ICTSAS530

Use network tools

Assessment 6 of 6

Project

Assessor Guide

Version 1

Assessment Instructions

Task Overview

This Project assessment is divided into five (5) parts. Read the simulated environment set-up and resource information in Part A and complete the associated tasks in Parts B, C, D and E. Project tasks include completing documentation and/or templated written communication, such as emails.

Please provide all required screenshot evidence and written responses in 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

ICTSAS530_06_Project_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_Report_template.docx
- AUS Retail_Records management policy.pdf
- AUS Retail_Stakeholder communication policy.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: Project scenario

All tasks in this assessment refer to a simulated environment where conditions are typical of a work environment that is experienced in the information and communications technology (ICT) 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

- **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 company manages a large volume of sensitive data, including customer information, financial transactions, inventory details, and employee records. To ensure the security of this data and maintain the trust of its customers, AUS Retail needs to implement robust network security measures.

- **Your role**

You work at AUS Retail as a **Network Administrator.** You are responsible for selecting, operating and testing an array of networking tools to maintain the network security of the existing network.

- **Project sponsors and key stakeholder contacts**

The key project sponsors are the following AUS Retail stakeholders to whom you must directly report regarding the project's progress.

  - Chief Information Security Officer (CISO): (David.Smith@ausretail.com.au)
  - IT Systems and Security Manager: Alex Dawson (Alex.Dawson@ausretail.com.au)

A2. Equipment and resources

To carry out the assigned job tasks, you must have access to:

- a computer installed with an operating system
- a reliable internet connection
- industry software packages such as:
  - Web browsing software (e.g. Microsoft Edge, Firefox, Chrome, Safari)
  - Microsoft Office software (e.g. WORD, Excel)
  - A PDF reader

A3. Organisational policies and procedures

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

- **AUS Retail_Email_template.docx** - This template is referred to in the 'AUS Retail_Stakeholder communications policy.pdf' and must be used when drafting emails to AUS Retail's stakeholders.
- **AUS Retail_Report_template.docx** – This report template should be used when reporting on the risk analysis findings and recommendations within the organisation's systems.

- **AUS Retail_Stakeholder communications policy.pdf** – includes organisational procedures, communication protocols and standards used when engaging with key stakeholders in the organisation and also includes records management, document access and sharing procedures.

Part B: Create risk analysis report

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

- refer to the relevant organisational templates outlined in Part A, section A3 of this assessment
- refer to the risk analysis findings from the previously completed portfolio assessment (ICTSAS530_05_Portfolio.docx)
- record textual and numerical data in a format specific to requirements.
- use problem-solving techniques to analyse outcomes and manage networks

Scenario:

You have previously conducted tests using a variety of network tools and have gathered threat data for risk analysis.

You are now tasked with documenting the risk analysis findings in a formal report according to the organisation's reporting structure and layout.

Tasks:

Create a report documenting the risk analysis findings using the AUS Retail's report template.

Your report must include the following:

B1. A summary of the risk analysis tests conducted using (at least three) different types of network tools. (Word count: 40-65 words for each tool)

Note: You may include screenshots of the test results where applicable.

B2. Distinguish the features between the three (3) different types of industry-recognised network tools used to conduct tests and outline how each can be used to maintain high-security networks (word count: 75-100 words for each tool).

B3. An outline of the network vulnerabilities and issues identified (word count: 100-125 words).

B4. Recommendations of computer safeguard guidelines according to the risk analysis findings (word count: 150-200 words).

Evidence of performing the task(s):

IMPORTANT: You must upload a copy of your completed threat analysis report with this assessment document for marking.

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

Assessor comments: ☐ S ☐ NYS

The student must demonstrate learning skills by identifying applicable organisational procedures for creating reports.

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 report template.

A sample answer is provided below.

