Sıkça Sorulan Sorular

Genel Sorular

Cuckoo ile URL'leri analiz edebilir miyim?

Sürüm 0.5 ile gelen yeni özellik: Cuckoo'ya URL analizi için yerleşik destek eklendi.

Sürüm 2.0-rc1'de değişiklik: Cuckoo artık sadece tarayıcıyı başlatmakla kalmayacak (örneğin Internet Explorer), aynı zamanda ilginç sonuçlar çıkarmak için etkili bir şekilde enstrüman yapmaya çalışacaktır; bu sonuçlar arasında yürütülen JavaScript, iframe URL'leri gibi veriler bulunur.

URL gönderimi hakkında ek ayrıntılar, bir Analiz Gönderme konusunda belgelenmiştir, ancak özünde şu komutu içerir:

```
cuckoo submit --url http://example.com
```

Cuckoo ile Volatility'i kullanabilir miyim?

Sürüm 0.5 ile yeni eklenen özellik: Cuckoo, analiz sürecinin sonunda oluşturulan isteğe bağlı memory dump destekler. Bu memory dumpları kullanarak Volatility gibi memory forensic analizlerini gerçekleştirebilirsiniz.

Ayrıca, lütfen bunu özellikle teşvik etmediğimizi göz önünde bulundurun: Cuckoo, işlemlerini gerçekleştirmek için bazı rootkit benzeri teknolojiler kullanır, bu nedenle bir forensic analizin sonuçları, sandbox'ın bileşenleri tarafından kirletilebilir.

Cuckoo'yu VMware ESXi ile kullanabilmek için neler gereklidir?

VMware vSphere Hypervisor (veya ESXi) ile çalıştırmak için, Cuckoo, libvirt veya VMware vSphere API için Python SDK olan pyVmomi'ye dayanır. Sanal makineler üzerinde kontrol sağlamak için VMware API'leri kullanılır, ancak bu API'ler yalnızca lisanslı sürümde bulunur. VMware vSphere ücretsiz sürümünde bu API'ler yalnızca okunurdur, bu nedenle Cuckoo ile kullanamazsınız. Minimum gerekli lisans için lütfen VMware web sitesine göz atın.

Sorun Giderme

Sorun Giderme

Cuckoo güncelleme sonrası çalışmayı durduruyor.

Muhtemelen yanlış bir şekilde güncellediniz. Cuckoo'nun karmaşıklığı ve hızlı gelişimi nedeniyle dosyaları yeniden yazmak iyi bir uygulama değildir.

Lütfen önceki bir sürümden güncelleme adımlarını açıklayan "Önceki Sürümden Güncelleme" adlı kılavuzu takip edin.

KVM ile mevcut anlık görüntüyü kontrol edin ve geri yükleyin

Sanal makinede bir şeyler ters giderse, mevcut anlık görüntü durumunu kontrol etmek en iyi uygulamadır. Bunu aşağıdakilerle yapabilirsiniz:

```
$ virsh snapshot-current "<Name of VM>"
```

Çıktı olarak uzun bir XML'iniz varsa, mevcut anlık görüntünüz yapılandırılmıştır ve bu bölümün geri kalanını atlayabilirsiniz; yine de, aşağıdaki gibi bir hata aldıysanız, mevcut anlık görüntünüz bozuk:

```
$ virsh snapshot-current "<Name of VM>"
error: domain '<Name of VM>' has no current snapshot
```

Mevcut bir anlık görüntüyü düzeltmek ve oluşturmak için önce tüm makinenin anlık görüntülerini listeleyin:

```
$ virsh snapshot-list "<Name of VM>"
 Name                 Creation Time           State
 ------------------------------------------------------------
 1339506531           2012-06-12 15:08:51 +0200 running
```

Bir anlık görüntü adı seçin ve güncel olarak ayarlayın:

```
$ snapshot-current "<Name of VM>" --snapshotname 1339506531
Snapshot 1339506531 set as current
```

Artık sanal makinenizi kullanabilirsiniz.

