Spionaggio Open Source

Le tecniche dei black hat per scovare le informazioni riservate sui loro target senza che la vittima si accorga di nulla

In collaborazione con thehackingquest.net

HACKING QUEST
JOIN THE QUEST

Una delle fasi fondamentali di un attacco è la sua preparazione. Più accurata ed esaustiva è l'analisi sull'obiettivo, più efficace sarà la nostra preparazione, la stesura della nostra strategia e, di conseguenza, più alte saranno le nostre probabilità di successo. Lo scopo della fase di ricognizione è attingere il maggior numero di informazioni utili sul target, essenziali da utilizzare nella fase d'attacco, senza lasciare che la vittima si accorga di cosa sta avvenendo. Per raggiungere il nostro obiettivo effettueremo una ricognizione servendoci di tecniche di investigazione su fonti pubbliche/aperte: Open Source Intelligence (**OSINT**).

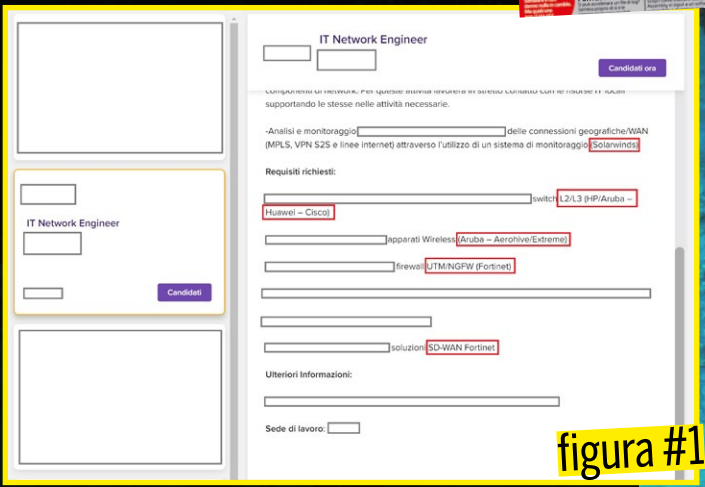

figura #1

CHE COS'È L'OSINT?

Potremmo definire l'OSINT come "la scansione, la ricerca, la raccolta, l'estrazione, l'utilizzo, la convalida, l'analisi e la condivisione delle informazioni pubbliche/aperte disponibili da fonti non classificate e non segrete". Si tratta di un vero e proprio percorso di investigazione fra i dedali della Rete, cercando tasselli di bit per una visione macro (e a volte anche micro) del nostro target, sia esso una grande azienda oppure un singolo soggetto.

PERCHÉ È FONDAMENTALE?

Tutte le informazioni che riusciremo a reperire durante il nostro percorso investigativo ci aiuteranno a individuare l'anello debole da attaccare, ma anche quale tipologia di attacco perpetrare. Facciamo qualche esempio:

- se dovessimo avvalerci di tecniche di phishing avremmo bisogno di identificare gli utenti più vulnerabili;
- nel caso dovessimo eseguire un "Password Guessing Attack", avremmo bisogno di scoprire il formato che la data azienda utilizza per creare lo username dei propri utenti;
- informazioni sull'infrastruttura possono aiutarci a capire quale sistema AV/EDR è in uso e quindi quali tecniche di evasione (vedi box **I pirati aggirano le difese così**) utilizzare affinché il nostro payload non venga rilevato;
- apprendere informazioni sulla tipologia di rete o dati architetturali potrebbe aiutarci nella fase di pivoting all'interno della rete (vedi box **Cos'è il pivoting?**);
- sfruttare numeri di telefono ed email, utilizzabili per mettere in atto tecniche di social engineering, fingendoci qualcuno del reparto IT oppure un utente che contatta l'Help Desk perché non riesce ad accedere al proprio computer;
- potremmo addirittura reperire credenziali utili da vecchi data breach e, anche se l'utente o la password non fossero più in uso, avremmo comunque reperito informazioni sulle regole applicate dall'azienda per la costruzione di nomi utente e password.

