Esercitazione WEEK 10 D4

Google Hacking, Dmitry, Recon-ng, Maltego

Ettore Farris - 10/01/2024

Descrizione sintetica

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 più che altro familiarizzare con i tool principali della fase di information gathering, quali:

- Google, per la raccolta passiva delle info
- dmirty
- Recon-ng
- 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 moduli utilizzati (dove applicabile)
- I risultati ottenuti

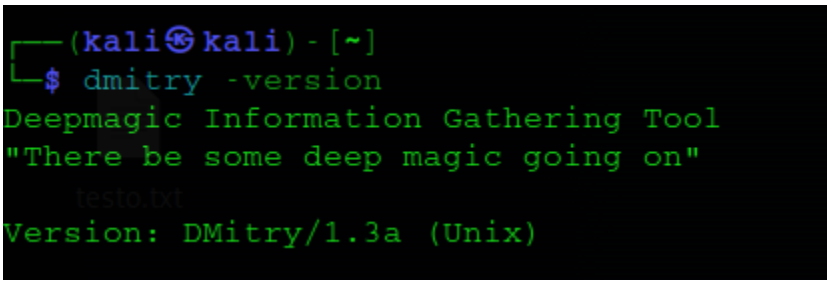
1) Google Hacking

Per effettuare la ricerca, utilizzerò il target dell'esercitazione precedente. Per i dorks, si veda il documento *Esercitazione WEEK 10_1 - Google Hacking.pdf*

