KLCP

0xjamesli228

Table des matières

Chapitre 1 - Linux Fundamentals

- Two types of device files : block and character. (b stands for block and c stands for character).

```
$ ls -l /dev/sda /dev/ttyS0
brw-rw---- 1 root disk    8,  0 Mar 21 08:44 /dev/sda
crw-rw---- 1 root dialout 4, 64 Mar 30 08:59 /dev/ttyS0
```

- ZSH is the default shell provided in Kali Linux.
- When in a shell, remember the trailing $ stands for normal user and # stands for root.
- Know the purpose and basic usage of the following common commands :
  - **cd** (change directory)
  - **pwd** (print working directory)
  - **ls** (list file or directory contents)
  - **mkdir** (create directory)
  - **rmdir** (remove empty directory)
  - **mv, rm, cp** (move, remove, or copy file or directory respectively)
  - **cat** (concatenate or show file)
  - **less/more** (show files a page at a time)
  - **editor** (start a text editor)
  - **find** (locate a file or directory)
  - **grep** (search contents of the files ; -r for recursive search on all files in the directory)
  - **free** (display memory information ; -h for human readable format)
  - **df** (show disk free space ; -h for human readable format)
  - **id** (display user identity along with the list of groups it belongs to)
  - **type** (provide information about whether a command is a built-in shell command, an alias, a function, or an external executable)
  - **which** (locate a command)
  - **echo** (display line of text on the terminal)
  - **dmesg** (review kernel logs)
  - **file** (determine file type)

- The PATH environment variable contains a list of directories where the system looks for executable files when you type a command.

```
$ echo \$PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

- FHS (Filesystem Hierarchy Standard).
/bin : basic programs.
/boot : kernel files.
/dev : device files.
/etc : configuration files.
/home : user's personal files.
/lib : basic libraries.
/media : mount points for removable devices.
/mnt : temporary mount point.
/opt : extra applications provided by third parties.
/root : root's personal files.
/run : volatile runtime data.
/sbin : system programs.
/srv : data used by servers hosted on the system.
/tmp : temporary files.
/usr : user applications.
/var : log files, queues, spools, and caches.
/proc, /sys : kernel objects and attributes

- **cd~** goes to the home directory and cd - goes back to the former working directory.
- **ps aux** lists all currently running processes.
- **kill -9 pid** force kill a process.
- A command can be run in the background if followed by &. The jobs command lists the processes running in the background ; **fg %job-number** restores a job to the foreground. When a command is running in the foreground, Control+Z can be used to pause the process and regain the control of the command line. The process can then be resumed in the background with **bg %job-number**.

- Each file or directory has permission for three categories of users :
  — owner : u
  — group : g
  — others : o
- Three types of rights for file and directory :
  — read : r
  — write : w
  — execute : x
- Access rights for directory (it is handled differently from a file) :
  — Read : List directory contents (e.g. when using the ls command).
  — Write : Create, rename and delete files and subdirectories.
  — Execute : Grants the ability to enter the directory and access its contents (e.g. when using the cd command).
- setuid and setgid on executables (s) : execute the program with the rights of the owner or the group, respectively.
- setgid on directories : Newly-created item in such directories is automatically assigned the owner group of the parent directory, instead of inheriting the creator's main group as usual.
- sticky bit (t) : When set on a directory, the sticky bit ensures that only the file owner, the directory owner, or the root user can delete or rename the files within that directory. This is commonly used on directories like /tmp to prevent users from deleting each other's files.
- Three commands control the permissions associated with a file :
  — **`chown user`** *`file`* - changes the owner of the file.
  — **`chgrp group`** *`file`* - alters the owner group.
  — **`chmod rights`** *`file`* - changes the permissions of the file.
- Octal representation of the rights :
  — read=4
  — write=2
  — execute=1
- Assign rights using symbolic representation and octal representation using the chmod command.

```
# rwx for owner, add rw to owner group, remove r for others
chmod u=rwx,g+rw,o-r file

# add x to all users
chmod a+x file

# rwx for owner, rx for group, r for others
chmod 754 file
```

- Special rights are prefixed by a fourth digit :
  — setuid=4
  — setgid=2
  — sticky=1
- The use of octal notation only allows you to set all the rights at once on a file ; you cannot use it to add a new right.
- The **`umask`** command is used to restrict permissions on newly created files. When an application creates a file, the system automatically removes the rights defined with umask.
- The command **`chmod -R a+X`** *`directory`* is used to recursively apply execute permissions in a specific way to a directory and its contents.
For directories : The command ensures that all directories within the specified path have the execute (x) permission. For files : The execute (x) permission is added only if the file already has execute permissions for any user (owner, group, or others). This means it won't indiscriminately make all files executable ; only those files that were already executable for some users will have the execute permission extended to all users.
- The **`uname -a`** command returns a single line documenting the kernel name, the hostname, the kernel release, the kernel version, the machine type, and the OS name. uname -r can be used to obtain only the kernel release.

```
$ uname -a
Linux kali 6.8.11-amd64 \#1 SMP PREEMPT\_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86\_64 GNU/Linux

$ uname -r
6.8.11-amd64
```

- The `textbfjournalctl` command can be used to query logs from Systemd's journal (stdout/stderr output of services, syslog messages, kernel logs) :
  — `-f` Continuously print new log entries.
  — `-u` Query messages from a specific systemd unit (e.g. journalctl -u ssh.service).
- Commands that can be used to summarize hardware details :

— **lspci** Lists PCI devices.
— **lsusb** Lists USB devices.
— **lspcmcia** Lists PCMCIA cards.
— **lshw** List various hardware devices and its configurations in a hierarchical manner.
- Example on using the hardware commands :
— To find out the type of CPU on Kali : **sudo dmesg | grep CPU0**
— Gather information on Ethernet adapter : **lspci | grep Ethernet**
— Gather information on GPU : **lspci -v -s `lspci | grep VGA | cut -f1 -d `**
- Linux has two distinct regions of memory space :
— User space : Memory area where user-mode application processes run.
— Kernel space : Memory area where the kernel executes and provides its services.
- Filenames that start with a dot are hidden by default ; ls -a can be used to list hidden files.

