



# Reconnaissance Passive

Rapport TP1

---

Par :

- ALIM Yanis
- DHIA Layadi

## Périmètre

[Promasidor](#): est une société multi-locale de produits alimentaires et de boissons qui ravitaille plus de 850 millions de personnes. Motivée, dynamique et progressiste, Promasidor est un exemple vibrant de ce qu'on peut accomplir sur ce grand continent.

## Notre but

On est censé récolter le maximum d'informations sur notre cible sans avoir un contact direct ( reconnaissance active ) avec la cible, en utilisant juste des données accessible publiquement.

## Méthodologie à suivre

**Détection des adresses IP et des sous-domaines** - généralement l'une des premières étapes de la reconnaissance passive, il est important d'identifier les plages et les sous-domaines nets associés à votre ou vos cibles, car cela vous aidera à cibler le reste de vos activités.

**Identification des sites externes/tiers** - bien qu'ils ne fassent pas partie des activités de tests d'intrusion actifs, il est important de comprendre les relations entre votre cible et les autres fournisseurs de contenu tiers.

**Identification des personnes** - L'identification de noms, adresses e-mail, numéros de téléphone et autres informations personnelles peut être utile pour les activités de simulation, d'hameçonnage ou autres activités d'ingénierie sociale.




**Identification des technologies** - L'identification des types et des versions des systèmes et des applications logicielles utilisés par une organisation est un précurseur important de l'identification des vulnérabilités potentielles.

**Identification du contenu d'intérêt** - L'identification des portails Web et de messagerie, des fichiers journaux, des fichiers de sauvegarde ou archivés, ou des informations sensibles contenues dans des commentaires HTML ou des scripts côté client est essentielle pour la découverte de vulnérabilités et les futures activités de tests d'intrusion.

## Détection des adresses IP et des sous-domaines

**Whois** lookup est utilisé pour déterminer où le site est hébergé, à qui appartient le bloc IP, s'il existe des contacts organisationnels répertoriés qui pourraient être utiles pour un exercice d'ingénierie sociale (en supposant que ce soit dans le cadre de votre test sanctionné), etc.

<http://whois.domaintools.com/promasidor.com>

Whois Record for PromasIdOr.com	
— Domain Profile	
Registrant Org	PromasIdOr IP Holdings, Limited
Registrant Country	mx
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: <a href="http://www.godaddy.com">http://www.godaddy.com</a> Whois Server: <a href="http://whois.godaddy.com">whois.godaddy.com</a> <a href="mailto:abuse@godaddy.com">abuse@godaddy.com</a> (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	6,322 days old Created on: 2002-06-11 Expires on: 2021-06-11 Updated on: 2019-01-06
Name Servers	NS 10.DNSMADEEASY.COM (has 35,12,77 domains) NS 11.DNSMADEEASY.COM (has 35,12,77 domains) NS 12.DNSMADEEASY.COM (has 35,12,77 domains) NS 13.DNSMADEEASY.COM (has 35,12,77 domains) NS 14.DNSMADEEASY.COM (has 35,12,77 domains)
Tech Contact	—
IP Address	40.69.56.10 - 27 other sites hosted on this server
IP Location	 Dublin - Dublin - Microsoft Corporation
ASN	 AS8075 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US (registered Mar 31, 1997)
Domain Status	Registered And Active Website
IP History	7 changes on 7 unique IP addresses over 14 years
Registrar History	5 registrars
Hosting History	3 changes on 4 unique name servers over 17 years
— Website	
Website Title	 PromasIdOr
Response Code	200
Terms	263 (Unique: 166, Linked: 22)
Images	19 (All tags missing: 19)
Links	36 (Internal: 30, Outbound: 4)

On trouve bien la plage d'adresse IP, la localisation de leur serveurs, nom des serveurs dns et d'autre informations utiles.

**Pentest-tools.com** est très pratique pour faire une énumération des sous-domaine en mode passive.

<https://pentest-tools.com/information-gathering/find-subdomains-of-domain#>

pentest-tools.com/information-gathering/find-subdomains-of-domain#

et to Rop NOYAU (Mast... Olivier Fou... How to Forc... GTF0Bins Locations i... 0xswitch

2 Free Scans TOOLS FEATURES PRICING SERVICES CUSTOMERS BLOG

DOWNLOAD REPORT

promasidor.com

Found 6 subdomains

Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title	Actions
promasidor.com	40.69.56.10	Windows	Microsoft-IIS	ASP.NET		Promasidor	Scan with
autodiscover.promasidor.com	40.101.12.56					Sign in to Outlook	Scan with
sip.promasidor.com	52.112.64.11		RTC 7.0				Scan with
intranet.promasidor.com	96.45.82.45		DNSME HTTP Redirection			Promasidor Intranet	Scan with
ftp.promasidor.com	196.31.27.150						Scan with
www.promasidor.com	208.80.127.4						Scan with

intoDNS.com est efficace pour trouver les zone de transfert DNS.

