome-themes-extra	i2c-tools	libalgorithm-diff-perl
binutils	desktop-base	firmware-linux-free	gnome-themes-extra-data	ieee-data	libalgorithm-diff-xs-perl
binutils-arm-linux-gnueabihf	desktop-file-utils	firmware-linux-nonfree	gnupg	ifupdown	libalgorithm-merge-perl
binutils-common	device-tree-compiler	firmware-misc-nonfree	gnupg-l10n	init	libaom0
bluez	dh-python	firmware-realtek	gnupg-utils	initramfs-tools	libapparmor1
bluez-firmware	dictionaries-common	fontconfig	gpg	initramfs-tools-core	libapr1
bsdmainutils	diffutils	fontconfig-config	gpg-agent	init-system-helpers	libaprutil1
bsdutils	dirmngr	fonts-croscore	gpgconf	iproute2	libaprutil1-dbd-sqlite3
build-essential	distro-info-data	fonts-crosextra-caladea	gpgsm	iptables	libaprutil1-ldap
bundler	dmidecode	fonts-crosextra-carlito	gpgv	iputils-ping	libapt-inst2.0
busybox	dmsetup	fonts-dejavu-core	gpg-wks-client	isc-dhcp-client	libapt-pkg5.0
bzip2	dnsmasq-base	fonts-lato	gpg-wks-server	isc-dhcp-common	libarchive13
ca-certificates	dnsrecon	fonts-quicksand	grep	iso-codes	libargon2-1
cewl	dns-root-data	freetds-common	groff-base	iw	libasan5
cgpt	dnsutils	fuse	gsettings-desktop-schemas	javascript-common	libasound2
console-common	dosfstools	g++	gstreamer1.0-plugins-base	john	libasound2-data
console-data	dpkg	g++-8	gtk2-engines-murrine	john-data	libasound2-plugins
console-setup	dpkg-dev	gcc		kali-archive-keyring	libassuan0
console-setup-linux	e2fsprogs	gcc-8		kali-debtags	libasyncns0
coreutils	easy-rsa			kali-defaults	
cpio	eject				
cpp	emacsen-common				

