This site is dedicated to sharing information about the practice, ideas, concepts and patterns regarding computer security.

How to securely isolate and execute chkrootkit and rkhunter from Kali Linux

Version 0.1, Last Updated: Oct 16

Table of Contents

Chapter 1. Introduction

The motivation behind this paper is to explore using the tools `chkrootkit` and `rkhunter` that comes with Kali Linux.

1.1. chkrootkit

`chkrootkit` is a tool used locally to check for signs of a rootkit.

1.2. rkhunter

`rkhunter` is a security monitoring and analyzing tool used locally to check for signs of a rootkit. This tool scans systems for known and unknown rootkits, backdoors, sniffers and exploits.

`rkhunter` checks for:

- SHA256 hash changes
- files commonly created by rootkits
- executables with anomalous file permissions
- suspicious strings in kernel modules
- hidden files in system directories
- can optionally scan within files

Using rkhunter alone does not guarantee that a system is not compromised.

Running additional tools, such as `chkrootkit`, is highly recommended.

1.3. rootkits

In Layman terms, what is a rootkit?

As defined on Wikipedia, they are: "A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a compound of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it after having obtained root or administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment."

Let’s jump into rootkit detection with our lab.

Chapter 2. Requirements

2.1. Writing Conventions

If you see the following $ symbol on a command line to execute, what that means is that the command is executed as a regular user; meaning an account that does not have administrative privileges. Ignore the leading $ and execute the rest of the command.

```
$ command to execute as a regular user
```

If you see a command line lead with the # symbol, then that means that the command is executed as the root user. This implies you need to elevate to the root user before running the command, e.g. with: `sudo su  root`.

```
# command to execute as the root user
```

2.2. VirtualBox

Go to: https://www.virtualbox.org/wiki/Downloads and download VirtualBox.

The author is running on Ubuntu 18.04, so following to this URL: https://www.virtualbox.org/wiki/Linux_Downloads

For Ubuntu, double click on the .deb file, i.e. virtualbox-5.2_5.2.0-118431-Ubuntu-zesty_amd64.deb, and install VirtualBox on your local workstation.

2.2.1. Clean VirtualBox Networking

This section is here in case you already had virtualbox installed from before. The intent is to clean up the previous networking. If you do not need to do this, skip to Add VirtualBox Networking

Run these two commands from a Terminal:

```
$ VBoxManage list natnetworks
$ VBoxManage list dhcpservers
```

Output (example):

```
NetworkName:    192.168.139-NAT
IP:             192.168.139.1
Network:        192.168.139.0/24
IPv6 Enabled:   No
IPv6 Prefix:    fd17:625c:f037:2::/64
DHCP Enabled:   Yes
```

```
Enabled:        Yes
loopback mappings (ipv4)
        127.0.0.1=2


NetworkName:    192.168.139-NAT
Dhcpd IP:       192.168.139.3
LowerIPAddress: 192.168.139.101
UpperIPAddress: 192.168.139.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None

NetworkName:    HostInterfaceNetworking-vboxnet0
Dhcpd IP:       172.20.0.3
LowerIPAddress: 172.20.0.101
UpperIPAddress: 172.20.0.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None
```

Now, delete ALL of the pre-installed VirtualBox networks (one at a time following the syntax below):

```
VBoxManage natnetwork remove --netname <NetworkName_from_above>
VBoxManage natnetwork remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

Now, delete ALL of the pre-installed DHCP services:

```
VBoxManage dhcpserver remove --netname <DHCP_Server_NetworkName_from_above>
```

```
VBoxManage dhcpserver remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

2.2.2. Add VirtualBox Networking

Now, add the new VirtualBox networks so the Kali Linux guides work.

```
VBoxManage natnetwork add \
    --netname 192.168.139-NAT \
    --network "192.168.139.0/24" \
    --enable --dhcp on

VBoxManage dhcpserver add \
    --netname 192.168.139-NAT \
    --ip 192.168.139.3 \
    --lowerip 192.168.139.101 \
    --upperip 192.168.139.254 \
    --netmask 255.255.255.0 \
    --enable

VBoxManage hostonlyif create

VBoxManage hostonlyif ipconfig vboxnet0 \
    --ip 172.20.0.1 \
    --netmask 255.255.255.0

VBoxManage dhcpserver add \
    --ifname vboxnet0 \
    --ip 172.20.0.3 \
    --lowerip 172.20.0.101 \
    --upperip 172.20.0.254 \
    --netmask 255.255.255.0

VBoxManage dhcpserver modify \
    --ifname vboxnet0 \
    --enable
```

VirtualBox install complete.

2.3. Vagrant

Go to: https://www.vagrantup.com/downloads.html, follow the appropriate link to your OS and 32 or 64 bit version representing your local workstation. Download.

For Ubuntu, double click on the .deb file, i.e. vagrant_2.0.1_x86_64.deb, and install Vagrant on your local system.

NOTE Update vagrant vm: `vagrant box update`

2.4. Kali Linux and Damn Vulnerable Web Application (DVWA)

The author highly recommends to create a directory structure that is easy to navigate and find your code. As an example, you could use something similar to:

```
${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Go ahead and make this structure with the following command (inside a Terminal):

```
$ mkdir p ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

2.4.1. Vagrantfile

Inside of the kali-linux-vm directory, populate a new file with the exact name, “Vagrantfile”. Case matters, uppercase the “V”. This file will contain both virtual machines for Kali Linux as well as setting up the DVWA virtual machine. Aggregating both virtual machines into one file has saved the author a lot of time. The coolness here is setting up the variables at the top of the Vagrantfile mimicing shell scripting inside of a virtual machine (passed in with provision: shell). I tested using: `apt-get update && apt-get upgrade -y`, but opted to take it out since it took over 45 minutes on my slower (old) hardware. See comment about downloading this file immediately preceding the code block.

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

$os_update = <<SCRIPT
apt-get update
SCRIPT

VAGRANTFILE_API_VERSION = "2"


Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
    config.vm.define "kali-linux-vagrant" do |conf|
        conf.vm.box = "kalilinux/rolling"

        # For Linux systems with the Wireless network, uncomment the line:
```

```
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux
Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)",
auto_config: true

        conf.vm.hostname = "kali-linux-vagrant"
        conf.vm.provider "virtualbox" do |vb|
            vb.gui = true
            vb.memory = "4096"
            vb.cpus = "2"
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Debian_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
    end

    config.vm.define "dvwa-vagrant" do |conf|

        conf.vm.box = "ubuntu/xenial64"

        conf.vm.hostname = "dvwa-vagrant"

        # For Linux systems with the Wireless network, uncomment the line:
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux
Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)",
auto_config: true

        config.vm.network "forwarded_port", guest: 80, host: 8080, auto_correct: true
        config.vm.network "forwarded_port", guest: 3306, host: 3306, auto_correct:
true

        conf.vm.provider "virtualbox" do |vb|
            vb.memory = "1024"
            vb.cpus = "2"
            vb.gui = false
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Ubuntu_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
```

```
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
        conf.vm.provision :shell, path: "bootstrap.sh"
    end
end
```

Save and write this file.

You can also download from:

