LAB 03 – BEACON SCAVENGER HUNT

INSTRUCTIONS

In this lab, we will scan the 2.4 & 5ghz wifi space and capture beacon frames, analyze them, and find specific pieces of information. To complete this lab, you will need to use the Wireless environment in the IA Lab. Do NOT log into the Projects or Learn environments (https://ialab.dsu.edu, click Wireless). A standard Kali virtual machine is deployed for you (kali/kali user/pass), however it also has a physical 802.11 adapter connected. Using this adapter in your virtual machine, scan the area to detect networks. Use a combination of Wireshark and airodump-ng to complete the following things below. Make sure to include a screenshot for each one of the items. If your screenshot is big, make sure to circle or point out where the answer is in your screenshot.

QUESTIONS

[1] Locate a beacon that's hiding its SSID. What is the SSID length?

The BSSID 02:18:4A:14:AB:FF is hiding its SSID and has a length of 4

```
CH 12 ][ Elapsed: 18 s ][ 2024-02-05 11:31

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

78:8A:20:08:CC:DF  -33       12        0    0   6  195   WPA2 CCMP   PSK  CubeFarm
7E:8A:20:08:CC:DF  -32       13        0    0   6  195   WPA2 CCMP   PSK  DSU_Mobile
18:64:72:E8:E0:63  -51       11        0    0  11  195   WPA2 CCMP   MGT  eduroam
18:64:72:E8:E0:62  -50       12        0    0  11  195   OPN              DSUGaming
18:64:72:E8:E0:61  -51       13        0    0  11  195   OPN              Guest
18:64:72:E8:E0:60  -50       12        0    0  11  195   WPA2 CCMP   MGT  GoTrojans
02:18:4A:14:AB:FF  -49       12        0    0  11  130   WEP  WEP         <length:  4>
E4:95:6E:4A:87:D6   -9       13        0    0   2   54e. WPA2 CCMP   PSK  Vlads_Place
E6:95:6E:4A:87:D6  -10       12        0    0   2   54e. WPA2 CCMP   PSK  CHP
```

[2] Locate two beacons that are operating on a channel other than 1, 6 or 11

"CHP" (E6:95:6E:4A:87:D6) and "Vlads_Place" (E4:95:6E:4A:87:D6)
are both operating on channel 2

```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

78:8A:20:08:CC:DF  -33       12        0    0   6  195   WPA2 CCMP   PSK  CubeFarm
7E:8A:20:08:CC:DF  -32       13        0    0   6  195   WPA2 CCMP   PSK  DSU_Mobile
18:64:72:E8:E0:63  -51       11        0    0  11  195   WPA2 CCMP   MGT  eduroam
18:64:72:E8:E0:62  -50       12        0    0  11  195   OPN              DSUGaming
18:64:72:E8:E0:61  -51       13        0    0  11  195   OPN              Guest
18:64:72:E8:E0:60  -50       12        0    0  11  195   WPA2 CCMP   MGT  GoTrojans
02:18:4A:14:AB:FF  -49       12        0    0  11  130   WEP  WEP         <length:  4>
E4:95:6E:4A:87:D6   -9       13        0    0   2   54e. WPA2 CCMP   PSK  Vlads_Place
E6:95:6E:4A:87:D6  -10       12        0    0   2   54e. WPA2 CCMP   PSK  CHP
```

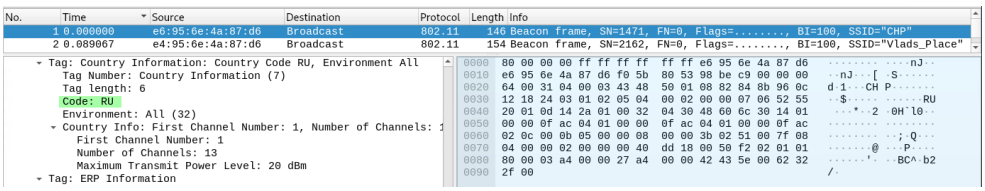
[3] The timestamps for the official DSU networks are all very consistent, find a non-DSU beacon containing a timestamp that is significantly different

