EGI Community Forum 2014

Software Vulnerability Handling and practical incident recognition

Idea: Sven Gabriel (NIKHEF)
All the hard work: Heiko Reese (KIT-CERT)

Sven Gabriel?

- 2004–2007: FZK Karlsruhe, T-1 GridKa Site Admin (FZK/KIT)
- 2007–: Nikhef Amsterdam, Security Officer Nikhef/NGI-NL/EGI
- Working on Security Monitoring, Global Security Drills, Trainings, Incident Response

Heiko Reese?

- Member of KIT-CERT for ~5 years
    - KIT == former University of Karlsruhe + former Forschungszentrum Karlsruhe (GridKa might ring a bell in this context)
    - CERT == Computer Incident Response Team
- KIT-CERT provides a broad range of security services to its constituency: forensics, monitoring, training, incident response, policies, etc…
- Strong affinity to Unix-like operating systems

Today's Agenda:

1. Distribute VM image & additional files
2. Rules of the Game
3. A short introduction into forensics
4. Get everyone up and running
5. Go!

Get the Image!

Please get **challenge_final.ova** from:
https://www.cert.kit.edu/downloads/challenge-final.ova

Download working?!

Please ignore it until the end of my talk.

What’s the general idea here?

- Investigate virtual machine.
- Report your findings.
- Collaborate.
- Have fun!

Story time!

Some time ago, you and your friends rented a virtual server at the respectable cloud provider SpaceRack. Everybody was having a great time until the following e-mail arrived at your virtual doorsteps:

> *Dear Customer,*
>
> *your virtual machine #23421337 is consuming lots of cpu time. We're also seeing some suspicious network connections. Please take appropriate measures to ensure the safety of our infrastructre … blah … legal buzzword … fines … best wishes …*

Oh noez! You’ve been hacked!

- Quick! What's the first thing you need to do?
- Nothing!
- Take a deep breath. Grab something to drink (stay away from alcohol for now). Get a pen and paper. Find a tech-savvy person for an additional pair of eyes.

Decision point: involve the authorities?

- Legal route? Step away and call the police. You're done.
- Then let's „clean“ the machine and carry on.
- Or just reinstall everything into a clean state.

NO!

- There's no such thing as cleaning a compromised machine!
- Installing from scratch will just restore the initial vulnerable state.

Our only option: start collecting leads

Once we know how the attack occured, we can fix the problem in the next installation.

Task #1: Investigate

- Examine your machine (more on that in a few moments)
- (Briefly) document your findings.

Task #2: Report

Tell us what you find. Once you feel that you have a solid understanding on a piece of malware or a compromised part of the system, write us a short e-mail describing your findings.

Our address is cf2014@heiko-reese.de.

Task #3: Collaborate

Talking to other security people and sharing information is often crucial to successfully understanding security incidents. Plus, it's more fun that way.

Task #4: Enjoy it!

- Take a break when you're getting frustrated.
- The real thing is usually very stressful; we highly recommend that you do this excercise with a “let's play” mindset

Task #4.5: Capture the Flag

We hid a few flags in the machine for you to find. A flag is a SHA-512 hash; »you'll know it when you see it«.

If you find one, include it in your findings report.

```
Example: 7863e3e8c07bcb6837b576c994874e38879c77124c7e3e0991c957ce1bd5f53dcd24
afb8c48638dd2de6c251f15ba861abb1104d5286e7fcbe9d10cb3860e881.docx
```

Disclaimer

This talk focuses on the technical aspects of investigating a compromised machine. We're ignoring (even violating) best practices of proper incident handling to focus on the “fun parts”.

If you encounter a security incident in real life, please follow proper local procedures & policies.

EGI offers trainings focussing on proper incident handling. We only have 90 minutes today, so this is more of an appetizer :-)

Forensics: Order of Volatility

Evidence has different lifetimes:

Type	**Volatility**
Memory	nanoseconds
Network state	milliseconds
Processes	seconds
Disk	minutes

Try to follow the order of volatility when collecting evidence.

Where to start

There are two exceptions to the “follow the order of volatility”-rule:

1. Start with open network connections (`netstat`). Don't write to the disk, copy/paste from terminal.
2. Filesystem timestamp data is often the most important data and should be captured as early in the process as possible.

So make sure not to change data on disk while collecting evidence that's only available while the system is online (memory, network state, processes).

Start looking for »odd« things!

I'll share some slides from another talk about this to give you some ideas where to find evidence.

