Assessment Brief

Submission and feedback dates

Submission deadline: Before (17-12-2024 at 4:00 PM GST) and is eligible for 48-hour late submission window.

Marks and Feedback within 15 days and formal marks will be published after the award board.

Submission details

Module title and code: Secure Computer Networks UFCFLC-30-2

Assessment type: Report

Assessment title: Final Assessment

Assessment weighting: 100% of total module mark

Module learning outcomes assessed by this assessment:

This assignment assesses the following module learning outcomes:

- Demonstrate an understanding of a range of protocols employed at various network layers.
- Appreciate the significance of end-to-end security in network communication.
- Communicate the nature and potential threats to the security of computer networks, systems, and operating systems.
- Discuss the relative merits of different solutions to these threats for a given system, business, or application.
- Analyse a typical business/application for security threats, using appropriate models and leading to proposed solutions.

Completing your assessment

What am I required to do on this assessment?

The assessment for this module consists of a written report, made up of 3 parts.

Assessment Specification

You are expected to complete three parts in this assessment. The details of these parts is provided below:

Part 1: Research on latest Vulnerabilities on Computer Networks and Cybersecurity (30% Marks)

Task 1: Identify and document 10 common vulnerabilities (15 Marks)

Identify and document 10 common vulnerabilities on Computer Networks and Cybersecurity from reputable vulnerability databases, such as:

- National Vulnerability Database (NVD)
- Common Vulnerabilities and Exposures (CVE)
- MITRE ATT&CK
- Exploit Database

Instructions: For each vulnerability, provide the following details:

- **Vulnerability Name and CVE ID:** (e.g., CVE-2023-XXXX)
- **Date of Discovery:** Indicate when the vulnerability was first reported.
- **Description:** Provide a brief description of the vulnerability, including how it can be exploited.
- **Impact:** Describe the potential risks and damages if the vulnerability is exploited.
- **Affected Systems/Software:** Mention the operating systems, software, or hardware affected by the vulnerability.
- **Mitigation Strategies:** Outline potential patches, updates, or strategies to mitigate the vulnerability.

Deliverables:

A well-organized report with a table or list of vulnerabilities, formatted to clearly present each of the required details. Cite the vulnerability databases you used for your research (e.g., NVD, CVE, MITRE ATT&CK).

Task 2: Research on Latest Computer Networks and Cybersecurity (15 Marks)

Select a recent paper from a reputable journal based on the vulnerabilities found in the task 1 from the well reputed databases, like, IEEE Explore, ACM Digital Library, Science Direct, Springer, etc.

Summary of the Research Paper:

Write a 300-500 word summary discussing the paper's main findings, methodologies, and contributions to the field of computer networks and cybersecurity. Your summary should provide a critical evaluation, highlighting the strengths, weaknesses, and the paper’s relevance to real-world cybersecurity applications. It is essential that the paper you choose has not been previously discussed with any other student to maintain the uniqueness and independence of your assessment.

Part II: Penetration Testing (40% Marks)

As a penetration tester, your assignment is to evaluate the security posture of a corporate environment utilizing two virtual machines (VMs). VM1 is configured with Kali Linux, a robust and widely-used

penetration testing distribution that provides a variety of tools for security assessment. VM2 is a Windows machine utilized by employees to manage sensitive corporate data. Your objective is to simulate a targeted attack from VM1 to VM2, focusing on the following critical areas:

Reconnaissance (10 Marks)

It aims to gather essential information about VM2, including open ports, running services, and the operating system version. This foundational knowledge will assist in identifying potential vulnerabilities and entry points for the simulated attack.

Vulnerability Assessment (10 Marks)

The vulnerability assessment phase involves systematically identifying and evaluating known vulnerabilities in VM2. Focus on outdated software, misconfigurations, and weak security practices. This process will help uncover weaknesses that could be exploited during the penetration test.

Privilege Escalation (10 Marks)

The privilege escalation phase aims to gain higher-level access within VM2 after an initial compromise. Identify and exploit vulnerabilities or configuration weaknesses to elevate permissions, thereby allowing greater control over the system and access to sensitive data.

Recommendations (10 Marks)

Provide a detailed set of recommendations aimed at enhancing the security of VM2 against potential attacks. These recommendations should focus on best practices for patch management, implementing strong password policies, and effective network segmentation. Consider additional security measures such as user access controls, regular audits, and employee training.

Part III: Examination of Firewall Implementation in Computer Networks (30%Marks)

The learning objectives of this part of the assessment are twofold:

1. To understand the fundamental concepts of firewall operation.
2. To gain practical experience in configuring a firewall for network protection.

Firewall Implementation (10 Marks)

Students will first implement a stateless packet-filtering firewall**.** This type of firewall operates by examining each packet individually without maintaining any connection state. The firewall will inspect incoming and outgoing packets and apply a set of firewall rules to determine whether to allow, drop, or forward the packets based on their attributes (such as IP address, port, and protocol).

