ES94P-15

Security Architecture and Network Defence

1 Overall Context

FiDo is a charity. FiDo is planning to move to offices in Lemington. 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 1200 individuals. A very large proportion of these are unsalaried volunteers. Most work predominantly online with a few days each month in the office. A few specialists work predominantly on site.

The system administration and security will be operated by salaried in-house specialists.

FiDo works closely with an Canadian collaborator organisation, MapCo on a range of projects.

FiDo has all its online assets within the domain `fido.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 `135.207.0.0/16` that they inherited from the original creator of the organisation in 1988.
2. a User Mode Linux realisation of this preliminary infrastructure layout, implemented in Netkit. 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 Architecture - 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 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 `135.207.0.0/16` address block. FiDo suspects that NAT and / or port-forwarding might be helpful with this but they are far from certain.
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 Netkit realisation.

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 extemely succinct report in pdf format (named `sand.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 four sections corresponding with Phase 1, Phase 2, and Phase 3 (see marking scheme below) and References.

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 `sand.tar.gz`) that contains your Netkit realisation of FiDo's security architecture.

- created using `tar -cvzf sand.tar.gz sand/` (where sand is the directory that you have used for your realisation)
- containing the configuration files for the netkit 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 `sand-hashes.sha1`) that contains the sha1 hashes of the individual files contained within `sand.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 ./sand -type f -print0 | \
xargs -0 sha1sum | tee sand-hashes.sha1
```

6 Marking scheme

6.1 Phase 1:

To achieve a mark up to 58% you must:

1. satisfy the case-sensitive file-naming requirements of the deliverable files.,
2. define and implement credible zones of trust,
3. define and implement re-organised IP addressing,
4. define and implement filters between zones of trust,
5. partially verify that connectivity is achieved / prevented as appropriate between clients and services,
6. have hashes at the demonstration that match the hashes in the submission sand-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 above 58% , you must

7. satisfy all the requirements of phase 1,

To achieve a mark up to 68%, you must also

8. implement NAT / port-forwarding,
9. robustly verify that connectivity is achieved / prevented as appropriate between clients and services,
10. make a compelling case for your design and implementation of one augmented feature.

6.3 Phase 3

To achieve a mark above 68%, you must:

11. satisfy all the requirements of phase 2,

To achieve a mark up to 100%, you must also:

12. make a compelling case for your design and implementation of two further significant, distinct, augmented features,
13. demonstrate comprehensive mastery of all aspects of the the submission at all scales (detail through to overall concept)

7 Important Constraints

a) This assignment must be undertaken individually.

b) All activity must be conducted legally and ethically.

c) All source material must be referenced using the Harvard referencing convention. There should be a conventional Harvard references section at the end of the pdf report giving full bibliographic details of all source used. Use Harvard inline citation for example (eg SMITH, 2019a) within comments 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) Changes in hashes of significant files, discovered at the viva will be penalised to a maximum equivalent of a 10 day late submission penalty.

f) The demo / vivas are **provisionally scheduled for 4th to 7th January 2022.** The detailed demo / viva schedule will be published on Moodle for the module.

g) The demo / vivas will take place via MSTeams. You must be able to screenshare the running implementation that that you submitted to tabula via MSTeams. 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.

h) The demo / viva will be recorded. This enables you to review feedback given verbally at the viva. It also supports the moderation process.

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

j) **Failure to attend the viva will result in a mark of zero**.

k) 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**.

l) For Phase 3, trivial tweaks will not make a compelling case, nor will they permit you to demonstrate your comprehensive mastery.

8 Submission Deadline

Files to be submitted to Tabula by:

- **12:00 Monday 13th December 2021**.

Late submission of coursework without approval for an extension will result in marks being deducted up to a maximum of 10 University working days late. After this period, the work may be counted as a non-submission.