Automated Perimeter Mapping and Drift Detection

Pete Wills (he/him)

This document is provided for information purposes only. The contents, including any views expressed by **nbn** are indicative only and subject to change. This document is subject to the information classification set out on each page. If no information classification has been included, this document must be treated as '**nbn**-Confidential: Commercial' and must not be disclosed other than with the consent of **nbn**. The recipient (including third parties) must make and rely on their own inquiries as to the currency, accuracy and completeness of the information contained herein and must not use this document other than with the consent of **nbn**.

Incidents in 2022

How do we respond to the following scenario:

- Unauthenticated,
- non-rate-limited,
- unintentional access to production data.

Response:

- Take inventory of all APIs, check their configurations.
- Minor tweaks as a result, but mostly a control-validation exercise.

Thanks for listening.

Just Kidding!

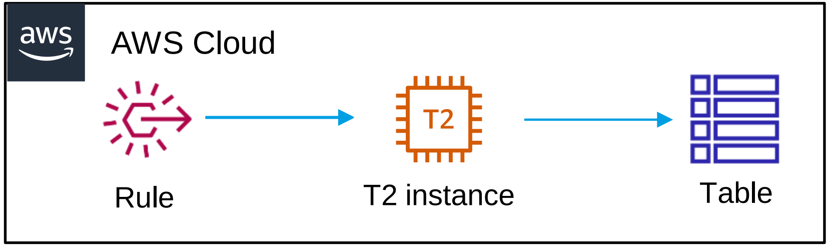
What we did was necessary, but insufficient.

Two major shortcomings:

1. It was a one-time exercise (the need is ongoing); and

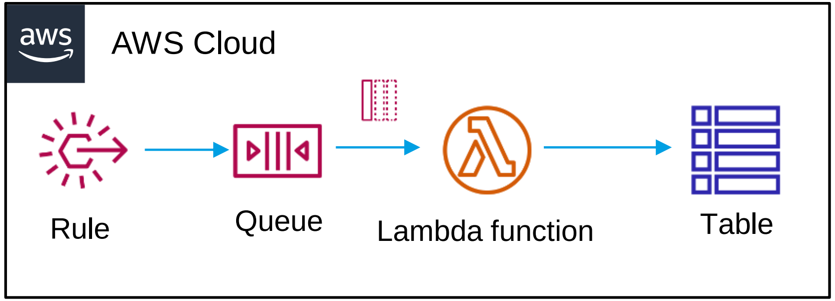
2. We investigated what we *knew* was there.

Built Application



Stage 1 – subdomain enumeration

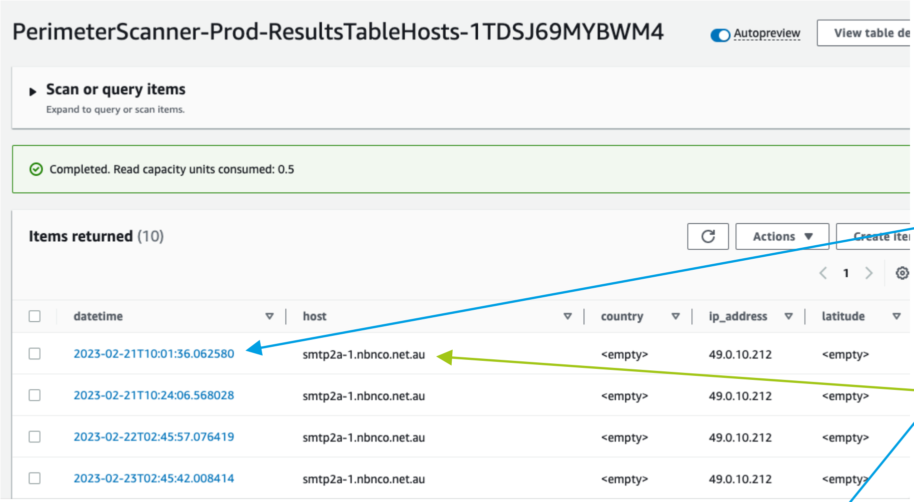
- Uses recon-ng, to enumerate using brute force / dictionary, Hacker Target, Google & Bing, and Certificate Transparency.
- Enumerates ~900 subdomains from 2.
- Persists to a DynamoDB *hosts of interest* table.