- libatasmart4
- libatk1.0-0
- libatk1.0-data
- libatk-bridge2.0-0
- libatkmm-1.6-1v5
- libatomic1
- libatspi2.0-0
- libattr1
- libaudit1
- libaudit-common
- libauthen-sasl-perl
- libavahi-client3
- libavahi-common3
- libavahi-common-data
- libavcodec58
- libavresample4
- libavutil56
- libayatana-appindicator3-1
- libayatana-ido3-0.4-0
- libayatana-indicator3-7
- libbdplus0
- libbind9-161
- libbinutils
- libblas3
- libblkid1
- libblockdev2
- libblockdev-crypto2
- libblockdev-fs2
- libblockdev-loop2
- libblockdev-part2
- libblockdev-part-err2
- libblockdev-swap2
- libblockdev-utils2
- libbluetooth3
- libbluray2
- libbrotli1
- libbsd0
- libbson-1.0-0
- libbz2-1.0
- libc6
- libc6-dev
- libcairo2
- libcairo-gobject2
- libcairomm-1.0-1v5
- libcanberra0
- libcanberra-gtk0
- libcanberra-gtk3-0
- libcanberra-gtk3-module
- libcanberra-gtk-module
- libcap2
- libcap2-bin
- libcap-ng0
- libc-ares2
- libc-bin
- libcc1-0
- libccid
- libc-dev-bin
- libcdparanoia0
- libc-l10n
- libcodec2-0.8.1
- libcolord2
- libcom-err2
- libcroco3
- libcryptsetup12
- libcryptsetup4
- libct4
- libcups2
- libcurl3-gnutls
- libcurl4
- libdata-dump-perl
- libdatrie1
- libdb5.3
- libdbus-1-3
- libdbus-glib-1-2
- libdbusmenu-glib4
- libdbusmenu-gtk3-4
- libdconf1
- libdebconfclient0
- libdevmapper1.02.1
- libdns1104
- libdns-export1104
- libdouble-conversion3
- libdpkg-perl
- libdrm2
- libdrm-amdgpu1
- libdrm-common
- libdrm-etnaviv1
- libdrm-nouveau2
- libdrm-radeon1
- libdw1
- libedit2
- libegl1
- libegl1-mesa
- libegl-mesa0
- libelf1
- libencode-locale-perl
- libepoxy0
- liberror-perl
- libestr0
- libevdev2
- libevent-2.1-6
- libexif12
- libexo-1-0
- libexo-2-0
- libexo-common
- libexo-helpers
- libexpat1
- libexpat1-dev
- libext2fs2
- libfakeroot
- libfastjson4
- libfbclient2
- libfdisk1
- libffi6
- libfile-basedir-perl
- libfile-desktopentry-perl
- libfile-fcntllock-perl
- libfile-listing-perl
- libfile-mimeinfo-perl
- libflac8
- libfont-afm-perl
- libfontconfig1
- libfontenc1
- libfreerdp2-2
- libfreetype6
- libfribidi0
- libfstrm0
- libfuse2
- libgail18
- libgail-common
- libgarcon-1-0
- libgarcon-common
- libgbm1
- libgcc1
- libgcc-8-dev
- libgck-1-0
- libgcr-base-3-1
- libgcr-ui-3-1
- libgcrypt20
- libgdbm6
- libgdbm-compat4
- libgdk-pixbuf2.0-0
- libgdk-pixbuf2.0-bin
- libgdk-pixbuf2.0-common
- libgeoip1
- libgfortran5
- libgirepository-1.0-1
- libgl1
- libgl1-mesa-dri
- libglapi-mesa
- libgles2
- libglib2.0-0
- libglib2.0-bin
- libglib2.0-data
- libglibmm-2.4-1v5
- libglu1-mesa
- libglvnd0
- libglx0
- libglx-mesa0
- libgmp10
- libgmp-dev
- libgmpxx4ldbl
- libgnutls30
- libgomp1
- libgpg-error0
- libgpgme11
- libgpm2
- libgraphite2-3
- libgsm1
- libgssapi-krb5-2
- libgstreamer1.0-0
- libgstreamer-plugins-base1.0-0
- libgtk2.0-0
- libgtk2.0-bin
- libgtk2.0-common
- libgtk-3-0
- libgtk-3-bin
- libgtk-3-common
- libgtkmm-3.0-1v5
- libgudev-1.0-0
- libharfbuzz0b
- libhavege1
- libhogweed4
- libhtml-format-perl
- libhtml-form-perl
- libhtml-parser-perl
- libhtml-tagset-perl
- libhtml-tree-perl
- libhttp-cookies-perl
- libhttp-daemon-perl
- libhttp-date-perl
- libhttp-message-perl
- libhttp-negotiate-perl
- libhunspell-1.7-0
- libhwloc5
- libhwloc-plugins
- libi2c0
- libice6
- libicu63
- libidn11
- libidn2-0
- libimobiledevice6
- libindicator3-7
- libinput10
- libinput-bin
- libio-html-perl
- libio-socket-ssl-perl
- libio-stringy-perl
- libip4tc2
- libip6tc2
- libipc-system-simple-perl
- libiptc0
- libirs161
- libisc1100
- libisccc161
- libisccfg163
- libisc-export1100
- libisl19
- libiw30
- libjack-jackd2-0
- libjansson4
- libjbig0
- libjim0.77
- libjpeg62-turbo
- libjs-jquery
- libjson-c4
- libjsoncpp1
- libjson-glib-1.0-0
- libjson-glib-1.0-common
- libjs-skeleton
- libjs-sphinxdoc
- libjs-underscore
- libk5crypto3
- libkeybinder-3.0-0
- libkeyutils1
- libklibc
- libkmod2
- libkrb5-3
- libkrb5support0
- libksba8
- liblcms2-2
- libldap-2.4-2
- libldap-common
- libldb1
- liblightdm-gobject-1-0
- liblinear3
- libllvm7
- libllvm8
- liblmdb0
- liblocale-gettext-perl
- liblognorm5
- libltdl7
- liblua5.2-0
- liblua5.3-0
- liblwp-mediatypes-perl
- liblwp-protocol-https-perl
- liblwres161
- liblz4-1
- liblzma5
- liblzo2-2
- libmagic1
- libmagic-mgc
- libmailtools-perl
- libmariadb3
- libmaxminddb0
- libmbim-glib4
- libmbim-proxy
- libmemcached11
- libmm-glib0
- libmnl0
- libmongoc-1.0-0
- libmotif-common
- libmount1
- libmp3lame0
- libmpc3
- libmpdec2
- libmpfr6
- libmtdev1
- libncurses6
- libncursesw6
- libndp0
- libnet-dbus-perl
- libnetfilter-conntrack3
- libnet-http-perl
- libnet-smtp-ssl-perl

