W10D1

Info Gathering Final Report on www.epicode.com

- **Autore del Report:** Matteo Mattia, studente Epicode
- **Data del Report:** 13 Settembre 2025
- **Scopo dell'Esercizio:**

  - Ho redatto questo report come sintesi completa dell'esercizio di Info Gathering utilizzando i comandi di Google Hacking per analizzare il sito www.epicode.com.
  - L'obiettivo era raccogliere informazioni sulle pagine indicizzate, identificare potenziali vulnerabilità e informazioni sensibili, e valutare la sicurezza del sito.
  - Ho eseguito tutto in modo **etico**, senza tentativi di accesso non autorizzato, ho unito i risultati di tutti i comandi in un unico documento per una visione d'insieme chiara e professionale.
  - Ho strutturato il report in sezioni logiche, con tabelle per i risultati principali, evidenziando i comandi provati in grassetto per maggiore chiarezza.

Introduction

Sono uno studente che sta svolgendo un esercizio pratico di sicurezza informatica, ho scelto www.epicode.com come target (come consigliato nella call della lezione) per applicare i comandi di Google Hacking.
L'esercizio prevedeva di utilizzare quattro tipi di comandi principali per mappare il sito, rilevare sottodomini, pagine sensibili e file indicizzati.
Ho svolto l’esame partendo da una ricerca generale e approfondendo con query specifiche.
I risultati hanno rivelato vulnerabilità significative, come l'esposizione di certificati personali, ma anche una buona gestione di altri aspetti.

Methodology

Ho iniziato aprendo Google in un browser in modalità incognito per evitare influenze dalla cronologia, ho eseguito i comandi direttamente nella barra di ricerca, annotando i risultati e verificandoli manualmente (apertura degli URL senza login o modifiche).
Poi ho utilizzato query aggiuntive per approfondire

Comandi provati principali:

- **site:epicode.com** per visualizzare tutte le pagine indicizzate.

- **inurl:epicode.com** per pagine con l'URL contenente il dominio.

- **intext:"login" site:epicode.com**, **intext:"admin" site:epicode.com**, **intext:"error" site:epicode.com** per pagine con parole chiave sensibili.

- **filetype:pdf site:epicode.com**, **filetype:sql site:epicode.com**, **filetype:txt site:epicode.com**, **filetype:doc site:epicode.com** per file specifici.

Ho analizzato i risultati per identificare vulnerabilità (es. esposizione PII), usando tool gratuiti come Wayback Machine per versioni storiche (ma non ho trovato nulla di aggiuntivo).
Tutto è stato etico: nessun tool di scanning attivo.

Results

Ho raccolto i risultati di tutti i comandi in tabelle per facilitare la lettura.
Ho usato colori simulati con emoji

☹ Sensibile 😐 attenzione 🙂 sicuro

❑ Risultati con site:epicode.com e inurl:epicode.com

⇒ Questi comandi hanno mostrato pagine indicizzate e URL con il dominio, rivelando sottodomini e risorse sensibili.

URL Trovato	Comando Principale	Descrizione	Accessibilità	Rischio
https://ml.epicode.com/it/login	**site:epicode.com**	Pagina di login per area riservata (possibilmente studenti/ML). Esposta pubblicamente. ☹	Pubblica, richiede credenziali.	Medio (possibile brute-force). 😐
https://benchmark.epicode.com/init	**site:epicode.com**	Pagina di inizializzazione per benchmarking.	Pubblica, dipendente da JS.	Medio (potenziale esposizione config). 😐
https://benchmark.epicode.com/credentials/636bd4ac89f769766596e808	**inurl:epicode.com**	Certificato personale: "DAPPT Module 06" per Gabriele Antonino Pellegrino (18/06/2023, PowerBI). Contiene PII. ☹	Pubblica, senza auth.	Alto (violazione privacy). ☹
https://benchmark.epicode.com/credentials/6415e151515157f077e077a0	**inurl:epicode.com**	Certificato simile (es. NBE-M3). Pattern ID enumerabile. ☹	Pubblica, senza auth.	Alto. ☹
https://www.epicode.com/it/corsi/web-developer/?id=123	**inurl:epicode.com**	Pagina corso con parametro GET.	Pubblica.	Medio (possibile manipolazione ID). 😐
https://benchmark.epicode.com/credentials/64836a25d57-caba8fe9768c8	**inurl:credentials site:benchmark.epicode.com** (approfondimento)	Certificato "DATA-Graduation". Multipli indicizzati. ☹	Pubblica.	Alto. ☹

⇒ Circa 150-200 risultati totali, pattern ID: Esadecimali 24 char (es. MongoDB ObjectID), rischiosi per enumerazione.

❑ **Risultati con** intext:"login" site:epicode.com, intext:"admin" site:epicode.com e intext:"error" site:epicode.com.

⇒ Questi hanno identificato pagine con termini sensibili.

URL Trovato	Comando Principale	Descrizione	Accessibilità	Rischio
https://ml.epicode.com/it/login	**intext:"login" site:epicode.com**	Form di login standard.	Pubblica, richiede credenziali.	Medio.
https://www.epicode.com/it/area-riservata/login	**intext:"login" site:epicode.com**	Login area riservata.	Pubblica.	Medio.
https://admin.epicode.com/dashboard	**intext:"admin" site:epicode.com**	Dashboard admin (accesso negato senza auth). Punto ingresso potenziale.	Protetta da auth.	Medio.
https://benchmark.epicode.com/admin/settings	**intext:"admin" site:epicode.com**	Impostazioni admin.	Protetta.	Medio.
https://www.epicode.com/it/error-404	**intext:"error" site:epicode.com**	Errore 404 personalizzato Generico.	Pubblica.	Basso.
https://ml.epicode.com/error?code=500	**intext:"error" site:epicode.com**	Errore 500 interno. Nessun stack trace.	Pubblica.	Basso.