<https://intodns.com/promasidor.com>

intodns.com/promasidor.com

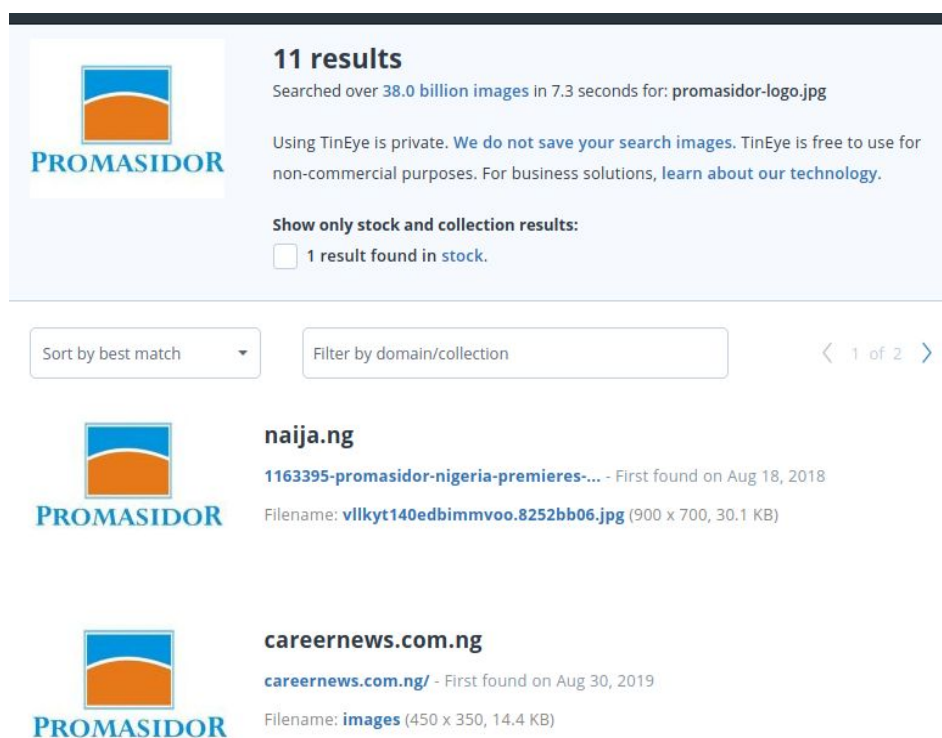
Ret to Rop NOYAU (Mast... Olivier Fou... How to Forc... GTF0Bins Locations i... 0xswitch

Category	Status	Test name	Information
Parent	i	Domain NS records	Nameserver records returned by the parent servers are: ns10.dnsmadeeasy.com. [208.94.148.4] [TTL=172800] ns11.dnsmadeeasy.com. [208.80.124.4] [TTL=172800] ns12.dnsmadeeasy.com. [208.80.126.4] [TTL=172800] ns13.dnsmadeeasy.com. [208.80.125.4] [TTL=172800] ns14.dnsmadeeasy.com. [208.80.127.4] [TTL=172800] j.gtld-servers.net was kind enough to give us that information.
	✓	TLD Parent Check	Good. j.gtld-servers.net, the parent server I interrogated, has information for your TLD. This is a good thing as there are some other domain extensions like "co.us" for example that are missing a direct check.
	✓	Your nameservers are listed	Good. The parent server j.gtld-servers.net has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.
	✓	DNS Parent sent Glue	Good. The parent nameserver sent GLUE, meaning he sent your nameservers as well as the IPs of your nameservers. Glue records are A records that are associated with NS records to provide "bootstrapping" information to the nameserver.(see RFC 1912 section 2.3)
	✓	Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.
NS	i	NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: ns12.dnsmadeeasy.com [208.80.126.4] [TTL=86400] ns11.dnsmadeeasy.com [208.80.124.4] [TTL=86400] ns15.dnsmadeeasy.com [208.94.149.4] [TTL=86400] ns10.dnsmadeeasy.com [208.94.148.4] [TTL=86400] ns14.dnsmadeeasy.com [208.80.127.4] [TTL=86400] ns13.dnsmadeeasy.com [208.80.125.4] [TTL=86400]
	✓	Recursive Queries	Good. Your nameservers (the ones reported by the parent server) do not report that they allow recursive queries for anyone.
	✓	Same Glue	The A records (the GLUE) got from the parent zone check are the same as the ones got from your nameservers. You have to make sure your parent server has the same NS records for your zone as you do according to the RFC. This tests only nameservers that are common at the parent and at your

## Identification des sites externes/tiers

Identifier des sites externes liés peut être utile car ils impliquent souvent des transferts de données bidirectionnels présentant un intérêt.

