Lab06- Graylog Hunting

Having centrally located information is essential to finding and removing threats on any network. The primary challenge brought by 802.11 networks is that our virtual world now enters the physical realm: attacks not only can have an origin from an electronic address, they can have a physical location within the enterprise. In this lab, we will explore how we can leverage several sensors deployed in a small geographic area for the detection of attacks and analysis of real-time information, coupled with historical context.

Background

For this lab, use the information available at http://graylog.ialab.dsu.edu:9000 . Log in using csc841/Password1! As the username/password. Since we're leveraging real-world 802.11 traffic for this lab, we will detect many things that we're not interested in (aka: The Neighbors). 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.
You may also want to verify certain findings using an OUI reference tool.

Hunting

For all questions, include a screenshot that clearly shows the answer.

1. What network has the most association frames?
2. Which network has the most probe requests? Why are most probes wildcards (or null)?
3. Who is the manufacturer of the network DSUnix?
4. What is the most popular channel in use?
5. How many association requests exist for GoTrojans?
6. Identify the SSID with the most BSSIDs
7. A deauth attack occurred. Those are super annoying. What client was attacked specifically?
8. Around where did the deauth attack take place (hint: think of the sensor names here, as they're room numbers).
9. What time did the deauth attack take place?
10. Identify the SSID or network that the client was DoS'd from in the deauth attack