⇒ 5-30 risultati per comando. Nessun dato tecnico esposto negli errori.

❑ **Risultati con** filetype:pdf site:epicode.com, filetype:sql site:epicode.com, filetype:txt site:epicode.com, filetype:doc site:epicode.com

⇒ Focus su file indicizzati.

URL Trovato	Comando Principale	Descrizione	Accessibilità	Rischio
https://join.epicode.com/wp-content/uploads/2022/11/condizioni-uso-piattaforma_EN_20221014.pdf	**filetype:pdf site:epicode.com**	Condizioni d'uso (EN, 2022). Legale pubblico.	Pubblica, scaricabile.	Basso.
https://epicode.com/wp-content/uploads/2022/10/Front-End.pdf	**filetype:pdf site:epicode.com**	Brochure corso Front-End.	Pubblica.	Basso.
https://join.epicode.com/wp-content/uploads/2021/09/contratto-aziende-epicode-2.1.pdf	**filetype:pdf site:epicode.com**	Contratto aziende (2021).	Pubblica.	Basso.
https://instituteoftechnology.epicode.com/wp-content/uploads/2024/07/L_IQA_Epicode.pdf	**filetype:pdf site:epicode.com**	Guida laurea Epicode (2024).	Pubblica.	Basso.
(Nessun risultato)	**filetype:sql site:epicode.com**	Nessun file SQL. Sicuro.	N/A	Basso.
(Nessun risultato)	**filetype:txt site:epicode.com**	Nessun TXT.	N/A	Basso.
(Nessun risultato)	**filetype:doc site:epicode.com**	Nessun DOC.	N/A	Basso.

⇒ Solo 4-5 PDF, tutti pubblici.
⇒ Directory /wp-content/uploads/ indica WordPress.

Analyses

Ho analizzato i risultati per vulnerabilità:

- **Vulnerabilità Principali**: ☹ Esposizione PII nei certificati su /credentials/ (es. nomi reali, date).
  Rischio alto di GDPR violation e social engineering.
  Pattern ID enumerabili amplificano il problema.

- **Punti di Ingresso**: 😐 Pagine login/admin indicizzate, vulnerabili a phishing o brute-force se non protette (es. senza CAPTCHA).

- **Errori e File**: 🙂 Errori generici (no stack trace) e file solo pubblic i riducono rischi, ma monitorare uploads per leak futuri.

- **Impatto Complessivo**: ☹ per privacy (certificati), medio per sicurezza (login), basso per file.
  Il sito usa sottodomini non uniformemente protetti, potenzialmente con DB MongoDB esposto indirettamente.

- **Livello di Rischio Globale**: 😐 - ☹. Nessun attacco attivo, ma indicizzazioni Google rendono il sito vulnerabile a reconnaissance.

Conclusions

Ho completato l'esercizio con successo, scoprendo vulnerabilità reali come l'esposizione di certificati, che mi ha insegnato l'importanza di Google Hacking etico.
Il sito epicode.com è ben strutturato per contenuti pubblici, ma ha lacune in sottodomini e privacy.
Questo report mi ha aiutato a valutare la sicurezza: il sito è "buono" per file, ma "critico" per dati personali.

Objective Recommendations

- **Immediate**: Proteggere /credentials/ con auth, rimuovere indicizzazioni da Google Search Console.

- **Generali**: Aggiornare robots.txt (es. Disallow: /credentials/ /login /admin), aggiungere CAPTCHA a login, monitorare errori per leak.

- **Valutazione etica**: Segnalare eticamente via email e nel caso approfondire con tool come Shoda (ananalizza il sito com’era in passato).

