Manuel Di Gangi

S5_L2

20 febbraio 2024

Traccia

Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è di familiarizzare con i tool principali della fase di information gathering, quali:

- Google, per la raccolta delle info.
- Maltego.

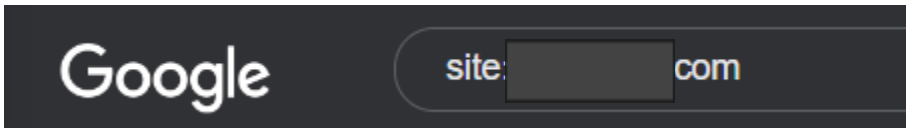
Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato: il target; le query utilizzate (dove applicabile) ed i risultati ottenuti.

Come **target** è stata scelta una nota azienda multinazionale di consulenza informatica

Google Hacking - ricerca passiva

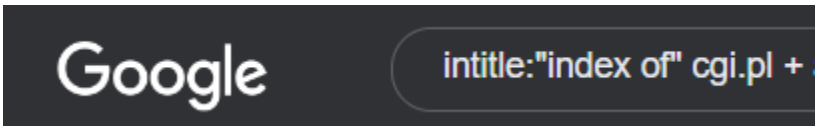
Con l'ausilio del motore di ricerca google avviamo una ricerca passiva delle informazioni, ovvero utilizzando fonti di pubblico dominio. Con una banale ricerca su google risaliamo immediatamente: a cosa fa l'azienda, alle varie sedi, il numero di dipendenti, i vari profili social e i recapiti.

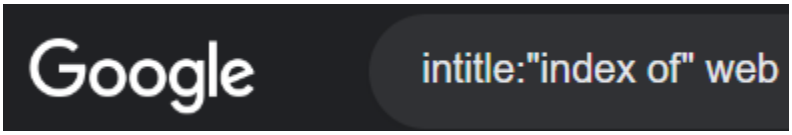
Da qui cominciamo a muoverci per studiare la sua infrastruttura, partendo dal dominio del target ricerchiamo i vari sottodomini utilizzando la query: **site:nome_target.com**



Essendo un'azienda con sedi in tutto il mondo come primi risultati otteniamo le varie piattaforme in lingua italiana, come ad esempio la newsroom e i diversi blog di divulgazione, successivamente il browser ci mostra i vari sottodomini delle sedi estere come giappone, romania, irlanda.

Lanciamo le query **intitle:"index of" cgi.pl + nome_target** ed **intitle:"index of" web** alla ricerca di una Directory listing

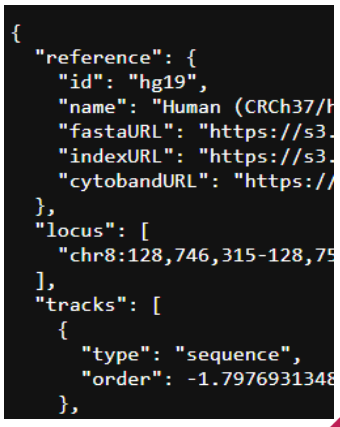




La ricerca non ottiene alcun risultato, rammentando che l'azienda target lavora nel settore IT questa è una nota positiva. A scopo didattico continuiamo la ricerca tramite la suddetta query e troviamo le directory list di alcuni siti di divulgazione scientifica. All'interno di uno di questi, navigando fra le directory, troviamo un file nominato ***nome_target_sessio.xml*** informazione che potrebbe esser sfruttata per instaurare una connessione al server target e studiare i comportamenti.

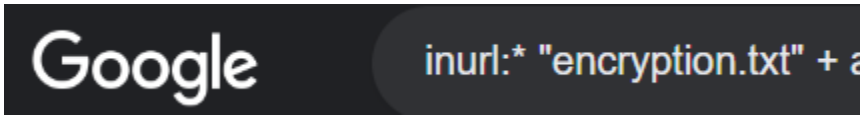
Index of /web

Name	Last modified	Size	Description
Parent Directory		-	
app/	2023-09-15 01:39	-	
beta/	2018-04-27 12:22	-	
demo/	2016-06-14 21:13	-	
google-embed.html	2017-10-12 20:13	1.9K	
img/	2015-05-12 08:32	-	
jb/	2022-06-01 14:04	-	
juicebox.html	2020-03-03 01:20	18K	
release/	2023-09-15 01:14	-	
snapshot/	2021-11-03 01:58	-	
test/	2020-03-29 00:14	-	