**TinyEye.com:** un moyen d'identifier les sites associés consiste à utiliser un outil de correspondance d'images tel que TinEye. Ici, j'ai récupéré le logo de la General Services Administration sur son site Web et, en utilisant TinEye, j'ai identifié d'autres sites faisant référence à une image identique ou similaire. Cela peut permettre d'identifier des relations d'intérêt organisationnelles directes ou indirectes en fonction de la portée de votre évaluation.



The screenshot shows the TinEye search interface. At the top, it displays the search results for the Promasidor logo. The search was performed over 38.0 billion images in 7.3 seconds. The results show 11 matches. Below the search results, there are two filters: 'Sort by best match' and 'Filter by domain/collection'. The first result is from naija.ng, showing the Promasidor logo and the filename 'vllkyt140edbimmvoo.8252bb06.jpg' (900 x 700, 30.1 KB). The second result is from careernews.com.ng, showing the Promasidor logo and the filename 'images' (450 x 350, 14.4 KB).

**11 results**  
Searched over 38.0 billion images in 7.3 seconds for: promasidor-logo.jpg

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, [learn about our technology](#).

Show only stock and collection results:  
☐ 1 result found in stock.

Sort by best match ▼ Filter by domain/collection < 1 of 2 >

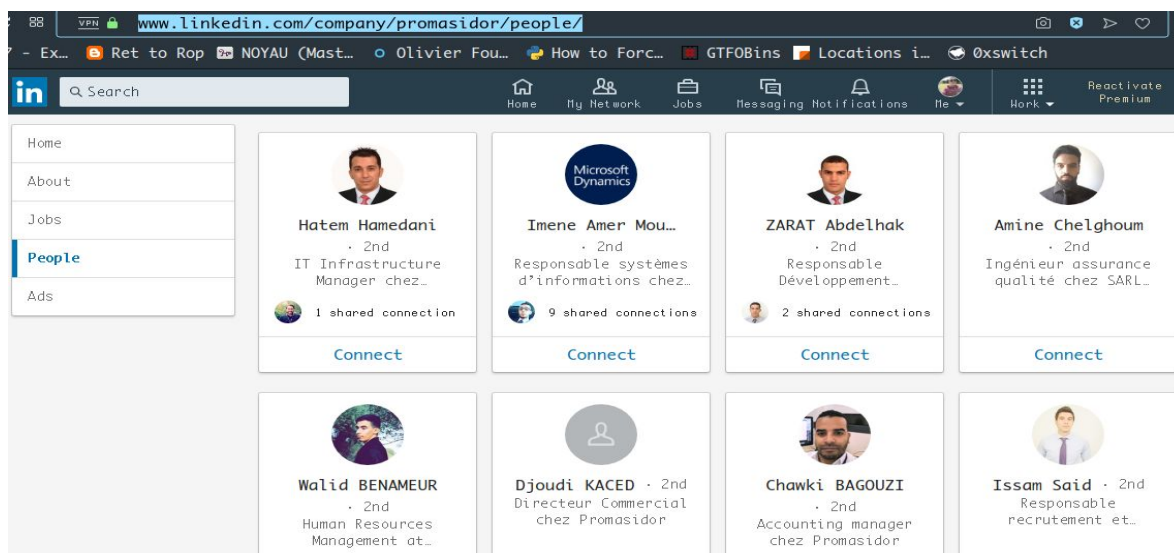
**naija.ng**  
1163395-promasidor-nigeria-premieres-... - First found on Aug 18, 2018  
Filename: [vllkyt140edbimmvoo.8252bb06.jpg](#) (900 x 700, 30.1 KB)

**careernews.com.ng**  
[careernews.com.ng/](#) - First found on Aug 30, 2019  
Filename: [images](#) (450 x 350, 14.4 KB)

