6 OSINT

Linki

- https://osintframework.com/
- https://osintframework.pl/
- https://whatsmyname.app/
- https://hunter.io/
- https://pimeyes.com/en
- https://github.com/jivoi/awesome-osint
- https://thispersondoesnotexist.com/
- https://www.earthcam.com/mapsearch/
- http://www.insecam.org/
- https://myip.ms/view/ip_owners/109634/Lubman_Umcs_Sp_Z_O_o.html
- https://myip.ms/view/ip_addresses/3568703488/212.182.24.0_212.182.24.255
- https://www.hidglobal.com/product-mix/vertx
- https://vemco.pl/upload/Kontrolery_KD_RCP/Kontroler_Drzwiowy_HID_VertX_V100.pdf
- https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases

Shodan

- https://sekurak.pl/shodan-czyli-google-dla-urzadzen-sieciowych/
- https://www.shodan.io/
- https://help.shodan.io/the-basics/what-is-shodan
- https://help.shodan.io/the-basics/search-query-fundamentals
- https://www.shodan.io/explore
- https://blog.shodan.io/understanding-the-shodan-search-query-syntax/
- https://beta.shodan.io/search/examples
- https://help.shodan.io/the-basics/academic-upgrade
- https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/
- https://www.shodan.io/explore/recent
- https://www.shodan.io/explore/popular
- https://github.com/mr-exo/shodan-dorks
- https://github.com/jakejarvis/awesome-shodan-queries
- https://securitytrails.com/blog/top-shodan-dorks
- https://github.com/lothos612/shodan
- https://blog.shodan.io/

Inne, warte uwagi wyszukiwarki:

- https://search.censys.io/
- https://hunter.how/
- https://www.zoomeye.org/

Zadania

6.1 Pobierz na dysk zdjęcie `img61.jpg`. Odpowiedź na poniższe pytania:

(a) Kiedy zrobiono zdjęcie? Podaj datę i czas.

(b) Jaka była temperatura (w stopniach Celsjusza) w momencie, gdy robiono zdjęcie? Czy wiał wtedy wiatr? Z jaką prędkością?

(c) Gdzie zrobiono zdjęcie? Podaj dokładny adres.

(d) Jakim urządzeniem zrobiono zdjęcie (telefon, aparat)? Podaj model.

6.2 Pobierz na dysk zdjęcie `img61.jpg`, następnie:

(a) Usuń z obrazka dane geolokalizacyjne,

(b) Zmień dane geolokalizacyjne obrazka i zapisz go pod nazwą `img61-new.jpg`,

(c) Za pomogą dostępnych w Internecie serwisów, np. `https://www.pic2map.com` sprawdź, czy lokalizacja została zmieniona.

6.3 Pobierz na dysk zdjęcie `img62.jpg`. Wiedząc, że zdjęcie zostało zrobione `2023:09:19` w lokalizacji o współrzędnych geograficznych `GPS Latitude: 41 deg 43' 13.43" N` oraz `GPS Longitude: 2 deg 56' 2.45" E`, odpowiedź na pytanie, o której godzinie zostało zrobione zdjęcie?

6.4 Korzystając z bazy danych agregującej wycieki haseł / danych z różnych serwisów, sprawdź, sprawdź, czy Twój adres mailowy znajduje się na liście `https://haveibeenpwned.com/`.

6.5 *Maltego is the all-in-one tool for link analysis. Maltego offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.*

Sprawdź, ile informacji o sobie będziesz w stanie znaleźć za pomocą Maltego. Wykorzystaj jedynie imię i nazwisko.

6.6 *Shodan is a Search Engine for the Internet of Everything. Shodan is the world's first search engine for Internet-connected devices. Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between.*

UWAGA Należy pamiętać, że bez zgody właściciela serwera nie należy wchodzić do niezabezpieczonych systemów znalezionych przez Shodana. Nie można łączyć się przez niezabezpieczony pulpit zdalny, czy próbować pobierać danych z bazy danych.

6.6.1 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z otwartym portem o numerze 22.

6.6.2 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z otwartym portem o numerze 22 i serwerem OpenSSH działającym w wersji 7.4.

6.6.3 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z zamkniętym portem o numerze 80.

6.6.4 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia na których działa serwer OpenSSH zwracający następujący baner: `SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7`.

6.6.5 Wykorzystując `Shodana` i odpowiedni filtr, przeskanuj zakres adresów IPv4 `212.182.24.0 - 212.182.27.255` należący do uczelni.

6.6.6 Wykorzystując `Shodana` i odpowiedni filtr, przeskanuj zakres adresów IPv4 `212.182.24.0 - 212.182.27.255` należący do uczelni. (Wykorzystaj notację CIDR).

6.6.7 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z zainstalowanym serwerem Apache z lokalizacją w Lublinie.

6.6.8 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia, należące do uczelni (UMCS), które znajdują się w Lublinie i jest na nich zainstalowany serwer Apache.

6.6.9 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia, należące do uczelni (Politechnika Lubelska), na których można się zalogować na serwer FTP (umożliwiające *Anonymous Login*).

6.6.10 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z publicznie dostępną bazą danych MongoDB w Polsce.

6.6.11 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj publicznie dostępne urządzenia Cisco, których właścicielem jest UMCS.

6.6.12 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj publicznie dostępne komputery z systemem Windows, których właścicielem jest KUL.

6.6.13 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia podatne na CVE-2021-41773 w Polsce.

6.6.14 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia z dostępem RDP. Zawęż wyszukiwanie do wyników, które posiadają screenshoot zdalnego pulpitu. (*RDP = Ransomware Deployment Protocol* 😛)

6.6.15 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia należące do Orange, z otwartm portem SSH.

6.6.16 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia (webcamery) w Polsce, które posiadają screenshoot.

6.6.17 Wykorzystując `Shodana` i odpowiedni filtr znajdź pracę w Niemczech 😁.

6.6.18 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj urządzenia, do których można połaczyć się za pomocą Telnetu, łącząc się bezpośrednio na konto roota.

6.6.19 Wykorzystując `Shodana` i odpowiedni filtr, wyszukaj drukarki sieciowe na porcie 9100, do których można uzyskać dostęp bez uwierzytelnienia. Sprawdź, czy takie drukarki dostępne są w Polsce.

6.7 Odpowiedz na pytanie: jak się chronić i nie zostać wykrytym przez Shodana?