Stage 2 – service enumeration

- Scans the table, enqueues one item per host.
- A lambda worker function consumes the queue, *very slowly*, and nmap's the surface.
- Persists those results to a DynamoDB *host-ports of interest* table. ~800 entries.

What’s it found? (1 / 2)

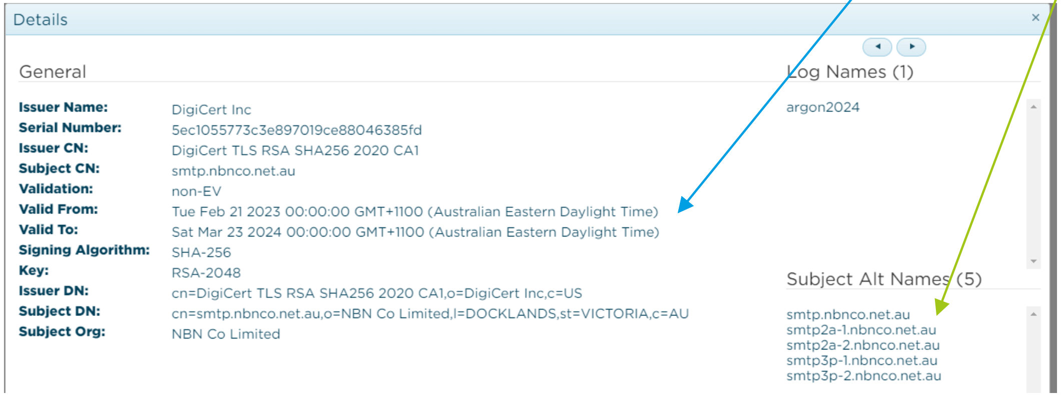


PerimeterScanner-Prod-ResultsTableHosts-1TDSJ69MYBWM4

Completed. Read capacity units consumed: 0.5

Items returned (10)

□	datetime	host	country	ip_address	latitude
□	2023-02-21T10:01:36.062580	smtp2a-1.nbnco.net.au	<empty>	49.0.10.212	<empty>
□	2023-02-21T10:24:06.568028	smtp2a-1.nbnco.net.au	<empty>	49.0.10.212	<empty>
□	2023-02-22T02:45:57.076419	smtp2a-1.nbnco.net.au	<empty>	49.0.10.212	<empty>
□	2023-02-23T02:45:42.008414	smtp2a-1.nbnco.net.au	<empty>	49.0.10.212	<empty>



Details

General

Issuer Name:	DigiCert Inc
Serial Number:	5ec1055773c3e897019ce88046385fd
Issuer CN:	DigiCert TLS RSA SHA256 2020 CA1
Subject CN:	smtp.nbnco.net.au
Validation:	non-EV
Valid From:	Tue Feb 21 2023 00:00:00 GMT+1100 (Australian Eastern Daylight Time)
Valid To:	Sat Mar 23 2024 00:00:00 GMT+1100 (Australian Eastern Daylight Time)
Signing Algorithm:	SHA-256
Key:	RSA-2048
Issuer DN:	cn=DigiCert TLS RSA SHA256 2020 CA1,o=DigiCert Inc,c=US
Subject DN:	cn=smtp.nbnco.net.au,o=NBN Co Limited,l=DOCKLANDS,st=VICTORIA,c=AU
Subject Org:	NBN Co Limited

Log Names (1)

argon2024

Subject Alt Names (5)

smtp.nbnco.net.au
smtp2a-1.nbnco.net.au
smtp2a-2.nbnco.net.au
smtp3p-1.nbnco.net.au
smtp3p-2.nbnco.net.au

A routine certificate rotation:

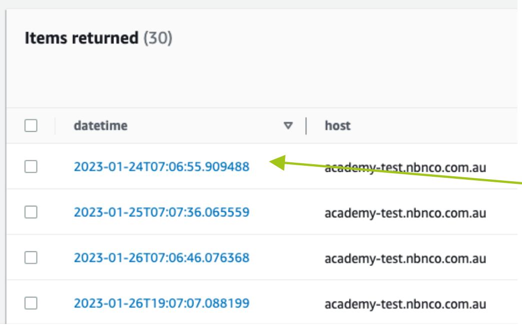
Here’s the detection.

