WM143 NCCD - cw3 - Security Architecture Coursework

1 Overall Context

FiDo (FiDo) is a charity. FiDo is planning to move to offices in Coventry. As part of the move, they are planning to implement a better security architecture and network design. This is in comparison to their current arrangement which has evolved haphazardly over the last three decades.

FiDo currently has a workforce of approximately 1300 individuals. A significant proportion of these workers are unsalaried volunteers. Most work predominantly online with a few days each month in the office.

There are several departments including HR, Finance, Corporate Comms and System Administration.

FiDo works closely with a New Zealand collaborator organisation on a range of projects.

FiDo has all its online assets within the domain `fido22.cyber.test`

FiDo needs the proposed security architecture and network design to accommodate significant expansion over the next three years.

The FiDo foundation charter requires them to utilise open source solutions where these exist. Currently and for the foreseeable future, they adopt a Debian by default operating system on all end points and infrastructure.

2 Your Role

You have been engaged as a Security Architect and Network Design consultant by FiDo. You have been supplied with a starter pack. This starter pack comprises:

1. a preliminary infrastructure layout that summarises what FiDo believe to be the main components of their infrastructural needs. This utilises the historic IP address block `80.64.0.0/16` that they inherited from the original creator of the organisation in 1988.
2. a preliminary emulation of this infrastructure. This deliberately incorporates negligible security architecture and summarises many bulk features (user endpoints for example) into a small number of representative examples.

3 Your Task

3.1 Zones of trust

1. Re-design the infrastructure to group assets into zones of trust. As well as re-organising existing assets, you should identify and position any infrastructure assets that you believe should be present but are missing. Similarly, you should remove any assets that are present but not appropriate.
2. Implement the reconfigured zones of trust as LANs or VLANs within the Netkit realisation. Insofar as is reasonable, you should utilise what is provided in the starter pack with the minimum essential change.

3.2 IP addressing

3. Re-organise the IP address utilisation of the organisation so as to reduce to a realistic minimum, the number of public IP addresses that FiDo should retain from within the `80.64.0.0/16` address block. Utilise NAT and / or port-forwarding as appropriate.
4. Implement the re-organised IP address allocation and associated routing within the Netkit realisation.

3.3 Traffic filters

5. Determine the filters that should apply between zones of trust (network firewalls) and where significant on endpoints (host firewalls).
6. Implement the filters within the emulated infratructure.

3.4 Verify

7. Verify that connectivity is achieved between appropriate clients and the services they should be able to utilise.
8. Verify that connectivity is prevented between inappropriate clients and the services they should not be able to access.

3.5 Augment

9. Design, implement / configure and test additional features that will usefully enhance the organisation's security posture. You should select features that you consider to be particularly important to FiDo and that will also showcase your comprehensive mastery of security architecture and network defence, above and beyond what you have already demonstrated in tasks 3.1 to 3.4 above.

4 Assessment

The assessment will comprise two parts:

- conventional submitted material via tabula.
- a short demo / viva where you will be asked to demonstrate some of the claims made in the conventional submitted material.

5 Deliverables

5.1 Report

An extremely succinct report in pdf format (named `nccd-arch.pdf`):

- highlighting the significant design, implementation / configuration decisions that you made (your claims) ranked in order of significance,
- highlighting the evidence that exists to support your claims,
- identifying the further work that is needed but that you were unable to realise.

The report is to have three sections corresponding with Phase 1, Phase 2, and Phase 3 (see marking scheme below) and References. The report must start with a clear network diagram, overlaid with your zone definitions.

Within each section, you are advised to have a table with three columns [Reference, Claim, Evidence].

It will be the content of these tables that will be verified at the viva.

5.2 Netkit Implementation

A file (named `nccd-arch.tar.gz`) that contains your Netkit-ng realisation of FiDo's security architecture.

- created using `tar -cvzf nccd-arch.tar.gz nccd-arch/` (where nccd-arch is the directory that you have used for your realisation)
- containing the configuration files for the emulated prototype (lab.conf, xyz.startup, xyz/etc/important-config-file etc)
- **not containing** the virtual disk files (xyz.disk etc - they are too big),
- containing any evidence files that you refer to in your report. Make these as small as possible to demonstrate whatever point you are making. Use a clear naming convention.

