

Simulazione fase di raccolta

Sommario

Traccia esercizio principale	2
Traccia esercizio facoltativo	2
Svolgimento esercizio principale	4
Google Hacking.....	4
Valutazione dei risultati della ricerca	5
Svolgimento esercizio facoltativo	6
Recon-ng	6
Cos'è recon-ng	6
Installazione moduli.....	6
Procedimento di ricerca.....	6
Utilizzo di whois nel terminale.....	7
Modifica del target da istituzionale a privato epicode.com	8
Ricerca sulla società epicode tramite il sito	9
Maltego	11
Cos'è ed a cosa serve	11
Ricerca su Xi Jinping.....	12

Traccia esercizio principale

Utilizzare i comandi di Google Hacking per raccogliere informazioni su un sito web.

Istruzioni:

1. Aprire un browser web e accedere a Google.
2. Utilizzare i seguenti comandi di Google Hacking per raccogliere informazioni sul sito web:
 - "site:nome-del-sito.com" per visualizzare tutte le pagine indicizzate di quel sito.
 - "inurl:nome-del-sito.com" per visualizzare tutte le pagine con l'URL contenente il nome del sito.
 - "intext:'parola chiave' site:nome-del-sito.com" per visualizzare tutte le pagine che contengono la parola chiave specificata nel testo del sito.
 - "filetype:estensione site:nome-del-sito.com" per visualizzare tutti i file con l'estensione specificata presenti sul sito.
3. Utilizzare i risultati per identificare eventuali informazioni sensibili o vulnerabilità presenti sul sito.
4. Utilizzare queste informazioni per valutare la sicurezza del sito e prendere le misure necessarie per proteggere le informazioni sensibili.

Traccia esercizio facoltativo

Estendere la raccolta delle informazioni utilizzando:

- 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

Nome	Versione	Scopo	Note
Maltego			

Hint:

- ❖ Ricordate che potete utilizzare le query su Google Hacking DB – basta capire quale di quelle elencate può fare al caso vostro
- ❖ Per recon-ng, che come ricorderete è basato sui moduli, è fondamentale conoscere quanti più moduli utili possibile e i parametri necessari per eseguirli. Potete utilizzare da interfaccia di recon-ng la keyword «marketplace» seguita da «search» per cercare una specifica parola all'interno di un modulo.

Esempio: **marketplace search email**

```
[recon-ng][default] > marketplace
info  install refresh remove search
[recon-ng][default] > marketplace in
info  install
[recon-ng][default] > marketplace search email
[*] Searching module index for 'email' ...

+-----+-----+-----+-----+-----+-----+
| Path                                     | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/companies-contacts/censys_email_address | 2.0     | installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen                 | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/pen                 | 1.1     | installed | 2019-10-15 |   |   |
| recon/contacts-contacts/mailtester          | 1.0     | installed | 2019-06-24 |   |   |
| recon/contacts-contacts/mangle              | 1.0     | installed | 2019-06-24 |   |   |
| 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/domains-contacts/hunter_io            | 1.3     | installed | 2020-04-14 |   | * |
| recon/domains-contacts/pgp_search           | 1.4     | installed | 2019-10-16 |   |   |
| recon/domains-contacts/wikileaker           | 1.0     | installed | 2020-04-08 |   |   |
+-----+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > █
```

Per capire il modulo cosa fa, utilizziamo sempre la keyword marketplace come di seguito:

marketplace info «path modulo»

Questo comando vi darà diverse informazioni sul modulo ed una breve descrizione.

