Bezpieczeństwo komputerowe

Lista 1

Mateusz Kochanek

30 X 2020

1 Zadanie 1

Opisane poniżej statystyki zostały stworzone na podstawie danych zebranych przez program Wireshark. Dane były zbierane w trybie monitor karty sieciowej, a także bezpośrednio z hostowanej na laptopie sieci bezprzewodowej. Warto zaznaczyć, że przez okoliczności epidemiologiczne wykonanie tego zadania w sposób jaki został opisany na liści było bardzo trudne, dlatego jest to raczej symulacja takich danych. W zadaniu 1.1 pokazuje rekordy z pliku dane1.pcapng, a w zadaniach 1.2-1.5 z pliku data_final.pcapng. W pliku notes.txt są pełne zestawienia zadań 1.3 i 1.4.

1.1 SSID

poszukiwania	SSID
317	*Wildcard*
71	my_som_koksy
35	GILL_U_GAWRONA
18	wlan_autobusy
17	Delrico
12	UPC243146243
4	Adiuto5
1	AERO 2
8	antek-EXT
4	ASUS
1	Darmowe_Orange_WiFi
6	Galaxy J574E1
1	GOOOO
6	HUAWEI Mate 20 lite
6	KabelBox-2F24
9	moto g(6) play 8968
3	NETIASPOT-5GHz-B12065
3	NETIASPOT-6D1F20
1	Nokia 5
2	Orange_Swiatlowod_3C90
4	UPC1721703
6	UPC2484209
1	UPCC2D2C42
3	WiFi_Endoscope
8	WLAN-417845

Warto zaznaczyć, że dane do tej sekcji zostały zebrane w trybie monitor. Wireshark zbierał dane z których potem wyfiltrowano probe requesty wraz z wyszukiwanymi

SSID sieci przy użyciu komendy "tshark -r dane1.pcapng -Y 'wlan.fc.type_subtype eq 4' -T fields -e wlan.ssid — sort — uniq -c". Widzimy w zestawieniu sieci i urządzenia jakie znajdują się w okolicy mieszkania, w którym wykonano badanie. Jest też puste pole, oznaczone jako *Wildcard*, które pozwala na dopasowanie do dowolnej nazwy sieci.

1.2 Urządzenia połączone

Tutaj z uwagi na okoliczności zbadano tylko jedną sieć, do której trzeba było zasymulować połączenia. Dane z wiresharka odfiltrowano skryptem "countSources.py — uniq — sort -c". Jest to lista unikalnych adresów MAC jakie były podłączone do sieci. Widać, że z sieci korzystało 5 urządzeń.

ilość DNS-ów	urządzenie
791	"08:d4:6a:ec:60:cb"
18386	"3c:22:fb:c9:b3:5c"
45968	"82:00:0b:3b:17:53"
8367	"a0:88:69:de:04:c7"
2271	"c0:f4:e6:e8:09:7f"

1.3 Strony odwiedzone

Na podstawie zapytań DNS ustalono odwiedzane w trakcie badania strony. Do filtrowania użyto polecenia "tshark -r data_final.pcapng -T fields -Y dns -e dns.qry.name". Poniżej przedstawione są tylko niektóre strony, ponieważ pełne zestawienie jest bardzo długie i znajduje się w pliku notes.txt.

ilość DNS-ów	strona
10	api.github.com
15	github.com
9	runmageddon.pl
3	facebook.com
14	dnd.wizards.com
2	www.wireshark.org
10	www.youtube.com

1.4 Użyte protokoły

Rodzaje protokołów jakie uzyskano z danych za pomocą "tshark -r data_final.pcapng -T fields -e frame.protocols". Pełne zestawienie jest długie, można je znaleźć w pliku notes.txt:

