



**ICTSAS530**

# Use network tools

Assessment 5 of 6

Portfolio

**Assessor Guide**



## Assessment Instructions

### Task Overview

This Portfolio 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. Portfolio tasks include completing hands-on practical tasks in a simulated workplace environment, documenting processes and capturing screenshot evidence of the tasks performed.

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

To perform the tasks in this skills assessment, you will need to have a simulated environment set up. Refer to this module's learning topic, 'Simulated environment set-up' for the required resources and set-up instructions.

## 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: Simulated environment set-up and resources

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. Simulated environment access and set-up instructions

- **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.

- **Work environment**

To carry out the assigned job tasks you must have access to a simulated environment that consists of two (2) virtual machines [Kali Linux and Metasploitable2] that are connected via a virtual network.

- A reliable internet connection
- A computer installed with an operating system having hardware virtualisation capabilities (i.e. the ability to run virtualisation software such as Oracle Virtual Box, Hyper-V, VMWare Workstation Player etc.)  
Refer to [Introduction to virtualisation \(linkedin.com\)](#) and [Setting up a virtual lab \(linkedin.com\)](#)
- Access to a 'Kali Linux VM' – This is a virtual machine (VM) for conducting threat data gathering activities
  - Download 'Kali Linux VM' virtual image from [Get Kali | Kali Linux](#) (Long URL: <https://www.kali.org/get-kali/#kali-virtual-machines>)
  - For a virtualisation platform of your choice, refer to the relevant documentation to set up and open the 'Kali Linux VM'. [Virtualisation | Kali Linux Documentation](#)
  - For example, if you have installed 'Oracle Virtual Box' on your computer, and you want to set up 'Kali Linux VM' as a guest Virtual Machine, you should refer to [Kali inside VirtualBox \(Guest VM\) | Kali Linux Documentation](#) (Long URL: <https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/>)
  - Refer to the access credentials of the virtual machine at [Kali's Default Credentials | Kali Linux Documentation](#) (Long URL: <https://www.kali.org/docs/introduction/default-credentials/>)
  - Refer to the LinkedIn Learning video on [Installing Kali as an appliance \(linkedin.com\)](#)
  - For further information on how to use the tools available in Kali Linux refer to [Kali Tools | Kali Linux Tools](#)
- Access to 'Metasploitable VM' – This is a web server with built-in vulnerabilities for testing.
  - Download 'Metasploitable2' virtual image from [Metasploitable - Browse /Metasploitable2 at SourceForge.net](#)
  - Refer to the LinkedIn Learning video on: [Installing Metasploitable from a virtual disk \(linkedin.com\)](#) to install and set-up this VM.

## A2. Industry software packages

You must use the following industry software packages to carry out the job tasks assigned to you.

- Web browsing software (e.g. Microsoft Edge, Firefox, Chrome, Safari)
- Microsoft Office software (e.g. WORD, Excel)
- A PDF reader
- Network vulnerability scanning software
  - CLI tools (nmap, nikto)
  - OWASP-ZAP

## Part B: Assess hardware quality standards

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

- follow the instructions in Part A1 to setup the 'Kali Linux' virtual machine in the simulated environment
- perform the tasks within the 'Kali Linux' virtual machine following organisational procedures.

### Scenario:

You have been provided with a computer installed with the 'Kali Linux' operating system to run the required command-line tools for network security testing. Prior to using this hardware equipment you need to assess whether it has the required hardware specification to be able to conduct the tests successfully.

The recommended/minimum hardware specification according the work brief is as follows:

- RAM/Memory: 2GB
- Processor: 32 or 64-bit CPU with a minimum 2 GHz of speed or better.
- An ethernet controller

### Organisational procedure for installing and running hardware quality assessment software

- To check for hardware quality in a system and to conduct hardware benchmark tests, the tool 'hardinfo' needs to be available in the 'Kali Linux VM'.

### Procedure to install 'hardinfo':

[HardInfo - Community Help Wiki \(ubuntu.com\)](#)

- To install the 'hardinfo' tool, execute the following command at the shell prompt.

```
sudo apt install hardinfo
```

- To use the 'hardinfo' tool, execute the following command at the shell prompt.

```
hardinfo
```

### Tasks:

#### Task B1 – Obtain hardware equipment specifications

Obtain information about the 'Kali Linux' machine's processor, memory and network adaptor (Ethernet controller) specifications following organisational procedures.

Provide evidence of completing this task in 'Table 1' by including:



- three (3) screenshots showing 'Kali Linux' machine's hardware specifications for the processor, memory and Ethernet controller.
- a summary of the hardware specifications and a brief outline of your assessment of whether the quality standard of the hardware is sufficient for conducting security tests. (Word count: 35-55 words)

**Note:** Your screenshots should clearly indicate the details of identified hardware equipment.

**Evidence of performing task :**

**Assessor instructions:** Students must demonstrate their ability to:

- correctly identify the computing hardware component specifications
- assess hardware the quality standard according to the work brief [recommended/minimum hardware specification] provided in the scenario
- interpret information from the test results obtained and explain how the quality standard of the hardware was assessed. The interpretation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
  - be within the specified word limit
  - reflect the characteristics described in the exemplar answer.

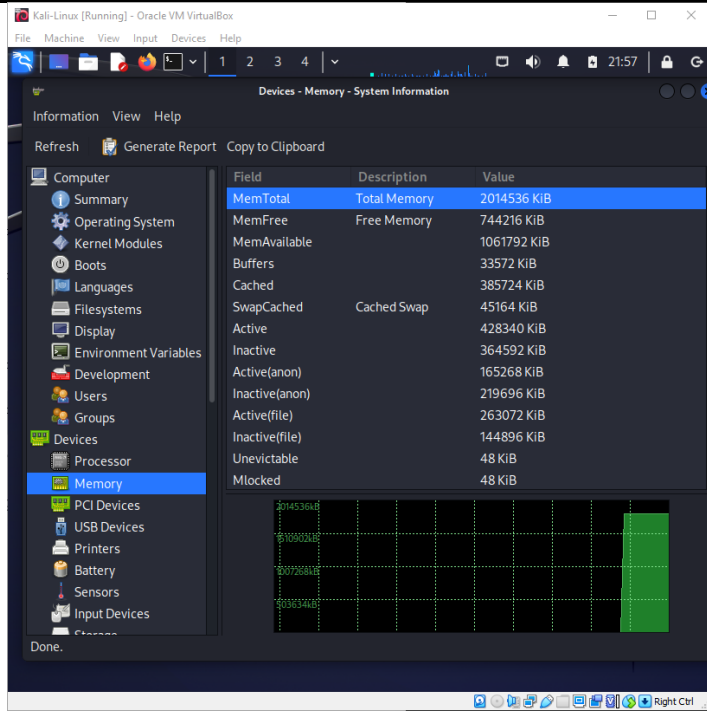
A sample answer is provided below.