Dopo ogni keyword potete utilizzare il tasto «tab» per ricevere dei suggerimenti di quali comandi sono accettati da recon-ng.

```
[recon-ng][default] > marketplace info recon/contacts-contacts/mailtester

+-----+-----+
| path                                     | recon/contacts-contacts/mailtester |
| name                                    | MailTester Email Validator          |
| author                                   | Tim Tomes (@lanmaster53)           |
| version                                  | 1.0                                  |
| last_updated                             | 2019-06-24                          |
| description                              | Leverages MailTester.com to validate |
| required_keys                             | []                                   |
| dependencies                             | []                                   |
| files                                    | []                                   |
| status                                    | installed                            |
+-----+-----+

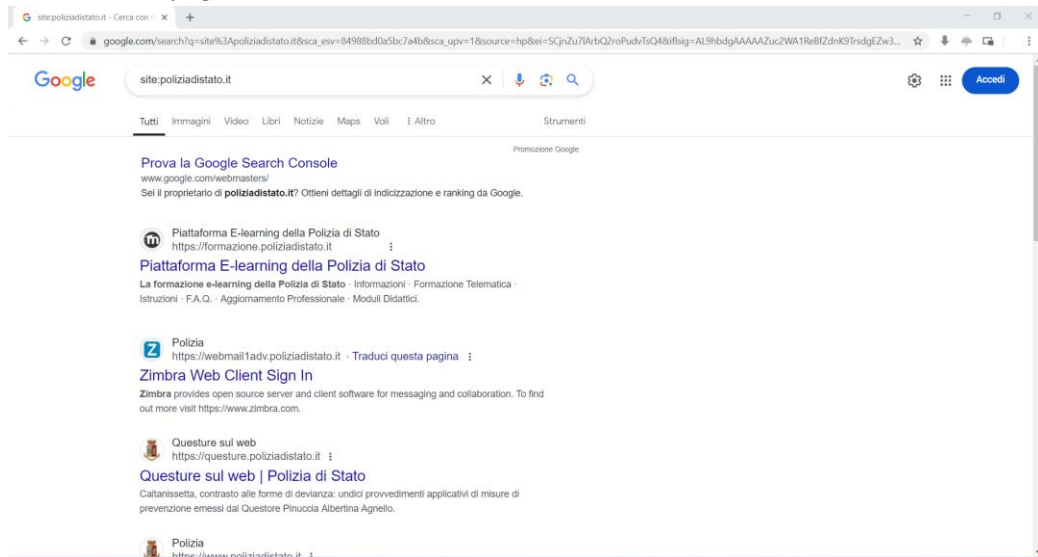
[recon-ng][default] > █
```

Svolgimento esercizio principale

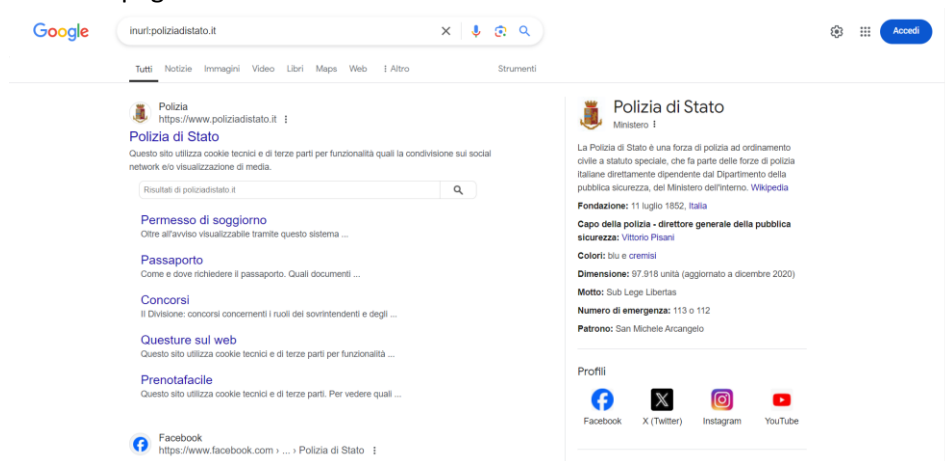
Google Hacking

La consegna chiede di eseguire una raccolta dati su un sito a scelta discrezionale. Per la stesura di questo report, pertanto, si è scelto il sito <https://www.poliziadistato.it/>. Aprirlo con browser e digitare

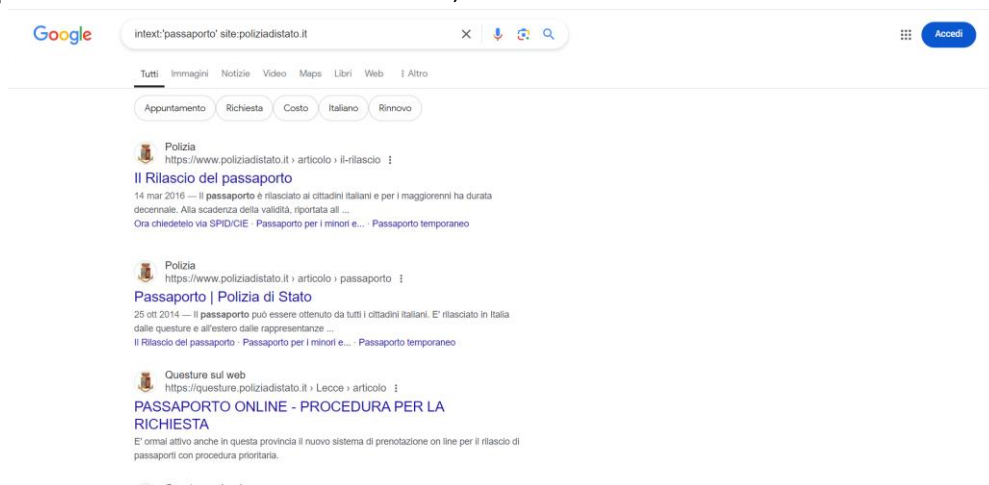
1. Visualizzare tutte le pagine indicizzate **site:nome-del-sito.com;**



