





Raccolta Informazioni

Con questo esercizio di oggi, andremo a fare una raccolta dati di un target definito, nel mio caso Huawei. Come prima cosa andiamo a fare una ricerca passiva tramite Google scrivendo nella barra di ricerca “index.of inurl:Huawei”, così da poter vedere tutte le directory del sito:

Index of /huawei

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 classroommanagement(PC)/	2021-05-17 14:39	-	
 classroommanagement/	2021-05-17 14:31	-	
 languagelab/	2021-05-17 14:41	-	

Fatto ciò, con il tool recon-ng, andremo ad inserire un modulo per stampare a schermo le email degli impiegati:

```
[*] URL: http://whois.arin.net/rest/pocs;domain=consumer.huawei.com
[*] No contacts found.
[recon-ng][default][whois_pocs] > options set SOURCE huawei.com
SOURCE ⇒ huawei.com
[recon-ng][default][whois_pocs] > run

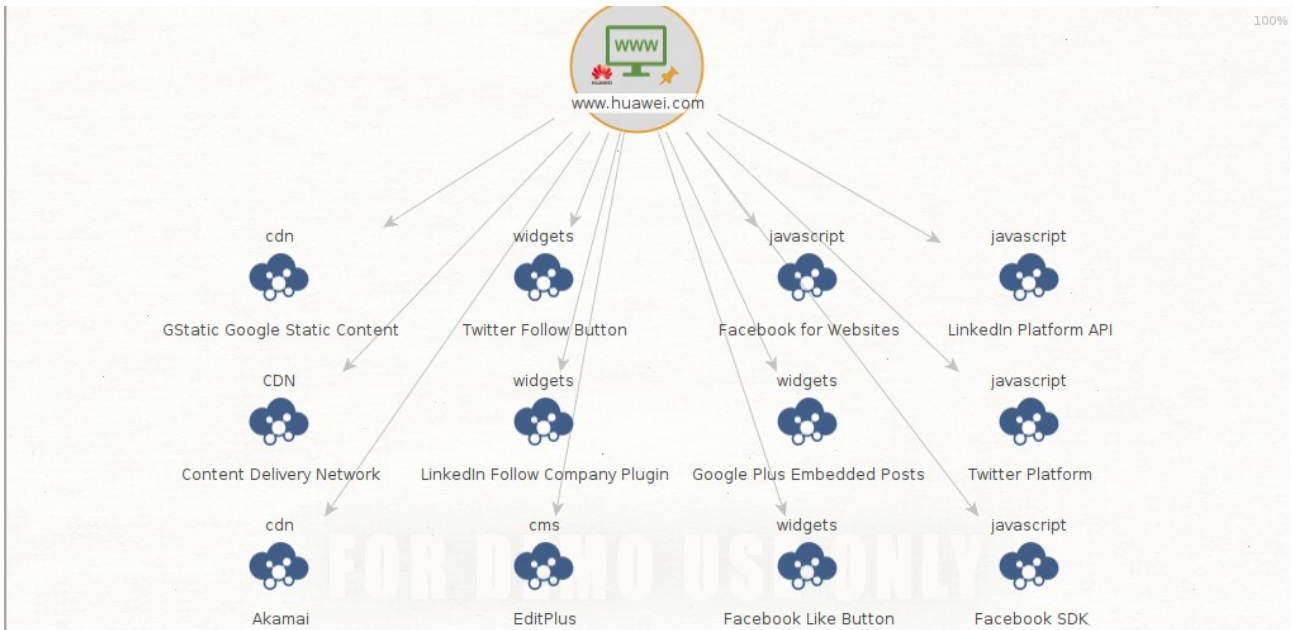
_____
HUAWEI.COM
```

```
[recon-ng][default][whois_pocs] > options set SOURCE huawei.com
SOURCE ⇒ huawei.com
[recon-ng][default][whois_pocs] > run
```

HUAWEI.COM

```
[*] URL: http://whois.arin.net/rest/pocs;domain=huawei.com
[*] URL: http://whois.arin.net/rest/poc/BUTLE74-ARIN
[*] Country: Jamaica
[*] Email: carey.butler@huawei.com
[*] First_Name: Carey
[*] Last_Name: Butler
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Kingston
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/BUTLE140-ARIN
[*] Country: Jamaica
[*] Email: Carey.Butler@huawei.com
[*] First_Name: Carey
[*] Last_Name: Butler
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Kingston
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/GFA28-ARIN
[*] Country: United States
[*] Email: gfang@huawei.com
[*] First_Name: Gordon
[*] Last_Name: Fang
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Plano, TX
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/WANGG15-ARIN
[*] Country: United States
[*] Email: guangkuo.wang@huawei.com
[*] First_Name: guangkuo
[*] Last_Name: wang
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: S Clara, CA
[*] Title: Whois contact
[*]
```

Ora non ci manca altro che usare Maltego per ottenere altri dati, per farlo apriamo una pagina vuota su maltego ed aggiungiamo un WebSite, andando a mettere l'url di Huawei:



ut - Transform Output

Running transform To Web Technologies [BuiltWith] on 1 entities (from entity "www.huawei.com")
Included BuiltWith Transform runs: 98 of 100 credits remaining. Current quota period ends at 2022-12-21T14:22:07.569Z[UTC] (from entity "www.hu")
Transform To Web Technologies [BuiltWith] returned with 12 entities (from entity "www.huawei.com")
Transform To Web Technologies [BuiltWith] done (from entity "www.huawei.com")