Table 1 - Answer table for Task B1

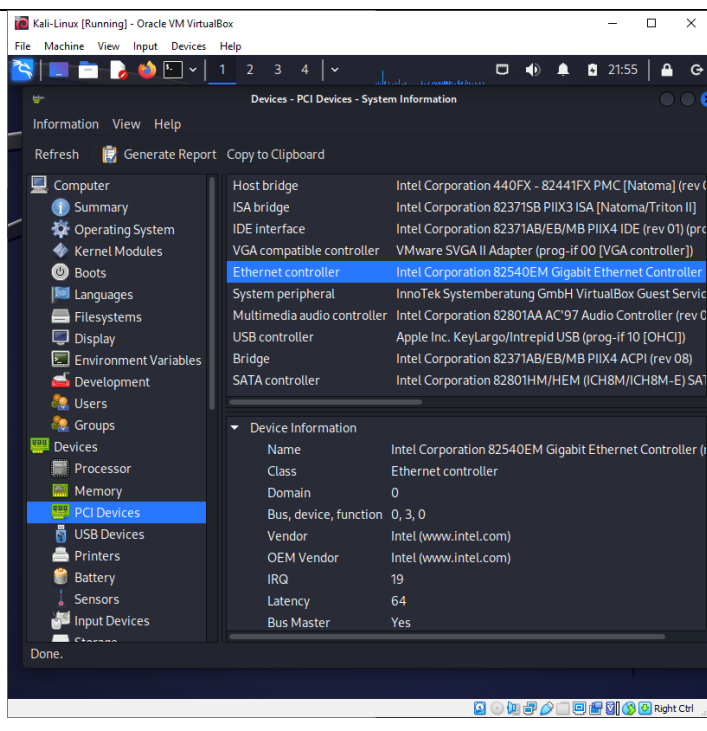
Criterion	Screenshot evidence
Processor specification of 'Kali Linux' machine.	

**Criterion**      **Screenshot evidence**

*Memory specification of 'Kali Linux' machine.*



*Ethernet controller specification of 'Kali Linux' machine.*



*Interpretation and outcome of the result:*

Summary of the hardware specification of the Kali Linux VM:

**Processor:** 11<sup>th</sup> Gen Intel® Core™ i5-1145G7 @ 2.60GHz

**RAM:** 2048MB

**Ethernet controller:** Intel Corporation 82540EM Gigabit Ethernet Controller

The current equipment's hardware specification meets the specifications provided in the work brief.

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



## Assessor comments:

S  NYS

## Task B2 – Run a hardware benchmark test

Run a hardware benchmark test to check 'Kali Linux' machine's ability to perform 'Blowfish' encryptions using the organisation's recommended tool.

As evidence of performing the task, you must provide:

- a screenshot of the completed benchmark test under 'Evidence of performing task:' section.
- a brief outline of your understanding of the benchmark test results. (Word count: 35–55 words)

## Evidence of performing task :

**Assessor instructions:** Students must demonstrate their ability to:

- run a benchmark test to assess the hardware quality standard using the organisation's recommended tool.
- interpret information from the test results obtained and explain how the quality standard of the hardware was assessed. The interpretation is likely to include different wording than the sample answer provided. 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.

Results	CPU	CPU Config
17.81	Pentium III (Coppermine)	2x 999.00 MHz
16.76	Intel(R) Atom(TM) CPU N280 @ 1.66GHz	2x 1660.00 MHz
12.58	AMD Turion(tm) 64 X2 TL-58	2x 800.00 MHz
12.06	Intel(R) Pentium(tm) 4 CPU 3.20GHz	2x 3200.00 MHz
11.86	AMD Turion(tm) X2 Dual-Core Mobile RM-72	2x 500.00 MHz
11.70	Intel(R) Pentium(R) 4 CPU 2.80GHz	2x 2800.00 MHz
11.65	11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz	1x 1497.60 MHz
11.60	Intel(R) Pentium(R) DualCPU T2310 @ 1.46GHz	2x 1463.00 MHz
10.84	Intel(R) Pentium(R) D CPU 3.00GHz	2x 3000.00 MHz
10.79	AMD Turion(tm) 64 X2 Mobile Technology TL-56	2x 800.00 MHz
10.71	AMD Athlon(tm) 64 X2 Dual Core Processor 3800+	2x 2200.00 MHz
10.67	Genuine Intel(R) CPU T1400 @ 1.60GHz	2x 1595.00 MHz
10.59	AMD Athlon(tm) X2 Dual-Core QL-60	2x 1900.00 MHz
10.10	AMD Turion(tm) 64 X2 Mobile Technology TL-58	2x 1900.00 MHz
9.58	Intel(R) Pentium(R) DualCPU T2370 @ 1.73GHz	2x 1733.00 MHz
9.37	Intel(R) Core(TM)2 CPU T7400 @ 2.16GHz	2x 2161.00 MHz
9.11	Intel(R) Xeon(R) CPU 3040 @ 1.86GHz	2x 1862.00 MHz
8.97	AMD Turion(tm) X2 Dual-Core Mobile RM-74	2x 600.00 MHz
8.84	AMD Turion(tm) 64 X2 Mobile Technology TL-62	2x 800.00 MHz
8.73	AMD Athlon(tm) 64 X2 Dual Core Processor 4800+	2x 2512.00 MHz
8.29	Intel(R) Core(TM)2 Duo CPU P8400 @ 2.26GHz	2x 2260.00 MHz

**Benchmark Result**

- Threads: 1
- Machine
  - Board: 1.2 / VirtualBox (Oracle Corporation)
  - CPU Name: 11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz
  - CPU Description: 1 physical processor; 1 core; 1 thread
  - CPU Config: 1x 1497.60 MHz

## Brief explanation of the benchmark test:

According to the benchmark test specification, the results are provided in seconds. The lower the numeric value for the result of the current machine's CPU (which is 11th Gen Intel Core i5, as highlighted in the screenshot) is better for handling Blowfish encryptions.

