Appunti: Fase di Raccolta Informazioni

Raccolta informazioni passiva su Google
Cosa fa l'azienda target?
La struttura dei dipartimenti? Informazioni sulla rete dell'azienda?
Ci sono siti web o piattaforme e-commerce? E se si, come sono strutturati?

intitle:(ricerca) restituisce tutte le pagine che hanno nel title di html la mia ricerca
ctrl u: fa visualizzare il codice sorgente della pagina web che sto visitando
inurl: ricerca restituisce tutte le pagine che nel proprio url contengono la ricerca e non necessariamente solo nel titolo
Site:ricerca.com restituisce tutti i risultati nella forma "*.Ricerca.com": ci aiuta a capire l'esposizione sul web del target
Filetype:doc -usabile anche in concatenazioni, es:inurl:ricerca filetype:doc (dove doc è .xlsx, .docx, .pptx, .txt, .pdf)- che restituisce documenti
link cerca pagine che mandano link ad altre pagine
cache restituisce le pagine web in cache, che sono state eliminate da meno di 90 giorni e ci fa vedere da quanto sono state eliminate. la sintassi è "*cache:sito.com*" o "*cache:https://www.sito.dominio2*"
numrange restituisce tutti i numeri dentro al range specificato (non serve selezionare numrange ma basta scrivere i due numeri (es. di cellulare) divisi da un trattino. es: insite: azienda num1-num2
stocks:ricerca restituisce informazioni di mercato finanziario sull'azienda target
define:ricerca restituisce la definizione del termine di ricerca
phonebook: ricerca restituisce i numeri di telefono. Ho 2 varianti:
rphonebook per i contatti privati o residenziali
bphonebook per i business contact
allintext:ricerca restituisce una stringa all'interno di una pagina
directory listing è un tipo di pagina web che elenca directory e file su un web server. es: *intitle:index.of inurl:admin* troverebbe nell'url i documenti con la parola admin.
directory trasversal restituisce i suggerimenti per spostarsi su altre directory, una volta trovatane una.

Nella fase di information gathering puo essere utile recuperare info anche sui dipendenti:
(es: n dell help desk, info sul dipartimento it, email degli impiegati, ma anche curriculum, pagine web personali, cover letter, social network, n di cellulare)

il dominio top level: .com/.it/...
il sottodominio es: www.shop.google.com
site crawling scova tutti i sottodomini. La sua sintassi è site:esempio.com -site:www.esempio.com.

Su recon-ng abbiamo usato il modulo whois

```
[recon-ng][default] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0
```

```
Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' 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][whois_pocs] > options set SOURCE google.com
SOURCE => google.com
```

Mando il comando run

```
[*] URL: http://whois.arin.net/rest/pocs;domain=google.com
[*] URL: http://whois.arin.net/rest/poc/ABH14-ARIN
[*] Country: United States
[*] Email: alan.hoshor@google.com
[*] First_Name: Alan
[*] Last_Name: Hoshor
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Everett, WA
[*] Title: Whois contact
[*] ---------- ----------------------------------
[*] URL: http://whois.arin.net/rest/poc/ABA104-ARIN
[*] Country: United States
[*] Email: ari@google.com
[*] First_Name: Ari
[*] Last_Name: Barkan
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Mountain View, CA
[*] Title: Whois contact
[*] ---------- ----------------------------------
[*] URL: http://whois.arin.net/rest/poc/ABA105-ARIN
[*] Country: United States
[*] Email: ari@google.com
[*] First_Name: Ari
[*] Last_Name: Barkan
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Mountain View, CA
[*] Title: Whois contact
[*]
```

```
-------
SUMMARY
-------
[*] 31 total (7 new) contacts found.
[recon-ng][default][whois_pocs] >
```