Cerca di anticipare i piani del nemico, e individua i suoi punti forti e deboli: potrai decidere quale strategia usare per avere successo e quale no

TIPOLOGIA DI DATI

I dati utili che potremmo reperire rispetto al nostro scopo potrebbero essere stati condivisi in maniera intenzionale o non intenzionale. Tra i primi possiamo citare: URL di siti Web; nomi di progetti; report annuali sull'andamento delle aziende; offerte di lavoro. Tra i dati pubblicati/esposti non intenzionalmente, troviamo invece: informazioni sugli account ottenuti da breach di ▸

figura #2

```
└─# whois thehackingquest.net --verbose
Using server whois.verisign-grs.com.
   Domain Name: THEHACKINGQUEST.NET
   Registry Domain ID: 2644512615_DOMAIN_NET-VRSN
   Registrar WHOIS Server: whois.tucows.com
   Registrar URL: http://www.tucows.com
   Updated Date: 2021-09-29T19:17:07Z
   Creation Date: 2021-09-29T19:17:07Z
   Registry Expiry Date: 2022-09-29T19:17:07Z
   Registrar: Tucows Domains Inc.
   Registrar IANA ID: 69
   Registrar Abuse Contact Email: domainabuse@tucows.com
   Registrar Abuse Contact Phone: +1.4165350123
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.HOVER.COM
   Name Server: NS2.HOVER.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-01-17T07:29:56Z <<<
```

```
Name Server: ns1.hover.com
Name Server: ns2.hover.com
```

figura #3

terze parti; social media del nostro target (sia esso un privato o un dipendente); metadati; server banner. Vediamo adesso quali fonti, tool e luoghi potremmo dover visitare o utilizzare durante la nostra caccia alle informazioni. Supponiamo che il nostro target sia una grande azienda.

WIKIPEDIA

Un semplice quanto banale punto di partenza, potrebbe essere consultare **Wikipedia** (se l'organizzazione/il soggetto da attaccare è grande o famoso abbastanza). Potremmo reperire alcune informazioni basilari sulla relativa storia, che non sempre sono presenti sul sito Web, tra cui magari note su compagnie collegate o affiliati che potrebbero avere indirettamente accesso all'organizzazione o semplicemente essere più vulnerabili al phishing.

POSIZIONI DI LAVORO APERTE

Moltissime organizzazioni hanno posizioni aperte sul loro sito Internet. Questo potrebbe aiutarci a capire quali informazioni, tecnologie o prodotti vengono utilizzati dal nostro target:

- tipologia del server Web;
- tipologie di firewall;
- router presenti nella LAN;
- ambienti software utilizzati dagli sviluppatori.

Per esempio, potremmo decidere di cercare sul sito *www.monster.it* (o un qualunque altro sito dedicato alla ricerca di lavoro) la parola "Sistemista" e la zona geografica **[figura #1]**.

WHOIS

Whois è un protocollo di rete che permette di stabilire a quale provider Internet appartiene un determinato indirizzo IP o uno specifico DNS. Nelle informazioni contenute da un'interrogazione fatta a un database Whois (che contiene, appunto, i dati pubblici sui provider), spesso vengono rilevati anche i dati dell'intestatario. Eseguiamo come esempio il Whois sul nostro blog, *thehackingquest.net*, usando il comando **whois** seguito dal dominio target (l'URL del blog) e dall'opzione **--verbose**, così da avere un output esteso **[figura #2]**.

```
whois thehackingquest.net --verbose
```

Gli elementi finali dell'interrogazione Whois rilevano le informazioni relative al Domain Name System (DNS) associato al target. Nel prossimo paragrafo, proveremo ad attingere informazioni dai record del **name server [figura #3]**.

