Introduzione all'OSINT

OSINT:

Open Source INTelligence

Febbraio 2018

OSINT

- **Definizione:**

  E' un metodo di investigazione ovvero :

  è l'attività sistematica di raccolta, elaborazione e analisi di informazioni liberamente e legalmente accessibili.

  Qualsiasi fonte di informazione liberamente e legalmente accessibile come:

  - Internet (siti web, social network, blog, ecc...);
  - Giornali, riviste;
  - Registri pubblici (anagrafe, camera commercio, PRA, catasto, ecc...).

OSINT

- **Definizione di Intelligence**

  Il termine intelligence (esemplificato in italiano come informazione militare o civile) può essere esplicato concettualmente come la raccolta e la successiva analisi di notizie e dati dalla cui elaborazione ricavare informazioni utili al processo decisionale militare, nonché a quello relativo alla sicurezza nazionale ed alla prevenzione di attività destabilizzanti di qualsiasi natura.

  In senso più ampio vengono intese tutte le attività legate al controspionaggio, e allo spionaggio.

  Deputate a tale attività vi sono delle strutture statali, identificate spesso con la locuzione di servizi segreti.

  (fonte: Wikipedia)

OSINT

- OSINT è solo una fra le diverse discipline legate all'intelligence; ad esempio, oltre ad essa, esistono:

- **HUMINT:** Human INTelligence
  Attivita' di gestione rete informatori

- **SIGINT:** Signal INTelligence
  Attivita' di interpretazione delle comunicazioni

- **IMINT:** Imagery INTelligence
  Elaborazioni immagini derivanti da satelliti, aerei spia , droni

- **MASINT:** measurement and signature INTelligence
  analisi firme chimiche, spettografiche , radiologiche di sistemi d'arma che possono nuocere alla sicurezza nazionale

OSINT

- **La demodoxalogia, l'OSINT (Open Source INTelligence) italiana**
  (demo=popolo, doxa=opinione, logos=discorso)

  Pochi sanno che l'OSINT ha una versione nata in Italia nel 1928 dalla scienza della demodoxalogia e che quest'ultima si differenzia dalla prima perché più complessa e precisa.

  Le differenze consistono nel rilevamento dei dati che possono alterare i pubblici di riferimento e nel condizionare l'orientamento della pubblica opinione sul nascere.

(Fonte: http://www.difesaonline.it/evidenza/approfondimenti/la-demodoxalogia-losint-open-source-intelligence-italiana)

OSINT

OSINT limitato a Internet:

- La “Cyber Intelligence”, l’attività di intelligence in Internet che si basa su fonti aperte, può attualmente essere definita come il lavoro sistematico di raccolta, elaborazione, analisi, produzione, classificazione e diffusione di informazioni liberamente e legalmente accessibili.

OSINT

- L'OSINT utilizza tecniche, strumenti e procedure utilizzate anche da attività quali:

  - Hacking
  - Penetration Testing
  - Giornalismo investigativo
  - Investigazioni
  - Intelligence

OSINT

“***Se riveli al vento i tuoi segreti,***
non devi poi rimproverare al vento di rivelarli agli alberi”

(Kahlil Gibran)

Frase con la quale Leonida Reitano nel suo manuale

“*Esplorare Internet – Manuale di investigazioni digitali e Open Source Intelligence*”

inquadra l’argomento.

OSINT

- I requisiti per avere un’attività di tipo OSINT, sono l’impiego di:

- informazioni non classificate;
- informazioni acquisite in modo lecito (no hacking, no intercettazioni, no spionaggio);
- Informazioni disponibili al pubblico.

OSINT

- **Google Dorks**

  - Dall'inglese possiamo constatare che *dork* è un termine utilizzato nello slang per indicare una persona stupida, inetta.

  - Le *Google dorks* sono paragonabili a delle query specifiche è possibile richiedere al motore di ricerca per ottenere le informazioni che desideriamo.

    Il campo di applicazione delle dorks è veramente ampio, infatti attraverso questo strumento potremo individuare in pochissimo tempo determinati file nel web come PDF, MP3 e così via, oppure addirittura pagine web particolari che contengono login e password degli utenti un determinato servizio.

OSINT

- **Google Dorks – Utilizzo**

  Attraverso l'utilizzo di operatori avanzati nel motore di ricerca si individuano specifiche stringhe di testo all'interno dei risultati.

  Gli operatori avanzati, quali ad esempio

  - `allintext:`
  - `allintitle:`
  - `allinurl:`
  - `filetype:`
  - `site:`

  utilizzati congiuntamente agli operatori booleani (`AND`, `NOT` e `OR`) possono fornire interessanti risultati anche nell'ambito dell'OSINT e non solo in quello della ricerca di vulnerabilità e problemi di sicurezza dei siti.