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

## Part C: Run command-line tools

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

- follow the instructions in Part A1 to setup the 'Metasploitable' virtual machine in the simulated environment
- use appropriate technological tools (network, hardware, software and operating systems) within the simulated environment
- in the event of network connectivity issues in the simulated environment, use problem solving techniques to analyse outcomes and manage the simulated environment network.

### Tasks:

**Note:** Ensure that both the 'Kali Linux VM' and 'Metasploitable VM' are running before doing the tasks.

Do the following tasks by writing command-line text within the Kali Linux GUI environment.

C1. Check network connectivity of the Kali Linux VM with the Metasploitable VM.

**Note:** Write the command-line using the required command options to ensure that:

- an echo request is sent from the Kali Linux VM only five (5) times and does not run continuously by default.
- a successful echo reply is received from the target machine. If not, you need to use problem-solving techniques to find and resolve the issue.

C2. Check routing information in the Kali Linux VM.

**Note:** Writing and running this command should result in obtaining the routing information of your virtual network. If the command fails to show this information, you will need to use problem-solving techniques to find and resolve the issue.

C3. Trace route trace information from the Kali Linux VM to the Metasploitable VM.

**Note:** Writing and running this command should result in obtaining the routing trace information to the correct target machine. If the command fails to show this information, you will need to use problem-solving techniques to find and resolve the issue.

C4. Check DNS server configuration details in Metasploitable VM, from the Kali Linux VM.

**Note:** Writing and running this command should result in obtaining DNS server configuration information from the correct target machine. If the command fails to show this required information, you will need to use problem-solving techniques to find and resolve the issue.

Provide 1-4 screenshots as evidence of performing tasks C1-4. Your screenshot(s) should clearly indicate the written command-line text and the result of running command-line.

C5. If you encountered any issues while doing tasks C1-4, provide a brief explanation of:

- the problem and what it was



- what actions were taken to fix the problem

[Approximate word count: 35-65 words]

### Evidence of performing the tasks:

Provide screenshot evidence here.

**Assessor instructions:** Students must demonstrate their ability to run the required commands successfully in the 'Kali Linux VM'.

A sample screenshot is provided below.

```

kali@kali: ~
┌──(kali@kali)-[~]
│   └─$ ping 10.0.2.4 -c5
│   PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
│   64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.699 ms
│   64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.446 ms
│   64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.463 ms
│   64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.500 ms
│   64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.462 ms
│
│   ── 10.0.2.4 ping statistics ──
│   5 packets transmitted, 5 received, 0% packet loss, time 4079ms
│   rtt min/avg/max/mdev = 0.446/0.514/0.699/0.094 ms
└─(kali@kali)-[~]
┌──(kali@kali)-[~]
│   └─$ route
│   Kernel IP routing table
│   Destination Gateway Genmask Flags Metric Ref Use Iface
│   default 10.0.2.1 0.0.0.0 UG 100 0 0 eth0
│   10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
└─(kali@kali)-[~]
┌──(kali@kali)-[~]
│   └─$ traceroute 10.0.2.4
│   traceroute to 10.0.2.4 (10.0.2.4), 30 hops max, 60 byte packets
│   1 10.0.2.4 (10.0.2.4) 0.564 ms 0.528 ms 0.519 ms
└─(kali@kali)-[~]
┌──(kali@kali)-[~]
│   └─$ dig 10.0.2.4
│
│   ; <<>> DiG 9.18.16-1-Debian <<>> 10.0.2.4
│   ;; global options: +cmd
│   ;; Got answer:
│   ;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 18655
│   ;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
│
│   ;; QUESTION SECTION:
│   ;10.0.2.4. IN A
│
│   ;; ANSWER SECTION:
│   10.0.2.4. 0 IN A 10.0.2.4
│
│   ;; Query time: 4 msec
│   ;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
│   ;; WHEN: Wed Feb 21 17:52:18 EST 2024
│   ;; MSG SIZE rcvd: 42

```

Brief explanation of problems encountered and how it was fixed:

**Assessor instructions:** Students must demonstrate their ability to:

- clearly articulate the problem, what it was and what actions were taken to fix the problem.
- the explanation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
  - be within the specified word limit
  - reflect the characteristics described in the exemplar answer.

Characteristics of the response are as follows:

- issues encountered when writing command-line text, due to:
  - not using the correct command-line syntax when writing the commands
  - not using the correct command-line options to get the desired result,
  - not considering case sensitivity when writing command-line text
  - not using the correct IP address of the target machine when writing the command-line text.
- problem solved network connectivity issues occurred due to:
  - errors in setting up the virtual machines and their network configuration in the simulated environment
  - the two virtual machines being in different virtual networks in the virtualisation platform

Fixes applied:

- Followed command-line syntax rules when writing command-line text
- Fixed network adapter configurations in the host/target machine.
- Restarted the machine[s]

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

**Assessor comments:**

S     NYS

## Part D: Apply organisational procedures

To complete this part of the assessment, you are required to perform the tasks within the 'Kali Linux' and 'Metasploitable' virtual machines in the simulated environment following organisational procedures.

### Scenario:

AUS Retail had recently noticed an increase in suspicious network activity and wants to proactively gather threat intelligence to bolster its security posture.

Therefore, you are planning to use network tools in order to gather the required threat intelligence data.

To prepare for the network threat investigation you are now required to follow the organisational procedures.

### Tasks:

Note: Ensure that both the 'Kali Linux VM' and 'Metasploitable VM' are running. Then perform the following preparation tasks following the given Organisational procedures for each task.