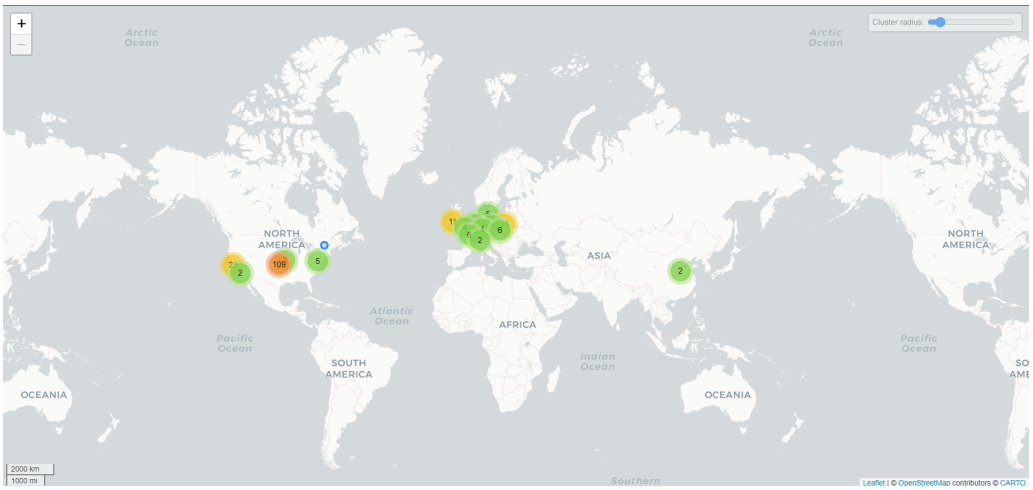
Protokoły
tcp
tls
udp
dns

1.5 Lokalizacje

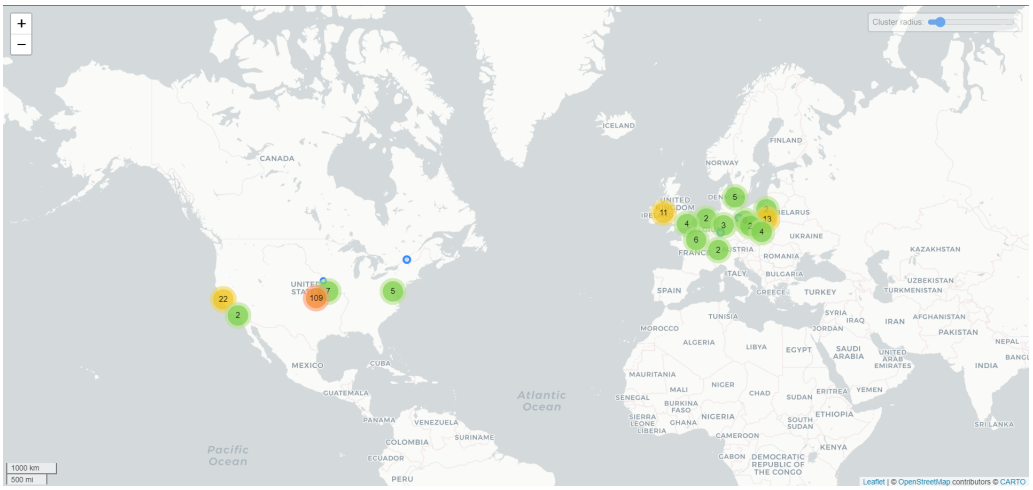
Dzięki zaimportowaniu bazy danych GeoLITE2 do wiresharka udało się znaleźć znaczną ilość krajów do jakich kierowane były zapytania.

ilość zapytań	kraj
146	"United States"
29	"Poland"
11	"Ireland"
6	"France"
5	"Denmark"
5	"Germany"
4	"United Kingdom"
2	"China"
2	"Netherlands"
1	"Canada"
1	"Country"

A także stworzyć mapę lokalizacji:



Rysunek 1: Mapa całego świata



Rysunek 2: Mapa pokazująca Amerykę Północną i Europę

2 Zadanie 2

Napisano prosty program używający pysharka i selenium. Pyshark jest użyty aby przychwycić protokół http z ciasteczkiem, a sterownik selenium dodaje je do naszej przeglądarki. Dzięki temu mamy na czas trwania sesji te same przywileje co osoba która się zalogowała. Testy były przeprowadzane hostując wifi na laptopie i logując się na stronę http://testphp.vulnweb.com/login.php przez komórkę podłączoną do hostowanej sieci.

2.1 Uruchamianie

Aby uruchomić zadanie należy wpisać polecenie "python3 get_session.py", program zacznie wtedy monitorować połączenia, jeżeli złapie połączenie http to wyciągnie z niego cookie i doda do wybranej przeglądarki. Program był stworzony z myślą o przeglądarce firefox wiec potrzebuje webdrivera "geckodriver", a dodatkowo zainstalowanej w systemie paczki selenium. Trzeba też pozwolić wireshark-owi na przychwytywanie pakietów jako zwyczajny użytkownik (nie root).

2.2 Wyniki

Udało się przechwycić ciasteczko i zalogować na konto użytkownika wykorzystując jego sesję.