OSINT

Per fare un esempio che rende l'idea di ciò che è possibile ottenere tramite gli operatori avanzati, si prenda in considerazione la semplice query su Google:

```
spese filetype:xls site:comune.roma.it
```

Questa query restituirà i link a quei file con estensione .xls (una delle possibili estensioni dei file Excel) contenenti la parola "spese" all'interno del file o della pagina e che risiedono sul sito comune.roma.it.

È quindi evidente come la potenza del motore di ricerca, attraverso un controllo molto più fine e granulare, possa diventare uno strumento utilissimo nelle ricerche OSINT: i dati sono lì, disponibili a tutti, basta saperli cercare...

OSINT

Elenco di alcune Dorks...

- `intitle:<parola chiave>`: cerca nel titolo del sito e ritorna la parola esatta cercata.
- `allintitle:<parola chiave>`: differisce da quella precedente per il fatto che cerca nel titolo tutte le parole nella ricerca.
- `allintext:<parola chiave>`: come prima, ma invece che nel titolo cerca nel testo del sito.
- `inurl:<parola chiave>` e `allinurl:<parola chiave>`: cerca la parola nell'url del sito, nello stesso modo di prima.
- `filetype:<tipodifile>`: cerca uno specifico tipo di file, che può essere un PDF, un CSV o un ODT.
- `cache:<sito web>`: cerca nella cache di Google l'indirizzo specificato, utile quando quel sito è down, o la pagina è stata rimossa dall'admin.
- `info:<sito web>`: Google espone tutte le informazioni che può darti in merito a quella ricerca, quindi ti indirizza a tutte le ricerche più simili

(https://sites.google.com/site/gwebsearcheducation/advanced-operators)

OSINT

- **MALTEGO** (https://www.paterva.com/web7/)

  Lo scopo principale di questa applicazione è l'analisi delle relazioni esistenti nel mondo reale fra persone, gruppi, siti web, domini Internet, reti e appartenenza a social network quali Facebook e Twitter.

  Ciò che si può ottenere è la rappresentazione dell'ambiente nel quale un'organizzazione opera, la complessità di questo ambiente viene dunque evidenziata insieme ai propri punti deboli e alle relazioni che lo costituiscono.

  Ogni dato relativo all'organizzazione oggetto dell'analisi (che sia la configurazione di un router o il luogo in cui si trova il Vice Presidente durante i suoi viaggi all'estero) viene reperito, aggregato e l'informazione che ne viene tratta viene presentata in forma grafica.

OSINT

Maltego può essere usato per analizzare le relazioni e i collegamenti esistenti nel mondo reale fra persone, gruppi di persone (ad esempio sui social network), aziende, organizzazioni e siti web.

Il software analizza anche i domini Internet, i nomi DNS e gli indirizzi IP, oltre che file e documenti (che rimangono sempre una fonte essenziale di informazioni).

Ognuna di questa entità viene messa in relazione con le altre a supporto dell'attività di OSINT.

L'interfaccia grafica dello strumento rende possibile "vedere" in maniera istantanea le relazioni esistenti fra le entità e le connessioni a volte nascoste da diversi gradi di separazione.

Maltego Showcase
https://www.paterva.com/web7/docs/use_cases.php

OSINT

- **FOCA** (Fingerprinting Organizations with Collected Archives)
  (https://www.elevenpaths.com/labstools/foca/index.html)

  È uno strumento utilizzato principalmente per estrarre metadati e informazioni nascoste all'interno dei documenti sottoposti a scansione.

  Tali documenti possono risiedere su pagine web e possono essere scaricati e analizzati tramite FOCA.

  I documenti analizzabili sono quelli di Microsoft Office, Open Office, i file PDF o i file SVG.
  I documenti possono essere ricercati attraverso tre possibili motori di ricerca (fra cui Google e Bing), tuttavia anche file locali possono essere analizzati.

OSINT

Dai file di immagini fotografiche FOCA è in grado di estrarre i metadati Exif (quali ad esempio data e ora dello scatto, il modello ed il produttore della fotocamera, il luogo degli scatti).

FOCA riesce ad analizzare l'informazione residente nell'URL sottoposto a scansione prima ancora che il file venga in effetti scaricato.

Una volta scaricati i file (che possono risultare anche in numero considerevole), FOCA si occupa di incrociare le informazioni nel tentativo di identificare quali documenti sono stati creati dallo stesso gruppo all'interno di un'organizzazione o magari scoprire il nome dei server o dei client utilizzati, il loro sistema operativo.