#### Task D1: Enable firewall logging

The 'Metasploitable VM' includes an operating system firewall 'iptables'. Configure this OS Firewall to log all incoming traffic.

#### Procedure to enable firewall logging:

To enable firewall logging, execute the following command in the 'Metasploitable2 VM':

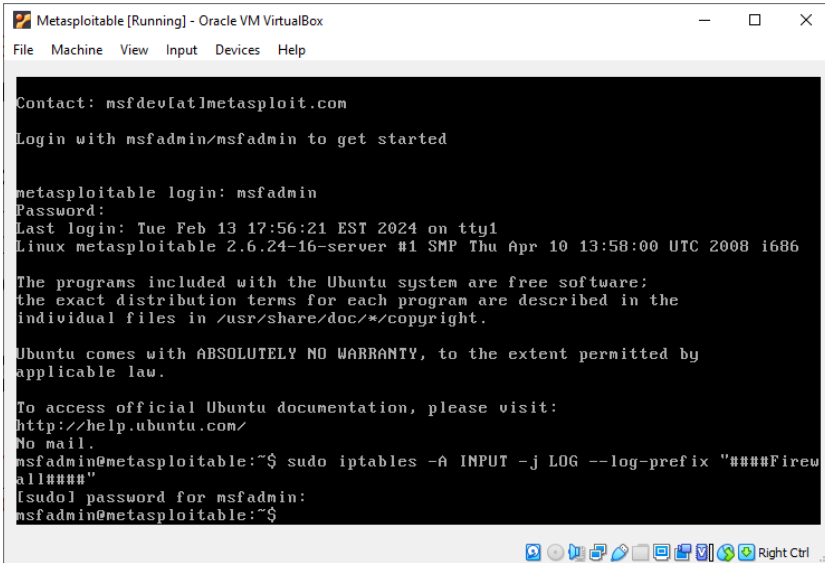
```
sudo iptables -A INPUT -j LOG --log-prefix "#### Firewall ####"
```

As evidence of performing the task provide a screenshot of the command executed under 'Evidence of performing the task:'.

**Evidence of performing the task:**

**Assessor instructions:** Students must follow the given organisational procedure and run the required command successfully in the 'Metasploitable VM'.

A sample screenshot is provided below.



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

**Assessor comments:**

S       NYS

**Task D2: Create a folder to store threat data logs**

Create a dataset folder in the 'Kali Linux VM', to store threat data logs. All the log files that you'll be gathering in Tasks E1-4, must be saved in this folder.

You must follow the organisation's policy for standard naming conversion. An excerpt of this policy as it relates to the given task, is as follows:

**Policy: Standard folder naming conversion**

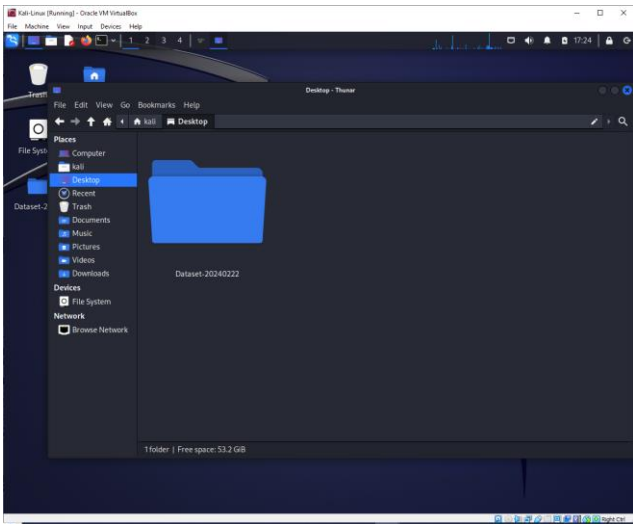
When creating a new folder to store threat data logs, the folder should be named as 'Dataset-yyyyymmdd'. For example, if today is the 22<sup>nd</sup> of February 2024, the folder name to be created is 'Dataset-20240222'.

As evidence of performing the task provide a screenshot of created folder under 'Evidence of performing the task:'.

**Evidence of performing the task:**

**Assessor instructions:** Students must follow the given organisational procedure to create the required folder in the 'Kali Linux VM'.

A sample screenshot is provided below.



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

**Assessor comments:**

S       NYS

### Task D3: Install network vulnerability assessment software

To check for vulnerabilities in a system, the organisation requires the software tool 'OWASP-ZAP' to be available in the 'Kali Linux VM'. Install this tool according to the following installation procedure.

#### Procedure for installing OWASP-ZAP:

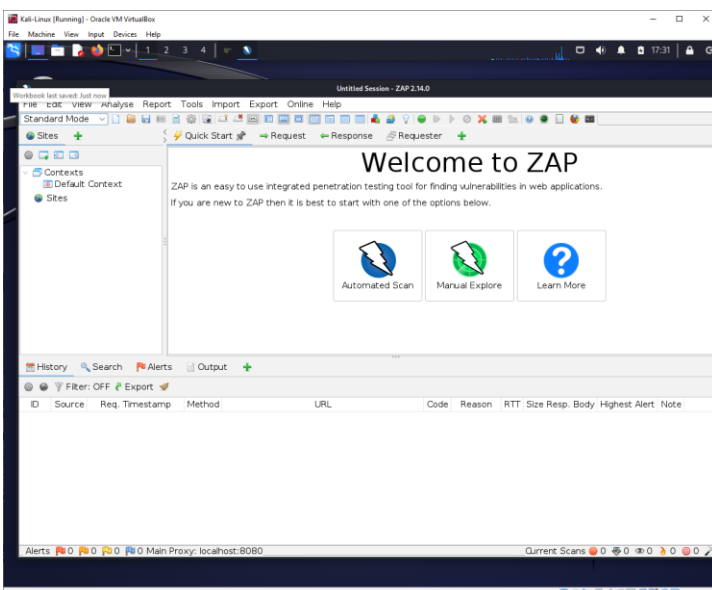
Follow instructions from the vendor to install 'OWASP-ZAP' tool on the 'Kali Linux VM' [ZAP – Download \[zaproxy.org\]](https://www.zaproxy.org/)

As evidence of performing the task provide a screenshot of the successfully installed software tool under 'Evidence of performing the task:'.