VirtualBox ile mevcut anlık görüntüyü kontrol edin ve geri yükleyin

Sanalda bir şeyler ters giderse, sanal makine durumunu ve mevcut anlık görüntüyü kontrol etmek en iyi uygulamadır. Öncelikle sanal makine durumunu aşağıdakilerle kontrol edin:

```
$ VBoxManage showvminfo "<Name of VM>" | grep State
State:          powered off (since 2012-06-27T22:03:57.000000000)
```

Durum "powered off" ise bir sonraki kontrole devam edebilirsiniz, durum "aborted" veya başka bir şeyse, daha önce "powered off" durumuna geri yüklemeniz gerekir:

```
$ VBoxManage controlvm "<Name of VM>" poweroff
```

Aşağıdaki komutla mevcut anlık görüntülerin durumunu kontrol edin:

```
$ VBoxManage snapshot "<Name of VM>" list --details
Name: s1 (UUID: 90828a77-72f4-4a5e-b9d3-bb1fdd4cef5f)
Name: s2 (UUID: 97838e37-9ca4-4194-a041-5e9a40d6c205) *
```

Yıldız "*" ile işaretlenmiş bir anlık görüntünüz varsa, anlık görüntünüz hazırdır, yine de geçerli anlık görüntüyü geri yüklemeniz gerekir:

```
$ VBoxManage snapshot "<Name of VM>" restorecurrent
```

Unable to bind result server hatası

Cuckoo başlangıcında bunun gibi bir hata mesajı alırsanız:

`2014-01-07 18:42:12,686 [root] CRITICAL: CuckooCriticalError: Unable to bind result server on 192.168.56.1:2042: [Errno 99] Cannot assign requested address`

Bu, Cuckoo'nun cuckoo.conf'ta (veya içinde resultserver_ip seçeneğini kullanıyorsanız machinery.conf'ta) yazılan IP adresinde result server başlatamadığı anlamına gelir. Bu genellikle, result server IP adresiyle ilişkili sanal arayüzü getirmeden Cuckoo'yu başlattığınızda olur. Manuel olarak getirebilirsiniz, bir sanallaştırma yazılımından diğerine bağlıdır, ancak nasıl yapacağınızı bilmiyorsanız, iyi bir yol bir analiz sanal makinesini manuel olarak başlatmak ve durdurmaktır, bu sanal ağı getirecektir.

VirtualBox tarafında host-only arayüzü vboxnet0 aşağıdaki gibi oluşturulabilir:

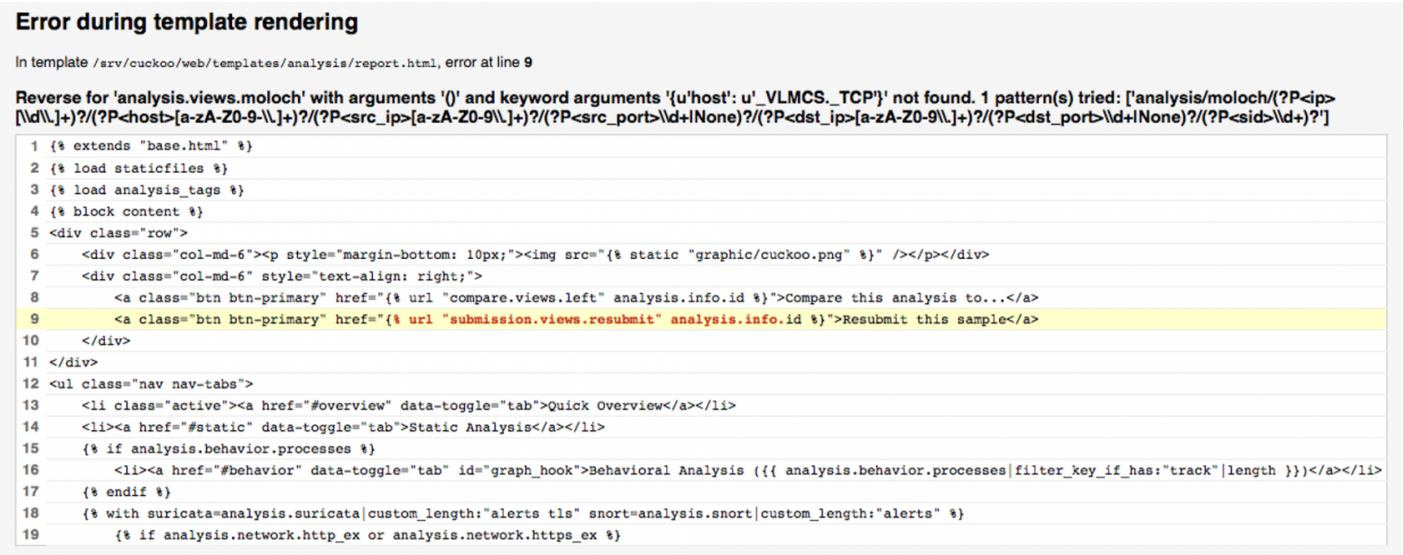
```
# If the hostonly interface vboxnet0 does not exist already.
$ VBoxManage hostonlyif create

# Configure vboxnet0.
$ VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask
255.255.255.0
```

