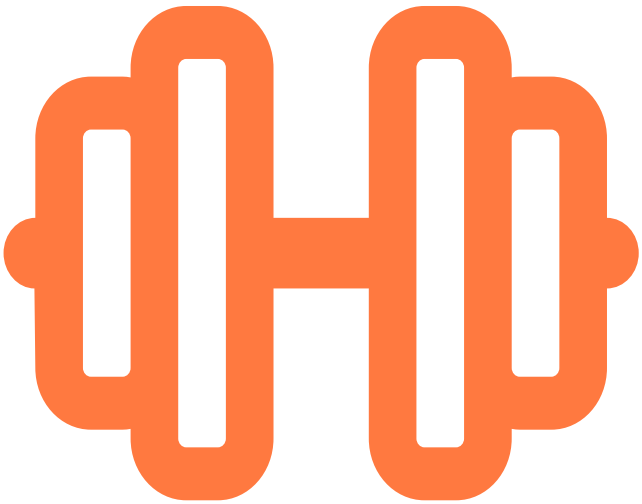
Autobahn security

Cyber Fitness Workout

Prevent subdomain takeovers



Prevent subdomain takeovers

Objective

In this workout, we remediate DNS misconfigurations that may be abused to perform subdomain takeovers. For this, you remove the DNS entries for subdomains associated with expired services.

About

A subdomain takeover issue may arise when a company's DNS records contain entries for subdomains related to expired services.

In the past, GitHub, Shopify, Help Scout, and WordPress were taken over to name just a few.

Risk

A subdomain takeover poses a significant security risk and requires immediate remediation. Adversaries can abuse this vulnerability in two ways:

1. **Phishing.** For example, adversaries may host a web page similar to a login page used by the target company and leverage it to harvest employee credentials.
2. **Session hijacking.** Adversaries may use the subdomain takeover to harvest session cookies and then hijack user sessions within the associated web application.

Fitness Workout

You fix current subdomain takeover issues in one easy step, for which you have two alternative options. If you feel like doing even more, you can then optionally prevent future issues in two additional steps.

1a - Option 1: Remove the DNS entries for the subdomain associated with the expired service

The best method to remediate the subdomain takeover issue is to review your DNS entries and remove all the active entries that are no longer in use. This can be achieved by logging in to the portal for your domain management solution and updating the DNS record.

If the service is still in use but the resource location has changed, the CNAME record should be updated to reference the legitimate resource location used on the third-party service.

1b - Option 2: Reclaim or purchase expired domains

Alternatively, or in addition to the previous step, you can reclaim subdomains. The exact steps will differ. If the affected domain, for example, is a GitHub subdomain, you want to create a GitHub user account with this user name. Act similarly for other online services.

2 - (optional) Review your process for updating DNS records

When creating a new resource, make the DNS record creation the last step in the process to avoid pointing to a non-existing resource.

In contrast to resource creation, for resource destruction the opposite is true: the affected DNS records need to be removed as the first step in this process.

It is a good practice to always add the 'off-boarding' procedure for domains to your checklist. This way you will ensure timely and accurate removal of stale DNS entries.

3 - (optional) Monitor your DNS records

Monitor your DNS records continuously for dangling DNS records.

You can use special tools such as aquatone to checks for subdomain takeovers. Such checks should periodically be performed to verify that there are no vulnerable domains.

In case you discover expired domains, follow steps 1a and 1b.

To query DNS and examine its records, you can use dig, a software tool that comes with all the major Linux distributions and can help you troubleshoot DNS issues.

For details on dig, check this documentation.

3.1 - Install dig

Ubuntu / Debian

```
sudo apt update && sudo apt install dnsutils -y
```

Red Hat / CentOS

```
sudo dnf install blind-utils
```

3.2 - Use the dig command to reveal CNAME records

- **Run the dig command**

The command syntax is as follows: `dig <@DNS server> <subdomain name> <type>`

```
dig @8.8.8.8 www.autobahn-security.de CNAME
```

Once you execute the command, dig displays the response from the DNS server.

- **Examine the authority section**

To find out which domains are linked to the subdomain, you need to examine the pieces of information in the authority section. To illustrate, the two domains listed to the right from autobahn-security.de in the command below are linked to autobahn-security.de and need to be checked for validity.

```
[autobahn-security.de](<http://autobahn-security.de/>). 1800 IN SOA [nsa1.schlundtech.de]
(<http://nsa1.schlundtech.de/>). [do-not-reply.autobahn-security.de](<http://do-n ot-reply.
autobahn-security.de/>).
```

Congratulations on taking these vital steps to prevent subdomain takeovers!
Your cyber health is definitely on the rise.

Get cyber-fit in just 3 months!