- libnet-ssleay-perl
- libnettle6
- libnewt0.52
- libnfc5
- libnfc-bin
- libnfnetlink0
- libnftnl11
- libnghttp2-14
- libnl-3-200
- libnl-genl-3-200
- libnl-route-3-200
- libnm0
- libnma0
- libnotify4
- libnotify-bin
- libnpth0
- libnspr4
- libnss3
- libnss-systemd
- libntfs-3g883
- libogg0
- libopenjp2-7
- libopus0
- liborc-0.4-0
- libp11-kit0
- libpam0g
- libpam-gnome-keyring
- libpam-modules
- libpam-modules-bin
- libpam-runtime
- libpam-systemd
- libpango-1.0-0
- libpangocairo-1.0-0
- libpangoft2-1.0-0
- libpangomm-1.4-1v5
- libparted2
- libparted-fs-resize0
- libpcap0.8
- libpci3
- libpciaccess0
- libpcre2-16-0
- libpcre2-8-0
- libpcre3
- libpcsclite1
- libperl5.28
- libpipeline1
- libpixman-1-0
- libpkcs11-helper1
- libplist3
- libplymouth4
- libpng16-16
- libpolkit-agent-1-0
- libpolkit-gobject-1-0
- libpoppler82
- libpoppler-glib8
- libpopt0
- libpq5
- libprocps7
- libprotobuf-c1
- libproxy1v5
- libproxychains3
- libpsl5
- libpulse0
- libpulsedsp
- libpulse-mainloop-glib0
- libpython2.7
- libpython2.7-dev
- libpython2.7-minimal
- libpython2.7-stdlib
- libpython2-dev
- libpython2-stdlib
- libpython3.7
- libpython3.7-dev
- libpython3.7-minimal
- libpython3.7-stdlib
- libpython3-dev
- libpython3-stdlib
- libpython-all-dev
- libpython-dev
- libpython-stdlib
- libqmi-glib5
- libqmi-proxy
- libqt5core5a
- libqt5dbus5
- libqt5gui5
- libqt5multimedia5
- libqt5multimedia5-plugins
- libqt5multimediagsttools5
- libqt5multimediaquick5
- libqt5multimediawidgets5
- libqt5network5
- libqt5opengl5
- libqt5printsupport5
- libqt5qml5
- libqt5quick5
- libqt5svg5
- libqt5widgets5
- libraspberrypi0
- libraspberrypi-bin
- libraspberrypi-dev
- libraspberrypi-doc
- libreadline8
- librest-0.7-0
- librsvg2-2
- librsvg2-common
- librtmp1
- libruby2.5
- libsamplerate0
- libsasl2-2
- libsasl2-modules
- libsasl2-modules-db
- libsbc1
- libseccomp2
- libsecret-1-0
- libsecret-common
- libselinux1
- libsemanage1
- libsemanage-common
- libsensors5
- libsensors-config
- libsepol1
- libserf-1-1
- libshine3
- libsigc++-2.0-0v5
- libslang2
- libsm6
- libsmartcols1
- libsmbclient
- libsmi2ldbl
- libsnappy1v5
- libsndfile1
- libsnmp30
- libsnmp-base
- libsoup2.4-1
- libsoup-gnome2.4-1
- libsoxr0
- libspandsp2
- libspeex1
- libspeexdsp1
- libsqlite3-0
- libss2
- libssh2-1
- libssh-4
- libssh-gcrypt-4
- libssl1.0.2
- libssl1.1
- libssl-dev
- libstartup-notification0
- libstdc++6
- libstdc++-8-dev
- libsvn1
- libswresample3
- libsystemd0
- libtalloc2
- libtasn1-6
- libtdb1
- libteamdctl0
- libtevent0
- libtext-charwidth-perl
- libtext-iconv-perl
- libtext-wrapi18n-perl
- libthai0
- libthai-data
- libtheora0
- libthunarx-3-0
- libtie-ixhash-perl
- libtiff5
- libtimedate-perl
- libtinfo6
- libtommath1
- libtry-tiny-perl
- libtumbler-1-0
- libtwolame0
- libubsan1
- libuchardet0
- libudev1
- libudisks2-0
- libunistring2
- libunwind8
- libupower-glib3
- liburi-perl
- libusb-0.1-4
- libusb-1.0-0
- libusbmuxd4
- libutempter0
- libutf8proc2
- libuuid1
- libva2
- libva-drm2
- libva-x11-2
- libvdpau1
- libvdpau-va-gl1
- libvisual-0.4-0
- libvolume-key1
- libvorbis0a
- libvorbisenc2
- libvorbisfile3
- libvpx5
- libvpx6
- libvte-2.91-0
- libvte-2.91-common
- libwacom2
- libwacom-bin
- libwacom-common
- libwavpack1
- libwayland-client0
- libwayland-cursor0
- libwayland-egl1
- libwayland-server0
- libwbclient0
- libwebp6
- libwebpmux3
- libwebrtc-audio-processing1
- libwinpr2-2
- libwireshark12
- libwireshark-data
- libwiretap9
- libwnck22
- libwnck-common
- libwrap0
- libwscodecs2
- libwsutil10
- libwww-perl
- libwww-robotrules-perl
- libx11-6
- libx11-data
- libx11-protocol-perl
- libx11-xcb1
- libx264-155
- libx265-176
- libxau6
- libxaw7
- libxcb1
- libxcb-dri2-0
- libxcb-dri3-0
- libxcb-glx0
- libxcb-icccm4
- libxcb-image0
- libxcb-keysyms1
- libxcb-present0
- libxcb-randr0
- libxcb-render0
- libxcb-render-util0
- libxcb-shape0
- libxcb-shm0
- libxcb-sync1
- libxcb-util0
- libxcb-xfixes0
- libxcb-xinerama0
- libxcb-xkb1
- libxcomposite1
- libxcursor1
- libxdamage1
- libxdmcp6
- libxext6
- libxfce4panel-2.0-4
- libxfce4ui-1-0
- libxfce4ui-2-0
- libxfce4ui-common
- libxfce4ui-utils
- libxfce4util7
- libxfce4util-bin
- libxfce4util-common
- libxfconf-0-2
- libxfixes3
- libxfont2
- libxft2
- libxi6
- libxinerama1
- libxkbcommon0
- libxkbcommon-x11-0
- libxkbfile1
- libxklavier16
- libxm4
- libxml2
- libxml2-utils
- libxml-parser-perl
- libxml-twig-perl
- libxml-xpathengine-perl
- libxmu6
- libxmuu1
- libxpm4
- libxrandr2
- libxrender1
- libxres1
- libxshmfence1
- libxslt1.1
- libxss1
- libxt6
- libxtables12

