Assessment Brief of Task 1

Module Leader: Dr Jims Marchang		Level: 5	
Module Name: SECURE NETWORK SERVICES AND ADMINISTRATION		Module Code: 55-508828	
Assignment Title: Task 1 SECURING NETWORKS, SYSTEMS AND DATA (PRESENTATION AND DEMONSTRATION)			
~~Individual /~~Group	Weighting: 50%	Magnitude: Present and Demo	
Submission date/time: **In the last tutorial session of your tutorial group** **Week 12 of the 1st Sem.**	Blackboard submission: ~~Yes~~/No Turnitin submission: ~~Yes~~/No	Format: Presentation and Demonstration	
Planned feedback date: **Week 11 of the 1st Sem.**	Mode of feedback: Electronic/In-Person	In-module retrieval available: ~~Yes/~~No	
In this assessment are students asked to consider:	Inclusivity and accessability		Yes/~~Not applicable~~
	Sustainability		~~Yes~~/Not applicable

Module Learning Outcomes

- **LO3 :** Understand the fundamentals of securing different TCP/IP layers in wired and wireless environments. Distinguish and examine security requirements of both data and network in an organisation.
- **LO4 :** Understand policy, regulation and the need and impact of data and network security in society.
- **LO5:** Design, develop, implement, test, analyse and validate security mechanisms through secure data and network application programming and secure software development.

As an academic community it is expected that all students and staff demonstrate the highest ethical standards of academic integrity. Please refer to the statement on avoiding plagiarism and other unacceptable academic conduct on Blackboard.

Who do I contact if I have a question?

Ask the tutor most closely related to the issue first. If you don't feel the matter is resolved, then ask the module leader i.e. Dr Jims Marchang (jims.marchang@shu.ac.uk), or other teaching staff e.g. Mark Townley (mark.townley@shu.ac.uk), Ahmed Al-Ani (a.r.al-ani @shu.ac.uk). If you still don't feel it's resolved, then ask course leader and then the subject leader (Dr Shahrzad Zargari; s.zargari@shu.ac.uk). If it's still not resolved, ask the Deputy Head of Computing (Mark Jacobi, m.jacobi@shu.ac.uk).

PS: Please note that marks are the subjective opinion of your teaching team and not debatable, but your tutors will be happy to explain the feedback you have been given. Please let your tutor know right away if you think there's been a mistake in any assessment procedures.

1. Assessment Requirements

Task 1 assessment consists of presenting your work through a LIVE demonstration in Laboratory followed by question and answers. Demonstration is the aspect of showing us what you have developed for the assessment. The mark weight distribution of the is given in Table 1.

Table 1: Presentation and Demonstration Mark Distribution

Task Name	Weighting
Group Demonstration	80%
Question and Answer	20%
TOTAL	100%

This assignment allows you to build your knowledge and develop critical understanding of the information security over a network. This is an opportunity to solve and address real issues using different platforms, operating systems and services. This is a **group-based** coursework.

1.1. Deliverables:

Group Presentation (submit the slides and source codes and configuration files via BB submission point) and Recorded video for demonstration (upload in private YouTube).

You are to work in self-organised **groups of 3 members**. However, the questions-and-answer (discussion) is marked individually during the demonstration. Use the peer-review feedback form of Appendix A if and only if you feel that the partners are not contributing equally, and this is to be summitted on the day of demonstration (by each member) to the assessor and marks will be adjusted accordingly ***.

1.2 Assignment objectives:

Design, develop and test a secure network application and secure the network so that it is safe to adopt and use during the data transmission and network connection within an organisation.

2. Assessment Brief:

Brief: In Bletchley Park, three building need to be connected to securely interact and engage so that no unauthorised individuals can access the systems and the network. In such system, they need to develop a **Secure Reporting System (SRS)**. However, all the people working in each building should not be allowed to report and be allowed to see or capture the network traffic except the **assigned** individuals and the systems of each group in each building. In each building there are three tiers of work group with three levels of access priority: Level 1 (Lowest), Level 2 (Mid), and Level 3 (Highest). The systems with level 3 access rights can manually update any reports to the server while the reports from all the other remote machines are collected automatically at the assigned specific time of each day. Each tier working group are securely separated even if they are all accessing the same network in the room/building. The SRS ensure secure communication with the server and allow monitoring of certain remote systems within the network for potential security threats or for observation or scanning the systems. So, all communication between clients and the server must be encrypted, authenticated, and secure to protect from unauthorised access.

