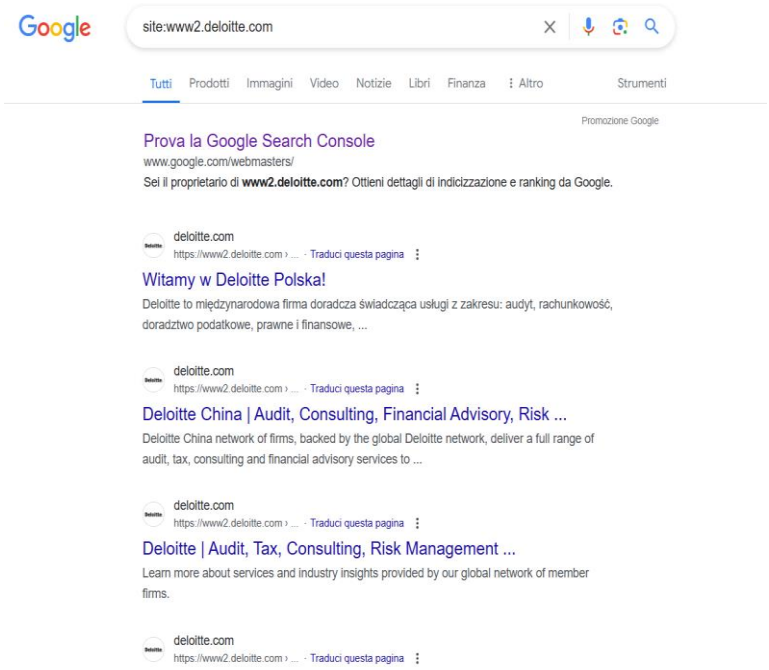
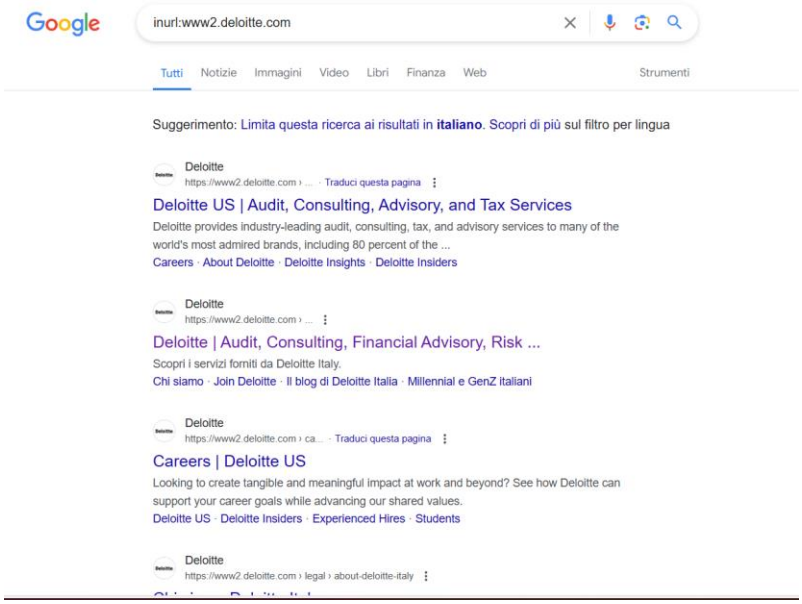
W10D1 – Raccolta di informazioni.

Google Hacking

Ho scelto il sito di Deloitte www2.deloitte.com come target per questa raccolta di informazioni ed ho cominciato la ricerca da Google Hacking eseguendo le queries indicate nella consegna e combinandole per cercare ulteriori informazioni e vulnerabilità.

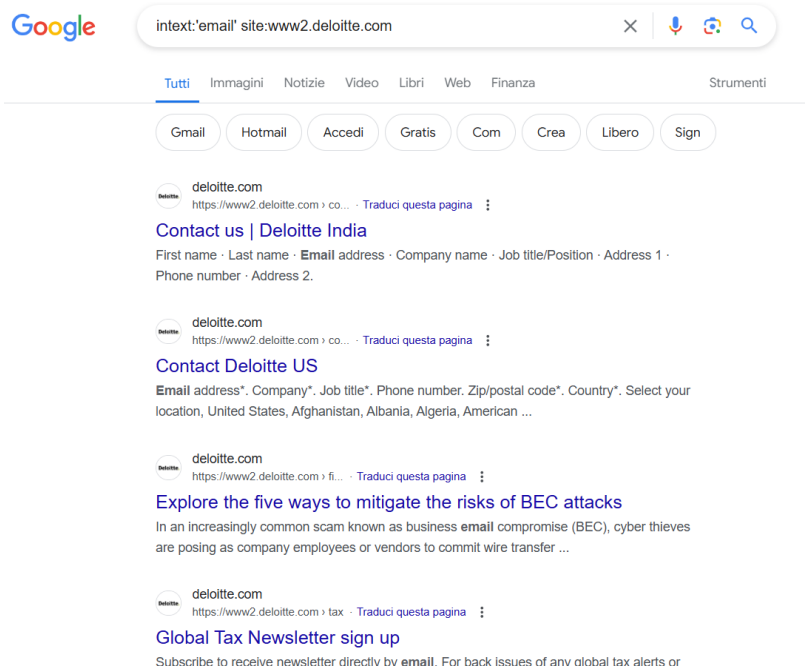


Con una query "site" ho trovato tutte le pagine indicizzate di quel sito, trovando numerose pagine delle divisioni di Deloitte presenti in tutto il mondo e degli ambiti tematici di cui si occupa Deloitte.