#### Evidence of performing the task:

**Assessor instructions:** Students must follow the given organisational procedure to install the required software tool in the 'Kali Linux VM'.

A sample screenshot is provided below.



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

**Assessor comments:**

S  NYS

## Part E: Collect threat data using command-line tools

To complete this part of the assessment, you are required to use appropriate technological tools and software within the simulated environment to run command-line tools.

### Tasks:

#### Task E1 – Gather TCP/UDP open port data using 'nmap'

- a. Conduct a TCP port scan on the target/source machine 'Metasploitable', using the 'nmap' tool in 'Kali Linux'. The requirement and specification of this scan is to:
  - use the TCP SYN scan technique
  - probe open ports to determine service/version information
  - enable OS detection
  - generate an output in XML format into a file called 'nmap-tcpscan.xml'.
- b. Conduct a UDP port scan using 'nmap' and save the output in XML format into a file called 'nmap-udpscan.xml'.
- c. Provide evidence of completing this task in 'Table 2' by including:
  - a screenshot of the TCP port scan results
  - a screenshot of the UDP port scan results
  - an interpretation of the obtained results and a brief explanation of any issues detected. (Word count: 75-100 words)

### Evidence of performing task E1:

**Assessor instructions:** Students must:

- perform the nmap scans using the correct command line options as shown in the screenshots provided.
  - `sudo nmap -sS -sV -O <target ip address> -oX nmap-tcpscan`
  - `sudo nmap -sU <Target IP Address> -oX nmap-udpscan.xml`

**Note:** The students should use the 'Metasploitable2 VM' IP address as the target IP address, according to the configuration of their simulated virtual environment.

- correctly interpret information from the scan results obtained and issues present. The interpretation is likely to include different wording than the sample answer provided. 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.



Table 2 - Answer table for Task E1

Criterion	Screenshot evidence
<p>TCP port scan result:</p>	
<p>UDP port scan result:</p>	
<p>Interpretation of the obtained results and issues identified:</p>	<p>These port scan results help 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).</p> <p>It is important to note that UDP scans can cause a lot of false positives. This happens when a firewall blocks a single port, which gets falsely reported in the UDP scan as an open port.</p>

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

Assessor comments:

S       NYS

## Task E2 – Gather threat data from web server software using the tool 'nikto'

Conduct a scan of the web server (i.e. metasploitable2 virtual machine) using the information gathering tool 'nikto' and save this information to a file called 'nikto-webscan.csv' in CSV format.

Provide evidence of completing this task in 'Table 3', by including:

- a screenshot of the web scan results
- an interpretation of the obtained results, issues identified and a brief explanation of how this information is useful when assessing software quality standards. (Word count: 85-115 words)

### Evidence of performing task E2:

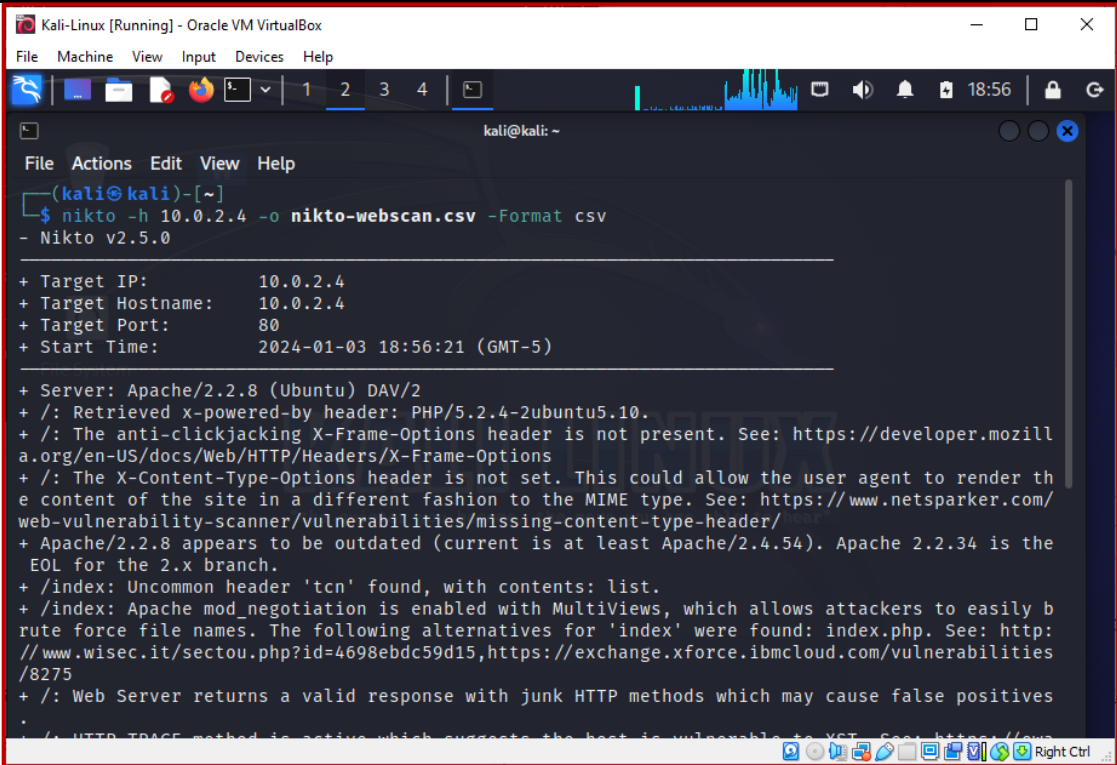
#### Assessor instructions: Students must:

- perform the web scan using the correct command line options as shown in the screenshots provided.
  - nikto -h <target IP address> -o nikto-webscan.csv -Format csv

Note: The students should use the 'Metasploitable2 VM' IP address as the target IP address, according to the configuration of their simulated virtual environment.
- correctly interpret information from the scan results obtained and identified current issues. The interpretation is likely to include different wording than the sample answer provided. 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.