2) dmitry

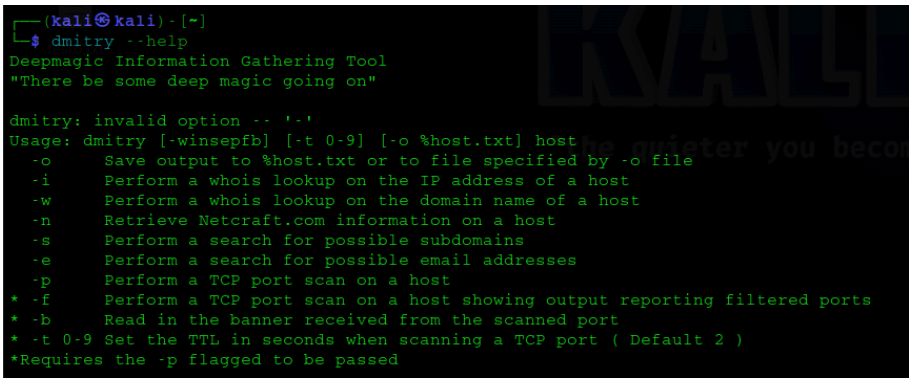
- *Versione*

Lanciando il comando dmitry -version otteniamo la versione del di dmitry

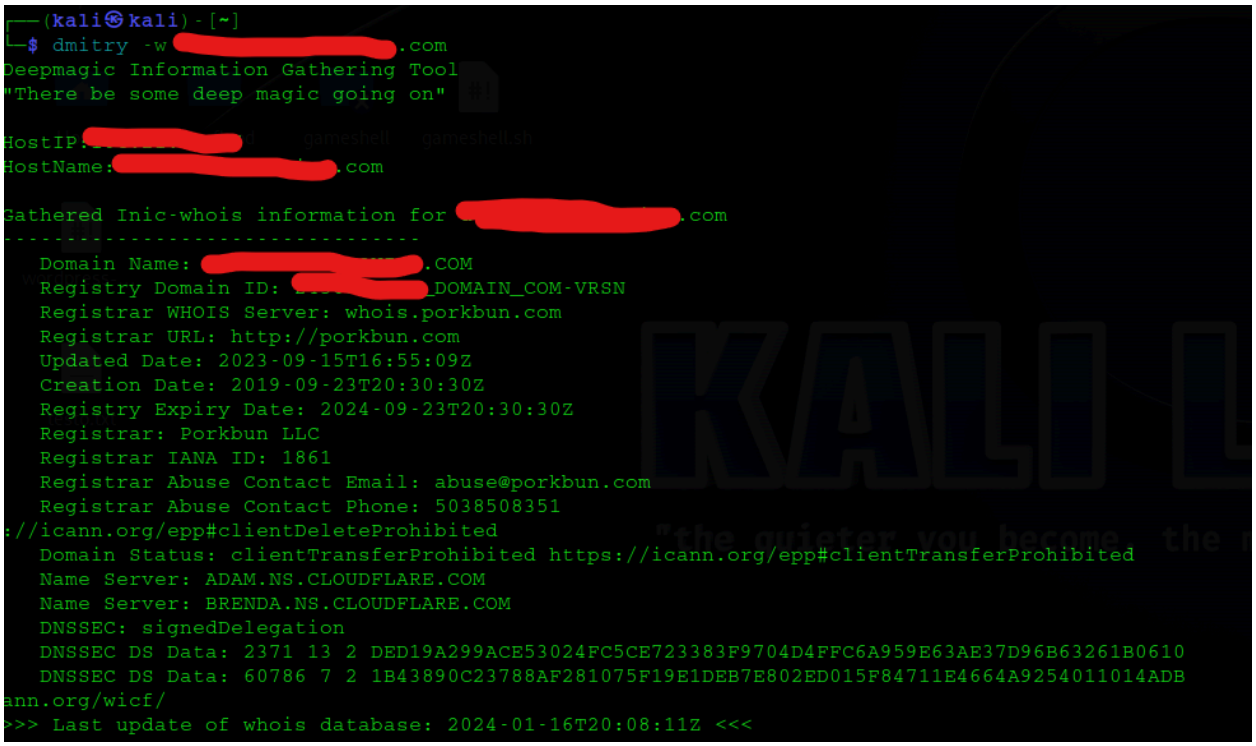


- Scopo

Il tool è utilizzato per scoprire informazioni preziose sul target, come ricerche *whois lookups,* indirizzi email, sottodomini, scansioni TCP, informazioni netcraft e tante altre. E' possibile fare ricerche mirate utilizzando flag specifici. Dall'help del tool:



Per il target selezionato, ho scelto di svolgere una ricerca *whois lookup* indicando il dominio del target utilizzando il comando *dmitry -w esempio.com*



Con questa scan abbiamo ottenuto l'indirizzo IP del target e i dati sul dominio, come registrazione, scadenza e provider, in questo caso *porkbun.com.*

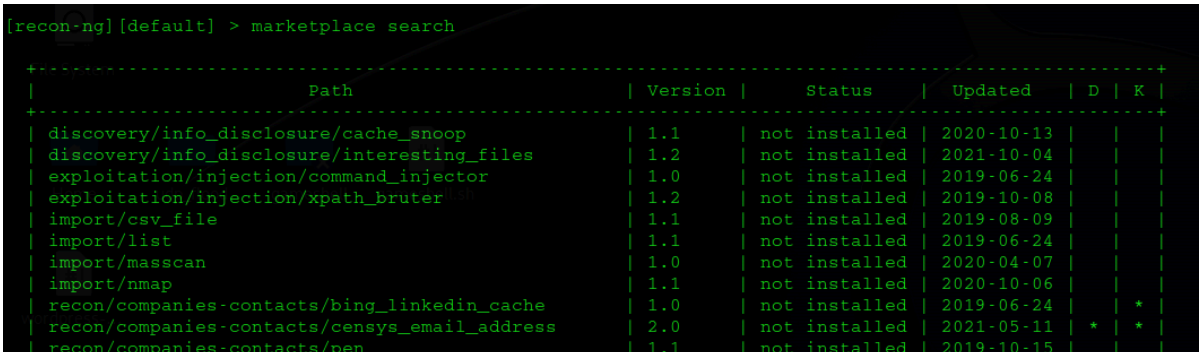
3) Recon-ng

- **Versione**

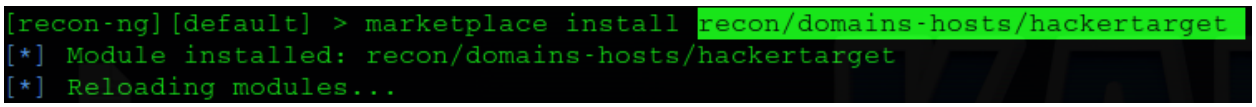
Lanciando il tool col comando *recon-ng* è possibile scoprire la versione del tool

- ***Utilizzo e risultati***

Recon-ng è un potente tool di *information gathering* che mette a disposizione un nutrito numero di moduli per diversi scopi, come scansioni nmap, ricerca di sottodomini, email harvesting, dati netcraft, OSINT (Open-Source Intelligence) ecc...Una volta lanciato il programma, è possibile vedere tutti i moduli a disposizione con il comando *marketplace search*.