- libxtst6
- libxv1
- libxvidcore4
- libxxf86dga1
- libxxf86vm1
- libyaml-0-2
- libzstd1
- libzvbi0
- libzvbi-common
- lightdm
- lightdm-gtk-greeter
- light-locker
- linux-base
- linux-libc-dev
- locales
- locales-all
- login
- logrotate
- logsave
- lsb-base
- lsb-release
- lshw
- lsof
- lua-lpeg
- make
- man-db
- manpages
- manpages-dev
- mariadb-common
- mawk
- medusa
- mesa-va-drivers
- mesa-vdpau-drivers
- metasploit-framework
- mfoc
- mime-support
- mlocate
- mobile-broadband-provider-info
- modemmanager
- mount
- mysql-common
- nano
- nasm
- ncrack
- ncurses-base
- ncurses-bin
- ncurses-term
- netbase
- netcat-traditional
- net-tools
- network-manager
- network-manager-gnome
- nmap
- nmap-common
- node-normalize.css
- notification-daemon
- ntfs-3g
- ntpdate
- ocl-icd-libopencl1
- opensc
- opensc-pkcs11
- openssh-client
- openssh-server
- openssh-sftp-server
- openssl
- openvpn
- p11-kit
- p11-kit-modules
- parted
- passing-the-hash
- passwd
- patch
- pavucontrol
- pcscd
- perl
- perl-base
- perl-modules-5.28
- perl-openssl-defaults
- pigz
- pinentry-curses
- pinentry-gnome3
- plymouth
- plymouth-label
- policykit-1
- policykit-1-gnome
- poppler-data
- postgresql
- postgresql-11
- postgresql-client-11
- postgresql-client-common
- postgresql-common
- ppp
- procps
- proxychains
- psmisc
- publicsuffix
- pulseaudio
- pulseaudio-utils
- python
- python2
- python2.7
- python2.7-dev
- python2.7-minimal
- python2-dev
- python2-minimal
- python3
- python3.7
- python3.7-dev
- python3.7-minimal
- python3-apt
- python3-asn1crypto
- python3-blinker
- python3-bs4
- python3-certifi
- python3-cffi-backend
- python3-chardet
- python3-click
- python3-colorama
- python3-crypto
- python3-cryptography
- python3-dbus
- python3-debian
- python3-decorator
- python3-dev
- python3-dicttoxml
- python3-distutils
- python3-dnspython
- python3-entrypoints
- python3-flask
- python3-future
- python3-gi
- python3-html5lib
- python3-idna
- python3-ipython-genutils
- python3-itsdangerous
- python3-jinja2
- python3-jsonschema
- python3-jupyter-core
- python3-keyring
- python3-keyrings.alt
- python3-lib2to3
- python3-lxml
- python3-markupsafe
- python3-minimal
- python3-nbformat
- python3-openssl
- python3-pip
- python3-pkg-resources
- python3-plotly
- python3-pycurl
- python3-pyinotify
- python3-pyparsing
- python3-requests
- python3-retrying
- python3-secretstorage
- python3-setuptools
- python3-simplejson
- python3-six
- python3-soupsieve
- python3-traitlets
- python3-tz
- python3-unicodecsv
- python3-urllib3
- python3-webencodings
- python3-werkzeug
- python3-wheel
- python3-xdg
- python3-xlsxwriter
- python3-yaml
- python-all
- python-all-dev
- python-apt-common
- python-asn1crypto
- python-backports.functools-lru-cache
- python-bs4
- python-certifi
- python-cffi-backend
- python-chardet
- python-configobj
- python-configparser
- python-crypto
- python-cryptography
- python-dbus
- python-dev
- python-dnspython
- python-entrypoints
- python-enum34
- python-gi
- python-gpg
- python-html5lib
- python-idna
- python-ipaddress
- python-keyring
- python-keyrings.alt
- python-ldb
- python-lxml
- python-magic
- python-minimal
- python-netaddr
- python-openssl
- python-pip
- python-pip-whl
- python-pkg-resources
- python-requests
- python-rpi.gpio
- python-samba
- python-secretstorage
- python-setuptools
- python-six
- python-smbus
- python-soupsieve
- python-talloc
- python-tdb
- python-urllib3
- python-webencodings
- python-wheel
- python-xdg
- qt5-gtk-platformtheme
- qttranslations5-l10n
- rake
- read-edid
- readline-common
- realvnc-vnc-viewer
- recon-ng
- rfkill
- rlinetd
- rpi.gpio-common
- rsyslog
- rtkit
- ruby
- ruby2.5
- ruby2.5-dev
- ruby2.5-doc
- ruby-activesupport
- ruby-addressable
- ruby-atomic
- ruby-bundler
- ruby-cms-scanner
- ruby-concurrent
- ruby-dev
- ruby-did-you-mean
- ruby-ethon
- ruby-ffi
- rubygems-integration
- ruby-i18n
- ruby-json
- ruby-mime
- ruby-mime-types
- ruby-mime-types-data
- ruby-mini-exiftool
- ruby-minitest
- ruby-molinillo
- ruby-net-http-digest-auth
- ruby-net-http-persistent
- ruby-net-telnet
- ruby-nokogiri
- ruby-opt-parse-validator
- ruby-pkg-config
- ruby-power-assert
- ruby-progressbar
- ruby-public-suffix
- ruby-spider
- ruby-test-unit
- ruby-thor
- ruby-thread-safe
- ruby-typhoeus
- ruby-tzinfo
- ruby-xmlrpc
- ruby-yajl
- ruby-zip
- samba-common
- samba-common-bin
- samba-dsdb-modules

