



UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

Kali Setup + Command Injection

Downloading kali

Get Kali | Kali Linux

https://www.kali.org/get-kali/#kali-virtual-machines

Bare Metal VMs ARM Mobile Cloud Containers Live Box


Virtual Machines

Kali Linux **VMware** & **VirtualBox** images are available for users who prefer, or whose specific needs require a virtual machine installation.

These images have the **default credentials "kali/kali"**.


[Virtual Machines Documentation >](#)

64-bit 32-bit



64
VMware

↓ 2.7G torrent sum




64
VirtualBox

↓ 4.0G torrent sum

qBittorrent Official Website x Transmission

https://www.qbittorrent.org/download.php

Latest: v4.3.8



qBittorrent

Free and reliable P2P BitTorrent client

Home News Forum Download Screenshots Wiki Development Bugs

qBittorrent Official Website x Transmission

https://transmissionbt.com/download/

TRANSMISSION

A Fast, Easy, and Free BitTorrent Client

MAIN ABOUT DOWNLOAD DEVELOPMENT ADD-ONS SUPPORT IRC

Download Transmission

The current release version is 3.00

Mac OS X
Transmission-3.00.dmg
Requires Mac OS X 10.10 or later
Nightly builds
Previous Releases

Source Code
transmission-3.00.tar.xz
Nightly tarballs
Previous tarballs
How to build

Windows (early preview)
transmission-3.00-x86.msi
transmission-3.00-x64.msi
Requires Windows 7 or later
Nightly builds



Why kali?

- Kali is a linux distribution designed to be used by cyber security professionals, as such it has a lot of the tools we will use pre-installed. This means you likely will not have to install any additional software for most of our CTF challenges.
- Alternatives: ParrotSEC, black arch



Why VM?

- Allows you to run OS without removing your current OS
- Separate's files used for hacking in VM from cluttering your hard-drive