```
$ curl -o Vagrantfile  http://securityhardening.com/files/Vagrantfile_20200928.txt
```

2.4.2. bootstrap.sh

Inside of the kali-linux-vm directory, populate a new file with the exact name, `bootstrap.sh`. Case matters, all lowercase. See comment about downloading this file immediately preceding the code block. `bootstrap.sh` (include the shebang in your file: the first line with `#!/usr/bin/env bash`):

```
#!/usr/bin/env bash
PHP_FPM_PATH_INI='/etc/php/7.0/fpm/php.ini'
PHP_FPM_POOL_CONF='/etc/php/7.0/fpm/pool.d/www.conf'
MYSQL_ROOT_PW='Assword12345'
MYSQL_dvwa_user='dvwa'
MYSQL_dvwa_password='sunshine'
DVWA_admin_password='admin'
recaptcha_public_key='u8392ihj32kl8hujalkshuil32'
recaptcha_private_key='89ry8932873832lih32ilj32'


install_base() {
    add-apt-repository -y ppa:nginx/stable
    sudo apt-get update
    sudo apt-get dist-upgrade -y
    sudo apt-get install -y \
        nginx \
        mariadb-server \
        mariadb-client \
        php \
        php-common \
        php-cgi \
        php-fpm \
        php-gd \
        php-cli \
```

```
        php-pear \
        php-mcrypt \
        php-mysql \
        php-gd \
        git \
        vim
}

config_mysql(){
    mysqladmin -u root password "${MYSQL_ROOT_PW}"
## Config the mysql config file for root so it doesn't prompt for password.
## Also sets pw in plain text for easy access.
## Don't forget to change the password here!!

cat <<EOF > /root/.my.cnf
[client]
user="root"
password="${MYSQL_ROOT_PW}"
EOF
    mysql -BNe "drop database if exists dvwa;"
    mysql -BNe "CREATE DATABASE dvwa;"
    mysql -BNe "GRANT ALL ON *.* TO '"${MYSQL_dvwa_user}"'@'localhost' IDENTIFIED BY
'"${MYSQL_dvwa_password}"';"

    systemctl enable mysql
    systemctl restart mysql
    sleep 2
}


config_php(){
    ## Config PHP FPM INI to disable some security settings:

    sed -i 's/^;cgi.fix_pathinfo.*$/cgi.fix_pathinfo = 0/g' ${PHP_FPM_PATH_INI}
    sed -i 's/allow_url_include = Off/allow_url_include = On/g' ${PHP_FPM_PATH_INI}
    sed -i 's/allow_url_fopen = Off/allow_url_fopen = On/g' ${PHP_FPM_PATH_INI}
    sed -i 's/safe_mode = On/safe_mode = Off/g' ${PHP_FPM_PATH_INI}
    echo "magic_quotes_gpc = Off" >> ${PHP_FPM_PATH_INI}
    sed -i 's/display_errors = Off/display_errors = On/g' ${PHP_FPM_PATH_INI}

    ## explicitly set pool options
    ## (these are defaults in ubuntu 16.04 so i'm commenting them out.
    ## If they are not defaults for you try uncommenting these)
    #sed -i 's/^;security.limit_extensions.*$/security.limit_extensions = \
    #.php .php3 .php4 .php5 .php7/g' /etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.owner.*$/listen.owner = www-data/g'
/etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.group.*$/listen.group = www-data/g'
/etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^;listen.mode.*$/listen.mode = 0660/g' /etc/php/7.0/fpm/pool.d/www.conf
```

```
    systemctl restart php7.0-fpm
}


config_nginx(){

cat << 'EOF' > /etc/nginx/sites-enabled/default
server
{
    listen  80;
    root /var/www/html;
    index index.php index.html index.htm;
    #server_name localhost
    location "/"
    {
        index index.php index.html index.htm;
        #try_files $uri $uri/ =404;
    }

    location ~ \.php$
    {
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $request_filename;
    }
}
EOF

    systemctl restart nginx
}


install_dvwa(){

    if [[ ! -d "/var/www/html" ]];
    then
          mkdir -p /var/www;
          ln -s /usr/share/nginx/html /var/www/html;
          chown -R www-data. /var/www/html;
    fi

    cd /var/www/html
    rm -rf /var/www/html/.[!.]*
    rm -rf /var/www/html/*
    git clone https://github.com/ethicalhack3r/DVWA.git ./
    chown -R www-data. ./
    cp config/config.inc.php.dist config/config.inc.php

    ### chmod uploads and log file to be writable by nobody
```

```
    chmod 777 ./hackable/uploads/
    chmod 777 ./external/phpids/0.6/lib/IDS/tmp/phpids_log.txt

    ## change the values in the config to match our setup (these are what you need to
update!
    sed -i '/db_user/ s/root/'${MYSQL_dvwa_user}'/'
/var/www/html/config/config.inc.php
    sed -i '/db_password/ s/p@ssw0rd/'${MYSQL_dvwa_password}'/'
/var/www/html/config/config.inc.php
    sed -i "/recaptcha_public_key/ s/''/'"${recaptcha_public_key}"'/"
/var/www/html/config/config.inc.php
    sed -i "/recaptcha_private_key/ s/''/'"${recaptcha_private_key}"'/"
/var/www/html/config/config.inc.php

}


update_mysql_user_pws(){
## The mysql passwords are set via /usr/share/nginx/html/dvwa/includes/DBMS/MySQL.php.
#  If you edit this every time they are reset it will reset to those.
#  Otherwise you can do a sql update statement to update them all (they are just md5's
of the string.
#  The issue is the users table doesn't get created until you click that button T_T to
init.

#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'admin';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'gordonb';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'1337';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'pablo';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user =
'smithy';"

sed -i '/admin/ s/password/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/gordonb/ s/abc123/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/1337/ s/charley/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/pablo/ s/letmein/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/smithy/ s/password/'${DVWA_admin_password}'/g'
/var/www/html/dvwa/includes/DBMS/MySQL.php
}


install_base
config_mysql
```

```
install_dvwa
update_mysql_user_pws
config_php
config_nginx
```

Save and write this file.

If you have issues with copying and pasting the above file because code blocks in PDFs always copy correctly [NOT!], you could use curl, i.e. Make sure the bootstrap.sh file ends up in the same directory as the Vagrantfile.

```
$ curl -o bootstrap.sh  http://securityhardening.com/files/bootstrap_sh_20200928.txt
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Then run (inside the directory kali-linux-vm):

```
$ vagrant up
```

This will download the appropriate images and start the virtual machines. Once running, through the VirtuaBox GUI, login as root. Password is “toor”, root backwards. Edit the following file: `/etc/ssh/sshd_config`

And change the line: `#PermitRootLogin prothibit-password` To: `PermitRootLogin yes` Meaning strip the comment out on the beginning of the line and alter `prohibit-password` to `yes`.

Then restart the ssh daemon:

```
# kill HUP $(pgrep sshd)
```

Notice, you are on a Bridged adapter, this will open the instance to allow root to ssh in with the most unsecure password in the world. Only make this change (allowing root to login via SSH) if you require root SSH access. You can change the root user’s password, which is highly recommended.

