Instalação do Cuckoo Sandbox

Autor: p3tr0v

versão 1.1

Sobre o autor

Após alguns anos como desenvolvedor java, p3tr0v (pronuncia petrov) hoje trabalha na área de segurança da informação, analisando ameaças e estudamento remediações; é um curioso e, quando consegue ser, contribuidor em estudos de malwares na comunidade brasileira

About author

After some years as java developer, nowadays p3tr0v (says petrov) works in cybersecurity, analysing threats and looking for mitigation; is a curious and, when ir can be, contributor in malware studies in the Brazilian community

Telegram: @p3tr0v

Para instalação, recomendamos o Ubuntu 17.10 64 bits, para tornar mais prático, o tutorial abaixo foi realizado com ambiente gráfico nativo da instalação.

A instalação do Cuckoo é a partir do repositório oficial oferecido pelo Pip (Python), sem o adicional de módulos, portanto, o Cuckoo instalado é o mais limpo possível, porém, funcional.

Requisitos

Entender a arquitetura do Cuckoo e suas terminologias (ver em documentação oficial)

1. Preparação de ambiente

Certifique-se que os repositórios estão atualizados com *apt-get update* e instale as dependências

```
$ sudo apt-get install -y python build-essential python-pip python-dev libffi-dev
libssl-dev python-virtualenv python-setuptools libjpeg-dev zlib1g-dev swig mongodb
postgresql libpq-dev tcpdump apparmor-utils libcap2-bin git wireshark elasticsearch
samba-common-bin autoconf libtool libjansson-dev libmagic-dev htop net-tools yara

$ sudo apt-get clean ; sudo apt-get autoremove
```

Durante a instalação do wireshark, ele irá perguntar se *não-superusuarios* poderão interceptar pacotes, selecione a opção *sim*

OBS : Os programas wireshark e htop não são pré-requisitos, foram usados apenas como utilitários opcionais para identificar eventuais problemas de rede e consumo de recursos de hardware, respectivamente.

Instale o volatility

Instale primeiro as dependências usadas pelo volatility

```
$ pip install openpyxl

$ pip install ujson

$ pip install pycrypto

$ pip install distorm3

$ pip install pytz
```

Para instalar, siga os comandos

```
$ git clone https://github.com/volatilityfoundation/volatility.git

$ cd volatility

$ python setup.py build

$ sudo python setup.py install

$ python vol.py -h #para validar a instalação
```

Atualize o pip e setuptools

```
$ pip install -U pip setuptools
```

Criação de diretórios

No diretório */opt* crie um diretório onde será instalado um virtualenv para o Cuckoo e dê permissões para usuário da máquina *não-superusuario*

```
$ sudo mkdir /opt/envCuckoo
$ sudo chown <usuario>.<usuario> /opt/envCuckoo/ -R
$ virtualenv /opt/envCuckoo/
$ . envCuckoo/bin/activate
```

Crie o diretório onde será o *CWD (Cuckoo Working Directory)*

```
(cuckooVenv) ..... $ sudo mkdir /opt/cuckoo
(cuckooVenv) ..... $ sudo chown <usuario>.<usuario> /opt/cuckoo -R
```

2. Instale o Cuckoo

Criado os diretórios, instale o cuckoo com opção de atualização de pacote

```
(cuckooVenv) ..... $ pip install -U cuckoo
```

Inicialize o CWD, esse diretório por padrão fica em <HOME_USER>/.cuckoo , mas será instalado em */opt/cuckoo*. Neste momento, os arquivos de trabalho apenas serão criados, o cuckoo não entra em operação agora, e sim na próxima vez que voce executar o comando

```
(cuckooVenv) ..... $ cuckoo --cwd /opt/cuckoo -d
```

Sempre que for iniciar o Cuckoo, certifique-se de que está usando o *virtualenv* do Cuckoo que voce definiu. Para entrar no modo virtualenv digite

```
$ . /opt/envCuckoo/bin/activate
```