About the »malware« in your VM

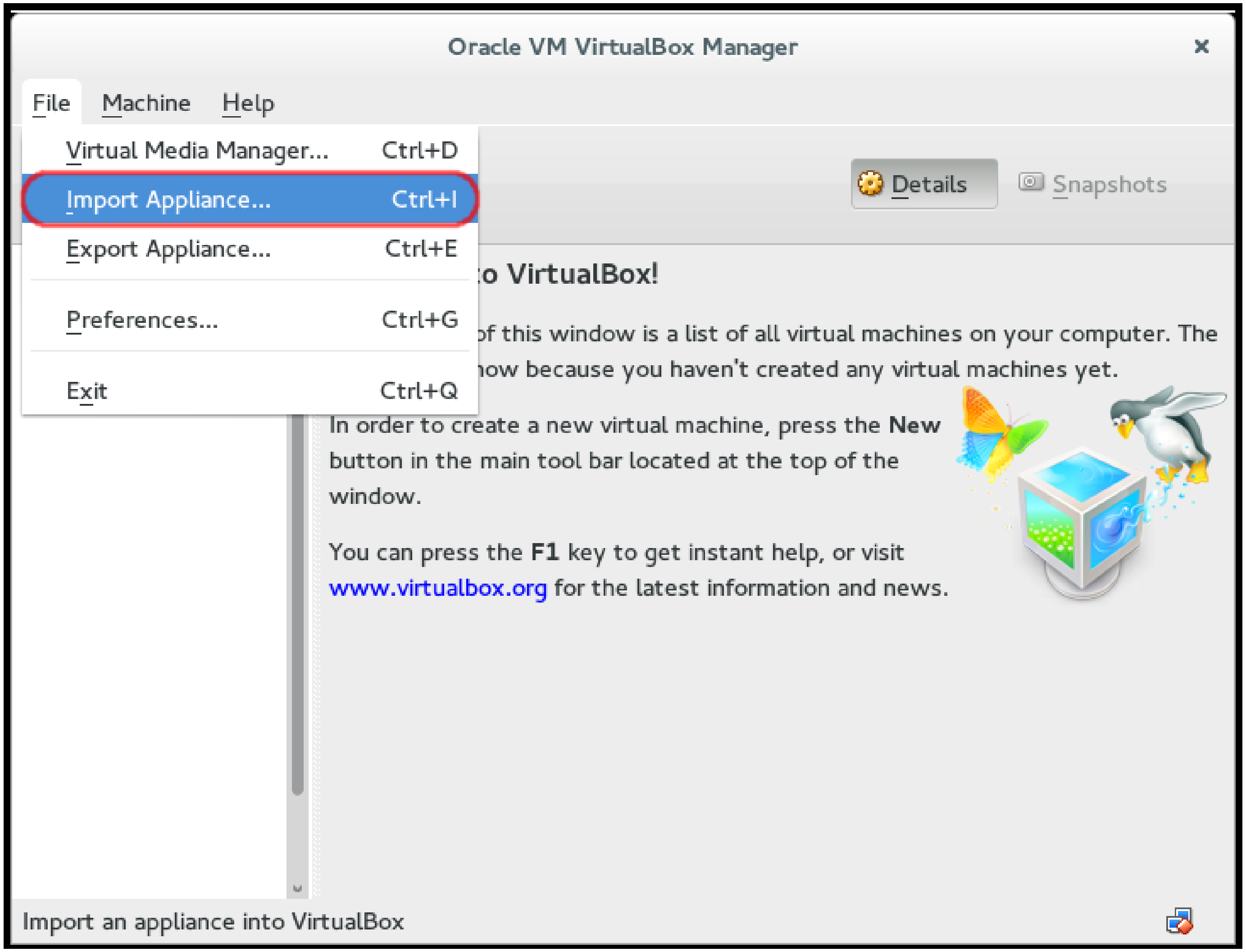
- Almost completly inspired by reality
- One piece of actual malware found a few weeks ago at KIT (it's pretty useful, please **don't** use it on your machines)
- VM should be safe™ to run on the local network.

TBD: Debriefing on Friday

Let’s get this thing running on your computer!

Anyone unhappy about Virtualbox?

We should be able to get this to run on VMWare or qemu/kvm.


Oracle VM VirtualBox Manager
File
Machine
Help
Virtual Media Manager... Ctrl+D
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Preferences... Ctrl+G
Exit Ctrl+Q
Details
Snapshots

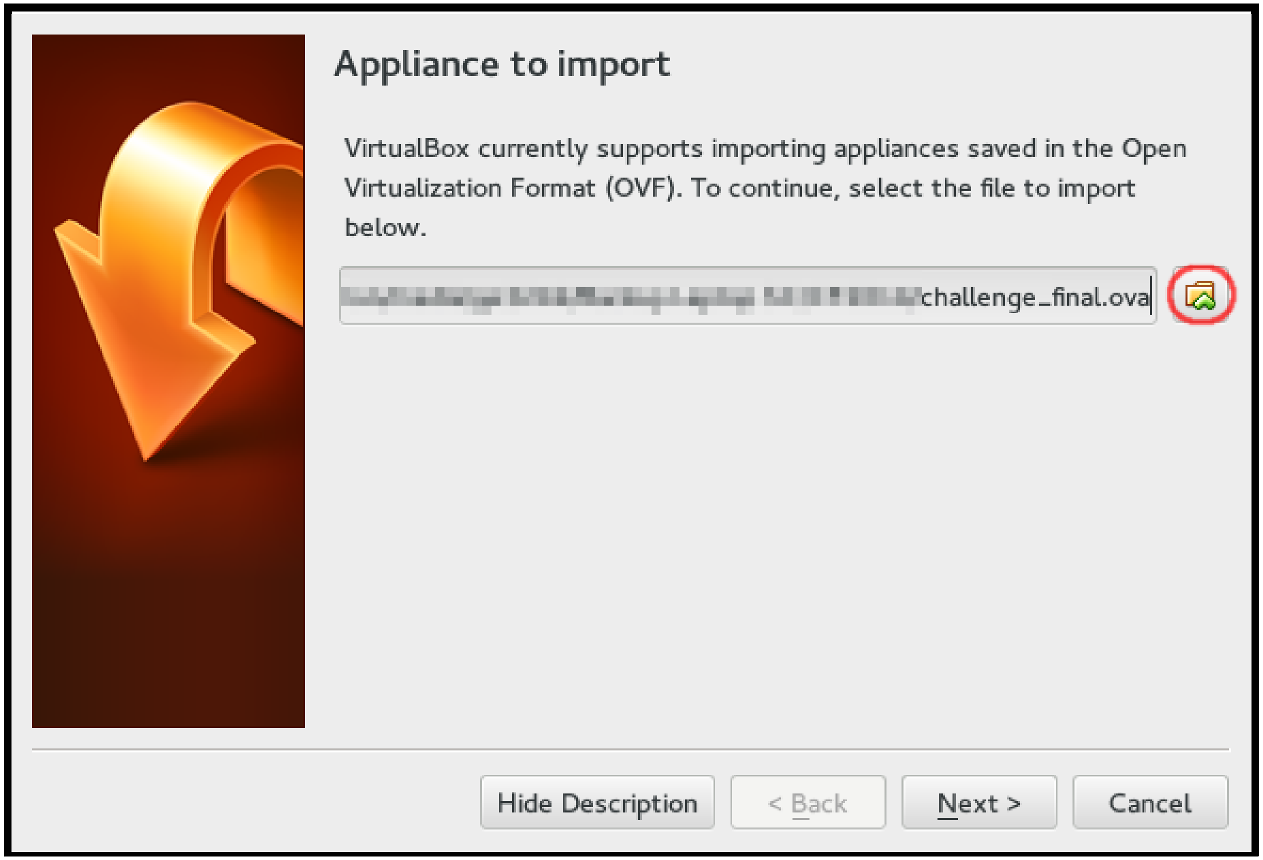
:o VirtualBox!

