**Lab 06 – Graylog Hunting**

## Instructions

* 1. a

## Questions

### What network has the most association frames?

* + DSUGaming
  + A screenshot of a computer

    Description automatically generated

### Which network has the most probe requests? Why are most probes wildcards (or null)?

* 1. NULL
     + A screenshot of a computer

       Description automatically generated

### Who is the manufacturer of the network DSUnix?

* + Ubiquiti Inc
  + A screenshot of a computer

    Description automatically generatedA screenshot of a computer

    Description automatically generated

### What is the most popular channel in use?

* + Channel 1
  + A screenshot of a video game

    Description automatically generated

### How many association requests exist for GoTrojans?

* + There are 0 association requests for GoTrojans
  + A screenshot of a computer

    Description automatically generated
  + A screenshot of a computer

    Description automatically generated

### Identify the SSID with the most BSSIDs

* + Most Overall:
    1. NULL
    2. DSU\_Mobile
    3. A screenshot of a computer

       Description automatically generated
  + Most Unique:
    1. NULL
    2. GoTrojans
    3. A screenshot of a computer

       Description automatically generated

### A deauth attack occurred. Those are super annoying. What client was attacked specifically?

* + There is a mutual deauthentication attack being executed by 00:c0:ca:a7:7f:6d, associated with Alfa, Inc., and 34:fc:b9:7b:94:22, linked to Hewlett Packard Enterprise (HPE). In this exchange, a total of 1,392 deauthentication frames were exchanged.
  + Initially, it appeared that Alfa faced a deauthentication attack from HPE, which sent 722 deauthentication frames. In a potential retaliatory or automated response to this attack, it seemed that Alfa responded with 670 deauthentication frames.
  + However, a closer look at timestamps revealed that the initial deauthentication frames originated from Alfa to HPE, which altered my interpretation of the attack. TGiven this new information, there are a few potential scenarios:
  + 1) HPE as a Malicious Entity: HPE may have engaged in malicious behavior on the network. Alfa detected suspicious activity or anomalies and initiated a legitimate deauthentication process. In response to being discovered, HPE launched a deauthentication attack, which caused Alfa to responded to with its own attack.
  + 2) Alfa as a Malicious Entity: Despite HPE's legitimate presence on the network, Alfa initiated a malicious deauthentication attack against HPE. In this scenario, the attack by HPE was retalitory in nature.
  + 3) Mutual Misunderstanding: Both Alfa and HPE may have misinterpreted each other's actions or network behavior, which lead to a cycle of defensive responses.
  + 4) Third-Party Interference: In an attempted network-based denial-of-service (DoS) attack, an external device may have instigated the deauthentication attack between Alfa and HPE, causing both of them to responded defensively
  + A screenshot of a computer

    Description automatically generated
  + A screenshot of a search box

    Description automatically generated
  + A screenshot of a computer

    Description automatically generated

### Around where did the deauth attack take place (hint: think of the sensor names here, as they’re room numbers).

* + BIT235 – Beacom Institute of Technology, Room 235
  + A screenshot of a computer

    Description automatically generated

### What time did the deauth attack take place?

* + The deauth attack took place from
  + 2024-02-15 13:10:03.030
  + to
  + 2024-02-15 13:10:19.853
  + A screenshot of a computer

    Description automatically generated

### Identify the SSID or network that the client was DoS’d from in the deauth attack

* + The primary network the client was DoS’d from in the deauth attack was Guest
  + A screenshot of a computer

    Description automatically generated