Hint: The system operates in a secure LAN with authenticated dynamic routing, ACL-based communication control, VLAN segmentation, port security, and encryption techniques like RSA-2048 and AES-256 and maintain message Integrity using SHA-512.

Application Description:

- **Client Application**: Installed on remote MI6 machines, this monitors the system and securely sends reports to the central server automatically all the logs at the end of the day. They are also allowed to send selective reports anytime manually.
- **Server Application**: Receives reports, validates integrity, and stores them securely.

The following data, system and network security aspects **must** be considered to ensure that the organisation's communication network and interaction between the SRS's client and server are secure.

➢ Designing the Client and Server Application

Client Application (Python)

The client-side application will run on remote machines and perform the following:

- Scan the log files automatically and allow to manually send it too.
- Encrypt the report using AES-256/RSA-2048. And Message integrity considered using SHA-512. Choose the most efficient yet secure method.
- Send the encrypted report to the server using a secure communication protocol.

Server Application (Python)

The server application will run centrally and:

- Receive the encrypted log report or any report from the client.
- Decrypt the report using the shared AES-256 key/RSA-2048.
- Validate the integrity of the report using SHA-512.
- Store the report securely for analysis.

➢ Network and Security Design

Dynamic Routing with Authentication

- E.g. OSPF with Authentication: use OSPF (Open Shortest Path First) as the dynamic routing protocol with MD5 authentication to ensure that only authorized routers can participate in routing.
- Routing Table Access: Only authenticated routers can access the network routing table, preventing unauthorized route injection.

Access Control Lists (ACLs)

- Allowlist specific IP addresses for clients and the server in the ACL configuration of the network firewall to restrict access to authorized nodes only.
- Block unauthorized nodes or other networks from accessing the server application by using strict ACL rules.

Port Security & VLAN

- Port Security: Allow only trusted MAC addresses to communicate over critical ports, limiting access to physical devices.
- VLAN Partitioning: Create VLANs to segment the network. Only the VLAN where MI6 devices (clients) and the server are located will have access to the server, ensuring isolation from other parts of the network.

➢ Ensuring Data Confidentiality, Integrity, and Availability

Data Confidentiality

- You can use AES-256 encryption to ensure that the communication between the client and the server is secure.
- RSA-2048 is used for securely sharing the AES-256 key between the client and server for encryption/decryption.

Data Integrity and Source Authentication

- Use SHA-512 to hash the threat report before sending it. The server will verify this hash to ensure the data hasn't been tampered with in transit. Create a digital signature to maintain non-repudiation and system authentication.

➢ Network Performance Metrics

To measure performance, you should test the system using different file sizes and key sizes and analyse the following:

Delay:

- Measure the round-trip time (RTT) for sending a report from the client to the server and receiving an acknowledgment.
- Average delay will be calculated by sending multiple reports and averaging the transmission time.

Throughput:

- Throughput is calculated by measuring the amount of data sent from the client to the server over a specified period (e.g., MB/s).
- This can be tested by sending reports of different sizes (e.g., 1MB, 10MB, 100MB) and calculating the rate at which the server receives the data.

➢ Validation and Testing

To ensure that the **Secure Reporting System (SRS)** is secure, you must perform the following validation and testing steps:

Penetration Testing

- Conduct penetration tests to simulate attacks on the network, such as unauthorized access, man-in-the-middle (MITM) attacks, and DoS attacks.

Functional Testing

- Verify that clients can securely send reports to the server and that the server can decrypt and store them securely.
- Ensure unauthorized clients cannot communicate with the server due to the ACL and port security measures.

Security Evidence

- Log attempts to access the server from unauthorized clients to show that the ACL rules are working correctly.
- Demonstrate data integrity, encryption, and decryption to prove that data confidentiality is maintained.

Performance Evidence

- Measure the delay and throughput metrics and compare them with expected performance.
- Provide logs showing the average delay and throughput for sending reports of different sizes.

Thus, this SRS ensures secure communication between remote MI6 machines and a central server. By using encryption (AES-256, RSA-2048), hashing (SHA-512), and implementing strict network security measures (ACLs, VLANs, port security, authenticated dynamic routing), we ensure that only authorized clients can communicate with the server, and the data is secure in transit. The system's performance should be measured in terms of delay and throughput and undergo rigorous testing to validate its security and performance.

2.2. How to Present and Demonstrate:

- You should set up your application for your assessment in ANY of the Cantor Networking and Cyber Labs and present your demonstration at the **allotted time**.