Şablon oluşturma sırasında hata:

2.0-rc1 sürümünde değiştirildi.

2.0-rc1 sürümünde aşağıdaki ekran görüntüsünde gösterildiği gibi bir hata tanıtıldı. Bu sorunu yerel kurulumunuzda çözmek için lütfen `web/analysis/urls.py` dosyasını açın ve 21. satıra bir alt çizgi ekleyerek aşağıdaki gibi değiştirin:

```
-       "/(?P<ip>[\d\.]+)?/(?P<host>[a-zA-Z0-9-\.]+)?"
+        "/(?P<ip>[\d\.]+)?/(?P<host>[ a-zA-Z0-9-_\.]+)?"
```



Error during template rendering

In template /srv/cuckoo/web/templates/analysis/report.html, error at line 9

Reverse for 'analysis.views.moloch' with arguments '()' and keyword arguments '{u'host': u'_VLMCS._TCP'}' not found. 1 pattern(s) tried: ['analysis/moloch/(?P<ip>[\\d\\.]+)?/(?P<host>[a-zA-Z0-9-\\.]+)?/(?P<src_ip>[a-zA-Z0-9\\.]+)?/(?P<src_port>\\d+|None)?/(?P<dst_ip>[a-zA-Z0-9\\.]+)?/(?P<dst_port>\\d+|None)?/(?P<sid>\\d+)?']

```
1  {% extends "base.html" %}
2  {% load staticfiles %}
3  {% load analysis_tags %}
4  {% block content %}
5  <div class="row">
6      <div class="col-md-6"><p style="margin-bottom: 10px;"><img src="{% static "graphic/cuckoo.png" %}" /></p></div>
7      <div class="col-md-6" style="text-align: right;">
8          <a class="btn btn-primary" href="{% url "compare.views.left" analysis.info.id %}">Compare this analysis to...</a>
9          <a class="btn btn-primary" href="{% url "submission.views.resubmit" analysis.info.id %}">Resubmit this sample</a>
10     </div>
11 </div>
12 <ul class="nav nav-tabs">
13     <li class="active"><a href="#overview" data-toggle="tab">Quick Overview</a></li>
14     <li><a href="#static" data-toggle="tab">Static Analysis</a></li>
15     {% if analysis.behavior.processes %}
16         <li><a href="#behavior" data-toggle="tab" id="graph_hook">Behavioral Analysis ({{ analysis.behavior.processes|filter_key_if_has:"track"|length }})</a></li>
17     {% endif %}
18     {% with suricata=analysis.suricata|custom_length:"alerts tls" snort=analysis.snort|custom_length:"alerts" %}
19         {% if analysis.network.http_ex or analysis.network.https_ex %}
```

