Kryptografia i bezpieczeństwo
Lista nr 6

Aleksander Spyra

3 I 2016

1 Zadanie 1

Nie odnaleziono otwartej sieci, która umożliwiłaby podglądanie ruchu programem Wireshark, więc stworzono własną otwartą sieć za pomocą urządzenia mobilnego.

1.1 Lista dostępnych sieci

BSSID	SSID	Beac	Data	Req	Resp	Auth	Oth	Enc
Broadcast	biwizone	0	0	7	0	0	0	brak
Broadcast	<Broadcast>	0	0	135	0	0	0	
Broadcast	Daniel	0	0	4	0	0	0	
192.168.43.1	despota	401	30	0	34	2	3	WPA2-PSK
192.168.43.1	despota2	3780	48271	35	100	6	23	brak
Broadcast	NETIASPOT-5C86B0	0	0	23	0	0	0	
VtechTel_dc:7a:78	NETIASPOT-DC7A70	2801	27	0	57	0	0	WPA2-PSK
Tp-LinkT_67:62:aa	reno822	2108	2	0	81	0	0	WPA2-PSK
Tp-LinkT_62:68:14	TP-LINK	39	0	0	1	0	0	WPA2-PSK
D-Link_a0:88:8b	www802cz4845openDHCP	0	0	0	23	0	0	

Skorzystano z opcji Statistics -> WLAN Traffic.

Aby dowiedzieć się więcej o zabezpieczeniach poszczególnych sieci, skorzystano z filtrów dla odpowiednich BSSID i przeanalizowano informacje zawarte w beacon frame. Są to ramki wysyłane cyklicznie przez punkt dostępowy, aby rozgłaszać istnienie sieci. Użyteczne informacje o szyfrowaniu znaleźć można także w probe response. Aby wyświetlać jedynie ramki z odpowiednich sieci, użyto filtra wlan_mgt.ssid == "nazwa_sieci".

1.2 Lista odwiedzanych stron WWW

Pełną listę hostów HTTP, z którymi łączyły się urządzenia użytkowników sieci, można uzyskać poprzez skorzystanie z opcji Statistics -> Endpoints -> IPv4. Po przejrzeniu listy można wywnioskować, że użytkownicy urządzeń korzystali z serwisów o najbardziej czytelnych nazwach domenowych, a więc

www.wnp.pl
www.rynek-kolejowy.pl
www.nbp.pl
www.google.com
twitter.com
niezalezna.pl
www.bankier.pl
www.google.pl
www.idziesiec.pl
www.facebook.com
niebezpiecznik.pl
kubrynska.com
www.wp.pl
www.transport-publiczny.pl
(zał. ip.png)

1.3 Lista protokołów i usług

Listę protokołów i ich procentowego udziału w przechwyconym ruchu sieciowym można uzyskać korzystając z opcji Statistics -> Protocol Hierarchy. Najistotniejsze, czyli dane, były transportowane poprzez TCP (41575 pakietów), a tylko 5477 pakietów z tego stanowiły pakiety wysłane z użyciem SSL-a.

1.4 Mapa lokalizacji

Uzyskano dzięki pobraniu bazy danych GeoIP oraz wybraniu opcji Statistics -> Endpoints -> IPv4 -> Map (dostępne w wersji 1.10.2 dla Windows). (zał. world.png, us.png, europe.png)

1.5 Lista modeli generujących ruch

198.168.	
.43.221	Dalvik/1.6.0 (Linux;U;Android 4.4.2; SAMSUNG-SGH-I257 Build/KOT49H)
.43.79	Mozilla/5.0 (Android 4.4.2;Mobile;rv:43.0) Gecko/43.0 Firefox/43.0
.43.188	Mozilla/5.0 (Windows NT 6.3;WOW64;rv:43.0) Gecko/20100101 Firefox/43.0
.43.189	Mozilla/5.0 (Linux; U; Android 4.1.2; pl-pl; SAMSUNG GT-I8190N/ I8190NXXANR6 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30

Te szczegółowe dane uzyskano z analizy żądań HTTP GET dla wybranych adresów IP w sieci. Ogólne dane (dla wszystkich sieci, po rozpoznanym numerze MAC) uzyskano dzięki opcji Statistics -> WLAN Traffic. (zał. dev1.png, dev2.png).