2.3. What to Submit and where and when (if not submitted then it will be deemed as failed)?

- You must submit a **README file with instructions**, **your network diagram**, **the source codes**, **network configuration details** in a single TEXT or Word document with relevant comments.
- You are NOT required to submit a report, but a document that contain the mentioned above information.
- You must submit on or before the assessment deadline of the Task 1 of this module.
- The Plagiarism score of source codes should NOT be more than 40%, otherwise it will be deemed FAILED. Similarity index score on network configuration can be ignored. It means that even if you use functions and code segments from internet, you must amend to fit the assessment requirements by re-defining the functions and variables.
- Note that if you copy paste codes from ChatGPT or GitHub then it will become evident during the demonstration if not picked-up by Turnitin. So, get help from these amazing online resources, but never simply copy paste, because it will become evident during the demonstration in the Lab.

2.5. Where to Deploy and Test?

The system you have developed have to be developed, tested and demonstrated in **the lab** and **NO simulation and Local execution (using loopback adapter) will be accepted.**

2.5. **When and where to present the demonstration?** It will happen during the last teaching week of the 1st semester. It will be conducted in a lab. At Cantor building. More detail information on group formation and presentation of the demonstration will follow.

3. Feedback Opportunities:

Formative (whilst you’re working on the coursework)

The lab sessions give you the opportunity to receive informal verbal feedback from your tutor regarding your development on the module and your work towards the assignment, so continue to ask question and engage in the class. In addition to these informal opportunities, there will be a drop-in session after middle of the semester to provide informal verbal feedback to improve your assessment.

Summative (after your presentation of demonstration is completed)

You will receive verbal feedback regarding your presentation and demonstration. Clearly, feedback provided with your coursework is an opportunity to reflect on your performance and for your development so that you can improve yourself for the next assessment or subject-related module.

Group Presentation and Demonstration Score Criteria:

Table 1: Group Presentation and Demonstration Score Criteria

	FAIL (Incompetent)	**THIRD (sufficient)**	**2.2 (Good)**	**2.1 (Very good)**	**1st**	**1st (Exceptional)**
Criteria and weighting	**Non-Submission: 0** **Low: 6-19** **Mid: 20-29** **Borderline: 30-39**	**Low: 40-43** **Mid: 44-46** **High: 47-49**	**Low: 50-53** **Mid: 54-56** **High: 57-59**	**Low: 60-63** **Mid: 64-66** **High: 67-69**	**Low:70-77** **Mid:78-84** **High:85-92**	**Exceptional 93-100**
Describing the Work Done: Aim and objectives. Level of completion of all the criteria listed in the assessment brief. Identify and explain all the network, system and data vulnerabilities and threats. Investigate, discuss, and assess all the threats and vulnerabilities in the application and network system development and conclusion. Explanation standard **50%**	The aim and objectives and how it were developed is not clear. The application built or developed is what is covered in the tutorial and there is no new component. Network and system security component is not complete, and the data security aspects is also not completed. The work has no clue on why and how the system, network or data security is maintained or design or identify. There is no discussion, no critical thinking in the process of addressing the problem. There is no valid conclusion. poorly designed and poorly explained.	Aim and objectives are clear, but not clear on how they were tested and what performance were analysed. The application developed is working, but there is no data security considered and there is limited network and system security considered. No context is given. There is very little evidence on the security threats and the issues and challenges that the assessment is looking for and there is very limited investigation and discussion. Presented the demo but explanation is not clear enough.	Aim and objectives are clear, some aspects on how they were tested and what performance were analysed is/are clear. The application developed is working, and some of the network security components are considered. However, it did not cover the all the aspects of data, system and network security provided in the assessment brief. Some of the security aspects are presented, but all the security aspect in terms of network, device and data security is not addressed. The discussion is available, but there is no in-depth study and critical reflection is weak. The explanation of the demonstration is good.	Aim and objectives are clear, most of the aspects on how they were tested and what performance were analysed is/are clear. The application developed is working, and most of the network security components are considered. However, it did not cover the all the aspects of data, system and network security provided in the assessment brief. The network, system and data security are done, but there is lack of in-depth analysis, have limited critical reflection during the explanation of the system. The explanation of the demonstration is very good with some insights.	Aim and objectives are clear, most of the aspects on how they were tested and what performance were analysed is/are clear. The application developed is working, and all the network security components are considered. It also covers all the aspects of data, system and network security provided in the assessment brief. The network, system and data security are considered. However, the wholistic system function is not captured like an expert but in-depth analysis is visible. The explanation of the demonstration is very good with clear insights.	Aim and objectives are clear, all of the aspects on how they were tested and what performance were analysed is/are clear at professional level. The application developed is working, and all the network security components are considered. It also covers all the aspects of data, system and network security provided in the assessment brief. The network, system and data security are considered and the wholistic picture is captured at an expert. Investigation, discussion, and in-depth analysis at as expert and the study is extensive. The explanation of the demonstration is very good with excellent insights.
Feedback:						
System Demonstration: Demonstration standard, Flow of the Demonstration, Understanding level. Wholistic view of the work and the level of expertise in capturing and demonstrating the work. **50%**	The demonstration quality is very poor and it’s very hard to understand what is demonstrated. The Demonstration standard is very poor and it’s very hard to understand how the activities are conducted. Flow of the Demonstration is weak and looks like there are not working as expected and the wholistic view of the aim is not achieved from the start and there is no added value and there is no evidence of expertise in the way demonstration was captured and no clear evidence on how the system was developed.	The demonstration quality is acceptable, but the demonstration but the flow of the Demonstration is very weak, and the understanding level of the work done is poorly captured in the demonstration process. The wholistic view of the work and the level of expertise in capturing and demonstrating the work is/are missing.	The demonstration quality is acceptable, but the demonstration standard is weak, because it is hard to follow and no clear evidence on how all the security mechanisms are considered. The flow of the Demonstration doesn’t capture all the security aspects in terms of data, system and network security. Some of the evidence of the work done are captured to some extent. The wholistic view of the work and the level of expertise in capturing and demonstrating the work is good.	The demo quality is good, and the demonstration, but the flow of the Demonstration is still weak, and the understanding level of the work done is captured at some level and the evidence of the work done are captured to some extent. The wholistic view of the work and the level of expertise in capturing and demonstrating the work is very good, except few aspects.	The Demo Quality is of high standard, and the flow of the Demonstration is good, and the understanding level of the work done is captured at high level and the evidence of the work done are captured very well. The wholistic view of the work and the level of expertise in capturing and demonstrating the work is very good.	The demo is of high standard, and presented like a highly skilled expertise, and the flow of the Demonstration is excellent, and the understanding level of the work done is captured at all levels of the demonstration and the evidence of the work done are captured excellently. The wholistic view of the work and the level of expertise in capturing and demonstrating the work is excellent.
Feedback:						
Overall mark:						

