ICTCYS407

Gather, analyse and interpret threat data

Assessment 3 of 5

Portfolio

Assessor Guide

SWINBURNE OPEN ED

Version 1

Assessment Instructions

Task Overview
This Portfolio assessment is divided into three (3) parts. Read the scenario in Part A and complete the associated tasks in Parts B and C. Portfolio tasks include completing simulated workplace documentation and/or templated written communication, such as emails.

Please type all responses into the spaces provided.

Important: Before commencing your work, you must update your *Student name* and *Student number* in the footer from **page 2** onwards.

Additional Resources and Supporting Documents
ICTCYS407_03_Portfolio_Scenario documents (compressed/zipped folder) - This folder contains the following scenario documents and templates required for completing the tasks in this assessment.

- AUS Retail_Email_template.docx
- AUS Retail_Simulated Network.pkt
- AUS Retail_Network device log collection procedure.pdf
- ISM - Guidelines for Gateways (September 2023).pdf
- ISM - Guidelines for System Monitoring (September 2023).pdf

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the Learning Platform. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:
- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Part A: Case study scenario

All tasks in this assessment refer to a simulated environment where conditions are typical of a work environment that is experienced in the cybersecurity threat analysis field of work. The scenario relates to a fictitious retail business organisation called '**AUS Retail**'.

Read the case study scenario carefully before completing the tasks in Part B.

A1. Company background

AUS Retail started as a single retail store based in Sydney, NSW. They now have retail store locations across several other states and territories in Australia, and the business continues to grow.

The increasing amount of reports on data breaches and security incidents in the online business space has raised many concerns for AUS Retail's management. Therefore, they want to ensure that security is paramount in their online retail system.

The management has specifically requested for a threat-hunting exercise to be conducted on their existing devices, security equipment, systems and data sources. Their requirement is to work towards a 'Maturity Level Three' implementation according to the 'Essential Eight Maturity Model'.

Your role

You work at AUS Retail as a **Cybersecurity Analyst**. You are responsible for gathering threat data from various sources, then analyse and interpret information for threats, inconsistencies and discrepancies.

You report to **David Smith** (Chief Security Officer, Email: David.Smith@ausretail.com.au), who is your manager at AUS Retail.

A2. Organisational policies, procedures and guidelines

You are provided with the following legislative requirements, organisational policies, procedures and document templates required for your job tasks.

- **AUS Retail_Email_template.docx** – This template must be used when drafting emails to AUS Retail's stakeholders.
- **AUS Retail_Network device log collection procedure.pdf** – provides guidelines on how to collect event logs from network devices.

Industry guidelines

- Guidelines for System Monitoring | Cyber.gov.au (Long URL: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring)
  PDF of this online version is included for reference in the resources folder provided:
  - ISM - Guidelines for System Monitoring (September 2023).pdf
- Guidelines for Gateways | Cyber.gov.au (Long URL: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-gateways)
  PDF of this online version is included for reference in the resources folder provided:
  - ISM - Guidelines for Gateways (September 2023).pdf

A3. Equipment and resources

To carry out the assigned job tasks in the cybersecurity threat analysis field of work you must have access to:

- a computer with a reliable internet connection
- an active Cisco Networking Academy (NetAcad) account (Go to https://www.netacad.com/ to create a new netacad student account if you do not already have one.)
- network simulation software 'Cisco Packet Tracer'
- other industry software packages such as:
    - Web browsing software (e.g. Microsoft Edge, Firefox, Chrome, Safari).
    - Microsoft Office software (e.g. WORD, PowerPoint, Excel).
    - A PDF reader.