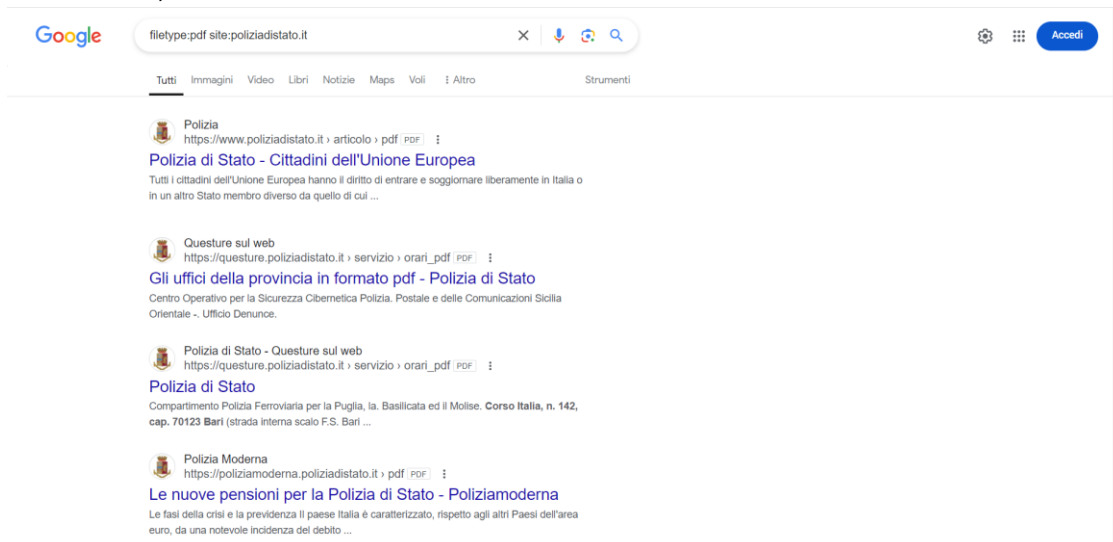
2. visualizzare tutte le pagine con l'URL contenente il nome del sito **inurl:nome-del-sito.com;**



3. visualizzare tutte le pagine che contengono la parola chiave specificata nel testo del sito **intext:'parola chiave' site:nome-del-sito.com;**

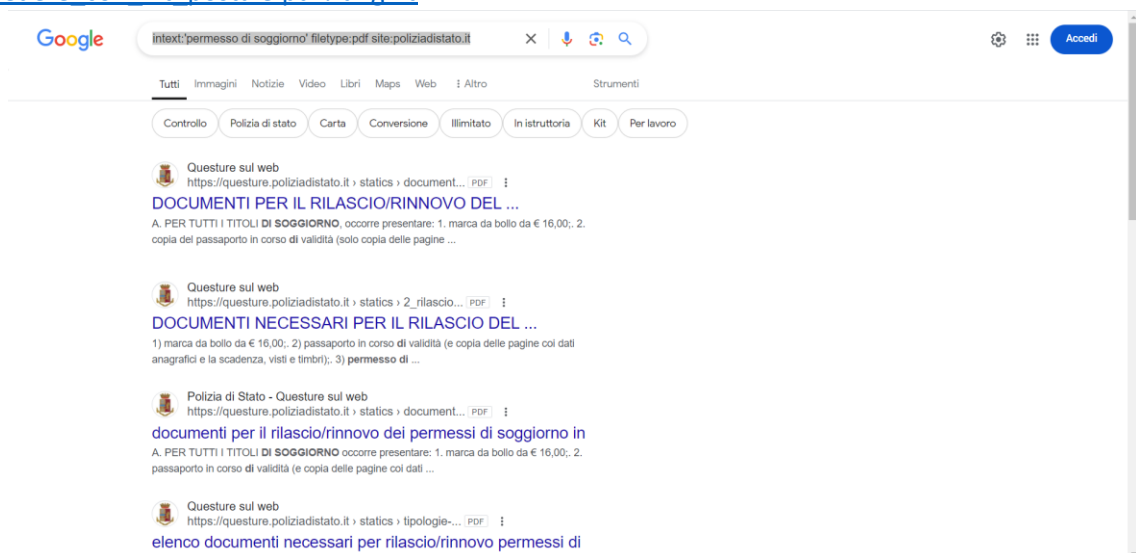


4. visualizzare tutti i file con l'estensione specificata presenti sul sito **filetype:estensione site:nome-del-sito.com**;



5. ricerca combinata inserendo: **"intext:'permesso di soggiorno' filetype:pdf site:poliziadistato.it"**
Come primo risultato dà una lista utile di documenti necessari per il rilascio o rinnovo del permesso di soggiorno.

https://questure.poliziadistato.it/statics/05/documenti_per_rilascio_permessi_di_soggiorno_da_richiedere_con_kit_postale.pdf?lang=it



Valutazione dei risultati della ricerca

Tramite la ricerca con Google Hacking non ha dato risultati soddisfacenti dal punto di vista di vulnerabilità da sfruttare, tuttavia tale ricerca è un ottimo strumento per coloro che cercano documentazione per svolgere pratiche burocratiche.