Installing Virtualbox

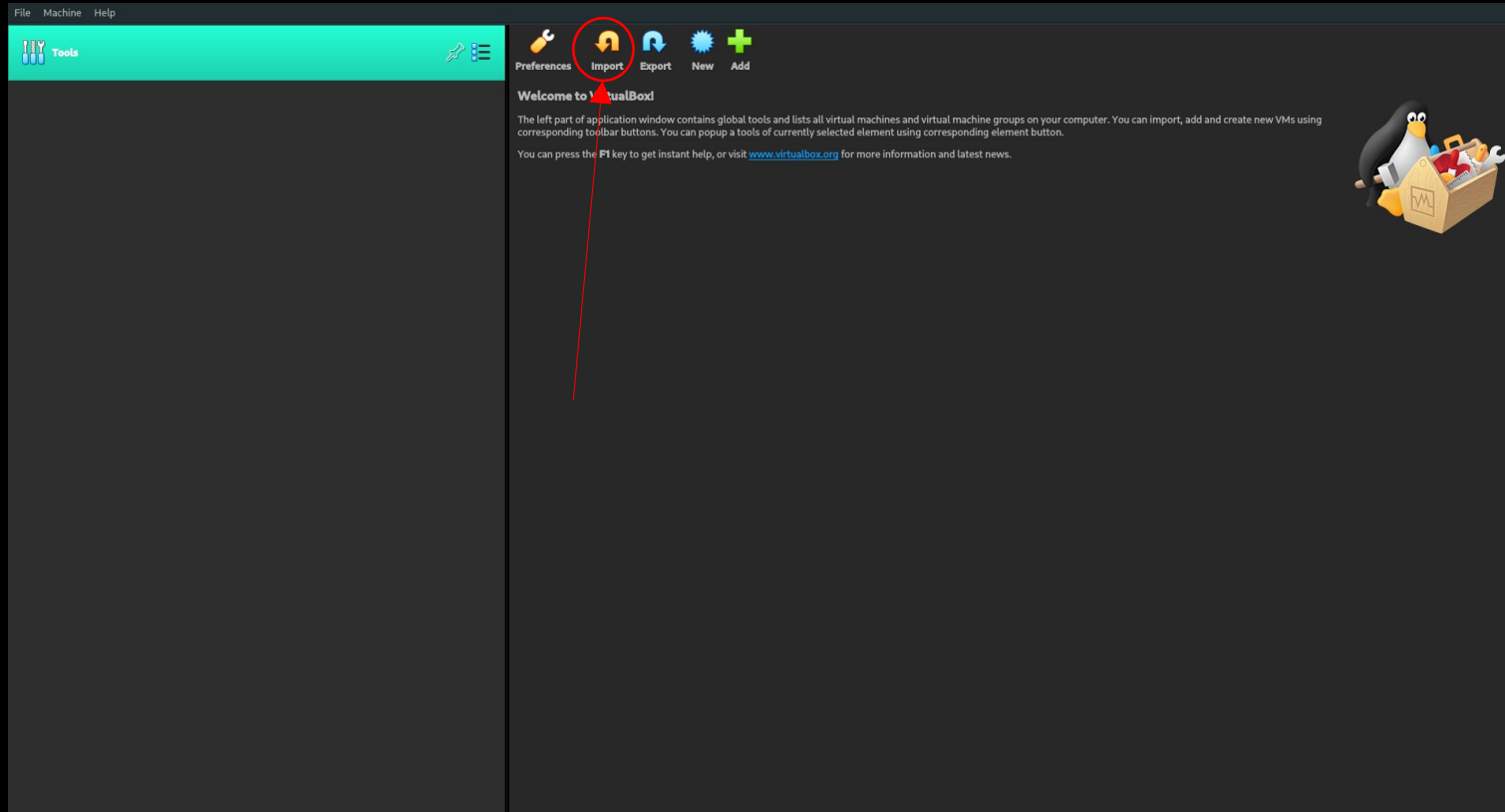
```
crewmate@amogos: ~  
File Actions Edit View Help  
└─(crewmate@ amogos) -[~]  
└─$ sudo apt-get install virtualbox  
[sudo] password for crewmate:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
virtualbox is already the newest version (6.1.26-dfsg-4).  
virtualbox set to manually installed.  
The following packages were automatically installed and are no longer required:  
bridge-utils cloud-image-utils cryptsetup-run distro-info exfat-fuse fakechroot genisoimage  
gstreamer1.0-pulseaudio libboost-log1.74.0 libboost-program-options1.74.0 libdistro-info-perl  
libepsilon1 libfakechroot libgdal28 libgeos-3.9.0 libgles2 libgsoap-2.8.104 libidn11 libiscsi7  
liblxc1 libntfs-3g883 libpam-cgfs librbd1 librest-0.7-0 libsdm-c++0 libSDL2-image-2.0-0 libyara4  
lxc lxc-templates lxcfs mmdebstrap python3-gevent python3-gevent-websocket python3-ipython-genutils  
python3-jupyter-core python3-m2crypto python3-nbformat python3-parameterized python3-plotly  
python3-zope.event qemu-block-extra qemu-utils tcpd uidmap  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 62 not upgraded.
```

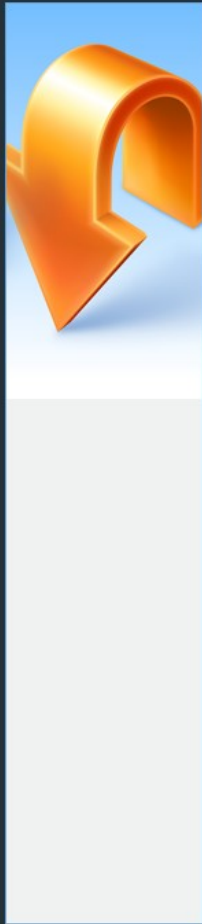


The screenshot shows the VirtualBox website's download page. The page title is "Download VirtualBox". It contains a sidebar with navigation links: About, Screenshots, Downloads, Documentation (with sub-links for End-user docs and Technical docs), Contribute, and Community. The main content area has a search bar and a "Login Preferences" link. The "Download VirtualBox" section includes a paragraph about finding links to binaries and source code, followed by "VirtualBox binaries" and "VirtualBox 6.1.26 platform packages" sections. The "VirtualBox 6.1.26 platform packages" section has a red circle around a list of operating systems: Windows hosts, OS X hosts, Linux distributions, Solaris hosts, and Solaris 11 IPS hosts. A red arrow points from this list to the right. Below this, there are sections for "VirtualBox 6.1.26 Oracle VM VirtualBox Extension Pack" with a red circle around "All supported platforms", and a note about SHA256 and MD5 checksums.



