**Lab 06 – Graylog Hunting**

## Instructions

The lab employs Graylog server and provided data to investigate the effectiveness of leveraging several sensors deployed in a small geographic area. The objective is to detect various attacks and conduct real-time analysis, complemented by historical data for context and insight.

Given the utilization of real-world 802.11 traffic, the detection of irrelevant signals (aka: The Neighbors) is anticipated. In an effort to leave the neighbors alone, the only SSIDs we will use for this lab will be GoTrojans, CubeFarm, CHP, Vlads\_Place, Putin\_Home, gencyber, DSUnix, DSUmobile, DSUGaming, eduroam, GoCrony!, FreeCandy, IA\_IOT and Guest. You can safely ignore all other SSID’s.

Note: it is recommended to verify certain findings using an OUI reference tool.

## Questions

### What network has the most association frames?

DSUGaming

A screenshot of a computer

Description automatically generated

1.1 - *Association frame count by network, filtering for assocreq and assocresp types*

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

“NULL” has the most probe requests.

Most probe requests are NULL or Wildcards because they function as "searching" probes. Unlike "directed" probes, which specifically request connection from certain access points, these broadcast probe requests are sent by client devices to all nearby access points. By using wildcards or null values, the client can broadcast their request and discover available networks within range without specifying a particular Service Set Identifier (SSID) or other parameters.

A screenshot of a computer

Description automatically generated

2.1 - *Aggregated probe request count by ESSID and type, filtered for 'type:probe-req'*

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

Ubiquiti Inc

A screenshot of a computer

Description automatically generated

3.1 - *BSSID for the network 'DSUnix' based on the aggregated count of sender MAC addresses, filtered for 'essid:DSUnix'*

A screenshot of a computer

Description automatically generated

3.2 - *OUI search results for the MAC addresses associated with the network 'DSUnix'*

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

Channel 1

A screenshot of a video game

Description automatically generated

4.1 *- Aggregating count of channels to determine the most popular channel in use*

### How many association requests exist for GoTrojans?

There are 0 association requests for GoTrojans

A screenshot of a computer

Description automatically generated

5.1 *- Aggregating count of association requests for the network 'GoTrojans'.*

A screenshot of a computer

Description automatically generated

5.2 *- Verification figure: Aggregating count of association requests for the network 'GoTrojans' with the filter 'type:assocreq'.*

### Identify the SSID with the most BSSIDs

Most Overall: (1) NULL, (2) DSU\_Mobile

A screenshot of a computer

Description automatically generated

6.1 *- Aggregating count of BSSIDs by SSID across all networks.*

Most Unique: (1) NULL, (2) GoTrojans

A screenshot of a computer

Description automatically generated

6.2 *- Aggregating cardinality of BSSIDs by SSID across all networks*

### 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. (7.1) (7.2)

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 (7.3) revealed that the initial deauthentication frames originated from Alfa to HPE, which altered my interpretation of the attack. Given 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 respond 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 retaliatory 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

7.1 *- Aggregating count of deauthentication frames by recipient and sender to identify the attacked client.*

A screenshot of a search box

Description automatically generated

7.2 *- OUI Lookup Results for Devices Involved in the Deauthentication Attack*

A screenshot of a computer

Description automatically generated

7.3 *- Timestamp Analysis for the Deauthentication Attack between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d*

### 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

8.1 *- Source Analysis for the Deauthentication Attack Between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d.*

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

The deauthentication 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

9.1 *- Timestamp Range for the Deauthentication Attack Between Devices 34:fc:b9:7b:94:22 and 00:c0:ca:a7:7f:6d.*

### 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

10.1 *- SSID Distribution for the Deauthentication Attack on Client (00:c0:ca:a7:7f:6d OR 34:fc:b9:7b:94:22)*