ARP Scanning & Denial-of-Service

We might discern additional aberrant behaviors within the ARP requests and replies. It is common knowledge that poisoning and spoofing form the core of most ARP-based `denial-of-service (DoS)` and `man-in-the-middle (MITM)` attacks. However, adversaries could also exploit ARP for information gathering. Thankfully, we possess the skills to detect and evaluate these tactics following similar procedures.

ARP Scanning Signs

Related PCAP File(s):

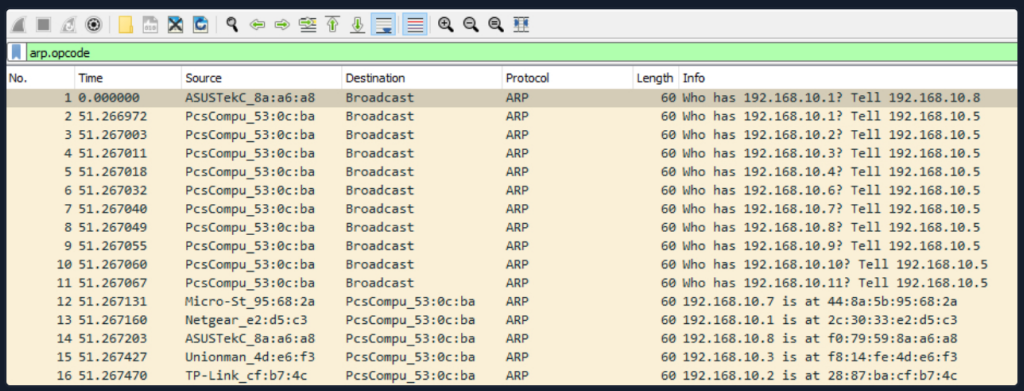
- `ARP_Scan.pcapng`

Some typical red flags indicative of ARP scanning are:

1. `Broadcast ARP requests sent to sequential IP addresses (.1,.2,.3,...)`
2. `Broadcast ARP requests sent to non-existent hosts`
3. `Potentially, an unusual volume of ARP traffic originating from a malicious or compromised host`

Finding ARP Scanning

Without delay, if we were to open the related traffic capture file (`ARP_Scan.pcapng`) in Wireshark and apply the filter `arp.opcode`, we might observe the following:



arp.opcode

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ASUSTekC_8a:a6:a8	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.8
2	51.266972	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.5
3	51.267003	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.2? Tell 192.168.10.5
4	51.267011	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.3? Tell 192.168.10.5
5	51.267018	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.4? Tell 192.168.10.5
6	51.267032	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.6? Tell 192.168.10.5
7	51.267040	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.7? Tell 192.168.10.5
8	51.267049	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.8? Tell 192.168.10.5
9	51.267055	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.9? Tell 192.168.10.5
10	51.267060	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.5
11	51.267067	PcsCompu_53:0c:ba	Broadcast	ARP	60	Who has 192.168.10.11? Tell 192.168.10.5
12	51.267131	Micro-St_95:68:2a	PcsCompu_53:0c:ba	ARP	60	192.168.10.7 is at 44:8a:5b:95:68:2a
13	51.267160	Netgear_e2:d5:c3	PcsCompu_53:0c:ba	ARP	60	192.168.10.1 is at 2c:30:33:e2:d5:c3
14	51.267203	ASUSTekC_8a:a6:a8	PcsCompu_53:0c:ba	ARP	60	192.168.10.8 is at f0:79:59:8a:a6:a8
15	51.267427	Unionman_4d:e6:f3	PcsCompu_53:0c:ba	ARP	60	192.168.10.3 is at f8:14:fe:4d:e6:f3
16	51.267470	TP-Link_cf:b7:4c	PcsCompu_53:0c:ba	ARP	60	192.168.10.2 is at 28:87:ba:cf:b7:4c

It's possible to detect that indeed ARP requests are being propagated by a single host to all IP addresses in a sequential manner. This pattern is symptomatic of ARP scanning and is a common feature of widely-used scanners such as `Nmap`.

Furthermore, we may discern that active hosts respond to these requests via their ARP replies. This could signal the successful execution of the information-gathering tactic by the attacker.

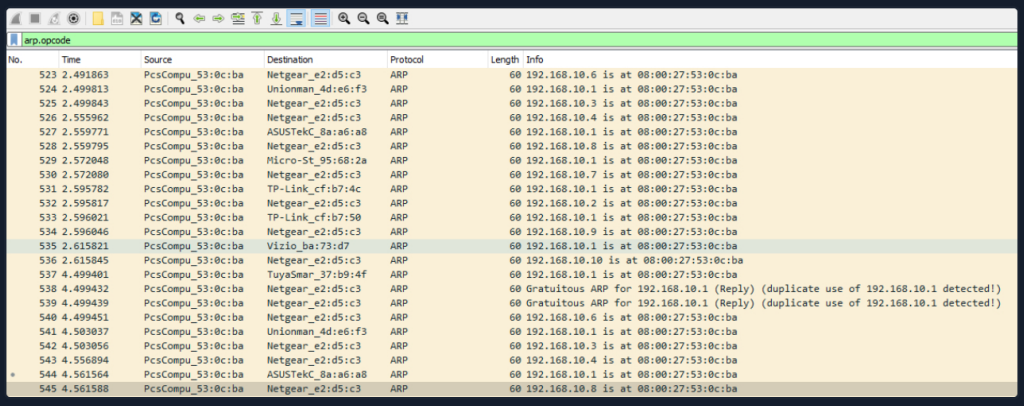
Identifying Denial-of-Service

Related PCAP File(s):

- `ARP_Poison.pcapng`

An attacker can exploit ARP scanning to compile a list of live hosts. Upon acquiring this list, the attacker might alter their strategy to deny service to all these machines. Essentially, they will strive to contaminate an entire subnet and manipulate as many ARP caches as possible. This strategy is also plausible for an attacker seeking to establish a man-in-the-middle position.

in the middle position.