For the DVWA instance, I would first run ‘vagrant status’ to capture the name that vagrant is using for the running instance.

```
# vagrant status
```

Choose

```
Current machine states:
```

```
kali-linux-vagrant running (virtualbox)
dvwa-vagrant running (virtualbox)
```

This environment represents multiple VMs. The VMs are all listed above with their current state. For more information about a specific VM, run `vagrant status NAME`.

From there, log into the DVWA instance with:

```
$ vagrant ssh dvwa-vagrant
```

And then get the current IP address.

```
$ ip a
```

Choose the second network adapter, it should look like:

```
ubuntu@dvwa:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 02:53:17:3c:de:80 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::53:17ff:fe3c:de80/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:f0:77:2d brd ff:ff:ff:ff:ff:ff
    inet 172.20.156.76/24 brd 172.20.156.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef0:772d/64 scope link
        valid_lft forever preferred_lft forever
```

The test network used for this paper uses 172.20.156.0/24 as the network range [shown here in section 3]. Therefore, the adapter, enp0s8 is what he is looking for. The IP to use as a target is 172.20.156.76. Write down your value.

Chapter 3. chkrootkit and rkhunter

Installation

Open a terminal and enter:

```
sudo -i
apt update
apt upgrade
systemctl reboot
```

wait for the system to come back online.

Open a terminal and enter:

```
sudo -i
apt install -y chkrootkit rkhunter
```

We should now be able to run the man pages to understand the tooling better.

```
chkrootkit(8)                                   System Manager's Manual
chkrootkit(8)

NAME
       chkrootkit - Scan the system for signs of rootkits

SYNOPSIS
       chkrootkit [OPTION]... [TESTNAME]...

DESCRIPTION
       chkrootkit  examines  the  target system for signs that it has been tampered
with. Some tools which chkrootkit
       uses can be found in /usr/lib/chkrootkit.

OPTIONS
       Unlike usual programmes, options cannot be 'combined', so you cannot need to
write '-q -n' instead of '-qn'

       -q     Enter quiet mode. This suppresses output of tests that find nothing
suspicious.

       -x     Enter expert mode. This makes many tests produces additional output
showing what they have found.
....
```

As well as:

```
rkhunter(8)                                                System Manager's Manual
rkhunter(8)

NAME
       rkhunter - RootKit Hunter

SYNOPSIS
       rkhunter {--check | --unlock | --update | --versioncheck |
                 --propupd [{filename | directory | package name},...] |
                 --list [tests | {lang | languages} | rootkits | perl |
                        propfiles] |
                 --config-check | --version | --help} [options]

DESCRIPTION
       rkhunter  is a shell script which carries out various checks on the local
system to try and detect known rootkits and malware. It also
       performs checks to see if commands have been modified, if the system startup
files have been modified, and various checks on the  net
       work interfaces, including checks for listening applications.

       rkhunter  has  been  written  to be as generic as possible, and so should run
on most Linux and UNIX systems. It is provided with some
       support scripts should certain commands be missing from the system, and some of
these are perl scripts.  rkhunter does require certain
       commands  to be present for it to be able to execute. Additionally, some tests
require specific commands, but if these are not present
       then the test will be skipped. rkhunter needs to be run under a Bourne-type
shell, typically bash or ksh. rkhunter can  be  run  as  a
       cron job or from the command-line.

COMMAND OPTIONS
       If no command option is given, then --help is assumed.  rkhunter will return a
non-zero exit code if any error or warning occurs.

       -c, --check
              This  command option tells rkhunter to perform various checks on the
local system. The result of each test will be displayed on
              stdout. If anything suspicious is found, then a warning will be
displayed. A log file of the tests and the results will be  au
              tomatically produced.

              It is suggested that this command option is run regularly in order to
ensure that the system has not been compromised.
....
```

Usage:

