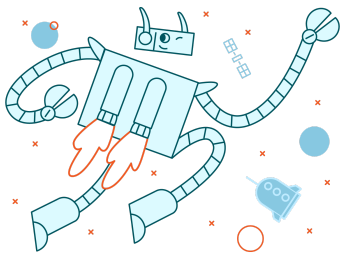
The Cookies Thief 🍪🔍



Background

In a shocking turn of events, the cookies in the cybersecurity startup's state-of-the-art smart fridge have vanished! The fridge, known for its advanced security features, keeps a log of the MAC addresses of devices that have been physically connected to it via Ethernet cable. Rumor has it that the only way to bypass the fridge's lock is through a wired connection.

As the network forensics expert, you have been tasked with analyzing the network capture from the time of the incident to uncover the identity of the cookie thief. Moreover, the police have asked for your help in creating a comprehensive list of all the devices in the office to aid in their investigation. Little do the workers know, there's an undercover cyber cop among them who has been gathering information on their devices.

Clue

The smart fridge's log reveals that a device with a MAC address ending in "8c:3a:e3" was physically connected to it during the time of the cookie heist.

Prerequisites

- Wireshark installed on your computer
- Understanding of network protocols (hint: revisit ARP and DNS)

Instructions

1. Download the provided network capture file.
2. Open the capture file in Wireshark.
3. Create a list of all the devices in the office, including the following information for each device:

    - MAC address
    - IP address
    - Device name
4. Analyze the capture to identify the suspect's device and name.
5. One of the workers is an undercover cyber cop. They are the one who queried the DNS server for the DNS names of all the workers' devices. Find their name.
6. We know that the real thief tried to incriminate one of their co-workers, and make the police suspect the co-worker instead. Who is the co-worker? How did the thief try to incriminate them?
7. Document your findings, the evidence that led you to the culprit, the list of devices, and the identity of the undercover cyber cop.

Guidelines

- Make a list of the protocols present in the capture. Think what information you can get from each.
- You can filter by protocol (e.g. `arp` to show only ARP requests/responses).
- You can click on the title of any of the fields (Source, Destination, Info, etc.) to sort by it, and have a capture that is easier to look at.

To submit

- A brief report detailing your analysis process and the conclusive evidence pointing to the cookie thief.
- Screenshots of relevant packets that support your findings.
- A table or list containing the MAC addresses, IP addresses, and device names of all the devices in the office.
- The identity of the undercover cyber cop who queried the DNS server for the names of all the workers' devices.

- The identity of the co-worker who the real cookie thief has tried to incriminate.

Happy investigating! 🕵️