Appendix A: Peer-Feedback FORM

Secure Network Services and Application

(Individual self- and peer-assessment of Presentation and Demonstration)

Please complete the table below and assess your own and each of your group member's contribution to the group when undertaking and completing the Group Presentation, and Demonstration for the Secure Networking Technologies module. Please do not collaborate with anyone else when undertaking this assessment. Using the assessment criteria below I would like you to give yourself and each of your fellow group members a score out of 5 as follows:

Score	What the score means?
5	I (or the group member) made an outstanding contribution to the team throughout
4	I (or the group member) made an effective contribution overall and a particularly valuable contribution to the team in one or more areas
3	I (or the group member) made an effective contribution to the team
2	At times I (or the group member) made an effective contribution to the team, at other times less so, but overall the contribution was adequate
1	I (or the group member) made an ineffective contribution to the team - the contribution was a cause for concern

You can give as many group members as you like high or low scores – in any combination, but in allocating individual scores they will be averaged out to indicate how much more or less each individual contributed compared to the average. So giving everyone a '5' would have exactly the same effect on individual scores as giving everyone a '1'.

Group Letter or Number:	
Names of group members *(starting with your name first)*	*Score (out of 5)* *for contribution to the team*
Your Name:	

***** PS:** If the point difference is 1 and is marked consistently across the peers then 5 marks will be adjusted and if the point difference is 2 then 10 marks will be adjusted and for 3 or more-point difference then 15 marks will be adjusted in both the presentation and the demonstration scores, so do attempt to contribute equally so that this situation doesn't arise.