`chkrootkit` example run:

```
┌──(root㉿kali-linux-vagrant)-[~]
└─# chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
Checking `ifconfig'...                                      not infected
Checking `inetd'...                                         not infected
Checking `inetdconf'...                                     not found
Checking `identd'...                                        not found
Checking `init'...                                          not infected
Checking `killall'...                                       not infected
Checking `ldsopreload'...                                   not infected
Checking `login'...                                         not infected
Checking `ls'...                                            not infected
Checking `lsof'...                                          not infected
Checking `mail'...                                          not infected
Checking `mingetty'...                                      not found
Checking `netstat'...                                       not infected
Checking `named'...                                         not found
Checking `passwd'...                                        not infected
Checking `pidof'...                                         not infected
Checking `pop2'...                                          not found
Checking `pop3'...                                          not found
Checking `ps'...                                            not infected
Checking `pstree'...                                        not infected
Checking `rpcinfo'...                                       not infected
Checking `rlogind'...                                       not found
Checking `rshd'...                                          not found
Checking `slogin'...                                        not infected
Checking `sendmail'...                                      not infected
Checking `sshd'...                                          not infected
Checking `syslogd'...                                       not tested
Checking `tar'...                                           not infected
```

```
Checking `tcpd'...                                         not found
Checking `tcpdump'...                                      not infected
Checking `top'...                                          not infected
Checking `telnetd'...                                      not found
Checking `timed'...                                        not found
Checking `traceroute'...                                   not infected
Checking `vdir'...                                         not infected
Checking `w'...                                            not infected
Checking `write'...                                        not infected
Checking `aliens'...                                       no suspect files
Searching for sniffer's logs, it may take a while...       nothing found
Searching for rootkit HiDrootkit's default files...        nothing found
Searching for rootkit t0rn's default files...              nothing found
Searching for t0rn's v8 defaults...                        nothing found
Searching for rootkit Lion's default files...              nothing found
Searching for rootkit RSHA's default files...              nothing found
Searching for rootkit RH-Sharpe's default files...         nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following
suspicious files and directories were found:
/usr/lib/llvm-11/build/utils/lit/tests/.coveragerc
/usr/lib/python3/dist-packages/numpy/f2py/tests/src/assumed_shape/.f2py_f2cmap
/usr/lib/python3/dist-packages/cme/.hooks
/usr/lib/python3/dist-packages/matplotlib/backends/web_backend/.prettierrc
/usr/lib/python3/dist-packages/matplotlib/backends/web_backend/.eslintrc.js
/usr/lib/python3/dist-packages/matplotlib/backends/web_backend/.prettierignore
/usr/lib/python3/dist-packages/matplotlib/tests/tinypages/_static/.gitignore
/usr/lib/python3/dist-packages/matplotlib/tests/tinypages/.gitignore
/usr/lib/python3/dist-packages/matplotlib/tests/baseline_images/.keep
/usr/lib/jvm/.java-1.11.0-openjdk-amd64.jinfo
/usr/lib/hashcat/modules/.lock
/usr/lib/llvm-13/build/utils/lit/tests/.coveragerc
/usr/lib/llvm-13/build/utils/lit/tests/Inputs/reorder/.lit_test_times.txt
/usr/lib/ruby/vendor_ruby/rubygems/optparse/.document
/usr/lib/ruby/vendor_ruby/rubygems/ssl_certs/.document
/usr/lib/ruby/vendor_ruby/rubygems/tsort/.document
/usr/lib/ruby/gems/3.0.0/gems/power_assert-1.2.0/.travis.yml
/usr/lib/ruby/gems/3.0.0/gems/rbs-1.4.0/.rubocop.yml
/usr/lib/ruby/gems/3.0.0/gems/minitest-5.14.2/.autotest
/usr/lib/llvm-14/build/utils/lit/tests/.coveragerc
/usr/lib/llvm-14/build/utils/lit/tests/Inputs/reorder/.lit_test_times.txt

Searching for LPD Worm files and dirs...                   nothing found
Searching for Ramen Worm files and dirs...                 nothing found
Searching for Maniac files and dirs...                     nothing found
Searching for RK17 files and dirs...                       nothing found
Searching for Ducoci rootkit...                            nothing found
Searching for Adore Worm...                                nothing found
Searching for ShitC Worm...                                nothing found
Searching for Omega Worm...                                nothing found
Searching for Sadmind/IIS Worm...                          nothing found
```

```
Searching for MonKit...                                    nothing found
Searching for Showtee...                                   nothing found
Searching for OpticKit...                                  nothing found
Searching for T.R.K...                                     nothing found
Searching for Mithra...                                    nothing found
Searching for OBSD rk v1...                                nothing found
Searching for LOC rootkit...                               nothing found
Searching for Romanian rootkit...                          nothing found
Searching for HKRK rootkit...                              nothing found
Searching for Suckit rootkit...                            nothing found
Searching for Volc rootkit...                              nothing found
Searching for Gold2 rootkit...                             nothing found
Searching for TC2 Worm default files and dirs...           nothing found
Searching for Anonoying rootkit default files and dirs...  nothing found
Searching for ZK rootkit default files and dirs...         nothing found
Searching for ShKit rootkit default files and dirs...      nothing found
Searching for AjaKit rootkit default files and dirs...     nothing found
Searching for zaRwT rootkit default files and dirs...      nothing found
Searching for Madalin rootkit default files...             nothing found
Searching for Fu rootkit default files...                  nothing found
Searching for ESRK rootkit default files...                nothing found
Searching for rootedoor...                                 nothing found
Searching for ENYELKM rootkit default files...             nothing found
Searching for common ssh-scanners default files...         nothing found
Searching for Linux/Ebury - Operation Windigo ssh...       nothing found
Searching for 64-bit Linux Rootkit ...                     nothing found
Searching for 64-bit Linux Rootkit modules...              nothing found
Searching for Mumblehard Linux ...                         nothing found
Searching for Backdoor.Linux.Mokes.a ...                   nothing found
Searching for Malicious TinyDNS ...                        nothing found
Searching for Linux.Xor.DDoS ...                           nothing found
Searching for Linux.Proxy.1.0 ...                          nothing found
Searching for CrossRAT ...                                 nothing found
Searching for Hidden Cobra ...                             nothing found
Searching for Rocke Miner ...                              nothing found
Searching for PWNLNX4 lkm...                               nothing found
Searching for PWNLNX6 lkm...                               nothing found
Searching for Umbreon lrk...                               nothing found
Searching for Kinsing.a backdoor...                        nothing found
Searching for RotaJakiro backdoor...                       nothing found
Searching for suspect PHP files...                         nothing found
Searching for anomalies in shell history files...          nothing found
Checking `asp'...                                          not infected
Checking `bindshell'...                                    not infected
Checking `lkm'...                                          chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                      not found
Checking `sniffer'...                                      Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
eth0: PACKET SNIFFER(/usr/sbin/dhclient[536])
eth1: PACKET SNIFFER(/usr/sbin/dhclient[599])
```

```
Checking `w55808'...                                       not infected
Checking `wted'...                                         chkwtmp: nothing deleted
Checking `scalper'...                                      not infected
Checking `slapper'...                                      not infected
Checking `z2'...                                           chklastlog: nothing
deleted
Checking `chkutmp'...                                      The tty of the following
process(es) was not found in /var/run/utmp:
! RUID          PID TTY    CMD
! vagrant      1405 pts/0  sudo -i
! vagrant      1318 pts/0  /usr/bin/zsh
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                   not tested
```

It is that simple! Just run the command, `chkrootkit` and this is what you might get for output.