Table 3 - Answer table for Task E2

Criterion	Screenshot evidence
'nikto' web scan result:	
Interpretation of the obtained	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)

Criterion	Screenshot evidence
results and issues identified:	<p>For example, according to the results obtained, this tool had identified vulnerabilities such as:</p> <ul style="list-style-type: none"> <li>• outdated web server software (Apache)</li> <li>• '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.</li> </ul> <p>By using Nikto to identify and mitigate security vulnerabilities, organisations can demonstrate compliance software quality standards such as ISO/IEC 25010, (which include requirements related to security), thereby ensuring that their software meets certain quality criteria, particularly in terms of security.</p>

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

**Assessor comments:**

S       NYS

### Task E3 – Gather alert data from a web application

Run an automated vulnerability scan of the web application hosted on the 'Metasploitable2 VM' using the 'OWASP-ZAP' tool installed on the 'Kali Linux' virtual machine and save this information to a file called 'ZAP-webscan.csv' in CSV format.

Ensure that the scan tests for 3-5 different vulnerability tests such as SQL injection, cross-site scripting, code injection, etc.

Provide evidence of completing this task in 'Table 4', by including:

- 3-5 screenshots of the web scan results (i.e. the running scan, types of vulnerabilities tested and result of the alerts captured)
- an interpretation of the obtained results, issues identified and a brief explanation of how this information is useful when assessing software quality standards. (Word count: 85-115 words)

Note: The scan will take a while to complete. Once you've captured enough amount of data and have scanned for a variety of vulnerabilities, you may stop the scan, take screenshots and export the captured results.

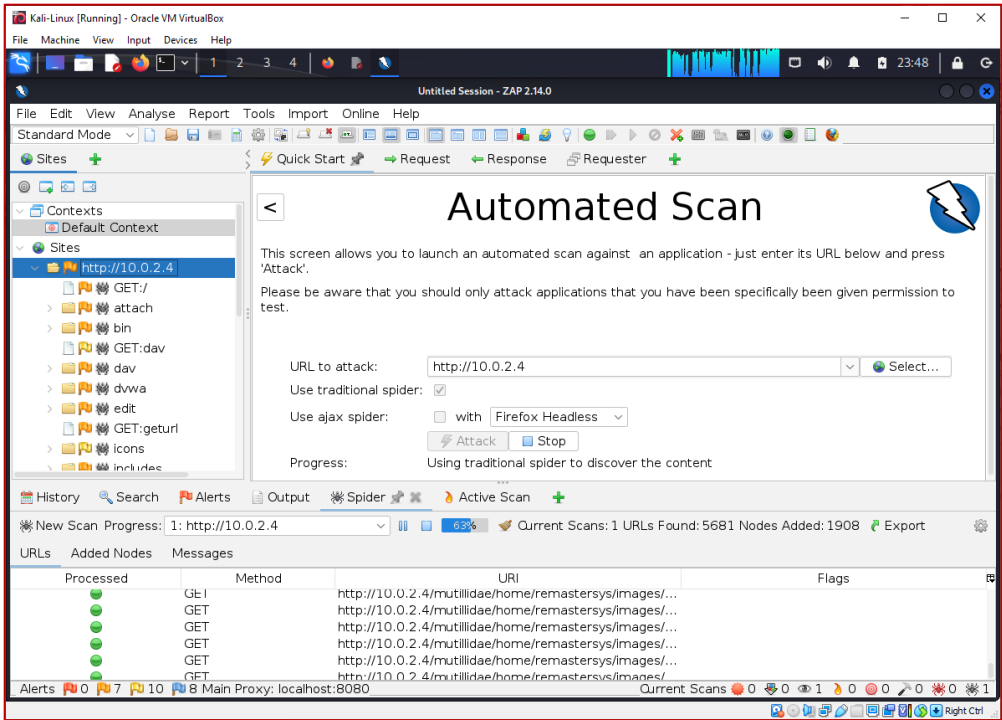
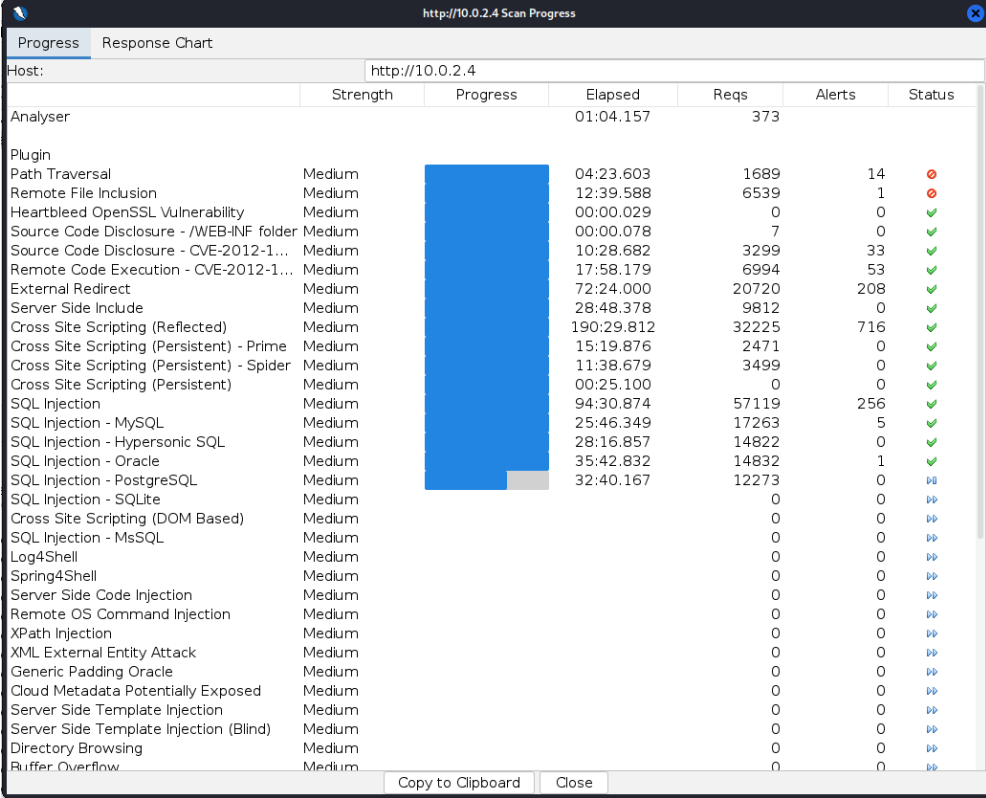
#### Evidence of performing task E3:

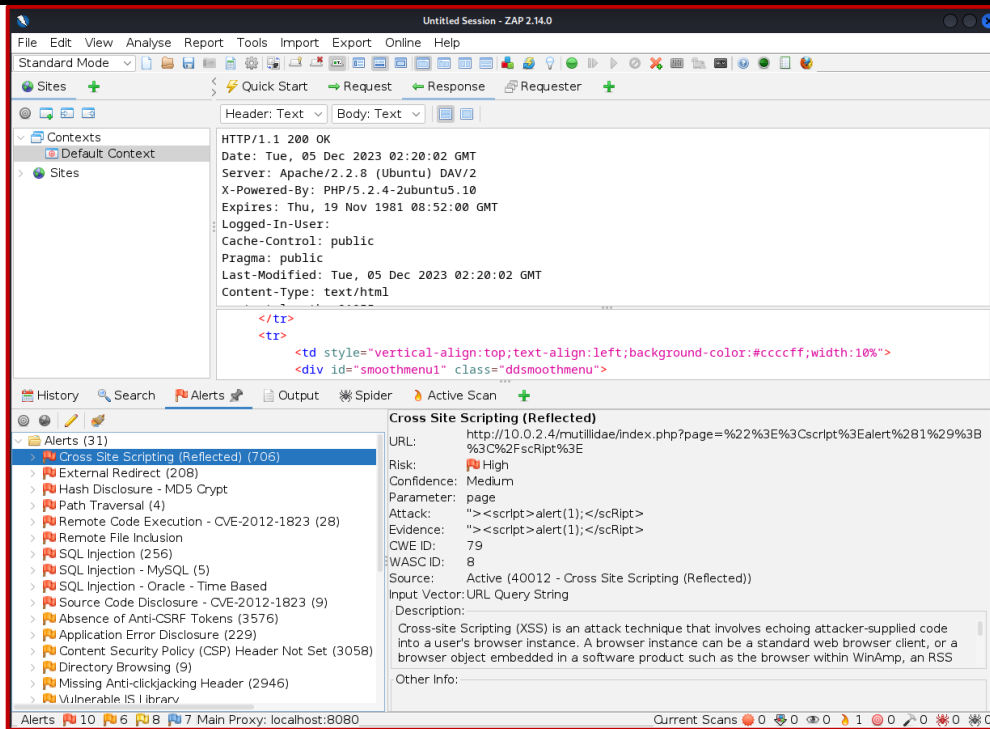
**Assessor instructions:** Students must:

- perform the web scan using ZAP tool as shown in the screenshots provided.  
Note: The students should use the 'Metasploitable2 VM' IP address to specify the attack URL, according to the configuration of their simulated virtual environment.
- correctly interpret information from the scan results obtained. The interpretation is likely to include different wording than the sample answer provided. However, the acceptable responses must:
  - be within the specified word limit
  - reflect the characteristics described in the exemplar answer.

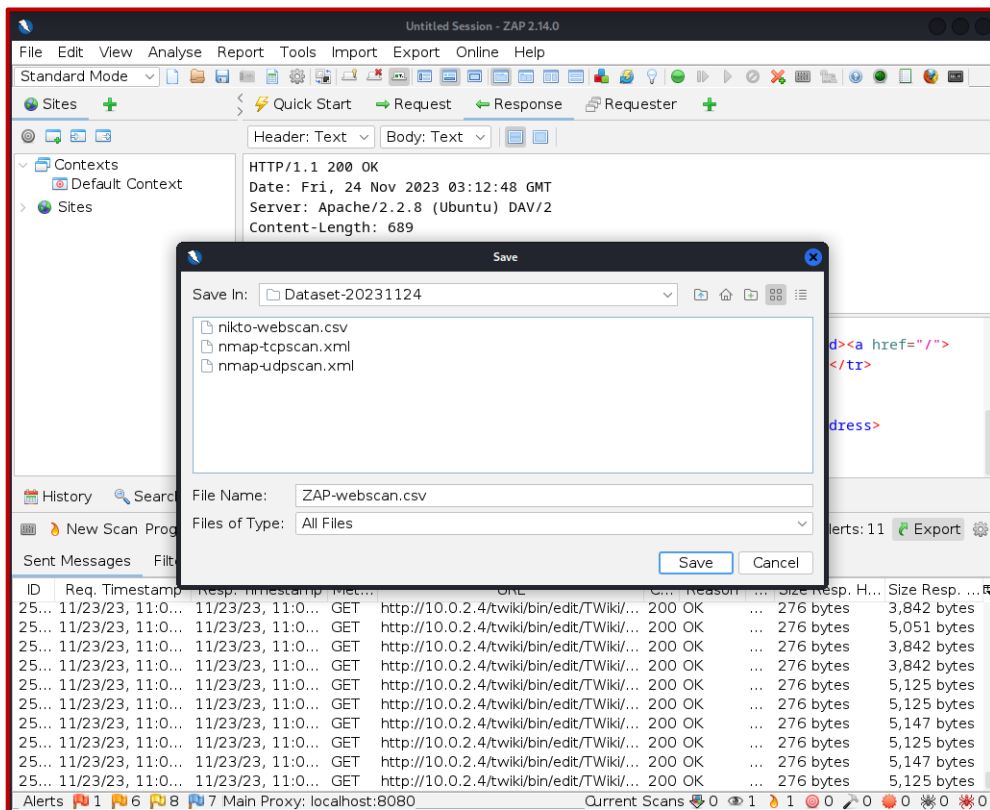
A sample answer is provided below.