```
\$ ls -a
.
..
.bash\_history
.bash\_logout
.bashrc
.bashrc.original
.cache
[...]
```

- The **locate** command should have taken less time then find command because it searches a precompiled database for the requested file. This database is generated using the **updatedb** command.

Chapter 2 - Introduction

This chapter is not relevant to the exam.

Chapter 3 - About Kali Linux

- Kali 1.0 is based on Debian 7 Wheezy ; Kali 2.0 is based on Debian 8 Jessie ; Kali rolling is based on Debian Testing.
- Kali Linux is a rolling distribution, which means that you will receive updates every single day.
- Xfce is Kali Linux's default desktop environment.
- In contrast to Debian, Kali disables by default any network services such as HTTP and SSH.
- Best way to suggest a new tool addition is to open a New Tool Requests ticket on Kali Bug Tracker.
- Live mode boots to RAM and an installed instance of Kali boots to a storage device.
- Live mode boots to RAM, but may auto-mount disks. Forensics mode does not auto-mount disks.

Chapter 4 - Getting Started with Kali Linux

- Ways to find out if the CPU is 32-bit or 64-bit :
uname -m x86_64, arm64, amd64 all mean 64-bit and i386 means 32-bit. Inspect /proc/cpuinfo
- Verify the checksum of the downloaded ISO image :
sha256sum kali-linux-2020.3-live-amd64.iso
shasum -a 256 kali-linux-2020.3-live-amd64.iso
- Ways to import Kali's public GPG key :
wget -q -O - https://archive.kali.org/archive-key.asc | gpg --import
gpg --keyserver hkps://keys.openpgp.org --recv-key 44C6513A8E4FB3D30875F758ED444FF07D8D0BF6
- Display the fingerprint of a specific GPG key : **gpg --fingerprint 44C6513A8E4FB3D30875F758ED444FF07D8D0BF6**
- Verify the checksum file with the associated signature file : **gpg --verify SHA256SUMS.gpg SHA256SUMS**
- Verify if the downloaded IOS file has the same checksums in the checksum file
grep kali-linux-2020.3-live-amd64.iso SHA256SUMS | sha256sum -c
- Create a bootable USB using command line :
dd if=kali-linux-2020.3-live-amd64.iso of=/dev/sdb bs=1M
if - input file.
of - output file.
bs - block size in bytes.
- It's possible to use the Disks Utility (in the gnome-disk-utility package) application for creating a bootable Kali USB drive on Linux.

Chapter 5 - Installing Kali Linux

- Kali minimal installation requirements : 2GB of RAM and 20GB of disk space.
- During disk partitioning, the "All files in one partition" method actually contains two partitions : the root ("/") partition and the swap partition (virtual memory).
- The default file system on Kali is ext4.
- Swap partition : When the Linux kernel lacks sufficient free memory, it will store inactive parts of RAM in a special swap partition on the hard disk.
- The boot loader is the first program started by the BIOS. This program loads the Linux kernel into memory and then executes it. GRUB is the default boot loader installed by Kali.
- Logical Volume Management (LVM) : It allows you to create virtual partitions that span several disks.
- Linux Unified Key Setup (LUKS) : Technology for encrypting partitions.
- When an encrypted partition is used, the encryption key is stored in memory (RAM), and when hibernating, a laptop will copy the key, along with other contents of RAM, to the hard disk's swap partition.
- The Debian and Kali installers are essentially just scripts based on debconf which can interact with users and store installation parameters. The installer can also be automated through debconf preseeding, a function that allows you to provide unattended answers to installation questions.
- You can preseed any installer question with boot parameters that end up in the kernel command-line, accessible through /proc/cmdline
- You can add a file named preseed.cfg at the root of the installer's initrd. This method also does not have any restrictions on the questions that you can preseed as the preseed file is available immediately after boot.
- Preseed file loaded from the network : boot parameter preseed/url=http ://server/preseed.cfg
- A preseed file is a plain text file in which each line contains the answer to one Debconf question. A line is split across four fields separated by white space or tab ; d-i mirror/suite string kali-rolling
- You can inspect and modify the debconf database with debconf-get and debconf-set
- Default Kail installation has the username kali and the password kali.
- Kali installer makes use of multiple virtual consoles ; the second and third consoles (CTRL+ALT+F2 and CTRL+ALT+F3, respectively) host shells that you can use to investigate the current situation in more detail ; the fourth console (CTRL+ALT+F4) displays logs of what is happening.
- Full system installation log is available in /var/log/syslog
- It's possible to install Kali Linux alongside an existing Windows operating system on the same machine. This technique is called dual booting.

Chapter 6 - Configuring Kali Linux

- In a typical desktop installation, you will have NetworkManager already installed and it can be controlled and configured through Xfce's system settings and through the top-right menu.
- You can configure the network from the command line with the ifup and ifdown tools, which read their instructions from the /etc/network/interfaces configuration file. An even newer tool, systemd-networkd works with the systemd init system.
- The **sudo** command allows privileged users to run commands with root permissions.
- The **su** command switches the current user to another user. By default, it switches to the root user if no username is provided. Flags (–login, or -l, or -) can be used to start the shell under substituted user's login environment.
- The wpasupplicant package (included in Kali by default) provides many wpa-* options that can be used in /etc/network/interfaces
- Note that system-networkd is disabled by default, so if you want to use it, you should enable it. It also depends on systemd-resolved for proper integration of DNS resolution, which in turn requires you to replace /etc/resolv.conf with a symlink to /run/systemd/resolve/resolv.conf

```
systemctl enable systemd-networkd
systemctl enable systemd-resolved
systemctl start systemd-networkd
systemctl start systemd-resolved
ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

- Database files of Unix users and groups :
  - /etc/passwd - list of users.
  - /etc/shadow - encrypted passwords of users.
  - /etc/group - list of groups.
  - /etc/gshadow - encrypted passwords of groups.
- The **getent** command is used to consult the user database and other system databases.
- The **adduser** command is used to create new user account.

`adduser user group` : Add a user to a group.
- The creation of an account triggers the population of the user's home directory with the contents of the /etc/skel/ template.
- Commands for modifying an existing user or password :
  - **`passwd`** Change user password.
  - **`passwd -e`** user Force user to change password at next login.
  - **`passwd -l`** user Lock user.
  - **`passwd -u`** user Unlock user.
  - **`chfn`** (Change Full Name) Modify GECOS (general information) field.
  - **`chsh`** (Change Shell) Change the user's login shell.
  - **`chage`** (Change Age) Change password expiration.
  - **`chage -l user`** List user's password settings.
- Commands related to group management :
  - **`addgroup`** Add a group.
  - **`delgroup`** Delete a group.
  - **`groupmod`** Modify a group.
  - **`gpasswd`** Change group password.
  - **`gpasswd -r group`** Remove group password.
  - **`newgrp`** Start a new shell with different group.
  - **`sg`** Execute command using different group.
- Service or program that runs as a background process is called daemon.
- Examples of configuration files of a package are provided in /usr/share/doc/package/examples/
- In Kali Linux, SSH service is disabled by default and is not started at boot time.
- SSH configuration file : /etc/ssh/sshd_config
- The default SSH configuration allows password-based logins. It can be disabled by setting PasswordAuthentication to no.
- Generate new SSH host keys :

```
# rm /etc/ssh/ssh_host_*
# dpkg-reconfigure openssh-server
# systemctl restart ssh
- PostgreSQL allows multiple versions of the database server to be co-installed. It is also possible to handle mu
```

- In order for clusters to run side-by-side, each new cluster gets assigned the next available port number, usually 5433 for the second cluster.
- By default, PostgreSQL listens for incoming connections in two ways : on TCP port 5432 of the localhost interface and on file-based socket /var/run/postgresql/.s.PGSQL.5432
- By default, connections on the file-based socket use the Unix user account as the name of the PostgreSQL user, and it assumes that no further authentication is required. On the TCP connection, PostgreSQL requires the user to authenticate with a username and a password.
- The postgres user has full administrative privileges over all databases.
- Database commands for PostgreSQL :
  - **`createuser`** Adds a new user.
  - **`dropuser`** Removes a user.
  - **`createdb`** Adds a new database.
  - **`dropdb`** Removes a database.
  - **`psql`** Command-line interface for interacting with PostgreSQL.
- Debian's postgresql-common package provides multiple tools to manage PostgreSQL clusters : pg_createcluster, pg_dropcluster, pg_ctlcluster, pg_upgradecluster, pg_renamecluster, and pg_lsclusters.
- A typical Kali Linux installation includes the Apache web server, provided by the apache2 package.
- In Apache 2, **`a2enmod`** enables a new module and a2dismod disable a module. These commands actually create or delete symbolic links in /etc/apache2/mods-enabled/, pointing at the actual files stored in /etc/apache2/mods-available/
- With Apache 2 default configuration, the web server listens on port 80 (as configured in /etc/apache2/ports.conf), and serves pages from /var/www/html/ (as configured in /etc/apache2/sites-enabled/000-default.conf).
- The default configuration for Apache 2 enables name-based virtual hosts. In addition, a default virtual host is defined in /etc/apache2/sites-enabled/000-default.conf. Requests concerning unknown virtual hosts will always be served by the first defined virtual host.
- The command **`a2ensite hostname`** is used to enable the new virtual host.
- Commonly-used Apache configuration directives : DirectoryIndex Contains a list of files to try when the client request matches a directory. The first existing file in the list is used and sent as a response.
AllowOverride Controls whether and how .htaccess files can override the server's default configuration settings.
Options Followed by a list of options to enable.