3. Instale o VirtualBox

Adicione o repositório do VirtualBox no *apt*, instale a chave pública, realize update, e instale o VirtualBox

```
$ echo 'deb http://download.virtualbox.org/virtualbox/debian stretch contrib' |sudo tee -a  /etc/apt/sources.list.d/virtualbox.list
$ wget https://www.virtualbox.org/download/oracle_vbox_2016.asc | sudo apt-key add oracle_vbox_2016.asc
$ sudo apt-get update
$ sudo apt-get install virtualbox-5.2
```

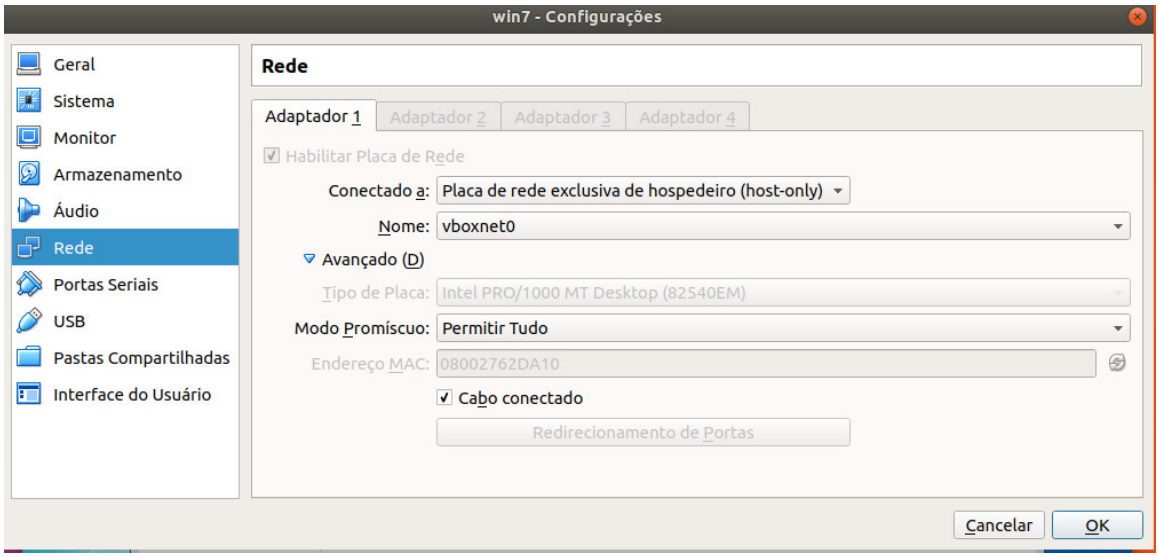
Utilize o comando *ifconfig* para verificar se foi criado a interface de rede para o VirtualBox, caso não tenha sido criado, crie

```
$ vboxmanage hostonlyif create

$ vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
```

Configurando o windows 7

Instale o Windows 7 como *guest* (ou outro Windows de preferência, neste tutorial, usaremos o 7 32 bits) no VirtualBox

Antes de instalar, configure a rede para *host-only* nas configurações da VM.



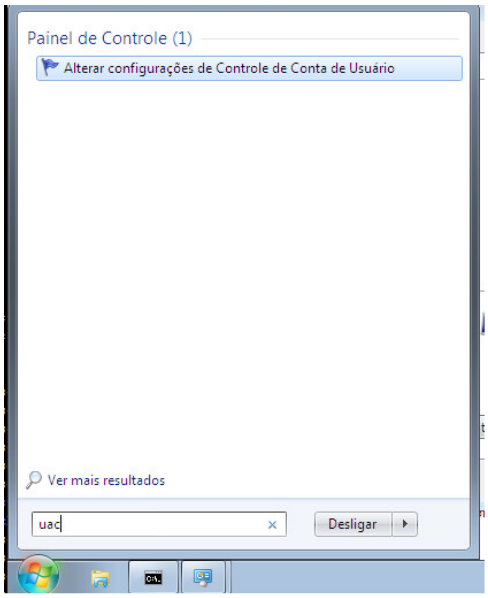
OBS: Para instalação do *guest* windows 7 são necessários no mínimo 12GB de espaço,