This exercise will provide a hands-on understanding of:

- How firewalls filter traffic based on packet-level data.

- How stateless filtering differs from stateful inspection techniques.

Practical Setup Using iptables (10 Marks)

Students will be provided with a network topology that simulates a real-world environment. Using iptables, a widely-used firewall utility in Linux, students will configure rules to secure the network. This task will include:

1. Defining and applying basic input/output rules.
2. Controlling traffic between internal and external networks.
3. Creating rules to mitigate common attacks, such as IP spoofing or port scanning.

By completing these steps, students will gain practical experience in securing networks using packet-filtering firewalls.

Exploration of Advanced iptables Features (10 Marks)

In addition to the basic setup, students will explore more advanced applications of iptables, such as:

- NAT (Network Address Translation) to enable multiple devices to share a single public IP address.
- Logging rules to monitor suspicious traffic.
- Rate-limiting rules to prevent denial-of-service attacks.

These tasks will further enhance students' understanding of firewall configurations in complex network environments.

Conduct an examination of the firewall through the seed lab, providing a comprehensive report on the completed lab available at:

https://seedsecuritylabs.org/Labs_20.04/Networking/Firewall/

Deliverables

Only one report file is to be submitted with section numbers.

- You need to submit a detailed report, with screenshots – needs to be clear and readable, to describe what you have done and observed.
- You also need to explain the observations that are interesting or surprising. Please also list the important code snippets and screenshots that need to be readable and explained.
- Simply attaching code or screenshots - need to be clear and readable- without any explanation. or demonstration of your understanding of the Learning Outcomes will not receive credits.
- **All screenshots in the report must have your student number and date and time in the user prompt, need to be clear and readable.**

Note: Please note that the report should encompass screenshots, testing details, findings, and references.

Plagiarism

In submitting this assignment, you make the following declaration: not fact-checking and providing citations for any of the work included information obtained from using AI tools will result in an Assessment Offence or mark of zero for that part.

- I declare that I am the sole author of this work.
- I have not copied work from any source (including my own previously submitted work for which credit has been/is due to be awarded at UWE or elsewhere).
- I have not shared any versions of my work being submitted with other students.
- I have not viewed any versions of the work being submitted by other students.
- I have fully acknowledged/referenced all sources of information used.
- I am aware that failure to comply with the above may constitute an assessment offence.

Marking Criteria

Part 1 Marking Criteria

Task-1:

Deliverables	Aspects	0 Marks	1-5 Marks	6-10 Marks	11-15 Marks	Total Marks
Identify and document 10 common vulnerabilities on Computer Networks and Cybersecurity	Includes correct identification of vulnerabilities (Name and CVE ID), date of discovery, description, impact, affected systems/software, and mitigation strategies.	No attempt or incomplete details for most vulnerabilities	Partial identification with vague or minimal details for 1-3 vulnerabilities; insufficient description or impact analysis	Adequate identification and relevant details for 4-6 vulnerabilities with minor gaps; mostly accurate but lacking in-depth analysis or some fields missing	All 10 vulnerabilities are correctly identified with comprehensive, accurate details, including clear description, impact analysis, affected systems, and thorough mitigation strategies	

Task-2:

Deliverables	Aspects	0 Marks	1-5 Marks	6-10 Marks	11-15 Marks	Marks
Summary of Paper	Relevance, analysis, and critical evaluation	No attempt	Paper is irrelevant or poorly selected; minimal analysis and weak evaluation.	Some relevance; basic analysis and evaluation with limited depth.	Highly relevant paper; thorough analysis of findings and methodologies; strong evaluation of strengths and weaknesses, highlighting real-world relevance.	

Part 2 Marking Criteria

Deliverables	Aspects	0 Marks	1-3 Marks	4-6 Marks	7-10 Marks	Marks
Reconnaissance Findings	Depth of Reconnaissance	No attempt	Only basic information gathered; lacks detail.	Some relevant information obtained but lacks depth.	Detailed findings with clear identification of potential vulnerabilities.	
Vulnerability Assessment	Identification and Evaluation of Vulnerabilities	No attempt	Only one vulnerability identified with weak explanation.	Two to three vulnerabilities identified with satisfactory explanations.	Comprehensive assessment identifying multiple vulnerabilities with strong explanations.	
Privilege Escalation Methods	Clarity and Effectiveness of Privilege Escalation Techniques	No attempt	One method described with weak justification.	Two methods explained with satisfactory clarity.	Multiple effective methods described with clear justification and methodology.	
Recommendations	Quality and Relevance of Security	No attempt	Weak or irrelevant recommendation	Some relevant recommendations provided but	Comprehensive recommendations focusing on patch	

Deliverables	Aspects	0 Marks	1-3 Marks	4-6 Marks	7-10 Marks	Marks
	Recommendations		s provided.	lacks comprehensiveness.	management, password policies, and network segmentation.	

