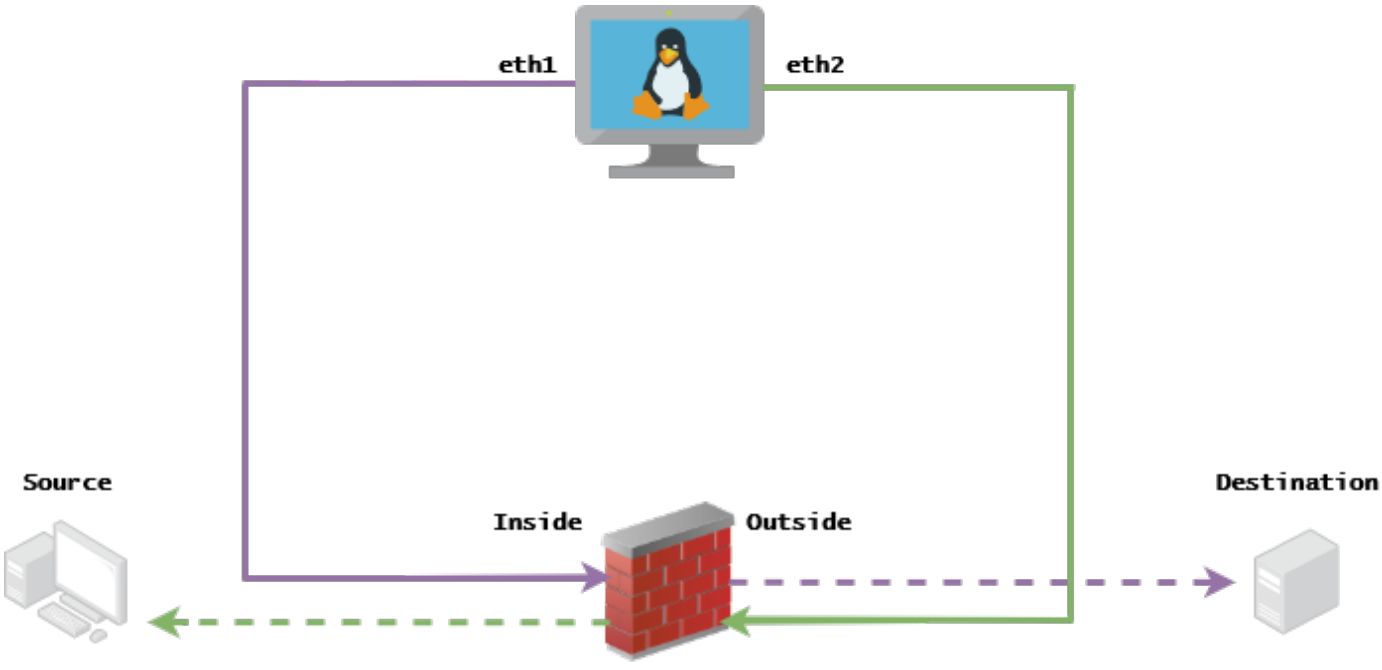
Configurazione di TCP Replay con 2 NIC su Kali Linux

Sommario

Introduzione

In questo documento viene descritto TCP Replay per riprodurre il traffico di rete dai file PCAP salvati con gli strumenti di acquisizione pacchetti.

Topologia



Requisiti

- VM con Kali Linux e due NIC
- FTD (di preferenza gestito dal CCP)
- Conoscenze di Linux per l'esecuzione dei comandi.

Premesse

Ripetizione TCPè uno strumento utilizzato per riprodurre il traffico di rete da file pcap salvati con strumenti di acquisizione pacchetti come wireshark o TCPdump. Può essere utile in situazioni in cui è necessario replicare il traffico per verificare il risultato sui dispositivi di rete.

L'operazione di base di TCP Replay consiste nel inviare nuovamente tutti i pacchetti dai file di input alla velocità a cui sono stati registrati, o a una velocità dati specificata, fino alla massima velocità consentita dall'hardware.

Esistono altri metodi per eseguire questa procedura, tuttavia lo scopo di questo articolo è quello di ottenere la riproduzione TCP senza la necessità di un router intermedio.

Implementazione

Configurazione FTD:

1. Configurare le interfacce interno/esterno con un indirizzo IP sullo stesso segmento che si trova sulle clip del pacchetto:

No.	Time	Source	Destination
1	0.000000	172.16.211.177	192.168.73.97

- **Fonte:** 172.16.211.177
- **Destinazione**: 192.168.73.97

FMC > Dispositivi > Gestione dispositivi > Interfacce > Modifica ciascuna interfaccia

> **Suggerimento**: è buona norma assegnare ciascuna interfaccia a una VLAN diversa per mantenere il traffico isolato.

Running-config (esempio)

```
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. Configurare le route statiche tra gli host e i relativi gateway e le voci ARP false per tali gateway, in quanto non esistono.

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

Running-config (esempio)

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

Utilizzare la backdoor LinaConfigTool per configurare le voci ARP false:

1. Accesso alla CLI FTD
2. Passa alla modalità esperto
3. Elevare i privilegi (sudo su)

Esempio di configurazione di LinaConfigTool

```
/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. Disattivare la randomizzazione del numero di sequenza uguale a.

1. Creare un elenco degli accessi estesi: **Go to FMC > Objects > Access List > Extended > Add Extended Access List**Creare l'ACL con i parametri "allow any" (consenti qualsiasi)
2. Disattiva l'assegnazione casuale dei numeri di sequenza: **Go to FMC > Policies > Access Control > Select your ACP > Advanced > Threat Defense Service Policy**Aggiungi regola e seleziona **Global**
   Selezionare il file creato in precedenza **Extended ACL**Deseleziona **Randomize TCP Sequence Number**

Running-config

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

Configurazione Linux:

1. Configurare l'indirizzo IP per ogni interfaccia (in base all'appartenenza dell'interfaccia alla subnet interna e a quella esterna) ifconfig ethX <indirizzo_ip> netmask <maschera>
   esempio: ifconfig eth1 172.16.211.35 netmask 255.255.255.0
2. (Facoltativo) Configurare ciascuna interfaccia in una VLAN diversa
3. Trasferire il file PCAP nel server Kali Linux (è possibile ottenere il file pcap con tcpdump, acquisizioni su FTD, ecc.)
4. Creare un file della cache di riproduzione TCP con **tcpprep** tcpprep -i file_input -o cache_input -c ip_server/32 esempio: tcpprep -i stream.pcap -o stream.cache -c 192.168.73.97/32
5. Riscrivere gli indirizzi MAC con **tcprewrite** tcprewrite -i file_input -o file_output -c cache_input -C —enet-dmac=<mac_interfaccia_server_ftd>,<mac_interfaccia_client_ftd>
   esempio: 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. Collegamento delle schede NIC all'ASA/FTD
7. Riprodurre il flusso con **tcpreplay** tcpreplay -c cache_input -i <interfaccia_server_nic> -I <interfaccia_client_nic> file_output
   esempio: tcpreplay -c stream.cache -i eth2 -I eth1 stream.pcap.replay

Convalida

Creare le acquisizioni dei pacchetti sull'FTD per verificare se i pacchetti che arrivano all'interfaccia sono:

1. Crea acquisizione pacchetti sull'interfaccia interna cap i interface All'interno di trace match ip any any
2. Crea acquisizione pacchetto sull'interfaccia esterna cap o interfaccia Outside trace match ip any

Eseguire il comando tcpreplay e verificare che i pacchetti arrivino all'interfaccia:

Scenario di esempio

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).