Let's test `rkhunter`. With this command, add the `--check` parameter.

```
┌──(root㉿kali-linux-vagrant)-[~]
└─# rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None found ]
    Checking for preloaded libraries                         [ None found ]
    Checking LD_LIBRARY_PATH variable                        [ Not found ]

  Performing file properties checks
    Checking for prerequisites                               [ OK ]
    /usr/sbin/adduser                                        [ OK ]
    /usr/sbin/chroot                                         [ OK ]
    /usr/sbin/cron                                           [ OK ]
    /usr/sbin/depmod                                         [ OK ]
    /usr/sbin/fsck                                           [ OK ]
    /usr/sbin/groupadd                                       [ OK ]
    /usr/sbin/groupdel                                       [ OK ]
    /usr/sbin/groupmod                                       [ OK ]
    /usr/sbin/grpck                                          [ OK ]
    /usr/sbin/ifconfig                                       [ OK ]
    /usr/sbin/ifdown                                         [ OK ]
    /usr/sbin/ifup                                           [ OK ]
    /usr/sbin/init                                           [ OK ]
    /usr/sbin/insmod                                         [ OK ]
    /usr/sbin/ip                                             [ OK ]
    /usr/sbin/lsmod                                          [ OK ]
```

```
    /usr/sbin/modinfo                                       [ OK ]
    /usr/sbin/modprobe                                      [ OK ]
    /usr/sbin/nologin                                       [ OK ]
    /usr/sbin/pwck                                          [ OK ]
    /usr/sbin/rmmod                                         [ OK ]
    /usr/sbin/route                                         [ OK ]
    /usr/sbin/rsyslogd                                      [ OK ]
    /usr/sbin/runlevel                                      [ OK ]
    /usr/sbin/sshd                                          [ OK ]
    /usr/sbin/sulogin                                       [ OK ]
    /usr/sbin/sysctl                                        [ OK ]
    /usr/sbin/useradd                                       [ OK ]
    /usr/sbin/userdel                                       [ OK ]
    /usr/sbin/usermod                                       [ OK ]
    /usr/sbin/vipw                                          [ OK ]
    /usr/sbin/unhide                                        [ OK ]
    /usr/sbin/unhide-linux                                  [ OK ]
    /usr/sbin/unhide-posix                                  [ OK ]
    /usr/sbin/unhide-tcp                                    [ OK ]
    /usr/bin/awk                                            [ OK ]
    /usr/bin/basename                                       [ OK ]
    /usr/bin/bash                                           [ OK ]
    /usr/bin/cat                                            [ OK ]
    /usr/bin/chattr                                         [ OK ]
    /usr/bin/chmod                                          [ OK ]
    /usr/bin/chown                                          [ OK ]
    /usr/bin/cp                                             [ OK ]
    /usr/bin/curl                                           [ OK ]
    /usr/bin/cut                                            [ OK ]
    /usr/bin/date                                           [ OK ]
    /usr/bin/df                                             [ OK ]
    /usr/bin/diff                                           [ OK ]
    /usr/bin/dirname                                        [ OK ]
    /usr/bin/dmesg                                          [ OK ]
    /usr/bin/dpkg                                           [ OK ]
    /usr/bin/dpkg-query                                     [ OK ]
    /usr/bin/du                                             [ OK ]
    /usr/bin/echo                                           [ OK ]
    /usr/bin/egrep                                          [ OK ]
    /usr/bin/env                                            [ OK ]
    /usr/bin/fgrep                                          [ OK ]
    /usr/bin/file                                           [ OK ]
    /usr/bin/find                                           [ OK ]
    /usr/bin/fuser                                          [ OK ]
    /usr/bin/GET                                            [ OK ]
    /usr/bin/grep                                           [ OK ]
    /usr/bin/groups                                         [ OK ]
    /usr/bin/head                                           [ OK ]
    /usr/bin/id                                             [ OK ]
    /usr/bin/ip                                             [ OK ]
    /usr/bin/ipcs                                           [ OK ]
```

```
    /usr/bin/kill                                               [ OK ]
    /usr/bin/killall                                            [ OK ]
    /usr/bin/last                                               [ OK ]
    /usr/bin/lastlog                                            [ OK ]
    /usr/bin/ldd                                                [ OK ]
    /usr/bin/less                                               [ OK ]
    /usr/bin/locate                                             [ OK ]
    /usr/bin/logger                                             [ OK ]
    /usr/bin/login                                              [ OK ]
    /usr/bin/ls                                                 [ OK ]
    /usr/bin/lsattr                                             [ OK ]
    /usr/bin/lsmod                                              [ OK ]
    /usr/bin/lsof                                               [ OK ]
    /usr/bin/mail                                               [ Warning ]
    /usr/bin/md5sum                                             [ OK ]
    /usr/bin/mktemp                                             [ OK ]
    /usr/bin/more                                               [ OK ]
    /usr/bin/mount                                              [ OK ]
    /usr/bin/mv                                                 [ OK ]
    /usr/bin/netstat                                            [ OK ]
    /usr/bin/newgrp                                             [ OK ]
    /usr/bin/passwd                                             [ OK ]
    /usr/bin/perl                                               [ OK ]
    /usr/bin/pgrep                                              [ OK ]
    /usr/bin/ping                                               [ OK ]
    /usr/bin/pkill                                              [ OK ]
    /usr/bin/ps                                                 [ OK ]
    /usr/bin/pstree                                             [ OK ]
    /usr/bin/pwd                                                [ OK ]
    /usr/bin/readlink                                           [ OK ]
    /usr/bin/rkhunter                                           [ OK ]
    /usr/bin/runcon                                             [ OK ]
    /usr/bin/sed                                                [ OK ]
    /usr/bin/sh                                                 [ OK ]
    /usr/bin/sha1sum                                            [ OK ]
    /usr/bin/sha224sum                                          [ OK ]
    /usr/bin/sha256sum                                          [ OK ]
    /usr/bin/sha384sum                                          [ OK ]
    /usr/bin/sha512sum                                          [ OK ]
    /usr/bin/size                                               [ OK ]
    /usr/bin/sort                                               [ OK ]
    /usr/bin/ssh                                                [ OK ]
    /usr/bin/stat                                               [ OK ]
    /usr/bin/strings                                            [ OK ]
    /usr/bin/su                                                 [ OK ]
    /usr/bin/sudo                                               [ OK ]
    /usr/bin/tail                                               [ OK ]
    /usr/bin/telnet                                             [ OK ]
    /usr/bin/test                                               [ OK ]
    /usr/bin/top                                                [ OK ]
    /usr/bin/touch                                              [ OK ]
```

```
    /usr/bin/tr                                                [ OK ]
    /usr/bin/uname                                             [ OK ]
    /usr/bin/uniq                                              [ OK ]
    /usr/bin/users                                             [ OK ]
    /usr/bin/vmstat                                            [ OK ]
    /usr/bin/w                                                 [ OK ]
    /usr/bin/watch                                             [ OK ]
    /usr/bin/wc                                                [ OK ]
    /usr/bin/wget                                              [ OK ]
    /usr/bin/whatis                                            [ OK ]
    /usr/bin/whereis                                           [ OK ]
    /usr/bin/which                                             [ OK ]
    /usr/bin/who                                               [ OK ]
    /usr/bin/whoami                                            [ OK ]
    /usr/bin/numfmt                                            [ OK ]
    /usr/bin/kmod                                              [ OK ]
    /usr/bin/systemd                                           [ OK ]
    /usr/bin/systemctl                                         [ OK ]
    /usr/bin/gawk                                              [ OK ]
    /usr/bin/lwp-request                                       [ Warning ]
    /usr/bin/plocate                                           [ OK ]
    /usr/bin/bsd-mailx                                         [ Warning ]
    /usr/bin/dash                                              [ OK ]
    /usr/bin/x86_64-linux-gnu-size                             [ OK ]
    /usr/bin/x86_64-linux-gnu-strings                          [ OK ]
    /usr/bin/inetutils-telnet                                  [ OK ]
    /usr/bin/which.debianutils                                 [ OK ]
    /usr/lib/systemd/systemd                                   [ OK ]

[Press <ENTER> to continue]


Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                   [ Not found ]
    ADM Worm                                                   [ Not found ]
    AjaKit Rootkit                                             [ Not found ]
    Adore Rootkit                                              [ Not found ]
    aPa Kit                                                    [ Not found ]
    Apache Worm                                                [ Not found ]
    Ambient (ark) Rootkit                                      [ Not found ]
    Balaur Rootkit                                             [ Not found ]
    BeastKit Rootkit                                           [ Not found ]
    beX2 Rootkit                                               [ Not found ]
    BOBKit Rootkit                                             [ Not found ]
    cb Rootkit                                                 [ Not found ]
    CiNIK Worm (Slapper.B variant)                             [ Not found ]
    Danny-Boy's Abuse Kit                                      [ Not found ]
    Devil RootKit                                              [ Not found ]
    Diamorphine LKM                                            [ Not found ]
```

```
    Dica-Kit Rootkit                                        [ Not found ]
    Dreams Rootkit                                          [ Not found ]
    Duarawkz Rootkit                                        [ Not found ]
    Ebury backdoor                                          [ Not found ]
    Enye LKM                                                [ Not found ]
    Flea Linux Rootkit                                      [ Not found ]
    Fu Rootkit                                              [ Not found ]
    Fuck`it Rootkit                                         [ Not found ]
    GasKit Rootkit                                          [ Not found ]
    Heroin LKM                                              [ Not found ]
    HjC Kit                                                 [ Not found ]
    ignoKit Rootkit                                         [ Not found ]
    IntoXonia-NG Rootkit                                    [ Not found ]
    Irix Rootkit                                            [ Not found ]
    Jynx Rootkit                                            [ Not found ]
    Jynx2 Rootkit                                           [ Not found ]
    KBeast Rootkit                                          [ Not found ]
    Kitko Rootkit                                           [ Not found ]
    Knark Rootkit                                           [ Not found ]
    ld-linuxv.so Rootkit                                    [ Not found ]
    Li0n Worm                                               [ Not found ]
    Lockit / LJK2 Rootkit                                   [ Not found ]
    Mokes backdoor                                          [ Not found ]
    Mood-NT Rootkit                                         [ Not found ]
    MRK Rootkit                                             [ Not found ]
    Ni0 Rootkit                                             [ Not found ]
    Ohhara Rootkit                                          [ Not found ]
    Optic Kit (Tux) Worm                                    [ Not found ]
    Oz Rootkit                                              [ Not found ]
    Phalanx Rootkit                                         [ Not found ]
    Phalanx2 Rootkit                                        [ Not found ]
    Phalanx2 Rootkit (extended tests)                       [ Not found ]
    Portacelo Rootkit                                       [ Not found ]
    R3dstorm Toolkit                                        [ Not found ]
    RH-Sharpe's Rootkit                                     [ Not found ]
    RSHA's Rootkit                                          [ Not found ]
    Scalper Worm                                            [ Not found ]
    Sebek LKM                                               [ Not found ]
    Shutdown Rootkit                                        [ Not found ]
    SHV4 Rootkit                                            [ Not found ]
    SHV5 Rootkit                                            [ Not found ]
    Sin Rootkit                                             [ Not found ]
    Slapper Worm                                            [ Not found ]
    Sneakin Rootkit                                         [ Not found ]
    'Spanish' Rootkit                                       [ Not found ]
    Suckit Rootkit                                          [ Not found ]
    Superkit Rootkit                                        [ Not found ]
    TBD (Telnet BackDoor)                                   [ Not found ]
    TeLeKiT Rootkit                                         [ Not found ]
    T0rn Rootkit                                            [ Not found ]
    trNkit Rootkit                                          [ Not found ]
```

```
    Trojanit Kit                                              [ Not found ]
    Tuxtendo Rootkit                                          [ Not found ]
    URK Rootkit                                               [ Not found ]
    Vampire Rootkit                                           [ Not found ]
    VcKit Rootkit                                             [ Not found ]
    Volc Rootkit                                              [ Not found ]
    Xzibit Rootkit                                            [ Not found ]
    zaRwT.KiT Rootkit                                         [ Not found ]
    ZK Rootkit                                                [ Not found ]

[Press <ENTER> to continue]


  Performing additional rootkit checks
    Suckit Rootkit additional checks                          [ OK ]
    Checking for possible rootkit files and directories       [ None found ]
    Checking for possible rootkit strings                     [ None found ]

  Performing malware checks
    Checking running processes for suspicious files           [ None found ]
    Checking for login backdoors                              [ None found ]
    Checking for sniffer log files                            [ None found ]
    Checking for suspicious directories                       [ None found ]
    Checking for suspicious (large) shared memory segments    [ Warning ]
    Checking for Apache backdoor                              [ Not found ]

  Performing Linux specific checks
    Checking loaded kernel modules                            [ OK ]
    Checking kernel module names                              [ OK ]

[Press <ENTER> to continue]


Checking the network...

  Performing checks on the network ports
    Checking for backdoor ports                               [ None found ]

  Performing checks on the network interfaces
    Checking for promiscuous interfaces                       [ None found ]

Checking the local host...

  Performing system boot checks
    Checking for local host name                              [ Found ]
    Checking for system startup files                         [ Found ]
    Checking system startup files for malware                 [ None found ]

  Performing group and account checks
    Checking for passwd file                                  [ Found ]
    Checking for root equivalent (UID 0) accounts             [ None found ]
```

```
    Checking for passwordless accounts                        [ None found ]
    Checking for passwd file changes                          [ None found ]
    Checking for group file changes                           [ None found ]
    Checking root account shell history files                 [ None found ]

  Performing system configuration file checks
    Checking for an SSH configuration file                    [ Found ]
    Checking if SSH root access is allowed                    [ Warning ]
    Checking if SSH protocol v1 is allowed                    [ Not set ]
    Checking for other suspicious configuration settings      [ None found ]
    Checking for a running system logging daemon              [ Found ]
    Checking for a system logging configuration file          [ Found ]
    Checking if syslog remote logging is allowed              [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                   [ None found ]
    Checking for hidden files and directories                 [ Warning ]

[Press <ENTER> to continue]



System checks summary
=====================

File properties checks...
    Files checked: 146
    Suspect files: 3

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 2

Applications checks...
    All checks skipped

The system checks took: 1 minute and 26 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Simply Beautiful output from both tools. Exactly what I Need to see/understand without a bunch of nonsense.

A more advance run with `rkhunter`.