None Disables all options.
All Enables all options except MultiViews.
ExecCGI Indicates that CGI scripts can be executed.
FollowSymLinks Tells the server that symbolic links can be followed.
SymLinksIfOwnerMatch Tells the server to follow symbolic links, but only when the link and its target have the same owner.
Includes Enables Server Side Includes (SSI).
Indexes Lists the contents of a directory if the request points to a directory without an index file.
MultiViews Enables content negotiation ; this can be used by the server to return a web page matching the preferred language as configured in the browser.
Require Controls access restrictions for a directory.
Require ip 192.168.0.0/16 Restricts access to the local network.
- Require basic authentication using .htaccess
Require valid-user
AuthName "Private directory"
AuthType Basic
AuthUserFile /etc/apache2/authfiles/htpasswd-private
- The basic HTTP authentication is encoded using base64 and sent in clear text.
- The /etc/apache2/authfiles/htpasswd-private file contains a list of users and passwords ; it is commonly manipulated with the htpasswd command.

```
# htpasswd /etc/apache2/authfiles/htpasswd-private user
New password:
Re-type new password:
Adding password for user user
```

- Kali uses systemd as its init system, which is not only responsible for the boot sequence, but also permanently acts as a full featured service manager, starting and monitoring services.
- Commonly-used commands to manipulate systemd :
  - **`systemctl list-units`** Outputs a list of the active units.
  - **`systemctl status`** Shows a hierarchical overview of the running services.
  - **`systemctl enable foo.service`** Enables the service to start at boot.
  - **`systemctl disable foo.service`** Disables the service to start at boot.
  - **`systemctl start foo.service`** Runs the service immediately.
  - **`systemctl stop foo.service`** Stops the service immediately.
  - **`systemctl reload foo.service`** Reloads the service after configuration change.
  - **`systemctl restart foo.service`** Restarts the service.
- Each service is represented by a service unit, which is described by a service file in one of the following locations :
/lib/systemd/system/
/run/systemd/system/
/etc/systemd/system/
- Add the user to the sudo group : **`usermod -a -G sudo user`**
- Change the user's login shell to bash : **`chsh -s /bin/bash user`**
- Bring down the eth0 interface : **`ifconfig eth0 down`** or **`ifdown eth0`**
- The Kali Linux policy of disabling network services by default is configured by /lib/systemd/system-preset/95-kali.preset,99-default.preset

Chapter 7 - Helping Yourself and Getting Help

- To view a manual page : man manual-page
- Manual page numbered sections :
1. Executable programs or shell commands
2. System calls
3. Library functions
4. Devices (special files placed in /dev)
5. Configuration files
6. Games
7. Macros and standards
8. Root commands
9. Kernel routines
- You can specify the section of the manual page that you are looking for. To view the documentation for the read system call, you would type man 2 read

- The apropos command returns a list of manual pages whose summary mentions the requested keywords, along with the one-line summary from the manual page.

```
$ apropos "copy file"
cp (1)               - copy files and directories
cpio (1)             - copy files to and from archives
gvfs-copy (1)        - Copy files
gvfs-move (1)        - Copy files
hcopy (1)            - copy files from or to an HFS volume
install (1)          - copy files and set attributes
ntfscp (8)           - copy file to an NTFS volume.
```

- The GNU project has written manuals for most of its programs in the info format ; this is why many manual pages refer to the corresponding info documentation. The command info can be used to view these pages. The pinfo command (from the pinfo package) can also be used to view the info documents.
- In addition to man, you can use konqueror (in KDE) and yelp (in GNOME) to search manual pages as well.
- Package documentation is generally placed in /usr/share/doc/package/ directory as a README file.
- The Kali project maintains a collection of useful documentation at https ://www.kali.org/docs/.
- The Kali Linux project uses the #kali-linux channel on the OFTC IRC network. You can use irc.otfc.net as IRC server, on port 6697 for a TLS-encrypted connection or port 6667 for a clear-text connection. To join the discussions on IRC, you have to use an IRC client such as hexchat (in graphical mode) or irssi (in console mode).
- The official community forums for the Kali Linux project are located at forums.kali.org.
- The two primary official Kali support community resources are Kali-Linux IRC channel and Kali Forums.
- Some bug reports should be filed to Kali, while others may be filed to Debian. Command like `dpkg -s package-name | grep^Version` : will reveal the version number and will be tagged as "kali" if it is a Kali-modified package.

```
$ dpkg -s cherrytree | grep ^Version:
Version: 0.38.8-0kali1
```

- Identifying the upstream project and finding where to file the bug report is usually easy. You just have to browse the upstream website, which is referenced in the Homepage field of the packaging meta-data.

```
$ dpkg -s wpscan | grep ^Homepage:
Homepage: https://wpscan.com/wordpress-security-scanner
```

- Kali uses a web-based bug tracker at https ://bugs.kali.org/ where you can consult all the bug reports anonymously, but if you would like to comment or file a new bug report, you will need to register an account.
- Debian uses mostly a email-based bug tracking system known as Debbugs. To open a new bug report, you can send an email (with a special syntax) to submit@bugs.debian.org or you can use the reportbug command, which will guide you through the process.
- Many projects are hosted on GitHub and use GitHub issues to track their bugs, there are also many others hosting their own trackers.