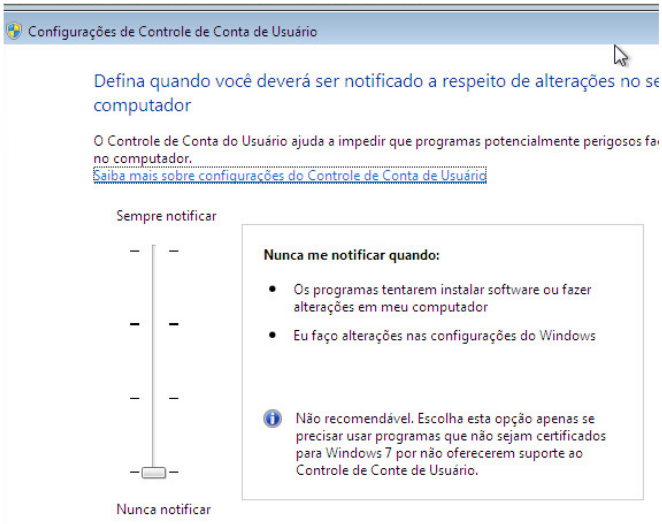
este tutorial usou um *guest* com 15GB de HD e 2.8GB de memória.

Após instalar o windows 7, faça os procedimentos a seguir

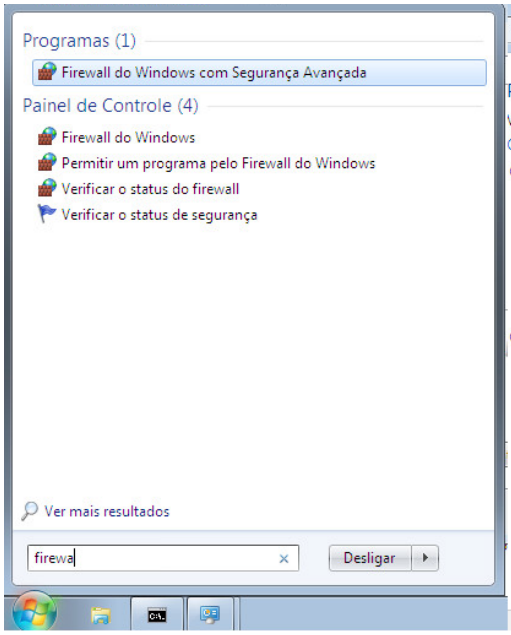
Instale o python 2.7 32 bits (lemvbre-se de marcar a opção para colocar o python no path da máquina) e o Java (para testes com malwares escritos em Java).