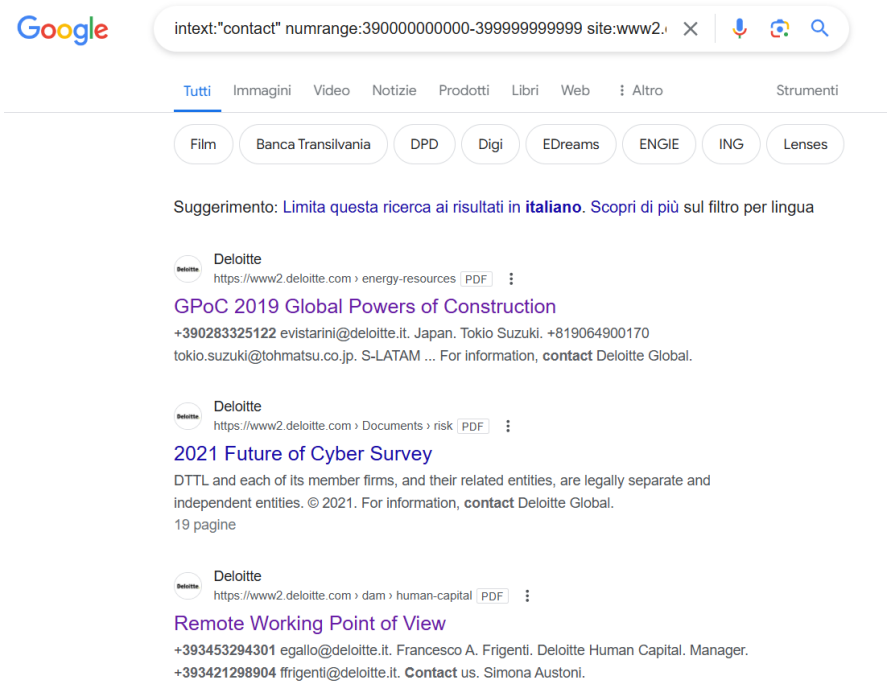


Con una query “inurl” ho trovato tutte le pagine contenti nell’URL il nome del sito, trovando ancora pagine delle divisioni di Deloitte nei vari Paesi e pagine legate ad argomenti specifici, come il placement.

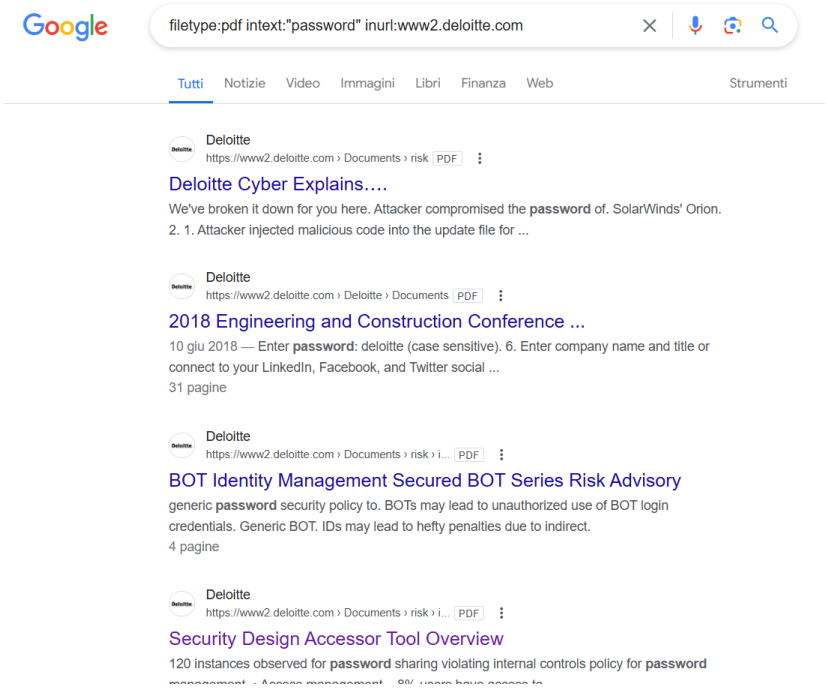
Successivamente, ho iniziato con le queries “intext” la ricerca di contenuti vulnerabili. Riporto solamente qualche screenshot di ricerche interessanti, mentre non riporto gli screenshot di ricerche con parole chiave come “mail” o “contact” che non hanno dato risultati particolari.