of this window is a list of all virtual machines on your computer. The
iow because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

Import an appliance into VirtualBox

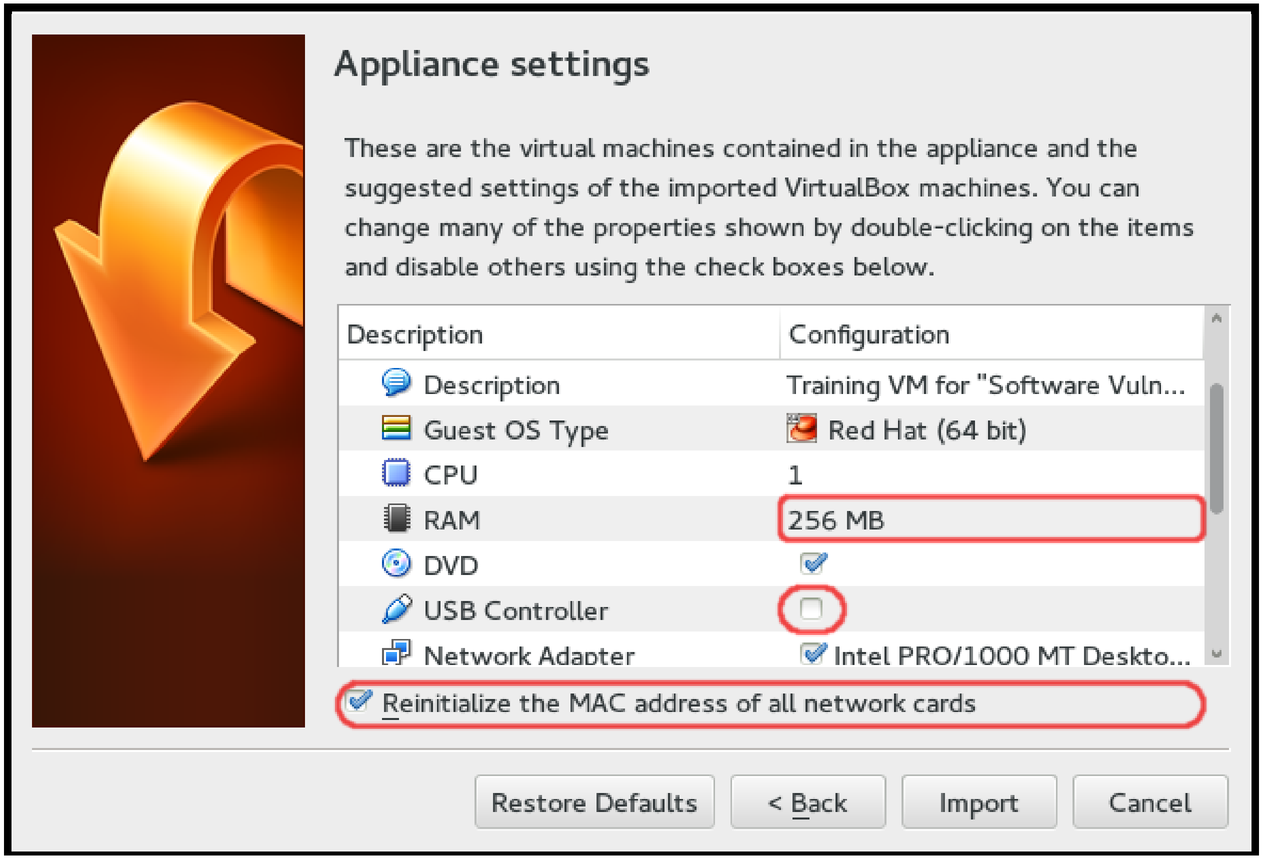


Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

[redacted]challenge_final.ova

Hide Description
< Back
Next >
Cancel



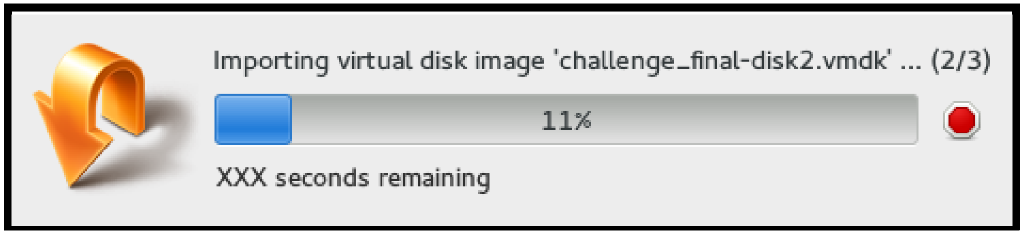
Appliance settings

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.

Description	Configuration