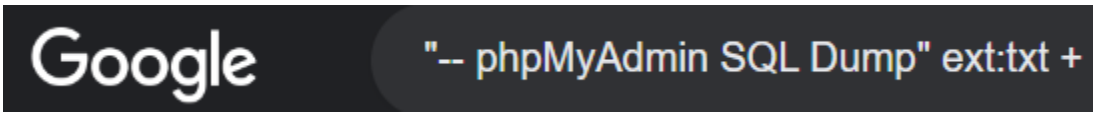
```
{
  "reference": {
    "id": "hg19",
    "name": "Human (CRCh37/h
    "fastaURL": "https://s3.
    "indexURL": "https://s3.
    "cytobandURL": "https://
  },
  "locus": [
    "chr8:128,746,315-128,75
  ],
  "tracks": [
    {
      "type": "sequence",
      "order": -1.7976931348
    },
```

Grazie alla query **inurl:* “encryption.txt” + nome_target** alla ricerca di un file contenente dati di login o comunque dati utili per studiare la criptazione dei dati.

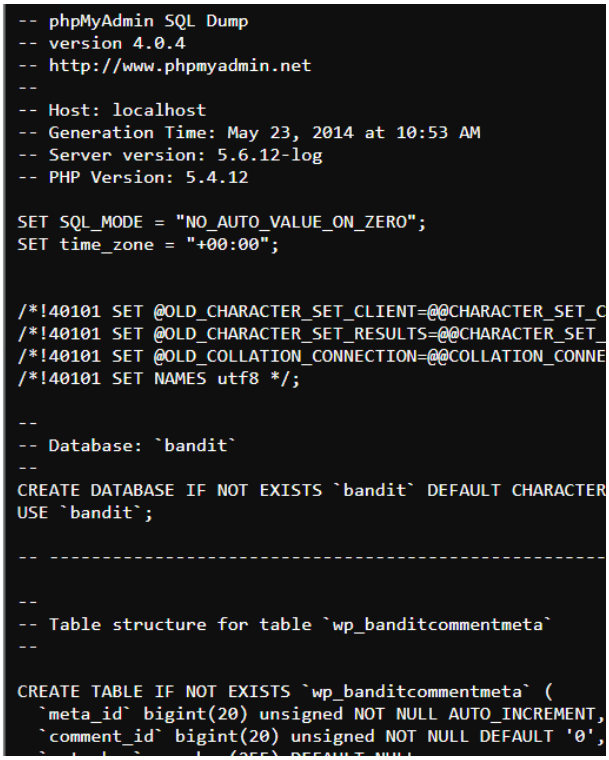


Anche questa volta, la ricerca non porta risultati relativi al nostro target.

Utilizzando la query **"-- phpMyAdmin SQL Dump" ext:txt + nome_target** andiamo a cercare eventuali falle nei database che ci permettano di accedere ai dati contenuti su di essi



Di nuovo, nessun risultato relativo al nostro target. Continuando la ricerca escludendo il nostro target troviamo diversi siti che espongono informazioni relativi alla struttura dei loro DB



```
-- phpMyAdmin SQL Dump
-- version 4.0.4
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: May 23, 2014 at 10:53 AM
-- Server version: 5.6.12-log
-- PHP Version: 5.4.12

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_C
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNE
/*!40101 SET NAMES utf8 */;

--
-- Database: `bandit`
--
CREATE DATABASE IF NOT EXISTS `bandit` DEFAULT CHARACTER
USE `bandit`;

-- --------------------------------------------------------


--
-- Table structure for table `wp_banditcommentmeta`
--

CREATE TABLE IF NOT EXISTS `wp_banditcommentmeta` (
  `meta_id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `comment_id` bigint(20) unsigned NOT NULL DEFAULT '0',
```

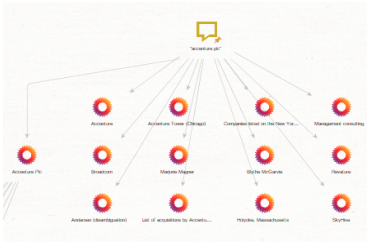
Analizzando gli scarsi risultati ottenuti deduciamo che il reparto IT del nostro target ha fatto particolare attenzione a non lasciare “incustodite” informazioni sensibili.

