Per-Analysis Network Routing Ayarları

Bir ağ arayüzü üzerinden analizleri yönlendirmenin old school yöntemini tartıştıktan sonra, şimdi çok daha ayrıntılı ağ yönlendirmesine izin veren dinamik ağ yönlendirme bileşenlerini inceleyeceğiz.

Dokümantasyonun bu bölümünün girişinde belirtildiği gibi, Cuckoo 2.0-rc1'den itibaren, Cuckoo Rooter tanıtıldığında, per-analysis network routing yapmak mümkün olmuştur. O zamandan beri çeşitli hatalar çözülmüş ve daha fazla ağ yönlendirme seçeneği eklenmiştir.

Aşağıda mevcut yönlendirme seçeneklerinin bir listesi bulunmaktadır.

Routing Seçeneği	Açıklama
None Routing	Hiçbir yönlendirme yapılmaz, Cuckoo Rooter'ın çalıştırılmasını gerektirmeyen (ve bu nedenle aynı zamanda varsayılan yönlendirme seçeneği olan) tek seçenek.
Drop Routing	Tüm Cuckoo trafiğini, VM'lerin alt ağındaki trafiği de içeren tüm trafiği tamamen engeller.
Internet Routing	Verilen ağ arayüzü tarafından sağlanan tam internet erişimi (Basit Global Routing kurulumuna benzer).
InetSim Routing	Tüm trafiği, ana makinede çalışan sahte hizmetler sağlayan bir InetSim örneğine yönlendirir.
Tor Routing	Tüm trafiği Tor üzerinden yönlendirir.
VPN Routing	Tüm trafiği belki de çoklu önceden tanımlanmış VPN uç noktalarından biri üzerinden yönlendirir.

None Routing

Cuckoo'nun üçüncü taraf tarafından tanımlanan şekilde analizi yönlendirmesine izin veren anlamda varsayılan yönlendirme mekanizması. Yani, gerçekten hiçbir şey yapmaz. Bir kişi, None Routing'i Basit Global Routing ile birlikte kullanabilir.

Drop Routing

Drop routing seçeneği, temelde hiçbir global `iptables` kuralı oluşturulmamış bir makinede (VM'lere tam internet erişimi sağlayan veya benzeri) varsayılan None Routing kurulumuna biraz

benzemektedir, ancak VM'lere sağlanan internet erişimini etkin bir şekilde kapatmak konusunda çok daha agresiftir.

Drop routing ile mümkün olan tek trafik içsel Cuckoo trafiğidir ve bu nedenle DNS istekleri veya çıkış `TCP/IP` bağlantıları engellenir.

Internet Routing

İnternet yönlendirmeyi kullanarak, VM'lere bağlı ağ arayüzlerinden biri aracılığıyla tam internet erişimi sağlanabilir. Bu seçeneği, tüm potansiyel olarak kötü amaçlı örneklerin aynı yükseltici üzerinden internete bağlanmasına izin verdiği doğası nedeniyle kirli hat olarak da adlandırıyoruz.

> Kirli hat ağ arayüzünü, iproute2 ile açıklandığı gibi kaydetmek gerekmektedir.

InetSim Routing

InetSim hakkında bilgi sahibi olmayanlar için, InetSim, kötü amaçlı yazılımların iletişim kurması için sahte hizmetler sağlayan bir projedir. InetSim yönlendirmesini kullanmak için, InetSim'i ana makinede (veya ayrı bir VM'de) kurmanız ve Cuckoo'yu, InetSim sunucusunu nerede bulacağını bilmesi için yapılandırmanız gerekecektir.

InetSim için yapılandırma kendinden açıklamalıdır ve `$CWD/conf/routing.conf` yapılandırma dosyasının bir parçası olarak bulunabilir:

```
[inetsim]
enabled = yes
server = 192.168.56.1
```

InetSim ile hızlı bir başlangıç yapmak için REMnux dağıtımının en son sürümünü indirmek mümkündür; bu dağıtım, birçok diğer aracın yanı sıra InetSim'in en son sürümünü içermektedir. Bu VM'nin doğal olarak kendi sabit IP adresine ihtiyacı olacak ve ardından bu adres, `routing.conf` yapılandırma dosyasında yapılandırılmalıdır.