SERVER DNS

Lo scopo primario del DNS è risolvere i nomi di dominio in indirizzi IP, ma non è il solo. Il DNS svela anche altre informazioni utili, per esempio fornisce indicazioni su quali macchine siano i mail server per un dato dominio. Esistono infatti diversi tipi di record:

- **NS** - il record Nameserver indica il nome dei server associati al dominio target;
- **A** - il record Address mappa il nome del dominio (domain name) nell'indirizzo IPv4 corrispondente;
- **AAAA** - il record "Quad-A" mappa il domain name nell'indirizzo IPv6 corrispondente;
- **HINFO** - Host Information Record, associa informazioni arbitrarie con il nome di dominio (solitamente viene usato per indicare la tipologia del sistema);
- **MX** - il record Mail Exchange identifica i server email per il dato dominio;
- **TXT** - Text Record, include una stringa di testo

figura #4

```
└─# dig thehakingquest.net

; <<>> DiG 9.17.21-1-Debian <<>> thehakingquest.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30402
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

COS'È IL PIVOTING?

Con questa tecnica, un attaccante può sfruttare una macchina compromessa come punto d'appoggio per attaccare altre macchine nella stessa o in altre reti che normalmente non potrebbe raggiungere. La maggior parte delle volte l'attaccante usa questa tecnica per compromettere altre macchine e sottoreti e arrivare così all'obiettivo finale.

per il dominio;
- **CNAME** - Canonical Name, indica un alias o un nome alternativo per il dominio;
- **SOA** - record Start of Authority, marca il server come "Autorevole" per la zona DNS;
- **RP** - Responsible Person Record, record informativo e non funzionale che indica l'incaricato o la persona responsabile per il dato dominio;
- **PTR** - Reverse Record, indica l'indirizzo IP per il dato server;
- **SRV** - Service Location Record, fornisce varie informazioni, inclusi porta e hostname, sui servizi disponibili.

Supponiamo adesso di voler eseguire delle query sui DNS utilizzando il comando Domain Information Groper (**dig**).
Digitiamo quindi **[figura #4]**

```
dig thehackingquest.net
```

Esiste un processo chiamato **Zone Transfer** per cui un server DNS passa una copia del suo database (chiamato "zona") a un altro server DNS. L'attacco chiamato **Zone Transfer Attack** consiste nel chiedere al DNS primario una copia dei record di zona e si basa sull'assunto che tutti i server si fidano gli uni degli altri (in gergo si dice che sono "trusted"). Per eseguire questo attacco utilizzando il tool dig dovremo dare il seguente comando:

```
dig @[server] [dominio] -t AXFR
```

dove
- **@[server]** è il server DNS;
- **[dominio]** è il nome del dominio da "attaccare";
- **-t** specifica la tipologia della query che sarà **AXFR**, cioè si richiede la copia della DNS Zone.

Esistono anche altri tool che permettono di automatizzare le query ai server DNS.
Per esempio, **DNSrecon** permette di eseguire anche attacchi bruteforce con una dictionary list.

```
dnsrecon -d [dominio] -t brt -D [wordlist]
```

Oppure si può usare **DNSDumpster** (*https://dnsdumpster.com*), uno strumento online gratuito per scoprire gli host collegati a un dominio. Ci fornisce più di un centinaio di record DNS A, con i corrispondenti indirizzi IP e i relativi Autonomous System Number (ASN).
Un AS è un insieme di IP appartenenti a una rete o a un insieme di reti gestite, controllate e supervisionate da una singola entità o organizzazione **[figura #5]**. Diversamente, potremmo scrivere in autonomia il nostro script: supponiamo di avere appena formulato una lista di potenziali nomi di host che la nostra organizzazione target espone pubblicamente sulla Rete e di aver chiamato il file **targethost.txt** (nomedelserver.nomeorganizzazione.com).
Per il nostro scopo utilizzeremo il comando **host**, che ci permetterà di interrogare il DNS al fine ▸

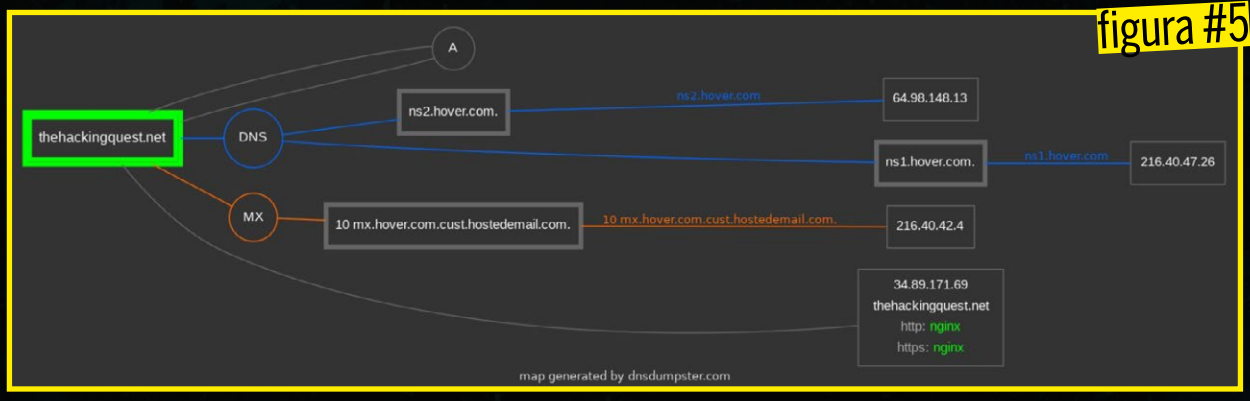

figura #5

figura #6

