EPICODE-CS0124
S5/L2 - Pratica

Flaviano Sedici

Pratica

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).
- I risultati ottenuti.

1. Selezione target e ricerca Google

1.1. Target selezionato

Un cantante italiano

1.2. Ricerca generica sui motori di ricerca

Abbiamo effettuato una normale ricerca per cercare il vero nome esteso del cantante.

1.3. Ricerca tramite Dork

Individuato il nome completo del target, di seguito **target**, abbiamo effettuato una analisi sui social e sul sito ufficiale del target.

*"**target**" intitle:(Facebook | Instagram | Tiktok | Linkedin | Ufficiale)*

A questo punto abbiamo provato a cercare sul sito ufficiale (**sito_target**) e sui social qualche numero di telefono.

*site:**sito_target**.it phonebook:**target***

Dalla ricerca l'unico numero identificato è quello presente in una pagina non aggiornata e di default che contiene un numero di telefono dello stato di New York, chiaramente non appartenente al sito del target che probabilmente utilizza un servizio terzo per il suo shop online.

https://shop.**sito_target**.it/pages/contact

Analizzando la pagine con il tool di ispezione del browser, abbiamo identificato che il servizio utilizzato per il portale è shopify con l'aiuto di iubenda per la stesura delle privacy policy. La

pagina dei contatti quindi risulta esposta, catalogata da Google ma non gestita e con informazioni errate.

Utilizzando un'altra dork abbiamo verificato che il portale avesse solo tre sottodomini. Infatti la dork che segue non ha prodotto alcun risultato:

site:**sito_target**.it -site:www.**sito_target**.it -site:fanclub.**sito_target**.it -site:shop.**sito_target**.it

Ci siamo poi dedicati alla ricerca di file e possibili accessi sul portale dedicato allo shop tramite i seguenti dork:

site:shop.**sito_target**.it ext:(db | txt | php | pdf)

site:shop.**sito_target**.it inurl:admin*

site:shop.**sito_target**.it inurl:phpmyadmin*

Non si è ottenuto alcun risultato, presumibilmente perché l'intero shop è gestito tramite l'account di shopify.

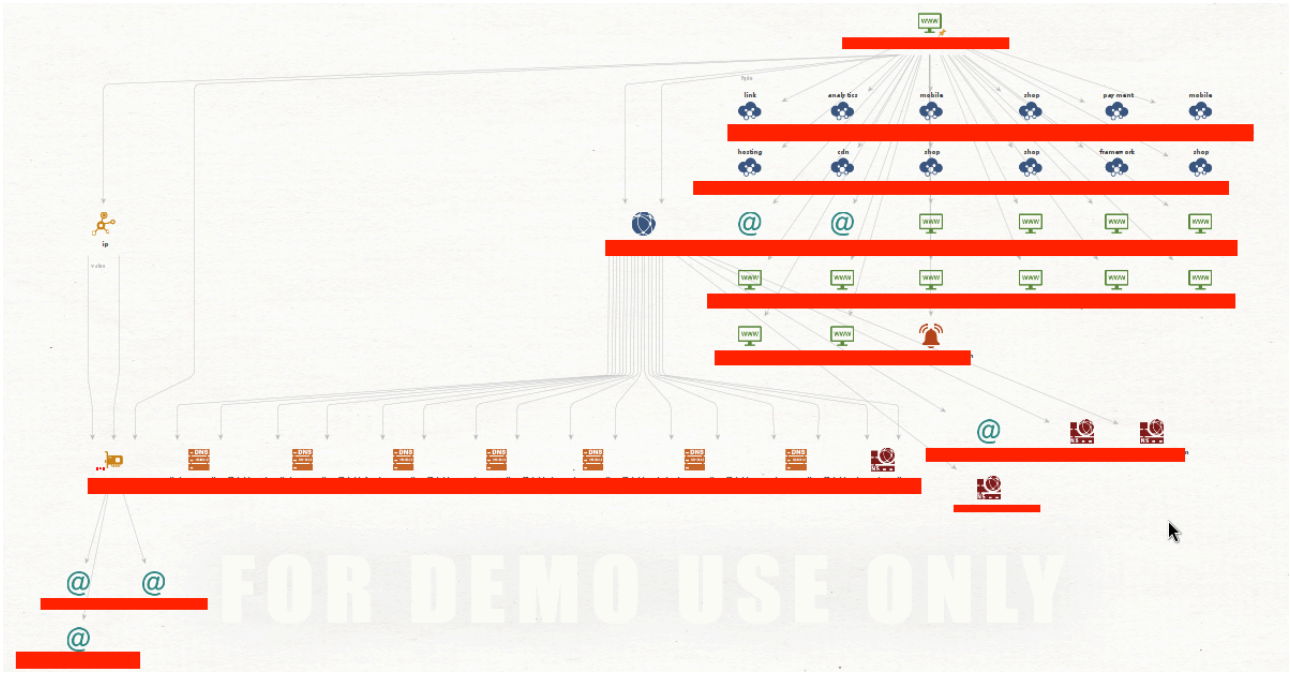
1.4. Risultati raggiunti

La sezione più interessante che abbiamo trovato risulta essere quella dello shop e quindi procederemo con Maltego per effettuare un ulteriore approfondimento alla ricerca di alcune mancanze di personalizzazione/gestione della piattaforma shopify.

---

2. Maltego

Abbiamo approfondito l'analisi tramite Maltego sul portale shop.**sito_target**.it.



Maltego ha rilevato 6 mail sicuramente non gestite/presidiate essendo visibilmente email standard con nome utente postmaster/hostmaster o con nomi non collegati direttamente al target, come ad esempio un account gmail.com.

E' stata inoltre identificata la piattaforma che ospita il portale, ovvero Aruba, e con un server Cloudflare probabilmente per ovviare a problemi di scalabilità o di attacchi di DDoS.

Abbiamo rilevato dei server per la gestione standard di alcuni servizi, probabilmente non necessari all'erogazione del servizio shop, ossia:

- mail
- webmail
- ftp
- mx
- imap
- admin (è stato verificato e porta all'admin di aruba)
- smtp