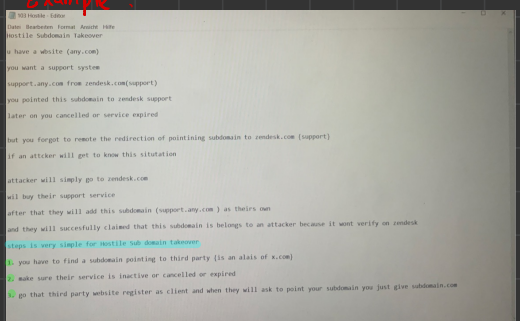
Hostile Subdomain Takeover

Attack Scenario

- Your company starts using a new service, eg an external Support Ticketing-service.
- Your company points a subdomain to the Support Ticketing-service, eg support.your-domain.com
- Your company stops using this service but does not remove the subdomain redirection pointing to the ticketing system.
- Attacker signs up for the Service and claims the domain as theirs. No verification is done by the Service Provider, and the DNS-setup is already correctly setup.
- Attacker can now build a complete clone of the real site, add a login form, redirect the user, steal credentials (e.g. admin accounts), cookies and/or completely destroy business credibility for your company.

3 / 6

Example :



Three things that make this scenario dangerous

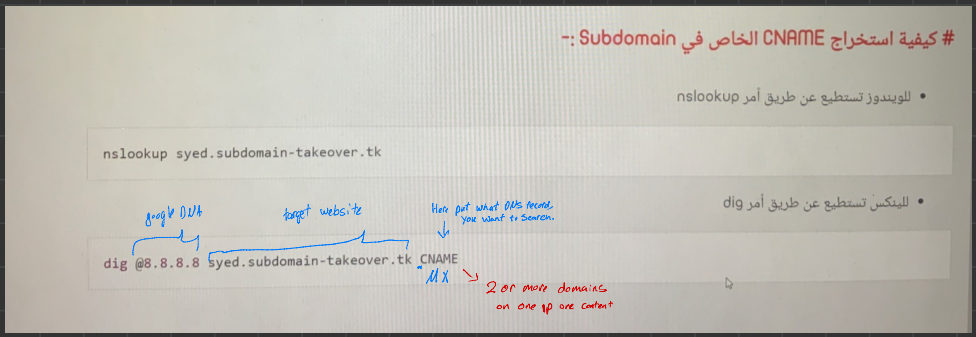
- It's SUPER easy. Sign up for a new account and claim the domain. Done.
- It's completely hidden. The Domain Owner won't notice. The attacker won't leave any traces for the Domain Owner. Good luck monitoring this in an IDS!
- The Service Provider is unlikely to be able to fix this in a feasible way.

Now if this wasn't bad enough, imagine this scenario

- A Domain Owner points their * (wildcard) DNS-entry to e.g. Heroku.
- They forget to add the wildcard-entry to their Heroku-app.
- Attacker can now claim any subdomain they want from the Domain Owner.
- A Domain Owner will be unaware of the subdomain being exploited.

* How to hunt

- Download HostileSubBruteforcer from github
- follow steps above



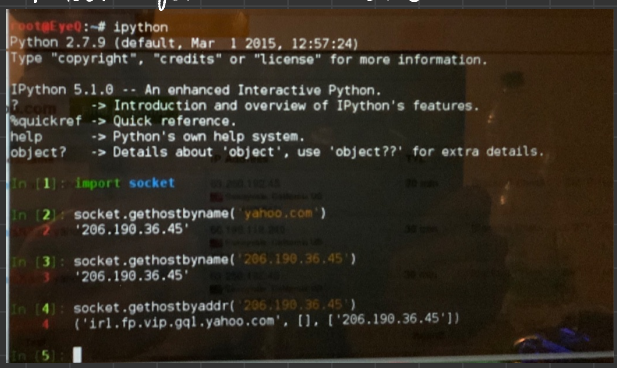
العلاج

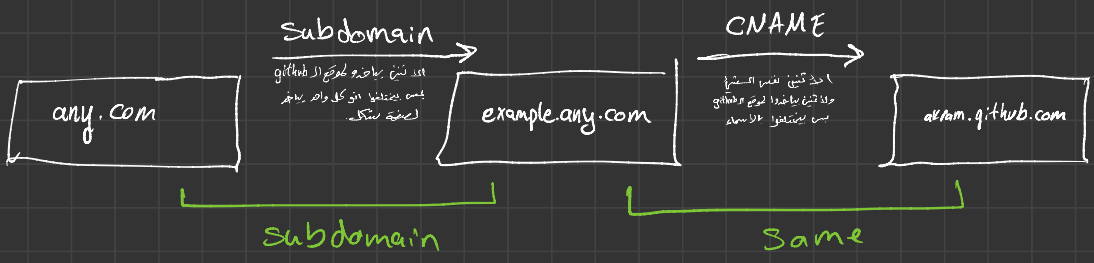
* خاص من سجلات DNS CNAME التي مستخدمة أو منتهية الصلاحية أو الخاطئة.

* Mxtoolbox is a site to check

Note
#> ipython is better than #> python

* tool to get alias website





Description

- One of the subdomains of the scanned domain is pointing to an external service but the external service account was cancelled or has expired. Because the account is not in use anymore, an attacker can claim this account and takeover your subdomain. The attacker can use this subdomain for phishing or to spread malware.

Steps to Hunt Subdomain takeover

1. You can use subtake to enumerate subdomains of a domain
2. Find all the subdomains which is pointing to third party
3. Make sure that subdomain is inactive or removed
4. Try to claim that subdomain

① Use hostilebruteforcer to hunt Subdomain takeover.

② See if the subdomain is inactive ? - yes → it is vulnerable
no → it is not.

③ > host subdomain.any.com

④ login and claim the subdomain is yours.

tools:
- Sublist3r
- hostilebruteforcer

See if subdomain is pointing to third party.

AWS S3 Bucket takeover