501 Unsupported Method (‘GET’)

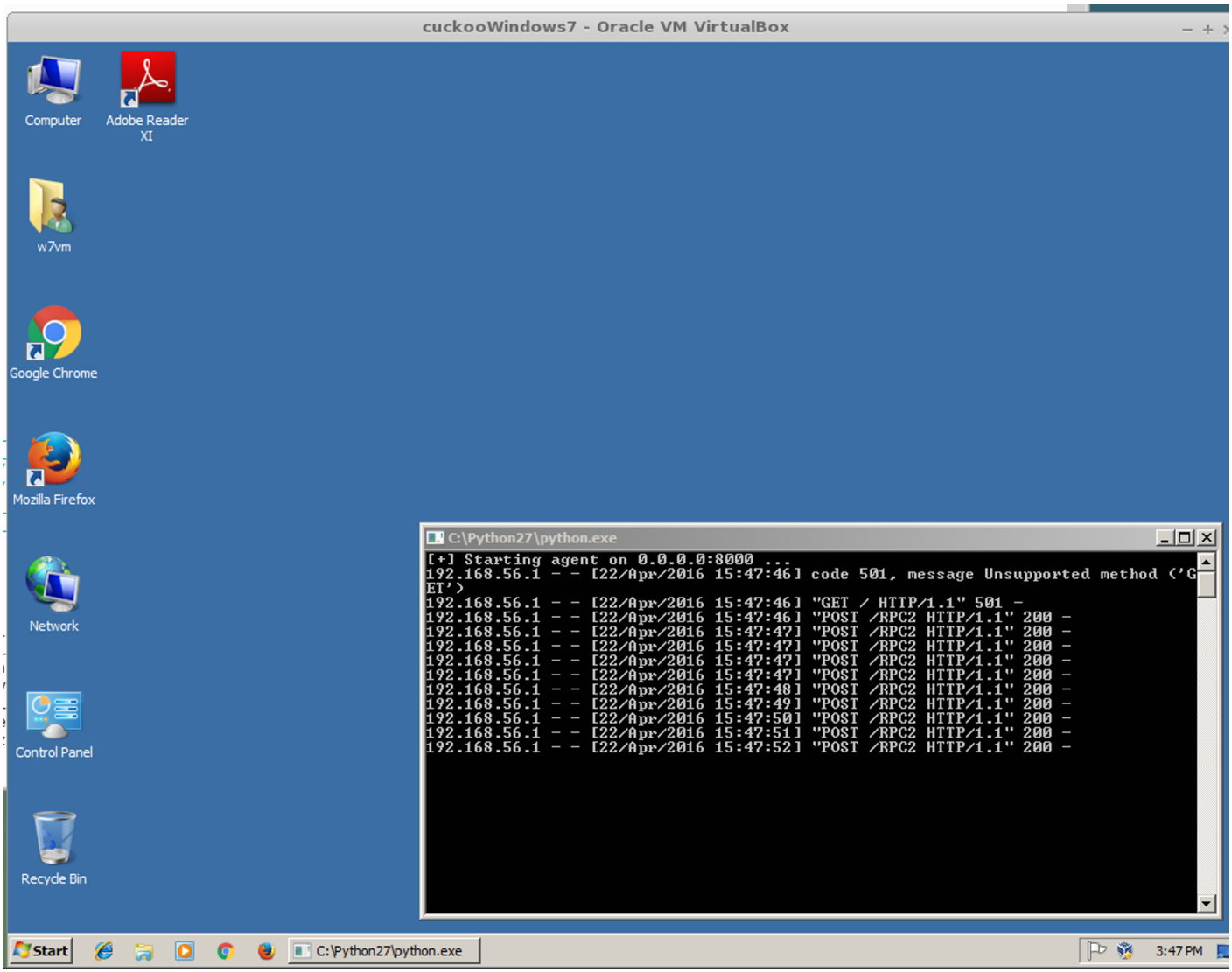
2.0-rc1 sürümünde değiştirildi.

