Bezpieczeństwo

Raport z listy 3 na laboratoria

Oskar Makowski

Grupa poniedziałek 17.07-18.45

1. Lista poszukiwanych SSID

Urządzenia mogące działać w sieci WLAN(Wireless Local Area Network) rozsyłają Probe Requests, sprawdzające czy znane im punkty dostępu znajdują się w zasięgu. Przechwytując takie pakiety, można dowiedzieć się, do jakich sieci chciały podłączyć się urządzenia.

Przykład:

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_d8:d7:95	Broadcast	802.11	131	Probe Request, SN=476, FN=0, Flags=......, SSID=eduroam

Takie dane można otrzymać ustawiając w `wireshark` filtr `wlan.fc.type_subtype eq 4`. W zebranych danych pojawiły się następujące SSID, które były poszukiwane: eduroam, Wildcard(Broadcast), Hello there, edc354, iPhone, McD-Hotspot, Pwr-Wi-Fi, AndroidAP, domekcaloroczny, domkicaloroczne. Ciekawym przypadkiem jest Wildcard(Boradcast), który oznacza, że pole SSID jest obecne, jednak jest puste. Jest to Null Probe Request.

2. Podłączone urządzenia

Ustawiając w `wireshark` filtr `dns` można sprawdzić ile różnych źródeł pytało się punktu dostępowego o adresy DNS wyszukiwanych stron.

No.	Time	Source	Destination	Protocol	Length	Info
1266	84.532528	192.168.12.54	192.168.12.1	DNS	146	Standard query 0x3445 A www.google.com

W przechwyconych pakietach znajdują się 2 różne adresy urządzeń.

3. Lista stron odwiedzonych przez użytkowników

Ustawiając w `wireshark` filtr `dns.qry.name contains „www”` można uzyskać strony www, na które wchodzili użytkownicy. Filtr ten pokazuje także obiekty ładowane na stronach odwiedzonych, toteż należy odzyskać jedynie pierwotny adres.

No.	Time	Source	Destination	Protocol	Length	Info
8253	174.395584	192.168.12.54	192.168.12.1	DNS	148	Standard query 0xc3af A www.facebook.com

4. Protokoły

Komunikacja odbywała się następującymi protokołami: 802.11, DNS, GQUIC(Google Quick UDP Internet Connections), HTTP, ICMP, ICMPv6, IGMPv3, MDNS, NTP, SSDP, TCP, TLSv1.2, TLSv1.3.

5. Mapa lokalizacji

Za pomocą programu `traceroute` można prześledzić ścieżkę, jaką pakiety podążają do serwera. Następnie można wykorzystać stronę `ipinfo.io` żeby otrzymać przybliżoną lokalizację serwera.

```
traceroute 31.13.81.36
traceroute to 31.13.81.36 (31.13.81.36), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  16.304 ms  19.509 ms  27.804 ms
 2  * * *
 3   89-75-12-1.infra.chello.pl (89.75.12.1)  77.331 ms  81.265 ms 81.284 ms
 4   pl-poz01a-rd1-ae10-2119.aorta.net (84.116.253.202)  81.284 ms 85.284 ms  81.278 ms
 5   pl-waw04a-rc1-ae11-2110.aorta.net (84.116.252.41)  85.296 ms 85.583 ms  90.200 ms
 6   pl-waw02a-ri1-ae13-0.aorta.net (84.116.138.210)  111.372 ms * pl-waw02a-ri1-ae1-0.aorta.net (84.116.138.90)  71.372 ms
 7  213.46.178.210 (213.46.178.210)  71.396 ms  71.982 ms  72.010 ms
 8     po106.psw03.waw1.tfbnw.net  (157.240.49.189)  72.124 ms po106.psw02.waw1.tfbnw.net  (157.240.49.181)  72.122 ms po106.psw04.waw1.tfbnw.net (157.240.49.221)  72.955 ms
 9    157.240.38.123  (157.240.38.123)  75.390 ms  173.252.67.105 (173.252.67.105)  75.345 ms 157.240.38.73 (157.240.38.73)  75.378 ms
10  edge-star-mini-shv-01-waw1.facebook.com (31.13.81.36)  79.382 ms 98.739 ms  43.880 ms
```

```
curl ipinfo.io/31.13.81.36
{
  "ip": "31.13.81.36",
  "hostname": "edge-star-mini-shv-01-waw1.facebook.com",
  "city": "",
  "region": "",
  "country": "IE",
  "loc": "53.3472,-6.2439",
  "org": "AS32934 Facebook, Inc."
}
```

6. Kradzież sesji

Została spreparowana niezabezpieczona strona pod adresem `www.mikolaj.ovh`, używająca protokołu HTTP. W `wireshark` w trakcie nasłuchu można odzyskać ciasteczko lub zrobić to za pomocą `tshark`. Komenda wygląda następująco: `tshark -r wireless.pcap -T fields -e http.host -e http.cookie -Y „http.host contains \"mikolaj\" && http.cookie"`. Następnie używamy skryptu napisanego w Pythonie wykorzystującego Selenium dla przeglądarki.