# Linux Host Kurulumu

Öncelikle, makine platformunuz için ana bilgisayar tarafındaki ağ yapılandırmasını hazırlayın. Örneğin, VirtualBox'ı host-only arabirimleriyle kullanıyorsanız ve vboxnet0 arabiriminiz varsa, ek bağımlılıkları kurmanıza gerek yoktur.

QEMU kullanıyorsanız, ana bilgisayarda ek bağımlılıkları kurmanız gerekebilir:

```
$ sudo apt install uml-utilities bridge-utils
```

Ardından, arabirimini yapılandırmak için sanal makinelerin listesini conf/qemu.conf'dan alın. Örneğin, ubuntu_x32, ubuntu_x64, ubuntu_arm, ubuntu_mips, ubuntu_mipsel vb. Her bir VM için, kök olarak başlatmak zorunda kalmamak için ana bilgisayarda bir ağ tap arabirimi önceden yapılandırın, örneğin:

```
$ sudo tunctl -b -u cuckoo -t tap_ubuntu_x32
$ sudo ip link set tap_ubuntu_x32 master br0
$ sudo ip link set dev tap_ubuntu_x32 up
$ sudo ip link set dev br0 up

$ sudo tunctl -b -u cuckoo -t tap_ubuntu_x64
$ sudo ip link set tap_ubuntu_x64 master br0
$ sudo ip link set dev tap_ubuntu_x64 up
$ sudo ip link set dev br0 up
```

> Cuckoo'yu farklı bir kullanıcı olarak çalıştırıyorsanız, -u'dan sonraki "cuckoo" ifadesini kendi kullanıcı adınızla değiştirin.

## x32/x64 Ubuntu 18.04 Linux Guest’i Hazırlamak

Agent’ın otomatik olarak başladığından emin olun. En kolay yol, crontab'a eklemektir:

```
```

```
$ sudo crontab -e
@reboot python /path/to/agent.py
```

Sanal makine içerisinde bağımlılıkları yükleyin:

```
$ sudo apt-get install systemtap gcc patch linux-headers-$(uname -r)
```

Kernel debugging symbols kurun:

```
$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
C8CAB6595FDFF622

$ codename=$(lsb_release -cs)
$ sudo tee /etc/apt/sources.list.d/ddebs.list << EOF
  deb http://ddebs.ubuntu.com/ ${codename}          main restricted universe
multiverse
  #deb http://ddebs.ubuntu.com/ ${codename}-security main restricted
universe multiverse
  deb http://ddebs.ubuntu.com/ ${codename}-updates  main restricted universe
multiverse
  deb http://ddebs.ubuntu.com/ ${codename}-proposed main restricted universe
multiverse
EOF

$ sudo apt-get update
$ sudo apt-get install linux-image-$(uname -r)-dbgsym
```

(Debian 9 amd64 için) Kernel debugging symbols kurun:

```
$ sudo apt-get install linux-image-$(uname -r)-dbg
```

SystemTap tapset'i düzeltin, böylece Cuckoo analyzer çıktıyı düzgün bir şekilde çözebilir:

```
$ wget
https://raw.githubusercontent.com/cuckoosandbox/cuckoo/master/stuff/systemt
ap/expand_execve_envp.patch
```

```
$ wget
https://raw.githubusercontent.com/cuckoosandbox/cuckoo/master/stuff/systemt
ap/escape_delimiters.patch
$ sudo patch /usr/share/systemtap/tapset/linux/sysc_execve.stp <
expand_execve_envp.patch
$ sudo patch /usr/share/systemtap/tapset/uconversions.stp <
escape_delimiters.patch
```

Kernel extension'ı derleyin:

```
$ wget
https://raw.githubusercontent.com/cuckoosandbox/cuckoo/master/stuff/systemt
ap/strace.stp
$ sudo stap -p4 -r $(uname -r) strace.stp -m stap_ -v
```

Derleme işlemi tamamlandığında aynı klasörde stap_.ko dosyasını görmelisiniz. Şimdi STAP kernel extension'ı aşağıdaki gibi test edebilirsiniz:

```
$ sudo staprun -v ./stap_.ko
```

Çıktı aşağıdaki gibi olmalıdır:

```
staprun:insert_module:x Module stap_ inserted from file path_to_stap_.ko
```

`stap_.ko` dosyasını `/root/.cuckoo` dizinine yerleştirmelisiniz:

```
$ sudo mkdir /root/.cuckoo
$ sudo mv stap_.ko /root/.cuckoo/
```

Eğer varsa, sanal makinedeki güvenlik duvarını devre dışı bırakın:

```
$ sudo ufw disable
```

Sanal makine içinde NTP'yi devre dışı bırakın:

```
$ sudo timedatectl set-ntp off
```

İsteğe bağlı - önceden yüklenmiş yazılım ve konfigürasyonları kaldırın:

```
$ sudo apt-get purge update-notifier update-manager update-manager-core ubuntu-release-upgrader-core
$ sudo apt-get purge whoopsie ntpdate cups-daemon avahi-autoipd avahi-daemon avahi-utils
$ sudo apt-get purge account-plugin-salut libnss-mdns telepathy-salut
```

Linux guest sistemini statik IP adresleriyle yapılandırmak önerilir. Konfigürasyondaki makine girişinin doğru IP adresine sahip olduğundan ve platform değişkeninin linux olarak ayarlandığından emin olun. VM yapılandırıldıktan sonra bir anlık görüntü oluşturun. Şimdi analiz için hazırız.

---

Revision #2
Created 28 December 2023 07:34:06 by Ertan Sözer
Updated 28 December 2023 07:39:17 by Ertan Sözer