OsecVM

1 Create Template

Install a normal Debian 7 32 Bit system as an Virtualbox VM (64Bit should also work, but we want to be compatible to 32 bit Windows)

```
1 CPU
768M RAM
15G Hardisk (VMDK, dynamic)
2 Network Interfaces:
 1 Host only Adapter (for connections between OsecVM and Hostsystem)
 2 NAT (for outgoing connections -> Secure brwosing)

Partitions (manual):
1GB Swap
14G / ext4

Pakets:
no ssh Server
no GUI
no Printserver
no Systemtools
as small as possible (we uninstall more pakates later -> ssh server will be
installaed manualy)

User:
osecuser (use a strong password -> we will only login with ssh key)
```

1.1 Reduce the system

https://wiki.debian.org/ReduceDebian
http://www.sabi.co.uk/blog/13-one.html#130414
http://aptitude.alioth.debian.org/doc/en/ch02s04s05.html

```
# Remove all not essential pakages (don't remove busybox -> see bug)
# ~i -> list all installed packages
# !~M -> don't list automatic installed packages
# !~prequired -> don't list packages with priority required
# !~pimportant -> don't list packages with priority important
# !~R~prequired -> don't list dependency packages of required packages
# !~R~pimportant -> don't list dependency packages of important packages
# !~R~R~prequired -> don't list dependency packages of dependency packages
of required packages -.- (hopefully two levels are enough)
# !~R~R~pimportant -> ... required packages
# !busybox -> don't list busybox
# !grub -> don't list grub (we need a boot manager. If LILO or something
else is used change this)
# !initramfs-tools -> don't list initramfs-tools (else the kernel is gone)
# !virtualbox- -> don't remove the Virtualbox guest tools

apt-get purge $(aptitude search
'~i!~M!~prequired!~pimportant!~R~prequired!~R~R~prequired!~R~pimportant!~R~R
~pimportant!busybox!grub!initramfs-tools!virtualbox-' | awk '{print $2}')
apt-get purge aptitude
apt-get autoremove
apt-get clean

# this should create a ~530 MB Template
# removing manpages ond other files reduce this to ~526MB -> useless
```

Reconfigure apt so that it does not install additional packages

```
vi /etc/apt/apt.conf.d/03noadditional
```

```
APT::Install-Recommends "0";
APT::Install-Suggests "0";
```

1.2 Install needed packages

https://www.grc.com/misc/truecrypt/truecrypt.htm

```
# zerofree to reduce the vmdk size
apt-get isntall openssh-server zerofree

tar -xvf truecrypt-7.1a-linux-console-x86.tar.gz
./truecrypt-7.1a-setup-console-x86
rm truecrypt-7.1a-*
```

Disable Grub Timeout

```
vi /etc/default/grub
#change "GRUB_TIMEOUT" to "0"

update-grub2
```

1.3 Config Network interfaces

```
vi /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp
```

1.4 Config remote ssh login for user

```
mkdir /home/osecuser/.ssh
chown osecuser:osecuser /home/osecuser/.ssh

vi /etc/fstab
```

```
# Replace default sr0 line
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
# with
/dev/sr0 /home/osecuser/.ssh/           udf,iso9660
ro,uid=osecuser,gid=osecuser    0       0
```

1.5 Optional (makes development easier)

```
apt-get install vim
```

Install Opensecurity pakages.
http://dpkg.opensecurity.at/

```
wget -O - http://dpkg.opensecurity.at/open_security.key | apt-key add -
wget http://dpkg.opensecurity.at/open-security.list -P
/etc/apt/sources.list.d/
apt-get update

# This installs all dependencys an configures the machine (its not designed
to be uninstalled!)
apt-get install osecvm-config
```

```
apt-get clean

# not really necessary (but why not)
reboot
```

1.6 Shrink the vmdk

On the VM

```
# clean up (you can do more here)
apt-get clean

# change to "maintainance mode" (no ssh server available)
init 1

# set root partion to readonly (first make sure that sda2 is the root partition)
mount -o remount,ro /dev/sda2

# zero out the free space
zerofree /dev/sda2

# stop the vm
halt
```

On the host

```
VBoxManage clonehd "oldimage.vmdk" "newimage.vmdk"

# After that remove the old vmdk file from the VM and add the new one to the VM
```

1.7 Export as OVA

In the Virtualbox GUI simply export the VM as OVA (OVF 1.0)