Description	Training VM for "Software Vuln...
Guest OS Type	Red Hat (64 bit)
CPU	1
RAM	256 MB
DVD	☑
USB Controller	☐
Network Adapter	☑ Intel PRO/1000 MT Deskto...

☑ Reinitialize the MAC address of all network cards

Decrease RAM (256–512M), remove USB Controller, reinitialize MAC address.



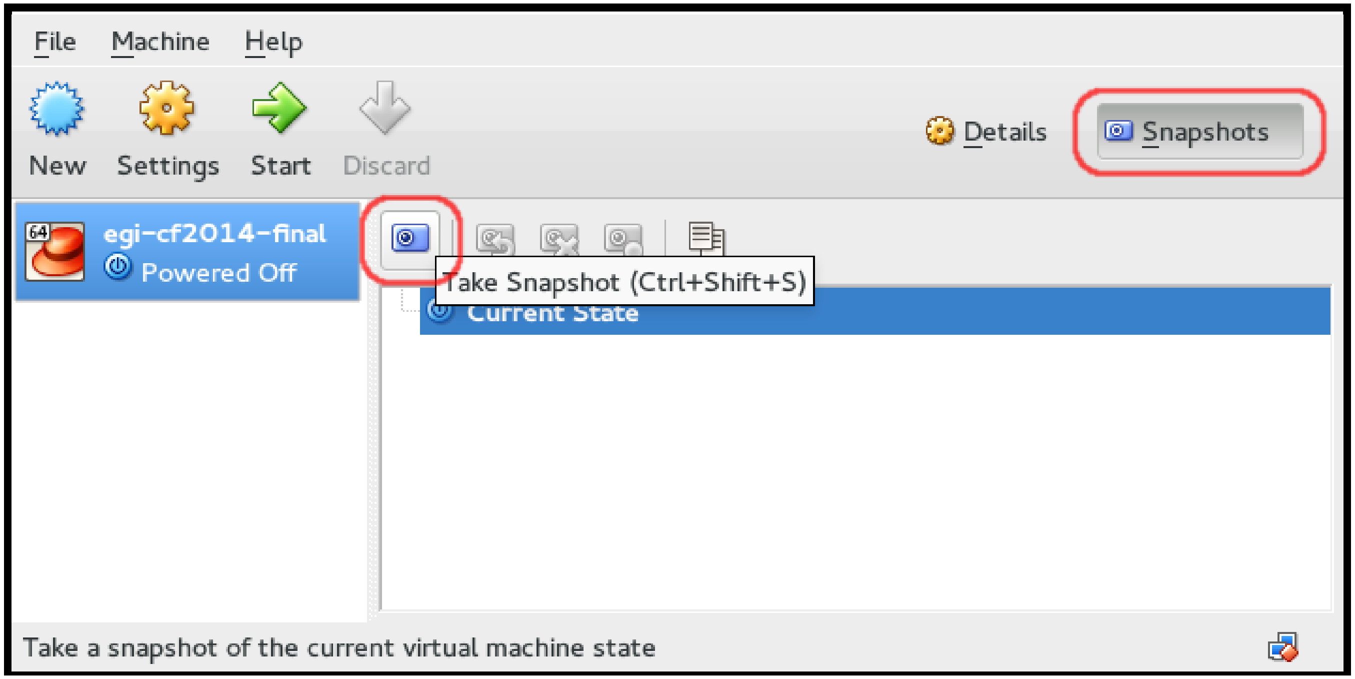
Importing virtual disk image 'challenge_final-disk2.vmdk' ... (2/3)

11%

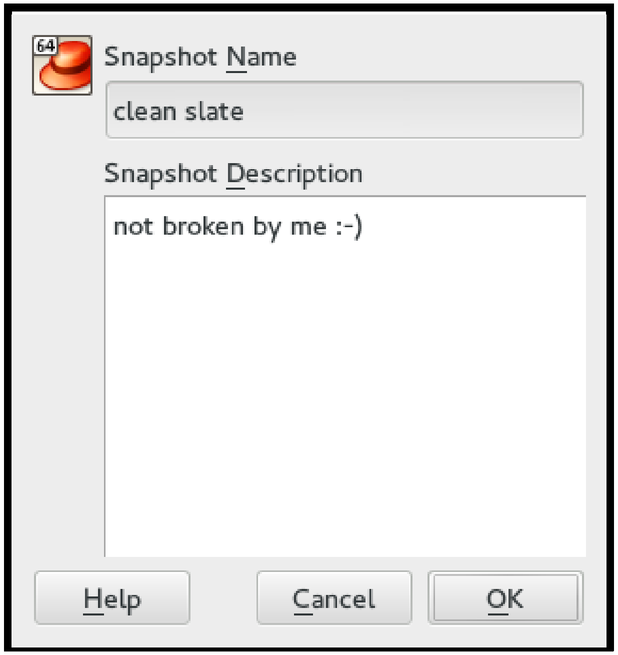
XXX seconds remaining

Wait. Don't start when finished!