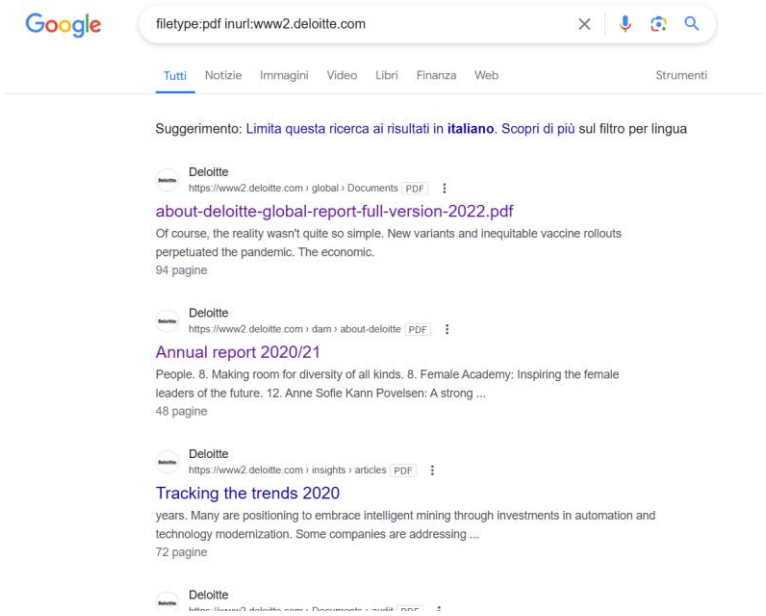


Combinando le queries ed utilizzando anche numrange, ho trovato moltissimi indirizzi e-mail e numeri di telefono di responsabili ed esperti collegati all’azienda, che potrebbero essere utilizzati per realizzare email di phishing o per sms di smishing.

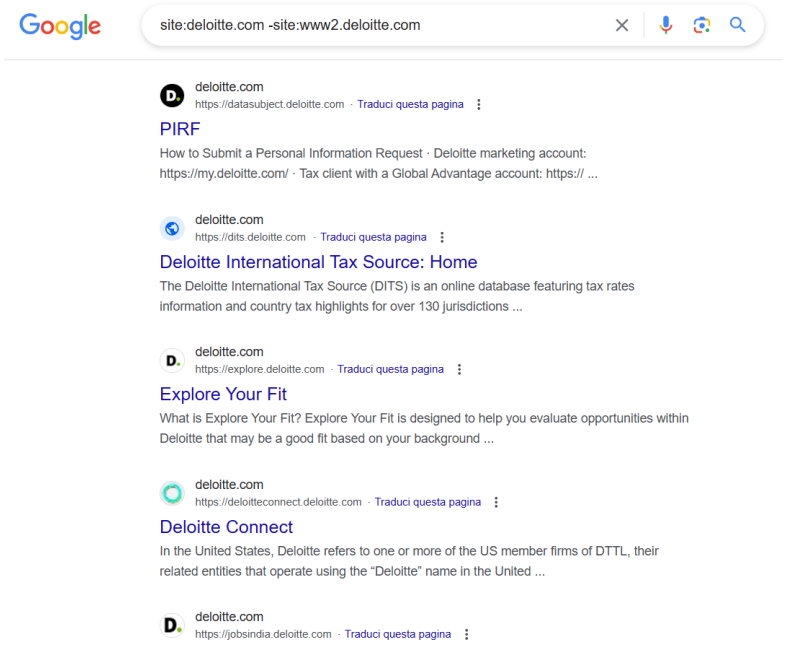


Con le queries "filetype" ho trovato soprattutto dei pdf, dato che l'azienda mette a disposizione dei pdf con i vari report e ricerche in tutti i settori di cui si occupa. Non si tratta di materiali sensibili o di vulnerabilità, ma sono presenti anche qui moltissimi numeri di telefono ed indirizzi e-mail anche di ricercatori ed esperti esterni all'azienda. Questi dati potrebbero essere usati per azioni di phishing e smishing.





Ho anche provato il site crawling, per trovare tutti i possibili sottodomini del dominio target.