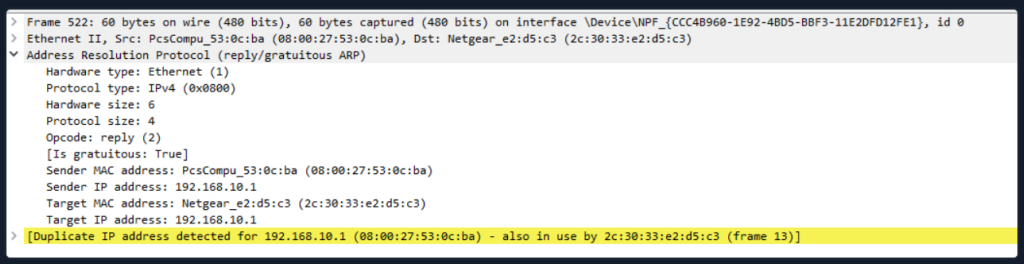


arp.opcode

No.	Time	Source	Destination	Protocol	Length	Info
523	2.491863	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.6 is at 08:00:27:53:0c:ba
524	2.499813	PcsCompu_53:0c:ba	Unionman_4d:e6:f3	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
525	2.499843	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.3 is at 08:00:27:53:0c:ba
526	2.555962	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.4 is at 08:00:27:53:0c:ba
527	2.559771	PcsCompu_53:0c:ba	ASUSTekC_8a:a6:a8	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
528	2.559795	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.8 is at 08:00:27:53:0c:ba
529	2.572048	PcsCompu_53:0c:ba	Micro-St_95:68:2a	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
530	2.572080	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.7 is at 08:00:27:53:0c:ba
531	2.595782	PcsCompu_53:0c:ba	TP-Link_cf:b7:4c	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
532	2.595817	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.2 is at 08:00:27:53:0c:ba
533	2.596021	PcsCompu_53:0c:ba	TP-Link_cf:b7:50	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
534	2.596046	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.9 is at 08:00:27:53:0c:ba
535	2.615821	PcsCompu_53:0c:ba	Vizio_ba:73:d7	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
536	2.615845	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.10 is at 08:00:27:53:0c:ba
537	4.499401	PcsCompu_53:0c:ba	TuyaSmar_37:b9:4f	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
538	4.499432	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	Gratuitous ARP for 192.168.10.1 (Reply) (duplicate use of 192.168.10.1 detected!)
539	4.499439	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	Gratuitous ARP for 192.168.10.1 (Reply) (duplicate use of 192.168.10.1 detected!)
540	4.499451	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.6 is at 08:00:27:53:0c:ba
541	4.503037	PcsCompu_53:0c:ba	Unionman_4d:e6:f3	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
542	4.503056	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.3 is at 08:00:27:53:0c:ba
543	4.556894	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.4 is at 08:00:27:53:0c:ba
544	4.561564	PcsCompu_53:0c:ba	ASUSTekC_8a:a6:a8	ARP	60	192.168.10.1 is at 08:00:27:53:0c:ba
545	4.561588	PcsCompu_53:0c:ba	Netgear_e2:d5:c3	ARP	60	192.168.10.8 is at 08:00:27:53:0c:ba

Promptly, we might note that the attacker's ARP traffic may shift its focus towards declaring new physical addresses for all live IP addresses. The intent here is to corrupt the router's ARP cache.

Conversely, we may witness the duplicate allocation of `192.168.10.1` to client devices. This indicates that the attacker is attempting to corrupt the ARP cache of these victim devices with the intention of obstructing traffic in both directions.



```
> Frame 522: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{CCC4B960-1E92-4BD5-BBF3-11E2DFD12FE1}, id 0
> Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: Netgear_e2:d5:c3 (2c:30:33:e2:d5:c3)
v Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: PcsCompu_53:0c:ba (08:00:27:53:0c:ba)
    Sender IP address: 192.168.10.1
    Target MAC address: Netgear_e2:d5:c3 (2c:30:33:e2:d5:c3)
    Target IP address: 192.168.10.1
> [Duplicate IP address detected for 192.168.10.1 (08:00:27:53:0c:ba) - also in use by 2c:30:33:e2:d5:c3 (frame 13)]
```

Responding To ARP Attacks

Upon identifying any of these ARP-related anomalies, we might question the suitable course of action to counter these threats. Here are a couple of possibilities:

1. `Tracing and Identification`: First and foremost, the attacker's machine is a physical entity located somewhere. If we manage to locate it, we could potentially halt its activities. On occasions, we might discover that the machine orchestrating the attack is itself compromised and under remote control.
2. `Containment`: To stymie any further exfiltration of information by the attacker, we might contemplate disconnecting or isolating the impacted area at the switch or router level. This action could effectively terminate a DoS or MITM attack at its source.

Link layer attacks often fly under the radar. While they may seem insignificant to identify and investigate, their detection could be pivotal in preventing the exfiltration of data from higher layers of the OSI model.

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 1 Inspect the ARP_Poison.pcapng file, part of this module's resources, and submit the first MAC address that was linked with the IP 192.168.10.1 as your answer.

2c:30:33:e2:d5:c3

Submit

← Previous Next →

Mark Complete & Next