Si conclude pertanto che il sito della polizia di stato, analizzato solamente tramite il Google Hacking, è sicuro.

Svolgimento esercizio facoltativo

Recon-ng

Cos'è recon-ng

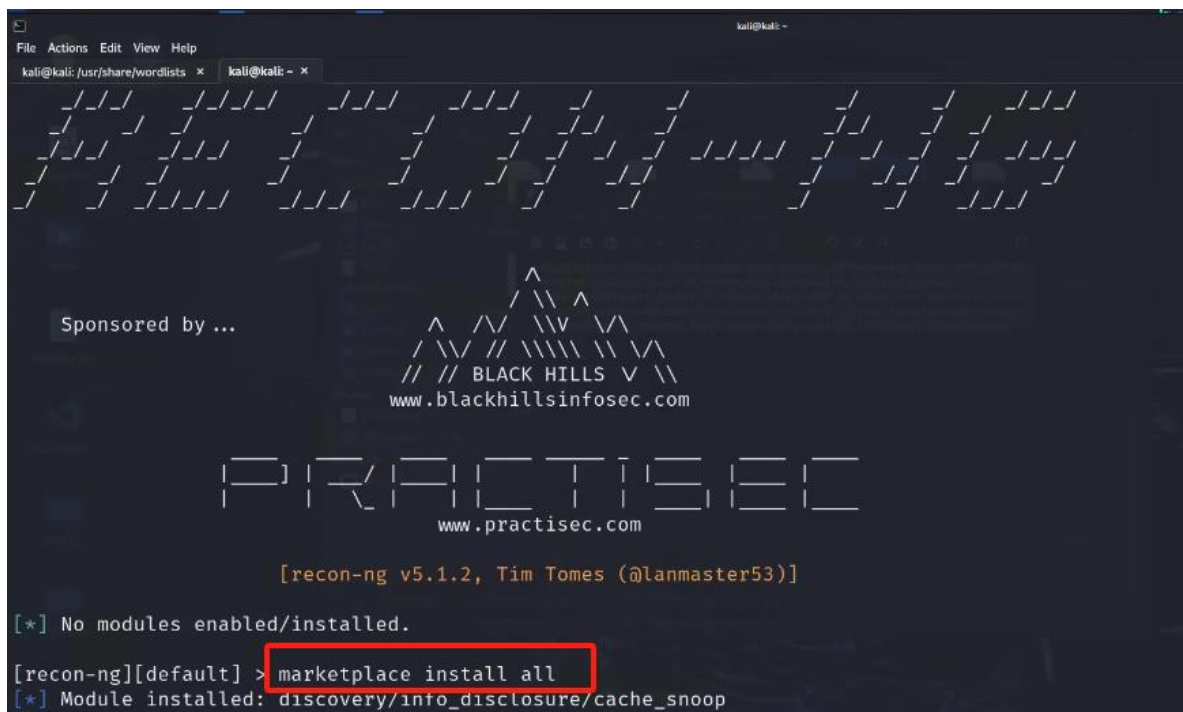
Recon-ng è uno strumento open-source di **ricognizione** per raccogliere informazioni durante la fase di **information gathering** nel penetration testing o nel campo della sicurezza informatica. È scritto in Python e offre un framework simile a Metasploit, con vari moduli per eseguire diverse attività di raccolta dati, come trovare informazioni su domini, IP, email, utenti e tanto altro.

Cos'è Recon-ng?

- **Framework di ricognizione:** È progettato per raccogliere informazioni da fonti pubblicamente disponibili (OSINT - Open Source Intelligence).
- **Modulare:** Dispone di vari moduli (simili ai plugin) che puoi caricare in base alle tue necessità, per eseguire diverse tecniche di ricognizione.
- **Automatizzato:** Permette di automatizzare vari task, come interrogare API di servizi esterni per raccogliere dati su domini o persone.

Installazione moduli

Per avviare lo strumento recon-ng, aprire il terminale di Kali e lanciare il comando **recon-ng**.
Installare tutti i moduli di recon-ng se assenti, comando **marketplace install all**



```
kali@kali: /usr/share/wordlists x kali@kali - x
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
```

Procedimento di ricerca

Per la ricerca sul dominio utilizzare il modulo WHOIS comando per l'avvio **modules load recon/domains-contacts/whois_pocs**

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

Impostazione del dominio target: Dopo aver caricato il modulo, il dominio target viene impostato utilizzando il comando **options set SOURCE poliziadistato.it**

```
[recon-ng][default][whois_pocs] > options set SOURCE poliziadistato.it
SOURCE ⇒ poliziadistato.it
[recon-ng][default][whois_pocs] > █
```

Eseguire il modulo: Una volta impostate le opzioni, si può eseguire il modulo con il comando **run**

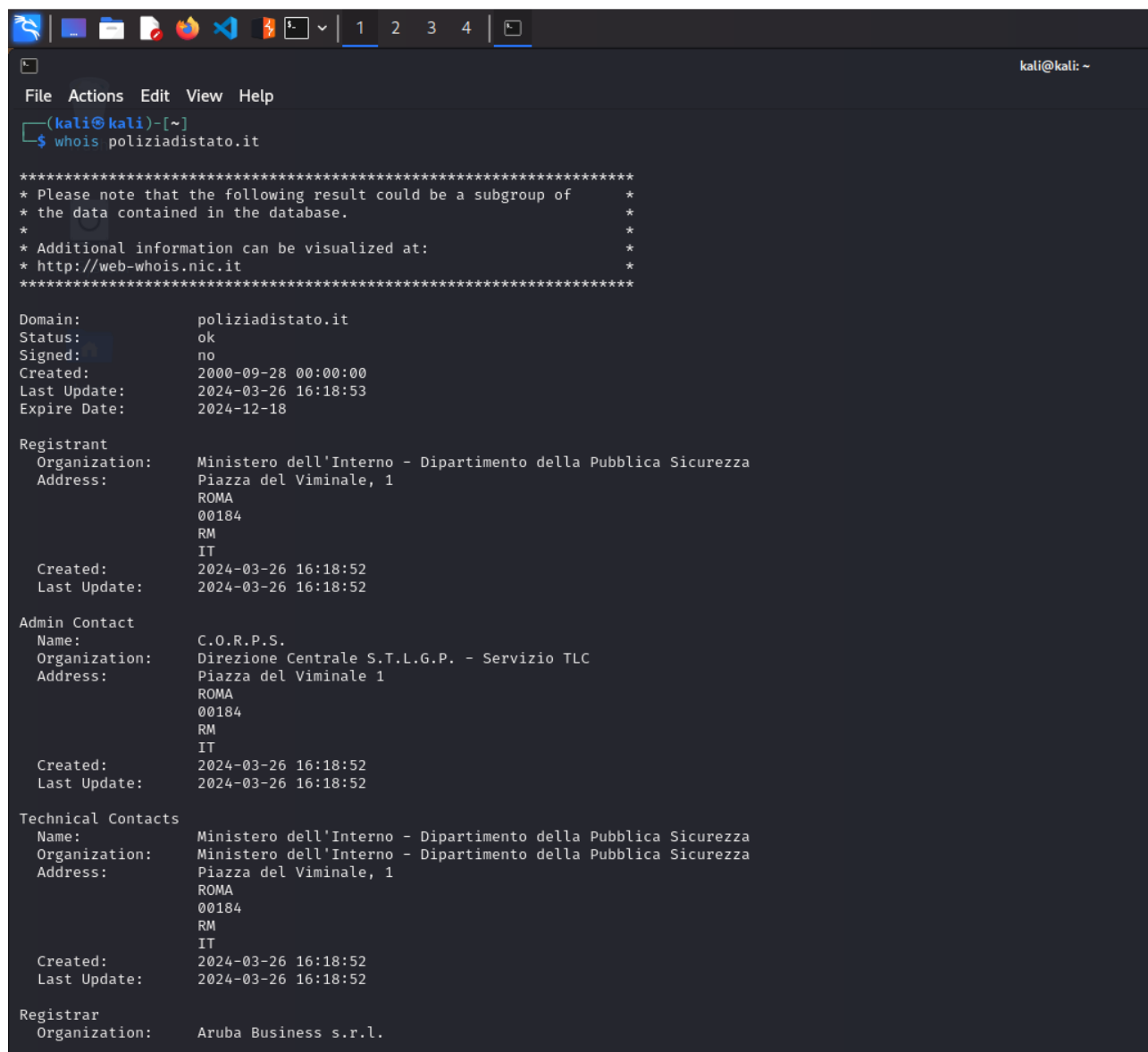
```
[recon-ng][default][whois_pocs] > options set SOURCE poliziadistato.it
SOURCE ⇒ poliziadistato.it
[recon-ng][default][whois_pocs] > run

=====
POLIZIADISTATO.IT
=====

[*] URL: http://whois.arin.net/rest/pocs;domain=poliziadistato.it
[*] No contacts found.
[recon-ng][default][whois_pocs] > █
```

Utilizzo di whois nel terminale

Attraverso il comando **whois poliziadistato.it** si ottengono varie informazioni sul dominio.



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ whois poliziadistato.it

*****
* Please note that the following result could be a subgroup of *
* the data contained in the database. *
* *
* Additional information can be visualized at: *
* http://web-whois.nic.it *
*****

Domain:                poliziadistato.it
Status:                ok
Signed:                no
Created:               2000-09-28 00:00:00
Last Update:           2024-03-26 16:18:53
Expire Date:           2024-12-18

Registrant
  Organization:         Ministero dell'Interno - Dipartimento della Pubblica Sicurezza
  Address:              Piazza del Viminale, 1
                      ROMA
                      00184
                      RM
                      IT
  Created:              2024-03-26 16:18:52
  Last Update:          2024-03-26 16:18:52

Admin Contact
  Name:                C.O.R.P.S.
  Organization:         Direzione Centrale S.T.L.G.P. - Servizio TLC
  Address:              Piazza del Viminale 1
                      ROMA
                      00184
                      RM
                      IT
  Created:              2024-03-26 16:18:52
  Last Update:          2024-03-26 16:18:52

Technical Contacts
  Name:                Ministero dell'Interno - Dipartimento della Pubblica Sicurezza
  Organization:         Ministero dell'Interno - Dipartimento della Pubblica Sicurezza
  Address:              Piazza del Viminale, 1
                      ROMA
                      00184
                      RM
                      IT
  Created:              2024-03-26 16:18:52
  Last Update:          2024-03-26 16:18:52

Registrar
  Organization:         Aruba Business s.r.l.
```


Modifica del target da istituzionale a privato epicode.com

Dato che poliziadistato.it è un dominio istituzionale, pertanto molto sicuro, ripetere la ricerca su un sito privato come epicode.com

- Tramite il Google Hacking non si è trovato nulla di rilevante per un possibile exploit da sfruttare.
- Tramite recon-ng con il modulo whois

```
[recon-ng][default] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > options set SOURCE epicode.com
SOURCE ⇒ epicode.com
[recon-ng][default][whois_pocs] > run

=====
EPICODE.COM
=====

[*] URL: http://whois.arin.net/rest/pocs;domain=epicode.com
[*] No contacts found.
[recon-ng][default][whois_pocs] > █
```

- Tramite shell whois