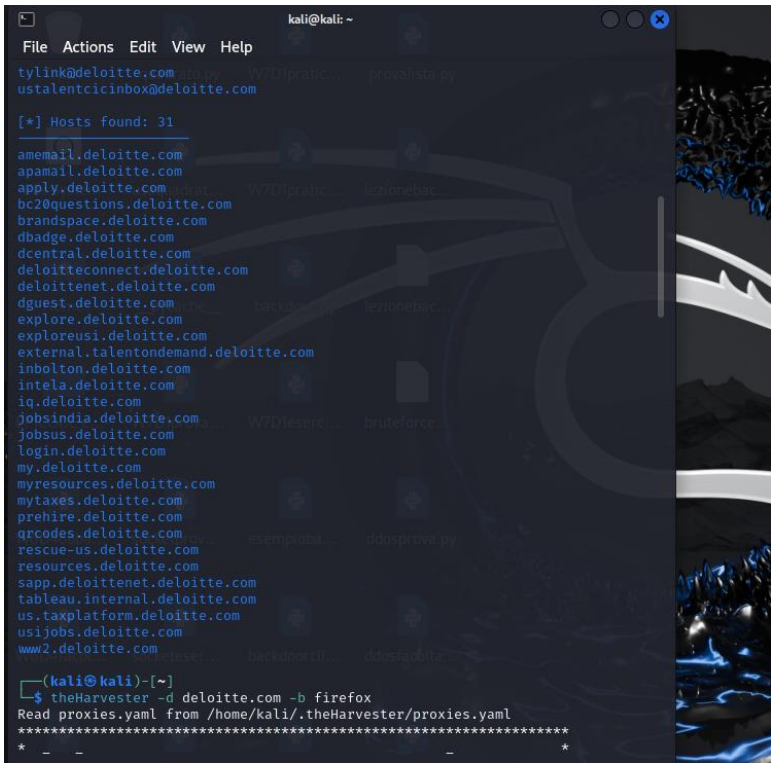


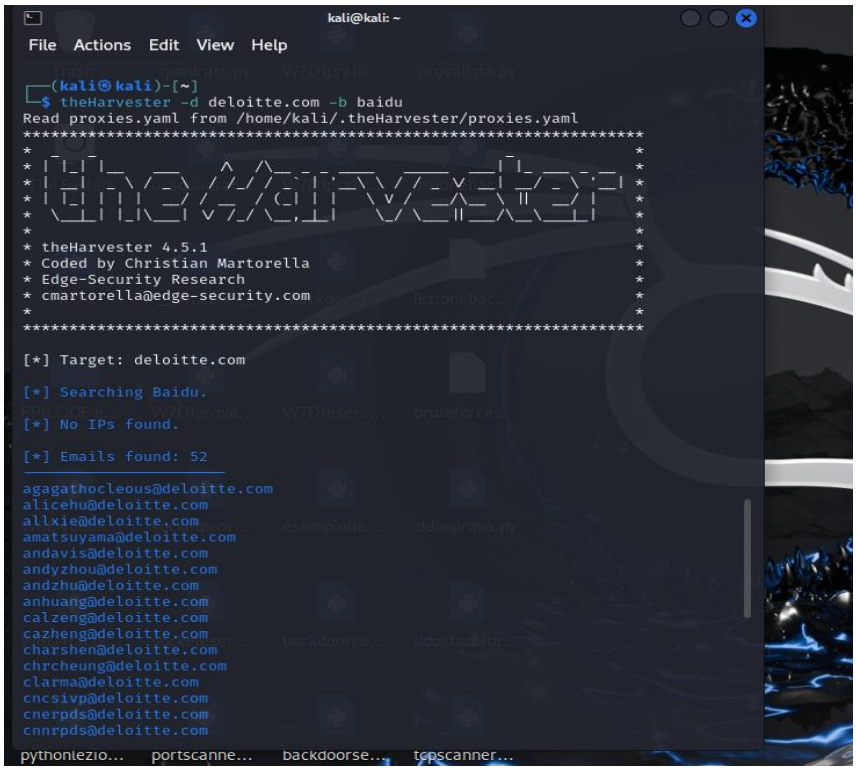
Tool per la raccolta di informazioni.

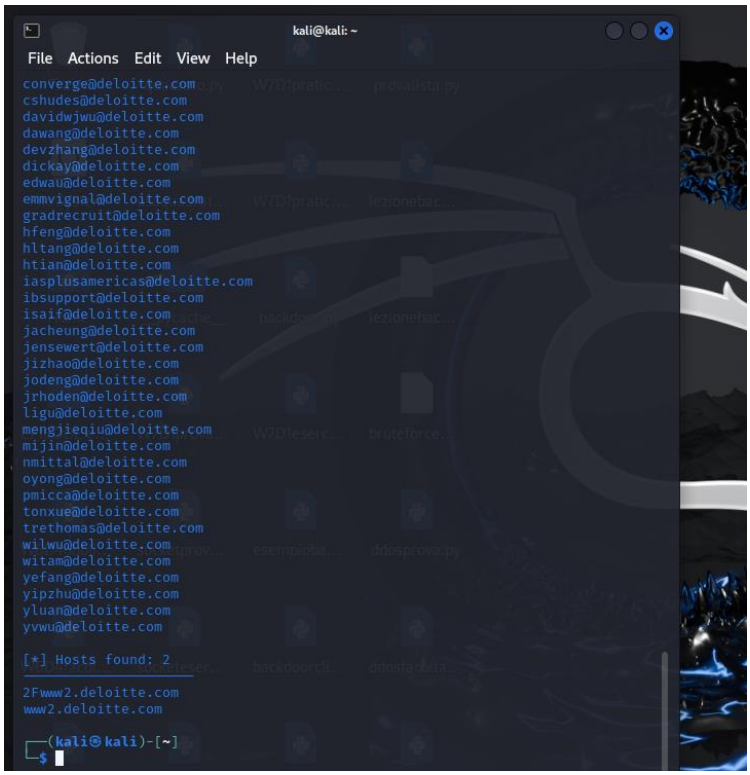
The Harvester

Ho utilizzato vari tool per la raccolta di informazioni, a paritre da the Harvester, per esaminare il sito target della mia ricerca, ovvero www2.deloitte.com. Per la ricerca ho mantenuto sempre come parametro -d il dominio deloitte.com, mentre come sorgente -b ho provato varie opzioni, ossia Yahoo, Bing e Baidu. La ricerca con Bing non ha dato risultati, mentre con Yahoo e Baidu ho trovato numerosi indirizzi e-mail ed hosts che possono essere target di azioni di phishing o di altri tipi di attacchi, magari contro web applications. Negli screenshot si vedono molti dei risultati che ho trovato.