A4. Simulated network environment

Logical network diagram

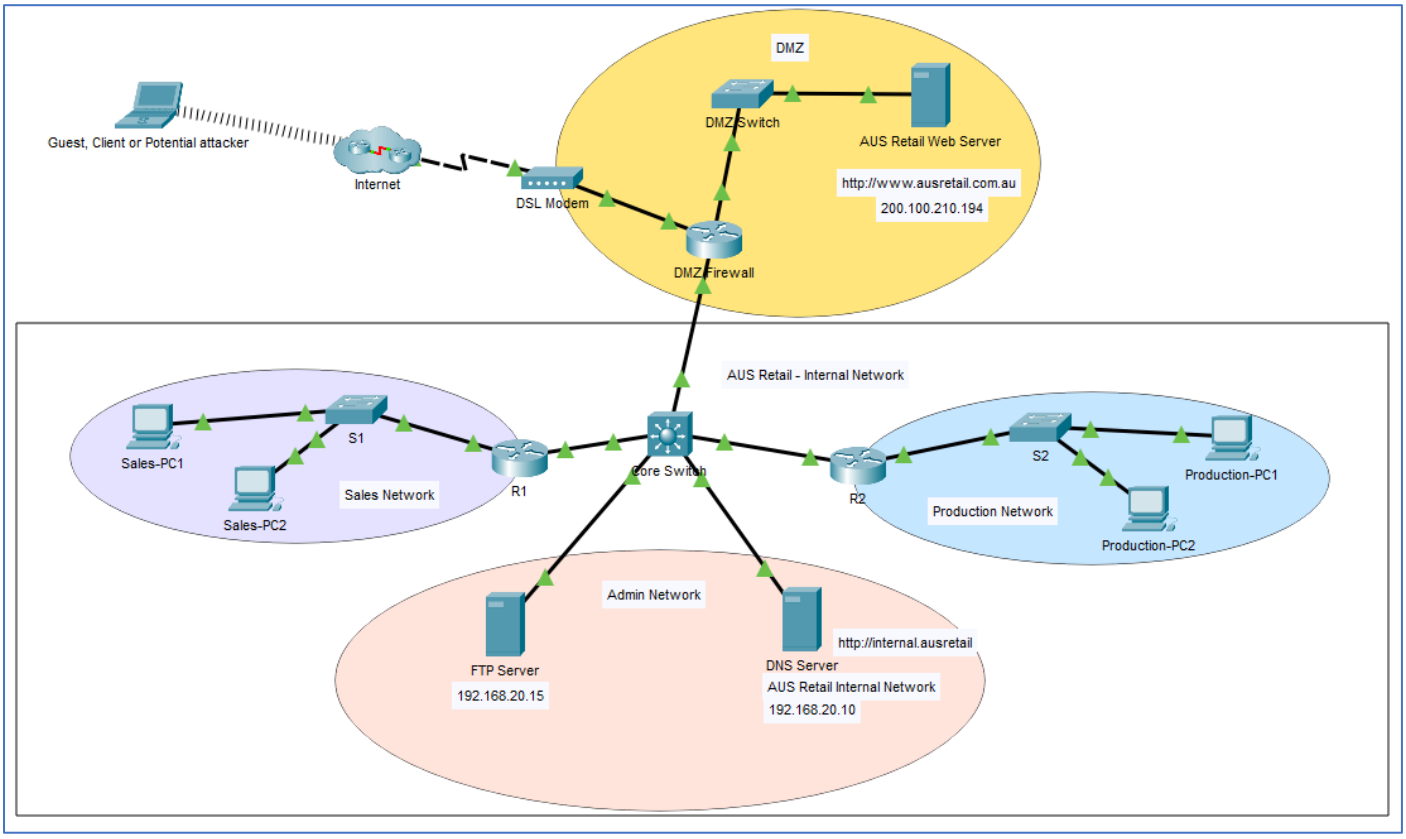


Figure 1 - AUS Retail Network Diagram © Cisco Packet Tracer

AUS Retail's current information system uses:

- multi-factor authentication on devices
- Microsoft Office applications and some Macro executions to perform operations
- PowerShell script executions to perform certain operations
- privileged access for group and account management.

Part B: Discuss data log requirements and investigation strategy

To complete this part of the assessment, you are required to:

- read the scenario in Part A and the organisational documentation provided
- discuss data log requirements for AUS Retail's network and the strategy to collect log data from various equipment and data sources via email.

Scenario:

Your manager had asked you to confirm the data log requirements for the analysis and the strategy you'll be using to process data.

The details of AUS Retail's network (logical diagram) and systems information are provided to you for reference. (See Part A, section A4).

Tasks:

Discuss and confirm the following with your Manager.

- **Data log requirements** – This should include any legislative requirements for log retention and other log requirements applicable for a 'Maturity Level Three' implementation according to the 'Essential Eight Maturity Model'.
- **The strategy to process data** – This should include information on how data needs to be collected, what tools to be used, and how it should be processed.