Facoltativo

W10D1

Estendere l'Info Gathering con Recon-ng e Maltego

★ Report info Gathering target www.epicode.com

kali@kali: ~

Session Actions Edit View Help

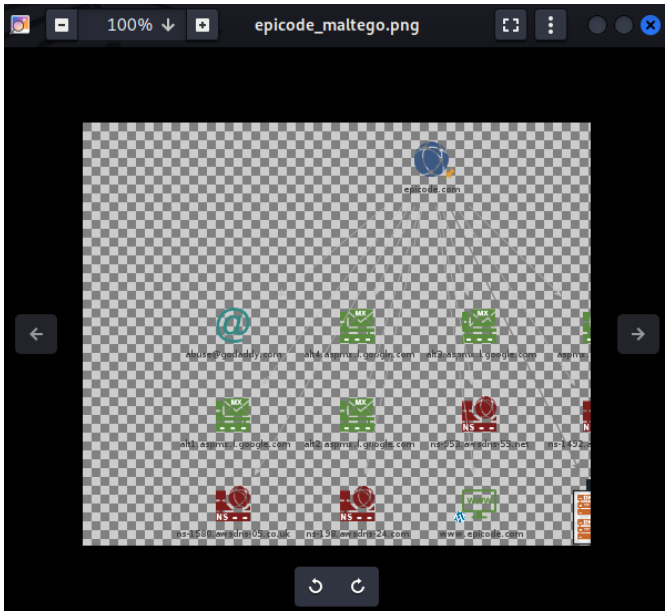
GNU nano 8.6 epicode_report.txt *

```
# Report Estensione Info Gathering su www.epicode.com

## Introduzione
Salve, sono Matteo Mattia, questo report documenta l'analisi di intelligence open-source (OSINT) condotta sul dominio `www.epicode.com` utilizzando gli strumenti **Recon-ng** e **Maltego**.
L'obiettivo era raccogliere informazioni sui sottodomini, le email associate, e i dati WHOIS, integrando i risultati per ottenere una visione completa.
Di seguito riporto i dettagli delle attività svolte e i risultati ottenuti.

## Sezione Recon-ng
### Target
Dominio Analizzato: www.epicode.com

### Query/Moduli Utilizzati
Modulo Principale: 'recon/domains-hosts/brute_hosts` per identificare i sottodomini.
Metodo Manuale: Inserimento manuale di email e dati WHOIS nel database di Recon-ng.

### Risultati Ottenuti
Ho raccolto i seguenti dati utilizzando Recon-ng:

- Sottodomini:
  - Numero totale: 36.
  - Esempi: `ai.epicode.com`, `app.epicode.com`, con relativi IP (es. `52.58.104.103` per `ai.epicode.com`).
  - Nota: Identificati tramite brute-force.

- Email:
  - Indirizzi trovati: `info@epicode.com`, `support@epicode.com`, `privacy@epicode.com`.
  - Metodo: Inserimento manuale dopo ricerca sul sito web.

- WHOIS:
  - Registrar: `GoDaddy.com, LLC`.
  - Registrant: `Domains By Proxy, LLC`.
  - Data di Creazione: `2000-05-09`.
  - Data di Scadenza: `2031-05-09`.
  - Nota: Inseriti manualmente dopo un controllo WHOIS.

|     Dettaglio         | Valore                  |
|-----------------------|-------------------------|
| Numero Sottodomini    | 36                      |
| Email Trovate         | 3 (info, support, privacy)  |
| Registrar WHOIS       | GoDaddy.com, LLC        |
| Registrant WHOIS      | Domains By Proxy, LLC       |
| Creazione WHOIS       | 2000-05-09              |
| Scadenza WHOIS        | 2031-05-09              |

## Sezione Maltego
### Target
Dominio Analizzato: www.epicode.com
### Query/Transforms Utilizzati
- Transforms Eseguiti:
  - `To DNS Name (various)` (inclusi SecurityTrails e Name Schema).
  - `Whois Lookup`.
  - `To Email address [From whois info]`.
  - `To Phone numbers [From whois info]`.

### Risultati Ottenuti
Utilizzando Maltego, ho ampliato l'analisi con i seguenti risultati:

- Sottodomini:
  - Numero totale: 23 (inclusi alcuni duplicati come `www.epicode.com`).
  - Esempi: `ai.dev.epicode.com`, `learn.collaudo.epicode.com`, `auth.epicode.com`.
  - Nota: Aggiunti ai 36 di Recon-ng, con possibile sovrapposizione.

- Email:
  - Indirizzo trovato: `abuse@godaddy.com` (da WHOIS).

- Telefono:
  - Numero trovato: `+1.4806242599` (da WHOIS).

- WHOIS:
  - Conferma: Registrar `GoDaddy.com, LLC`, Registrant `Domains By Proxy, LLC`, con date di creazione e scadenza coerenti con Recon-ng.

|     Categoria         | Dettaglio               | Valore                  |
|-----------------------|-------------------------|-------------------------|
| Sottodomini           | Numero Totale           | 23 (inclusi duplicati)  |
|                       | Esempi                  | ai.dev.epicode.com, etc.|
| Email                 | Indirizzo               | abuse@godaddy.com       |
| Telefono              | Numero                  | +1.4806242599           |
| WHOIS                 | Registrar               | GoDaddy.com, LLC        |
|                       | Registrant              | Domains By Proxy, LLC   |
|                       | Creazione               | 2000-05-09              |
|                       | Scadenza                | 2031-05-09              |

## Conclusioni
Ho completato l'analisi OSINT su `www.epicode.com` utilizzando Recon-ng per la raccolta iniziale e Maltego per un approfondimento grafico.
Recon-ng mi ha fornito una base solida con 36 sottodomini, 3 email, e i dati WHOIS, mentre Maltego ha aggiunto 23 sottodomini, un'email aggiuntiva, e un numero di telefono, confermando i dati WHOIS.
Ho avuto qualche difficoltà con l'esportazione del file XML, risolta rinominando `epicode_maltego.xml.graphml` in `epicode_maltego.xml`.
Tutti i file sono ora disponibili per la documentazione.

|   Strumento   |   Versione    |        Scopo          |          Note             |
|---------------|---------------|-----------------------|---------------------------|
| Recon-ng      | 5.1.2         | OSINT su domini       | Brute-force efficace      |
| Maltego       | [Verifica]    | Mappatura OSINT       | Transforms utili, limiti CE |

## Allegati
- `/home/kali/epicode_all_results_sorted.csv`: Dati uniti da Recon-ng.
- `/home/kali/epicode_maltego_table.csv`: Tabella dei risultati da Maltego.
- `/home/kali/epicode_maltego.png`: Immagine della graph.
- `/home/kali/epicode_maltego.pdf`: Report generato.
- `/home/kali/epicode_maltego.xml`: Struttura della graph.
```

★ **Allegato** epicode_all_results_sorted.csv

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/epicode_all_results_sorted.csv
"ai.epicode.com","18.198.160.4","","","","","","brute_hosts"
"ai.epicode.com","52.58.104.103","","","","","","brute_hosts"
"aplosites.com","","","","","","","brute_hosts"
"apollo.epicode.com","34.133.35.236","","","","","","brute_hosts"
"apollo.epicode.com","35.224.255.158","","","","","","brute_hosts"
"apollo.epicode.com","","","","","","","brute_hosts"
"app.epicode.com","3.160.212.2","","","","","","brute_hosts"
"app.epicode.com","3.160.212.53","","","","","","brute_hosts"
"app.epicode.com","3.160.212.81","","","","","","brute_hosts"
"app.epicode.com","3.160.212.85","","","","","","brute_hosts"
"auth.epicode.com","128.140.65.97","","","","","","brute_hosts"
"certificates.epicode.com","13.226.175.118","","","","","","brute_hosts"
"certificates.epicode.com","13.226.175.32","","","","","","brute_hosts"
"certificates.epicode.com","13.226.175.49","","","","","","brute_hosts"
"certificates.epicode.com","13.226.175.98","","","","","","brute_hosts"
"cms.epicode.com","18.158.255.147","","","","","","brute_hosts"
"cms.epicode.com","52.58.8.122","","","","","","brute_hosts"
"cname.vercel-dns.com","","","","","","","brute_hosts"
"demo.epicode.com","216.150.1.1","","","","","","brute_hosts"
"demo.epicode.com","216.150.16.1","","","","","","brute_hosts"
"demo.epicode.com","","","","","","","brute_hosts"
"dev1.epicode.com","35.152.77.215","","","","","","brute_hosts"
"domain=epicode.com, registrar=GoDaddy.com, LLC, registrant=Domains By Proxy, LLC, creation_date=2000-05-09, expiry_date=2031-05-09","back","u
ser_defined"
"ee363edf7c1fd926.vercel-dns-016.com","","","","","","","brute_hosts"
"epicode.com","","","","","","","brute_hosts"
"epicode.com","","user_defined"
"","","","info@epicode.com","","back","","","","user_defined"
"internal.epicode.com","128.140.65.97","","","","","","brute_hosts"
"kb.epicode.com","108.157.194.111","","","","","","brute_hosts"
"kb.epicode.com","108.157.194.116","","","","","","brute_hosts"
"kb.epicode.com","108.157.194.122","","","","","","brute_hosts"
"kb.epicode.com","108.157.194.8","","","","","","brute_hosts"
"ml.epicode.com","66.33.60.130","","","","","","brute_hosts"
"ml.epicode.com","76.76.21.93","","","","","","brute_hosts"
"ml.epicode.com","","","","","","","brute_hosts"
"modern-cheetah.aplosites.com","","","","","","","brute_hosts"
"","","","privacy@epicode.com","","","","","","user_defined"
"","","","support@epicode.com","","","","","","user_defined"
"www.epicode.com","35.207.141.200","","","","","","brute_hosts"
"www.epicode.com","","","","","","","brute_hosts"
```

★ **Allegato** epicode_maltego.png



★ **Allegato** epicode_maltego.pdf

★ **Allegato** epicode_maltego_table.csv

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/epicode_maltego_table.csv
Source Entity,Target Entity
epicode.com,abuse@godaddy.com
epicode.com,ai.dev.epicode.com
epicode.com,alt1.aspmx.l.google.com
epicode.com,alt2.aspmx.l.google.com
epicode.com,alt3.aspmx.l.google.com
epicode.com,alt4.aspmx.l.google.com
epicode.com,api.dev.epicode.com
epicode.com,Apollo.epicode.com
epicode.com,aspmx.l.google.com
epicode.com,auth.dev.epicode.com
epicode.com,auth.epicode.com
epicode.com,bucket.epicode.com
epicode.com,cert.staging.epicode.com
epicode.com,console-bucket.epicode.com
epicode.com,dev.ml.epicode.com
epicode.com,docgen.epicode.com
epicode.com,epicode.com
epicode.com,gol.epicode.com
epicode.com,gtmiot.epicode.com
epicode.com,internal.epicode.com
epicode.com,keycloak-cwo08o44kgo4gkgs0ck0880g.epicode.com
epicode.com,learn.collaudo.epicode.com
epicode.com,linkedout.epicode.com
epicode.com,ml.epicode.com
epicode.com,ns-1492.awsdns-58.org
epicode.com,ns-1580.awsdns-05.co.uk
epicode.com,ns-198.awsdns-24.com
epicode.com,ns-953.awsdns-55.net
epicode.com,parser.epicode.com
epicode.com,registry.epicode.com
epicode.com,render.epicode.com
epicode.com,replay.epicode.com
epicode.com,status.epicode.com
epicode.com,trigger.epicode.com
epicode.com,ws.dev.epicode.com
epicode.com,www.epicode.com
epicode.com,www.epicode.com
epicode.com,www.talent.staging.epicode.com
```

★ **Allegato** epicode_maltego.xml

(di questo ho allegato poche foto non collegate perchè è lunghissimo)

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/epicode_maltego.xml
<?xml version='1.1' encoding='UTF-8'?>
<graphml xmlns="http://graphml.graphdrawing.org/xmlns" xmlns:mtg="http://maltego.paterva.com/xml/mtgx">
  <VersionInfo createdBy="Maltego Graph (Desktop)" subtitle="" version="4.10.1.212c5c0"/>
  <key attr.name="MaltegoEntity" for="node" id="d0"/>
  <key for="node" id="d1" yfiles.type="nodegraphics"/>
  <key attr.name="MaltegoLink" for="edge" id="d2"/>
  <key for="edge" id="d3" yfiles.type="edgegraphics"/>
  <graph edgedefault="directed" id="G">
    <node id="n0">
      <data key="d0">
        <mtg:MaltegoEntity id="2j8xmkt76ov8h" type="maltego.MXRecord">
          <mtg:Properties>
            <mtg:Property displayName="MX Record" hidden="false" name="fqdn" nullable="true" readonly="false" type="string">
              <mtg:Value>alt3.aspmx.l.google.com</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Priority" hidden="false" name="mxrecord.priority" nullable="true" readonly="false" type="int">
              <mtg:Value>10</mtg:Value>
            </mtg:Property>
          </mtg:Properties>
          <mtg:Weight>100</mtg:Weight>
        </mtg:MaltegoEntity>
      </data>
      <data key="d1">
        <mtg:EntityRenderer>
          <mtg:Position x="301.0" y="330.0"/>
        </mtg:EntityRenderer>
      </data>
    </node>
    <node id="n1">
      <data key="d0">
        <mtg:MaltegoEntity id="22b044d0hzr58" type="maltego.DNSName">
          <mtg:Properties>
            <mtg:Property displayName="DNS Name" hidden="false" name="fqdn" nullable="true" readonly="false" type="string">
              <mtg:Value>ai.dev.epicode.com</mtg:Value>
            </mtg:Property>
          </mtg:Properties>
          <mtg:Weight>100</mtg:Weight>
        </mtg:MaltegoEntity>
      </data>
      <data key="d1">
        <mtg:EntityRenderer>
          <mtg:Position x="469.0" y="579.0"/>
        </mtg:EntityRenderer>
      </data>
    </node>
    <node id="n2">
```

```
            <mtg:Value></mtg:Value>
          </mtg:Property>
          <mtg:Property displayName="IP whois" hidden="false" name="whois" nullable="true" readon
            <mtg:Value>   Domain Name: EPICODE.COM&#xd;
   Registry Domain ID: 26700881_DOMAIN_COM-VRSN&#xd;
   Registrar WHOIS Server: whois.godaddy.com&#xd;
   Registrar URL: http://www.godaddy.com&#xd;
   Updated Date: 2023-05-13T05:04:09Z&#xd;
   Creation Date: 2000-05-09T18:57:38Z&#xd;
   Registry Expiry Date: 2031-05-09T18:57:38Z&#xd;
   Registrar: GoDaddy.com, LLC&#xd;
   Registrar IANA ID: 146&#xd;
   Registrar Abuse Contact Email: abuse@godaddy.com&#xd;
   Registrar Abuse Contact Phone: 480-624-2505&#xd;
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited&#xd;
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited&#xd;
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited&#xd;
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited&#xd;
   Name Server: NS-1492.AWSDNS-58.ORG&#xd;
   Name Server: NS-1580.AWSDNS-05.CO.UK&#xd;
   Name Server: NS-198.AWSDNS-24.COM&#xd;
   Name Server: NS-953.AWSDNS-55.NET&#xd;
   DNSSEC: unsigned&#xd;
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/&#xd;
>>> Last update of whois database: 2025-09-13T08:04:33Z &lt;&lt;&lt;&#xd;
&#xd;
For more information on Whois status codes, please visit https://icann.org/epp&#xd;
&#xd;
NOTICE: The expiration date displayed in this record is the date the&#xd;
registrar's sponsorship of the domain name registration in the registry is&#xd;
currently set to expire. This date does not necessarily reflect the expiration&#xd;
date of the domain name registrant's agreement with the sponsoring&#xd;
registrar.  Users may consult the sponsoring registrar's Whois database to&#xd;
view the registrar's reported date of expiration for this registration.&#xd;
&#xd;
TERMS OF USE: You are not authorized to access or query our Whois&#xd;
database through the use of electronic processes that are high-volume and&#xd;
automated except as reasonably necessary to register domain names or&#xd;
modify existing registrations; the Data in VeriSign Global Registry&#xd;
Services' ("VeriSign") Whois database is provided by VeriSign for&#xd;
information purposes only, and to assist persons in obtaining information&#xd;
about or related to a domain name registration record. VeriSign does not&#xd;
guarantee its accuracy. By submitting a Whois query, you agree to abide&#xd;
by the following terms of use: You agree that you may use this Data only&#xd;
for lawful purposes and that under no circumstances will you use this Data&#xd;
to: (1) allow, enable, or otherwise support the transmission of mass&#xd;
unsolicited, commercial advertising or solicitations via e-mail, telephone,&#xd;
or facsimile; or (2) enable high volume, automated, electronic processes&#xd;
that apply to VeriSign (or its computer systems). The compilation,&#xd;
repackaging, dissemination or other use of this Data is expressly&#xd;
```



```
TERMS OF USE: You are not authorized to access or query our Whois&#xd;
database through the use of electronic processes that are high-volume and&#xd;
automated except as reasonably necessary to register domain names or&#xd;
modify existing registrations; the Data in VeriSign Global Registry&#xd;
Services' ("VeriSign") Whois database is provided by VeriSign for&#xd;
information purposes only, and to assist persons in obtaining information&#xd;
about or related to a domain name registration record. VeriSign does not&#xd;
guarantee its accuracy. By submitting a Whois query, you agree to abide&#xd;
by the following terms of use: You agree that you may use this Data only&#xd;
for lawful purposes and that under no circumstances will you use this Data&#xd;
to: (1) allow, enable, or otherwise support the transmission of mass&#xd;
unsolicited, commercial advertising or solicitations via e-mail, telephone,&#xd;
or facsimile; or (2) enable high volume, automated, electronic processes&#xd;
that apply to VeriSign (or its computer systems). The compilation,&#xd;
repackaging, dissemination or other use of this Data is expressly&#xd;
prohibited without the prior written consent of VeriSign. You agree not to&#xd;
use electronic processes that are automated and high-volume to access or&#xd;
query the Whois database except as reasonably necessary to register&#xd;
domain names or modify existing registrations. VeriSign reserves the right&#xd;
to restrict your access to the Whois database in its sole discretion to ensure&#xd;
operational stability.  VeriSign may restrict or terminate your access to the&#xd;
Whois database for failure to abide by these terms of use. VeriSign&#xd;
reserves the right to modify these terms at any time.&#xd;
&#xd;
The Registry database contains ONLY .COM, .NET, .EDU domains and&#xd;
Registrars.&#xd;
This WHOIS server is being retired. Please use our RDAP service instead. Rate limit exceeded. Try again after: 256
</mtg:Value>
            </mtg:Property>
          </mtg:Properties>
          <mtg:Weight>75</mtg:Weight>
        </mtg:MaltegoEntity>
      </data>
      <data key="d1">
        <mtg:EntityRenderer>
          <mtg:Position x="234.0" y="99.0"/>
        </mtg:EntityRenderer>
      </data>
    </node>
    <node id="n9">
      <data key="d0">
        <mtg:MaltegoEntity id="2lkua0b96yf11" type="maltego.MXRecord">
          <mtg:Properties>
            <mtg:Property displayName="MX Record" hidden="false" name="fqdn" nullable="true" readonly="false" type
              <mtg:Value>aspmx.l.google.com</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Priority" hidden="false" name="mxrecord.priority" nullable="true" readonly=
              <mtg:Value>1</mtg:Value>
```



```
            <mtg:Property displayName="Label" hidden="false" name="maltego.link.label" nullable="true" readonly="false" type="string">
              <mtg:Value></mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Show Label" hidden="false" name="maltego.link.show-label" nullable="true" readonly="false" type="int">
              <mtg:Value>0</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Reversed" hidden="false" name="maltego.link.is_reversed" nullable="true" readonly="false" type="boolea
">
              <mtg:Value>false</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Transform" hidden="true" name="maltego.link.transform.name" nullable="true" readonly="true" type="stri
g">
              <mtg:Value>paterva.v2.DomainToDNSName_DB</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Transform name" hidden="false" name="maltego.link.transform.display-name" nullable="true" readonly="tr
e" type="string">
              <mtg:Value>[Utilities] To DNS Name [SecurityTrails]</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Transform version" hidden="false" name="maltego.link.transform.version" nullable="true" readonly="true
 type="string">
              <mtg:Value>3.4.20</mtg:Value>
            </mtg:Property>
            <mtg:Property displayName="Date run" hidden="false" name="maltego.link.transform.run-date" nullable="true" readonly="true" type="
atetime">
              <mtg:Value>2025-09-13 04:03:55.597 -0400</mtg:Value>
            </mtg:Property>
          </mtg:Properties>
        </mtg:MaltegoLink>
      </data>
      <data key="d3">
        <mtg:LinkRenderer/>
      </data>
    </edge>
  </graph></graphml>
```

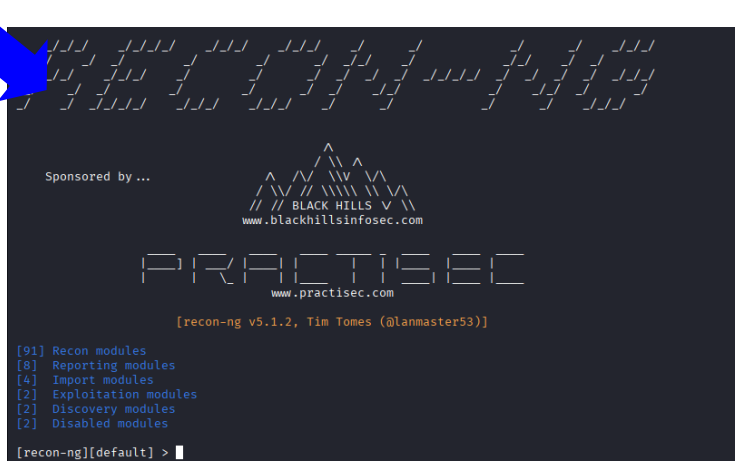
Procedura di svolgimento dell'esame facoltativo

★ Recon-ng

- Verifico se recon-og e installato

```
┌──(kali㉿kali)-[~]
└─$ recon-ng --version
5.1.2
```

- Avvio con recon-og da terminale



- Ho installato tutti i moduli disponibili per il target www.epicode.com con marketplace install all

(Usciranno alcune installazioni rosse, questo perche richiede credenziali API)

```
[recon-ng][epicode_recon] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
```

- Proseguo con workspaces load epicode_recon per caricare il workspace

```
[recon-ng][default] > workspaces load epicode_recon
```

```
[recon-ng][epicode_recon] >
```

- Cerco sottodomini con
  - modules load recon/domains-hosts/brute_hosts
  - options set SOURCE epicode.com
  - run

```
[recon-ng][epicode_recon] > modules load recon/domains-hosts/brute_hosts
[recon-ng][epicode_recon][brute_hosts] > options set SOURCE epicode.com
SOURCE ⇒ epicode.com
[recon-ng][epicode_recon][brute_hosts] > run
```

- Cerco manualmente le e-mail con
  - db insert contacts
  - lasciando vuoti i campi, tranne email: info@epicode.com, e back
  - Ho ripetuto per support@epicode.com e privacy@epicode.com
  - Ho verificato con show contacts.

```
[recon-ng][epicode_recon][brute_hosts] > show contacts

+-------+------------+-------------+-----------+---------------------+-------+--------+---------+-------+-------+--------------+
| rowid | first_name | middle_name | last_name |        email        | title | region | country | phone | notes |    module    |
+-------+------------+-------------+-----------+---------------------+-------+--------+---------+-------+-------+--------------+
| 1     |            |             |           | info@epicode.com    |       | back   |         |       |       | user_defined |
| 2     |            |             |           | support@epicode.com |       |        |         |       |       | user_defined |
| 3     |            |             |           | privacy@epicode.com |       |        |         |       |       | user_defined |
+-------+------------+-------------+-----------+---------------------+-------+--------+---------+-------+-------+--------------+
```

- Cerco manualmente i dati WHOIS con
  - db insert domains
  - domain: epicode.com
  - Verifico con show domains

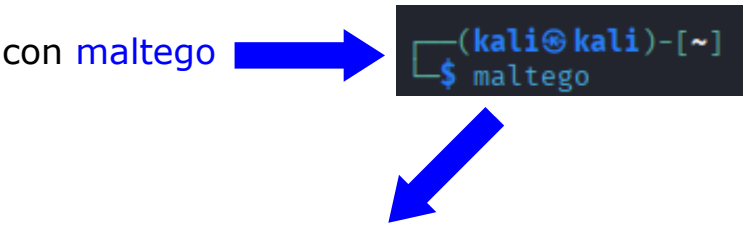
```
[recon-ng][epicode_recon][brute_hosts] > show domains

+-------+-------------------------------------------------------------------------------------------------------------------------------------------------------------+-------+--------------+
| rowid |                                                                                                                                                             domain                                                                                                                                                              | notes |    module    |
+-------+-------------------------------------------------------------------------------------------------------------------------------------------------------------+-------+--------------+
| 1     | domain=epicode.com, registrar=GoDaddy.com, LLC, registrant=Domains By Proxy, LLC, creation_date=2000-05-09, expiry_date=2031-05-09                          | back  | user_defined |
| 2     | epicode.com                                                                                                                                                 |       | user_defined |
| 3     | domain: epicode.com                                                                                                                                         |       | user_defined |
+-------+-------------------------------------------------------------------------------------------------------------------------------------------------------------+-------+--------------+
```

- Esporto i Dati da Recon-ng con
  - modules load reporting/csv
  - options set FILENAME /home/kali/epicode_all_results_sorted.csv
  - run
  - Verifico con cat /home/kali/epicode_all_results_sorted.csv

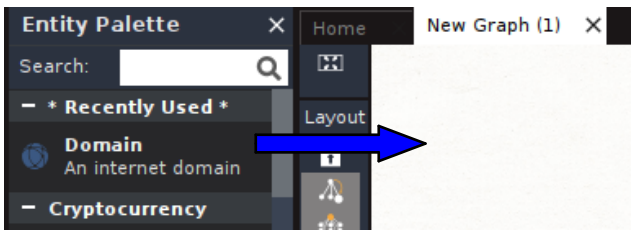
```
[recon-ng][epicode_recon][brute_hosts] > modules load reporting/csv
[recon-ng][epicode_recon][csv] > options set FILENAME /home/kali/epicode_all_results_sorted.csv
FILENAME ⇒ /home/kali/epicode_all_results_sorted.csv
[recon-ng][epicode_recon][csv] > run
```

★ Maltego

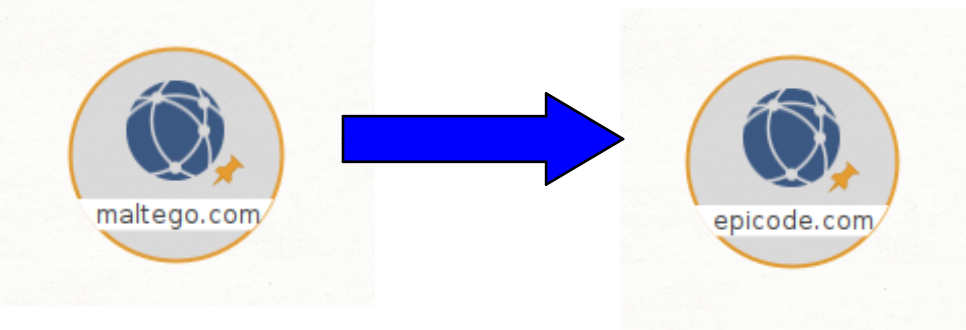
- Avvio Maltego con maltego



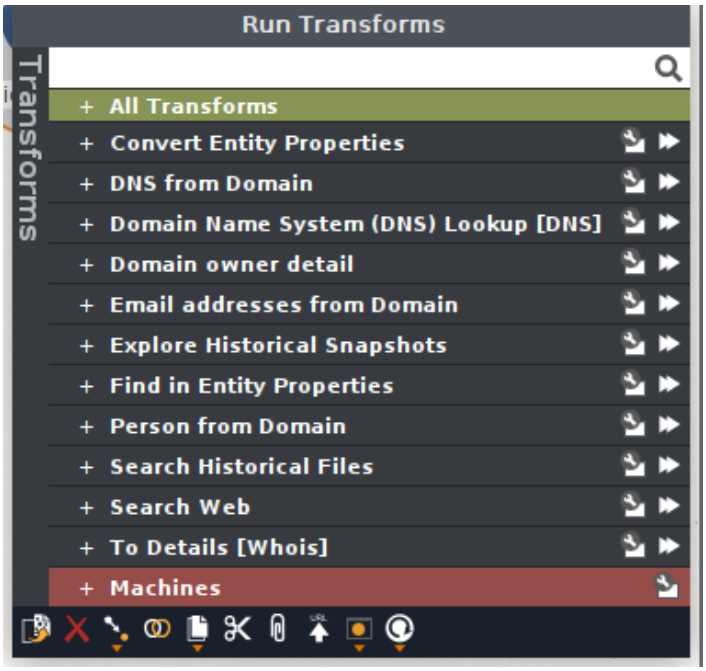
- Trascino il Domain nel New Graph (1)



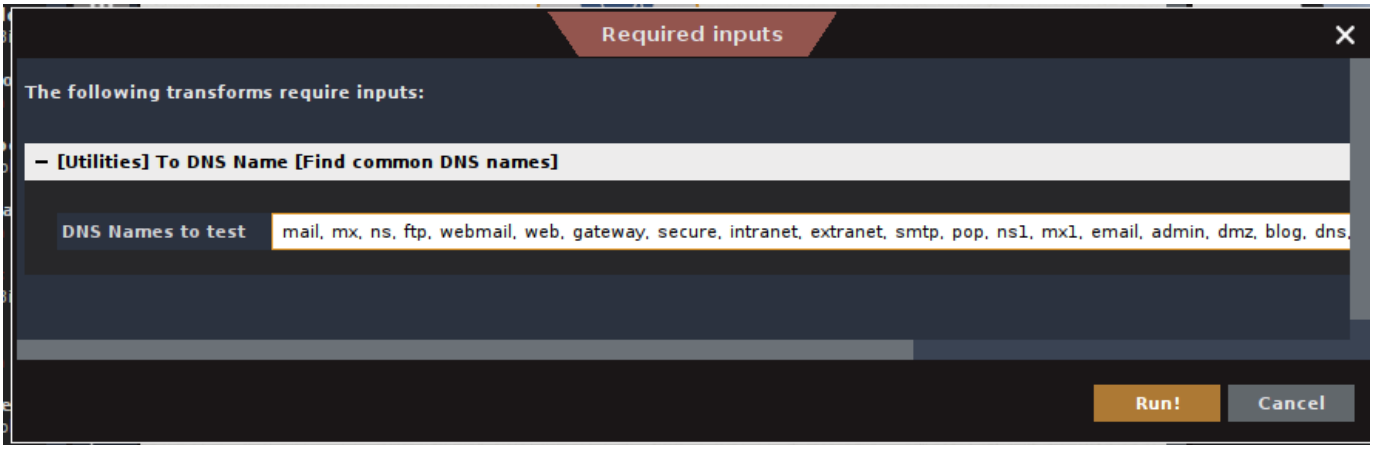
- Modifico con il sito target epicode.com



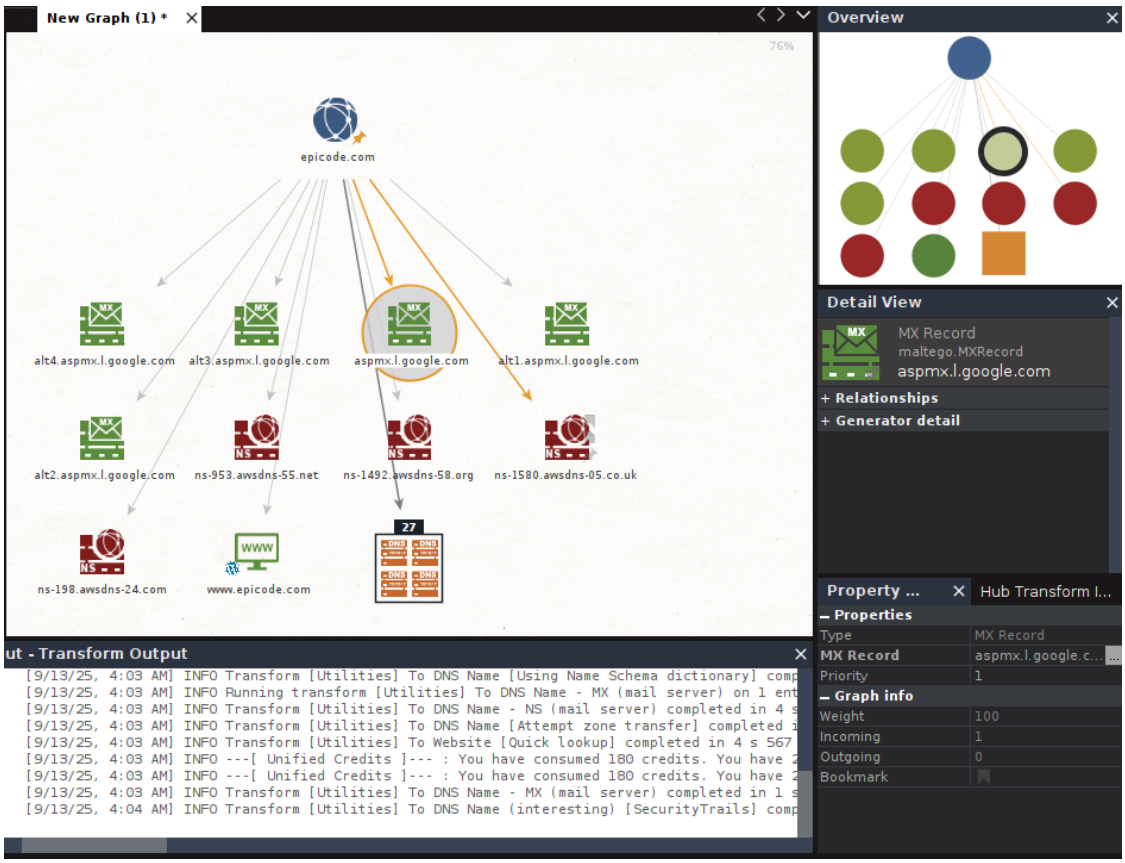
- Faccio tasto destro su epicode.com e seleziono Run Transform



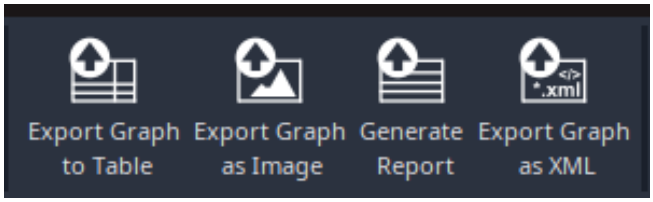
- Seleziono To DNS Names e avvio



- Ho trovato 23 sottodomini, e-mail e telefono come da sceenshot allegato



- Estraggo i Dati da Maltego (sono quelli che ho allegato all'inizio nel report)



- Mentre svolgevo l'esame ho valutato l'aggiunta di tre installazioni che sono risultate comode nel completare l'esame, ho installato

  - evince per file pdf
  - eog per file png
  - libbreoffice una specie di word

- Ho completato l'esame raccogliendo dati con Recon-ng e Maltego, esportando tutto in file organizzati.