

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

17524	...	e0:51:63:b3:75:1c	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.1.77? Tell 192.168.1.1
17525	...	80:e6:50:1c:98:c2	e0:51:63:b3:75:1c	ARP	42	192.168.1.77 is at 80:e6:50:1c:98:c2
17902	...	e0:51:63:b3:75:1c	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.1.18? Tell 192.168.1.1

Opcode: request (1)

Sender MAC address: e0:51:63:b3:75:1c

Sender IP address: 192.168.1.1

Target MAC address: ff:ff:ff:ff:ff:ff

Target IP address: 192.168.1.77

ff	ff	ff	ff	ff	ff	e0	51	63	b3	75	1c	08	06	00	01Q c·u.....
08	00	06	04	00	01	e0	51	63	b3	75	1c	c0	a8	01	01·Q c·u·.....
ff	ff	ff	ff	ff	ff	c0	a8	01	4d	00	00	00	00	00	00·M.....
00	00	00	00	00	00	00	00	00	00	00	00				

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)	