

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

```
01 Hostile Takeover
02 Hostname: Heroku, Azure, AWS
03 Hostile Subdomain Takeover
04 I have a website (any.com)
05 you want a support system
06 support.any.com from zendesk.com(support)
07 you pointed this subdomain to zendesk support
08 later on you cancelled or service expired
09 but you forgot to remove the redirection of pointing subdomain to zendesk.com (support)
10 if an attacker will get to know this situation
11 attacker will simply go to zendesk.com
12 will buy their support service
13 after that they will add this subdomain (support.any.com) as theirs own
14 and they will successfully claimed that this subdomain is belongs to an attacker because it wont verify on zendesk
15 steps is very simple for hostile subdomain takeover.
16 1. you have to find a subdomain pointing to third party (is an alias of x.com)
17 2. make sure their service is inactive or cancelled or expired
18 3. go that third party website register as client and when they will ask to point your subdomain you just give subdomain.com
```

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

كيفية استخراج CNAME الخاص في Subdomain :-

- للويندوز تستطيع عن طريق أمر nslookup

```
nslookup syed.subdomain-takeover.tk
```

- لللينكس تستطيع عن طريق أمر dig

```
dig @8.8.8.8 syed.subdomain-takeover.tk CNAME
      MX
```

2 or more domains on one up one content

* كل من سجلات DNS CNAME التي مسجلة أو في سجلات الـ DNS.

* mxtoolbox is a site to check

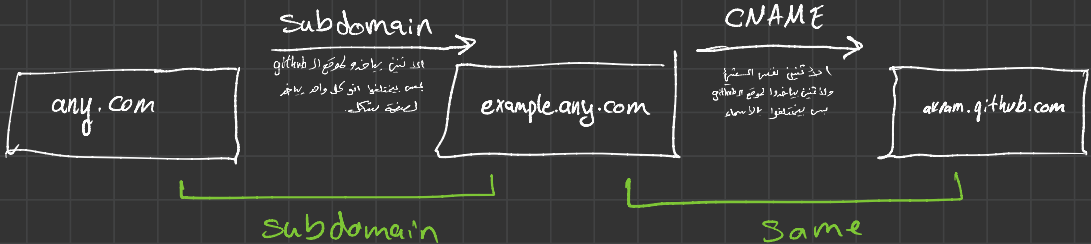
Python is better than PHP

* tool to get alias web site

```
root@kali:~# ipython
Python 2.7.9 (default, Mar 1 2015, 12:57:24)
Type "copyright", "credits" or "license()" for more information.

IPython 5.1.0 -- An enhanced Interactive Python.
?      -> Introduction and overview of IPython's features.
quickref -> Quick reference.
help    -> Python's own help system.
object? -> Details about 'object', use 'object??' for extra details.

In [1]: import socket
In [2]: socket.gethostbyname('yahoo.com')
Out[2]: '206.190.36.45'
In [3]: socket.gethostbyname('206.190.36.45')
Out[3]: '206.190.36.45'
In [4]: socket.gethostbyaddr('206.190.36.45')
Out[4]: ('url.fp.vip.gql.yahoo.com', [], ['206.190.36.45'])
In [5]:
```



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.

See if subdomain is pointing to third party.

tools:

- sublist3r
- hostilebruteforcer

AWS S3 Bucket takeover