Part 3 Marking Criteria

Deliverables	Aspects	0 Marks	1-3 Marks	4-6 Marks	7-10 Marks	Marks
Firewall Implementation	Understanding and implementation of stateless packet filtering, including rule creation and application.	No attempt or incomplete implementation of firewall rules.	Basic implementation of firewall rules with minimal relevance.	Some relevant rules created, but lacking effectiveness.	Complete and effective implementation of all required rules, including advanced applications, demonstrating a strong understanding of firewall operation.	
Practical Setup Using iptables	Configuration of iptables for network protection, including defining input/output rules and controlling traffic.	No attempt or significant errors in iptables configuration.	Partial setup with several errors or irrelevant rules.	Adequate setup with most rules defined but lacking effectiveness.	Complete setup of iptables, effectively controlling all specified traffic with advanced features, demonstrating proficiency.	
Exploration of Advanced iptables Features	Understanding and application of advanced iptables features, such as NAT, logging, and rate-limiting rules.	No attempt or incorrect implementation of advanced features.	Basic exploration of advanced features with minimal effectiveness.	Some relevant advanced features implemented but lacking depth or clarity.	Complete and thorough exploration of advanced features, demonstrating proficiency and relevance to network security.	

Performance Level Criteria

Performance Level	Part 1: Research on Vulnerabilities	Part 2: Penetration Testing	Part 3: Firewall Implementation
Fail (< 40%)	The report lacks sufficient research on the 10 vulnerabilities. Vulnerabilities are incomplete or poorly documented, missing key details such as CVE IDs, descriptions, and mitigation strategies. No clear connection is made between vulnerabilities and the cybersecurity field.	The report lacks clarity and coherence, failing to adequately assess the penetration test. Minimal or no coverage of key areas such as reconnaissance, vulnerability assessment, and privilege escalation. Findings and evidence are incomplete or missing, with no meaningful recommendations.	The firewall implementation and iptables setup are incomplete or missing. There is little to no understanding of packet filtering or iptables configuration. The exploration of advanced features is absent, and no evidence or justification is provided.
3rd Class (40% - 49%)	The report provides a basic overview of the 10 vulnerabilities, but lacks depth and detail. Some key components such as the CVE ID, descriptions, and mitigation strategies are present but incomplete. The analysis and connection to cybersecurity applications are minimal.	A basic assessment of the penetration test is presented, but lacks depth. Some areas are covered, but there are gaps in the methodology, findings, and evidence. Recommendations are provided, but they are not comprehensive. Limited screenshots or evidence are included.	A minimal setup of the firewall and iptables is presented. Some rules are defined but are insufficient in terms of effectiveness. The exploration of advanced features such as NAT or logging is either missing or inadequately implemented.
Lower 2nd Class (50% - 59%)	The report addresses the 10 vulnerabilities with sufficient detail. Most of the required information is included, but the analysis lacks depth. Basic descriptions and mitigation strategies are provided, but the connection to real-world cybersecurity applications is limited.	The penetration testing report covers key areas such as reconnaissance, vulnerability assessment, and privilege escalation. Findings are presented with evidence, but the analysis could be more thorough. Recommendations for improvement are included but lack detailed justification.	A clear firewall setup is presented with effective packet filtering. Basic iptables rules are implemented, and some exploration of advanced features is present. However, the justification and depth of the implementation could be improved.
Upper 2nd Class (60% - 69%)	The report thoroughly documents the 10 vulnerabilities, providing detailed descriptions, CVE IDs, and mitigation strategies. The analysis connects the findings to cybersecurity practices and demonstrates a good	A thorough assessment of the penetration test is provided, with detailed findings in key areas such as reconnaissance, vulnerability assessment, and privilege escalation. Recommendations are well-justified, and the report includes substantial evidence	The firewall implementation is comprehensive, with effective iptables rules and some advanced features (e.g., NAT, logging). The setup is well-documented, and the configuration shows a good understanding of firewall operations in

Performance Level	Part 1: Research on Vulnerabilities	Part 2: Penetration Testing	Part 3: Firewall Implementation
	understanding of their impact. The report is well-organized and supported by credible sources.	such as screenshots and logs.	securing networks.
1st Class (70%+)	The report is exceptionally well-researched and provides a deep analysis of the 10 vulnerabilities. All required details are thoroughly documented, including CVE IDs, descriptions, impact, and mitigation strategies. The analysis is critically evaluated, connecting the vulnerabilities to practical cybersecurity measures. The report is well-organized and cites credible databases.	The penetration testing report is comprehensive and well-executed, covering all key areas in detail. The findings are supported by extensive evidence and clear documentation. Recommendations are insightful and practical, demonstrating a deep understanding of security weaknesses and mitigation strategies.	The firewall implementation is flawless, with advanced iptables features fully explored and justified. The rules are effective in controlling traffic, and the setup includes NAT, logging, and rate-limiting. The implementation demonstrates a high level of proficiency in firewall configuration and network security.