```
┌──(root💀 a1rk)-[/tmp]
└─# cat targethost.txt
thehackingquest.net

┌──(root💀 a1rk)-[/tmp]
└─# for targethost in $(cat targethost.txt); do host $targethost; done
thehackingquest.net has address 34.89.171.69
thehackingquest.net mail is handled by 10 mx.hover.com.cust.hostedemail.com.
```

figura #7

```
159.226.36.183   7002
93.90.222.28     37215   Softline Trade JSC
159.75.125.176   587     Tencent Cloud Computing (Beijing) Co., Ltd
164.128.164.31   50000   Swisscom (Schweiz) AG   31.164.128.164.static.wline.lns.ent.cust.swisscom.ch
164.128.164.32   50000   Swisscom (Schweiz) AG   32.164.128.164.static.wline.lns.ent.cust.swisscom.ch
43.130.66.10     1311    Asia Pacific Network Information Center, Pty. Ltd.
2.143.136.110    8080    TELEFONICA DE ESPANA    110.red-2-143-136.dynamicip.rima-tde.net
129.226.36.183   2181
82.0.237.47      86      LEWISHAM        cpc145676-lewi19-2-0-cust302.2-4.cable.virginm.net
164.128.164.109  7001    Swisscom (Schweiz) AG   109.164.128.164.static.wline.lns.ent.cust.swisscom.ch
43.130.66.10     3952    Asia Pacific Network Information Center, Pty. Ltd.
81.71.46.239     7474    Tencent Cloud Computing (Beijing) Co., Ltd
81.71.46.239     221     Tencent Cloud Computing (Beijing) Co., Ltd
43.130.64.95     50000   Asia Pacific Network Information Center, Pty. Ltd.
164.128.164.34   8081    Swisscom (Schweiz) AG   34.164.128.164.static.wline.lns.ent.cust.swisscom.ch
43.130.66.10     5432    Asia Pacific Network Information Center, Pty. Ltd.
43.130.64.95     2222    Asia Pacific Network Information Center, Pty. Ltd.
72.194.143.118   37215   Linode  ip1659-118.members.linode.com
```

di identificare quale indirizzo IP si cela dietro a un dato hostname (ovviamente se il nome non esiste, non verrà fornito nessun IP). Quindi scriviamo il nostro comando:

```
for targethost in $(cat targethost.txt); do
host $targethost; done
```

Se l'hostname esiste, il nostro script ci fornirà il suo indirizzo IP **[figura #6]**.

WHOIS DATABASE

Un altro elemento importante per ampliare la superficie del nostro attacco consiste nell'identificare il blocco di IP pubblici assegnati alla nostra società bersaglio. Diverse regioni offrono il database whois contenente le informazioni degli IP relativi a uno specifico dominio. Vediamo quali sono le regioni principali:

- **ARIN** - American Registry for Internet Numbers;
- **RIPE NCC** - The Réseaux IP Européens Network Coordination Centre;
- **APNIC** - The Latin American and Caribbean Internet Address Registry;
- **AS** - Autonomous System.

Ovviamente, non tutte le organizzazioni hanno un blocco di IP a loro designato, ma a molte viene assegnato un indirizzo IP pubblico dal loro Internet Service Provider (ISP).

SHODAN

Shodan (*www.shodan.io*) è un motore di ricerca un po' particolare: effettua costantemente scansioni su Internet al fine di mappare gli host connessi e raccogliere informazioni su porte e servizi in ascolto, come certificati SSL (che possono rivelare altri sottodomini, geolocalizzazione degli IP, etc...). Facciamo un breve esempio: supponiamo di voler cercare con Shodan tutte le webcam, scegliendo di visualizzarne solamente IP, porta, organizzazione e hostname. Come prima cosa, dobbiamo inserire la nostra **API Key** (reperibile registrandosi sul sito del motore di ricerca anche se, cercando con cura in Rete, si trovano delle chiavi anche senza registrarsi...). Apriamo un terminale sulla nostra macchina attaccante e digitiamo:

```
shodan init [La nostra API Key]
```

Una volta che la sincronizzazione sarà avvenuta decidiamo cosa cercare, per esempio le webcam, e digitiamo **[figura #7]**

I PIRATI AGGIRANO LE DIFESE COSÌ

Ecco le tipologie di tecniche di evasione più usate:

- **crittografia e tunneling** - i sistemi IPS monitorano la rete e catturano i dati mentre passano sulla rete, ma sensori di questo tipo ipotizzano che i dati siano trasmessi in chiaro. Un modo per evitarli è quello di usare connessioni cifrate;
- **tempistica degli attacchi** - gli aggressori possono eludere i sistemi di rilevamento eseguendo le loro azioni più lentamente del solito. Questa tipologia di "evasione" può essere effettuata verso tecnologie che usano una finestra temporale di osservazione fissa e un livello di soglia per la classificazione degli eventi malevoli;
- **errata interpretazione dei protocolli** - l'attaccante gioca sul fatto che un sensore sia portato a ignorare o meno un certo traffico, ottenendo come risultato che l'azienda veda quel traffico in maniera differente rispetto alla vittima.

Cercate un tool dotato di interfaccia grafica per le vostre investigazioni OSINT? Provate Maltego