2.0-rc1'den bu yana Cuckoo, Gelişmiş Cuckoo Agent'ını ve yeni bir REST API tabanlı Cuckoo Agent'ını destekler. Bu Agentlar, Konuk ve Ana makine arasında iletişim için kullanılır. Yeni Cuckoo Agent, Cuckoo dışında da kullanılabilme özelliğine sahip bir geliştirilmiş Agent olarak kabul edilir. Örnek olarak, VMCloak tarafından kullanılır ve Otomatik olarak Sanal Makineler oluşturmak, yapılandırmak ve gizlemek için kullanılır.

Cuckoo Host, Cuckoo'nun yeni veya eski Agent ile iletişim kurup kurmadığını belirlemek için kök dizine (/) bir HTTP GET isteği gönderir. Eski Cuckoo Agent, xmlrpc tabanlı olduğu için bu belirli yolun işlenmesini sağlamaz ve bu nedenle bir hata olan 501 Desteklenmeyen yöntem döndürür.

Bununla birlikte, bu mesaj aslında bir hata değildir, sadece Cuckoo'nun hangi sürümdeki Cuckoo Agent ile iletişim kurmaya çalıştığını belirlemeye çalıştığı bir durumdur.

> Yeni bir Cuckoo Agent mevcut olsa da, eski Cuckoo Agent için geriye dönük uyumluluk hala mevcut ve düzgün bir şekilde çalışıyor.


cuckooWindows7 - Oracle VM VirtualBox
Computer
Adobe Reader XI
w7vm
Google Chrome
Mozilla Firefox
Network
Control Panel
Recycle Bin
C:\Python27\python.exe
[+] Starting agent on 0.0.0.0:8000 ...
192.168.56.1 - - [22/Apr/2016 15:47:46] code 501, message Unsupported method ('GET')
192.168.56.1 - - [22/Apr/2016 15:47:46] "GET / HTTP/1.1" 501 -
192.168.56.1 - - [22/Apr/2016 15:47:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [22/Apr/2016 15:47:52] "POST /RPC2 HTTP/1.1" 200 -
Start
C:\Python27\python.exe
3:47 PM

tcpdump Permission Denied hatası

Sürüm 2.0.0'da değiştirildi.

Yeni Cuckoo yapısıyla birlikte, tüm depolama varsayılan olarak `~/.cuckoo` içinde bulunur, bu arada PCAP dosyası, `~/.cuckoo/storage/analyses/task_id/dump.pcap` konumunda saklanır. Ubuntu'da varsayılan olarak etkin olan AppArmor (AppArmor profili) ile dot-dizinlerine ($HOME içinde) yazma izni olmayan tcpdump, izin reddedildiği bir hata mesajı alır ve Cuckoo'nun PCAP dosyalarını yakalamasını engeller.

AppArmor araçlarını yükleyerek ve basitçe tcpdump AppArmor profilini tamamen devre dışı bırakarak çözülebilir:

```
sudo apt-get install apparmor-utils
sudo aa-disable /usr/sbin/tcpdump
```

DistributionNotFound / No distribution matching the version hatası

Sürüm 2.0.0'da değiştirildi.

Cuckoo'yu Python paketi aracılığıyla kurmak, esasen güncel olmayan Python package manager sorunlarına yol açar. Bu SSS girişi, aşağıdaki sorunu hedeflemektedir:

```
$ cuckoo
Traceback (most recent call last):
File "/usr/local/bin/cuckoo", line 5, in <module>
    from pkg_resources import load_entry_point
File "/usr/lib/python2.7/dist-packages/pkg_resources.py", line 2749, in
<module>
    working_set = WorkingSet._build_master()
File "/usr/lib/python2.7/dist-packages/pkg_resources.py", line 446, in
_build_master
    return cls._build_from_requirements(__requires__)
File "/usr/lib/python2.7/dist-packages/pkg_resources.py", line 459, in
_build_from_requirements
    dists = ws.resolve(reqs, Environment())
File "/usr/lib/python2.7/dist-packages/pkg_resources.py", line 628, in resolve
    raise DistributionNotFound(req)
pkg_resources.DistributionNotFound: tlslite-ng==0.6.0a3
```

