Virtualization Notes (For Metasploitable and Kali)

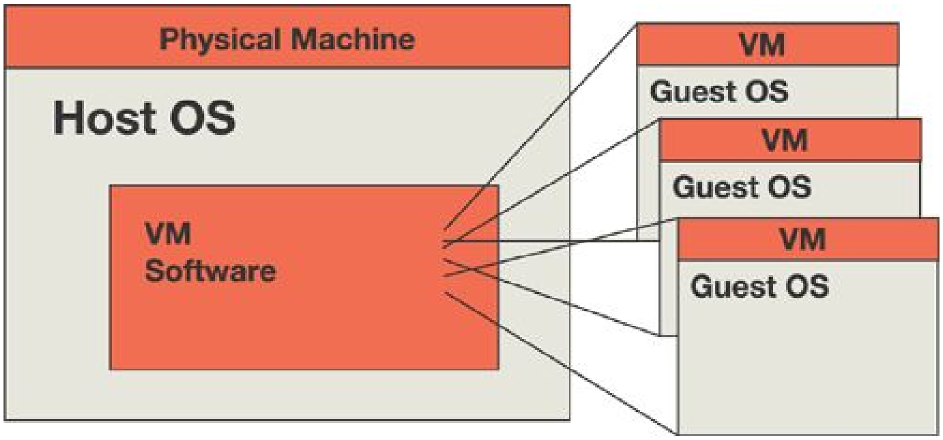


Figure 1: Relationship of VM software and host and guest OSs

Desktop Virtualization Platforms (VM Software)

1. KVM/libvirt - Kernel modules for linux to execute a guest OS directly on the host CPU (uses faster VTX)
2. QEMU/libvirt - Userland application to execute a guest OS on a virtual CPU (full CPU emulation, slower)
3. Oracle Virtualbox - Supports both VTX and userland virtualization
4. Vmware player - Supports VTX and Binary translation (both of which are faster than full emulation)

Virtual Hard Drive Formats

Note: There are tools available to convert between these file formats

raw
(default) the raw format is a plain binary image of the disc image, and is very portable. On filesystems that support sparse files, images in this format only use the space actually used by the data recorded in them.
cloop
Compressed Loop format, mainly used for reading Knoppix and similar live CD image formats
cow
copy-on-write format, supported for historical reasons
qcow
copy-on-write format, supported for historical reasons and superseded by qcow2
qcow2

copy-on-write format with a range of special features, including the ability to take multiple snapshots, smaller images on filesystems that don't support sparse files, optional AES encryption, and optional zlib compression