samba-libs	tcpdump	update-inetd	winexe	xfce4-panel	xfwm4
screen	tftp	upower	wireless-regdb	xfce4-power-manager	xinit
sed	theharvester	usb.ids	wireless-tools	xfce4-power-manager-data	xkb-data
sensible-utils	thunar	usb-modeswitch	wireshark	xfce4-power-manager-plugins	xorg
shared-mime-info	thunar-data	usb-modeswitch-data	wireshark-common	xfce4-pulseaudio-plugin	xorg-docs-core
smbclient	thunar-volman	usbmuxd	wireshark-qt	xfce4-session	xserver-common
snmp	tightvncserver	usbutils	wpasupplicant	xfce4-settings	xserver-xorg
snmpd	tmux	util-linux	wpscan	xfce4-terminal	xserver-xorg-core
sound-theme-freedesktop	tor	va-driver-all	x11-apps	xfconf	xserver-xorg-input-evdev
sqlmap	tor-geoipdb	vboot-kernel-utils	x11-common	xfdesktop4	xserver-xorg-input-synaptics
sqsh	torsocks	vboot-utils	x11-session-utils	xfdesktop4-data	xserver-xorg-legacy
ssl-cert	triggerhappy	vdpau-driver-all	x11-utils	xfonts-100dpi	xserver-xorg-video-fbdev
sudo	tshark	vim	x11-xkb-utils	xfonts-75dpi	xxd
sysstat	tumbler	vim-common	x11-xserver-utils	xfonts-base	xz-utils
systemd	tumbler-common	vim-runtime	xauth	xfonts-encodings	zerofree
systemd-sysv	tzdata	vim-tiny	xbitmaps	xfonts-scalable	zip
sysvinit-utils	u-boot-tools	wfuzz	xdg-user-dirs	xfonts-terminus	zlib1g
tango-icon-theme	ucf	wget	xdg-utils	xfonts-utils	
tar	udev	whiptail	xfce4		
tasksel	udisks2	whois	xfce4-appfinder		
tasksel-data	unrar	windows-binaries	xfce4-notifyd		
	unzip				

