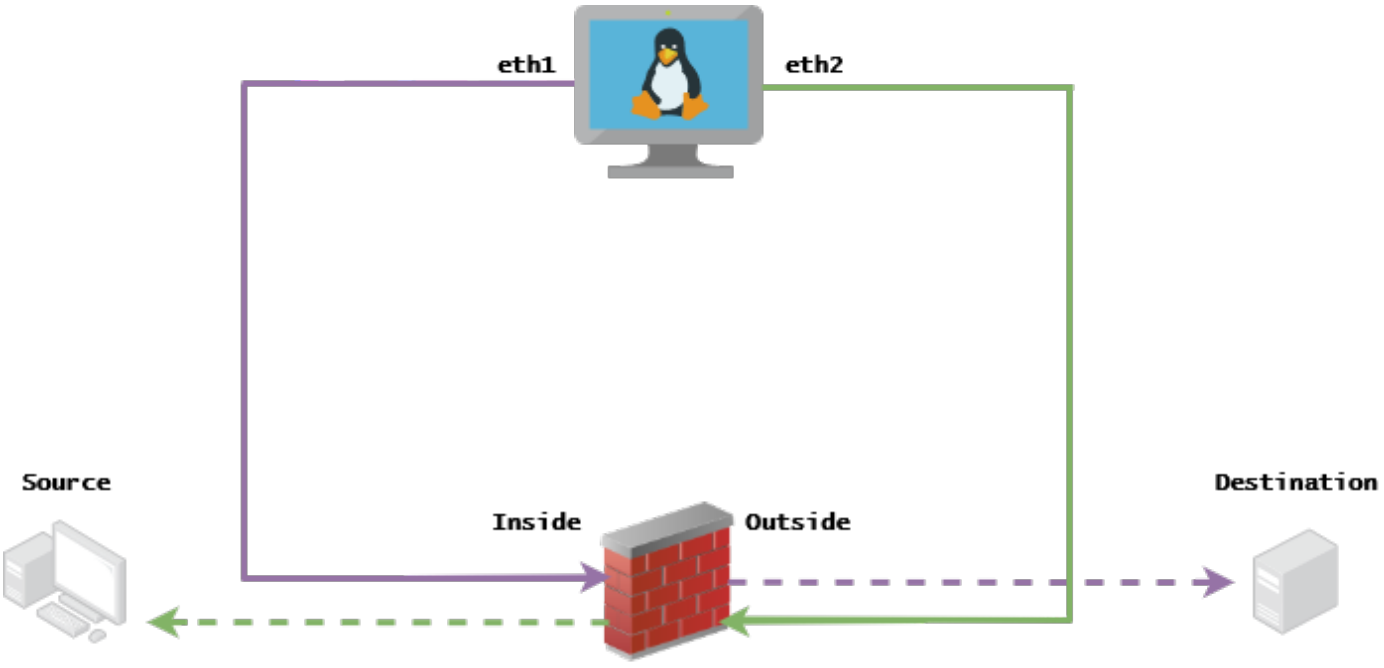
在Kali Linux上使用2个NIC配置TCP重播

目录

简介

本文档介绍如何使用TCP重播来重放数据包捕获工具保存的PCAP文件中的网络流量。

拓扑



必备条件

- 具有Kali Linux和两个NIC的VM
- FTD（最好由FMC管理）
- Linux运行命令的知识。

背景信息

TCP重播是一个用于重放数据包捕获工具（如wireshark或TCPdump）保存的pcap文件中的网络流量的工具。在需要复制流量以测试网络设备上的结果的情况下，它可能会非常有用。

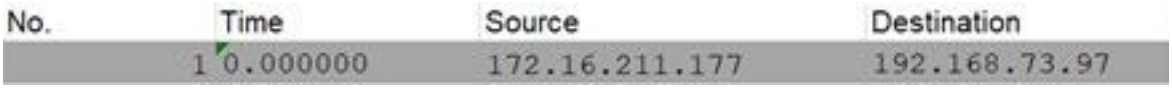
TCP重播的基本操作是以记录数据包的速度或指定的数据速率重新发送来自输入文件的所有数据包，其速度最高可达硬件所能支持的速度。