Bu ve buna benzer sorunlar güncel olmayan Python package manager yazılımından kaynaklanır. Neyse ki bunların düzeltilmesi oldukça basittir ve bu nedenle aşağıdaki komut işe yaramalıdır:

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

IOError: [Errno 24] Too many open files

Bu sorun, çok sayıda bırakılmış dosyası olan örnekleri analiz ederken karşılaşılabilecek bir sorundur, bu kadar çok dosya ki İşleme Yardımcısı artık yeni dosya tanımlayamaz hale gelir.

Bu sorunun en kolay çözümü, mevcut kullanıcı için dosya tanımlama sınırlarını artırmaktır. Bu işlemi buradaki yolu izleyerek yapabilirsiniz.

Open Files Sınırını Arttırmak Yazısını İnceleyin

Eğer Supervisor kullanıyorsanız, `supervisord.conf` dosyasında `minfds`'yi ayarlamayı unutmayın.

Değişikliklerin etkili olabilmesi için genellikle önce oturumu kapatmanız (yani çıkış yapmanız) ve ardından yeni bir kabuk oturumu açmanız gerektiğini unutmayın.

Open Files Sınırını Arttırmak

Eğer 'Too many open files (24)' hatası alıyorsanız, application/command/script Linux tarafından izin verilen maksimum açık dosya sınırına ulaşıyor demektir. Aşağıdaki gibi açık dosya sınırını artırmanız gerekecek:

Limiti Arttırmak

Per User Limit

/etc/security/limits.conf dosyasını açın ve aşağıdaki kısmı yapıştırın:

```
*         hard    nofile      500000
*         soft    nofile      500000
root      hard    nofile      500000
root      soft    nofile      500000
```

Dosyayı kaydettikten sonra sisteme çıkış yapın ve tekrar giriş yapın.

pam-limits

Sınırın daemon işlemleri için değiştirilmesi için ek bir adım gerekebilir. Buna ihtiyaç duymayabilirsiniz, ancak yukarıdaki değişiklikler sizin için işe yaramazsa, bu yolu denemeyi düşünebilirsiniz.

/etc/pam.d/common-session dosyasını açın ve aşağıdaki satırı ekleyin:

```
session required pam_limits.so
```

System-Wide Limit

Değeri yukarıda belirlenen kullanıcı sınırından daha yüksek bir şekilde ayarlayabilirsiniz.

/etc/sysctl.conf dosyasını açın ve aşağıdaki satırı ekleyin:

```
fs.file-max = 2097152
```

Sonrasında aşağıdaki komutu çalıştırın:

```
sysctl -p
```

Yukarıdaki işlem, sistem genelinde açık kalabilen toplam dosya sayısını artırır.

Yeni Limit Belirlemek

Dosya tanımlarının maksimum sınırını görmek için aşağıdaki komutu kullanın:

```
cat /proc/sys/fs/file-max
```

Hard Limit:

```
ulimit -Hn
```

Soft Limit:

```
ulimit -Sn
```

Eğer root kullanıcı ile giriş yaptıysanız:

Diğer kullanıcılar için limiti görmek

Sadece `www-data` yerine kontrol etmek istediğiniz Linux kullanıcı adınızı (username) yazarak değiştirin:

```
su - www-data -c 'ulimit -aHS' -s '/bin/bash'
```

Çalışan process’in limitini görmek

Process id’yi (PID) öğrenmek için:

```
```

```
ps aux | grep process-name
```

XXX PID'dir, buna göre limitleri kontrol etmek için aşağıdaki komutu çalıştırın:

```
cat /proc/XXX/limits
```

pkg_resources.ContextualVersionConflict

Eğer Cuckoo Paketi kuruyorsanız veya güncelliyorsanız, aşağıdaki gibi bir hata alabilirsiniz:

```
pkg_resources.ContextualVersionConflict: (HTTPReplay 0.1.5
(/usr/local/lib/python2.7/dist-packages),
Requirement.parse('HTTPReplay==0.1.17'), set(['Cuckoo']))
```

Bu sorunun kaynağı ilgili pip bağımlılıklarının güncel sürümlerinin değil de eski sürümlerinin yüklenmiş olmasıdır.

