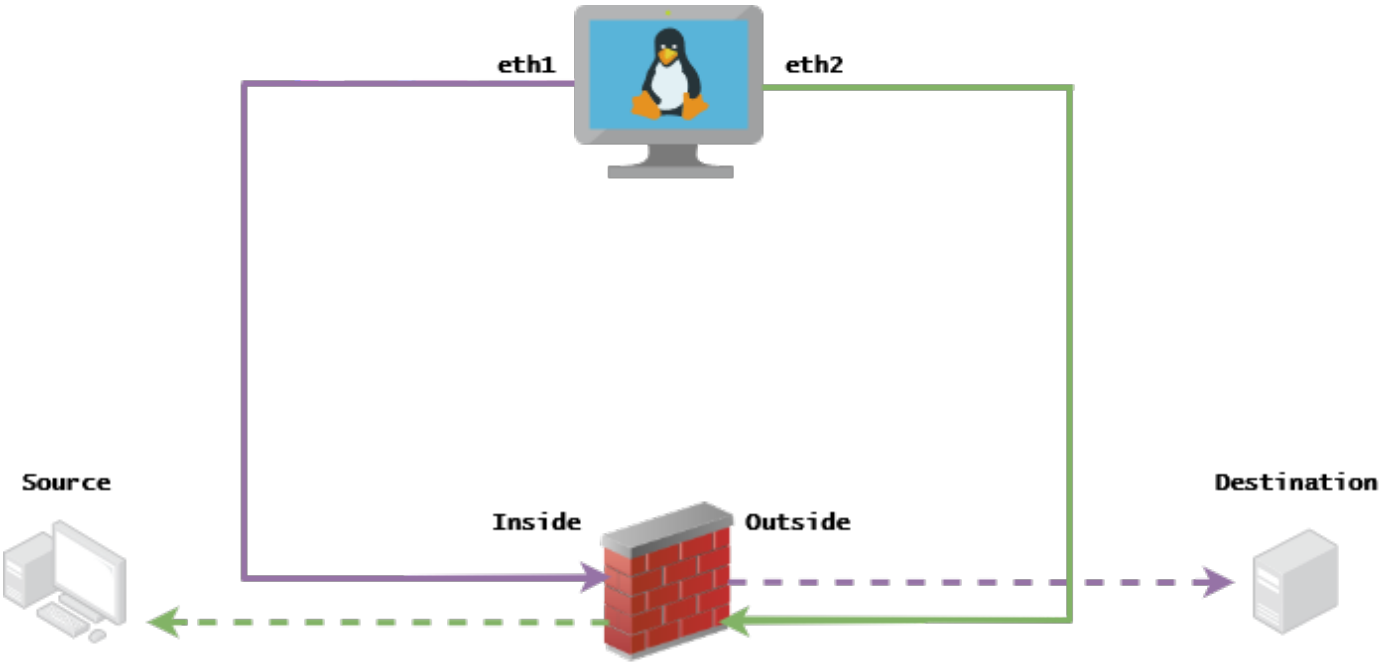
在Kali Linux上使用2個NIC配置TCP重播

目錄

簡介

本文檔介紹使用TCP重播來重放資料包捕獲工具儲存的PCAP檔案的網路流量。

拓撲



必要條件

- 具有Kali Linux和兩個NIC的虛擬機器
- FTD（最好由FMC管理）
- Linux運行命令的知識。

背景資訊

TCP重播是用於重播來自資料包捕獲工具（如wireshark或TCPdump）儲存的pcap檔案的網路流量的工具。在需要複製流量以測試網路裝置上的結果的情況下，它可能會很有用。

TCP重播的基本操作是從輸入檔案重新傳送所有資料包，其速度為記錄速度或指定資料速率，最高為硬體所能提供的速度。

執行此過程還有其它方法，但本文的目的是實現TCP重放，而無需中間路由器。

實現

FTD組態：

1.使用資料包捕獲上同一網段上的IP配置內部/外部介面：

No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **來源**:172.16.211.177
- **目**的地：192.168.73.97

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

提示：最佳實踐是將每個介面分配到不同的VLAN中，以使流量保持隔離。

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.配置從主機到其網關的靜態路由和偽造ARP條目，因為這些網關不存在。

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後門配置虛假ARP條目：

1. 登入FTD CLI
2. 轉到專家模式
3. 提升您的許可權(sudo su)

LinaConfigTool組態範例

```
/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equals序列號隨機化。

1. 建立延伸存取清單： **Go to FMC > Objects > Access List > Extended > Add Extended Access List**使用引數「allow any」建立ACL
2. 禁用序列號隨機化： **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**新增規則並選擇 **Global** 選擇您先前建立的 **Extended ACL**取消選中 **Randomize TCP Sequence Number**

Running-config

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

Linux配置：

1. 為每個介面配置IP（這取決於哪個介面屬於內部子網和外部子網） ifconfig ethX <ip_address> netmask <mask> 示例： ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. （可選）將每個介面配置為不同的VLAN
3. 將PCAP檔案傳輸到Kali Linux伺服器（您可以使用tcpdump獲取pcap檔案，在FTD上獲取捕獲等）
4. 使用tcpprep建立TCP重放快取文**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重寫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. 將NIC連線到ASA/FTD
7. 使用tcpreplay重播該**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

驗證

在FTD上建立封包擷取，以測試是否封包到達您的介面：

1. 在Inside介面上建立資料包捕獲 cap i interface Inside trace match ip any any
2. 在外部介面上建立資料包捕獲 cap o interface Outside trace match ip any

執行播放，並驗證封包是否到達您的介面：

範例案例

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。