A questo punto ci troviamo due opzioni per proseguire la ricerca, effettuare operazioni di social engineering o passare alla ricerca attiva.

Maltego - ricerca attiva

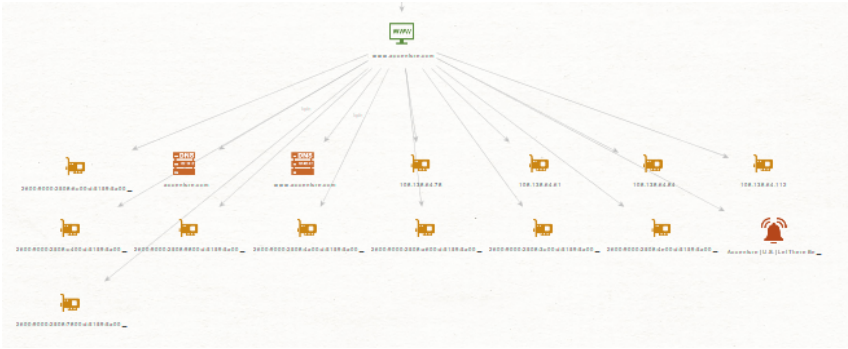
Per la parte di ricerca attiva ci spostiamo sul Maltego, dove per avviamo l’operazione partendo da una frase, nel nostro caso “Nome target”.

Da qui otteniamo svariati risultati tra i quali troviamo la ragione sociale del nostro target.



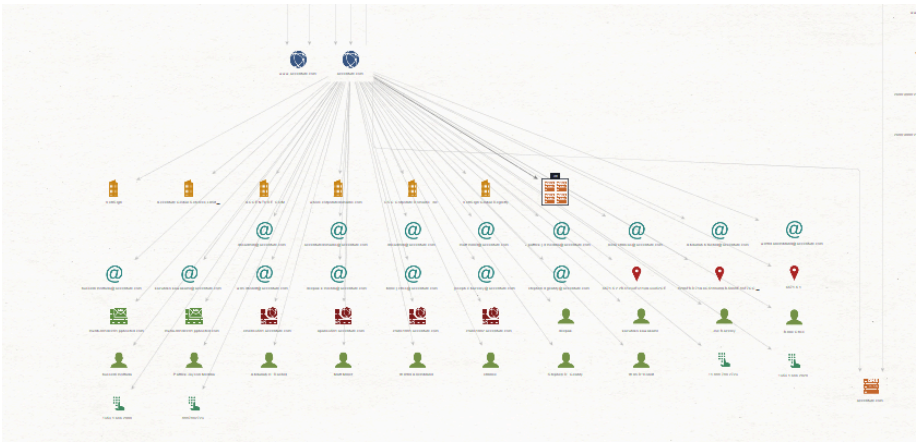
Partendo da questo punto avviamo una ricerca sul web , fra i risultati che otteniamo molti sono siti che abbiamo incontrato nella prima fase della ricerca passiva

Scegliendo il sito principale, avviamo la ricerca dei dns, ip, domini ed eventuali criticità



Partendo dal dominio del nostro target effettuiamo le seguenti ricerche:

- whois
- dns
- email address
- location
- NS record
- person
- phone number



Come risultati otteniamo informazioni sull'azienda che supporta i domini, server mail DNS e NAS, mail, numeri di telefono e le persone a cui questi appartengono.

Partendo da queste informazioni si potrebbe partire con delle azioni di social engineering

Social engineering

La caratteristica principale della social engineering è che non agisce su computer o software,

ma sulle persone. Non prova a individuare i bug del sistema per riuscire ad hackerare ma punta sul fattore umano.

Partendo da linkedin si potrebbe risalire ai vari dipendenti e relativa posizione, tramite i social e pensare una serie di dict di possibili username e password, studiare una strategia di phishing per carpire informazioni utili l'accesso alla mail aziendale per ottenere accesso alla rete aziendale o continuare la campagna di phishing per ottenere privilegi più alti.