```
shodan search --fields
ip_str,port,org,hostnames webcam
```

BUILTWITH

BuiltWith (*https://builtwith.com/*) è un utile strumento che ci può dare una lista di tutte le tecnologie in uso per un determinato dominio e sottodominio:

- Web Host
- Web Server
- Detected CDN
- Framework
- Widget

Ricordiamo che una CDN è una rete per la distribuzione dei contenuti. Cioè si tratta di un gruppo di server distribuiti in più aree geografiche che serve a velocizzare il recapito dei contenuti Web facendoli arrivare dalla posizione geografica più vicina possibile al luogo in cui si trovano gli utenti.

DIRETTAMENTE L'HOSTNAME

È bene tenere presente che il nome della macchina molte volte indica anche il suo scopo. Per il **password spraying attack** è utile verificare l'esistenza delle seguenti macchine:

- nomi che contengono login, portal, sso, adfs o remote;
- online email: mail, autodiscover, owa;
- Citrix: ctx, citrix storefront
- VPN: vpn, access

Un attacco password spraying è un tipo di attacco a forza bruta in cui l'attaccante forza una procedura di login usando un elenco di nomi utente e le password predefinite.

MOTORI DI RICERCA "CLASSICI"

La tecnica è anche nota come **Dorking** o **Google Hacking** ed è utilizzata per effettuare interrogazioni sul Web sfruttando il motore di ricerca Google. Ne avevamo parlato in maniera estesa, per esempio, su HJ 217 e lo faremo anche nel prossimo numero, ma vediamo subito qualche esempio.
Esiste poi un database di riferimento con cui sbizzarrirsi: *https://www.exploit-db.com/google-hacking-database*.
Vediamo le basi. Se scriviamo, nel campo di ricerca di Google, non una normale stringa di testo, ma alcuni particolari parametri, è possibile definire in modo preciso cosa si sta cercando. Per esempio:

- **site** - consente all'attaccante di cercare in un singolo sito o dominio;
- **intitle** - cerca i criteri specificati nella page-title;
- **inurl** - cerca nell'URL specificato.

Possiamo inoltre specificare l'estensione di ciò che cerchiamo (.pdf , .docx , .xlsx, etc...). Quindi, per esempio, se vogliamo cercare tutti i documenti PDF contenuti nel sito *microsoft.com*, inseriremo nella barra di ricerca di google la seguente stringa: ▶

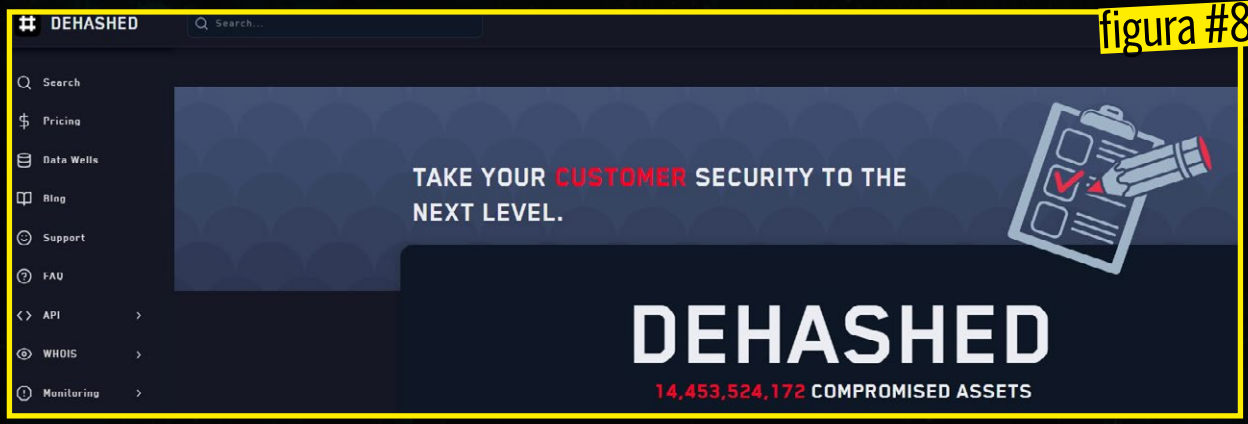

figura #8

figura #9

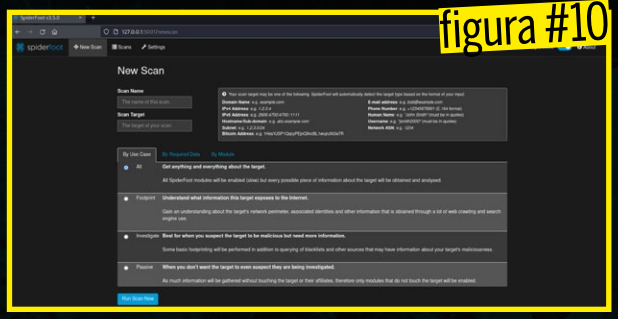

figura #10

```
site: microsoft.com filetype:pdf
```

Altri esempi di Dork potrebbero essere:

```
site:example.net  ext:xml | ext:conf |
ext:cnf | ext:reg | ext:inf | ext:rdp |
ext:cfg | ext:txt | ext:ora | ext:ini
```

dove "site" è il sito target ed "ext" sta per "estensione". Ergo, nei tre siti registrati a nome della holding Example S.p.A verranno ricercati eventuali file di configurazione esposti.
Al fine di cercare le pagine di login in correlazione con il target, possiamo digitare:

```
site:example.net inurl:login
```

DOCUMENT METADATA

Solitamente, quando viene creato un documento utilizzando un determinato software, questo porta con sé numerose informazioni che non sempre vengono eliminate, per esempio:

- Nome utente (username);
- percorso nel filesystem;
- indirizzi email;
- software usato lato client;

e altre informazioni. Ci sono molti tool impiegati per estrarre metadati dai documenti, i più comuni sono:

- **PowerMeta** - *https://github.com/dafthack/PowerMeta*
- **ExifTool** - *https://exiftool.org/*
- **FOCA** - *https://github.com/ElevenPaths/FOCA*
- **Metadata Extraction** - *https://github.com/DIA-NZ/Metadata-Extraction-Tool/*

PUBLIC DATA BREACH CREDENTIAL

I data breach sono una fonte inesauribile di risorse e anche quando username o password sono state cambiate, possono fornire comunque informazioni sulle regole di creazione utilizzate dall'azienda target.
Dove possiamo reperire i data breach?
Ecco alcune possibili fonti:

- *HaveIBeenPwned.com*
- *Dehashed.com* **[figura #8]**
- *Scylla.so*
- Dump su forum pubblici
- Siti Torrent
- Altro, per esempio *Archive.org*.

SOCIAL – LINKEDIN

LinkedIn è un'ottima piattaforma per fare ricognizione ai danni di una data organizzazione. Offre, infatti, l'opportunità di profilare i dipendenti, ottenendo: nomi, titoli, indirizzi email, affiliati, etc. Un buon tool per raccogliere informazioni sui dipendenti nomi/indirizzi email è **LinkedInt** scaricabile al seguente indirizzo: *https://github.com/vysecurity/LinkedInt* **[figura #9]**. Oppure, possiamo scegliere di utilizzare un'estensione di **Burp Suite** chiamata **GatherContacts**, scaricabile al seguente link: *https://github.com/clr2of8/GatherContacts*.

SPIDERFOOT

SpiderFoot è un OSINT scanner automatico che utilizza più di cento moduli differenti. Vediamo come utilizzarlo per fare la nostra ricerca.
Come prima cosa, al fine di scaricare l'ultima release disponibile, apriamo sulla macchina attaccante un nuovo terminale e digitiamo

Hunter.io è un servizio a pagamento che esegue regolarmente profilazioni OSINT di aziende e fornisce i pattern email comuni

```
wget https://github.com/smicallef/
spiderfoot/archive/v3.5.tar.gz
```

Estraiamo il contenuto del file **.gz** con

```
tar zxvf v3.5.tar.gz
```

Entriamo nella directory così creata:

```
cd spiderfoot-3.5
```

Installiamo i requisiti necessari:

```
pip3 install -r requirements.txt
```

Infine avviamo il nostro tool in locale sulla porta 5001:

```
python3 ./sf.py -l 127.0.0.1:5001
```

Da un altro terminale apriamo il nostro browser (nel nostro caso Firefox):

```
firefox -private
```

Sulla barra degli indirizzi digitiamo *http://127.0.0.1:5001/*. A questo punto, dovrebbe esserci apparsa la pagina di SpiderFoot. Clicchiamo su **New Scan** in alto a sinistra **[figura #10]**. Scegliamo una delle quattro opzioni:

- **All** - utilizza tutti i moduli disponibili, ma impiega molto tempo (giorni);
- **Footprint** - esegue la scansione circoscritta al perimetro della rete (per la maggior parte offre risultati derivanti da search engine e Web crawling);
- **Investigate** - utile soprattutto ai Blue Team in quanto designata ad analizzare potenziali siti e IP malevoli o sospetti;
- **Passive** - nessuna query diretta al target o ad affiliati, puro OSINT.

Infine, inseriamo nella maschera a sinistra Nome e Target. Ci vorrà del tempo a seconda dell'opzione che abbiamo selezionato, ma alla fine otterremo il nostro risultato **[figura #11]**.

DUMPSTERDIVING

Esistono altre tecniche "rudimentali", ma non meno efficaci, utilizzate per carpire informazioni potenzialmente utili. Per esempio, la ricerca di informazioni là dove la vittima cestina i suoi rifiuti...

figura #11