Chapter 8 - Securing and Monitoring Kali Linux

- The term risk is used to refer collectively to these three factors : what to protect, what should be prevented, and who might make this happen.
- fail2ban can be used to detect and block password-guessing attacks and remote brute force password attacks.
- The Linux kernel embeds the netfilter firewall. You can control netfilter with iptables and ip6tables commands (for IPv4 and IPv6 respectively). The GUI-based fwbuilder tool provides a graphical representation of the filtering rules.
- Netfilter uses four distinct tables :
  - filter - concerns filtering rules (accepting, refusing, or ignoring a packet).
  - nat - concerns translation of source or destination addresses and ports of packets.
  - mangle - concerns other changes to the IP packets (including the ToS-Type of Service-field and options).
  - raw - allows other manual modifications on packets.
- The filter table has three standard chains :
  - INPUT - concerns packets whose destination is the firewall itself.
  - OUTPUT - concerns packets emitted by the firewall.
  - FORWARD - concerns packets passing through the firewall.
- The nat table also has three standard chains :
  - PREROUTING - to modify packets as soon as they arrive.
  - POSTROUTING - to modify packets when they are ready to go on their way.
  - OUTPUT - to modify packets generated by the firewall itself.
- Netfilter rule actions :

— ACCEPT : allow the packet to go on its way.
— REJECT : reject the packet with an ICMP error packet.
— DROP : delete (ignore) the packet.
— LOG : log a message via syslogd with a description of the packet. This action does not interrupt processing. The execution of the chain continues at the next rule.
— ULOG : log a message via ulogd, which can be more efficient than syslogd for handling large numbers of messages. chain_name : jump to the given chain and evaluate its rules.
— RETURN : interrupt processing of the current chain and return to the calling chain.
— SNAT (only in the nat table) : apply Source Network Address Translation (SNAT) which defines the new source IP address and/or port.
— DNAT (only in the nat table) : apply Destination Network Address Translation (DNAT) which defines the new destination IP address and/or port.
— MASQUERADE (only in the nat table) : apply masquerading (a special case of Source NAT).
— REDIRECT (only in the nat table) : transparently redirect a packet to a given port of the firewall itself.

- Internet Control Message Protocol (ICMP) is the protocol used to transmit ancillary information on communications. It tests network connectivity with the ping command.
- Note that although an IPv4 network can work without ICMP, ICMPv6 is strictly required for an IPv6 network.
- iptables -t table option indicates which table to operate on (by default, filter).
- Major options for interacting with iptables/ip6tables chains :
— L chain lists the rules in the chain.
— N chain creates a new chain.
— X chain deletes an empty chain.
— A chain rule adds a rule at the end of the given chain.
— I chain rule_num rule inserts a rule before the specified rule number.
— D chain rule_num (or -D chain rule) deletes a rule in a chain.
— F chain flushes a chain (deletes all its rules). If no chain is mentioned, all the rules in the table are deleted.
— P chain action defines the default action for a given chain.
— iptables -P INPUT DROP drop all incoming traffic by default.
- Each iptables rule is expressed as conditions -j action action_options. For example, to silently block incoming traffic from the IP address 10.0.1.5 and the 31.13.74.0/24 class C subnet :

```
# iptables -A INPUT -s 10.0.1.5 -j DROP
# iptables -A INPUT -s 31.13.74.0/24 -j DROP
# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  -- 10.0.1.5             0.0.0.0/0
DROP       all  -- 31.13.74.0/24        0.0.0.0/0
```

- Dropping a rule will renumber all the rules appearing further down in the chain.

```
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  -- 10.0.1.5             0.0.0.0/0
2    DROP       all  -- 31.13.74.0/24        0.0.0.0/0
3    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
4    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
5    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
# iptables -D INPUT 2
# iptables -D INPUT 1
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
2    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
3    ACCEPT     tcp  -- 0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
```

- The logcheck program monitors log files every hour by default and sends unusual log messages in emails to the administrator for further analysis.
- The use of braces in a bash command can be used as a shorthand for repeating parts of the command. Bash will expand out the command before executing it. The example below has the same outcome.

```
# touch /home/kali/file1.txt /home/kali/file2.txt /home/kali/file3.txt
# touch /home/kali/file{1,2,3}.txt
```

- `top` is an interactive tool that displays a list of currently running processes.
- `dpkg --verify` (or dpkg -V) displays the system files that have been modified, but relies on checksums.

- Advanced Intrusion Detection Environment (AIDE) checks file integrity and detects any changes against a previously-recorded image of the valid system.
- Tripwire is very similar to AIDE but uses a mechanism to sign the configuration file, so that an attacker cannot make it point at a different version of the reference database.
- rkhunter, checksecurity, and chkrootkit can be used to detect rootkits on the system.

Chapter 9 - Debian Package Management

- APT installs the package from an online source and works to resolve dependencies while dpkg installs a package located on the local system and does not automatically resolve dependencies.
- The /etc/apt/sources.list file is the key configuration file for defining package sources.
- The first field of /etc/apt/sources.list indicates the source type :
  - deb for binary packages.
  - deb-src for source packages.
  - deb http ://http.kali.org/kali kali-rolling main non-free contrib
  - deb-src https ://http.kali.org/kali kali-rolling main contrib non-free
- Debian and Kali use three sections to differentiate packages according to the licenses chosen by the authors of each work :
  - main contains all packages that fully comply with the Debian Free Software Guidelines.
  - non-free contains software that does not entirely conform to the Free Software Guidelines but can nevertheless be distributed without restrictions.
  - contrib includes open source software that cannot function without some non-free elements.
- Kali maintains several repositories :
  - kali-rolling main repository for end-users and should always contain installable and recent packages.
  - kali-dev used by Kali developers and is not for public use.
- Download the list of currently-available packages : apt update
- Install new package : apt install package. APT will automatically install the necessary dependencies.
- Reinstall a package : **apt --reinstall install package**
- To remove a package : **apt remove package**. It will also remove the reverse dependencies of the package (i.e. packages that depend on the package to be removed).
- To purge a package : **apt purge package**. Unlike a removal, this will not only remove the package but also its configuration files and the associated user data.
- To install regular upgrades and security updates, use either apt upgrade, apt-get upgrade, or aptitude safe-upgrade. These commands look for installed packages that can be upgraded without removing any packages.
- For more important upgrades, such as major version upgrades, use apt full-upgrade. With this instruction, apt will complete the upgrade even if it has to remove some obsolete packages or install new dependencies.
- The http.kali.org in sources.list is a server running Mirrorbits which will redirect your HTTP requests to an official mirror close to you. The command **curl -sI http://http.kali.org/README** can be used to see where you are being redirected.

```
$ curl -sI http://http.kali.org/README
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 26 Jan 2024 06:05:36 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: private, no-cache
Link: <http://kali.download/kali/README>; rel=duplicate; pri=1; geo=ae
Link: <http://archive-4.kali.org/kali/README>; rel=duplicate; pri=2; geo=fr
Location: http://mirror.accuris.ca/kali/README
```

- dpkg options that can be used to interact with Debian packages :
  - **dpkg -i file.deb** (or –install) - installs a package.
  - **dpkg -i --force-overwrite file.deb** - ignore errors and forcible install a package.
  - **dpkg -L package** (or –listfiles) - lists the files that were installed by the specified package.
  - **dpkg -S file** (or –search) - finds any packages containing the file or path.
  - **dpkg -l** (or –list) - displays the list of packages known to the system and their installation status.
  - **dpkg -c file.deb** (or –contents) - lists all the files of the specified .deb file.
  - **dpkg -I file.deb** (or –info) - displays the headers of the specified .deb file.
  - **dpkg -s package** (or –status) - displays the headers of an installed package.
  - **dpkg -r package** - removes a package.
  - **dpkg -P package** - purges a package and all associated user data.
  - **dpkg --print-architecture** - prints host's architecture.
  - **dpkg --print-foreign-architectures** - prints foreign architecture.

— `dpkg --add-architecture arch` - Adds foreign architecture to the list of architectures for which packages can be installed.
— `dpkg --remove-architecture arch` - Drops support of a foreign architecture.