OSINT

- **Web - Tools**
  (http://whois.domaintools.com/

- Chi ha registrato un determinato sito? Chi ha avuto interesse a farlo? Oltre a quel sito ne ha registrati altri, ora o in passato? Quali altri domini sono ospitati sullo stesso server e che relazioni potrebbero quindi esserci fra siti web apparentemente non correlati fra loro?

  DomainTools viene in aiuto a chi vuole o deve rispondere a queste domande.

  È un portale che fornisce informazioni a partire da indirizzi IP o nomi a dominio, dal portale è possibile risalire alla proprietà attuale e storica di un nome a dominio, si possono fare ricerche a partire da un indirizzo email o un numero di telefono per verificare se quell'indirizzo o quel numero sono legati in questo momento in storicamente alla registrazione di un certo dominio.

OSINT

- **WayBackMachine**
  https://www.waybackmachine.org

  A volte potrebbe essere importante risalire all'aspetto, ma soprattutto ai contenuti di cui un sito disponeva in passato.
  Le attività di OSINT non possono prescindere dal fattore storico, una vera indagine deve andare a "scavare" anche nel passato per ritrovare tracce che qualcuno ha volutamente cercato di eliminare o informazioni che il tempo, fisiologicamente, tende ad offuscare.
  Il sito WayBackMachine viene in soccorso dell'analista, investigatore o giornalista di turno che può scoprire legami o dichiarazioni non più presenti online, ma gelosamente custoditi da WayBackMachine.

  A proposito della rete che "non dimentica" le aziende (ma anche i privati cittadini) farebbero bene a tener conto del cosiddetto "*effetto Streisand*" secondo il quale:

  "***un tentativo di censurare o rimuovere un'informazione ne provoca, contrariamente alle attese, l'ampia pubblicizzazione***".

OSINT

- **Shodan** (https://www.shodan.io/)

  Shodan è un motore di ricerca che permette all'utente di rilevare specifici dispositivi (computer, router, server, ecc.) collegati ad Internet servendosi di una grande varietà di filtri.

  Alcuni lo definiscono un motore di ricerca di "service banner", intesi come "meta-dati" che il server restituisce al client che lo interroga.

  I meta-dati forniti in risposta possono dare indicazioni sul sofware, su quali opzioni il servizio ospitato offre, un messaggio di benvenuto (a volte "troppo" informativo...) e qualsiasi altra informazione ritenuta più o meno utile ancora prima che il client stabilisca una vera e propria connessione col server.

OSINT

Shodan colleziona dati principalmente riguardanti web server (che rispondono tipicamente sulla porta 80, HTTP), ma è possibile trovar dati relativi a server FTP (21), SSH (22), Telnet (23), SNMP (161) e SIP (5060).

Molto spesso ciò che Shodan scopre è una quantità di server (e servizi) che risultano esposti su Internet per negligenza di chi li ha configurati o di chi ha il compito di proteggerli e gestirli.

OSINT

- **OSINT nel Deep Web**

  - Tuttavia è certamente evidente che se il Web di superficie è una fonte di dati (e quindi informazioni) di inestimabile valore, a maggior ragione possiamo ritenere il “Deep Web”, ossia la parte della rete non indicizzata dai motori di ricerca comuni, come un vera e propria miniera dal punto di vista dell’OSINT considerata l’enorme quantità del materiale che giace sotto la superficie che è di gran lunga superiore a quella di ciò che affiora.

OSINT

- **ESC1622 Open Source Intelligence e imprudenza dell'utente - Quello che la Rete sa di noi**
  https://www.youtube.com/watch?v=5LSqmiJgS34
- **OSINT Tools: Recommendations List**
  http://www.subliminalhacking.net/2012/12/27/osint-tools-recommendations-list/
- **La demodoxalogia, l'OSINT (Open Source INTelligence) italiana**
  http://www.difesaonline.it/evidenza/approfondimenti/la-demodoxalogia-losint-open-source-intelligence-italiana
- **Google Dorks**
  https://sites.google.com/site/gwebsearcheducation/advanced-operators
  https://hacktips.it/google-hacking/

OSINT

- **Maltego**
  https://www.paterva.com/web7/
  http://www.html.it/articoli/osint-con-maltego-2/
- **Foca**
  https://www.elevenpaths.com/labstools/foca/index.html
- **WayBackMachine**
  https://www.waybackmachine.org
- **Shodan**
  https://www.shodan.io/