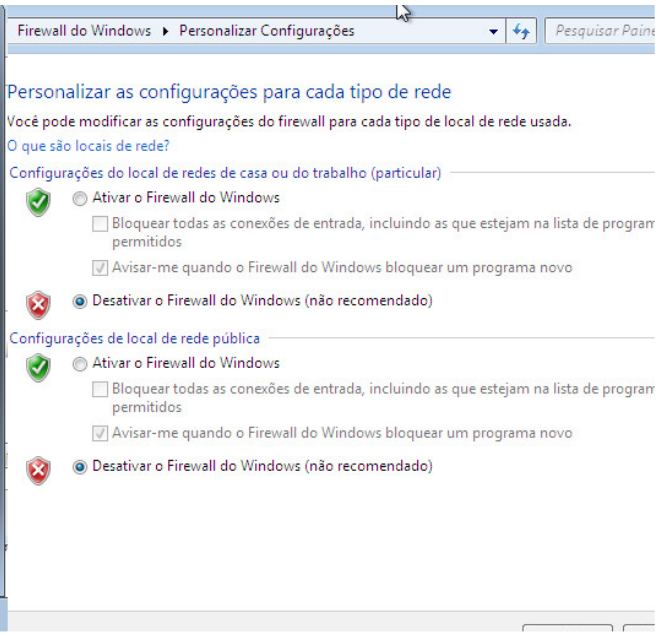
Desabilite o UAC



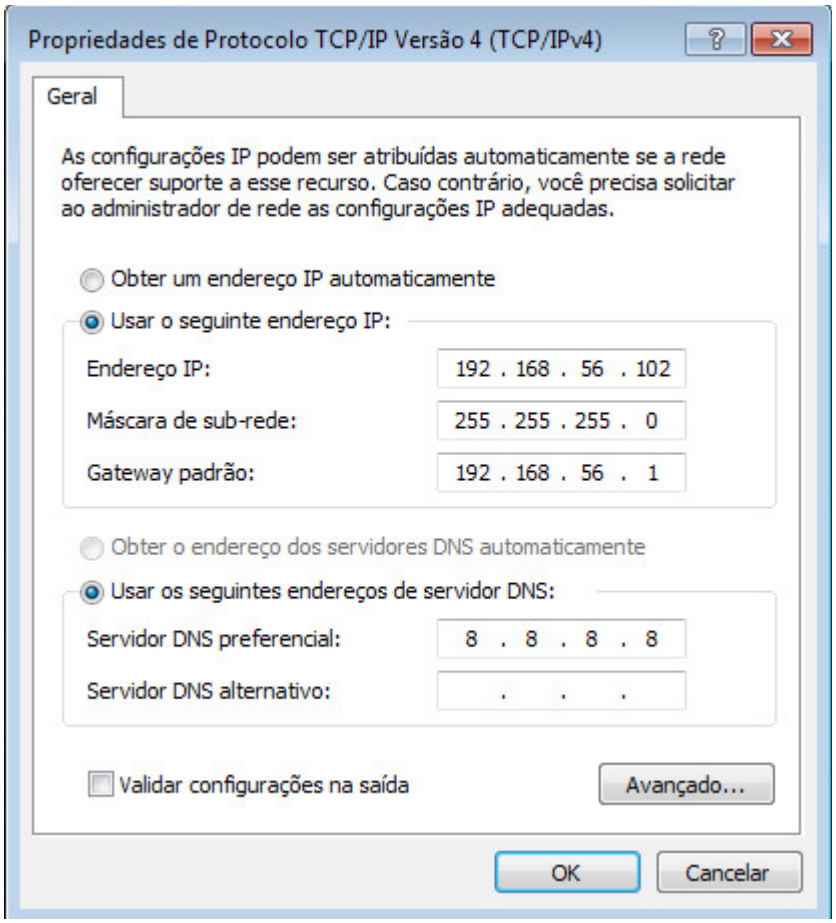


Desabilite o firewall





Adicione o gateway 192.168.56.1 como configuração de IPV4

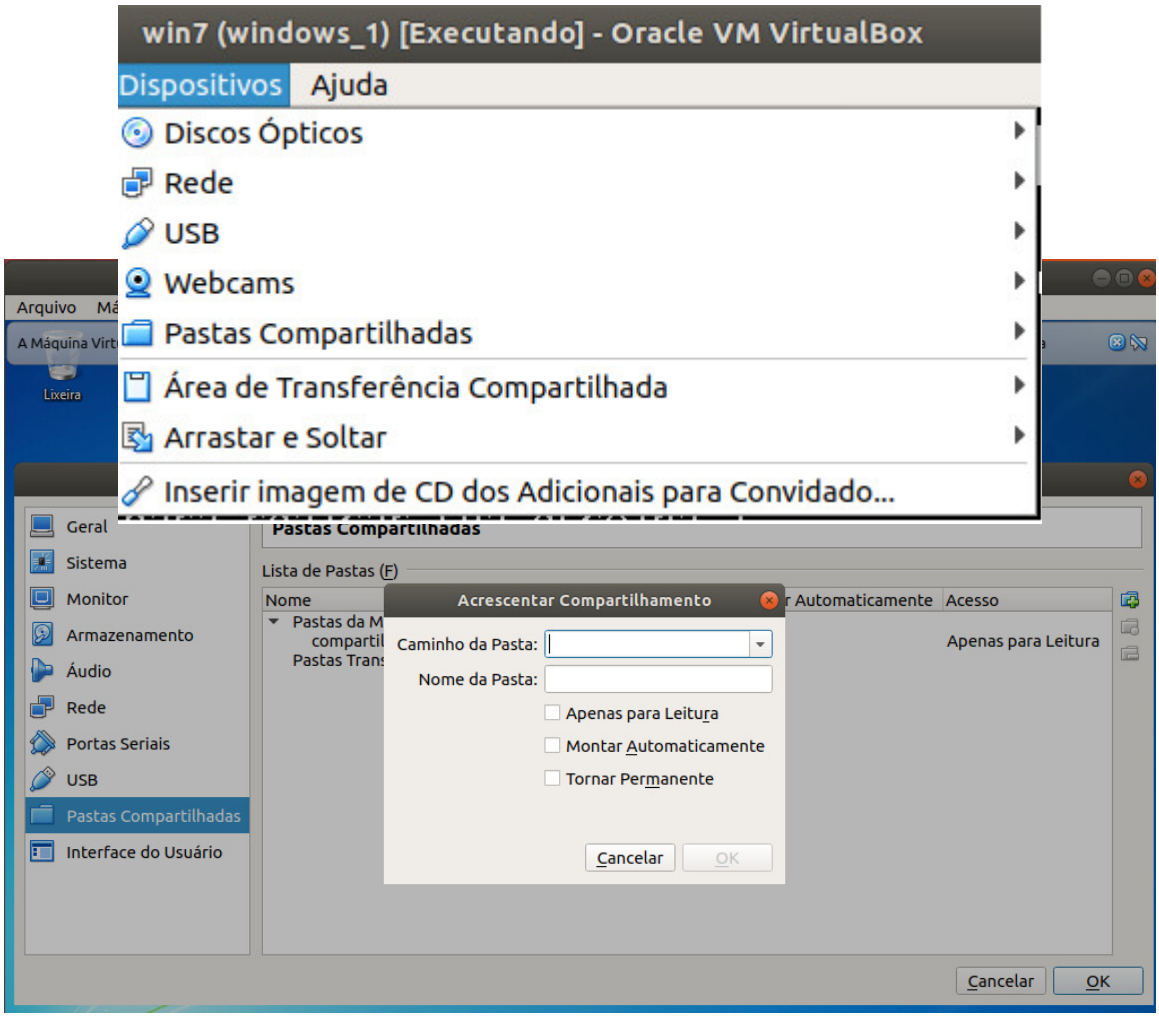


Execute os seguintes comandos via CMD para alterar os registros

```
reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultUserName /d <usuario> /t REG_SZ /f

reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultPassword /d <senhaUsuario> /t REG_SZ /f

reg add "hklm\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v AutoAdminLogon /d 1 /t REG_SZ /f

reg add "hklm\system\CurrentControlSet\Control\TerminalServer" /v AllowRemoteRPC /d 0x01 /t REG_DWORD /f

reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LocalAccountTokenFilterPolicy /d 0x01 /t REG_DWORD /f
```

Instale o VBoxGuestAdditions_5.x no windows 7, para obter a ISO, vá em *Dispositivos -> Inserir imagem de CD dos adicionais*, será solicitado o download. Isto é para podermos compartilhar diretórios entre *host* e *guest* da maneira que o Cuckoo usa para

compartilhar arquivos. Instalado os adicionais, acrescente um diretório de compartilhamento na opção "pastas da máquina", marque todas as 3 opções no checkbox.

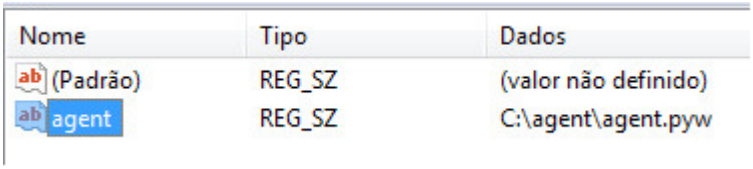


Utilize esse compartilhamento para transferir o arquivo *%CWD/agent/agent.py* para o *guest*, renomeia o arquivo para *agent.pyw* (para rodar sem mostrar console).