```
┌──(root㉿kali-linux-vagrant)-[~]
└─# rkhunter -check --enable all --disable none
```

```
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None found ]
    Checking for preloaded libraries                         [ None found ]
    Checking LD_LIBRARY_PATH variable                        [ Not found ]

  Performing file properties checks
    Checking for prerequisites                               [ OK ]
    /usr/sbin/adduser                                        [ OK ]
    /usr/sbin/chroot                                         [ OK ]
    /usr/sbin/cron                                           [ OK ]
    /usr/sbin/depmod                                         [ OK ]
    /usr/sbin/fsck                                           [ OK ]
    /usr/sbin/groupadd                                       [ OK ]
    /usr/sbin/groupdel                                       [ OK ]
    /usr/sbin/groupmod                                       [ OK ]
    /usr/sbin/grpck                                          [ OK ]
    /usr/sbin/ifconfig                                       [ OK ]
    /usr/sbin/ifdown                                         [ OK ]
    /usr/sbin/ifup                                           [ OK ]
    /usr/sbin/init                                           [ OK ]
    /usr/sbin/insmod                                         [ OK ]
    /usr/sbin/ip                                             [ OK ]
    /usr/sbin/lsmod                                          [ OK ]
    /usr/sbin/modinfo                                        [ OK ]
    /usr/sbin/modprobe                                       [ OK ]
    /usr/sbin/nologin                                        [ OK ]
    /usr/sbin/pwck                                           [ OK ]
    /usr/sbin/rmmod                                          [ OK ]
    /usr/sbin/route                                          [ OK ]
    /usr/sbin/rsyslogd                                       [ OK ]
    /usr/sbin/runlevel                                       [ OK ]
    /usr/sbin/sshd                                           [ OK ]
    /usr/sbin/sulogin                                        [ OK ]
    /usr/sbin/sysctl                                         [ OK ]
    /usr/sbin/useradd                                        [ OK ]
    /usr/sbin/userdel                                        [ OK ]
    /usr/sbin/usermod                                        [ OK ]
    /usr/sbin/vipw                                           [ OK ]
    /usr/sbin/unhide                                         [ OK ]
    /usr/sbin/unhide-linux                                   [ OK ]
    /usr/sbin/unhide-posix                                   [ OK ]
    /usr/sbin/unhide-tcp                                     [ OK ]
    /usr/bin/awk                                             [ OK ]
    /usr/bin/basename                                        [ OK ]
```