In questo esempio, ho effettuato la ricerca di sottodomini per il target scelto con il modulo *recon/domains-hosts/hackertarget.* Per installare in modulo i lancia in comando *marketplace install <path del modulo modulo>,* in questo caso *recon/domains-hosts/hackertarget,* trovato tramite la ricerca *marketplace search.*



Per poter usare questo modulo contro il nostro target è necessario seguire alcuni passaggi che sono simili per tutti i moduli:

- *modules load <path del modulo>*

Con questo comando abilitiamo il modulo installato. Questo passaggio è necessario in quanto i moduli installati possono essere molteplici.

- *info*

Una volta caricato il modulo, si usa questo comando per avere informazioni sul suo funzionamento e per verificare quali parametri (options) è necessario impostare per lanciare la ricerca delle informazioni.

- *options set <OPZIONE> <target>*

Per impostare i parametri è necessario specificare il loro nome e impostarne il valore. Nel caso della nostra ricerca, il parametro è *SOURCE*, il cui valore sarà impostato con il dominio del target. Per verificare che questo sia stato impostato correttamente, rilanciare il comando *info.*

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
 Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default         SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>        string representing a single input
  <path>          path to a file containing a list of inputs
  query <sql>     database query returning one column of inputs

[recon-ng][default][hackertarget] > options set SOURCE [redacted].com
SOURCE => [redacted].com
```

```
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
 Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value          Required  Description
  ------  -------------          --------  -----------
  SOURCE  [redacted].com  yes       source of input (see 'info' for details)