- The dpkg installation actually performs two steps automatically : it unpacks the package and runs the configuration scripts. These two steps can be performed independently (as apt does behind the scenes) with the –unpack and –configure options.

```
# dpkg --unpack man-db_2.9.3-2_amd64.deb
(Reading database ... 309317 files and directories currently installed.)
Preparing to unpack man-db_2.9.3-2_amd64.deb ...
Unpacking man-db (2.9.3-2) over (2.9.3-2) ...
Processing triggers for kali-menu (2020.4.0) ...
Processing triggers for mime-support (3.64) ...
# dpkg --configure man-db
Setting up man-db (2.9.3-2) ...
Updating database of manual pages ...
```

- /var/cache/apt/archives/ contains a cached copy of already downloaded packages to avoid downloading them again if you need to reinstall them.
- To avoid excessive disk usage, you should regularly sort through /var/cache/apt/archives/. Two commands can be used for this : `apt clean` (or `apt-get clean`) entirely empties the directory ; `apt autoclean` (or `apt-get autoclean`) only removes packages that can no longer be downloaded.
- You can specify the package version with apt install package=version or indicate its distribution of origin (kali-rolling or kali-dev) with apt install package/distribution

```
# apt install zsh=5.7.1-1
# apt install zsh/kali-dev
```

- As with dpkg, you can also instruct apt to forcibly install a package and overwrite files.
`# apt -o Dpkg::Options::="--force-overwrite" install zsh`
- aptitude is an interactive program that can be used in semi-graphical mode on the console. It can help you to install and troubleshoot packages.
- synaptic is a graphical package manager that features a clean and efficient graphical interface.
- Kali can receive upgrades several times a day. You should upgrade :
— When you are aware of a security issue that is fixed in an update.
— When you suspect that an updated version might fix a bug that you are experiencing.
— Before reporting a bug to make sure it is still present in the latest version that you have available.
— To get the security fixes that you have not heard about.
- Two different ways in APT to install package1 and to remove package2 through the addition of suffixes to package names.

```
# apt install package1 package2-
# apt remove package1+ package2
```

- The apt-cache command can display much of the information stored in APT's internal database :
`apt-cache search keyword` Performs keyword-based package searches. `apt-cache show package` Provides the package's description, its dependencies, and the name of its maintainer. `apt-cache policy` Displays the priorities of package sources. `apt-cache dumpavail` Displays the headers of all available versions of all packages. `apt-cache pkgnames` Displays the list of all packages that appear at least once in the cache. - `axi-cache search term` provides better search results. It uses the Xapian search engine and is part of the apt-xapian-index package, which indexes all package information.

```
$ axi-cache search forensics graphical
7 results found.
Results 1-7:
100% autopsy - graphical interface to SleuthKit
94% forensics-all-gui - Debian Forensics Environment - GUI components (metapackage)
87% forensics-extra-gui - Forensics Environment - extra GUI components (metapackage)
86% forensics-colorize - show differences between files using color graphics
44% gpart - Guess PC disk partition table, find lost partitions
39% testdisk - Partition scanner and disk recovery tool, and PhotoRec file recovery tool
8% texlive-publishers - TeX Live: Publisher styles, theses, etc.
More terms: tools experts autopsy picture ethical pentesters hackers
More tags: admin::forensics security::forensics admin::recovery interface::commandline admin::boot scope::utility
```

- The dpkg tool keeps a log of all of its actions in /var/log/dpkg.log

```
# tail /var/log/dpkg.log
2021-01-06 23:16:37 status installed kali-tools-gpu:amd64 2021.1.0
2021-01-06 23:16:37 remove kali-tools-gpu:amd64 2021.1.0
2021-01-06 23:16:37 status half-configured kali-tools-gpu:amd64 2021.1.0
2021-01-06 23:16:37 status half-installed kali-tools-gpu:amd64 2021.1.0
```

- All of the files in /etc/apt/apt.conf.d/ are instructions for the configuration of APT. APT processes the files in alphabetical order, so that the later files can modify configuration elements defined in the earlier files.
- Managing package priorities :
  — Each installed package version has a priority of 100. A non-installed version has a priority of 500 by default but it can jump to 990 if it is part of the target release.
  — You can modify the priorities by adding entries in the /etc/apt/preferences file.
  — If two packages have the same priority, APT installs the newest one (whose version number is the highest).
  — If two packages of same version have the same priority but differ in their content, APT installs the version that is not installed.
  — A package whose priority is less than 0 will never be installed.
  — A package with a priority ranging between 0 and 100 will only be installed if no other version of the package is already installed.
  — With a priority between 100 and 500, the package will only be installed if there is no other newer version installed or available in another distribution.
  — A package of priority between 501 and 990 will only be installed if there is no newer version installed or available in the target distribution.
  — With a priority between 990 and 1000, the package will be installed except if the installed version is newer.
  — A priority greater than 1000 will always lead to the installation of the package even if it forces APT to downgrade to an older version.
  — If Debian experimental is listed in sources.list, the corresponding packages will almost never be installed because their default APT priority is 1.
- There is no official syntax for comments in /etc/apt/preferences, but some textual descriptions can be provided by prepending one or more Explanation fields into each entry :
  — Explanation : The package xserver-xorg-video-intel provided
  — Explanation : in experimental can be used safely
  — Package : xserver-xorg-video-intel
  — Pin : release a=experimental
  — Pin-Priority : 500
- The command apt autoremove can be used to remove unnecessary packages that were installed as dependencies but are no longer required.
- All Debian packages have an Architecture field in their control information. This field can contain either ”all” (for packages that are architecture-independent) or the name of the architecture that it targets (like amd64, or armhf). By default, dpkg will only install the package if its architecture matches the host's architecture.
- Packages containing the Multi-Arch : same header field tells the packaging system that the various architectures of the package can be safely co-installed.

```
$ dpkg -s libwine:amd64 libwine:i386 | grep  ^Multi
Multi-Arch: same
Multi-Arch: same
```

- The trusted keys are managed with the apt-key command found in the apt package. This program maintains a keyring of GnuPG public keys, which are used to verify the authenticity of packages and their sources. These keys are automatically kept up-to-date by the kali-archive-keyring package (which puts the corresponding keyrings in /etc/apt/trusted.gpg.d).
- Display the fingerprints of all GPG keys stored in the system's APT keyring : apt-key fingerprint

```
# apt-key fingerprint
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
/etc/apt/trusted.gpg.d/debian-archive-buster-automatic.gpg
-----------------------------------------------------------
pub   rsa4096 2019-04-14 [SC] [expires: 2027-04-12]
      80D1 5823 B7FD 1561 F9F7  BCDD DC30 D7C2 3CBB ABEE
uid           [ unknown] Debian Archive Automatic Signing Key (10/buster)
sub   rsa4096 2019-04-14 [S] [expires: 2027-04-12]

/etc/apt/trusted.gpg.d/debian-archive-buster-security-automatic.gpg
-------------------------------------------------------------------
pub   rsa4096 2019-04-14 [SC] [expires: 2027-04-12]
      5E61 B217 265D A980 7A23  C5FF 4DFA B270 CAA9 6DFA
uid           [ unknown] Debian Security Archive Automatic Signing Key (10/buster)
sub   rsa4096 2019-04-14 [S] [expires: 2027-04-12]
```

- The .deb file is simply an ar archive containing three files :
  — debian-binary - contains a single version number describing the format of the archive.
  — control.tar.gz - contains meta-information.
  — data.tar.xz - contains the actual files to be installed on the system.

```
$ ar t /var/cache/apt/archives/apt_1.4~beta1_amd64.deb
debian-binary
control.tar.gz
data.tar.xz
```

- The control.tar.gz archive contains meta-information :

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb control.tar.gz | tar -tzf -
./
./conffiles
./control
./md5sums
./postinst
./postrm
./preinst
./prerm
./shlibs
./triggers
```

- The md5sums file in control.tar.gz contains the MD5 checksums for all of the package's files.
- The conffiles file in control.tar.gz lists package files that must be handled as configuration files. Configuration files can be modified by the administrator, and dpkg will try to preserve those changes during a package update.
- The control file from control.tar.gz contains the most vital information about the package. It uses a structure similar to email headers and can be viewed with the dpkg -I command.