AUS Retail

Risk analysis report

Report prepared by: <Student Full Name> [Network Administrator at AUS Retail]

Date: <dd/mm/yyyy>

Contents:

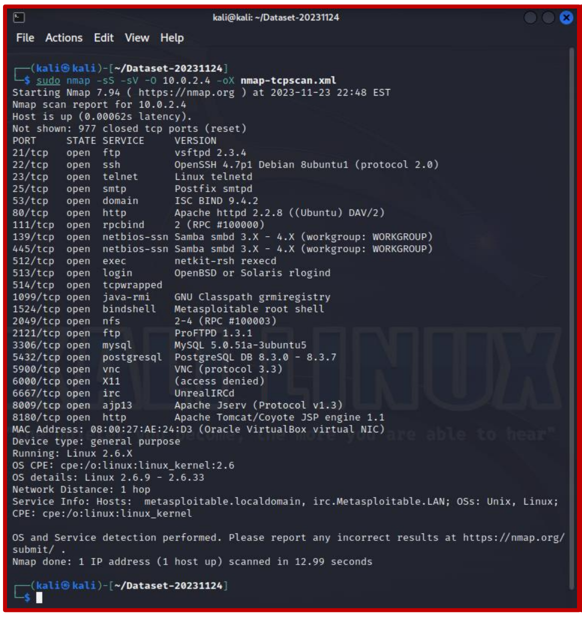
1. Tests conducted and tools used

Nmap, Nikto, and OWASP ZAP are all tools used for different aspects of network and web application security testing. Here's a brief overview of each tool and how they can be used to maintain high-security networks:

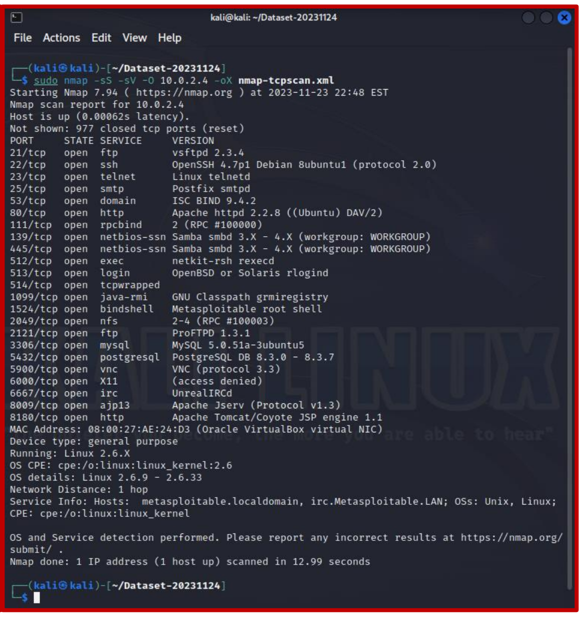
1.1 Network scan using 'nmap'

Nmap is a powerful network scanning tool used for discovering hosts and services on a computer network.

TCP and UDP port scans conducted using nmap results helped identify whether any unwanted ports are open that are not required for the operation of the web server (port 80, 443 are the required ports, anything else is not necessary and should be closed).



```
┌──(kali㉿kali)-[~/Dataset-20231124]
└─$ sudo nmap -sS -sV -O 10.0.2.4 -oX nmap-tcpscan.xml
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-23 22:48 EST
Nmap scan report for 10.0.2.4
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:AE:24:D3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds

┌──(kali㉿kali)-[~/Dataset-20231124]
└─$
```