5.3 File of Hashes

A file (named `nccd-hashes.sha1`) that contains the sha1 hashes of the individual files contained within `nccd-arch.tar.gz`. This will be sampled at the demo to confirm no significant changes have been made between the submission and the demo / viva. One way to achieve this is via:

```
find ./nccd-arch -type f -print0 | \
xargs -0 sha1sum | tee nccd-hashes.sha1
```

6 Marking scheme

6.1 Phase 1:

To achieve a mark up to 55% you must:

1. use the specified file names,
2. define and implement credible zones of trust,
3. define and implement re-organised IP addressing,
4. clearly represent the zones of trust, the network topology and ip addressing used in the network diagram in the pdf,
5. define and implement filters between zones of trust,
6. partially verify connectivity is achieved / prevented between the zones,
7. have hashes at the demonstration that match the hashes in the submission nccd-hashes.sha1 file (ie provide evidence that nothing significant has changed between the submission and the demonstration).

6.2 Phase 2

To achieve a mark up to 65%, you must satisfy the following:

8. satisfy all the requirements of phase 1,
9. fully implement implement NAT / port-forwarding,
10. robustly verify that connectivity is achieved / prevented as appropriate within and between zones, clients and services,

6.3 Phase 3

To achieve a mark up to 100%, you must satisfy the following:

11. satisfy all the requirements of phase 2,
12. implement well-organised DNS using zone files,
13. utilise VLANs to good effect,
14. usefully augment the security architecture in ways of your choosing (this should demonstrate ability not evident already in the submission),

15. demonstrate comprehensive mastery of all aspects of the the submission at all scales (detail through to overall concept)

7 Important Constraints

a) This assignment should be undertaken in pairs. Exceptionally, it may be undertaken individually. Pairings must be notified to the module tutor during the final class of the Spring Term (**week commencing 13th March 2023**). By choosing to work as a pair, both members:
   - acknowledge that they have **set up appropriate mechanisms for collaboration** across the Easter Vacation.
   - **commit not to break the pairing** prior to submission,
   - agree to **work equitably** on the assignment.
   - agree to **make steady progress** through the assignment (ie not leave it until a few days before the submission deadline)

b) All activity must be conducted legally and ethically.

c) All source material must be referenced using the Harvard referencing convention. Put full bibliographic references at the end of the pdf report. Use comments for inline citation of these sources in config files.

d) In order to achieve a given mark, there must be consistency between the claims made in the submission and evidence at the demo/viva. Evidence at the demo / viva is fundamentally of two types: firstly technical evidence via the execution of commands, observation of outputs etc in the Netkit realisation of FiDo's infrastructure; secondly intellectual ownership evidence through familiarity with all aspects of the submission.

e) At the demo / viva, **both members of the pair should be fully familiar with all aspects of the submission**.

f) Changes in hashes discovered at the viva will be penalised to a maximum equivalent of a 10 day late submission penalty.

g) The demo / vivas are **provisionally scheduled for some time during the week commencing 8th May 2023.** The detailed demo / viva schedule will be published on Moodle for the module. Your exam schedule require the viva dates to be in a different week.

h) The demo / vivas will take place over MSTeams. One team member should screenshare the running implementation from their own laptop. You are advised to ensure that both members of the pair are able to do this should any technical shortcomings affect either of you on the day. Both members of the pair must be capable of handling audio during the viva. You must be able to stop and start individual machines during the viva. You must be able to adjust and explain any of the configurations that you submitted during the viva. You must be able to capture traffic and explain the content of pcap files during the viva.

i) Your submission will comprise three separate files, submitted via tabula.

j) The presumption is that both team members will contribute equitably and thus be awarded the same grade. Where this is clearly grossly unfair, then individually distinct marks may be awarded by exception.

k) **Failure to attend the viva will result in a mark of zero for the individual concerned**.

l) At the demo / viva, you must be fully familiar with all aspects of your submission that represent any change from the original starter pack. Evidence at the viva of lack of familiarity may be reported as possible academic misconduct. **Be sure you re-familiarise yourself with your submission shortly before your viva**.

8 Submission Deadline

Files to be submitted to Tabula by:

- **12:00 Thursday 4th May 2023**.

Each member must individually submit identical files to tabula, explicitly identifying the joint authors' student IDs on the pdf submission cover page.

9 Late Submission Penalties

Work that is received after the submission time (UK time), will be recorded as having arrived the next working day.

Work that is not submitted on Tabula by the deadline will be considered late. Penalties for lateness are applied at the rate of 5 percentage points per university working day after the due date, up to a maximum of 10 university working days late. After this period, the work will be counted as a non-submission.

10 Learning Outcomes

The following module learning outcomes are addressed by this coursework:

1. articulate the key principles behind the organisation and operation of typical communication networks and layered protocols using domain terminology.
2. configure network devices to achieve required operating characteristics.
3. explain network behaviour from captured network traffic.

11 Submission Coversheet

Your submission coversheet on the pdf should have the following fields:

- MODULE TITLE: Networks, Communications and Cyber Defence
- MODULE CODE: WM143-24 (cw3)
- YOUR STUDENT ID NUMBER:
- PARTNER'S STUDENT ID NUMBER: