# Relazione Tecnica – OSINT su Mediaset S.p.A.

## 1. Introduzione

In questo esercizio è stata simulata una fase di Information Gathering (ricognizione passiva) su un'organizzazione reale, utilizzando esclusivamente fonti aperte (OSINT) e strumenti gratuiti.
La raccolta di informazioni pubblicamente accessibili rappresenta il primo passo fondamentale in qualsiasi attività di ethical hacking, cyber intelligence o penetrazione controllata, poiché consente di identificare asset, contatti, tecnologie e potenziali punti deboli di un'infrastruttura senza interazione diretta con il target.

## 2. Target Analizzato

- **Nome:** Mediaset S.p.A.
- **Dominio principale:** mediaset.it
- **Settore:** Media, broadcasting, comunicazione
- **Tipo di organizzazione:** Azienda privata italiana
- **Motivazione della scelta:** Mediaset rappresenta un ottimo esempio di target reale con visibilità pubblica elevata, numerosi sottodomini e presenza diffusa online, ideale per un'esercitazione OSINT completa.

## 3. Raccolta Informazioni via Google: tecniche e strumenti utilizzati

Per la raccolta iniziale è stato utilizzato **Google** sfruttando tecniche di ricerca avanzata, note come **Google Dorks**, ovvero operatori booleani e parametri specifici per filtrare risultati mirati.

### Obiettivo dei Dorks

- Rintracciare documenti sensibili pubblicati involontariamente.
- Individuare sottodomini o portali nascosti.
- Identificare e-mail, nomi, ruoli e riferimenti aziendali.
- Rivelare directory indicizzate o indici di file accessibili.
- Collegare persone e dipendenti tramite i social professionali.

**Google Dorks utilizzati e risultati**

- site:mediaset.it filetype:pdf
  Ricerca di documenti PDF pubblicati da Mediaset.
  **Risultato:** codice_etico.pdf, privacy_policy.pdf, modello_231.pdf, bandi e informative contenenti e-mail, riferimenti interni e firme digitali.

- site:mediaset.it inurl:login
  Ricerca di portali di autenticazione e aree riservate.
  **Risultato:**
    - corporate.mediaset.it/login
    - recruitment.mediaset.it/admin/
      Entrambe accessibili solo previa autenticazione, nessuna vulnerabilità visibile ma endpoint pubblici identificabili.

- site:linkedin.com/in "mediaset"
  Ricerca di profili professionali associati all'azienda.
  **Risultato:**
    - Decine di dipendenti con ruoli in ambito IT, legale, produzione e commerciale.
    - Alcuni profili contenevano dettagli su tecnologie utilizzate (es. Microsoft Azure, Active Directory, CDN Akamai).

- site:mediaset.it intitle:"index of"
  Ricerca di directory indicizzate su server web.
  **Risultato:** Alcune cartelle contenenti materiale video e immagini pubblicitarie, con struttura di file leggibile (es. index of /mediafiles/).

- intext:@mediaset.it
  Ricerca di indirizzi e-mail associati al dominio.
  **Risultato:**
    - info@mediaset.it, ufficiostampa@mediaset.it, assistenza.clienti@mediaset.it
    - Presenti in comunicati, bandi e articoli stampa.

- site:mediaset.it ext:doc OR ext:xls OR ext:csv
  Ricerca di file Microsoft Office (potenzialmente informativi).
  **Risultato:** Nessun dato sensibile, ma file interni con tabelle e report di policy e investitori.

## 4. Mappatura e Analisi con Maltego

Utilizzando **Maltego CE**, è stata costruita una mappa relazionale a partire dal nodo principale mediaset.it.

**Transform eseguite:**

- **DNS to IP**, **NS Records**, **MX Records**, **Whois Info**, **Linked Entities**
- **Email from domain**, **Website metadata**, **Affiliate domains**

**Entità ottenute:**

- Dominio principale → mediaset.it
- Sottodomini: play.mediaset.it, news.mediaset.it, corporate.mediaset.it, recruitment.mediaset.it
- IP pubblici su AS italiani (es. 91.211.156.x)
- Email pubbliche e nomi associati
- Hostname CDN e provider tecnici (Akamai)

La mappa generata ha permesso di evidenziare **relazioni tra dominio, IP, mail, sottodomini e persone**, rendendo visibile la struttura di superficie dell'organizzazione.

## 5. Considerazioni Finali

L'attività di OSINT ha permesso di raccogliere una **quantità significativa di informazioni pubbliche** su Mediaset, senza interagire direttamente con i sistemi.
Le tecniche utilizzate hanno mostrato quanto possa essere esposta un'azienda tramite:

- Documenti ufficiali online.
- Portali di autenticazione pubblici.
- Profili social professionali.
- E-mail non mascherate.

Tutto ciò rappresenta materiale potenzialmente sfruttabile per campagne di **social engineering**, **phishing** o per attacchi mirati.

## 6. Conclusione

La simulazione ha dimostrato l'efficacia degli strumenti OSINT nella raccolta passiva di informazioni, con particolare valore per attività di sicurezza preventiva e red teaming.
Strumenti come **Google (dorks)** e **Maltego** permettono di ricostruire il perimetro informativo di un'organizzazione in modo rapido, legale e silenzioso.
Conoscere la propria esposizione è fondamentale per proteggersi: ciò che è visibile online può diventare un'arma nelle mani sbagliate.

## 7. Considerazioni Aggiuntive

Durante l'attività di raccolta informazioni su Mediaset è emerso quanto possa essere ampio il volume di dati accessibili tramite fonti pubbliche, senza la necessità di interazioni dirette o intrusive con i sistemi aziendali. Anche in presenza di infrastrutture strutturate e protette, la visibilità online resta una superficie di attacco concreta, spesso sottovalutata.

Questa esperienza ha messo in luce diversi aspetti rilevanti:

- **I Google Dorks** si confermano uno strumento semplice ma potentissimo: se utilizzati correttamente, permettono di ottenere accesso a documenti, portali e dati aziendali che l'organizzazione non sempre intendeva rendere facilmente accessibili.

- **Maltego** si è rivelato essenziale per rappresentare visivamente le relazioni tra domini, sottodomini, email, IP e altri asset digitali. Questa mappatura visiva aiuta a capire la complessità e l'estensione della presenza digitale di un'organizzazione.

- L'**uso inconsapevole di metadati**, la pubblicazione di PDF con nomi interni o riferimenti personali, e la presenza di e-mail aziendali online sono tutti elementi che, pur non essendo "vulnerabilità tecniche", rappresentano **vettori di rischio** in scenari di attacco reali.

- È emersa l'importanza dell'**approccio proattivo alla sicurezza**: le aziende dovrebbero eseguire periodicamente attività di OSINT su sé stesse per comprendere cosa è visibile all'esterno e correggere eventuali esposizioni indesiderate.

In sintesi, questa attività ha permesso di acquisire consapevolezza su come un attaccante potrebbe iniziare la propria analisi e preparare un attacco, ma anche su come un analista della sicurezza possa intervenire in fase preventiva per migliorare la postura di sicurezza aziendale.