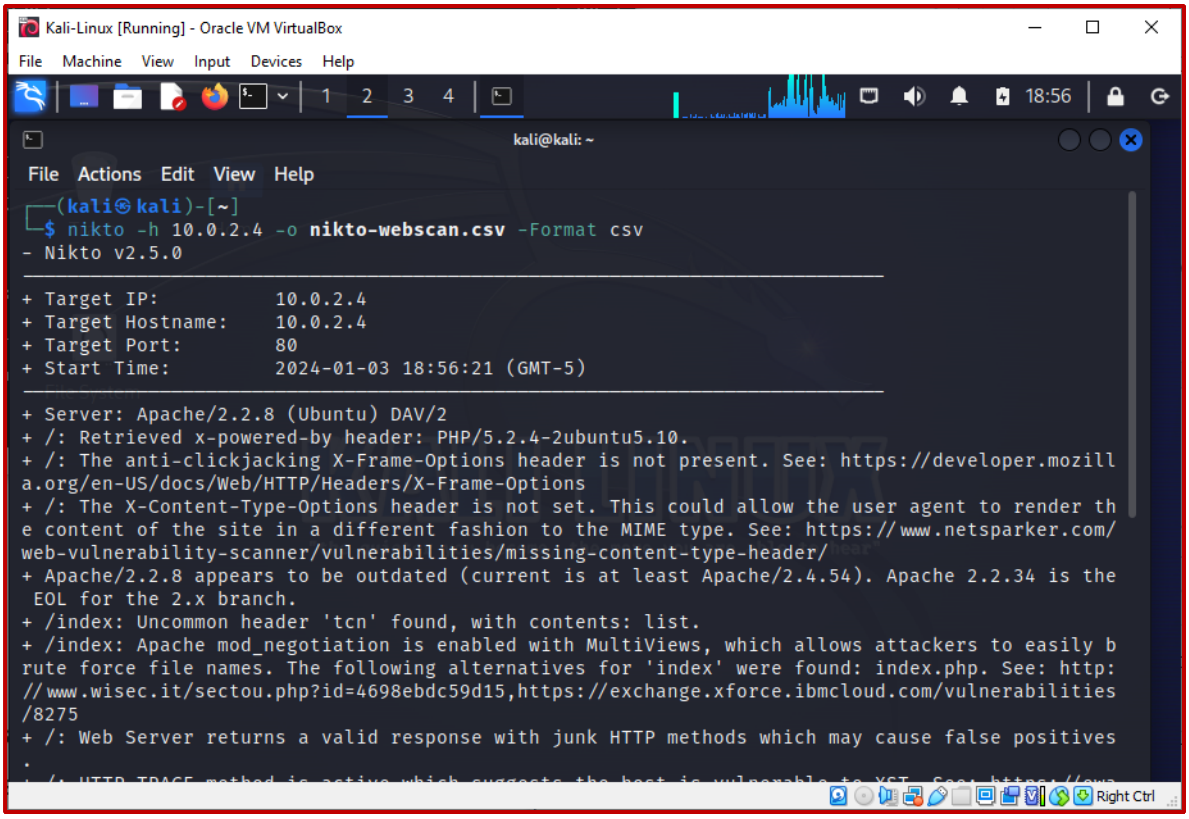


```
┌──(kali㉿kali)-[~/Dataset-20231124]
└─$ sudo nmap -sS -sV -O 10.0.2.4 -oX nmap-tcpscan.xml
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-23 22:48 EST
Nmap scan report for 10.0.2.4
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:AE:24:D3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds

┌──(kali㉿kali)-[~/Dataset-20231124]
└─$
```

1.2 Web server scan using ‘nikto’

Nikto is a web server scanner that performs comprehensive tests against web servers for multiple items, including dangerous files/CGIs, outdated server software, and other potential vulnerabilities.

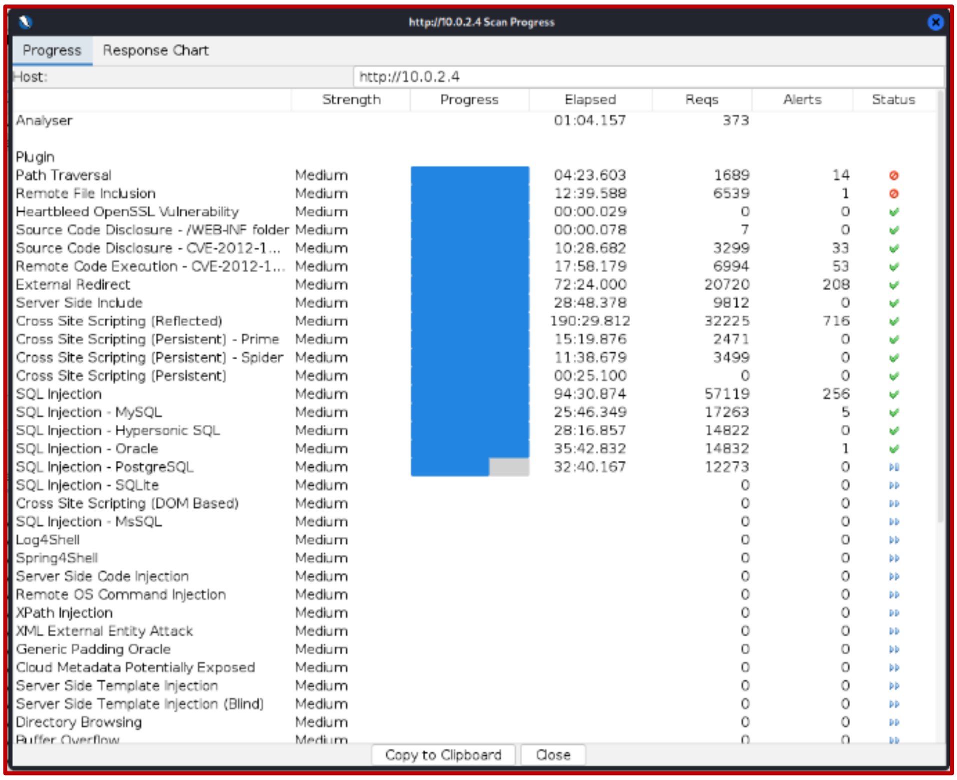
Using the tool ‘nikto’ helps to identify details of the web service [scanning the web host 10.0.2.4 specifically the http port 80]