Adding kali to virtual box





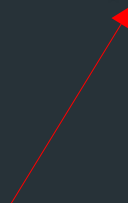
Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File: </home/tom/Downloads/os-isos/kali-linux-2021-3-vbox-amd64-ova/kali-linux-2021.3-vbox-amd64.ova>



Expert Mode

< Back

Next >

Cancel





Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1

Name	Kali-Linux-2021.3-vbox-amd64
Product	Kali Linux
Product-URL	https://www.kali.org/
Vendor	Offensive Security
Vendor-URL	https://www.offensive-security.com/
Version	Rolling (2021.3) x64
Description	Kali Rolling (2021.3) x64...
Guest OS Type	Debian (64-bit)
CPU	2
RAM	2048 MB
DVD	<input checked="" type="checkbox"/>
USB Controller	<input checked="" type="checkbox"/>
Sound Card	<input checked="" type="checkbox"/> ICH AC97
Network Adapter	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SATA)	AHCI
Virtual Disk Image	Kali-Linux-2021.3-vbox-amd64-disk001.vmdk

Machine Base Folder:

MAC Address Policy:

Additional Options: Import hard drives as VDI

Appliance is not signed

Restore Defaults

< Back

Import

Cancel



The virtual system "Kali-Linux-2021.3-vbox-amd64" requires that you agree to the terms and conditions of the software license agreement shown below.

Click **Agree** to continue or click **Disagree** to cancel the import.