```
    /usr/bin/bash                                                [ OK ]
    /usr/bin/cat                                                 [ OK ]
    /usr/bin/chattr                                              [ OK ]
    /usr/bin/chmod                                               [ OK ]
    /usr/bin/chown                                               [ OK ]
    /usr/bin/cp                                                  [ OK ]
    /usr/bin/curl                                                [ OK ]
    /usr/bin/cut                                                 [ OK ]
    /usr/bin/date                                                [ OK ]
    /usr/bin/df                                                  [ OK ]
    /usr/bin/diff                                                [ OK ]
    /usr/bin/dirname                                             [ OK ]
    /usr/bin/dmesg                                               [ OK ]
    /usr/bin/dpkg                                                [ OK ]
    /usr/bin/dpkg-query                                          [ OK ]
    /usr/bin/du                                                  [ OK ]
    /usr/bin/echo                                                [ OK ]
    /usr/bin/egrep                                               [ OK ]
    /usr/bin/env                                                 [ OK ]
    /usr/bin/fgrep                                               [ OK ]
    /usr/bin/file                                                [ OK ]
    /usr/bin/find                                                [ OK ]
    /usr/bin/fuser                                               [ OK ]
    /usr/bin/GET                                                 [ OK ]
    /usr/bin/grep                                                [ OK ]
    /usr/bin/groups                                              [ OK ]
    /usr/bin/head                                                [ OK ]
    /usr/bin/id                                                  [ OK ]
    /usr/bin/ip                                                  [ OK ]
    /usr/bin/ipcs                                                [ OK ]
    /usr/bin/kill                                                [ OK ]
    /usr/bin/killall                                             [ OK ]
    /usr/bin/last                                                [ OK ]
    /usr/bin/lastlog                                             [ OK ]
    /usr/bin/ldd                                                 [ OK ]
    /usr/bin/less                                                [ OK ]
    /usr/bin/locate                                              [ OK ]
    /usr/bin/logger                                              [ OK ]
    /usr/bin/login                                               [ OK ]
    /usr/bin/ls                                                  [ OK ]
    /usr/bin/lsattr                                              [ OK ]
    /usr/bin/lsmod                                               [ OK ]
    /usr/bin/lsof                                                [ OK ]
    /usr/bin/mail                                                [ OK ]
    /usr/bin/md5sum                                              [ OK ]
    /usr/bin/mktemp                                              [ OK ]
    /usr/bin/more                                                [ OK ]
    /usr/bin/mount                                               [ OK ]
    /usr/bin/mv                                                  [ OK ]
    /usr/bin/netstat                                             [ OK ]
    /usr/bin/newgrp                                              [ OK ]
```

```
    /usr/bin/passwd                                         [ OK ]
    /usr/bin/perl                                           [ OK ]
    /usr/bin/pgrep                                          [ OK ]
    /usr/bin/ping                                           [ OK ]
    /usr/bin/pkill                                          [ OK ]
    /usr/bin/ps                                             [ OK ]
    /usr/bin/pstree                                         [ OK ]
    /usr/bin/pwd                                            [ OK ]
    /usr/bin/readlink                                       [ OK ]
    /usr/bin/rkhunter                                       [ OK ]
    /usr/bin/runcon                                         [ OK ]
    /usr/bin/sed                                            [ OK ]
    /usr/bin/sh                                             [ OK ]
    /usr/bin/sha1sum                                        [ OK ]
    /usr/bin/sha224sum                                      [ OK ]
    /usr/bin/sha256sum                                      [ OK ]
    /usr/bin/sha384sum                                      [ OK ]
    /usr/bin/sha512sum                                      [ OK ]
    /usr/bin/size                                           [ OK ]
    /usr/bin/sort                                           [ OK ]
    /usr/bin/ssh                                            [ OK ]
    /usr/bin/stat                                           [ OK ]
    /usr/bin/strings                                        [ OK ]
    /usr/bin/su                                             [ OK ]
    /usr/bin/sudo                                           [ OK ]
    /usr/bin/tail                                           [ OK ]
    /usr/bin/telnet                                         [ OK ]
    /usr/bin/test                                           [ OK ]
    /usr/bin/top                                            [ OK ]
    /usr/bin/touch                                          [ OK ]
    /usr/bin/tr                                             [ OK ]
    /usr/bin/uname                                          [ OK ]
    /usr/bin/uniq                                           [ OK ]
    /usr/bin/users                                          [ OK ]
    /usr/bin/vmstat                                         [ OK ]
    /usr/bin/w                                              [ OK ]
    /usr/bin/watch                                          [ OK ]
    /usr/bin/wc                                             [ OK ]
    /usr/bin/wget                                           [ OK ]
    /usr/bin/whatis                                         [ OK ]
    /usr/bin/whereis                                        [ OK ]
    /usr/bin/which                                          [ OK ]
    /usr/bin/who                                            [ OK ]
    /usr/bin/whoami                                         [ OK ]
    /usr/bin/numfmt                                         [ OK ]
    /usr/bin/kmod                                           [ OK ]
    /usr/bin/systemd                                        [ OK ]
    /usr/bin/systemctl                                      [ OK ]
    /usr/bin/gawk                                           [ OK ]
    /usr/bin/lwp-request                                    [ Warning ]
    /usr/bin/plocate                                        [ OK ]
```

```
    /usr/bin/bsd-mailx                                          [ OK ]
    /usr/bin/dash                                               [ OK ]
    /usr/bin/x86_64-linux-gnu-size                              [ OK ]
    /usr/bin/x86_64-linux-gnu-strings                           [ OK ]
    /usr/bin/inetutils-telnet                                   [ OK ]
    /usr/bin/which.debianutils                                  [ OK ]
    /usr/lib/systemd/systemd                                    [ OK ]

[Press <ENTER> to continue]


Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                    [ Not found ]
    ADM Worm                                                    [ Not found ]
    AjaKit Rootkit                                              [ Not found ]
    Adore Rootkit                                               [ Not found ]
    aPa Kit                                                     [ Not found ]
    Apache Worm                                                 [ Not found ]
    Ambient (ark) Rootkit                                       [ Not found ]
    Balaur Rootkit                                              [ Not found ]
    BeastKit Rootkit                                            [ Not found ]
    beX2 Rootkit                                                [ Not found ]
    BOBKit Rootkit                                              [ Not found ]
    cb Rootkit                                                  [ Not found ]
    CiNIK Worm (Slapper.B variant)                              [ Not found ]
    Danny-Boy's Abuse Kit                                       [ Not found ]
    Devil RootKit                                               [ Not found ]
    Diamorphine LKM                                             [ Not found ]
    Dica-Kit Rootkit                                            [ Not found ]
    Dreams Rootkit                                              [ Not found ]
    Duarawkz Rootkit                                            [ Not found ]
    Ebury backdoor                                              [ Not found ]
    Enye LKM                                                    [ Not found ]
    Flea Linux Rootkit                                          [ Not found ]
    Fu Rootkit                                                  [ Not found ]
    Fuck`it Rootkit                                             [ Not found ]
    GasKit Rootkit                                              [ Not found ]
    Heroin LKM                                                  [ Not found ]
    HjC Kit                                                     [ Not found ]
    ignoKit Rootkit                                             [ Not found ]
    IntoXonia-NG Rootkit                                        [ Not found ]
    Irix Rootkit                                                [ Not found ]
    Jynx Rootkit                                                [ Not found ]
    Jynx2 Rootkit                                               [ Not found ]
    KBeast Rootkit                                              [ Not found ]
    Kitko Rootkit                                               [ Not found ]
    Knark Rootkit                                               [ Not found ]
    ld-linuxv.so Rootkit                                        [ Not found ]
    Li0n Worm                                                   [ Not found ]
```