And here’s a corresponding record from the public Certificate Transparency logs.

This is innocuous.

What’s it found? (2 / 2)

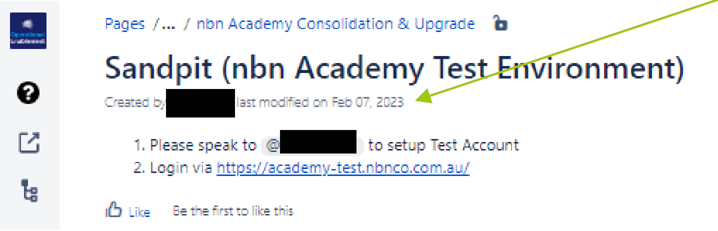
A pre-production test website:



Items returned (30)

☐	datetime ▽	host
☐	2023-01-24T07:06:55.909488	academy-test.nbnco.com.au
☐	2023-01-25T07:07:36.065559	academy-test.nbnco.com.au
☐	2023-01-26T07:06:46.076368	academy-test.nbnco.com.au
☐	2023-01-26T19:07:07.088199	academy-test.nbnco.com.au

Here’s the detection.



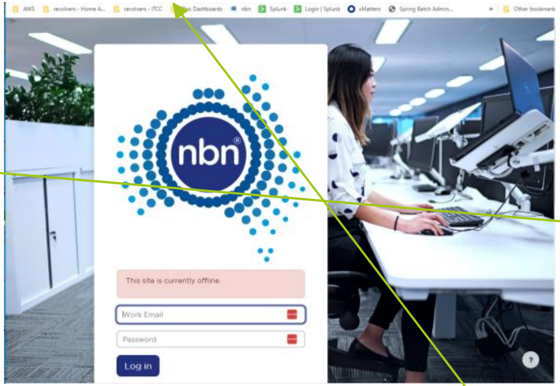
Pages / ... / nbn Academy Consolidation & Upgrade

Sandpit (nbn Academy Test Environment)

Created by [redacted] last modified on Feb 07, 2023

1. Please speak to @[redacted] to setup Test Account
2. Login via https://academy-test.nbnco.com.au/

Here’s some discussion on an internal platform (note the datetime).



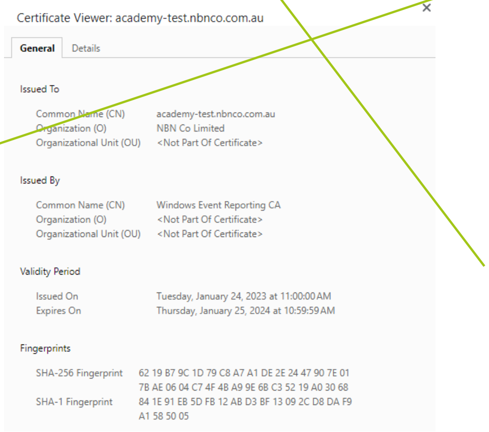
This site is currently offline.

Work Email

Password

Log in

Here’s the website in question. Should such pre-prod artefacts really be on the public internet?



Certificate Viewer: academy-test.nbnco.com.au

Issued To

Common Name (CN)	academy-test.nbnco.com.au
Organization (O)	NBN Co Limited
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Windows Event Reporting CA
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Tuesday, January 24, 2023 at 11:00:00 AM
Expires On	Thursday, January 25, 2024 at 10:59:59 AM

Fingerprints

SHA-256 Fingerprint	62 19 B7 9C 1D 79 C8 A7 A1 DE 2E 24 47 90 7E 01 7B AE 06 04 C7 4F 4B A9 9E 6B C3 52 19 A0 30 68
SHA-1 Fingerprint	84 1E 91 EB 5D FB 12 AB D3 BF 13 09 2C D8 DA F9 A1 58 50 05

Some observations

Understanding what’s *normal* is important.

Automating the detection process makes it a lot easier.

Yes, you can *buy* software to do this. Building it yourself though – forces you to understand the techniques that are possibly being used against you.

And… it’s not difficult.

Let me know if I can help.

Thank you

Pete Wills

IT Rapid Response @ nbn | 6x AWS certified