Bu sorunu çözmenin en kolay yolu, ilgili bağımlılığın tüm sürümlerini kaldırmak ve Cuckoo'yu yeniden yüklemektir. Aşağıda sunulan HTTPReplay örneğinde, işlem şöyle görünebilir:

```
$ sudo pip uninstall httpreplay
Uninstalling HTTPReplay-0.1.17:
/usr/local/bin/httpreplay
/usr/local/bin/pcap2mitm
/usr/local/lib/python2.7/dist-packages/HTTPReplay-0.1.17-py2.7.egg-info
...
Proceed (y/n)? y
Successfully uninstalled HTTPReplay-0.1.17

$ sudo pip uninstall httpreplay
Uninstalling HTTPReplay-0.1.5:
/usr/local/lib/python2.7/dist-packages/HTTPReplay-0.1.5-py2.7.egg-info
Proceed (y/n)? y
Successfully uninstalled HTTPReplay-0.1.5

$ sudo pip uninstall httpreplay
Cannot uninstall requirement httpreplay, not installed
```

Sonrasında Cuckoo'yu yeniden yüklemek için basitçe `pip install -U cuckoo` komutunu kullanabilirsiniz.

Sorun Giderme

ValueError: incomplete format key hatası

Bu sorun, $CWD/conf içindeki ayarları değiştirdikten sonra runtime anında ortaya çıkabilir, çünkü input, runtime sırasında kaçırılmadan configuration parser’a iletilir. Yapılandırma dosyalarınızı, olası sorunlu karakter kombinasyonlarına (örneğin %() gibi) karşı kontrol ederken dikkatli bir şekilde gözden geçirmeniz önemlidir.

Sanal makine (VM) ağ yapılandırması sorunu

Sanal Makinenizin ağ yapılandırması beklenildiği gibi çalışmıyorsa, Cuckoo analizlerini bu şekilde kullanamayacağınıza dair bir bildirim alacaksınız. Ağ yapılandırması ve/veya kurulumunuzun neden yanlış olduğuyla ilgili birçok olasılık vardır. Bununla birlikte, genellikle sorun aşağıdaki nedenlerden birinde bulunur:

1. Sanal makinenin IP adresi yanlış yapılandırılmış olabilir. Lütfen VM'in sabit bir IP adresine sahip olduğundan, bu IP adresinin Cuckoo yapılandırması ile eşleştiğinden ve yapılandırılmış ağ arabiriminin var ve aktif olduğundan emin olun. Ayrıca, VirtualBox kullanıyorsanız, ağ arabirimini `Host-Only` arabirim olarak yapılandırdığınızdan emin olun.
2. Ana Makine ve Konuk arasındaki iletişimi engelleyen bir güvenlik duvarının olmadığından ve Ana Makine ile Konuk'un birbirlerine ping atabildiğinden ve birbirlerine bağlanabildiğinden emin olun.
3. Cuckoo Ana Makine'den Konuk'a bağlantılar çalışıyorsa, ancak ters yönde çalışmıyorsa, bazı ek sorunlar olabilir:
   - Ana Makine ve Konuk üzerinde ağ yapılandırması eşit mi? Değilse, örneğin VM farklı IP aralıklarını görüyorsa, `resultserver_ip` ve `resultserver_port`'u yapılandırmanız gerekebilir.
   - Eğer Cuckoo Analyzer'ı (genellikle `$CWD/analyzer` klasöründe bulunur) değiştirdiyseniz, bu hata mesajı, bir sözdizimi hatası veya başka bir istisna eklenmiş olabileceğini, Analyzer'ın düzgün başlatılamamasına ve dolayısıyla beklenildiği gibi analiz yapamamasına işaret edebilir.