Source Options:
  default         SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>        string representing a single input
  <path>          path to a file containing a list of inputs
  query <sql>     database query returning one column of inputs
```

- *run*

Una volta installato e caricato il modulo e impostati i parametri, si lancia la ricerca lanciando semplicemente *run.* Dopo un po' di tempo compariranno i risultati sul terminale

Dalla ricerca emergono due sottodomini con i relativi IP oltre a quello principale. Queste informazioni possono poi essere utilizzate per effettuare ulteriori ricerche.

4) Maltego

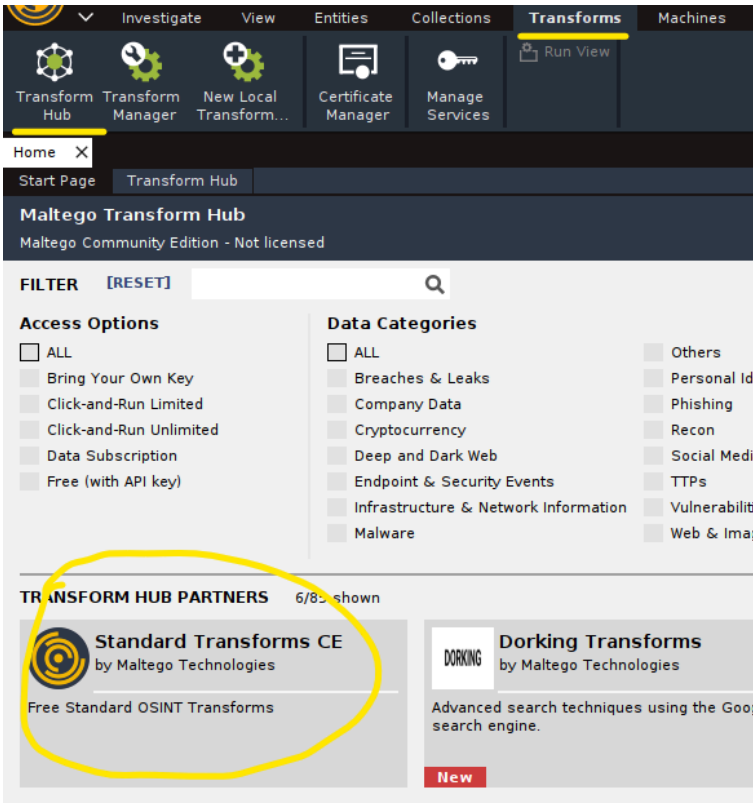
- ***Versione***

Maltego è un software che ha diverse versioni a seconda della licenza che si possiede. Quella presente su Kali è la Community Edition 4.4.1.

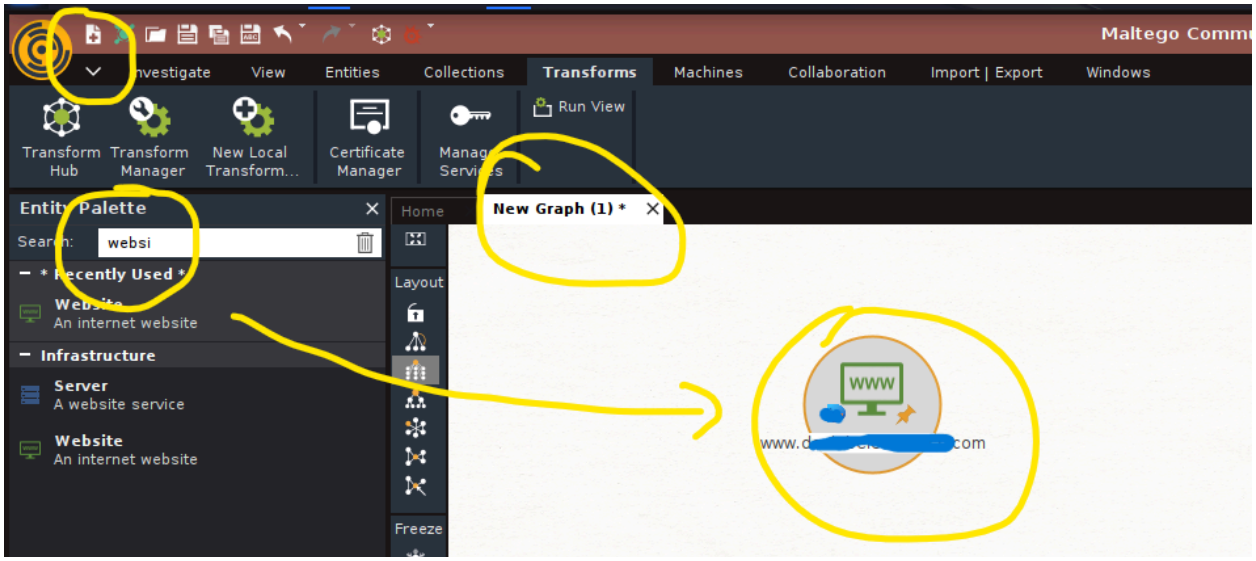
- ***Utilizzo e risultati***

Maltego è un potentissimo strumento *all-in-one* utilizzato per la ricerca di dati e informazioni sul target. Ha un'interfaccia grafica che offre una rappresentazione dei risultati che consente un'interpretazione intuitiva dei risultati. L'installer del programma è presente su Kali Linux.