(Word count: 175 - 250 for the Email body of the sent email)

To complete this task, you are required to:

- email the information related to your discussion to the required personnel and confirm your understanding of the requirements.
- provide evidence of confirming data log requirements via email correspondence – You can use your student email for this and provide a screenshot of the sent email and the responses received confirming the requirements. (Use AUS Retail's standard email template).

Evidence of performing the task(s):

Provide here screenshot(s) of the sent and received emails.

Assessor instructions:

Students are likely to use different wording than the answer guidelines provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the answer guidelines
- use the organisation's email template for sent/received emails.

Students, in their sent email body, must include information that relates to a 'Maturity Level Three' implementation according to the 'Essential Eight Maturity Model' as well as mention any legislative requirements for log retention.

A sample answer is as follows.

- **Data log requirements** –These requirements may include, the following:
  - The need to record sufficient detail for each event logged, in order for it to be useful. For example, the date, time of the event, the relevant user or process, the relevant filename, the event description, and the ICT equipment involved should be recorded.
  - Event logs, excluding those for DNS services and web proxies, should be retained for at least seven years.

- Event logs for DNS services and web proxies are retained for at least 18 months.
- Configure a logging system to centrally log:
  - allowed and blocked execution events on workstations and servers
  - successful and unsuccessful multi-factor authentication events
  - allowed and blocked Microsoft Office macro execution events
  - blocked PowerShell script execution events
  - privileged access events
  - privileged account and group management events

- **Strategy to process data** – what data needs to be collected, what tools to be used, and how it should be collected and processed. For example, event logs can be
  - protected from unauthorised modification or deletion (e.g. use of encryption, secure storage options etc.)
  - monitored for signs of compromise and actioned when any signs of compromise are detected.
  - collected using centralised logging systems (e.g. Syslog server) or Security Information and Event Management solution to centrally capture all required logs.
  - When processing and analysing collected data, one needs to:
    - Analyse event logs in a timely manner to detect cyber security events and incidents.

Other answers for data log requirements may include:

- Event logs should be collected from cross-domain solutions, databases, DNS services, gateways, email servers, multifunction devices, operating systems, remote access services, security devices, server applications, system access, user applications, web applications and web proxies. These logs should be retained for a suitable period of time to facilitate threat-hunting and incident-response activities
- Use of an automated method of asset discovery at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities
- Use of a vulnerability scanner with an up-to-date vulnerability database for vulnerability scanning activities.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S	☐ NYS

Part C: Collect network security device logs

To complete this part of the assessment, you are required to:

- access the simulated network environment using 'Cisco Packet Tracer' software and by opening the 'AUS Retail_Simulated Network.pkt' file provided.
- gather and log security event and alert data from devices including a basic router, firewall and systems in the organisation's simulated network.
- follow organisational procedures when collecting logs and reported events

Scenario:

After considering the data log requirements, new equipment and several device configuration changes were made to the AUS Retail's network to centrally capture and store data logs from network security devices.

AUS Retail's network now includes a Syslog server and the critical network security devices are configured as Syslog clients. Therefore, the devices R1, R2, Core Switch, and DMZ Firewall in the network are configured to send their log entries (alerts, logs, reported events) to the syslog server.

The syslog server collects the log entries and allows them to be read using the 'NetFlow collector' which is a data recognition software tool.

Refer to the following AUS Retail's procedure when collecting data logs and reported events from the organisation's network security devices.

- 'AUS Retail_Network device log collection procedure.pdf'

Additionally, refer to information from the device manufacturers on how to interpret log messages from devices such as routers and firewalls:

- Cisco System Messages - Cisco System Messages Overview [Support] - Cisco (Long URL: https://www.cisco.com/c/en/us/td/docs/ios/system/messages/guide/consol_smg/sm_cnovr.html)

Tasks:

Do the following tasks to collect the required logs and event reports from the simulated network following organisational policies and procedures.