Kali-Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:56
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.0.2.4 -o nikto-webscan.csv -Format csv
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.4
+ Target Hostname:    10.0.2.4
+ Target Port:        80
+ Start Time:         2024-01-03 18:56:21 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozill
a.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render th
e content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/
web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the
 EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily b
rute force file names. The following alternatives for 'index' were found: index.php. See: http:
//www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities
/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives
.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owa
```

1.3 Web application vulnerability scan using ‘OWASP-ZAP’



```
Host: http://10.0.2.4
                                         Strength   Progress   Elapsed      Reqs    Alerts  Status
Analyser                                                       01:04.157     373

Plugin
Path Traversal                           Medium                04:23.603    1689      14     ⊘
Remote File Inclusion                    Medium                12:39.588    6539       1     ⊘
Heartbleed OpenSSL Vulnerability         Medium                00:00.029       0       0     ✓
Source Code Disclosure - /WEB-INF folder Medium                00:00.078       7       0     ✓
Source Code Disclosure - CVE-2012-1...   Medium                10:28.682    3299      33     ✓
Remote Code Execution - CVE-2012-1...    Medium                17:58.179    6994      53     ✓
External Redirect                        Medium                72:24.000   20720     208     ✓
Server Side Include                      Medium                28:48.378    9812       0     ✓
Cross Site Scripting (Reflected)         Medium               190:29.812   32225     716     ✓
Cross Site Scripting (Persistent) - Prime  Medium              15:19.876    2471       0     ✓
Cross Site Scripting (Persistent) - Spider Medium              11:38.679    3499       0     ✓
Cross Site Scripting (Persistent)        Medium                00:25.100       0       0     ✓
SQL Injection                            Medium                94:30.874   57119     256     ✓
SQL Injection - MySQL                    Medium                25:46.349   17263       5     ✓
SQL Injection - Hypersonic SQL           Medium                28:16.857   14822       0     ✓
SQL Injection - Oracle                   Medium                35:42.832   14832       1     ✓
SQL Injection - PostgreSQL               Medium                32:40.167   12273       0     ▸▸
SQL Injection - SQLite                   Medium                                0       0     ▸▸
Cross Site Scripting (DOM Based)         Medium                                0       0     ▸▸
SQL Injection - MsSQL                    Medium                                0       0     ▸▸
Log4Shell                                Medium                                0       0     ▸▸
Spring4Shell                             Medium                                0       0     ▸▸
Server Side Code Injection               Medium                                0       0     ▸▸
Remote OS Command Injection              Medium                                0       0     ▸▸
XPath Injection                          Medium                                0       0     ▸▸