Abbiamo trovato 31 risultati, 7 nuovi contatti con relativo nome, cognome regione email e codice/i POC

```
URL: http://whois.arin.net/rest/pocs;domain=google.com
URL: http://whois.arin.net/rest/poc/ABH14-ARIN
Country: United States
Email: alan.hoshor@google.com
First_Name: Alan
Last_Name: Hoshor
Middle_Name: None
Notes: None
Phone: None
Region: Everett, WA
Title: Whois contact
---------- ----------------------------------
URL: http://whois.arin.net/rest/poc/ABA104-ARIN
Country: United States
Email: ari@google.com
First_Name: Ari
```

```
Last_Name: Barkan
Middle_Name: None
Notes: None
Phone: None
Region: Mountain View, CA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/ABA105-ARIN
Country: United States
Email: ari@google.com
First_Name: Ari
Last_Name: Barkan
Middle_Name: None
Notes: None
Phone: None
Region: Mountain View, CA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/ZG39-ARIN
Country: United States
Email: arin-contact@google.com
First_Name: None
Last_Name: Google LLC
Middle_Name: None
Notes: None
Phone: None
Region: Mountain View, CA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/ALS11-ARIN
Country: Switzerland
Email: arturolev@google.com
First_Name: Arturo
Last_Name: Servin
Middle_Name: None
Notes: None
```

```
URL: http://whois.arin.net/rest/poc/BROWN545-ARIN
Country: United States
Email: brownlow@google.com
First_Name: Tom
Last_Name: Brownlow
Middle_Name: None
Notes: None
Phone: None
Region: San Francisco, CA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/CJC43-ARIN
Country: United States
Email: cjac@google.com
First_Name: Carl
Last_Name: Collier
Middle_Name: None
Notes: None
Phone: None
Region: Seattle, WA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/CJC44-ARIN
Country: United States
Email: cjac@google.com
First_Name: Carl
Last_Name: Collier
Middle_Name: None
Notes: None
Phone: None
Region: Seattle, WA
Title: Whois contact
-----------------------------------------------------------
URL: http://whois.arin.net/rest/poc/SCHWA252-ARIN
Country: United States
Email: daveschwartz@google.com
First_Name: Dave
Last_Name: Schwartz
Middle_Name: None
Notes: None
Phone: None
Region: Mountain View, CA
Title: Whois contact
-----------------------------------------------------------
```

```
URL: http://whois.arin.net/rest/poc/SCHWA253-ARIN
Country: United States
Email: daveschwartz@google.com
First_Name: Dave
Last_Name: Schwartz
Middle_Name: None
Notes: None
```

Abbiamo scoperto ad esempio che Dave Schwartz è identificato da ben 26 codici POC (dal 252 al 271 e dal 278 al 283, numeri tutti preceduti dal prefisso SCHWA e seguiti dal suffisso -ARIN)
Quindi cerchiamo

Nota

Il codice POC (Point of Contact) è un identificatore univoco associato a un contatto nel database WHOIS di un registro di numeri Internet (ad esempio, ARIN, RIPE NCC, APNIC, ecc.) e viene utilizzato per identificare un punto di contatto tecnico o amministrativo per un determinato indirizzo IP o dominio.

Il codice POC può essere utile per identificare il punto di contatto di una particolare organizzazione o persona per un determinato indirizzo IP o dominio. Ad esempio, se si verificano problemi di rete o di sicurezza con un sito web o un indirizzo IP, è possibile utilizzare il codice POC per contattare la persona o l'organizzazione responsabile di quel particolare indirizzo.