First thing to do: create a snapshot!


File
Machine
Help
New
Settings
Start
Discard
Details
Snapshots
egi-cf2014-final
Powered Off
Take Snapshot (Ctrl+Shift+S)
Current State

Take a snapshot of the current virtual machine state



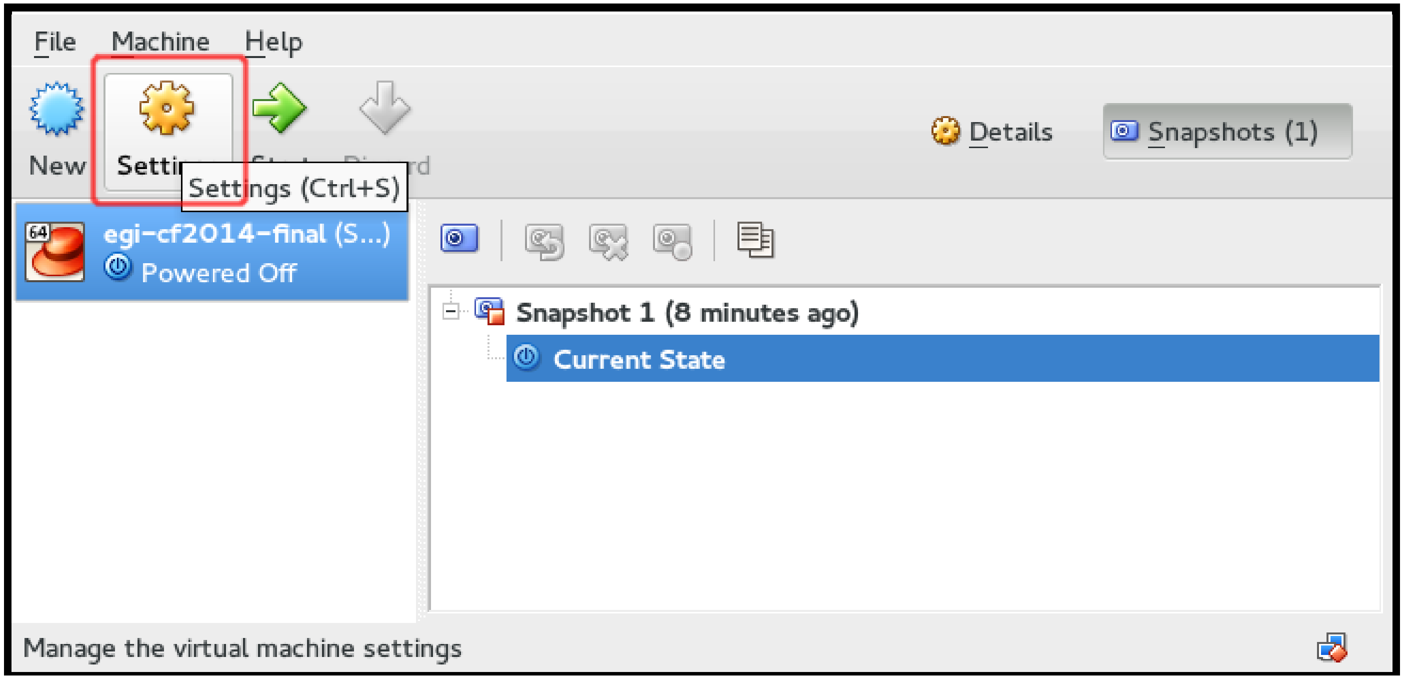
Snapshot Name

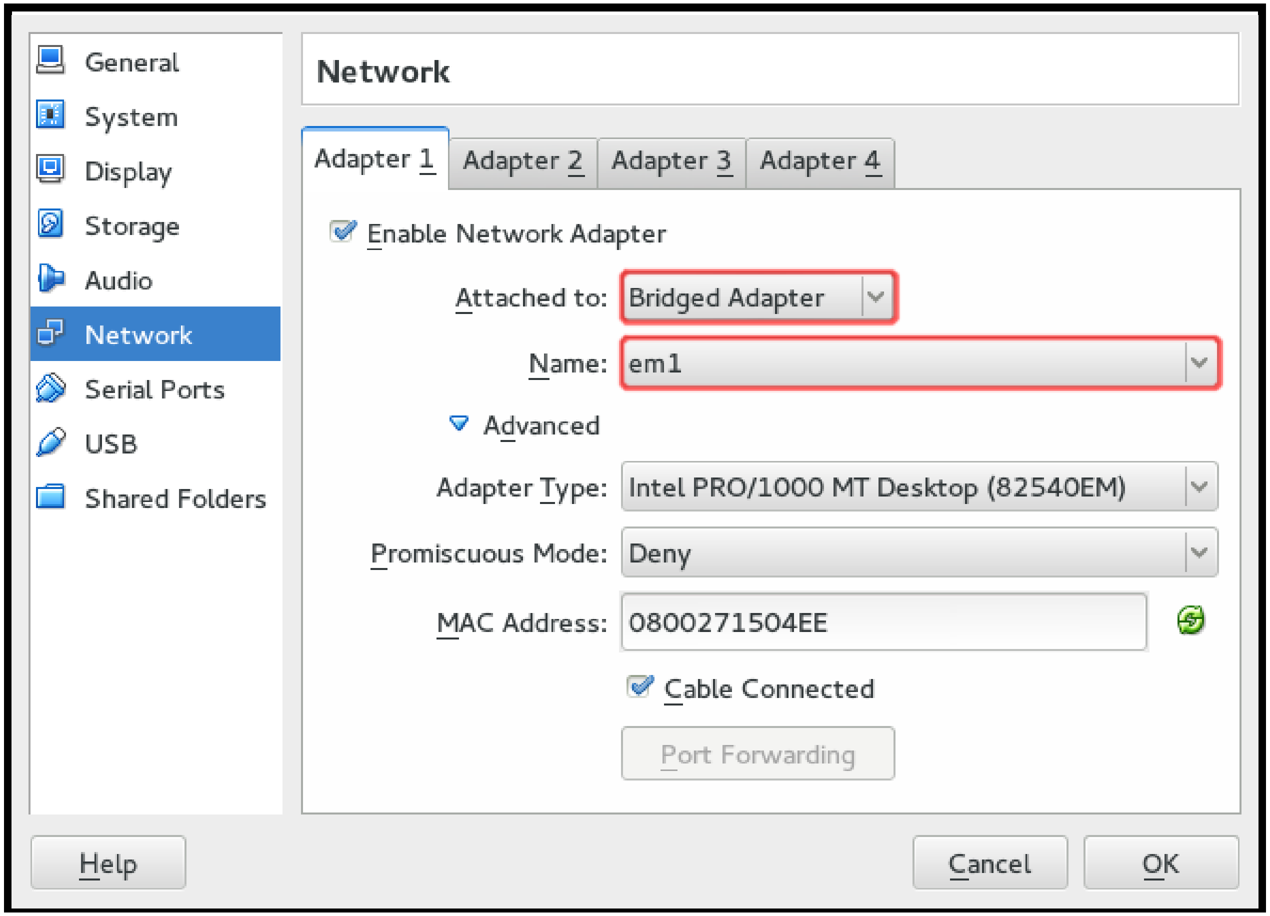
clean slate

Snapshot Description

not broken by me :-)

Help
Cancel
OK


File
Machine
Help