Task C1: Collect debug events from router 'R1'

Do the following in AUS Retail's simulated network environment following the relevant procedures where necessary.

a. Ensure that the 'NTP' service in the 'Access Control Server' is set to reflect the current date and time.

b. Turn on the Syslog service in the 'Syslog Server'.
Note: Have the Syslog service window open while doing the next sub-tasks (c and d).

c. Enable debugging to collect NTP information from the 'R1' router.
Observe the 'Syslog Server' window for log entries that will begin to appear. Ensure that the log message reflects the correct date and time. (Note: You may have to wait a few minutes until the NTP packets start to reflect the correct time.)

d. Enable debugging to collect EIGRP protocol information from the 'R1' router.

e. Observe the 'Syslog Server' window for log entries that will begin to appear. When you have captured the required types of debug messages, turn 'Off' the syslog service to stop capturing the messages. Note: Do not clear the log.

f. Provide evidence of the Syslog service window with captured log events (showing EIGRP and NTP) from the router 'R1', under 'Evidence of performing task C1'.

g. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. IP addresses, timestamps, device interface numbers etc.).

(Word Count: 60-100 words)

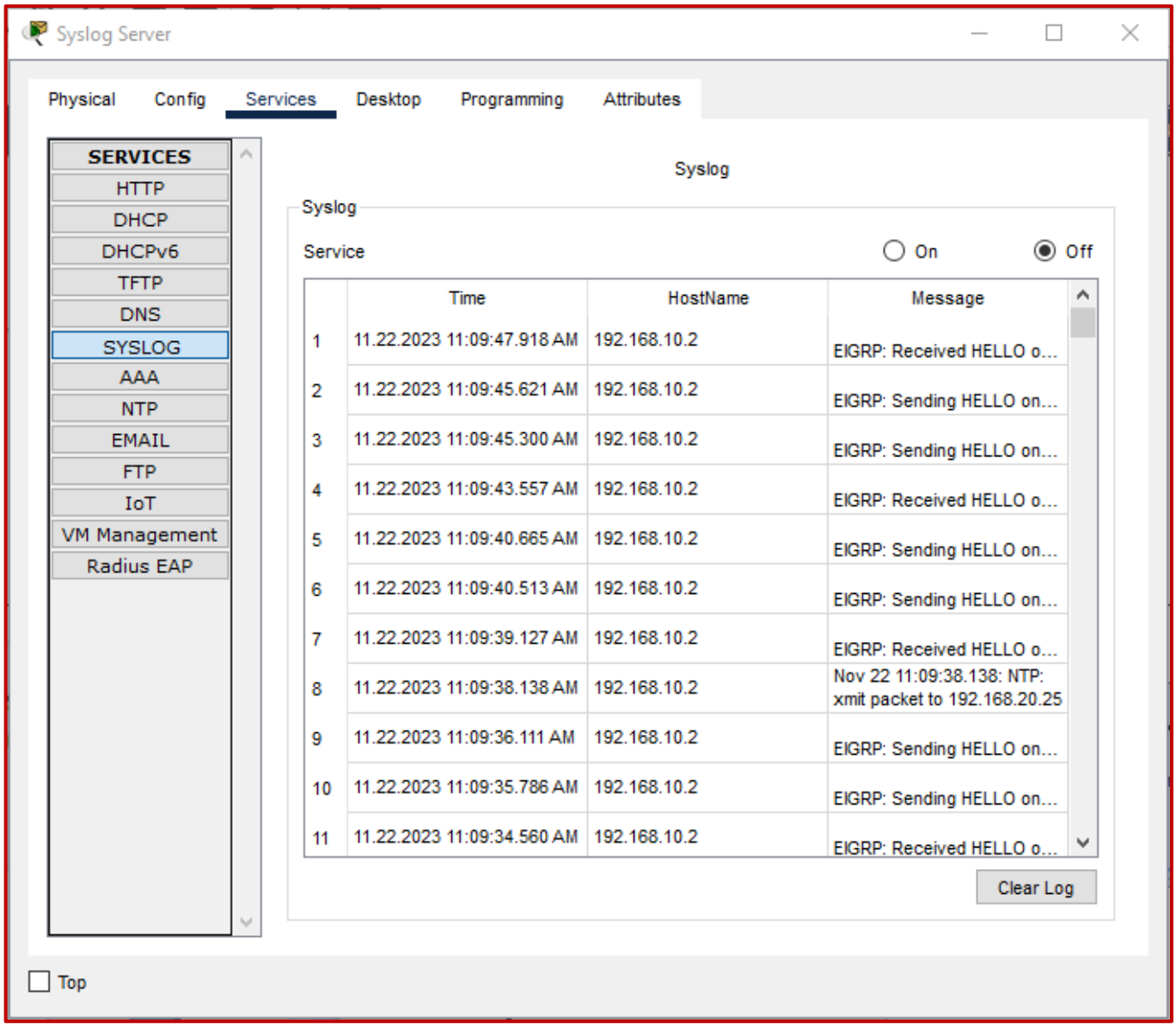
Evidence of performing task C1:

Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide evidence of the data logs collected from the router in the form of a screenshot.
- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, device interface numbers etc.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The data logs include:

- Time stamps of exact date (22nd November 2023) and time (around 11AM) of the logs collected,
- the hostname/ IP address (e.g. 192.168.10.2) from which the logs are generated from
- details of the eigrp packets sent/received (e.g. HELLO)
- details of the ntp information from ntp server at 192.168.20.25
- device interfaces from which packets were sent/received (e.g. GigabitEthernet0/0, GigabitEthernet0/1)

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C2: Collect user access event logs from router 'R2'

Router 'R2' is configured with the TACACS+ protocol which allows remote authentication through a centralised server. In this task, you will attempt to log in to 'R2' with login credentials and then collect user access event logs by accessing the 'AAA Accounting service records'.

a. From the 'Access Control Server', access 'Desktop' > 'AAA Accounting'. Keep the 'AAA Accounting Records' window open and do the rest of the sub-tasks.
Note: Observe the 'AAA Accounting Records' window for any log entries upon completing each of the following sub-tasks.

b. Go to 'R2' router's 'CLI' tab and press 'Enter'.
Here, R2 will ask for the username and password to be entered before granting access to its command line interface. Use the following credentials to log in to the router:
    a. Username: cyberanalyst
    b. Password: security15KEY

c. Logout from the 'R2' router's CLI by typing 'logout'.

d. Attempt to log in to 'R2' router's CLI using the following false credentials:
    - Username: Attacker
    - Password: some incorrect password

Note: Keep entering the above false credentials at least three (3) times.

h. Provide evidence of the 'AAA Accounting Records' window showing the captured user access log events from the router 'R2', under 'Evidence of performing task C2'.

i. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. timestamps, IP addresses etc.). You may include portions of the debug messages in your answer. (Word Count: 60-100 words)

Evidence of performing task C2:

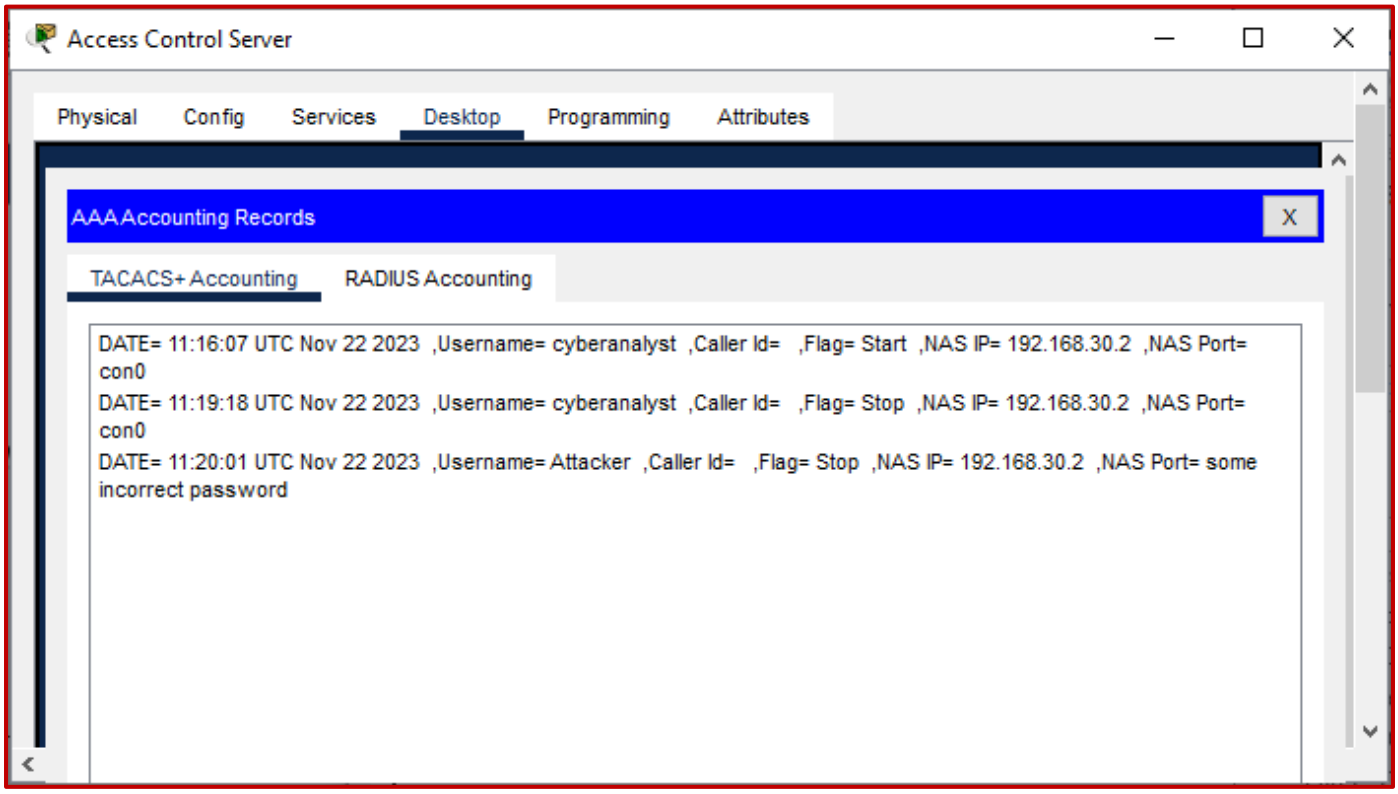
Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide evidence of the data logs collected from the router in the form of a screenshot.

- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, etc.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The data logs include:

- Time stamps of the date/time of when the event occurred.
- The username and password used
- The IP address of the host device (R2's IP address 192.168.30.2) from which the login attempt occurred.
- 'Start' flag indicates the time of login by the 'cyberanalyst' user and the 'Stop' flag indicates the time the user logged out. For example:
- Upon third time of the incorrect login attempt by the 'Attacker' was recorded with a 'Stop' flag with the incorrect password included in the log as plain text.

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C3: Collect and visualise network flow logs

In this task, you will use the data recognition software 'Netflow Collector' in the 'Syslog Server' to collect and visualise the network logs.

In the 'Syslog Server', go to the 'Desktop' tab, > 'Netflow Collector' service, and turn it 'On'. Keep this window opened and do the following:

a. From any PC on AUS Retail's internal network, ping the AUS Retail web server's IP address.
b. Observe the data visualisation in the 'Netflow Collector' window.
c. Select the wedge of the Pie chart that displays details of the traffic flow relevant to the web server ping request.
d. Provide evidence of the 'Netflow Collector' window with details of the captured network flow event under 'Evidence of performing task C3'.
e. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. timestamps, IP addresses, statistics of data traffic flows etc.)
(Word Count: 60-100 words)

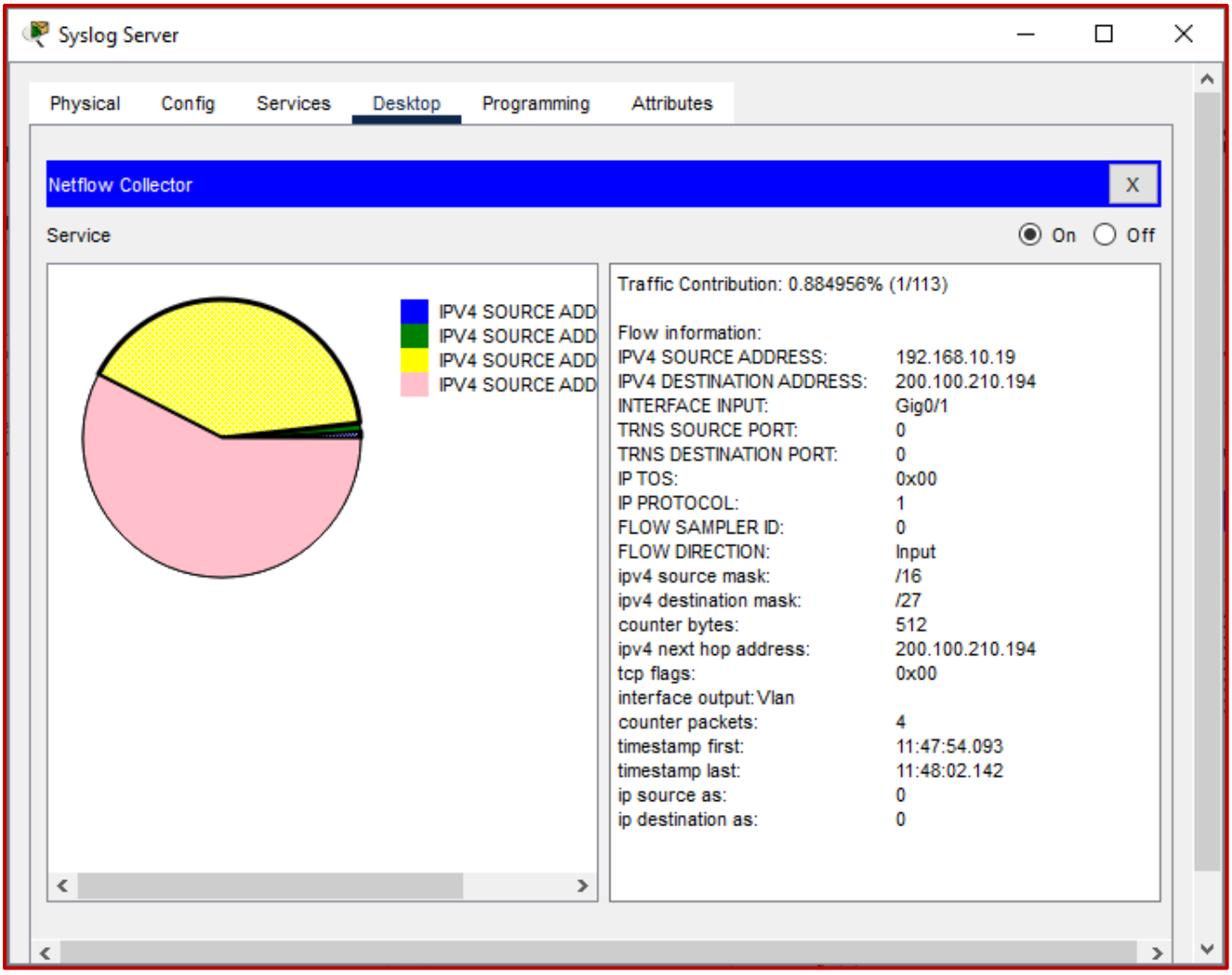
Evidence of performing task C3:

Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide a screenshot as evidence of the data logs collected from the 'Netflow Collector'.
- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, traffic contribution %, etc.
