ARP Spoofing

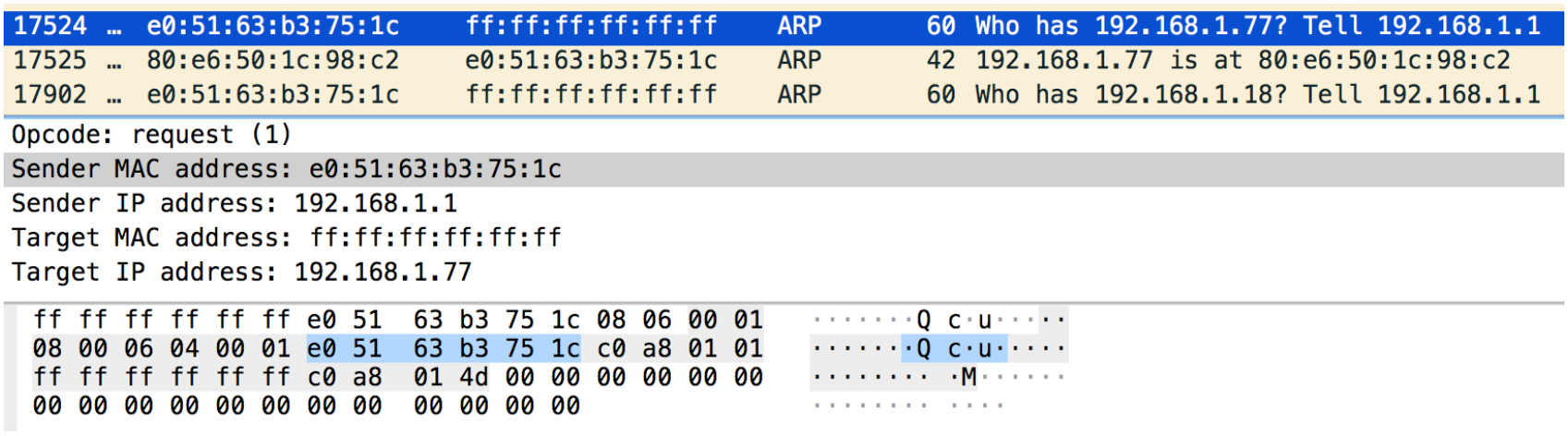
Elias Hernandis

mayo de 2019

ARP spoofing: description, implementation and mitigation of an ARP-based impersonation attack

ARP: Address Resolution Protocol

- ARP-Request: `Who-has 192.168.4.20? Tell 192.168.1.1?`
- ARP-Response: `192.168.4.20 is at f0:f3:e4:c2:01:b3`



ARP packets

Internet Protocol (IPv4) over Ethernet ARP packet

Octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	