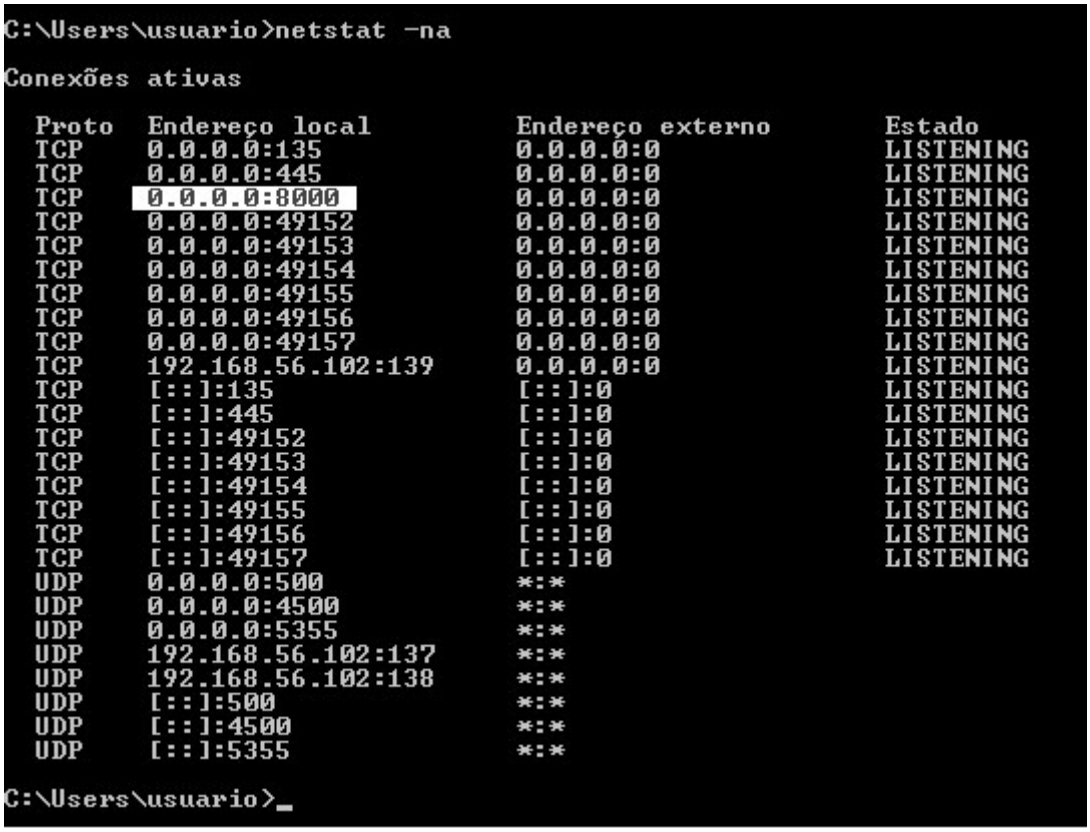
Coloque esse arquivo em *C:\agent*. Em seguida, cadastre-o na inicialização automática através do *regedit*. Vá no caminho

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

e adicione um novo "valor de sequiencia", com um nome qualquer, e o caminho onde foi colocado o arquivo com o nome do arquivo.



Reinicie a máquina virtual. Após ligar novamente, execute o comando *netstat -na* e procure por um serviço escutando na porta 8000, este é o agente python do Cuckoo, que configuramos para inciar quando o windows ligar.



Tire um snapshot da máquina **enquanto ela estiver rodando**. No host do Cuckoo , pela linha de comando, faça conforme orienta a documentação oficial.

```
$ vboxmanage snapshot "win7" take "windows_1" --pause
$ vboxmanage controlvm "win7" poweroff
$ vboxmanage snapshot "win7" restorecurrent
```

4. Configre a rede do *host Cuckoo*

No Debian, onde foi instalado o Cuckoo, deve ser feita uma configuração no IPtables, *forward* e tcpdump

iptables

Mantenha sempre essas regras ativas, ou por modo do iptables-persistent ou via script de inicialização

```
$ sudo iptables -A FORWARD -o <interfaceDeRedeFisica> -i
```

```
<interfaceRedeVirtualBox> -s 192.168.56.0/24 -m conntrack --ctstate NEW -j
ACCEPT

$sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT

$sudo iptables -A POSTROUTING -t nat -j MASQUERADE
```

ip_forward

Sempre mantenha o valor igual a 1, para permitir o fluxo de tráfego pelo Debian

```
$ sudo sysctl -w net.ipv4.ip_forward=1
```