New
Setti
Settings (Ctrl+S)
Details
Snapshots (1)
egi-cf2014-final (S...)
Powered Off
Snapshot 1 (8 minutes ago)
Current State
Manage the virtual machine settings


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Port Forwarding
Help
Cancel
OK

Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: em1

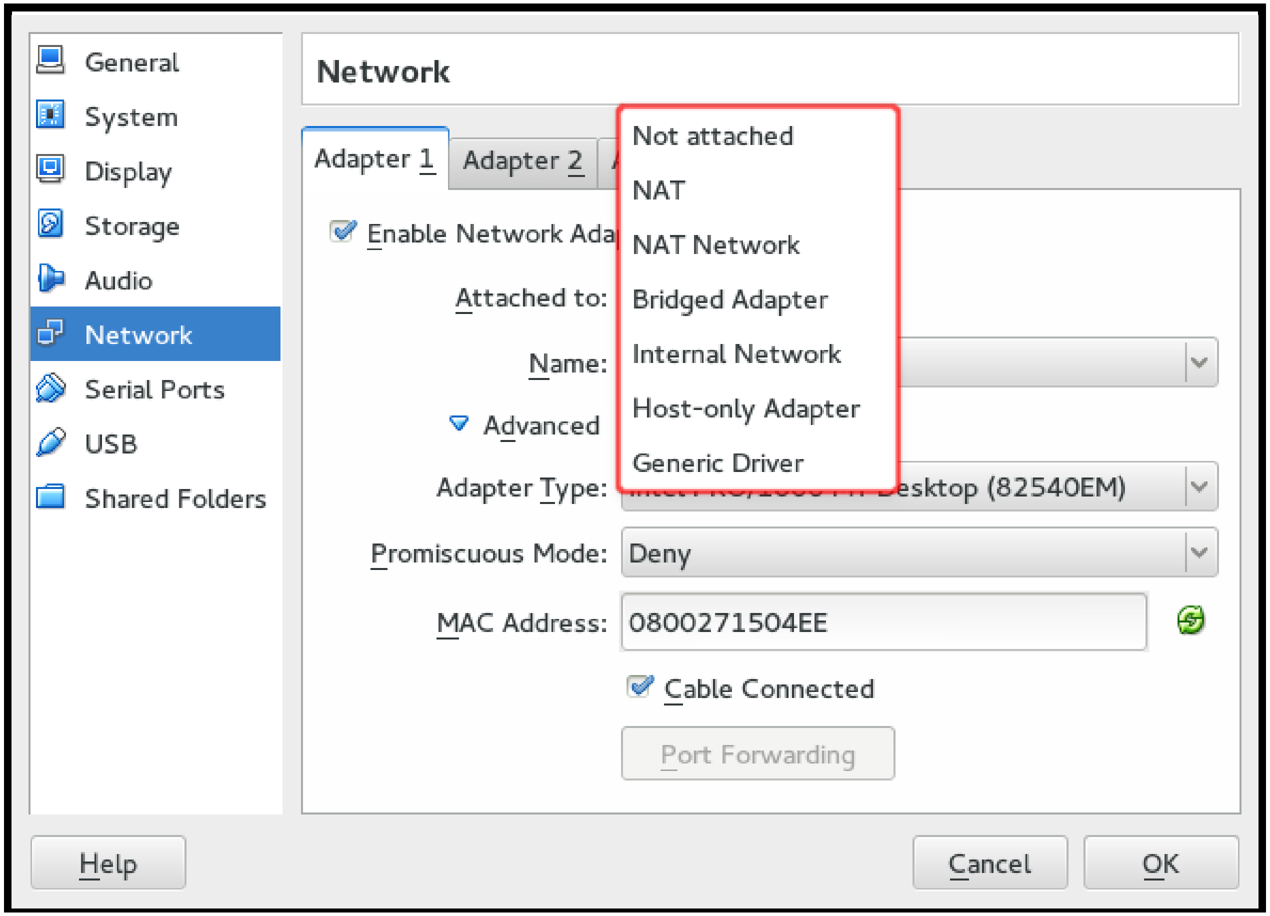
Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800271504EE