- the pie chart displayed will vary based on the traffic on the simulated network. As other packet flows such as eigrp, ntp and other traffic are being sent between devices, NetFlow will continue to capture these packets and export statistics to the NetFlow Collector. Therefore, the longer NetFlow is allowed to run on the network simulation, the more traffic statistics will be captured.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The particular traffic category selected from the pie chart representation accounts for 0.8849% of the total traffic collected.

The details of the logged data include:

- Time stamps of the date/ time of when the event occurred.
- Source IP addresses (192.168.10.19) Sales-PC2 and destination IP address of the web server (200.100.210.194)
- Interface input number G0/1
- No. of counter packets (4) as the ping/echo message sends out 4 requests/replies.

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S ☐ NYS

Appendix 1: Assessment submission checklist

Submit a PDF version of this completed assessment document. Make sure you have also included each of the following files as evidence of your performance. Remember to create a compressed folder for each module before uploading them for submission

Part B: Discuss data log requirements and investigation strategy		
1	Drafted email and responses to and from the required personnel discussing log requirements and strategy for data processing.	☐
Part C: Collect network security device logs		☐
C1	Screenshot of the captured data logs from router 'R1' Interpretation of the log data collected (brief description).	☐
C2	Screenshot of the captured data logs from router 'R2' Interpretation of the log data collected (brief description).	☐
C3	Screenshot of the captured data logs from network devices using the data recognition software 'Netflow Collector'. Interpretation of the log data collected (brief description).	☐

Assessment feedback

Assessors are to indicate the assessment outcome as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S ☐ NYS

Congratulations, you have reached the Assessment 3!