GPL v3 ~ <https://www.kali.org/docs/policy/kali-linux-open-source-policy/>

Agree

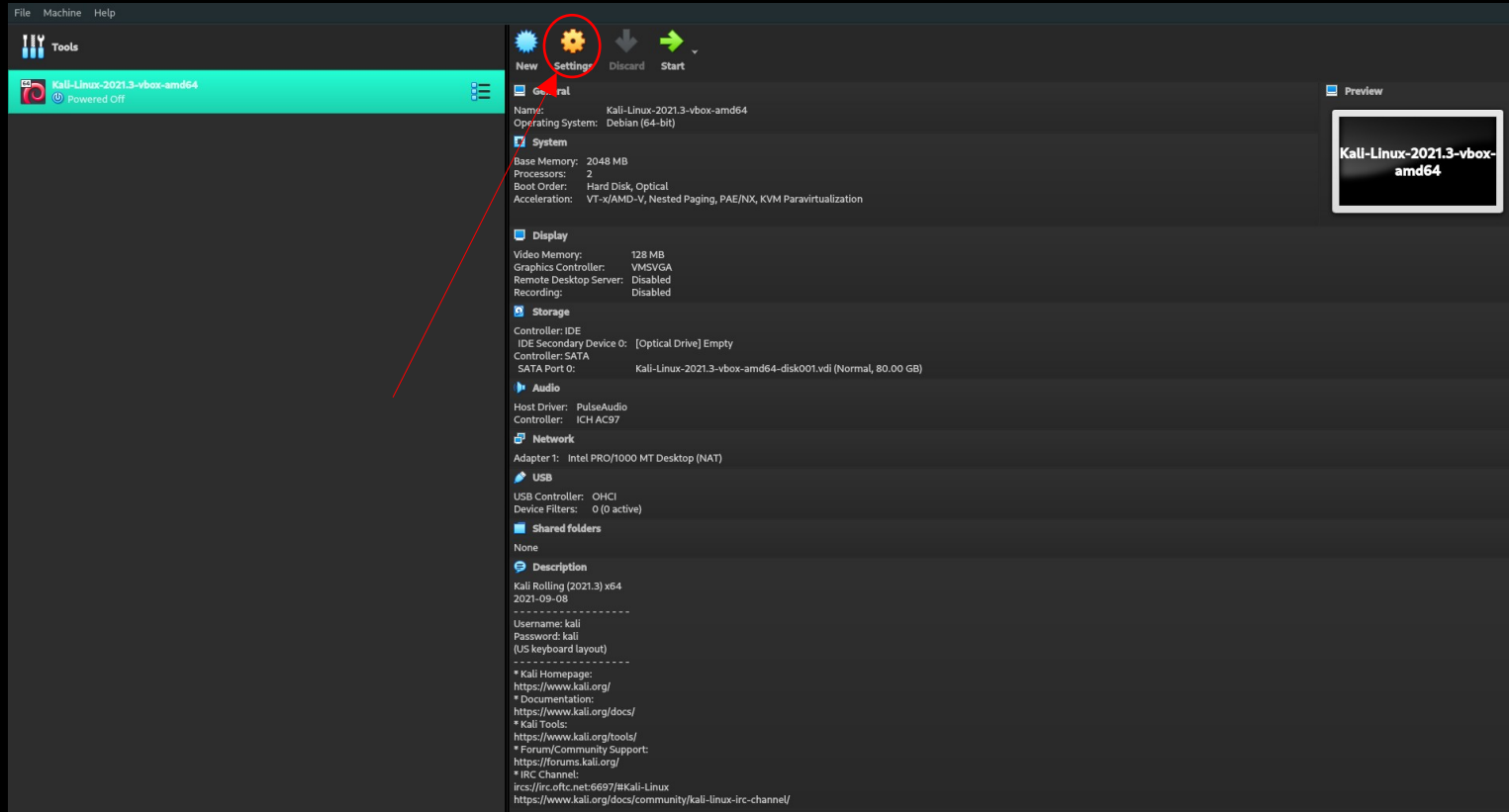
Disagree

Print...

Save...



Managing your VirtualMachine



The image shows a screenshot of the System Configuration utility, specifically the Motherboard tab. The interface is dark-themed with a sidebar on the left containing various system settings categories. The main area displays configuration options for the motherboard, including memory settings, boot order, chipset, pointing device, and extended features. The Base Memory is set to 4096 MB, and the boot order is configured as Hard Disk, Optical, Floppy, and Network. The chipset is PIIX3, and the pointing device is a USB Tablet. Extended features include Enable I/O APIC, Enable EFI (special OSes only), and Hardware Clock in UTC Time.

System Configuration

System

Motherboard | Processor | Acceleration

Base Memory: 4096 MB (4 MB to 8192 MB)

Boot Order:

- Hard Disk
- Optical
- Floppy
- Network

Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features:

- Enable I/O APIC
- Enable EFI (special OSes only)
- Hardware Clock in UTC Time

OK Cancel



The screenshot shows the 'System' settings window for a virtual machine, specifically the 'Processor' tab. The left sidebar lists various system components: General, System (selected), Display, Storage, Audio, Network, Serial Ports, USB, Shared Folders, and User Interface. The main area is divided into three sub-tabs: 'Motherboard', 'Processor' (selected), and 'Acceleration'. Under the 'Processor' tab, there are two sliders: 'Processor(s)' is set to 2 (range 1 CPU to 8 CPUs) and 'Execution Cap' is set to 100% (range 1% to 100%). Below the sliders, the 'Extended Features' section includes a checked checkbox for 'Enable PAE/NX' and an unchecked checkbox for 'Enable Nested VT-x/AMD-V'. At the bottom right, there are 'OK' and 'Cancel' buttons.

General

System

Display

Storage

Audio

Network

Serial Ports

USB

Shared Folders

User Interface

Motherboard Processor Acceleration

Processor(s): 2 - +
1 CPU 8 CPUs

Execution Cap: 100% - +
1% 100%

Extended Features: Enable PAE/NX
 Enable Nested VT-x/AMD-V

OK Cancel



Command Injection



But first some basic linux stuff

```
pi@worst-server-eu:~ $
pi@worst-server-eu:~ $ pwd
/home/pi
pi@worst-server-eu:~ $ ls -la
total 116
drwxr-xr-x  8 pi  pi   4096 Oct  4 17:17 .
drwxr-xr-x  4 root root 4096 Jul 22 17:40 ..
-rw-----  1 pi  pi  16521 Oct  4 23:04 .bash_history
-rw-r--r--  1 pi  pi   220 May  7 15:42 .bash_logout
-rw-r--r--  1 pi  pi  3523 May  7 15:42 .bashrc
drwxr-xr-x  3 pi  pi   4096 Jul 23 01:55 .cache
drwx-----  4 pi  pi   4096 Oct  4 16:46 .config
drwx-----  3 pi  pi   4096 Jul 22 16:39 .gnupg
-rw-----  1 pi  pi    72 Jul 30 22:03 .lessht
-rw-r--r--  1 pi  pi   807 May  7 15:42 .profile
drwxr-xr-x  2 pi  pi   4096 Oct  4 16:37 .ssh
-rw-----  1 pi  pi  9727 Oct  4 17:17 .viminfo
drwxr-xr-x 12 pi  pi   4096 Oct  4 17:18 Cuberite
-rw-r--r--  1 pi  pi   692 Oct  3 21:37 README.txt
-rw-r--r--  1 pi  pi  2233 Oct  3 21:37 favicon.png
-rw-r--r--  1 pi  pi  14750 Jul 30 23:27 get-docker.sh
-rw-r--r--  1 pi  pi  11652 Jul 30 23:18 seccomp_2.5.1-1_armhf.deb
drwxr-xr-x  3 pi  pi   4096 Oct  3 21:37 webadmin
pi@worst-server-eu:~ $ cd .ssh
pi@worst-server-eu:~/.ssh $ pwd
/home/pi/.ssh
pi@worst-server-eu:~/.ssh $
```



```
pi@worst-server-eu:/tmp/tmp.UhPBTgYLv4 $ ls
test.txt
pi@worst-server-eu:/tmp/tmp.UhPBTgYLv4 $ cat test.txt
This is an example file
pi@worst-server-eu:/tmp/tmp.UhPBTgYLv4 $ cd ..
pi@worst-server-eu:/tmp $ cd /home/pi
pi@worst-server-eu:~ $ pwd
/home/pi
pi@worst-server-eu:~ $ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),105(input),109(netdev),997(gpio),998(i2c),999(spi)
pi@worst-server-eu:~ $ whoami
pi
pi@worst-server-eu:~ $ █
```

