

Esercitazione WEEK 10 D1 (2)

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

```
(kali㉿kali) - [~]  
$ dmitry -version  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
testo.txt  
Version: DMitry/1.3a (Unix)
```

- 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:

```
(kali㉿kali) - [~]  
$ dmitry --help  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
dmitry: invalid option -- '-'  
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host  
-o Save output to %host.txt or to file specified by -o file  
-i Perform a whois lookup on the IP address of a host  
-w Perform a whois lookup on the domain name of a host  
-n Retrieve Netcraft.com information on a host  
-s Perform a search for possible subdomains  
-e Perform a search for possible email addresses  
-p Perform a TCP port scan on a host  
* -f Perform a TCP port scan on a host showing output reporting filtered ports  
* -b Read in the banner received from the scanned port  
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )  
* Requires the -p flagged to be passed
```

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

```
(kali㉿kali) - [~]
$ dmitry -w [REDACTED].com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP: [REDACTED] gameShell gameShell.sh
HostName: [REDACTED].com

Gathered Inic-whois information for [REDACTED].com
-----
Domain Name: [REDACTED].COM
Registry Domain ID: [REDACTED].DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.porkbun.com
Registrar URL: http://porkbun.com
Updated Date: 2023-09-15T16:55:09Z
Creation Date: 2019-09-23T20:30:30Z
Registry Expiry Date: 2024-09-23T20:30:30Z
Registrar: Porkbun LLC
Registrar IANA ID: 1861
Registrar Abuse Contact Email: abuse@porkbun.com
Registrar Abuse Contact Phone: 5038508351
: //icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ADAM.NS.CLOUDFLARE.COM
Name Server: BRENDA.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 DED19A299ACE53024FC5CE723383F9704D4FFC6A959E63AE37D96B63261B0610
DNSSEC DS Data: 60786 7 2 1B43890C23788AF281075F19E1DEB7E802ED015F84711E4664A9254011014ADB
ann.org/wicf/
>>> Last update of whois database: 2024-01-16T20:08:11Z <<<
```

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*.

- Versione

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

```
(kali)~[~]
$ recon-ng
[*] Version check disabled.
```

System

Home udp_flood gameshell gameshellsh

Sponsored by...

wordpress

test.txt

```

      /\
     /\ \
    /\  \
   /\    \
  /\      \
 /\        \
/\          \
\           \
 \          \
  \         \
   \        \
    \       \
     \      \
      \     \
       \    \
        \   \
         \  \
          \ \
           \|v \|
          /\  /\
         /  \/  \
        //  \\  \|v \|
       //  //  \\ \|v \|
      //  //  BLACK HILLS  \|v \|
      www.blackhillsinfosec.com

  _ _ _ _ _ _ _ _ _ _
 | |_|_|_|_|_|_|_|_|_|
|_|_|_|_|_|_|_|_|_|_|
www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
```

- 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*.

```
[recon-ng][default] > marketplace search
```

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
discovery/info_disclosure/interesting_files	1.2	not installed	2021-10-04		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		
import/nmap	1.1	not installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache	1.0	not installed	2019-06-24		*
recon/companies-contacts/censys_email_address	2.0	not installed	2021-05-11	*	*
recon/companies-contacts/censys_email_addresses	1.3	not installed	2022-02-15		

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*.

```
[recon-ng] [default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
```

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 default.hackertarget.com
SOURCE => default.hackertarget.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     default.hackertarget.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

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

```
-----  
[*] Country: None  
[*] Host: [REDACTED].COM  
[*] Ip_Address: [REDACTED]  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: [REDACTED].com  
[*] Ip_Address: [REDACTED]  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] Country: None  
[*] Host: [REDACTED].com  
[*] Ip_Address: [REDACTED]  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----
```

```
SUMMARY
```

```
[*] 3 total (3 new) hosts found.
```

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

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

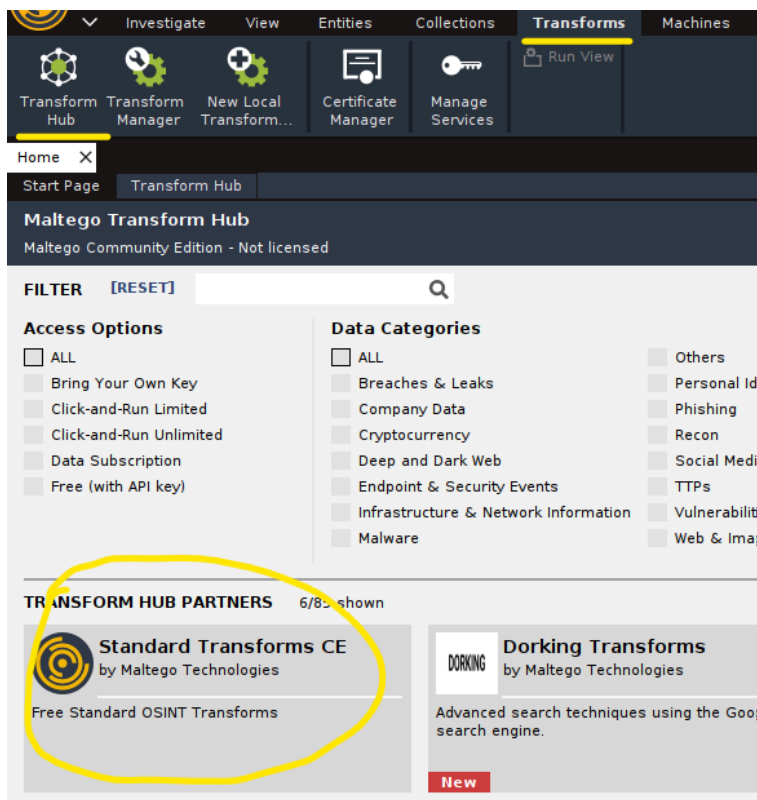
- Versione

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.

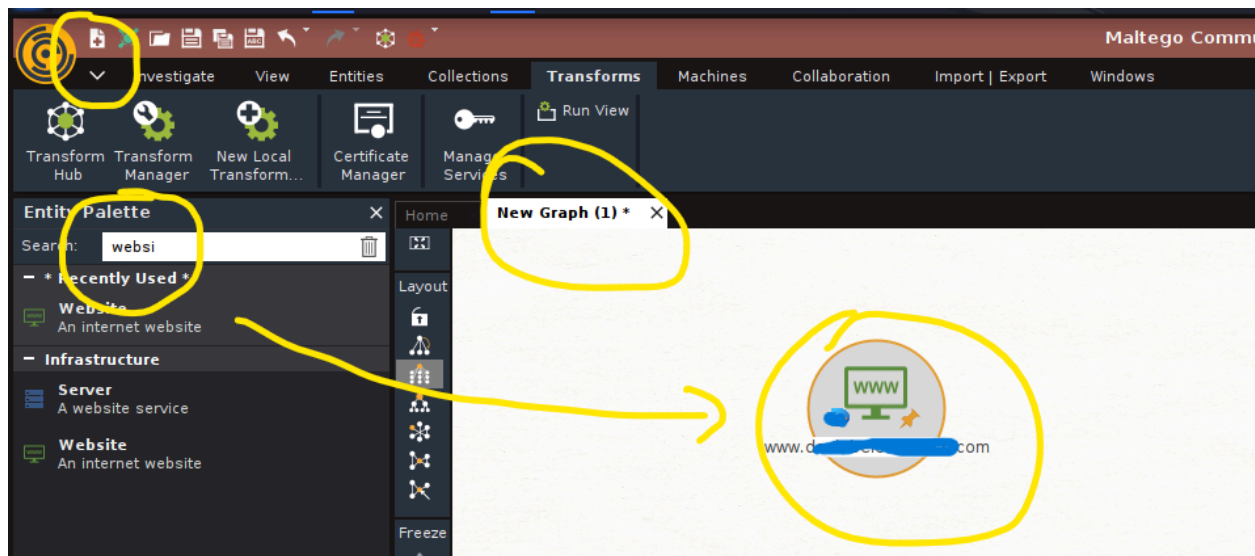
- Utilizzo e risultati

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.