5.2. Nmap

Vamos a realizar algunas pruebas sencillas del empleo de nmap.

```
acorletti@kali:~$ nmap -n -sT --open 192.168.1.0/24
        Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 20:28 UTC
        Nmap scan report for 192.168.1.200
        Host is up (0.0014s latency).
        Not shown: 500 closed ports, 499 filtered ports
        Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
        PORT   STATE SERVICE
        22/tcp open  ssh
        MAC Address: D4:6E:0E:06:1E:33 (Tp-link Technologies)

        Nmap scan report for 192.168.1.220
        Host is up (0.00084s latency).
        Not shown: 997 closed ports
        PORT     STATE SERVICE
        22/tcp   open  ssh
        5901/tcp open  vnc-1
        6001/tcp open  X11:1

        Nmap done: 256 IP addresses (2 hosts up) scanned in 11.69 seconds
```

5.3. Tcpdump

```
acorletti@kali:~$ sudo tcpdump -vv
```

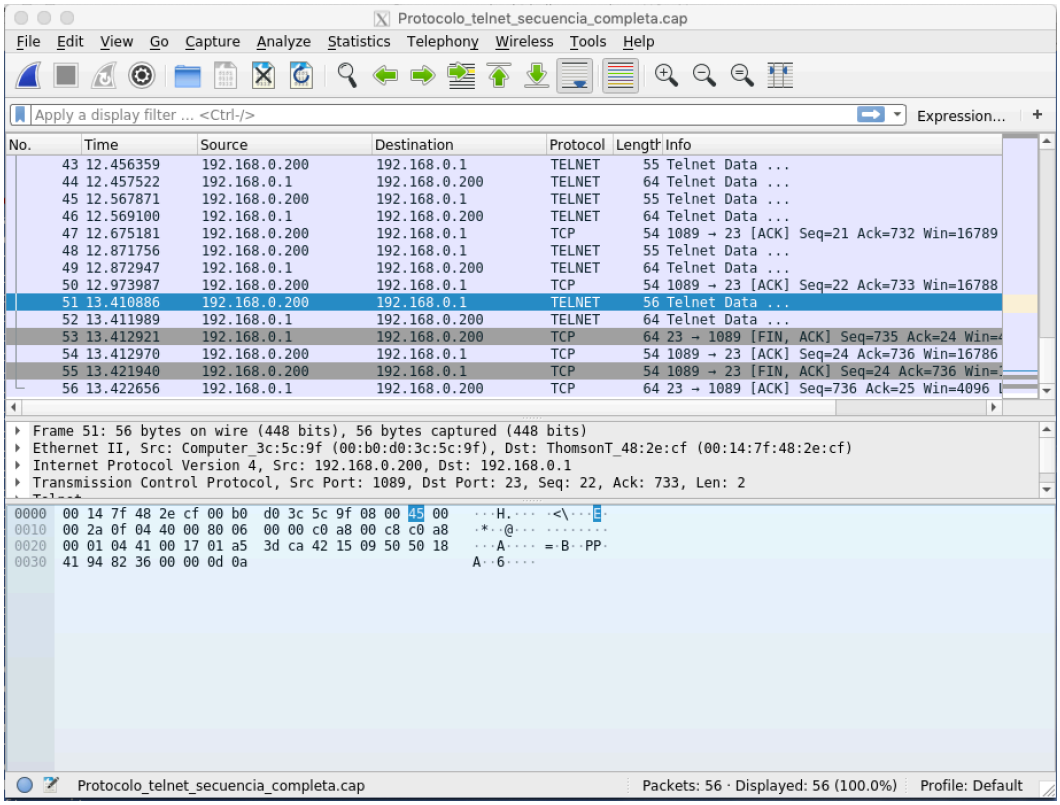
[sudo] password for acorletti:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:30:53.328900 IP (tos 0x12,ECT(0), ttl 64, id 53804, offset 0, flags [DF], proto TCP (6), length 176)
192.168.1.220.ssh > 192.168.1.200.49611: Flags [P.], cksum 0x8597 (incorrect -> 0x82f2), seq 741899841:741899965, ack 2603676647, win 292, options [nop,nop,TS val 1251197797 ecr 670397411], length 124

20:30:53.329634 IP (tos 0x12,ECT(0), ttl 64, id 53805, offset 0, flags [DF], proto TCP (6), length 192)
192.168.1.220.ssh > 192.168.1.200.49611: Flags [P.], cksum 0x85a7 (incorrect -> 0x0639), seq 124:264, ack 1, win 292, options [nop,nop,TS val 1251197798 ecr 670397411], length 140

20:30:53.329774 IP (tos 0x48, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.200.49611 > 192.168.1.220.ssh: Flags [.], cksum 0x4280 (correct), seq 1, ack 124, win 2046, options [nop,nop,TS val 670397804 ecr 1251197797], length 0

20:30:53.330233 IP (tos 0x48, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.200.49611 > 192.168.1.220.ssh: Flags [.], cksum 0x41f4 (correct), seq 1, ack 264, win 2045, options [nop,nop,TS val 670397804 ecr 1251197798], length 0
.....
....

5.4. Wireshark



En la sección de “Capturas de tráfico” de nuestra Web (www.darFe.es) se pueden encontrar varios tipos de capturas de tráfico con las cuales realizar prácticas y ejercicios con Wireshark

En el canal de **Youtube de darFe** puedes encontrar una serie de videos del curso de "Análisis de tráfico" empleando Wireshark.

Análisis de Tráfico - Tema-01: Wireshark - Presentación de la metodología

5.5. John the Ripper

Primero vamos a crear un par de usuarios con contraseñas triviales (para no demorar mucho en el ejercicio)

```
root@kali:/home/acorletti# adduser pepe
        Añadiendo el usuario `pepe' ...
        Añadiendo el nuevo grupo `pepe' (1001) ...
        Añadiendo el nuevo usuario `pepe' (1001) con grupo `pepe' ...
        Creando el directorio personal `/home/pepe' ...
        Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
        passwd: contraseña actualizada correctamente
        Cambiando la información de usuario para pepe
        Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
                Nombre completo []:
                Número de habitación []:
                Teléfono del trabajo []:
                Teléfono de casa []:
                Otro []:
        ¿Es correcta la información? [S/n]
root@kali:/home/acorletti# adduser juan
        Añadiendo el usuario `juan' ...
        Añadiendo el nuevo grupo `juan' (1002) ...
        Añadiendo el nuevo usuario `juan' (1002) con grupo `juan' ...
        Creando el directorio personal `/home/juan' ...
        Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
        passwd: contraseña actualizada correctamente
        Cambiando la información de usuario para juan
        Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
                Nombre completo []:
                Número de habitación []:
                Teléfono del trabajo []:
                Teléfono de casa []:
                Otro []:
        ¿Es correcta la información? [S/n]
root@kali:/home/acorletti# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
.......
...
pepe:x:1001:1001:,,,:/home/pepe:/bin/bash
juan:x:1002:1002:,,,:/home/juan:/bin/bash
```

Copiamos estas dos últimas líneas y las insertamos en el fichero "**pass_kali":**

```
root@kali:/home/acorletti# vi pass_kali
```

Miramos el hash de sus contraseñas:

```
root@kali:/home/acorletti# cat /etc/shadow
root:$6$GQJTjOdcLUOB6RlL$kaGTSvDPqJBSWcPOoD3B.1UQMp2JTZGQf7aTLX.cbSYEP62hUZ/HZY8B3.BcW3VcF0wrgH2AaCs8tNXOs6ZYB1:18142:0:99999:7:::
```

```
.....
...
pepe:$6$W.u3Q0FG93CNZGp5$F402.hDUMrSVHkOOwMBp9kwsm/smXopcE2b0DUCUp/ZRjHTs
9lddIWH70nKLwae8GCFn/uNjstqEFcSPvDE0g/:18204:0:99999:7:::
juan:$6$p5GT.YpYpQ6FtXfl$HFKH/3vJS5KJauTK36SBPqyh9T4cbt97HtycL5zGorLD3jTzojNz6XX3V
s8GQ1vEqaRAwuSx5Aiz6BqvsJrmk.:18204:0:99999:7:::
```

Copiamos estas dos últimas líneas y las insertamos en el fichero "**shadow_kali":**

```
root@kali:/home/acorletti# vi shadow_kali
```

Ejecutamos el comando "unshadow" que es parte de John the Ripper y lo copiamos en el fichero "**prueba":**

```
root@kali:/home/acorletti# unshadow pass_kali shadow_kali > prueba
```

Ejecutamos el comando **john**

```
root@kali:/home/acorletti# john prueba
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 32/32])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist

12345          (pepe)
qwerty         (juan)

2g 0:00:00:10 DONE 2/3 (2019-11-04 21:12) 0.1867g/s 157.7p/s 161.5c/s 161.5C/s
123456..maggie
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

5.6. Medusa.

A título de ejemplo de uso de "medusa" vamos a ejecutarlo sobre el puerto ssh de la portátil, buscando un listado de usuarios y un diccionario de contraseñas.

```
medusa -h 192.168.1.200 -U user_ssh.txt -P passwd_ssh.txt -M ssh -T 10 | tee
salida_medusa_lista_ssh_.txt
```

5.7. SSH forwarding (redirección de puertos SSH).

Una de las más grandes ventajas que ofrece **SSH** (Secure Shell) es la redirección de puertos (SSH Forwarding). Esta funcionalidad, nos permite ir redirigiendo los puertos locales ("-L") o remotos ("-R") de cada una de las máquinas a as cuáles nos estamos conectando, de forma tal de "reflejar" ese puerto de la máquina remota hacia los puertos de mi propia máquina.

En el libro "**Seguridad en Redes**", cuya descarga es gratuita en:
http://darfe.es/joomla/index.php/descargas/viewdownload/5-seguridad/1310-seguridad-en-redes

En el punto 9.3. "Túneles" podéis profundizar todo lo que deseéis sobre este tema.

En este texto, solo presentaremos uno de sus usos, a través de la posibilidad de abrir una página Web en nuestra Raspberry (que NO tiene salida a Internet), empleando únicamente el puerto 22 y pasando por la portátil física a la cuál estamos conectado. Tengamos en cuenta que la información que está viajando entre la Raspberry y la portátil está cifrada pues va a través del protocolo SSH.

En nuestro caso, emplearemos la redirección de puertos para abrir la página de: www.darFe.es en la Raspberry, el comando a ejecutar será:

ssh -L 8000:149.62.170.30:80 ace@192.168.1.200

Luego en la interfaz gráfica de la Raspberry, abrimos un navegador y colocamos como URL:

http://localhost:8000, con lo cual se despliegará la página de darFe.

5.8. Otros ejercicios.

En el canal de **Youtube de darFe**, existen varios ejercicios más que pueden ser de utilidad en la práctica de estas herramientas de Kali.

Ejercicio de fragmentación IP empleando HPING3 y Wireshark
https://www.youtube.com/watch?v=mBqvwdoJVOw&t=205s

Ejercicios de direccionamiento IP con la herramienta "ipcalc" sobre Kali
https://www.youtube.com/watch?v=uvRuuXjQ-Po&t=2s

Yersinia_ataque_STP
https://www.youtube.com/watch?v=U0byfzRY3UU&t=40s

Envenenamiento caché ARP empleando Ettercap sobre Kali
https://www.youtube.com/watch?v=XEEjeBY4Aus

TCP/IP usando Wireshark
https://www.youtube.com/watch?v=Moe5Mj_Wo5w&t=3s

SSH Forwarding
https://www.youtube.com/watch?v=dYK1blKK3xc&t=3s