Level 5 - Generic grade descriptor: relationship of degree classification to Grade Point and equivalent percentage

Class	Category	Grade	Mark range	%	General Characteristics
1st	Exceptional 1st	16	93 - 100	96	Exceptional breadth and depth of knowledge and understanding of the area of study, **significantly beyond what has been taught in all areas**; evidence of extensive and appropriate selection and critical evaluation/synthesis/analysis and of reading/research beyond the prescribed range, in both breadth and depth, to advance work/direct arguments; excellent communication; performance beyond expectation. The ability to make decisions and carry out tasks/processes with autonomy; excellent leadership skills in group contexts; creative flair; extremely well-developed problem-solving skills; the ability to carry out sustained critical reflection on practical work within the wider context of industry/workplace. Fully meets expectations set by the industry/employment context.
1st	High 1st	15	85 - 92	89	Outstanding/excellent knowledge and understanding of the area of study as the student is **typically able to go beyond what has been taught (particularly for a mid/high 1st)**; evidence of extensive and appropriate selection and critical evaluation/synthesis/analysis of reading/research **beyond the prescribed range**, to advance work/direct arguments; excellent communication; performance deemed beyond expectation of the level. The ability to make decisions and carry out tasks/processes with autonomy; creative flair and the ability to (re)interpret predefined rules/conventions to select and justify individual working practice; highly developed problem-solving skills; accuracy and fluency; excellent command of skills appropriate to the task; the ability to reflect critically on practical work within the wider context of industry/workplace. Broadly meets expectations set by the industry/employment context.
	Mid 1st	14	78 - 84	81	
	Low 1st	13	70 - 77	74	
2.1	High 2.1	12	67 - 69	68	Very good knowledge and understanding of the area of study as the student is **typically able to relate facts/concepts together with some ability to apply to known/taught contexts**; evidence of appropriate selection and evaluation of reading/research, some beyond the prescribed range, may rely on set sources to advance work/direct arguments; demonstrates autonomy in approach to learning; strong communication skills. Broadly autonomous completion of practical tasks/processes; ability to adapt in response to change or unexpected experiences; technical/artistic decision making is highly developed; a clear command of the skills relevant to the task/process; ability to reflect on practical work and set future goals within the wider context of industry/workplace. Adherence to standards set by the industry/employment context.
	Mid 2.1	11	64 -66	65	
	Low 2.1	10	60 - 63	62	
2.2	High 2.2	9	57 - 59	58	Good knowledge and understanding of the area of **study balanced towards the descriptive rather than analytical**; evidence of appropriate selection and evaluation of reading/research but generally reliant on set sources to advance work/direct arguments; communication shows clarity, but structure may not always be coherent. A confident approach to practical tasks; a solid grasp of the related processes, tools, technology; creativity in the completion of the task; proficiency is demonstrated by an accurate and coordinated performance; tasks are completed with a good level of independent thought; some autonomy is evident; an ability to reflect on practical work and set future goals. General adherence to standards set by the industry/employment context.
	Mid 2.2	8	54 - 56	55	
	Low 2.2	7	50 - 53	52	
3rd	High 3rd	6	47 - 49	48	**Knowledge and understanding sufficient to deal with terminology, basic facts and concepts** but fails to make meaningful synthesis; some ability to select and evaluate reading/research however work may be more generally descriptive; strong reliance on available support set sources to advance work; arguments may be weak or poorly constructed; communication/presentation is generally competent but with some weaknesses. Competence in technical/artistic skills; tasks/processes are completed with a degree of proficiency and confidence; tasks are completed with a basic level of independent thought; effective judgements have been made; basic evaluation and analysis of performance in practical tasks is evident. Errors in workflow or completion of the task; general adherence to appropriate rules/conventions set by the industry/employment context.
	Mid 3rd	5	44 - 46	45	
	Low 3rd	4	40 - 43	40	
Fail	Borderline Fail	3	30 - 39	35	Insufficient knowledge and understanding of the subject and its underlying concepts; **some ability to evaluate given reading/research however work is more generally descriptive; naively follows or may ignore set material in development of work**; given brief may be only tangentially addressed or may ignore key aspects of the brief; communication shows limited clarity, poor presentation, structure may not be coherent. Practical tasks are attempted; skill displayed in some areas; there are a significant number of errors; a lack of proficiency in most areas; guidance may be needed to reproduce aspects of the task and/or apply learned skills. Tasks may be incomplete; failure to adhere to some of the rules/conventions set by the industry/employment context.
	Mid Fail	2	20 - 29	25	
	Low Fail	1	6-19	10	No evidence of knowledge or understanding of the subject; **no understanding of taught concepts, with facts being reproduced in a disjointed or decontextualised manner**; ignores set material in development of work; fails to address the requirements of the brief; lacks basic communication skills. A general level of incompetency in practical tasks; an evident lack of practice; set tasks are not completed; few or no skills relating to tasks are evident. No adherence to rules/conventions set by the industry/employment context.
Zero	Zero	0	0-5	0	Work not submitted, work of no merit, penalty in some misconduct cases.