(kali㉿kali)-[~]
$ theHarvester -d deloitte.com -b yahoo
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
* theHarvester 4.5.1
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: deloitte.com
[*] Searching Yahoo.
[*] No IPs found.
[*] Emails found: 22
agoodarzi@deloitte.com
cbrodzik@deloitte.com
dhelfrich@deloitte.com
ehardy@deloitte.com
ghdeloitte@deloitte.com
jamwatson@deloitte.com
jaybhatt@deloitte.com
jdoe@deloitte.com
kwmitchell@deloitte.com
labrash@deloitte.com
ldilorenzojr@deloitte.com
mmazzotta@deloitte.com
monoreilly@deloitte.com
ncooper@deloitte.com
nmerizzi@deloitte.com
nsloan@deloitte.com

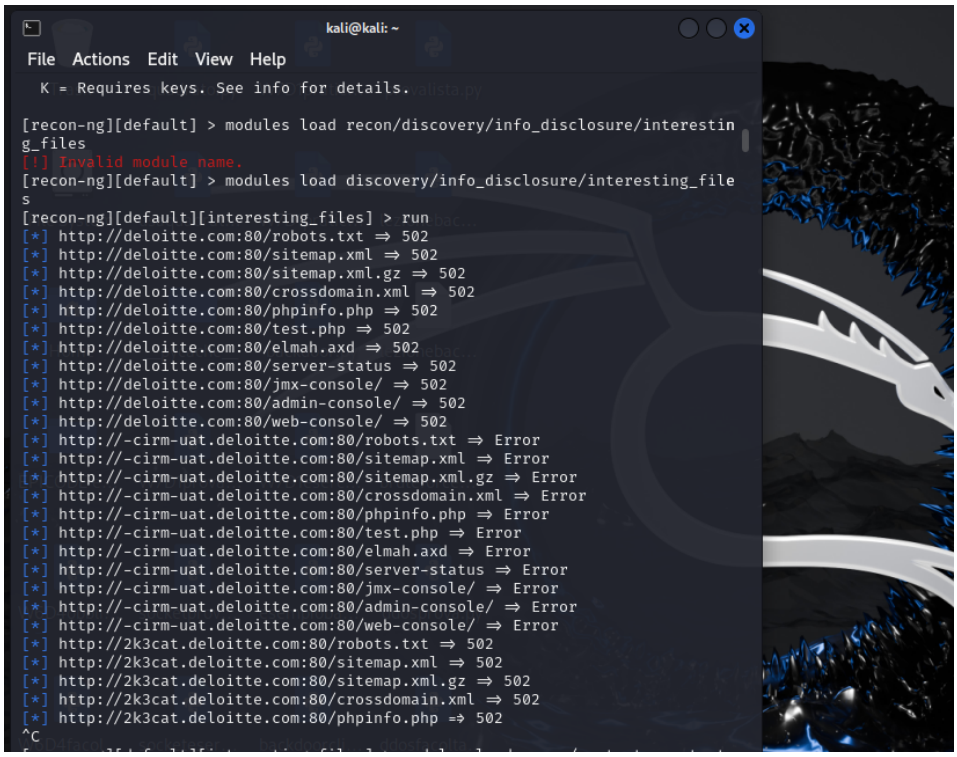

kali@kali: ~
File Actions Edit View Help
tylink@deloitte.com
ustalentcicinbox@deloitte.com
[*] Hosts found: 31
amemail.deloitte.com
apamail.deloitte.com
apply.deloitte.com
bc20questions.deloitte.com
brandspace.deloitte.com
dbadge.deloitte.com
dcentral.deloitte.com
deloitteconnect.deloitte.com
deloittenet.deloitte.com
dguest.deloitte.com
explore.deloitte.com
exploreusi.deloitte.com
external.talentondemand.deloitte.com
inbolton.deloitte.com
intela.deloitte.com
iq.deloitte.com
jobsindia.deloitte.com
jobsus.deloitte.com
login.deloitte.com
my.deloitte.com
myresources.deloitte.com
mytaxes.deloitte.com
prehire.deloitte.com
qrcodes.deloitte.com
rescue-us.deloitte.com
resources.deloitte.com
sapp.deloittenet.deloitte.com
tableau.internal.deloitte.com
us.taxplatform.deloitte.com
usijobs.deloitte.com
www2.deloitte.com
(kali㉿kali)-[~]
$ theHarvester -d deloitte.com -b firefox
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml





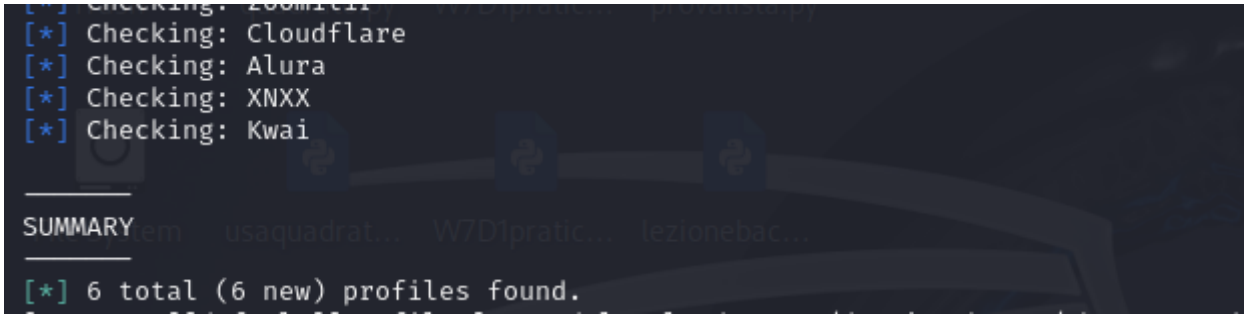
Recon-ng

Ho analizzato il sito target, ovvero www2.deloitte.com, anche con Recon-ng. Dopo averlo avviato, ho selezionato alcuni moduli utili per studiare il target. Con il modulo discovery/info_disclosure/interesting_files ho ricercato diversi file sensibili che potrebbero essere accessibili, anche se alcuni non erano accessibili direttamente.



