CA1 – OS FW Assignment Specification

Course: BSc. in Computing in Digital Forensics and Cyber Security

Module Title: Network Security **Module Code: H3015**

Lecturer's Name: Peter Alexander **Email: peter.alexander@tudublin.ie**

Date Assignment given out: 01/02/24 **Latest date for Submission: 11.59pm 03/03/24**

% of total CA marks allocated: 30% (of CA) **Max Group Size: 2 (or individual project)**

General Requirements for Students:

1. A proportion of assessment marks is allocated to the report presentation. All assignment scripts must be word-processed, where appropriate.
2. An Assignment Submission Form must be included with each assignment prior to submission.
3. Assignment scripts must be submitted via link on Moodle. Email submissions will not be accepted.
4. All relevant provisions of the Assessment Regulations must be complied with. Penalties for late submission of assignments are as follows:

   No marks for assignments submitted after the deadline.

5. Extensions to assignment submission deadlines will only be granted in exceptional circumstances. The appropriate "Application for Extension" form must be used and supporting documentation (e.g. medical certificate) must be attached. Applications for extensions should be made directly to the Programme Leader **in advance** of the deadline date.
6. Assignments that exceed the word count will be penalised.
7. Students are required to refer to the assessment regulations in their Student Guides and on the Student Website.
8. TU Dublin penalises students who engage in academic impropriety (i.e. plagiarism, collusion and/or copying). Please refer to the referencing guidelines on Moodle for information on correct referencing.
9. Please be aware that the use of such tools as LLMs (Large Language Models such as chatGPT) is unfair academic practice and, as listed in the QQI Academic Integrity Guidelines, will be treated as plagiarism. In summary, the work submitted for the assessment **must be your own work**.

Assignment Details

Outline of Assignment	Research and test two open source firewalls, one of which must be Nftables. (*Note: Second firewall cannot be IPTables as this is being replaced by Nftables. UFW or Firewalld also will not be accepted as these are essentially frontend based versions of IPTables. Any other firewalls that are just a frontend for Nftables or IPTables are also not appropriate. If in doubt, please check with your lecturer.)* Implement the two firewalls in a realistic testbed scenario. Design a series of tests to examine the effectiveness of the firewalls. Compare and contrast the two firewalls. Collate and analyse the results of your testing. Demonstrate your tests in the lab. Make a presentation on your findings (PowerPoint). Write a report on your assignment and findings (Maximum 2000 words for two people teams, 1500 words for individual submissions).
Detail of Assignment	Deliverables: • Report/paper. Maximum 2000 words in length (1500 if doing individually). This should be written in an academic style, and fully referenced using Harvard style referencing. • Presentation (mandatory) in the lab: 5 minutes – strictly enforced. • Demonstration (mandatory) in the lab: 7 minutes – strictly enforced. ○ (*Note: This may be reduced to 5 minutes depending on the number of individual submissions.)* Submission is through a dedicated link on Moodle. Late submissions will not be accepted. Files should be saved as MS Word or PDF files with the following filename structure: student number, name, netsecurity eg. B00012345WalterWhitenetsecurity.pdf
Lecturer this work is for	Peter Alexander
Handout date	1st February 2024
Hand-in date	Research paper to be submitted via Moodle by 11.59pm on Sunday 3rd March 2024. Presentations and demos due Tuesday 5th March 2024. **IMPORTANT: The presentation and demo are mandatory requirements and any assignments without one will not be accepted.**
Group	This is an individual or team project (maximum two persons per team).

Marking Scheme

Assessment Criteria	% weighting for each problem part
Appropriate background research.	10%
Effective research and demonstration of tests.	15%
Analysis of results presented in appropriate context.	15%
Extra relevant research/context	10%
Proper references and overall quality of the report.	10%
Effective presentation, showing understanding of the issues and depth of research and well-thought out, logical, relevant testing and analysis of results.	25%
Effective demonstration, showing understanding of firewall technologies and effective testing.	15%
(**Total**)	**100%**

*Note: The report, presentation and demonstration are each a mandatory component and any completed assignment that does not include all 3 components will be considered as an **invalid submission** which will receive **0%**.*

Other Information

What you should hand in	A structured report containing the research. Sources of information MUST be referenced. Harvard style referencing (see the resources on Moodle).
Guidelines/Length	The report would be expected to be in the region of 2000 words (1500 if doing individually), not including title page and references.
Resource Required	Internet. Open source firewalls include Nftables, pfSense, OPNsense, Smoothwall, Endian, IPCop, IPFire etc.
Plagiarism	Your attention is drawn to TU Dublin's Plagiarism Policy Guidebook, available on Moodle. This covers cheating, attempts to cheat, plagiarism, collusion and any other attempts to gain an unfair advantage in assessments. The work you submit must conform to those regulations.

Common Pitfalls for this Assignment:

- **Poorly thought out tests**
- **Lack of diversity in tests**
    - **E.g. only testing using different Nmap scans – these are all different versions of the same test (i.e. port scans). Should be aiming for 2-3 different relevant tests**
- **Poor understanding of Nftables rules, chains, filters**
- **Poor demonstration of Nftables' capabilities**
- **Poorly thought out testbed topology/layout**
- **Inability to put tests in the correct context – why was each test carried out and why was it successfully/unsuccessfully mitigated**
- **Ineffective configuration of the firewalls – an important aspect of this assignment is to implement rules on the firewalls to mitigate attacks**
- **Lack of details on tests conducted**
- **Lack of effective comparisons**
- **Lack of detail in the analysis**
- **Weak conclusion based on analysis and data**
- **Failure to submit a report before deadline – always submit something rather than nothing**
- **Failure to attend presentation and/or demonstration**