2.熟悉Kali Linux

勞動部 產業人才投資計畫
中國文化大學 推廣教育部
張耀鴻 副教授
2022年 暑期班

綱要

- 啟動Kali Linux
- Kali Menu
- Kali 說明文件
- Kali Linux 檔案系統與基本命令
- 管理Kali Linux 服務
- 搜尋、安裝和解除安裝工具

啟動Kali Linux

- Virtual Box 下載和安裝
- Kali Linux 下載和安裝
- Metasploitable下載和安裝
- Windows XP SP2下載和安裝
- (若還有硬碟空間)Win Server 2012下載和安裝

登入Kali Linux

- 預設帳密：kali/kali

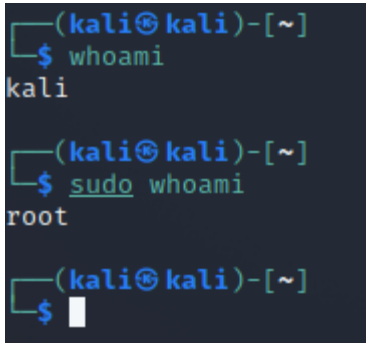
查看IP位址：ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe50:4c14  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:50:4c:14  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1328 (1.2 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 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

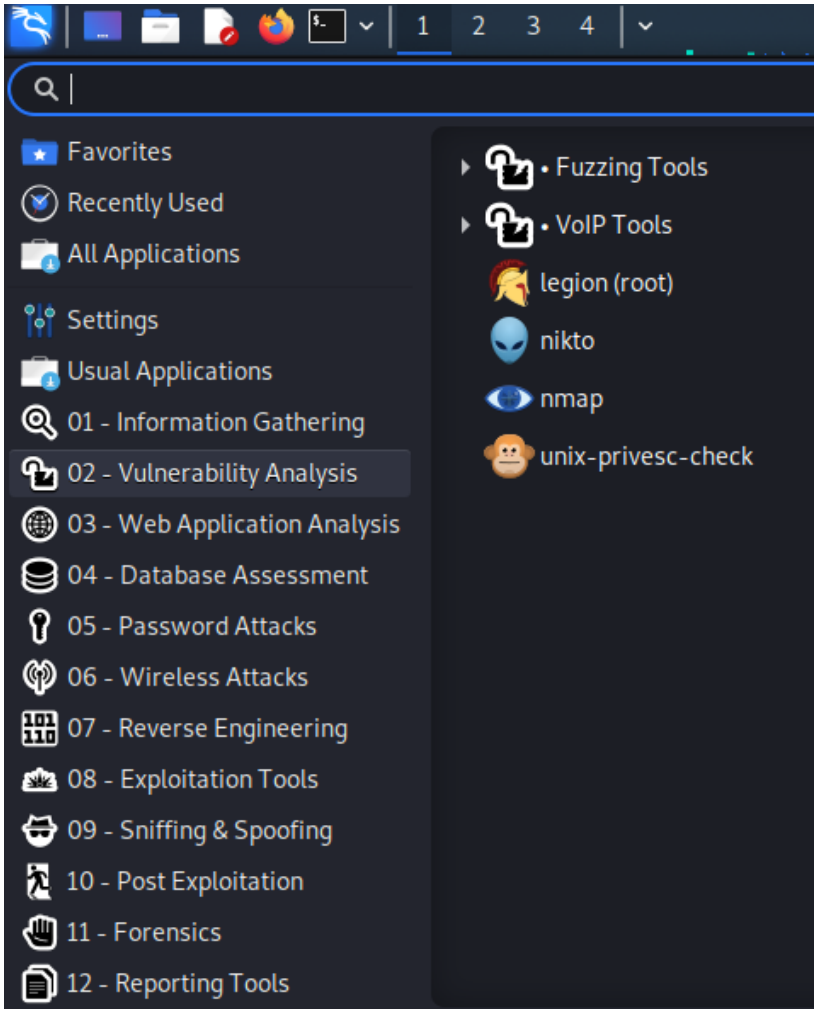
修改root密碼

```
┌──(kali㉿kali)-[~]
└─$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ su
Password:
┌──(root💀kali)-[/home/kali]
└─#
```

whoami



Kali Menu


1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
Fuzzing Tools
VoIP Tools
legion (root)
nikto
nmap
unix-privesc-check

Kali 說明文件

- Kali Linux官方文件
  - ✓ http://docs.kali.org
- Kali Linux支援論壇
  - ✓ https://forums.kall.org
- Kali Linux工具網站
  - ✓ https://tools.kali.org
- Kali Linux Bug追蹤器
  - ✓ https://bugs.kali.org
- Kali Linux培訓
  - ✓ https://kali.training

Exercise 2-1

1. 啟動Kali作業系統，並將kali使用者密碼改成更安全的密碼
2. 熟悉Kali Linux功能表。
3. 利用Kali 工具網站，找到任選幾個工具並查看其文件

Kali Linux 檔案系統

- Kali Linux遵循檔案系統階層式結構標準（filesystem hierarchy standard, FHS），為所有Linux用戶提供了一個熟悉的共通架構：
  - **/bin**：基本程式（ls、cd、cat等）
  - **/sbin**：系統程式（fdisk、mkfs、sysctl等）
  - **/etc**： 配置檔
  - **/tmp**：暫存檔案（通常會在開機時刪除）
  - **/usr/bin**：應用程式（apt、neat、nmap等）
  - **/usr/share**：應用程式支援和資料檔
- 熟悉Linux檔案系統的佈局對提高效率非常有幫助

Kali基本命令

- man
- apropos
- ls
- cd
- pwd
- mkdir
- which
- locate
- find

Exercise 2-2

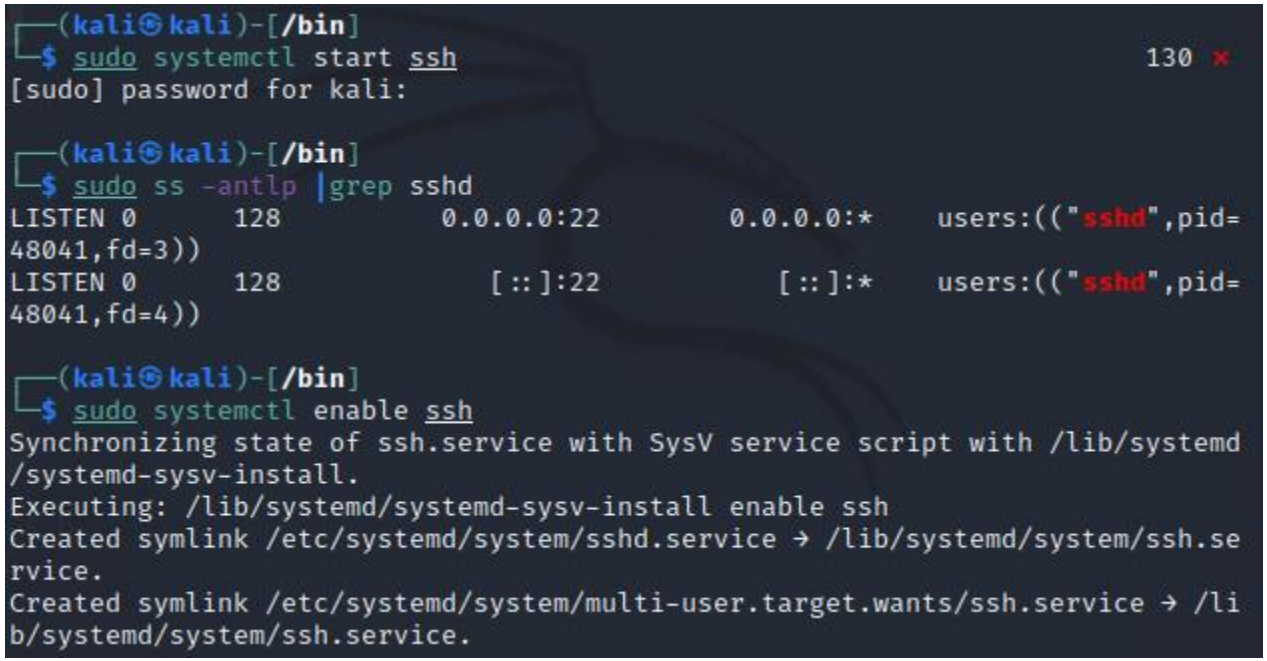
1. 用man查看手冊頁中的一條命令
2. 用man查找與檔案壓縮(compression)相關的關鍵字
3. 用where在Kali虛擬機器上找到pwd命令所在目錄
4. 用locate在Kali虛擬機器上找到**wce32.exe**位置
5. 用find找出在過去一天內修改過、不屬於root的任何檔案（非目錄），並執行ls -l。(不能使用chaining或piping命令

管理Kali Linux 服務

- Kali Linux是一個專門針對安全專業人士的Linux發行版本
- 包含幾個非標準功能
- 預設的Kali安裝附帶了幾個預先安裝的服務，例如SSH、HTTP、MySQL等
- 這些服務將在啟動時載入，這將導致Kali在預設情況下暴露幾個打開的埠，這是出於安全原因我們希望避免的
- Kali透過更新其設置來解決這個問題，以防止網路服務在啟動時啟動

ssh服務

- Secure SHell（SSH）服務最常用於使用安全、加密協定的遠端存取系統
- SSH服務基於TCP，預設情況下監聽通訊埠22
- 要在Kali中啟動SSH服務，可執行systemctl命令，後面跟著start、 再跟著服務名稱（本例為ssh）



http服務 1

- Apache HTTP服務通常會在滲透測試期間使用，用來託管網站，或提供一個用來將檔案下載到受害機器的平台
- HTTP服務是基於TCP，預設監聽埠為80
- 要在Kali中啟動HTTP服務，我們可以像啟動SSH服務一樣使用systemctl，將服務名稱替換為"apache2"：

```
┌──(kali㉿kali)-[/bin]
└─$ sudo systemctl start apache2
```

- 與SSH服務一樣，可以用ss和grep命令驗證HTTP服務是否正在TCP埠80上執行和偵聽
-

```
┌──(kali㉿kali)-[/bin]
└─$ sudo ss -antlp |grep apache
LISTEN 0      511                *:80              *:*    users:(("apache2",p
id=49604,fd=4),("apache2",pid=49603,fd=4),("apache2",pid=49602,fd=4),("apache
2",pid=49601,fd=4),("apache2",pid=49600,fd=4),("apache2",pid=49594,fd=4))
```

http服務 2

- 要讓HTTP服務在啟動時啟動，就像SSH服務一樣，我們需要用systemctl 及其enable選項來啟動apache2：

```
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

- Kali Linux中的大多數服務透過其服務或init腳本以與SSH和HTTP幾乎相同的方式執行。要查看所有可用服務的表格，可執行systemctl，後面跟著選項list-unit-files：

```
└─$ systemctl list-unit-files
UNIT FILE                                                  ST>
proc-sys-fs-binfmt_misc.automount                          st>
-.mount                                                    ge>
dev-hugepages.mount                                        st>
```

Exercise 2-3

1. 練習啟動和停止各種Kali服務
2. 在系統開機時啟用SSH服務

搜尋、安裝和解除安裝工具

- Kali Linux包含滲透測試領域最常用的工具
- 但是Kali中無法包含所有的工具
- 因此需要討論如何搜尋、安裝或刪除工具
- 本節將探索Advanced Package Tool（APT）工具集以及在Kali Linux作業系統上執行維護操作時有用的其他命令
- APT是一套管理Debian系統的套件或應用程式的工具
- 由於Kali基於Debian ，因此可用APT安裝和刪除應用程式、更新軟體，甚至升級整個系統

apt update

- 有關APT套件的資訊在本地緩存，以加快任何查詢APT資料庫的操作
- 可用套裝軟體的版本、描述等相關的資訊需要時常更新
- 可以透過apt update命令來實現：

```
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://packages.microsoft.com/repos/code stable InRelease [10.4 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:3 http://packages.microsoft.com/repos/code stable/main armhf Packages [73
.9 kB]
```

apt upgrade

- 更新APT資料庫後，我們可以用apt upgrade命令將已安裝的套裝軟體和核心系統升級到最新版本
- 要升級單個套件，可在命令後面添加套件名稱，例如**apt upgrade metasploit-framework**

apt-cache search

- apt-cache search命令顯示儲存在內部緩存套件資料庫中的大部分資訊
- 例如，假設想透過APT安裝pure-ftpd應用程式
- 所要做的第一件事是確定該應用程式是否存在於Kali Linux儲存庫中：

```
└─$ apt-cache search pure-ftpd
ftpd - File Transfer Protocol (FTP) server
mysqmail-pure-ftpd-logger - real-time logging system in MySQL - Pure-FTPd tra
ffic-logger
pure-ftpd - Secure and efficient FTP server
pure-ftpd-common - Pure-FTPd FTP server (Common Files)
pure-ftpd-ldap - Secure and efficient FTP server with LDAP user authenticatio
n
pure-ftpd-mysql - Secure and efficient FTP server with MySQL user authenticat
ion
pure-ftpd-postgresql - Secure and efficient FTP server with PostgreSQL user a
uthentication
resource-agents - Cluster Resource Agents
```

apt show

- resource-agents套件出現在前述的搜尋中，儘管它的名稱不包含"pure ftpd"關鍵字
- 這背後的原因是在apt-cache search的描述中查找的是所請求的關鍵字，而不是套件名稱本身
- 要確認 resource-agents 套件描述確實包含 "pure-ftpd"關鍵字，請將套件名稱傳給 apt show，如下所示：

```
└─$ apt show resource-agents
Package: resource-agents
Version: 1:4.7.0-1
Priority: optional
Section: admin
Maintainer: Debian HA Maintainers <debian-ha-maintainers@alioth-lists.debian.
net>
Installed-Size: 2,718 kB
Provides: resource-agents-dev
```

apt install

- apt install命令可用來在系統中添加一個套件，後跟套件名稱。以之前的pure-ftpd為例：

```
└─$ sudo apt install pure-ftpd
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 locales
  openbsd-inetd pure-ftpd-common tcpd
Suggested packages:
  glibc-doc libnss-nis libnss-nisplus manpages-dev
Recommended packages:
  manpages-dev libc-devtools
The following NEW packages will be installed:
```

apt remove --purge

- apt remove --purge命令將從Kali中將套件完全刪除
- 需要注意的是，用apt remove會刪除所有套件的資料，但通常會留下小的（修改過的）使用者設定檔，以防意外刪除
- 若加上--purge選項則會刪除所有剩餘內容

```
└─$ sudo apt remove --purge pure-ftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  pure-ftpd-common
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  pure-ftpd*
0 upgraded, 0 newly installed, 1 to remove and 987 not upgraded.
After this operation, 669 kB disk space will be freed.
Do you want to continue? [Y/n]
```

dpkg

- dpkg是用來直接或間接透過APT安裝套件的核心工具，也是離線操作時首選的工具，因為它不需要互聯網連接
- 請注意，dpkg不會安裝套件可能需要的任何依賴項
- 要用dpkg安裝套件，請提供-i或--install選項和.deb套件檔的路徑
- 以上是假設要安裝的.deb套件檔之前已下載或以其他方式獲得

```
└─$ sudo dpkg -i man-db_2.10.1-1_amd64.deb
[sudo] password for kali:
(Reading database ... 269441 files and directories currently installed.)
Preparing to unpack man-db_2.10.1-1_amd64.deb ...
Unpacking man-db (2.10.1-1) over (2.9.4-2) ...
Setting up man-db (2.10.1-1) ...
Installing new version of config file /etc/cron.daily/man-db ...
Installing new version of config file /etc/cron.weekly/man-db ...
Installing new version of config file /etc/manpath.config ...
Updating database of manual pages ...
man-db.service is a disabled or a static unit not running, not starting it.
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for mailcap (3.70) ...
```

Exercises 2-4

1. 拍攝Kali虛擬機器的快照
2. 搜尋目前未安裝在Kali中的工具
3. 安裝該工具
4. 解除該工具
5. 將Kali虛擬機器還原為以前拍攝的快照


END