Author: Phi Rapacz

EXECUTION

a) Kali MAC address: 8a:19:13:ec:b0:35
b) Kali IP address: 192.168.64.2
c) Metasploitable MAC address: a6:c8:5d:68:f3:01
d) Metasploitable IP address: 192.168.64.3
e) Kali routing table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
0.0.0.0         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f) Kali arp cache:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   3e:a6:f6:05:ba:64   C                     eth0
```

g) Metasploitable routing table:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
```

h) Metasploitable routing table: (currently empty)
i) 192.168.46.1, based on my pattern recognition. This is, I believe, the Eduroam router.
j) I do get an http response in Metasploitable; I do not see any packets in wireshark.
k) -
l) Metasploitable's new arp cache

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   8A:19:13:EC:B0:35   C                     eth0
192.168.64.2             ether   8A:19:13:EC:B0:35   C                     eth0
```

m) I would assume that it will send it to the one it thinks has the connection it needs based on its cache, Kali's.
n) -
o) I do see an http response on Metasploitable, and I see the packets in Wireshark. Seems like they exchanged a handshake, an HTTP GET and an HTTP response, along with a 'keep alive' request.
p) Kali is consistently sending out ARP responses to Metasploitable that its IP is the next jump to get to Eduroam's IP, without Metasploitable asking.
q) Well, considering I didn't have an arp cache in Metasploitable before Kali sent stuff out to it, I think I'd keep an eye out for un-prompted ARP responses, ARP response "spamming", and also different next hop addresses with the same HW addresses.

SYNTHESIS

Mal basically sets up a fake “shortcut” to the destination before the victim ever even asks for it, meaning that there’s basically no chance for the destination to send out directions over the true fastest route, because it’s never asked to. As far as I understand, the victim never sends an ARP request to prompt the shortest path, because as far as they are concerned they don’t need to - they already have a way to get there (the one Mal gave them), so why waste time trying to find another one?

From Alice’s perspective, this could be detectable. Perhaps the first time she wants to go somewhere, she sends an ARP request out no matter what, regardless if one has appeared in her cache, to check that it’s the same. Maybe she monitors it manually like we have, and keeps a lookout for warning signs, like some in E, q) above.

From Bob’s perspective, nothing odd is happening. He’s just getting a normal connection, as far as he’s concerned. He has no idea there is an Alice - there’s just a Mal (whose intent he is unaware of).

If the connection were over HTTPS, AITM attacks should be detectable because of signature anomalies. Basically, what Bob would send to Alice and what Mal sends to Alice pretending to be Bob would be unavoidably different, assuming everything is working properly.