```
$ dpkg -I apt_1.4~beta1_amd64.deb control
Package: apt
Version: 1.4~beta1
Architecture: amd64
Maintainer: APT Development Team
Installed-Size: 3478
Depends: adduser, gpgv | gpgv2 | gpgv1, debian-archive-keyring, init-system-helpers (>= 1.18~),
libapt-pkg5.0 (>= 1.3~rc2), libc6 (>= 2.15), libgcc1 (>= 1:3.0), libstdc++6 (>= 5.2)
Recommends: gnupg | gnupg2 | gnupg1
Suggests: apt-doc, aptitude | synaptic | wajig, dpkg-dev (>= 1.17.2), powermgmt-base, python-apt
Breaks: apt-utils (<< 1.3~exp2~)
Replaces: apt-utils (<< 1.3~exp2~)
[...]
```

- The control.tar.gz archive for each Debian package may contain a number of scripts called by dpkg at different stages in the processing of a package :
  - preinst - executed prior to installation of the package.
  - postinst - executed after the installation of the package.
  - prerm - executed before removal of a package.
  - postrm - executed after removal of a package.
- An example to view the preinst script of a package :

```
$ dpkg -I zsh_5.3-1_amd64.deb preinst
#!/bin/sh
set -e
# Automatically added by dh_installdeb
dpkg-maintscript-helper symlink_to_dir /usr/share/doc/zsh zsh-common 5.0.7-3 -- "$@"
# End automatically added section
```

- Here is what happens during a package removal :
  - `dpkg` calls prerm remove.
  - `dpkg` removes all of the package's files, with the exception of the configuration files and configuration scripts.
  - `dpkg` executes postrm remove. All of the configuration scripts, except postrm, are removed. If you have not used the purge option, the process stops here. For a complete purge of the package (with `dpkg --purge`), the configuration files and temporary files are also deleted ; `dpkg` then executes postrm purge.
- /var/lib/dpkg/ contains a running record of all the packages that have been installed on the system. All of the configuration scripts for installed packages are stored in the /var/lib/dpkg/info/ directory.

```
$ ls /var/lib/dpkg/info/zsh.*
/var/lib/dpkg/info/zsh.list
/var/lib/dpkg/info/zsh.md5sums
/var/lib/dpkg/info/zsh.postinst
/var/lib/dpkg/info/zsh.postrm
/var/lib/dpkg/info/zsh.preinst
/var/lib/dpkg/info/zsh.prerm
```

- The /var/lib/dpkg/status file contains a series of data blocks describing the status of each package. The information from the control file of the installed packages is also replicated there.

```
$ more /var/lib/dpkg/status
Package: gnome-characters
Status: install ok installed
Priority: optional
Section: gnome
Installed-Size: 1785
Maintainer: Debian GNOME Maintainers
Architecture: amd64
Version: 3.20.1-1
[...]
```

Chapter 10 - Advanced Usage

- To start rebuilding a Kali package, first download the source package, which is composed of a *.dsc (Debian Source Control) file and of additional files referenced from that control file.
- Source packages are stored on HTTP-accessible mirrors. The most efficient way to obtain them is with **apt source** *package*, which requires that you add a deb-src line to the /etc/apt/sources.list file.
- If you need a specific version of the source package, which is currently not available in the repositories listed in /etc/apt/sources.list, then the easiest way to download it is to find out the URL of its .dsc file by looking it up on https ://pkg.kali.org and then handing that URL over to dget (from the devscripts package).

```
$ dget http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.
ffde4d-1.dsc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   362  100   362    0     0   1117      0 --:--:-- --:--:-- --:--:-- 1120
100  1935  100  1935    0     0   3252      0 --:--:-- --:--:-- --:--:-- 3252
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548
.ffde4d.orig.tar.gz
[...]
```

- To extract source package manually : **dpkg-source -x** *dsc-file*

```
$ dpkg-source -x libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
gpgv: Signature made Wed 12 Aug 2015 12:14:03 AM EDT
gpgv:                using RSA key 43EF73F4BD8096DA
gpgv: Can't check signature: No public key
dpkg-source: warning: failed to verify signature on ./libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
dpkg-source: info: extracting libfreefare in libfreefare-0.4.0+0~git1439352548.ffde4d
dpkg-source: info: unpacking libfreefare_0.4.0+0~git1439352548.ffde4d.orig.tar.gz
dpkg-source: info: unpacking libfreefare_0.4.0+0~git1439352548.ffde4d-1.debian.tar.xz
```

- For Kali specific packages whose sources are hosted on gitlab.com/kalilinux/packages, you can retrieve the sources with git clone https ://gitlab.com/kalilinux/packages/source-package.git

```
$ git clone https://gitlab.com/kalilinux/packages/kali-meta.git
Cloning into 'kali-meta'...
remote: Counting objects: 760, done.
remote: Compressing objects: 100% (614/614), done.
remote: Total 760 (delta 279), reused 0 (delta 0)
Receiving objects: 100% (760/760), 141.01 KiB | 0 bytes/s, done.
Resolving deltas: 100% (279/279), done.
Checking connectivity... done.
```

- After downloading sources, install the packages listed in the source package's build dependencies with **sudo apt build-dep ./** (assuming that you are in a directory containing an unpacked source package).

```
$ sudo apt build-dep ./
Note, using directory './' to get the build dependencies
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  autoconf automake autopoint autotools-dev debhelper dh-autoreconf
  dh-strip-nondeterminism gettext intltool-debian libarchive-zip-perl
  libfile-stripnondeterminism-perl libtool po-debconf
0 upgraded, 13 newly installed, 0 to remove and 0 not upgraded.
Need to get 4 456 kB of archives.
After this operation, 14,6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
[...]
```

- Steps to update a source package :
The required first step is changing the version number to distinguish your package from the original with **dch**

`--local` version-identifier
Applying a patch with patch -p1 < patch-file or modifying quilt's patch series.
Tweaking build options, usually found in the package's debian/rules file.
- After modifying a source package, you can build the binary package with **`dpkg-buildpackage -us -uc -b`** from the source directory, which will generate an unsigned binary package.
`-us -uc` disables signatures on some of the generated files (.dsc, .changes). `-b` asks for a binary-only build.
- debuild is a wrapper of dpkg-buildpackage which runs many checks to validate the generated package against the Debian policy.
- The Debian kernel team maintains the Debian Kernel Handbook (also available in the debian-kernel-handbook package) with comprehensive documentation about most kernel-related tasks and about how official Debian kernel packages are handled.
- Packages needed for kernel modifications : build-essential, libncurses5-dev, fakeroot
`# apt install build-essential libncurses5-dev fakeroot` - List the latest kernel version packaged by Kali : **`apt-cache search^linux-source`**
- Install a compressed archive of the kernel source into /usr/src : **`apt install`** *`linux-source-version-number`*
- The kernel source files should be extracted with **`tar -xaf`** into a directory other than /usr/src (such as /kernel).

```
$ mkdir ~/kernel; cd ~/kernel
$ tar -xaf /usr/src/linux-source-4.9.tar.xz
```

- The preferred method to populate a kernel configuration file is to borrow Kali's standard configuration by copying /boot/config-version-string to /kernel/linux-source-version-number/.config
`$ cp /boot/config-4.9.0-kali1-amd64 /kernel/linux-source-4.9/.config`
- Once the kernel configuration is ready, the command make deb-pkg will generate up to five Debian packages in standard .deb format :
  — linux-image-version contains the kernel image and the associated modules.
  — linux-headers-version contains the header files required to build external modules.
  — linux-firmware-image-version contains the firmware files needed by some drivers.
  — linux-image-version-dbg contains the debugging symbols for the kernel image and its modules.
  — linux-libc-dev contains headers relevant to some user-space libraries like glibc.
- To actually use the built kernel, install the required packages with **`dpkg -i`** *`file.deb`*. The linux-image package is required ; you only have to install the linux-headers package if you have some external kernel modules to build.
- Official Kali ISO images are built with live-build, which is a set of scripts that allows the complete automation and customization of all facets of ISO image creation.
- The build.sh live-build wrapper creates the config directory by combining files from kali-config/common and kali-config/variant-X, where X is the name of a variant given with the –variant parameter. e.g. Create a Kali live image using KDE as desktop environment :
`# ./build.sh --variant kde --verbose`
- There are several ways to customize your ISO by modifying live-build's configuration directory :
  — Packages can be added to (or removed from) a live ISO by modifying package-lists/*.list.chroot files.
  — Custom packages can be included in the live image by placing the .deb files in a packages.chroot directory.
  — You can add files to the live filesystem by putting them at their expected location below the includes.chroot config directory.
  — You can add files to the ISO image by putting them at their expected location below the includes.binary config directory. For example, we can provide kali-config/common/includes.binary/isolinux/splash.png to override the background image used by the Isolinux bootloader.
  — You can execute scripts during the live system's chroot setup process by installing them as hooks/live/*.chroot files.
  — Binary hooks hooks/live/*.binary are executed in the context of the build process.
  — You can provide Debconf preseed files as preseed/*.cfg files.
- The kali-meta source package builds all the metapackages provided by Kali Linux :
  — `kali-linux-core` - Base system (pulled by all the other metapackages).
  — `kali-linux-headless` - Default Kali Linux installation command line tools.
  — `kali-linux-default` - Default Kali Linux installation, both command line and graphical.
  — `kali-linux-large` - Wider range set of tools, which are not as commonly used.
  — `kali-linux-everything` - Metapackage of all the metapackages and other packages.
  — `kali-tools-top10` - Ten most popular tools.
  — `kali-tools-web` - Web applications assessment tools.
  — `kali-tools-passwords` - Password cracking tools.
  — `kali-tools-wireless` - Collection of 802.11, Bluetooth, RFID and SDR tools.
  — `kali-tools-forensics` - Forensic tools.
  — `kali-tools-802-11` - Wireless assessment and analysis tools.

— `kali-tools-bluetooth` - Bluetooth focused tools.
— `kali-tools-crypto-stego` - Cryptography and steganography tools.
— `kali-tools-crypto-fuzzing` - Fuzzing attack tools.
— `kali-tools-gpu` - GPU-powered tools.
— `kali-tools-hardware` - Tools designed to attacking hardware.
— `kali-tools-rfid` - Radio Frequency Identification (RFID) tools.
— `kali-tools-sdr` - Software Defined Radio (SDR) tools.
— `kali-tools-voip` - Voice Over IP tools.
— `kali-tools-windows-resources` - Pre-compiled Microsoft Windows binaries.

- Setting up encrypted persistence on a USB Key :

```
# cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb4
[...]
# cryptsetup luksOpen /dev/sdb4 kali_persistence
[...]
# mkfs.ext4 -L work /dev/mapper/kali_persistence
[...]
# cryptsetup luksClose /dev/mapper/kali_persistence
```

- Nuke password (LUKS Nuke) is used to destroy all keys used to manage the encrypted partition. Kali provides this feature in the **`cryptsetup-nuke-password package`**.
`# dpkg-reconfigure cryptsetup-nuke-password`

Chapter 11 - Kali Linux in the Enterprise

- Boot machine from the network with PXE (Preboot eXecution Environment), with at least a TFTP file server, a DHCP/BOOTP server (and a web server for debconf preseeding). dnsmasq handles both DHCP and TFTP, and the apache2 web server comes pre-installed in Kali.
- The Debian installation manual covers the setup of isc-dhcp-server and tftpd-hpa for PXE booting.
- In order to set up dnsmasq, you must first configure it through /etc/dnsmasq.conf. Once configured, you will need to place the installation boot files in the /tftpboot/ directory.
- SaltStack is a centralized configuration management service : a Salt master manages many Salt minions. Install the salt-master package on a reachable server and salt-minion on managed hosts.
- Each minion must be told where to find their master. Edit the /etc/salt/minion YAML config file and set the master key to the DNS name or IP address of the Salt master.

```
minion# vim /etc/salt/minion
minion# grep ^master /etc/salt/minion
master: 192.168.122.105
```

- Set minion's unique identifier in /etc/salt/minion_id (defaults is the system hostname) :

```
minion# echo kali-scratch >/etc/salt/minion_id
minion# systemctl enable salt-minion
minion# systemctl start salt-minion
```

- Accept salt minion's identification key on the master side : **`salt-key --accept minion`**

```
master# salt-key --accept kali-scratch
The following keys are going to be accepted:
Unaccepted Keys:
kali-scratch
Proceed? [n/Y] y
Key for minion kali-scratch accepted.
```

- Executing commands on minions :
— **`salt '*' test.ping`** - asks all minions to execute the ping function from the test execution module (simple way to ensure the connection is working between master and minions).
— **`salt minion cmd.shell command`** - executes shell command on a minion.
— **`salt minion sys.doc`** - obtains a description of all the execution modules and their available functions.
— **`salt '*' pkg.refresh_db`** - perform apt-get update on all minions.
— **`salt '*' pkg.upgrade`** - perform apt-get upgrade on all minions.
— **`salt '*' pkg.upgrade dist_upgrade=True`** - perform apt-get dist-upgrade on all minions.
— **`salt "*" pkg.list_upgrades`** - list the pending upgrade operations on all minions.
— **`salt '*' pkg.install package`** - install a package on all minions.
— **`salt '*' service.enable ssh`** - enable SSH service to start at boot on all minions.
— **`salt '*' service.start ssh`** - start SSH service on all minions.

- Use salt state files (re-usable configuration templates) to schedule actions, collect data, orchestrate sequences of operations on multiple minions. The operations described in state files can then be performed with the

state.apply salt command.
- By default, state files are stored in /srv/salt on the master ; they are YAML files with a .sls extension.
- The salt state file /srv/salt/offsec.sls can be applied to a given minion with the command : **salt minion state.apply state**
server# salt kali-scratch state.apply offsec
- The state file can also be permanently associated to the minion by recording it in the /srv/salt/top.sls file, which is used by the state.highstate command to apply all relevant states in a single pass. **server# salt kali-scratch state.highstate** - In the process of creating custom configuration package, the command **dh_make --native** (from the dh-make package) is used to add Debian packaging instructions, which will be stored in a debian sub-directory.