XML External Entity Attack               Medium                                0       0     ▸▸
Generic Padding Oracle                   Medium                                0       0     ▸▸
Cloud Metadata Potentially Exposed       Medium                                0       0     ▸▸
Server Side Template Injection           Medium                                0       0     ▸▸
Server Side Template Injection (Blind)   Medium                                0       0     ▸▸
Directory Browsing                       Medium                                0       0     ▸▸
Buffer Overflow                          Medium                                0       0     ▸▸
```

OWASP ZAP is an open-source web application security scanner used for finding security vulnerabilities in web applications during the development and testing phases.

The output of the scan provide detailed information on the alerts captured. These alerts are classified into risk level priority.

1.4 Differentiation between the types of tools used

Criterion	Nmap	Nikto	OWASP-ZAP
Features	**Port scanning:** Nmap can identify open ports on target systems, which helps in understanding the network's topology and potential attack vectors. **Service detection:** It can detect the services running on discovered ports, providing information about the software versions and configurations. **OS detection:** Nmap can attempt to determine the operating system of the target hosts based on various characteristics.	**Checks for outdated software versions:** Nikto identifies old versions of web server software and known vulnerabilities associated with them. **Checks for common misconfigurations:** It looks for common web server misconfigurations that could lead to security vulnerabilities. **Identifies potentially dangerous files:** Nikto scans for potentially dangerous files and CGI scripts that may be accessible on the web server.	**Automated scanning:** ZAP can perform automated scans of web applications to identify common security vulnerabilities such as cross-site scripting (XSS), SQL injection, and insecure configurations. **Manual testing capabilities:** It provides tools for manual testing, allowing security professionals to interact with web applications and analyze their behavior for vulnerabilities. **API support:** ZAP offers API support for integration with other security tools and processes.
Use in high-security networks	Nmap can be used to regularly scan the network for any unauthorised or unexpected services running on hosts. It helps in identifying potential vulnerabilities and misconfigurations that could be exploited by attackers.	Nikto can be used to regularly scan web servers and web applications within the network for vulnerabilities and misconfigurations. It helps in identifying and remediating potential security weaknesses before they can be exploited by attackers.	OWASP ZAP is valuable for assessing the security of web applications deployed within the network. Regular scans with ZAP can help identify and remediate vulnerabilities in web applications, reducing the risk of successful attacks targeting those applications.

2. Network vulnerabilities

According to the results obtained from the web server scan, the nikto tool had identified vulnerabilities such as:

- outdated web server software (Apache)
- 'The X-Content-Type-Options header is not set' – The result further states that this could allow the user agent to render the content of the site in a different fashion to the MIME type. The results also provide useful references to the type of vulnerability found.