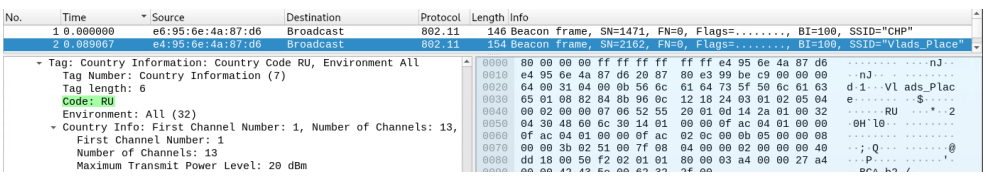
02:18:4A:14:AB:FF has an unusual uptime value of 131d 11:52:25,
which is significantly different from the uptime values of the other networks

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	UPTIME	ESSID
00:00:00:00:00:00	-1	0	4	0	11	-1	OPN			0d 00:00:00	<length: 0>
78:8A:20:08:CC:DF	-32	26	0	0	6	195	WPA2	CCMP	PSK	47d 23:07:54	CubeFarm
7E:8A:20:08:CC:DF	-33	27	0	0	6	195	WPA2	CCMP	PSK	47d 23:07:54	DSU_Mobile
18:64:72:E8:E0:63	-50	25	0	0	11	195	WPA2	CCMP	MGT	2d 19:45:16	eduroam
18:64:72:E8:E0:62	-50	27	0	0	11	195	OPN			2d 19:45:16	DSUGaming
18:64:72:E8:E0:61	-50	27	0	0	11	195	OPN			2d 19:45:16	Guest
18:64:72:E8:E0:60	-50	27	0	0	11	195	WPA2	CCMP	MGT	2d 19:45:16	GoTrojans
02:18:4A:14:AB:FF	-48	27	0	0	11	130	WEP	WEP		131d 11:52:25	<length: 4>
E4:95:6E:4A:87:D6	-27	28	0	0	2	54e.	WPA2	CCMP	PSK	10d 01:14:22	Vlads_Place
E6:95:6E:4A:87:D6	-9	28	0	0	2	54e.	WPA2	CCMP	PSK	10d 01:14:21	CHP

[4] Many AP's do not beacon any regulatory domain information, but one does. Can you find it?

There were a couple of AP's that contained regulatory domain information in the capture.
Two examples were "CHP" (E6:95:6E:4A:87:D6) and "Vlads_Place" (E4:95:6E:4A:87:D6)
which displayed the Country Code "RU"





[5] Create two screenshots, one with the best, one with the worst signal strength you can find

The strongest Signal is "Vlads_Place" (E4:95:6E:4A:87:D6) with a signal strength of -9 dBm

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
78:8A:20:08:CC:DF	-33	7	0	0	6	195	WPA2	CCMP	PSK	CubeFarm
7E:8A:20:08:CC:DF	-33	8	0	0	6	195	WPA2	CCMP	PSK	DSU_Mobile
18:64:72:E8:E0:63	-52	7	0	0	11	195	WPA2	CCMP	MGT	eduroam
18:64:72:E8:E0:62	-51	7	0	0	11	195	OPN			DSUGaming
18:64:72:E8:E0:61	-51	8	0	0	11	195	OPN			Guest
18:64:72:E8:E0:60	-50	7	0	0	11	195	WPA2	CCMP	MGT	GoTrojans
02:18:4A:14:AB:FF	-48	7	0	0	11	130	WEP	WEP		<length: 4>
E4:95:6E:4A:87:D6	-9	10	0	0	2	54e.	WPA2	CCMP	PSK	Vlads_Place
E6:95:6E:4A:87:D6	-10	9	0	0	2	54e.	WPA2	CCMP	PSK	CHP

The weakest signal is “eduroam” (18:64:72:E8:E0:63) with a signal strength of -52 dBm.

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
78:8A:20:08:CC:DF	-33	7	0	0	6	195	WPA2	CCMP	PSK	CubeFarm
7E:8A:20:08:CC:DF	-33	8	0	0	6	195	WPA2	CCMP	PSK	DSU_Mobile
18:64:72:E8:E0:63	-52	7	0	0	11	195	WPA2	CCMP	MGT	eduroam
18:64:72:E8:E0:62	-51	7	0	0	11	195	OPN			DSUGaming
18:64:72:E8:E0:61	-51	8	0	0	11	195	OPN			Guest
18:64:72:E8:E0:60	-50	7	0	0	11	195	WPA2	CCMP	MGT	GoTrojans
02:18:4A:14:AB:FF	-48	7	0	0	11	130	WEP	WEP		<length: 4>
E4:95:6E:4A:87:D6	-9	10	0	0	2	54e.	WPA2	CCMP	PSK	Vlads_Place
E6:95:6E:4A:87:D6	-10	9	0	0	2	54e.	WPA2	CCMP	PSK	CHP