执行此过程还有其他方法，但本文的目的是实现TCP重放，而不需要中间路由器。

实现

FTD配置：

1.使用数据包捕获上同一网段上的IP配置内部/外部接口：



No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **源：**172.16.211.177
- **目的地：**192.168.73.97

FMC > Devices > Device Management > Interfaces > Edit each interface

提示：最佳做法是将每个接口分配到不同的VLAN中，以保持流量隔离。

Running-config（示例）

```
interface Ethernet1/1
 nameif Outside
 ip address 192.168.73.34 255.255.255.0
!
interface Ethernet1/2
 nameif Inside
 security-level 0
 ip address 172.16.211.34 255.255.255.0
```

2.配置从主机到其网关的静态路由和伪造ARP条目，因为这些网关不存在。

FMC > Devices > Device Management > Routes > Select your FTD > Routing > Static Route > Add Route

Running-config（示例）

```
route Inside 172.16.211.177 172.16.211.100 1
route Outside 192.168.73.97 192.168.73.100 1
```

使用LinaConfigTool后门配置虚假ARP条目：

1. 登录FTD CLI
2. 转到专家模式
3. 提升您的权限(sudo su)

LinaConfigTool配置示例

```
/usr/local/sf/bin/LinaConfigTool "arp Inside 172.16.211.100 dead.deed.deed"
/usr/local/sf/bin/LinaConfigTool "arp Outside 192.168.73.100 dead.deed.deed"
/usr/local/sf/bin/LinaConfigTool "write mem"
```

3.禁用“等于”序列号随机化。

1. 创建扩展访问列表： **Go to FMC > Objects > Access List > Extended > Add Extended Access List**使用参数“allow any”创建ACL
2. 禁用序列号随机化： **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**添加规则并选择 **Global** 选择您之前创建的 **Extended ACL**取消选中 **Randomize TCP Sequence Number**

running-config

```
policy-map global_policy
class class-default
set connection random-sequence-number disable
```

Linux配置：

1. 为每个接口配置IP（这取决于接口属于内部子网和外部子网） ifconfig ethX <ip_address> netmask <mask> 示例：ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. （可选）将每个接口配置为不同的VLAN
3. 将PCAP文件传输到Kali Linux服务器（您可以通过tcpdump获取pcap文件，在FTD上进行捕获等）
4. 使用tcpprep创建TCP重播缓存文**件** tcpprep -i input_file -o input_cache -c server_ip/32 示例：tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. 使用tcprewrite重写MAC地**址** tcprewrite -i input_file -o output_file -c input_cache -C —enet-dmac=<ftd_server_interface_mac>,<ftd_client_interface_mac>
   示例：tcprewrite -i stream.pcap -o stream.pcap.replay -c stream.cache -C —enet-dmac=00:50:56:b3:81:35,00:50:56:b3:63:f4
6. 将NIC连接到ASA/FTD
7. 使用tcpreplay重播该**流** tcpreplay -c input_cache -i <nic_server_interface> -I <nic_client_interface> output_file
   示例：tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

验证

在FTD上创建数据包捕获，以测试数据包是否到达您的接口：

1. 在内部接口上创建数据包捕获 cap i interface Inside trace match ip any any
2. 在外部接口上创建数据包捕获 cap o interface Outside trace match ip any any

运行tcpreplay并验证数据包是否到达您的接口：

示例 情景

```
firepower# show cap
capture i type raw-data trace interface Inside interface Outside [Capturing - 13106 bytes]
match ip any any
capture o type raw-data trace interface Outside [Capturing - 11348 bytes]
match ip any any
firepower# show cap i
```

```
47 packets captured

1: 00:03:53.657299 172.16.211.177.23725 > 192.168.73.97.443: S 1610809777:1610809777(0) win 8192
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。