Una volta installato, si lancia il programma ricercando tra le applicazioni installate oppure tramite linea di comando scrivendo semplicemente *maltego.* Il programma ha una GUI con molti elementi e una suddivisione in pagine per ogni scansione. E' dotato inoltre di plugin chiamati *transforms.* Per prima cosa, si installano questi nella tab Transform. Maltego mette a disposizione una libreria standard che verrà usata nell'esempio.

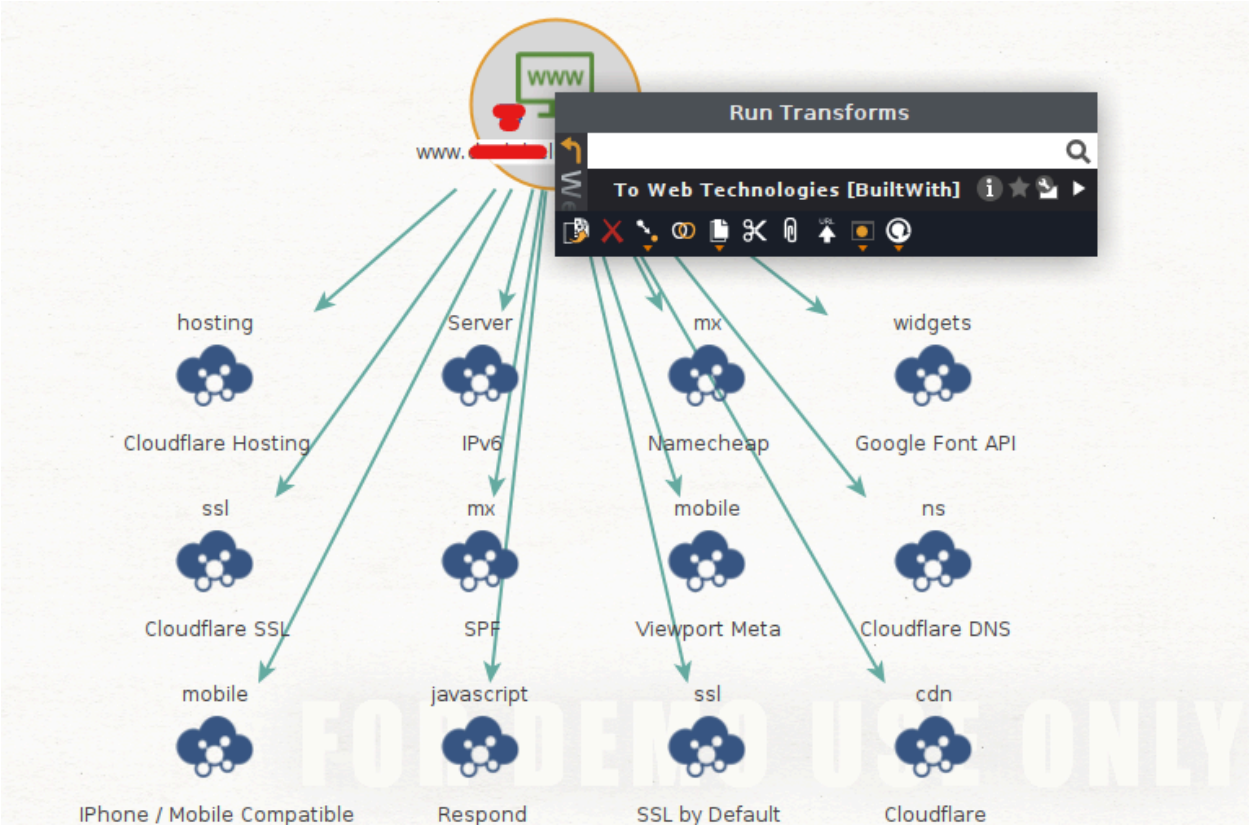


Per effettuare una ricerca sul target creiamo un nuovo *graph* (ovvero una pagina con la visualizzazione grafica delle informazioni) e trasciniamo un elemento di partenza. In questo caso, vogliamo informazioni sul sito web target, quindi trasciniamo un elemento "*website*".



Cliccando tasto destro sul nostro elemento appariranno tutti i tipi di ricerca disponibili. In questo caso, la ricerca svolta sul target è quella "web technologies", ovvero quella sulle tecnologie che compongono il sito web (vedi pagina successiva).

I risultati ottenuti mostrano che il sito ha le numerose tecnologie attive come un CDN Cloudflare, l'API di Google Fonts e così via.


www
www.[redacted]
Run Transforms
To Web Technologies [BuiltWith]
hosting
Cloudflare Hosting
ssl
Cloudflare SSL
mobile
IPhone / Mobile Compatible
Server
IPv6
mx
SPF
javascript
Respond
mx
Namecheap
mobile
Viewport Meta
ssl
SSL by Default
widgets
Google Font API
ns
Cloudflare DNS
cdn
Cloudflare