☑ Cable Connected


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Adapter 1
Adapter 2
Not attached
NAT
NAT Network
Bridged Adapter
Internal Network
Host-only Adapter
Generic Driver
Advanced
Port Forwarding
Help
Cancel
OK

Network

☑ Enable Network Ada

Attached to:

Name:

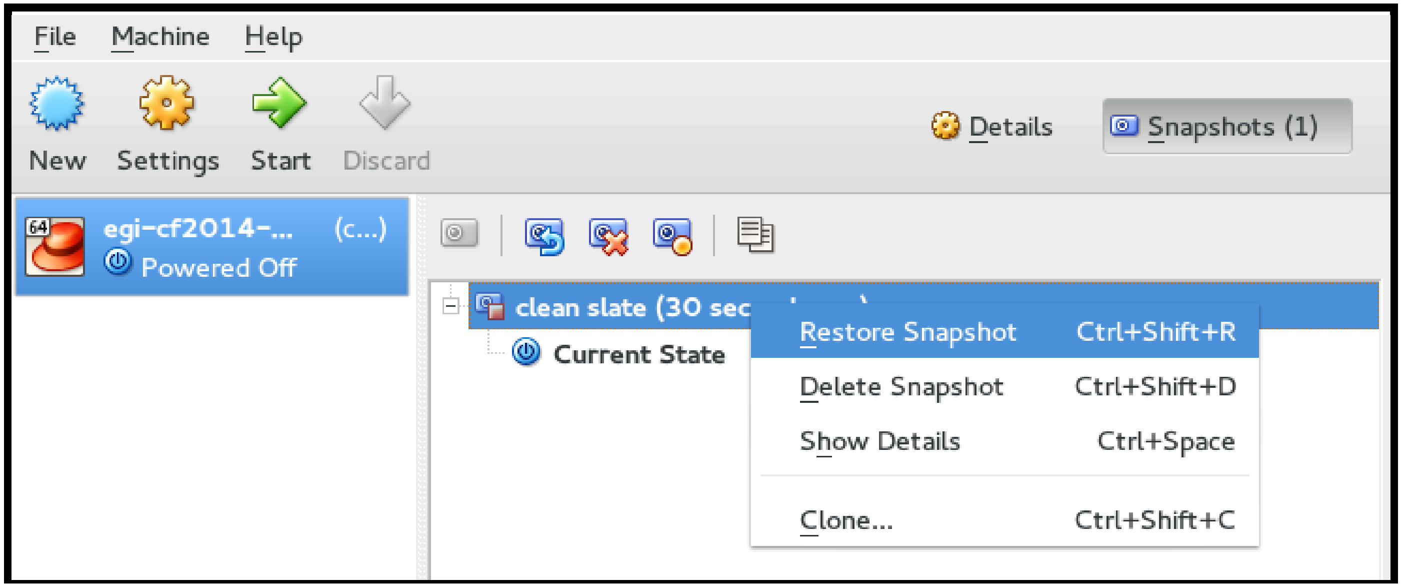
Adapter Type: Desktop (82540EM)

Promiscuous Mode: Deny

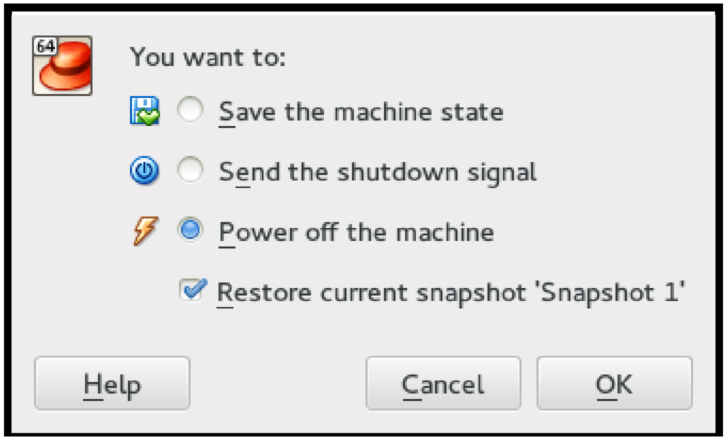
MAC Address: 0800271504EE

☑ Cable Connected

Broke it? Roll back!