The network vulnerability scan conducted using OWASP-ZAP captured a total of 31 alerts, out of which 10 are high risk, 6 medium risks and 8 low risk. The high risks include vulnerabilities for:

- Cross-site scripting (706 alerts)
- External Redirect (208 alerts)
- Hash disclosure MD5 crypt
- Path traversal
- SQL injection
- Remote code execution
- Remote file inclusion

3. Computer safeguard guidelines

Implementing these safeguard guidelines can significantly enhance the security posture of the network and mitigate the risks associated with the mentioned vulnerabilities. Regular security assessments and updates should be performed to ensure ongoing protection against emerging threats.

Outdated web server software (Apache):

- Regularly update the Apache web server software to the latest stable version released by the Apache Software Foundation.
- Employ a system to monitor for new updates and security advisories related to Apache software.
- Establish a patch management process to apply security patches promptly after they are released.
- Use vulnerability scanning tools to identify outdated software versions and prioritise updates accordingly.

Cross-site scripting (XSS):

- Implement strict input validation on both client and server sides to prevent malicious input from being processed.
- Encode user-controlled data before rendering it to prevent it from being interpreted as code.
- Implement a Content Security Policy to restrict the sources from which content can be loaded on web pages.

SQL injection:

- Use parameterised queries or prepared statements in database interactions to prevent SQL injection attacks.
- Validate and sanitise user input before using it in SQL queries.
- Limit the database user's permissions to only what is necessary for its intended functionality.

Part C: Digitally store documentation

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

- refer to the relevant organisational policies and procedure documents outlined in Part A, section A3 of this assessment
- use the risk analysis report you created in Part B of this assessment
- store threat data documentation to key stakeholders following organisational policy and procedure.

Scenario:

You have created a threat analysis report documenting the results and findings. Now you are tasked with storing the documentation according to the organisation's records management policy and procedures outlined in section 2 of the 'AUS Retail_Records management policy.pdf'.

Tasks:

Rename and save the risk analysis document appropriately according to the organisation's records management procedure.

Note: Assume that your Student account's OneDrive is the organisation's cloud storage. Create a folder in your OneDrive called 'AUS Retail' and demonstrate how you would store the risk analysis documentation within this folder. Provide a screenshot as evidence of storing the documentation under 'Evidence of performing the task(s)'.

Evidence of performing the task(s):

Provide here a screenshot(s) showing how risk analysis documentation is stored.

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

Assessor comments: ☐ S ☐ NYS

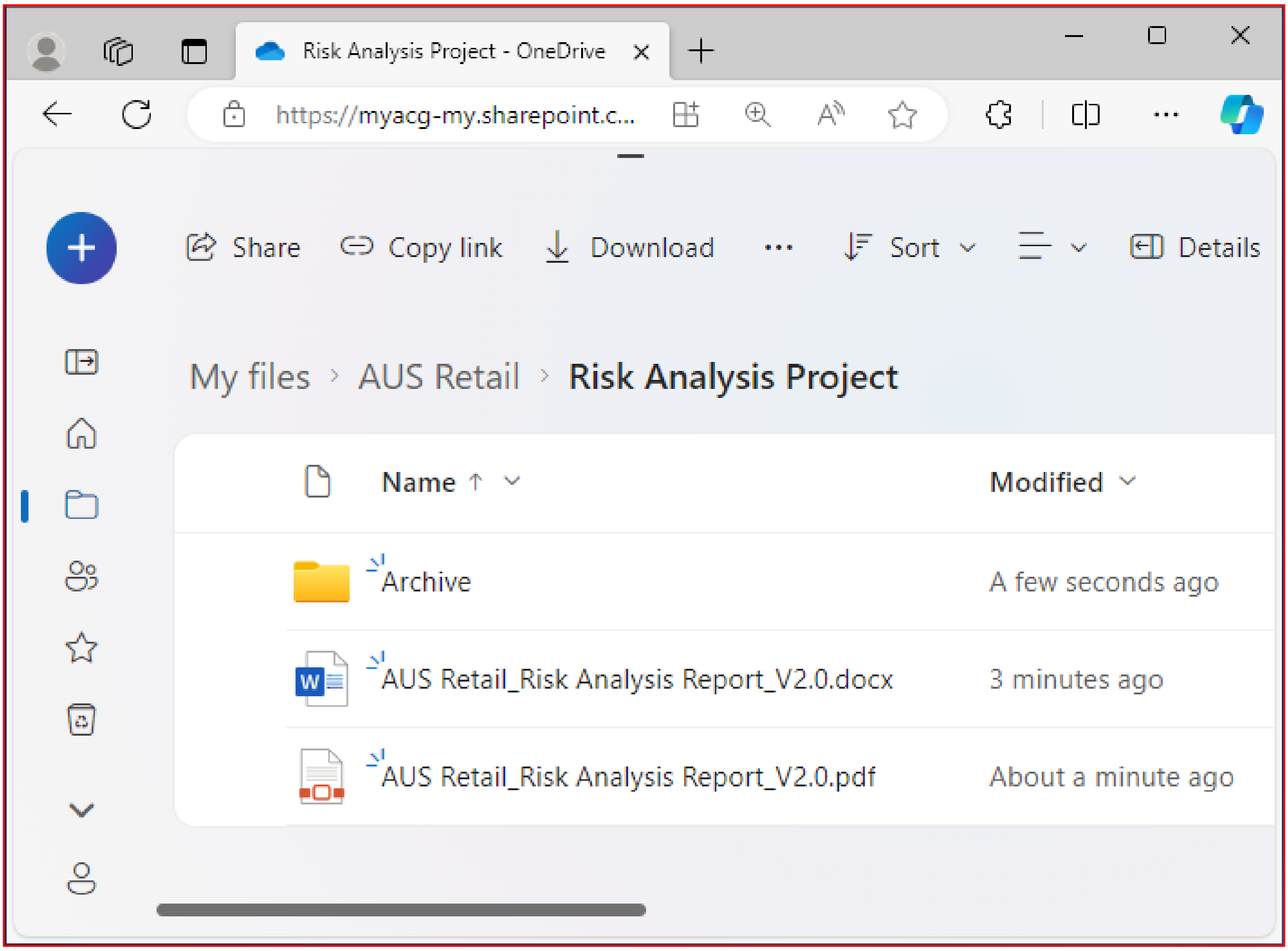
The screenshot provided by the student should indicate a folder structure on the student's **OneDrive** cloud storage, similar to the following, to show that they have followed the organisation's policies and procedures for storing documents. Note: The version number (e.g. V1.0, V2.0) may differ depending on the document revisions the student would have worked on before the final version is created.