[6] Find a network that does not have the Privacy flag set

“Guest” (18:64:72:E8:E0:61) does not have the Privacy flag set

```
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 241941200278
      Beacon Interval: 0.102400 [Seconds]
    ▾ Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... .... .... .0.. = Reserved: 0
        .... .... .... 0... = Reserved: 0
        .... .... ...0 .... = Privacy: Data confidentiality not required
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = Reserved: 0
        .... .... 0... .... = Reserved: 0
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... ..0. .... .... = QoS: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = EPD: Not Implemented
        .0.. .... .... .... = Reserved: 0
        0... .... .... .... = Reserved: 0
  ▾ Tagged parameters (148 bytes)
    ▾ Tag: SSID parameter set: "Guest"
        Tag Number: SSID parameter set (0)
        Tag length: 5
        SSID: "Guest"
```

[7] Display a list of all of the unique ESSID’s you can detect in a given area

CubeFarm, AAA_Mobile, eduroam (AAA), AAAGaming,
Guest, GoTrojans (AAA), Vlads_Place, CHP, and two hidden SSIDs

```
ESSID

<length:  0>
CubeFarm
DSU_Mobile
eduroam
DSUGaming
Guest
GoTrojans
<length:  4>
Vlads_Place
CHP
```

[8] Display a list of all of the unique BSSID's you can detect in a given area

00:00:00:00:00:00, 78:8A:20:08:CC:DF, 7E:8A:20:08:CC:DF, 18:64:72:E8:E0:63, 18:64:72:E8:E0:62, 18:64:72:E8:E0:61, 18:64:72:E8:E0:60, 02:18:4A:14:AB:FF, E4:95:6E:4A:87:D6, and E6:95:6E:4A:87:D6

```
BSSID

00:00:00:00:00:00
78:8A:20:08:CC:DF
7E:8A:20:08:CC:DF
18:64:72:E8:E0:63
18:64:72:E8:E0:62
18:64:72:E8:E0:61
18:64:72:E8:E0:60
02:18:4A:14:AB:FF
E4:95:6E:4A:87:D6
E6:95:6E:4A:87:D6
```

[9] Many beacons contain "vendor specific" information, you can see this in Wireshark if you look at a beacon frame. What is this for?

Vendor-specific information in beacon frames contains additional data that is specific to a particular manufacturer or vendor. This can include information such as the product model/serial number, firmware version, hardware capabilities, and other proprietary features. This enables vendors to differentiate their products and provide specific functionality based on their unique specifications.

[10] Researchy question! 802.11ax, marketed to the muggles as WiFi 6, is pretty neat. It's introduced a lot of new features, they're really only useful in dense environments. Advice: don't bother upgrading to AX in order to improve your home's wifi performance. To that end, one of the neat features that are introduced is the notion of "spatial reuse". We achieve this through coloring (basic service set coloring or more broadly as a network color code). No crayons needed. What is this?

Spatial reuse was developed by Cisco for 802.11ax (WiFi 6) networks to enhance efficiency and throughput in dense wireless environments, known as Basic Service Set (BSS), where large groups of wireless devices communicate through a centralized access point [1]. However, radio frequencies bands for Wi-Fi communication are finite, and within these bands, there are only a limited number of channels available for wireless communication [2]. As such, in environments with many wireless networks or devices, it is common for "multiple BSSs [to] operate [within] the same channel" [3]. This overlapping operation known as Overlapping BSS (OBSS) can lead to signal interference, degraded communication quality, packet collisions, and reduced throughput.

To address this challenge, spatial reuse provides a mechanism that assigns colors to different BSSs. By assigning distinct 'BSS color' values within the HE PHY headers of nearby BSSs, devices are able to distinguish between simultaneous packets from different BSSs and avoid interference [4]. This approach enables multiple BSSs to efficiently operate in dense environments by minimizing interference, degradation, and collisions.

SOURCES:

[1] https://www.geeksforgeeks.org/introduction-of-basic-service-set-bss/
[2] https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php
[3] https://www.mathworks.com/help/wlan/ug/spatial-reuse-with-bss-coloring-in-an-802.11ax-network-simulation.html#responsive_offcanvas
[4] https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/b_wl_17_11_cg_chapter_010000101.html