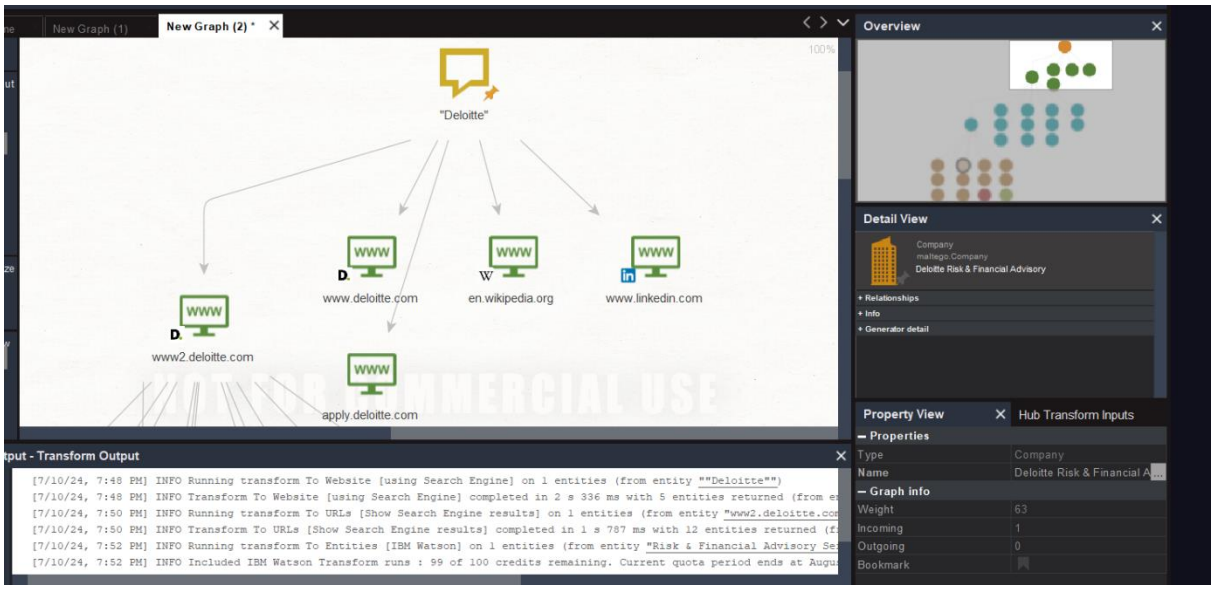
Il modulo recon/domains-hosts/hackertarget serve a trovare hostnames e sottodomini ed ho trovato in tutto 501 hosts con i loro indirizzi IP.

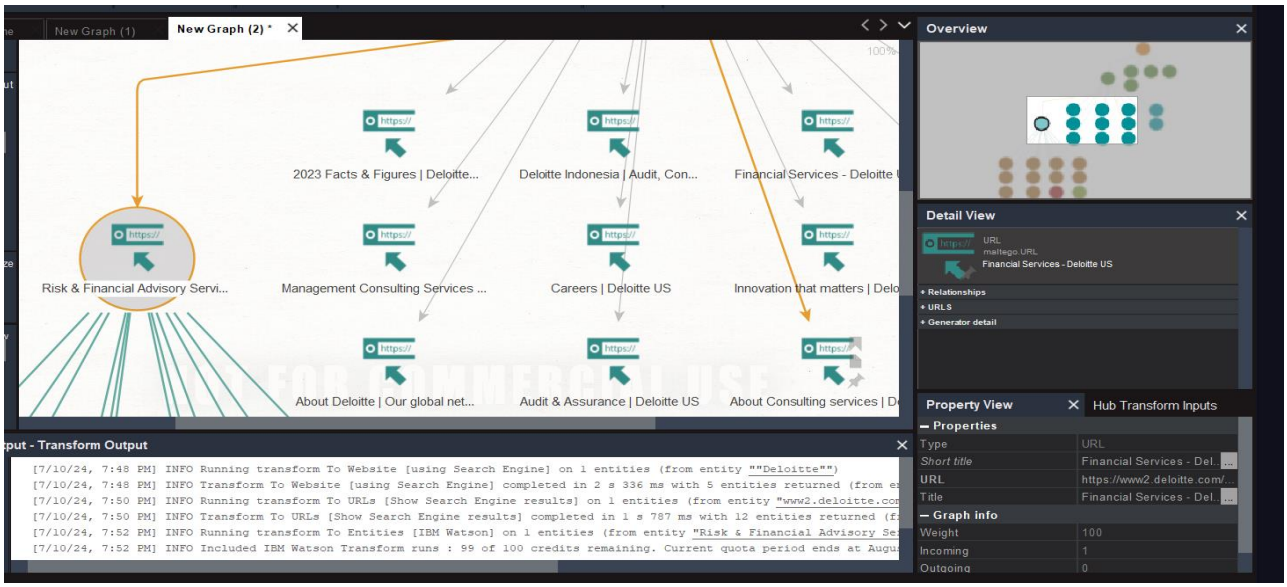
Ho infine provato il modulo recon/profiles-profiles/profiler per trovare degli username e la ricerca ha dato 6 risultati in tutto.