Tor Routing

> Tor'un kötü amaçlı yazılım analizi için kullanılması kesinlikle tavsiye edilmiyor.

Öncelikle Tor'un kurulması gerekmektedir. Tor'un en son kararlı sürümünü yüklemek için buradaki talimatları bulabilirsiniz.

Ardından Tor yapılandırma dosyasını değiştirmemiz gerekecek (Henüz Cuckoo'nun Tor için yapılandırması hakkında konuşmuyoruz!). Bunun için, Tor'a TCP/IP bağlantıları ve UDP istekleri için

dinleme adresi ve bağlantı noktasını sağlamamız gerekecek. Varsayılan bir VirtualBox kurulumunda, ana makinenin IP adresi 192.168.56.1 ise, aşağıdaki satırlar /etc/tor/torrc dosyasında yapılandırılmalıdır:

```
TransPort 192.168.56.1:9040
DNSPort 192.168.56.1:5353
```

Tor'u yeniden başlatmayı unutmayın (`/etc/init.d/tor restart`).Bu bizi Cuckoo için Tor yapılandırmasıyla bırakır, bu dosya $CWD/conf/routing.conf dosyasında bulunabilir:

```
[tor]
enabled = yes
dnsport = 5353
proxyport = 9040
```

Unutulmaması gereken bir nokta, `/etc/tor/torrc` ve `$CWD/conf/routing.conf` dosyalarındaki bağlantı noktası numaralarının, ikisinin de doğru şekilde etkileşimde bulunabilmesi için eşleşmesi gerektiğidir.

VPN Routing

Son olarak, analizleri bir dizi VPN üzerinden yönlendirmek mümkündür. Birkaç farklı ülkede sona eren birkaç VPN tanımlayarak, potansiyel olarak kötü amaçlı örneklerin IP adresinin ülkesine bağlı olarak farklı davranıp davranmadığını görmek mümkün olabilir.

VPN için yapılandırma, bir VM'nin yapılandırması gibi. Her VPN için `$CWD/conf/routing.conf` yapılandırma dosyasında ilgili bilgileri detaylandıran bir bölüme ihtiyacınız olacak. Yapılandırmada VPN, mevcut VPN'lerin listesine kaydedilmelidir (tam olarak daha fazla VM kaydetmek için yapacağınız gibi).

Tek bir VPN için yapılandırma yaklaşık olarak aşağıdaki gibi görünür:

```
[vpn]
# Are VPNs enabled?
enabled = yes

# Comma-separated list of the available VPNs.
vpns = vpn0
```

```
[vpn0]
# Name of this VPN. The name is represented by the filepath to the
# configuration file, e.g., cuckoo would represent /etc/openvpn/cuckoo.conf
# Note that you can't assign the names "none" and "internet" as those would
# conflict with the routing section in cuckoo.conf.
name = vpn0

# The description of this VPN which will be displayed in the web interface.
# Can be used to for example describe the country where this VPN ends up.
description = Spain, Europe

# The tun device hardcoded for this VPN. Each VPN *must* be configured to use
# a hardcoded/persistent tun device by explicitly adding the line "dev tunX"
# to its configuration (e.g., /etc/openvpn/vpn1.conf) where X in tunX is a
# unique number between 0 and your lucky number of choice.
interface = tun0

# Routing table name/id for this VPN. If table name is used it *must* be
# added to /etc/iproute2/rt_tables as "<id> <name>" line (e.g., "201 tun0").
# ID and name must be unique across the system (refer /etc/iproute2/rt_tables
# for existing names and IDs).
rt_table = tun0
```

Her VPN ağ arayüzünü, iproute2 ile açıklandığı gibi kaydetmek gerekmektedir.

Revision #3
Created 25 December 2023 09:12:41 by Ertan Sözer
Updated 25 December 2023 09:21:10 by Ertan Sözer