Tuttavia, è importante notare che il codice POC non è sempre aggiornato e potrebbe non essere l'unico punto di contatto disponibile per un determinato indirizzo IP o dominio. Inoltre, il codice POC non fornisce informazioni dettagliate sul proprietario del dominio o sull'organizzazione che possiede o gestisce l'indirizzo IP, quindi potrebbe essere necessario utilizzare altre fonti di informazioni per ottenere maggiori dettagli.

```
[recon-ng][default] > marketplace search [<daveschwartz@google.com >]
[*] Searching module index for '[<daveschwartz@google.com >]' ...

+-----------------------------------------------+---------+-----------+------------+---+---+
|                     Path                      | Version |   Status  |  Updated   | D | K |
+-----------------------------------------------+---------+-----------+------------+---+---+
| discovery/info_disclosure/cache_snoop         | 1.1     | installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files   | 1.2     | installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector       | 1.0     | installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter           | 1.2     | installed | 2019-10-08 |   |   |
| import/csv_file                               | 1.1     | installed | 2019-08-09 |   |   |
| import/list                                   | 1.1     | installed | 2019-06-24 |   |   |
| import/masscan                                | 1.0     | installed | 2020-04-07 |   |   |
| import/nmap                                   | 1.1     | installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache  | 1.0     | installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-contacts/pen                  | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains     | 2.0     | installed | 2021-05-10 | * | * |
| recon/companies-domains/pen                   | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois | 1.1     | installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns             | 1.1     | installed | 2020-06-17 |   | * |
| recon/companies-hosts/censys_org              | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-hosts/censys_tls_subjects     | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-multi/github_miner            | 1.1     | installed | 2020-05-15 |   | * |
| recon/companies-multi/shodan_org              | 1.1     | installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner             | 1.1     | installed | 2019-10-15 |   |   |
| recon/contacts-contacts/abc                   | 1.0     | installed | 2019-10-11 | * |   |
| recon/contacts-contacts/mailtester            | 1.0     | installed | 2019-06-24 |   |   |
| recon/contacts-contacts/mangle                | 1.0     | installed | 2019-06-24 |   |   |
| recon/contacts-contacts/unmangle              | 1.1     | installed | 2019-10-27 |   |   |
| recon/contacts-credentials/hibp_breach        | 1.2     | installed | 2019-09-10 |   | * |
| recon/contacts-credentials/hibp_paste         | 1.1     | installed | 2019-09-10 |   | * |
| recon/contacts-domains/migrate_contacts       | 1.1     | installed | 2020-05-17 |   |   |
| recon/contacts-profiles/fullcontact           | 1.1     | installed | 2019-07-24 |   | * |
| recon/credentials-credentials/adobe           | 1.0     | installed | 2019-06-24 |   |   |
| recon/credentials-credentials/bozocrack       | 1.0     | installed | 2019-06-24 |   |   |
```

```
| recon/credentials-credentials/hashes_org                | 1.0 | installed | 2019-06-24 |   |   | * |
| recon/domains-companies/censys_companies                | 2.0 | disabled  | 2021-05-10 | * |   | * |
| recon/domains-companies/pen                             | 1.1 | installed | 2019-10-15 |   |   |   |
| recon/domains-companies/whoxy_whois                     | 1.1 | installed | 2020-06-24 |   |   | * |
| recon/domains-contacts/hunter_io                        | 1.3 | installed | 2020-04-14 |   |   | * |
| recon/domains-contacts/metacrawler                      | 1.1 | disabled  | 2019-06-24 | * |   |   |
| recon/domains-contacts/pen                              | 1.1 | installed | 2019-10-15 |   |   |   |
| recon/domains-contacts/pgp_search                       | 1.4 | installed | 2019-10-16 |   |   |   |
| recon/domains-contacts/whois_pocs                       | 1.0 | installed | 2019-06-24 |   |   |   |
| recon/domains-contacts/wikileaker                       | 1.0 | installed | 2020-04-08 |   |   |   |
| recon/domains-credentials/pwnedlist/account_creds       | 1.0 | disabled  | 2019-06-24 | * |   | * |
| recon/domains-credentials/pwnedlist/api_usage           | 1.0 | installed | 2019-06-24 |   |   | * |
| recon/domains-credentials/pwnedlist/domain_creds        | 1.0 | disabled  | 2019-06-24 | * |   | * |
| recon/domains-credentials/pwnedlist/domain_ispwned      | 1.0 | installed | 2019-06-24 |   |   | * |
| recon/domains-credentials/pwnedlist/leak_lookup         | 1.0 | installed | 2019-06-24 |   |   |   |
```

Su Maltego ho usato le query viste a lezione per individuare notizie sull'azienda Epicode. Le query utilizzate sono: Website, URLs, Entity.