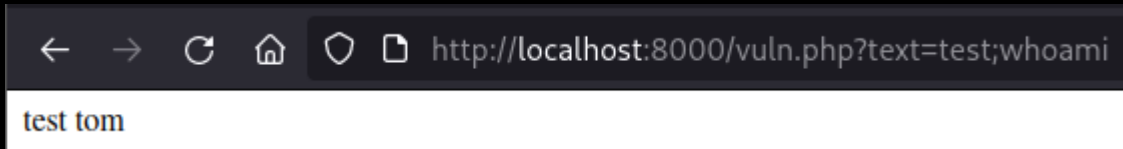
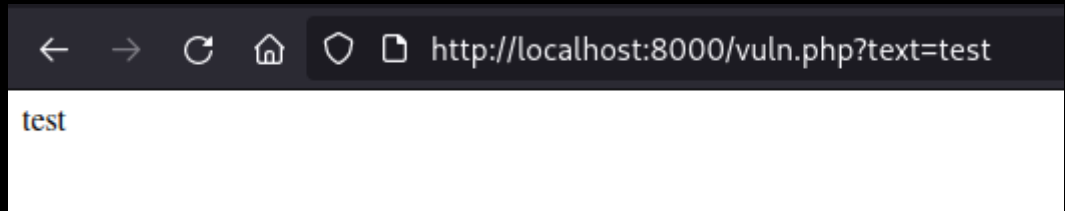


Command injection

- Command injection is when you exploit a website or service to run system level commands.
- The most basic form of this is when user input is passed directly to a command as an argument.




```
1 <?php
2 echo shell_exec("echo " . $_GET["text"]);
3 ?>
```



Command separators

<code>command1;command2</code>	Runs command1 then command2
<code>command1 && command2</code>	Runs command1 then command2 if command1 didn't error
<code>comamnd1 command2</code>	Runs command1 then command2 if command1 did error

Arguments don't matter

```
> echo foo bar baz; pwd && cd /  
foo bar baz  
/home/tom
```



Filtering

- When blocking command injection user input may be filtered.
- Regularly blocked characters include:
; & | ` \$
- Only way to get around this is keep trying a different method if you get blocked



Command substitution

- You can use `$(command)` or ``command`` to insert the output of the command as an argument to another.
- This is useful where other methods are filtered or you are in an escaped string.



```
1 <?php
2 echo shell_exec("echo \"\" . addslashes($_GET["text"]) . "\"");
3 ?>
```

← → ↻ 🏠 🛡️ 📄 http://localhost:8000/vuln2.php?text=test

test

← → ↻ 🏠 🛡️ 📄 http://localhost:8000/vuln2.php?text=test;whoami

test;whoami

← → ↻ 🏠 🛡️ 📄 http://localhost:8000/vuln2.php?text=\$(whoami)

tom



Blind

- For blind injection you cannot see the output of the command you run.
- You may still be able to see whether command succeeded: this can tell you if your injection is working.
- You will need to find another way to exfil data though. Reverse shells are especially useful when doing blind attacks.



Connecting to the vpn

`ctf.cybersoc.cf`

```
sudo apt-get update
```

```
sudo apt-get install -y openvpn
```

```
sudo openvpn ~/Downloads/cybersoc.ovpn
```

