COS80013 INTERNET SECURITY ASSIGNMENT 1 - REVIEW REPORT

A comparative review study of cyber-attacks and cyber security

This assessment is designed to deepen your understanding of contemporary research developments in cybersecurity. You will conduct a comparative review of **five (5)** different developments/research directions in **one** chosen domain of cybersecurity. You may select one from the following domains:

- Converged Security
- Operating Systems Security
- Malware & Vulnerabilities
- Network Security

You must choose **one** perspective for your review: either **attacker** or **defender**. This means you will either focus on advanced attacks (attacker perspective) or on sophisticated defense mechanisms (defender perspective).

In addition to reviewing existing literature, you will be required to **replicate and implement** at least one (1) or two (2) of the reviewed developments depending on the grade outcome you aim for. These implementations must be demonstrated through carefully chosen screenshots, logs, or other forms of evidence, ensuring that **all experiments are done in a sandbox environment**. **Live systems must not be used** for testing to prevent unintended disruptions or breaches.

The final deliverable is a comparative review report with evidence of your experimentation/implementation, concluding with a recommendation for the **best** (or most critical) development (if reviewing defensive measures) or the **most adversarial** approach (if reviewing attacks).

Assessment Requirements

You will produce a comparative review of five (5) different research developments.

1. **Select Your Domain**

Choose **one** domain from,

- Converged Security(week 1)
- Operating Systems Security (week 2)
- Malware & Vulnerabilities (week 3)
- Network Security (week 4)

Provide a brief justification for why you selected this domain and its relevance to modern cybersecurity challenges.

2. **Choose Your Perspective**

Attacker Perspective- Examine five advanced or emerging attacks

Or

Defender Perspective- Examine five defensive strategies or solutions

3. **Literature**

Papers with code are preferred. This means you should look for open-source implementations or code repositories (e.g., GitHub, GitLab) that accompany peer-reviewed articles.

You must rigorously review at least **five** developments.

Your review should be supplemented and justified by at least,

15 references for a High Distinction (HD)

10 references for a Distinction (D)

5 references for a Credit/Pass (C/P)

4. **Implementation Requirement**

The implementations should be demonstrated using screenshots (or equivalent evidence). Show how you set up your environment, how you installed/configured the tool or proof-of-concept code, and the observed outcomes/results.

- Students aiming for High Distinction (HD), **Implement 2** of these developments.
- Students aiming for Distinction (D), **Implement 1** of these developments.
- Students aiming for Credit (C) or Pass (P), **Only theoretical reviews** (no implementation required).

All implementations/experiments must occur in a controlled sandbox environment (virtual machines, containerized environments).

Using live or production systems for any testing or experimentation is **strictly prohibited and will result in an instant 0 grade**.

Guidelines

Choose the developments that have available source code (from platforms like GitHub or GitLab) or can be replicated through similar configurations or proof-of-concept implementations.

Ensure that your selected development aligns with your chosen domain and perspective (attacker or defender).

Analyse the results of your implementation, If you implemented an attack, explain its success rate, stealth, and effectiveness, If you implemented a defense mechanism, explain its detection accuracy, false positive/negative rates, and overall system impact.

A 3-minute live demonstration is required to demonstrate your implementations.

5. **Comparative Analysis**

Compare and contrast the five selected developments by highlighting their respective strengths, weaknesses, applicability, and overall impact on cybersecurity. If your review centers on attacks, determine which method poses the most severe adversarial threat based on factors such as stealth, destructive potential, and ease of execution. Conversely, if you are reviewing defensive measures, identify which approach offers the best protection for the chosen application or scenario by considering aspects like resource requirements, technical complexity, and integration with existing infrastructure.

Conclusion

Identify the best (or "most adversarial") development out of the five reviewed. Justify your conclusion with critical analysis and references to your experiments and literature review.

6. **References**

   - A references section listing all cited literature in a recognized citation style (APA/Harvard/IEEE, as per your program guidelines).

Submission Requirements

Submit assignment coversheets attached report through Canvas in a single upload. Do not use zip files. Failure to follow submission instructions may result in your assignment not being graded and potentially treated as a late submission.

For a grade above 75%

- Identify and review at least 15 additional academic resources, focusing on literature published in reputable journals or conferences within the last two years.
- Incorporate at least 2 implementation results of the developments you investigated
- 3-minute live demonstration on your implementation code

Expectations of your submitted document

- Assignment Coversheet

- Title page specified below

Overview statement outlining your chosen topic area, how many papers you reviewed, key aims of the selected literature and overall findings

Word count

- The spreadsheet do not count towards the word count

- Review report is required to be a maximum of 3,500 words excluding the overview statement. That is an expectation of 700 words per one development you investigate, and 875 words per week to complete • You will be assessed on a wordcount correct or within +/- 10%

Advice

- It's best to avoid quotes, so write without them . If you change words around to get around Turnitin you still might receive 0 marks. It's best to write in your own words