Hi Cristopher,

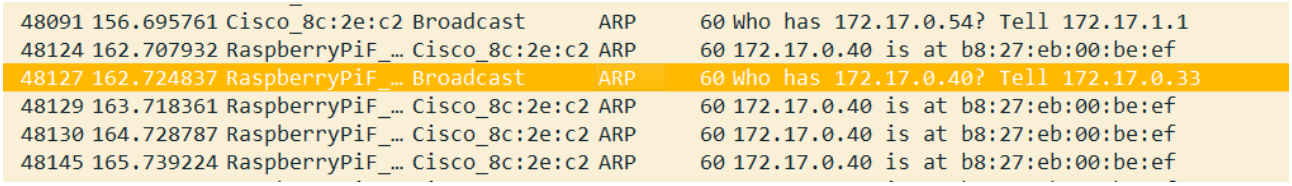
After examining the capture file, we detected ARP spoofing in your network. The attacker used a Raspberry Pi device to impersonate Peter Sunshine's IP address (IP hijacking) and thus carried out a Man-in-the-Middle attack.

As a result, the attacker saw Peter's traffic to the archive server and copied the offer file that Peter was viewing for themselves. The attacker's device left the network after Peter left the archive server, and Peter's correct MAC address returned to the ARP table.

It was nice to be at the service of your company, HaiTek Company Ltd.

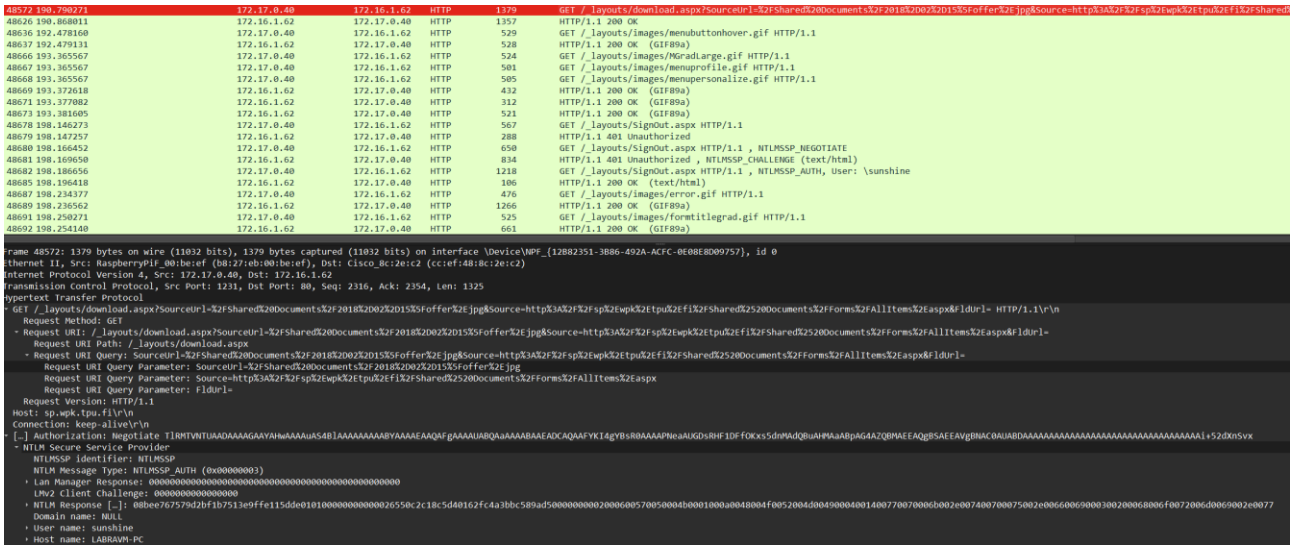
Best regards,

RH, KK



48091	156.695761	Cisco_8c:2e:c2	Broadcast	ARP	60	Who has 172.17.0.54? Tell 172.17.1.1
48124	162.707932	RaspberryPiF_…	Cisco_8c:2e:c2	ARP	60	172.17.0.40 is at b8:27:eb:00:be:ef
48127	162.724837	RaspberryPiF_…	Broadcast	ARP	60	Who has 172.17.0.40? Tell 172.17.0.33
48129	163.718361	RaspberryPiF_…	Cisco_8c:2e:c2	ARP	60	172.17.0.40 is at b8:27:eb:00:be:ef
48130	164.728787	RaspberryPiF_…	Cisco_8c:2e:c2	ARP	60	172.17.0.40 is at b8:27:eb:00:be:ef
48145	165.739224	RaspberryPiF_…	Cisco_8c:2e:c2	ARP	60	172.17.0.40 is at b8:27:eb:00:be:ef

The ARP table shows that Peter Sunshine's IP address (172.17.0.40) appears with two different MAC addresses simultaneously (ARP spoofing).



Peter Sunshine opens the offer file from the archive server. The same traffic is also routed to the attacker's Raspberry Pi device, which thus receives a copy of the file.

```
RaspberryPiF_00:be:ef  Cisco_8c:2e:c2 ARP          60         172.17.0.40 is at b8:27:eb:00:be:ef
RaspberryPiF_00:be:ef  Cisco_8c:2e:c2 ARP          60         172.17.0.40 is at 00:15:5d:38:01:02
RaspberryPiF_00:be:ef  Cisco_8c:2e:c2 ARP          60         172.17.0.40 is at 00:15:5d:38:01:02
RaspberryPiF_00:be:ef  Cisco_8c:2e:c2 ARP          60         172.17.0.40 is at 00:15:5d:38:01:02
```

After the attack ends, the Raspberry Pi leaves the network and Peter Sunshine's correct device returns to the ARP table.