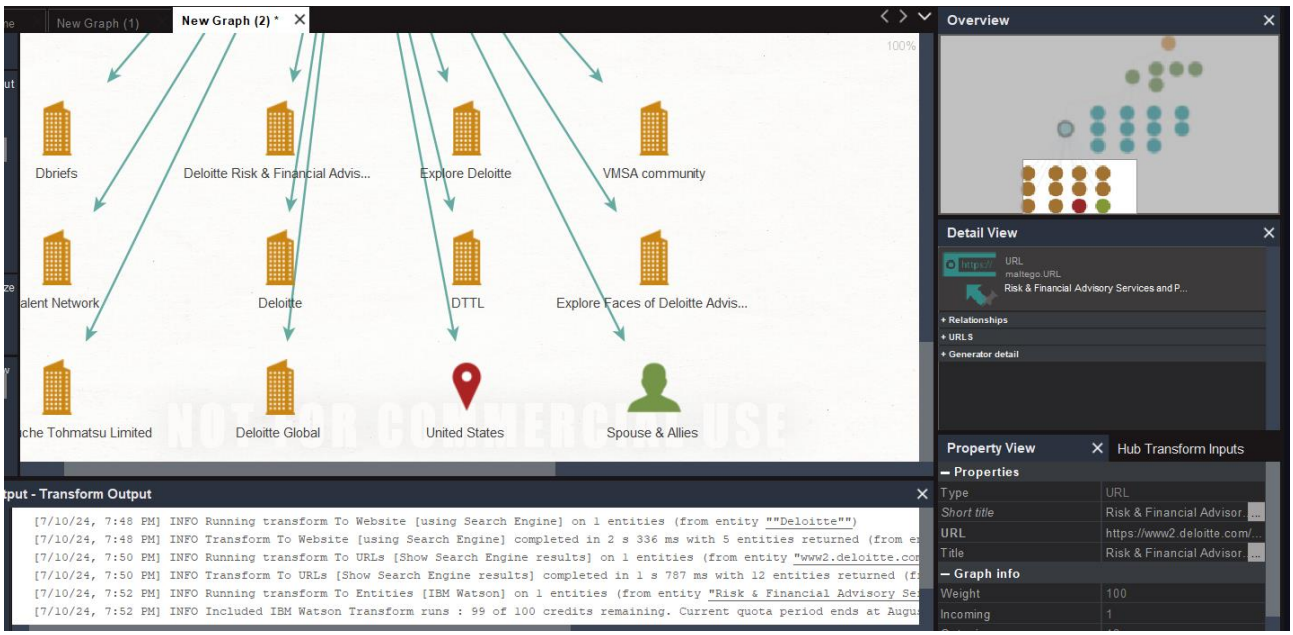


Maltego

Ho utilizzato anche Maltego per approfondire l'analisi del sito target. Per prima cosa sono partita dalla parola chiave "Deloitte" per eseguire una prima query "transforms to website using search engine" ed ho trovato dei siti collegati a "Deloitte", tra cui anche il target www2.deloitte.com ed altri siti ovviamente collegati a Deloitte. Approfondendo la ricerca a partire dal nodo del sito target, ho eseguito una query URLs (show search engine results), trovando numerosi siti di sedi di Deloitte nel mondo, siti relativi a tematiche specifiche di cui si occupa l'azienda e siti con offerte di lavoro. Per continuare la ricerca, ho scelto il nodo relativo all'analisi di rischi ed ho eseguito una query "entities" (IBM Watson), trovando dei contatti ed informazioni di persone e settori del nodo superiore, utili per approfondire la raccolta di informazioni e cercare altri contatti ed informazioni per pensare ad azioni malevole di phishing. Gli screenshot successivi riportano i tre livelli di ricerca che ho svolto.


New Graph (1)
New Graph (2) *
"Deloitte"
www.deloitte.com
en.wikipedia.org
www.linkedin.com
www2.deloitte.com
apply.deloitte.com
Overview
Detail View
Company
maltego.Company
Deloitte Risk & Financial Advisory
+ Relationships
+ Info
+ Generator detail
Property View
Hub Transform Inputs
Properties
Type
Company
Name
Deloitte Risk & Financial A...
Graph info
Weight
63
Incoming
1
Outgoing
0
Bookmark
Transform Output
[7/10/24, 7:48 PM] INFO Running transform To Website [using Search Engine] on 1 entities (from entity ""Deloitte"")
[7/10/24, 7:48 PM] INFO Transform To Website [using Search Engine] completed in 2 s 336 ms with 5 entities returned (from e
[7/10/24, 7:50 PM] INFO Running transform To URLs [Show Search Engine results] on 1 entities (from entity "www2.deloitte.com
[7/10/24, 7:50 PM] INFO Transform To URLs [Show Search Engine results] completed in 1 s 787 ms with 12 entities returned (f
[7/10/24, 7:52 PM] INFO Running transform To Entities [IBM Watson] on 1 entities (from entity "Risk & Financial Advisory Se
[7/10/24, 7:52 PM] INFO Included IBM Watson Transform runs : 99 of 100 credits remaining. Current quota period ends at Augu