```
(kali@kali)~$ whois epicode.com
Domain Name: EPICODE.COM
Registry Domain ID: 26708081.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2023-05-13T05:04:09Z
Creation Date: 2000-05-09T18:57:38Z
Registry Expiry Date: 2031-05-09T18:57:38Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1492.AWSDNS-58.ORG
Name Server: NS-1580.AWSDNS-05.CO.UK
Name Server: NS-198.AWSDNS-24.COM
Name Server: NS-953.AWSDNS-55.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-09-16T13:23:37Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrant's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrant. Users may consult the sponsoring registrant's Whois database to
view the registrant's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
```

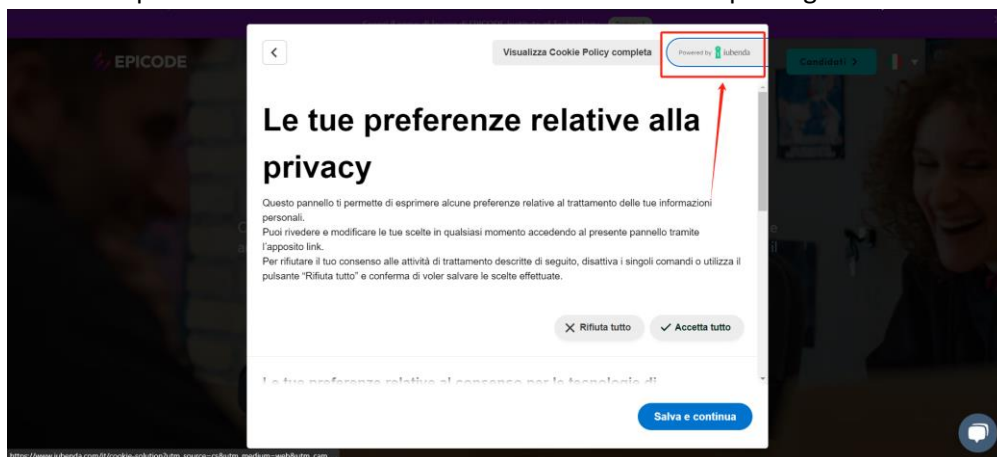
```
(kali@kali)~$ whois epicode.com
Domain Name: epicode.com
Registry Domain ID: 26708081.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-12-09T12:09:46Z
Creation Date: 2000-05-09T18:57:38Z
Registrar Registration Expiration Date: 2031-05-09T18:57:38Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1-480-624-2505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 100 S. Mill Ave, Suite 1600
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85281
Registrant Country: US
Registrant Phone: +1-4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=epicode.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 100 S. Mill Ave, Suite 1600
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85281
Admin Country: US
Admin Phone: +1-4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=epicode.com
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 100 S. Mill Ave, Suite 1600
```

Dall'ultima ricerca si scopre che il dominio **epicode.com** è registrato tramite il servizio godaddy nel 9 maggio 2000 in Arizona USA.

Tuttavia dal sito in chiaro bisogna tenere conto che il sito è in lingua italiana e per legge deve contenere elementi per l'individuazione amministrativa, pertanto si può continuare la ricerca tramite la parte burocratica.

Ricerca sulla società epicode tramite il sito

1. Aprendo il sito di epicode.com si nota che usano il servizio di lubeda per la gestione dei cookies.



2. Infondo al sito si trovano i riferimenti relativi alla società con tanto di partita IVA.

© 2024 EPICODE | Roma - Milano - Berlino | Codice Fiscale: 15878411006 | All rights reserved – [Privacy Policy](#) | [Cookie Policy](#)

3. Effettuando una ricerca tramite il sito dell'Agenzia delle Entrate, si scopre la denominazione sociale, <https://telematici.agenziaentrate.gov.it/VerificaPIVA/Scegli.do?parameter=verificaPiva>

La verifica per la partita Iva **15878411006** ha prodotto il seguente risultato:

PARTITA IVA ATTIVA

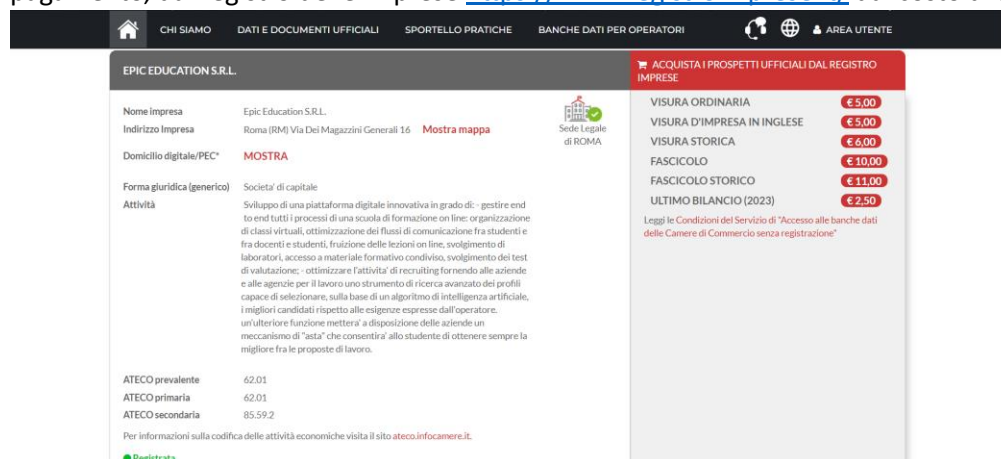
Denominazione/Cognome e nome: **EPIC EDUCATION S.R.L.**

Data inizio attività: **13/10/2020**

ATTENZIONE - Per verificare se la partita Iva è di un soggetto autorizzato ad effettuare operazioni intracomunitarie deve essere utilizzato il servizio [Controllo partite Iva comunitarie \(Vies\)](#).

Si evidenzia che la società ha aperto la partita Iva nel 13/10/2020, quindi è una start-up, che ha avuto un grande successo, dato le recensioni sui vari siti come trustpilot.

4. Per trovare le informazioni sui soci della società si potrebbe richiedere una visura camerale, a pagamento, dal registro delle imprese <https://www.registroimprese.it/> dal costo di 5 euro.



Anche solo dalla parte gratuita del sito si può già ottenere quali sono le informazioni relative alle sue attività.

5. Con l'analisi della visura camerale si scoprono tantissime informazioni utili per un possibile attacco tramite social engineering:

- a. Sede della società, si potrebbe recarsi personalmente per un sopralluogo fingendosi un potenziale studente;

Indirizzo Sede legale	ROMA (RM) VIA DEI MAGAZZINI GENERALI 16 CAP 00154
Domicilio digitale/PEC	epiceducation@legalmail.it
Partita IVA	15878411006
Numero repertorio economico amministrativo (REA)	RM - 1620997

- b. I soci, persone fisiche e giuridiche, soprattutto sono importanti le personalità fisiche, dato che ci sono anche gli indirizzi di residenza e codici fiscali: Pisa Diego, Ranza Ivan, Rosci Marco, Febbraio Andrea, Rota Andrea, De Angelis Tobia, Banovaz Diego, Trusiani Camelo Alessandro ecc... tutti i soci sono possibili exploit per un attacco tramite social engineering;
- c. Si potrebbe fare una valutazione grezza della società, in quanto dalla visura, l'anno precedente aveva 14 dipendenti, quindi sempre possibili vittime di attacchi di social engineering.