A sample answer is provided below.

AUS Retail_Risk Analysis

Archive

- AUS Retail_Risk Analysis Report_V1.0.docx
- AUS Retail_Risk Analysis Report_V2.0.docx
- AUS Retail_Risk Analysis Report_V2.0.pdf


Risk Analysis Project - OneDrive
https://myacg-my.sharepoint.c...
Share
Copy link
Download
Sort
Details

My files › AUS Retail › Risk Analysis Project

Name ↑	Modified
Archive	A few seconds ago
AUS Retail_Risk Analysis Report_V2.0.docx	3 minutes ago
AUS Retail_Risk Analysis Report_V2.0.pdf	About a minute ago

Part D: Control access to digitally stored documentation

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

- refer to the relevant organisational policies and procedure documents in Part A, section A3 of this assessment
- use the threat data analysis report you have stored in Part F of this assessment
- distribute threat data documentation to key stakeholders following organisational policy and procedure.

Scenario:

You have prepared a risk analysis report and have stored it in the cloud storage according to AUS Retail's policies and procedures.

The key stakeholders, David Smith (Chief Security Officer) and Alex Dawson (IT Systems and Security Manager), have requested you send them a copy of the completed risk analysis report for reference.

To ensure the key stakeholders can access the distributed document, you will follow AUS Retail's document access and sharing policy and procedures outlined in section 3 of the 'AUS Retail_Records management policy.pdf'.

Tasks:

Distribute the threat data analysis report to the key stakeholders following organisational policy and procedures.

To demonstrate completion of this task, you must provide a screenshot showing the share settings of the document. The captured screenshot must provide evidence that you are:

- sharing the document with the key stakeholders
- granting only the required level of access to the key stakeholders
- including a brief message to provide context to the shared document (Word count: 25 – 35 words).

Evidence of performing the task(s):

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

Assessor comments: ☐ S ☐ NYS

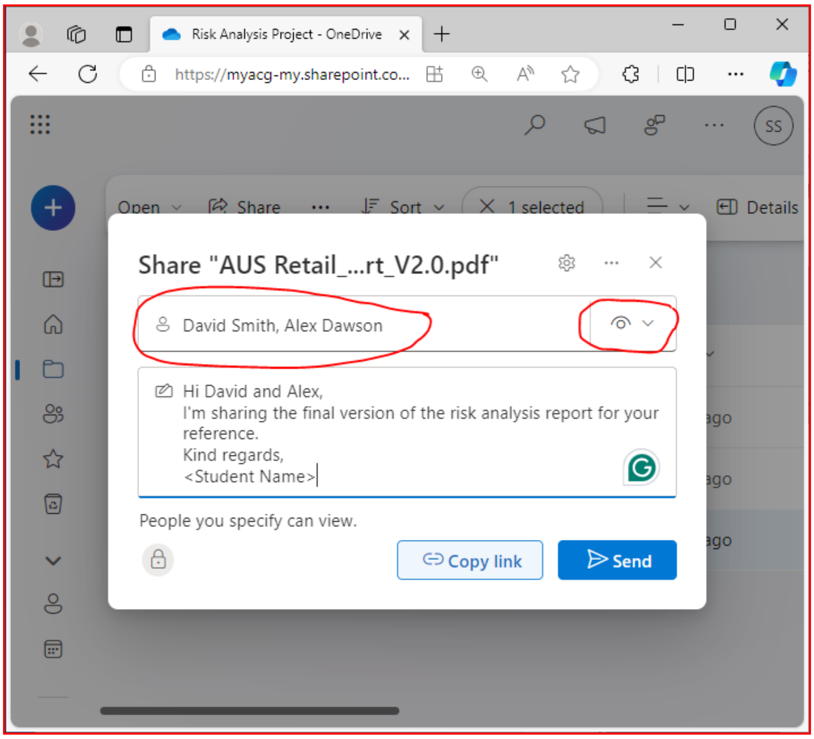
The student must demonstrate:

- learning skills by identifying applicable organisational procedures for distributing threat data documentation
- distributing the threat analysis report via cloud storage share settings
  - addressing the relevant personnel (David Smith and Alex Dawson)
  - providing 'View' only access
  - including a clear short message indicating what the document is and why it is shared.

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

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

A sample answer is provided below.


Risk Analysis Project - OneDrive
https://myacg-my.sharepoint.co...
SS
Open
Share
Sort
1 selected
Details
ago
ago
ago

Share "AUS Retail_...rt_V2.0.pdf"

David Smith, Alex Dawson

Hi David and Alex,
I'm sharing the final version of the risk analysis report for your reference.
Kind regards,
<Student Name>

People you specify can view.

Part E: Report issues and present recommendations

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

- read the scenario in Part A
- refer to the organisational documentation and guidelines for using organisational templates