```
    Lockit / LJK2 Rootkit                                    [ Not found ]
    Mokes backdoor                                           [ Not found ]
    Mood-NT Rootkit                                          [ Not found ]
    MRK Rootkit                                              [ Not found ]
    Ni0 Rootkit                                              [ Not found ]
    Ohhara Rootkit                                           [ Not found ]
    Optic Kit (Tux) Worm                                     [ Not found ]
    Oz Rootkit                                               [ Not found ]
    Phalanx Rootkit                                          [ Not found ]
    Phalanx2 Rootkit                                         [ Not found ]
    Phalanx2 Rootkit (extended tests)                        [ Not found ]
    Portacelo Rootkit                                        [ Not found ]
    R3dstorm Toolkit                                         [ Not found ]
    RH-Sharpe's Rootkit                                      [ Not found ]
    RSHA's Rootkit                                           [ Not found ]
    Scalper Worm                                             [ Not found ]
    Sebek LKM                                                [ Not found ]
    Shutdown Rootkit                                         [ Not found ]
    SHV4 Rootkit                                             [ Not found ]
    SHV5 Rootkit                                             [ Not found ]
    Sin Rootkit                                              [ Not found ]
    Slapper Worm                                             [ Not found ]
    Sneakin Rootkit                                          [ Not found ]
    'Spanish' Rootkit                                        [ Not found ]
    Suckit Rootkit                                           [ Not found ]
    Superkit Rootkit                                         [ Not found ]
    TBD (Telnet BackDoor)                                    [ Not found ]
    TeLeKiT Rootkit                                          [ Not found ]
    T0rn Rootkit                                             [ Not found ]
    trNkit Rootkit                                           [ Not found ]
    Trojanit Kit                                             [ Not found ]
    Tuxtendo Rootkit                                         [ Not found ]
    URK Rootkit                                              [ Not found ]
    Vampire Rootkit                                          [ Not found ]
    VcKit Rootkit                                            [ Not found ]
    Volc Rootkit                                             [ Not found ]
    Xzibit Rootkit                                           [ Not found ]
    zaRwT.KiT Rootkit                                        [ Not found ]
    ZK Rootkit                                               [ Not found ]

[Press <ENTER> to continue]


  Performing additional rootkit checks
    Suckit Rootkit additional checks                         [ OK ]
    Checking for possible rootkit files and directories      [ None found ]
    Checking for possible rootkit strings                    [ None found ]

  Performing malware checks
    Checking running processes for deleted files             [ Warning ]
    Checking running processes for suspicious files          [ None found ]
```

```
    Checking for hidden processes                              [ None found ]
    Checking for files with suspicious contents                [ None found ]
    Checking for login backdoors                               [ None found ]
    Checking for sniffer log files                             [ None found ]
    Checking for suspicious directories                        [ None found ]
    Checking for suspicious (large) shared memory segments     [ Warning ]
    Checking for Apache backdoor                               [ Not found ]

  Performing Linux specific checks
    Checking loaded kernel modules                             [ OK ]
    Checking kernel module names                               [ OK ]

[Press <ENTER> to continue]


Checking the network...

  Performing checks on the network ports
    Checking for backdoor ports                                [ None found ]
    Checking for hidden ports                                  [ None found ]

  Performing checks on the network interfaces
    Checking for promiscuous interfaces                        [ None found ]
    Checking for packet capturing applications                 [ Warning ]

Checking the local host...

  Performing system boot checks
    Checking for local host name                               [ Found ]
    Checking for system startup files                          [ Found ]
    Checking system startup files for malware                  [ None found ]

  Performing group and account checks
    Checking for passwd file                                   [ Found ]
    Checking for root equivalent (UID 0) accounts              [ None found ]
    Checking for passwordless accounts                         [ None found ]
    Checking for passwd file changes                           [ None found ]
    Checking for group file changes                            [ None found ]
    Checking root account shell history files                  [ None found ]

  Performing system configuration file checks
    Checking for an SSH configuration file                     [ Found ]
    Checking if SSH root access is allowed                     [ Warning ]
    Checking if SSH protocol v1 is allowed                     [ Not set ]
    Checking for other suspicious configuration settings       [ None found ]
    Checking for a running system logging daemon               [ Found ]
    Checking for a system logging configuration file           [ Found ]
    Checking if syslog remote logging is allowed               [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                    [ None found ]
```

```
    Checking for hidden files and directories                [ Warning ]

[Press <ENTER> to continue]


Checking application versions...

    Checking version of Exim MTA                             [ OK ]
    Checking version of GnuPG                                [ OK ]
    Checking version of OpenSSL                              [ OK ]
    Checking version of PHP                                  [ OK ]
    Checking version of OpenSSH                              [ OK ]


System checks summary
=====================

File properties checks...
    Files checked: 146
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 500
    Possible rootkits: 3

Applications checks...
    Applications checked: 5
    Suspect applications: 0

The system checks took: 3 minutes and 6 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Finally, trying to update `rkhunter`.

```
┌──(root㉿kali-linux-vagrant)-[~]
└─# rkhunter --update
Invalid WEB_CMD configuration option: Relative pathname: "/bin/false"
```

Googling for this error found:

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=893169

Stating:

"This is actually intended. The update mechanism is not secure and therefore is disabled in Debian.

See bug #893169 for the details.

Francois"

Which points to:

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=765895

Which from a security standpoint, this boils down to the author’s thought train:

"It seems to use wget/curl per default for downloading, which means at best, everything is SSL/TLS secured,… which basically means no security at all. wget/curl, both use per default still SSLv3 (which is broken since POODLE, latestly)… and even worse,… any CA which is activated in the system, which is per default a big list, including such untrustworthy fellows as CNNIC) could forge certificates for the source-forge mirrors and potentially deliver our users forged files (if MitM attacks are possible as well)."

Chapter 4. Conclusion

Both tools: `chkrootkit` and `rkhunter` have their place for searching for rootkits on a local system. The author of this paper has seen one rootkit that infected the BiOS of a computer. He would have never known it was in place unless the Developer of said rootkit had not mispelled the name of the BiOS's vendor. Both of these tools should be leveraged with a shell script that runs both tools sequentially, and then outputs to an external logging system, such as email, for analysis, compliance, and log retention.

Happy hunting!

Chapter 5. Appendix

References

https://www.kali.org/tools/chkrootkit/

http://www.chkrootkit.org/

https://www.kali.org/tools/rkhunter/

https://rkhunter.sourceforge.net/

https://en.wikipedia.org/wiki/Rootkit

rkhunter source code: https://salsa.debian.org/pkg-security-team/rkhunter

chkrootkit source code: ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz

Kali Credentials

https://www.kali.org/docs/introduction/default-credentials/