## Identification des personnes

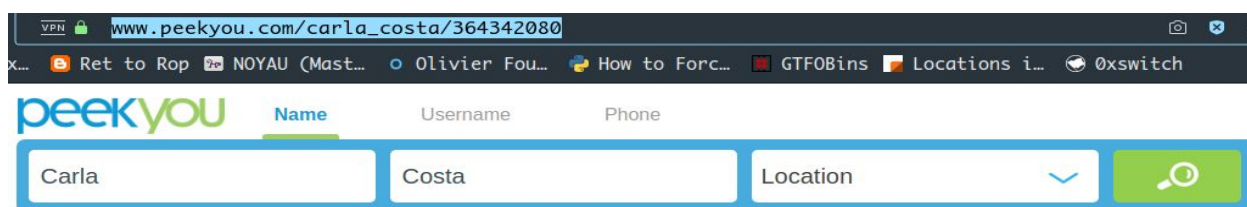
Une autre tâche importante de la reconnaissance passive consiste à identifier les personnes liées à votre organisation cible (employés, tiers contractuels, etc.) qui pourraient s'avérer utiles pour une activité d'ingénierie sociale ultérieure.

**Social Media:** C'est toujours bien de se baser sur LinkedIn pour avoir l'ensemble des employés



Puis à l'aide d'autres Social Media Website (Facebook, Twitter....), on peut trouver des informations de valeur sur le personnel choisi

**PeekYou.com:** c'est un moyen efficace pour collecter des informations sur des personnes et de donner accès à des numéros de téléphone, adresses e-mail, adresses (passées et présentes) et même des informations sur l'arbre généalogique (certains services ne sont payants).





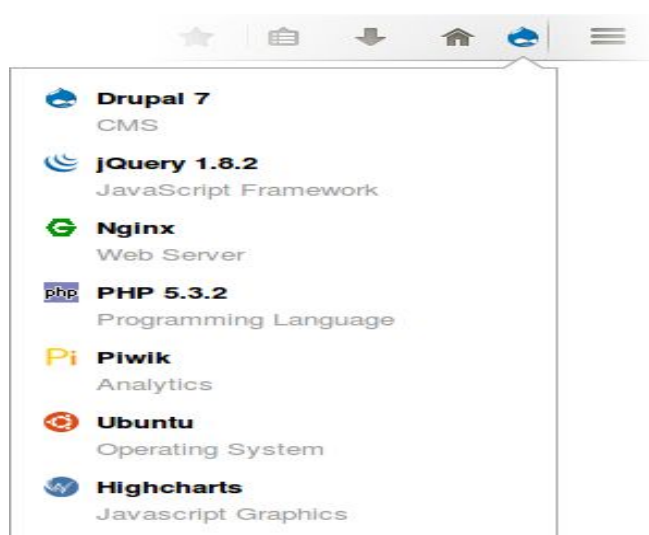
## Identification des technologies

Identifier les technologies utilisées par une organisation est fondamental pour détecter les vulnérabilités potentielles. Le fait de savoir qu'une organisation exécute un système d'exploitation ou une application logicielle obsolète ou non pris en charge peut suffire à développer un exploit et à s'implanter sur le réseau.

Vous pouvez identifier des technologies provenant de nombreuses sources, notamment:

- Extensions de fichiers
- Réponses du serveur
- Offres d'emploi
- Répertoire
- Login pages de démarrage
- Contenu du site Web
- Records d'acquisition publique
- Shodan
- Recherches de documents

**Wappalyzer** : est un plugin de navigateur très utile qui vous informe instantanément sur les technologies utilisées sur un site au fur et à mesure de votre navigation.



**Shodan.io:** peut être utilisé pour découvrir beaucoup plus de technologies et d'exploits connexes.

The screenshot shows the Shodan.io interface for the host 40.69.56.10. The left sidebar displays host details:

City	Dublin
Country	Ireland
Organization	Microsoft Azure
ISP	Microsoft Corporation
Last Update	2019-09-26T10:25:24.038894
ASN	AS8075

The right sidebar shows the 'Ports' and 'Services' sections. The 'Ports' section lists two open ports: 80 and 3389. The 'Services' section provides details for these ports:

- Port 80:** HTTP/1.1 404 Not Found. Cache-Control: private. Content-Type: text/html. Date: Thu, 26 Sep 2019 10:25:23 GMT. Content-Length: 1245.
- Port 3389:** Remote Desktop Protocol. The service is identified as rdp.