Para verificar o valor, se é 0 ou 1, execute o comando

```
$ cat  /proc/sys/net/ipv4/ip_forward
```

tcpdump

Permita que não super-usuários possam utilizar o tcpdump

```
$ sudo aa-disable /usr/sbin/tcpdump
$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

5. Configurando o Cuckoo

Existem vários arquivos de configuração, com dezenas de opções de configurações; neste tutorial, vamos configurar o suficiente para o Cuckoo funcionar, módulos adicionais não estão previstos nestas configurações. Ficará a cargo do leitor decidir quais configurações a mais desejará realizar.

Para deixar a ferramenta funcional, iremos alterar os arquivos *$CWD/conf/cuckoo.conf* , *$CWD/conf/virtualbox.conf* e *$CWD/conf/reporting.conf*. O segundo arquivo trata das configurações das VMs do VirtualBox, se voce estiver usando o VMware , por exemplo, voce alteraria o arquivo *$CWD/conf/vmware.conf*.

cuckoo.conf

Por padrão é habilitado o uso do VirtualBox, que fica definido no parâmetro *[cuckoo]-machinery* em *[resultserver]-ip* coloque o IP do VirtualBox que é apresentado no comando *ifconfig*, o resultado deste comando (no nosso ambiente, claro, no seu ambiente isso pode variar) é apresentado

```
vboxnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::800:27ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        ether 0a:00:27:00:00:00  txqueuelen 1000  (Ethernet)
```

```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2014  bytes 276971 (276.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Logo, na configuração, deve ser posto exatamente este IP. Para pouparmos tempo sempre que iniciar o Cuckoo debilite a verificação por update, ative-a apenas quando voce realmente tiver intenção de atualizar o Cuckoo. Para isso basta alterar o valor de *version_check*

```
[cuckoo]
version_check = no
machinery = virtualbox

(... outras configurações omitidas...)

[resultserver]
ip = 192.168.56.1 # este eh o IP de gateway do virtualbox

(... outras configurações omitidas...)
```

virtualbox.conf

Este é o arquivo que merece mais atenção, é nele que existem certas 'pegadinhas do malandro'.

Primeiro, configure a interface: em *[virtualbox]-interface* coloque o nome da interface do VirtualBox que criamos, no caso, vboxnet0.

Depois, configure o *[cuckoo1]-label*, coloque o nome cadastrado no VirtualBox, **não confundir** com o nome dado à máquina no isntante da instalação. MUITOS tutoriais não deixam isso bem explícito, pois eles criam a VM com o nome de *cuckoo1*, mas não falam o que deve ser feito se a VM for criada com outro nome, e quando criam com outro nome, os autores não explicitam sobre esse campo *label*. No meu caso, criei com o nome *win7*, então meu *label* ficará com esse valor.

O parâmetro *[virtualbox]-machines* serve para configurar "container" de máquinas *guest*, o valor ali deve coincidir com o valor cadastrados entre colchetes, imagine esse parâmetro como um índice de máquinas.

No parâmetro *[cuckoo1]-ip*, colocamos o IP da VM registrado no passo 3 "Configurando windows 7", no nosso exemplo, 192.168.56.102.

No parâmetro *[cuckoo1]-snapshot*, colocamos o nome do snapahot criado também no passo 3, no nosso exemplo, windows_1.

Não há necessidade de alterar os outros parâmetros, claro que isso também irá depender de como voce deseja-rá configurar.

reporting.conf

Ative o mongoDB, este será usado quando iniciarmos a parte web do Cuckoo.