```
$ mkdir offsec-defaults-1.0; cd offsec-defaults-1.0
$ dh_make --native
Type of package: (single, indep, library, python)
[s/i/l/p]? i
Email-Address       : buxy`
License             : gpl3
Package Name        : offsec-defaults
Maintainer Name     :¨Raphael Hertzog
Version             : 1.0
Package Type        : indep
Date                : Thu, 16 Jun 2020 18:04:21 +0200
Are the details correct? [Y/n/q] y
Currently there is not top level Makefile. This may require additional tuning
Done. Please edit the files in the debian/ subdirectory now.
```

- The **dh_make** command creates a debian subdirectory containing many files. Some are required, in particular rules, control, changelog, and copyright. The compat file should be kept, since it is required for the correct functioning of the debhelper suite of programs.
- Most of the programs involved in package maintenance will look for your name and email address in the DEBFULLNAME and DEBEMAIL or EMAIL environment variables.

```
export EMAIL="buxy@kali.org"
export DEBFULLNAME="Raphael Hertzog"
```

- A Makefile is a script file used by the make program ; it describes rules for how to build a set of files from each other in a tree of dependencies.
- To create a custom APT repository, you need to install `reprepro` and `gnupg2`
`kali@kali: $ sudo apt install reprepro gnupg2` - The tool reprepro will be used to create the desired APT repository. A dedicated directory is necessary for reprepro and inside that directory you have to create a conf/distributions file documenting which distributions are available in the package repository.
- Fields in conf/distributions file : Codename, Architectures, Components, Origin, Description, SignWith, AlsoAcceptFor

```
Codename: offsec-internal
AlsoAcceptFor: unstable
Origin: OffSec
Description: Offsec's Internal packages
Architectures: source amd64 i386
Components: main
SignWith: F8FE22F74F1B714E38DA6181B27F74F7B4EF2D0D
```

- Once the fields in conf/distributions file are defined, generate an empty repository using the command reprepro export

```
pkgrepo@kali:~/reprepro$ reprepro export
Exporting indices.
```

- reprepro creates the repository meta-information in dists sub-directory and an internal database in db sub-directory.

```
./db
./db/version
./db/references.db
./db/contents.cache.db
./db/checksums.db
./db/packages.db
./db/release.caches.db
./conf
./conf/distributions
./dists
./dists/offsec-internal
./dists/offsec-internal/Release.gpg
```

```
./dists/offsec-internal/Release
./dists/offsec-internal/main
[...]
```

- Include package using reprepro : reprepro include offsec-internal /tmp/offsec-defaults_1.0_amd64.changes. It will add the files into its own package pool in a pool sub-directory.

```
pkgrepo@kali:~/reprepro$ reprepro include offsec-internal /tmp/offsec-defaults_1.0_amd64.changes
Exporting indices...
pkgrepo@kali:~/reprepro$ find pool
pool
pool/main
pool/main/o
pool/main/o/offsec-defaults
pool/main/o/offsec-defaults/offsec-defaults_1.0.dsc
pool/main/o/offsec-defaults/offsec-defaults_1.0.tar.xz
pool/main/o/offsec-defaults/offsec-defaults_1.0_all.deb
```

- The dists and pool directories are the two directories that you need to make publicly available over HTTP to finish the setup of your APT repository. They contain all the files that APT will want to download.

Chapter 12 - Introduction to Security Assessments

- CIA triad examples :
  - Confidentiality - A SQL injection vulnerability that allows an attacker to extract the full contents of the web application.
  - Integrity - A SQL injection vulnerability that allows an attacker to change the existing information in the database.
  - Availability - A SQL injection vulnerability that initiates a long-running query, consuming a large amount of resources on the server.
- A vulnerability is a flaw that, when exploited, will compromise the confidentiality, integrity, or availability of an information system. An exploit is a software that has been specially crafted to take advantage of a vulnerability.
- Types of vulnerabilities :
  - File Inclusion : Vulnerability which allows you to include the contents of a local or remote file into the web application.
  - SQL Injection : Vulnerability that bypasses input validation routines to inject SQL commands into the targeted application.
  - Buffer Overflow : Vulnerability that bypasses input validation routines to write data into a buffer's adjacent memory which can lead to code execution.
  - Race Conditions : Vulnerability that takes advantage of timing dependencies in a program.
- Anti-exploit technologies in modern computing platforms include Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).
- Types of assessments :
  - Vulnerability Assessment : Objective is to create a simple inventory of discovered vulnerabilities within the target environment.
  - Compliance Test : Based on government and industry requirements (such as PCI DSS, DISA STIG, and FISMA), which are in turn based on a compliance framework.
  - Traditional Penetration Test : A thorough security assessment that is designed to improve the overall security posture of an organization based on certain real-world threats.
  - Application Assessment : A specialty that is narrowly focused on a single application. Applications that may be assessed in this manner include web applications, desktop applications and mobile applications.
- Key phases during penetration test : Information Gathering, Vulnerability Discovery, Exploitation, Pivoting, Exfiltration, Reporting.
- Burp Suite is a vulnerability scanner for web application.
- Black Box Assessment : The assessor interacts with the application with no special knowledge or access beyond that of a standard user.
- White Box Assessment : The assessor will often have full access to the source code, administrative access to the application, and so on.
- When dealing with signature matches, you can have a few different potential results :
  - True Positive : The signature is matched and it captures a true vulnerability.
  - False Positive : The signature is matched but the detected issue is not a true vulnerability.
  - True Negative : The signature is not matched and there is no vulnerability.
  - False Negative : The signature is not matched but there is an existing vulnerability.
- NIST SP 800-30 defines the true risk of a discovered vulnerability as a combination of the likelihood of occurrence and the potential impact.

likelihood of occurrence : Based on the probability that a particular threat is capable of exploiting a particular vulnerability.
impact : Determined by evaluating the amount of harm that could occur if the vulnerability in question were exploited.
- Once the likelihood of occurrence and impact have been determined, you can then determine the overall risk rating, which is defined as a function of the two ratings.
- Types of Attacks :
  — Denial of Service : Breaks the behavior of an application and makes it inaccessible.
  — Memory Corruption : Manipulation of process memory, often leads to code execution.
  — Stack Buffer Overflow : When a program writes more data to a buffer on the stack than there is space available for it.
  — Heap Corruption : By manipulating the data to overwrite through the linked list of heap memory pointers.
  — Integer Overflow : When an application tries to create a numeric value that can't be contained within its allocated storage space.
  — Format String : When a program accepts user input and formats it without checking it.
  — Web Vulnerabilities : Attack web services using techniques like SQL injection and XSS attacks.
  — Password Attacks : Leverage password lists to attack service credentials.
  — Client-Side Attacks : Tricks user to visit malicious web page which triggers vulnerabilities in client-side applications (Flash, Acrobat Reader, Java, HTA).

Chapter 13 - Conclusion : The Road Ahead

- This chapter is not relevant to the exam.