## Identification du contenu d'intérêt

Le contenu du site peut révéler des points d'accès potentiels (par exemple, des portails Web), des données sensibles (identifiants de connexion), etc. Lorsque vous naviguez sur le site, soyez attentif aux points suivants:

- Portails Web, messagerie Web et consoles d'administration tournés vers l'extérieur
- Pages de test
- Fichiers de log
- Fichiers de sauvegarde
- Fichiers de configuration
- Fichiers de vidage de la base de données
- Code côté client

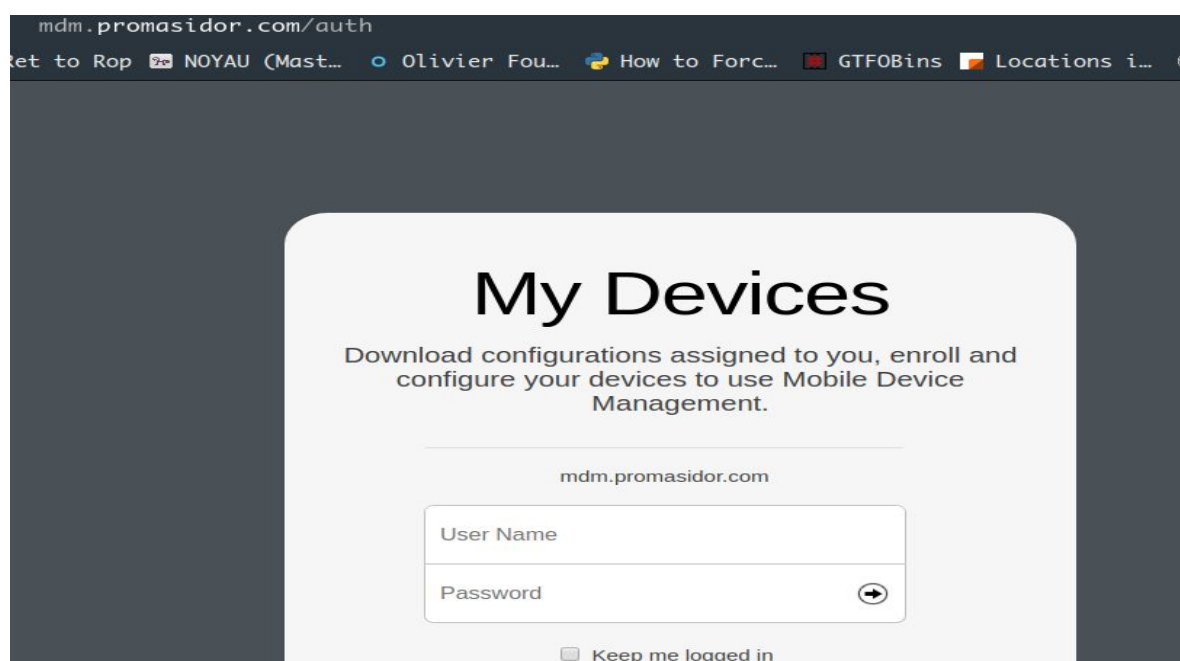
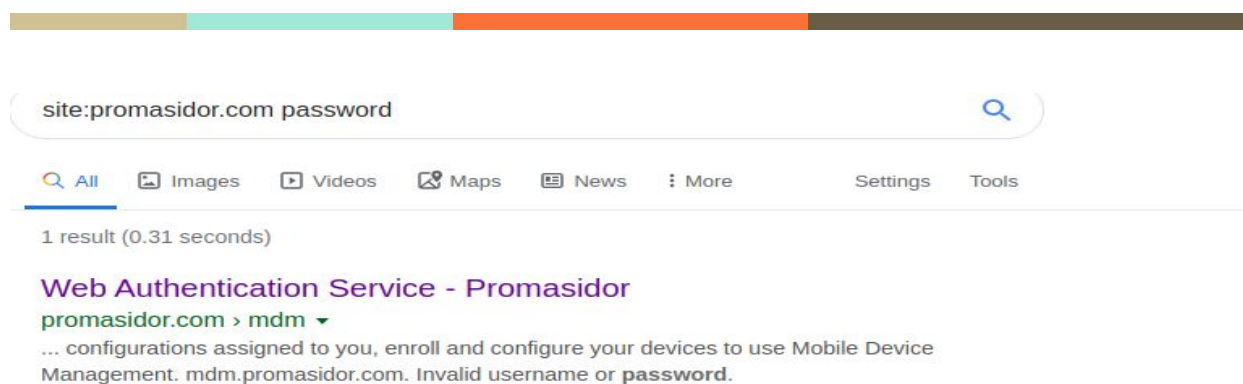
### Google dorks:

- `site: <target_site> intitle:portal employee`
- `site: <target_site> intitle:webmail`
- `site: <target_site> "outlook web access"`
- `site: <target_site> inurl:phpmyadmin`

En utilisant la requête : **site:promasidor.com password**

J'ai trouvé un nouveau sous-domaine !





Comme d'hab, **admin:admin** sont les bons. On peut contrôler à distance les périphériques connectés au serveur...