File
Machine
Help
New
Settings
Start
Discard
Details
Snapshots (1)
egi-cf2014-...
(c...)
Powered Off
clean slate (30 sec
Current State
Restore Snapshot Ctrl+Shift+R
Delete Snapshot Ctrl+Shift+D
Show Details Ctrl+Space
Clone... Ctrl+Shift+C

The *Close* command gets a new option to roll back:



You want to:

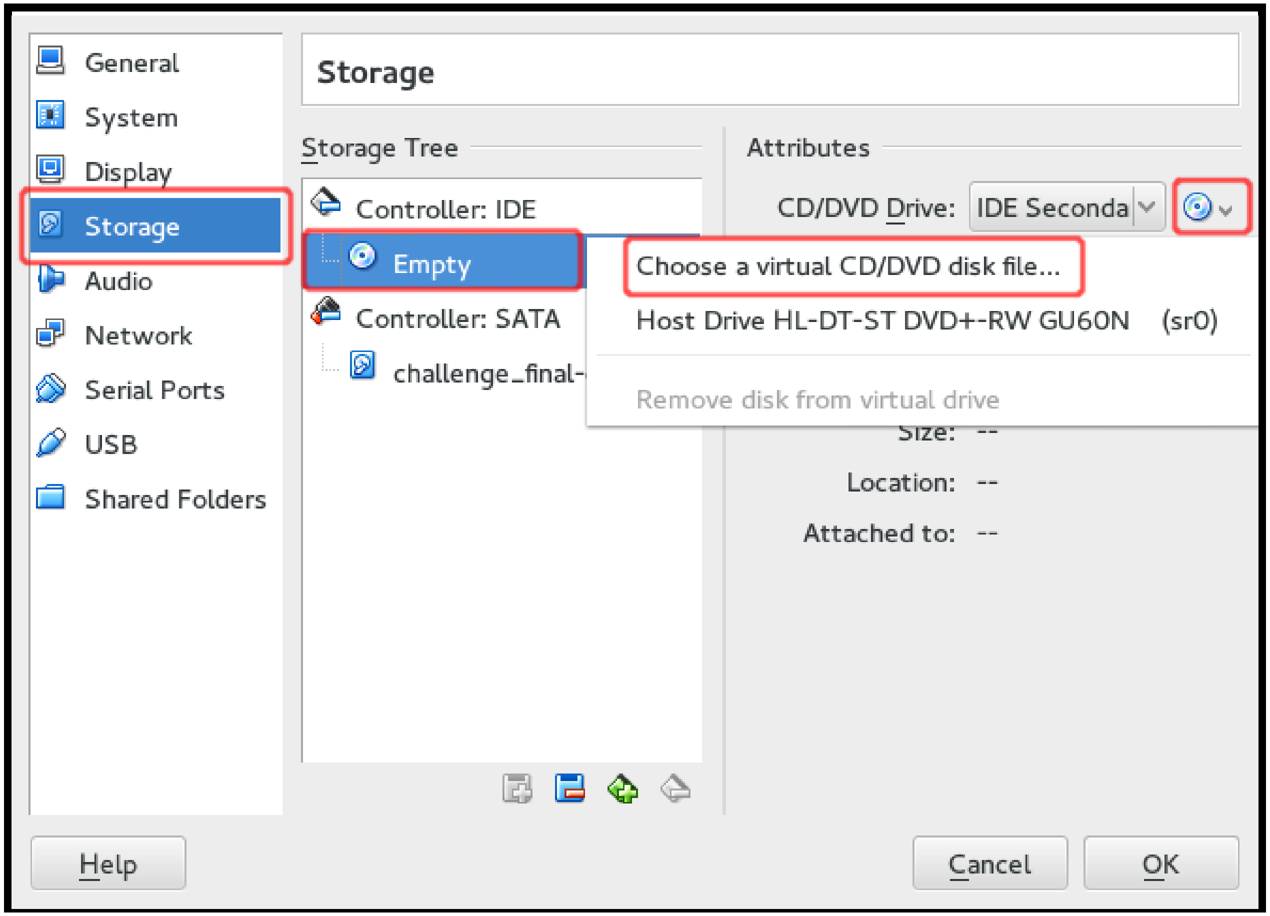
○ Save the machine state

○ Send the shutdown signal

● Power off the machine

☑ Restore current snapshot 'Snapshot 1'

Offline forensics:


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Storage
Storage Tree
Controller: IDE
Empty
Controller: SATA
challenge_final-
Attributes
CD/DVD Drive: IDE Seconda
Choose a virtual CD/DVD disk file...
Host Drive HL-DT-ST DVD+-RW GU60N (sr0)
Remove disk from virtual drive
Size: --
Location: --
Attached to: --
Help
Cancel
OK

Here's your account

- Username: **sherlock**
- Password: **cf2014**

Want to be **root**? Use **sudo.** Or find a better alternative ;-)

Depending on the remaining time: want me to give a fast walk through the forensic slides/checklist?

Questions?

Need the raw blockdev image?

```
# unpack ova
tar xvf challenge_final.ova

# patch image for qemu-img to work:
# to lazy to copy this link? do the "qemu" call and google
# the error message.
wget https://raw.githubusercontent.com/erik-smit/one-liners/master/qemu-img.vmdk3.hack.sh
sh qemu-img.vmdk3.hack.sh challenge_final-disk2.vmdk

# convert
qemu-img convert -O raw challenge_final-disk2.vmdk challenge_final.dd
```