New Graph (1)
New Graph (2) *
2023 Facts & Figures | Deloitte...
Deloitte Indonesia | Audit, Con...
Financial Services - Deloitte U
Risk & Financial Advisory Servi...
Management Consulting Services ...
Careers | Deloitte US
Innovation that matters | Delo
About Deloitte | Our global net...
Audit & Assurance | Deloitte US
About Consulting services | D
Overview
Detail View
URL
maltego.URL
Financial Services - Deloitte US
+ Relationships
+ URLS
+ Generator detail
Property View
Hub Transform Inputs
Properties
Type
URL
Short title
Financial Services - Del...
URL
https://www2.deloitte.com/...
Title
Financial Services - Del...
Graph info
Weight
100
Incoming
1
Outgoing
0
Transform Output
[7/10/24, 7:48 PM] INFO Running transform To Website [using Search Engine] on 1 entities (from entity ""Deloitte"")
[7/10/24, 7:48 PM] INFO Transform To Website [using Search Engine] completed in 2 s 336 ms with 5 entities returned (from e
[7/10/24, 7:50 PM] INFO Running transform To URLs [Show Search Engine results] on 1 entities (from entity "www2.deloitte.com
[7/10/24, 7:50 PM] INFO Transform To URLs [Show Search Engine results] completed in 1 s 787 ms with 12 entities returned (f
[7/10/24, 7:52 PM] INFO Running transform To Entities [IBM Watson] on 1 entities (from entity "Risk & Financial Advisory Se
[7/10/24, 7:52 PM] INFO Included IBM Watson Transform runs : 99 of 100 credits remaining. Current quota period ends at Augu


New Graph (1)
New Graph (2) *
Dbriefs
Deloitte Risk & Financial Advis...
Explore Deloitte
VMSA community
alent Network
Deloitte
DTTL
Explore Faces of Deloitte Advis...
che Tohmatsu Limited
Deloitte Global
United States
Spouse & Allies
Overview
Detail View
URL
maltego.URL
Risk & Financial Advisory Services and P...
+ Relationships
+ URLS
+ Generator detail
Property View
Hub Transform Inputs
Properties
Type
URL
Short title
Risk & Financial Advisor...
URL
https://www2.deloitte.com/...
Title
Risk & Financial Advisor...
Graph info
Weight
100
Incoming
1
Transform Output
[7/10/24, 7:48 PM] INFO Running transform To Website [using Search Engine] on 1 entities (from entity ""Deloitte"")
[7/10/24, 7:48 PM] INFO Transform To Website [using Search Engine] completed in 2 s 336 ms with 5 entities returned (from e
[7/10/24, 7:50 PM] INFO Running transform To URLs [Show Search Engine results] on 1 entities (from entity "www2.deloitte.com
[7/10/24, 7:50 PM] INFO Transform To URLs [Show Search Engine results] completed in 1 s 787 ms with 12 entities returned (f
[7/10/24, 7:52 PM] INFO Running transform To Entities [IBM Watson] on 1 entities (from entity "Risk & Financial Advisory Se
[7/10/24, 7:52 PM] INFO Included IBM Watson Transform runs : 99 of 100 credits remaining. Current quota period ends at Augu

Network Query Tool

Per la ricerca ho usato anche Network Query Tool, rintracciando l'IP del sito www2.deloitte.com, ossia 23.20183.17, i range di IP delle reti e trovando anche informazioni riguardo ai server e all'uso di tecnologie di Akamai Technologies.

Valutazione della sicurezza del sito a partire dalle informazioni trovate.

Queste ricerche hanno evidenziato che il livello di sicurezza del sito è alto e che sono già state prese delle misure per garantire la sicurezza del sito. Nonostante questo, sono comunque esposte varie informazioni sensibili, soprattutto contatti telefonici ed e-mail non solo di uffici e responsabili, ma anche di soggetti terzi collegati all'azienda, per esempio esperti esterni e ricercatori che hanno realizzato i report in pdf facilmente rintracciabili sul web. Per questo motivo, è fondamentale mettere in guardia non solo i responsabili e i dipendenti della ditta, ma anche i soggetti terzi collegati alle attività di ricerca e consulenza. Sono inoltre presenti anche hostnames, sottodomini ed IP che possono essere ulteriormente studiati per trovare delle vulnerabilità note, conoscendo per esempio le informazioni sui server e sulle tecnologie di Akamai Technologies. Per questo motivo, nonostante il sito dimostri di avere un buon livello di sicurezza, è necessario continuare ad impegnarsi per proteggere quegli IP e quelle tecnologie esposte sulla rete e rintracciabili con i tool, rimediando alle vulnerabilità già note e che si possono trovare. È inoltre importante investire sulla formazione del personale, fino ai livelli più alti, per renderli vigili ed insegnare a riconoscere possibili email di phishing ed sms di smishing. È necessario che anche esperti, consulenti e ricercatori esterni siano messi in guardia per riconoscere email ed sms malevoli, per evitare che diventino l'anello debole della sicurezza di un sito che ha già un buon livello di sicurezza.