- refer to the risk analysis report stored and made accessible in Parts B, C and D of this assessment
- present project sponsors your recommendations as a result of the risk analysis via email.

Task:

Draft an email addressing the AUS Retail stakeholders (project sponsors) presenting them with a summary of the recommendations along with a link to access the final PDF version of the risk analysis report.

Important: When drafting the email, you must:

E1. report issues identified as a result of the running command-line tools

E2. present a summary of your recommendations as a result of the risk analysis findings within the body of the email

E3. include a OneDrive link to access the PDF version of the risk analysis report

E4. use AUS Retail's standard email template to draft the email.

(Word count: 165 – 200 words in the email body).

Portfolio of evidence: *(Drafted email to project stakeholders)*

Draft your email in the space given below.

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

Assessor comments:	☐ S ☐ NYS

The student must present their recommendations to the stakeholders via email.

Student responses are likely to include different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit (for the email body)
- reflect the characteristics described in the exemplar answer

A sample answer is provided below.

Lastname, Firstname
From: Lastname, Firstname
Sent: Monday, 22nd February 2024 4:00 PM
To: David Smith (David.Smith@ausretail.com.au), Alex Dawson (Alex.Dawson@ausretail.com.au)
Subject: Risk analysis report

Hi David and Alex,

I hope this email finds you well.

I am writing to present you with a summary of the recommendations as a result of the risk analysis findings.

We will need to implement the following computer safeguard guidelines as soon as possible, in order to enhance the security posture of the network and to mitigate the risks associated with the vulnerabilities we've found from the analysis.

- Update the web server software (Apache) to the latest stable version released by the Apache Software Foundation.
- Implement strict input validation on both client and server sides to prevent malicious input from being processed.
- Use parameterised queries or prepared statements in database interactions to prevent SQL injection attacks.

To ensure ongoing protection against emerging threats we will need to conduct regular security assessments and updates.

Here's the link to access the final version of the risk analysis report. AUS Retail_Risk Analysis Report_V2.0.pdf. If you have any questions, feedback, or concerns, please don't hesitate to reach out to me directly.

Thanks and kind regards,
Firstname Lastname
Network Administrator
Firstname.Lastname@ausretail.com.au

Before printing this email, please consider the environment.
This message may contain privileged information or confidential information or both and is intended for the recipient named. If you are not the intended addressee, please delete it and notify the sender.

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: Create a threat analysis report		
	Submitted copy of the threat analysis report	☐
Part C: Digitally store documentation		
	One (1) screenshot of document storage	☐
Part D: Control access to digitally stored documentation		
	One (1) Screenshot of the share settings of the document in cloud storage.	☐
Part E: Report issues and Present recommendations		
	Drafted an email to project sponsors to present recommendations.	☐

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 6!