6. Il prossimo step, che ai fini didattici, non si prosegue, è quello di cercare ogni socio tramite i social e catturare qualsiasi informazione utile.
7. Si conclude che dal punto di vista tecnico epicode.com non ha exploit sfruttabili, l'unica strada possibile è il social engineering.

Maltego

Cos'è ed a cosa serve

Maltego è uno strumento di intelligence e analisi progettato per la raccolta e la visualizzazione di informazioni. È particolarmente utile nella fase di **ricognizione** e per l'analisi di dati complessi, risultando uno strumento prezioso per professionisti della sicurezza informatica, analisti di intelligence e ricercatori.

Caratteristiche Principali di Maltego

1. **Raccolta di Dati:** Maltego permette di raccogliere informazioni da una varietà di fonti pubbliche e private, come motori di ricerca, social media, database Whois e altre risorse di dati.
2. **Visualizzazione delle Relazioni:** Maltego offre la capacità di visualizzare le relazioni tra i dati in un formato grafico. Consente di creare grafici di rete che mostrano come elementi come domini, indirizzi IP, email e persone sono connessi tra loro.
3. **Trasformazioni:** Utilizza trasformazioni per convertire i dati da una forma a un'altra. Ad esempio, un dominio può essere trasformato in una lista di indirizzi IP associati o di sottodomini.
4. **Investigazione di Rete:** Le funzionalità di Maltego facilitano l'investigazione e l'analisi delle reti di contatti, delle strutture aziendali e delle relazioni complesse, fornendo una panoramica dettagliata e utile per la sicurezza e l'intelligence.

Usi Comuni di Maltego

1. **Ricerca di Intelligence:** È impiegato per raccogliere e analizzare informazioni su individui, organizzazioni e infrastrutture, scoprendo connessioni tra diverse entità.
2. **Penetration Testing:** Durante la fase di ricognizione di un test di penetrazione, Maltego può essere utilizzato per mappare le risorse di un'organizzazione, identificare punti di contatto e raccogliere dati utili per scoprire vulnerabilità.
3. **Investigazioni di Sicurezza:** È utilizzato per analizzare incidenti di sicurezza, come violazioni dei dati, e per identificare come e dove tali eventi sono avvenuti.
4. **OSINT (Open Source Intelligence):** Raccoglie informazioni pubblicamente disponibili e le organizza in modo significativo, facilitando l'analisi di dati utili per la sicurezza o la ricerca.

Esempio di Utilizzo di Maltego

Per investigare su un dominio web specifico, come **example.com**, il processo con Maltego include:

1. **Avviare Maltego** e creare un nuovo grafico.
2. **Aggiungere un'entità** per il dominio **example.com** al grafico.
3. **Eseguire trasformazioni** sul dominio per raccogliere dati relativi, come indirizzi IP associati, sottodomini, e contatti Whois.
4. **Visualizzare i risultati** come una rete di relazioni, mostrando come **example.com** è collegato a indirizzi IP, email e altre entità.

Maltego rappresenta uno strumento potente per analizzare informazioni dettagliate e interconnesse, offrendo un vantaggio significativo nelle investigazioni e nella sicurezza informatica.

Ricerca su Xi Jinping

The screenshot shows the Maltego Desktop 4.8.0 interface. The main workspace displays a graph with two entities: a person icon labeled '习近平' (Xi Jinping) and an email address icon labeled 'XUJinPing@gov.cn', connected by a directed link. The left sidebar contains an 'Entity Palette' with categories like 'Person', 'Bitcoin Cash Address', and 'Cryptocurrency'. The top toolbar includes various actions like 'Select All', 'Add Parents', 'Add Neighbors', etc. The bottom panel shows an 'Output - Transform Output' window with logs from the 'Unified Credits' and 'Transform To Datetime' transforms.

Output - Transform Output

```
[9/16/24, 4:13 PM] INFO ---[ Unified Credits ]--- : 191 of 200 credits remaining. Current quota period ends at October 1, 2024 at 12:00:00 AM Z (fr
[9/16/24, 4:13 PM] INFO Transform To Datetime (within Properties) completed in 1 s 57 ms (from entity "习近平")
[9/16/24, 4:14 PM] INFO Running transform To Datetime (within Properties) on 1 entities (from entity "习近平")
[9/16/24, 4:14 PM] INFO ---[ Unified Credits ]--- : 191 of 200 credits remaining. Current quota period ends at October 1, 2024 at 12:00:00 AM Z (fr
[9/16/24, 4:14 PM] INFO Transform To Datetime (within Properties) completed in 3 s 497 ms (from entity "习近平")
```