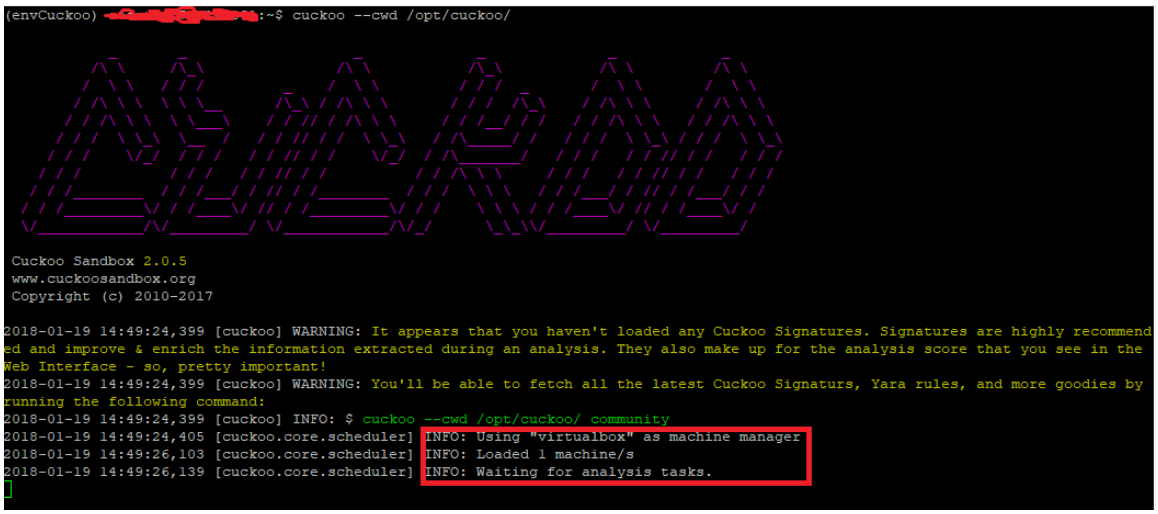
(... outras configurações omitidas...)
[mongodb]

enabled = yes

(... outras configurações omitidas...)

6. Faça a mágica acontecer

Depois de termos instalado as dependências do Cuckoo; o Cuckoo; criado a VM do windows 7 e feito as devidas configurações documentadas aqui; inicialize o Cuckoo (dentro de seu virtualenv)



Em outro console, inicie a parte web

(envCuckoo)..... $ cuckoo --cwd /opt/cuckoo/ web runserver 0.0.0.0:8080

No navegador, acesso o IP do *host* Cuckoo na porta 8080.

Faça upload de um sample.

Divirta-se e bons estudos.

Lembrando que aqui não foi abordado tunning do Yara com python, utilização do postgres como banco, ou outros módulos opcionais do Cuckoo, apenas fizemos o

necessário para torná-lo funcional.

7. Problemas comuns

- Máquina *guest* não conecta na rede.

Certifique-se de que os comandos do iptables e ipv4_forward estão válidos e se foram digitados corretamente;

Verifique se o *gateway* (nas propriedades do IPV4 do windows) foi configurado corretamente.

- Meu agente python não inicializa quando o windows inicia

Verifica se ele não está em modo 'somente leitura';

Verifique se ele possui a extensão *pyw*, que significa que não irá mostrar console ao ser executado.

- CuckooCriticalError: Please update your configuration. Unable to shut 'cuckoo1' down or find the machine in its proper state: The virtual machine 'cuckoo1' doesn't exist! Please create one or more Cuckoo analysis VMs and properly fill out the Cuckoo configuration!

Este erro acontece por conta do campo *label* no arquivo virtualbox.conf, o erro acima está procurando uma máquina virtual criada no VirtualBox com o ome 'cuckoo1', altere para o nome que voce criou.

- In order to use the Cuckoo Web Interface it is required to have MongoDB up-and-running and enabled in Cuckoo. Please refer to our official documentation as well as the $CWD/conf/reporting.conf file.

A parte web depende do mongoDB (instalado no primeiro passo do manual); a opção do mongo deve estar ativada no arquivo *%CWD/conf/reporting.conf* .

Referências

Instalação do VirtualBox no Debian 9
https://wiki.debian.org/VirtualBox#Debian_9_.22Stretch.22

Warunikaamali https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f

Cuckoo instalation http://docs.cuckoosandbox.org/en/latest/introduction/

Oktavianto, Digit & Muhardianto, Iqbal - Cuckoo Malware Analysis, Analyse malware using Cuckoo Sandbox. Editora PACKT PUBLISHING