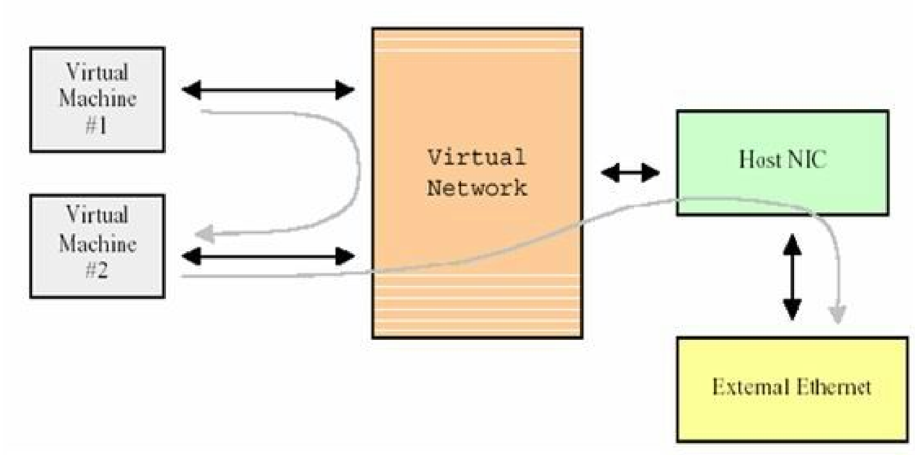
vmdk

VMware 3 & 4, or 6 image format, for exchanging images with that product

vdi

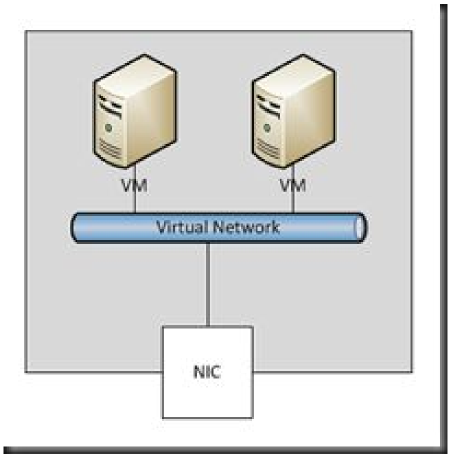
VirtualBox 1.1 compatible image format, for exchanging images with VirtualBox.

Virtual Network Topology

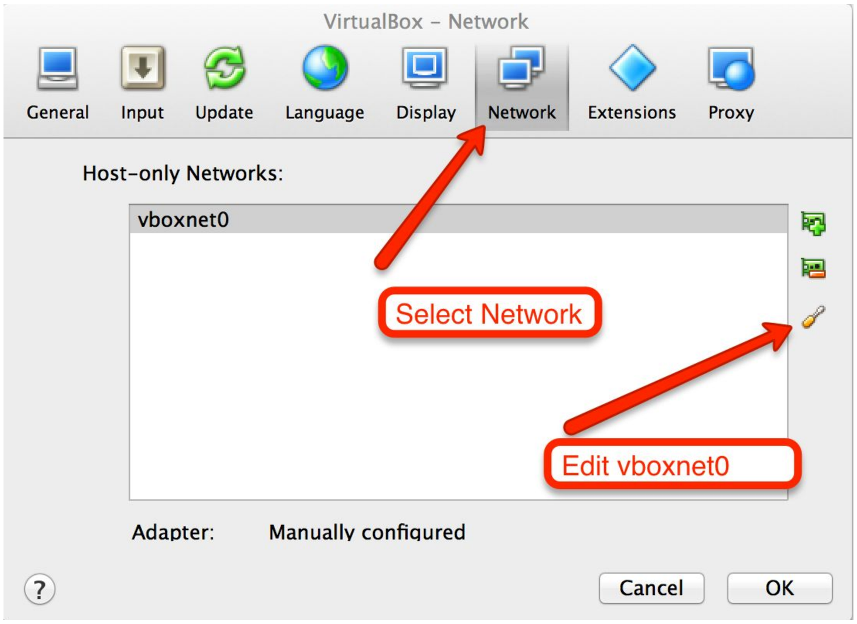


Virtual machine managers supports various virtual network configurations for the guest machines. The names of each network configuration can vary between virtual machine managers but typical examples would include:

- Bridged Networking (a single guest takes over host NIC exclusively)
- NAT Networking (guests share virtual router, both guests and host have internet access)
- Host-Only Networking (guests can only connect to host)
- Internal networking (guests share a virtual switch and can interact on a virtual LAN, no access to host or internet)
- Custom Networking Configurations



In VirtualBox create a LAN in the global configuration



Host-only Networks:

vboxnet0

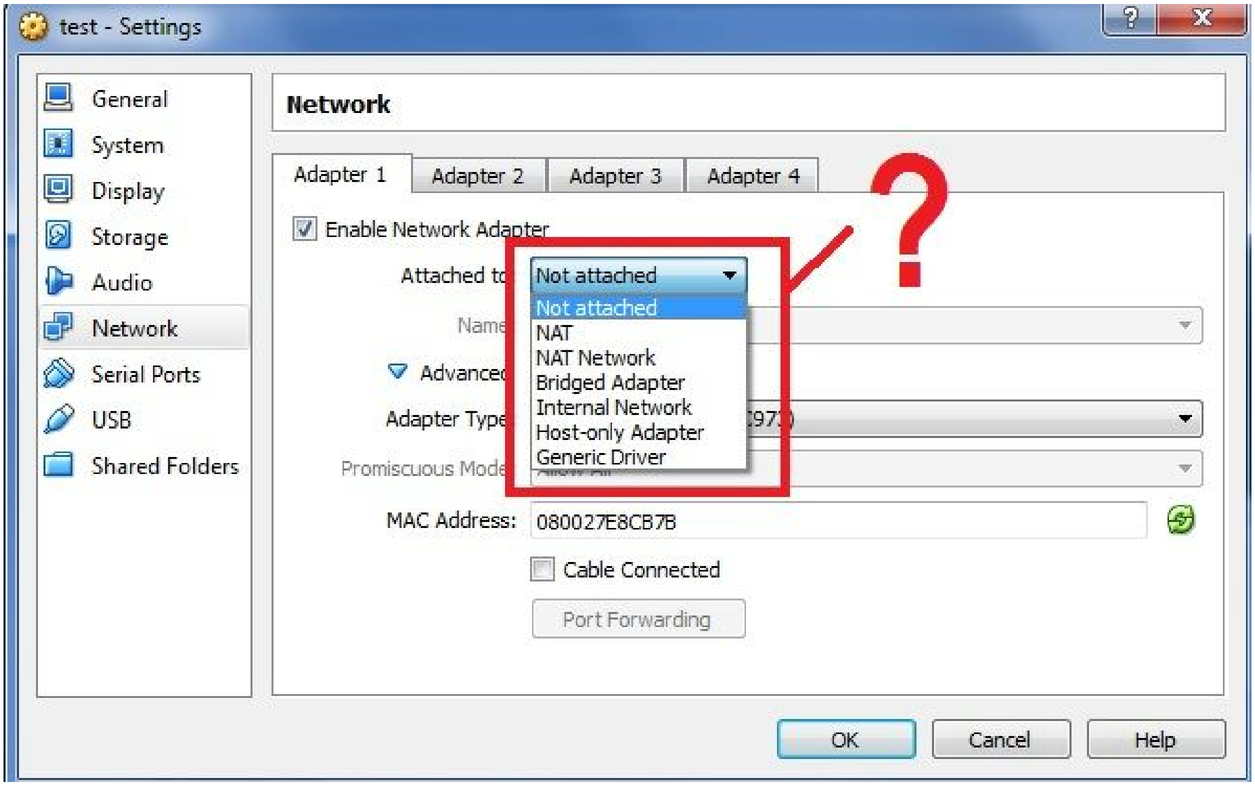
Adapter: Manually configured

Select Network

Edit vboxnet0

Then for each machine add 3 network adapters:

1. Your new "host-only" network adapter (lan) for communication between VMs and the host
2. A "NAT" network adapter for internet access
3. An "Internal" network adapter for access between the guests



test - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Not attached

MAC Address: 080027E8CB7B

□ Cable Connected

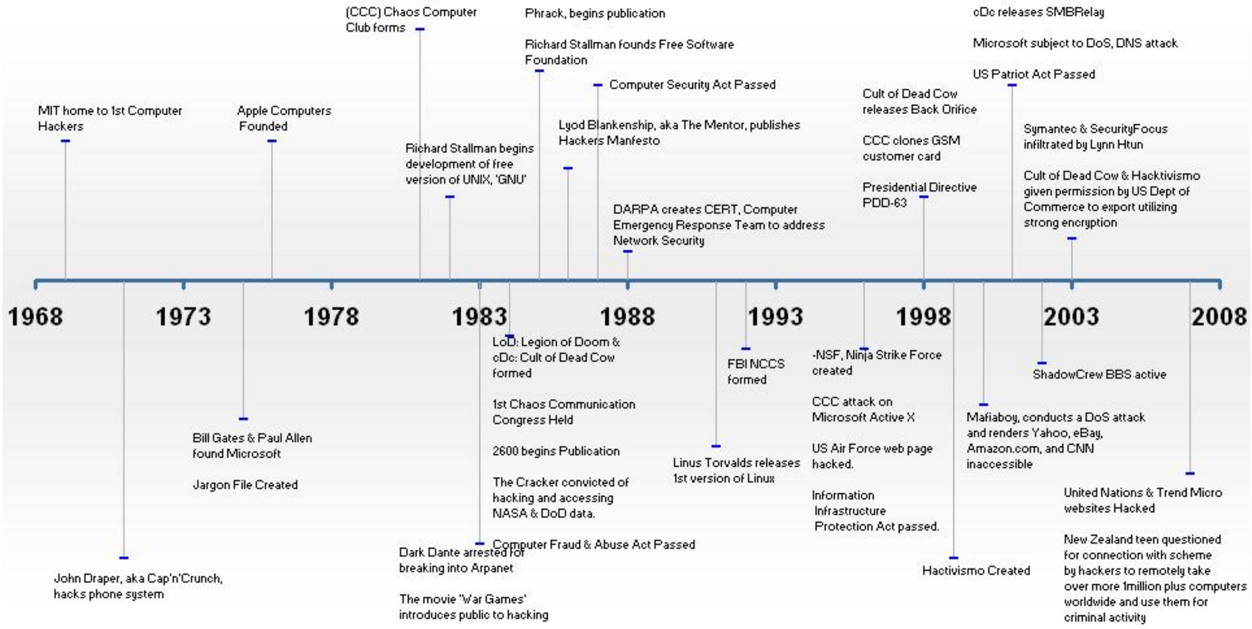
----

nmap, nessus, metasploit - https://www.youtube.com/watch?v=CMfO3g8eP-k

----

Hacking History

Search term: hackers timeline
Search term: exploit timeline:
Search term: cwe timeline
Search term: vulnerability timeline


MIT home to 1st Computer Hackers
Apple Computers Founded
(CCC) Chaos Computer Club forms
Richard Stallman begins development of free version of UNIX, 'GNU'
Phrack, begins publication
Richard Stallman founds Free Software Foundation
Computer Security Act Passed
Lyod Blankenship, aka The Mentor, publishes Hackers Manfesto
DARPA creates CERT, Computer Emergency Response Team to address Network Security
Cult of Dead Cow releases Back Orifice
CCC clones GSM customer card
Presidential Directive PDD-63
cDc releases SMBRelay
Microsoft subject to DoS, DNS attack
US Patriot Act Passed
Symantec & SecurityFocus infiltrated by Lynn Htun
Cult of Dead Cow & Hacktivismo given permission by US Dept of Commerce to export utilizing strong encryption
1968
1973
1978
1983
1988
1993
1998
2003
2008
John Draper, aka Cap'n'Crunch, hacks phone system
Bill Gates & Paul Allen found Microsoft
Jargon File Created
Dark Dante arrested for breaking into Arpanet
The movie 'War Games' introduces public to hacking
LoD: Legion of Doom & cDc: Cult of Dead Cow formed
1st Chaos Communication Congress Held
2600 begins Publication
The Cracker convicted of hacking and accessing NASA & DoD data.
Computer Fraud & Abuse Act Passed
Linus Torvalds releases 1st version of Linux
FBI NCCS formed
-NSF, Ninja Strike Force created
CCC attack on Microsoft Active X
US Air Force web page hacked.
Information Infrastructure Protection Act passed.
Hactivismo Created
Mafiaboy, conducts a DoS attack and renders Yahoo, eBay, Amazon.com, and CNN inaccessible
ShadowCrew BBS active
United Nations & Trend Micro websites Hacked
New Zealand teen questioned for connection with scheme by hackers to remotely take over more 1million plus computers worldwide and use them for criminal activity

http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
http://www.phrack.com/
http://www.phrack.com/issues/1/1.html