Table 4 - Answer table for Task E3

Criterion	Screenshot evidence																																																																																																																																																																																																																																																					
<p>'ZAP' vulnerability scan result:</p>	<p><b>Screenshot 1 - Running the scan using the web address using IP address</b></p>  <p><b>Screenshot 2 - Active scan progress</b></p>  <table border="1" data-bbox="304 1010 1294 1805"> <thead> <tr> <th>Host:</th> <th>Strength</th> <th>Progress</th> <th>Elapsed</th> <th>Reqs</th> <th>Alerts</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Analyser</td> <td></td> <td></td> <td>01:04.157</td> <td>373</td> <td></td> <td></td> </tr> <tr> <td>Plugin</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Path Traversal</td> <td>Medium</td> <td></td> <td>04:23.603</td> <td>1689</td> <td>14</td> <td>⚠</td> </tr> <tr> <td>Remote File Inclusion</td> <td>Medium</td> <td></td> <td>12:39.588</td> <td>6539</td> <td>1</td> <td>⚠</td> </tr> <tr> <td>Heartbleed OpenSSL Vulnerability</td> <td>Medium</td> <td></td> <td>00:00.029</td> <td>0</td> <td>0</td> <td>✓</td> </tr> <tr> <td>Source Code Disclosure - /WEB-INF folder</td> <td>Medium</td> <td></td> <td>00:00.078</td> <td>7</td> <td>0</td> <td>✓</td> </tr> <tr> <td>Source Code Disclosure - CVE-2012-1...</td> <td>Medium</td> <td></td> <td>10:28.682</td> <td>3299</td> <td>33</td> <td>✓</td> </tr> <tr> <td>Remote Code Execution - CVE-2012-1...</td> <td>Medium</td> <td></td> <td>17:58.179</td> <td>6994</td> <td>53</td> <td>✓</td> </tr> <tr> <td>External Redirect</td> <td>Medium</td> <td></td> <td>72:24.000</td> <td>20720</td> <td>208</td> <td>✓</td> </tr> <tr> <td>Server Side Include</td> <td>Medium</td> <td></td> <td>28:48.378</td> <td>9812</td> <td>0</td> <td>✓</td> </tr> <tr> <td>Cross Site Scripting (Reflected)</td> <td>Medium</td> <td></td> <td>190:29.812</td> <td>32225</td> <td>716</td> <td>✓</td> </tr> <tr> <td>Cross Site Scripting (Persistent) - Prime</td> <td>Medium</td> <td></td> <td>15:19.876</td> <td>2471</td> <td>0</td> <td>✓</td> </tr> <tr> <td>Cross Site Scripting (Persistent) - Spider</td> <td>Medium</td> <td></td> <td>11:38.679</td> <td>3499</td> <td>0</td> <td>✓</td> </tr> <tr> <td>Cross Site Scripting (Persistent)</td> <td>Medium</td> <td></td> <td>00:25.100</td> <td>0</td> <td>0</td> <td>✓</td> </tr> <tr> <td>SQL Injection</td> <td>Medium</td> <td></td> <td>94:30.874</td> <td>57119</td> <td>256</td> <td>✓</td> </tr> <tr> <td>SQL Injection - MySQL</td> <td>Medium</td> <td></td> <td>25:46.349</td> <td>17263</td> <td>5</td> <td>✓</td> </tr> <tr> <td>SQL Injection - Hypersonic SQL</td> <td>Medium</td> <td></td> <td>28:16.857</td> <td>14822</td> <td>0</td> <td>✓</td> </tr> <tr> <td>SQL Injection - Oracle</td> <td>Medium</td> <td></td> <td>35:42.832</td> <td>14832</td> <td>1</td> <td>✓</td> </tr> <tr> <td>SQL Injection - PostgreSQL</td> <td>Medium</td> <td></td> <td>32:40.167</td> <td>12273</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>SQL Injection - SQLite</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Cross Site Scripting (DOM Based)</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>SQL Injection - MsSQL</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Log4Shell</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Spring4Shell</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Server Side Code Injection</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Remote OS Command Injection</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>XPath Injection</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>XML External Entity Attack</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Generic Padding Oracle</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Cloud Metadata Potentially Exposed</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Server Side Template Injection</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Server Side Template Injection (Blind)</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Directory Browsing</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> <tr> <td>Buffer Overflow</td> <td>Medium</td> <td></td> <td></td> <td>0</td> <td>0</td> <td>⏸</td> </tr> </tbody> </table> <p><b>Screenshot 3 - Scan result and alert details</b></p>	Host:	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	⏸
Host:	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	⏸																																																																																																																																																																																																																																																



Exporting results to a file called 'ZAP-webscan.csv'.



Interpretation of the obtained results and issues identified:

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

For example, the highest priority resulted:

The scan 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)



Criterion	Screenshot evidence
	<ul style="list-style-type: none"> <li>External Redirect (208 alerts)</li> <li>Hash disclosure MD5 crypt</li> <li>Path traversal</li> <li>SQL injection</li> <li>Remote code execution</li> <li>Remote file inclusion</li> </ul> <p>OWASP-ZAP's ability to uncover security vulnerabilities aligns with various software quality standards' requirements related to security, such as ISO/IEC 25010. By using OWASP-ZAP to assess and address security vulnerabilities, organizations can demonstrate compliance with these standards, ensuring that their software meets predefined quality criteria, particularly in terms of security.</p>

**Assessor instructions:** Assessors are to indicate the task result as Satisfactory [S] or Not Yet Satisfactory [NYS].

**Assessor comments:**

S  NYS

### Task E4 – Gather data from the Linux OS Firewall 'iptables'

The Linux web server's Operating System [OS] firewall (i.e. a form of virtual security service), commonly known as 'iptables' provides security and access control to the web server. The OS firewall (i.e. 'iptables') logs are captured in the '/var/log/kern.log' file within the 'Metasploitable2 VM'.

In this task, you are required to gather threat data logged by the firewall by doing the following.

- Transfer the /var/log/kern.log file from the 'Metasploitable2 VM' to the 'Kali Linux VM'. To do this, you may use an appropriate file transfer protocol [e.g. ftp] from the 'Kali Linux VM' or another suitable method [e.g. via folder sharing, removable device].
- Create a log file that only contains all incoming traffic from the iptables firewall. To do this, filter the contents of the 'kern.log' file (which was transferred to the 'Kali Linux VM') using the log-prefix "#### Firewall ####" and obtain only the logs relevant to iptables. Save the result into a new file called 'firewall-logs.txt'
- Verify that the 'firewall-logs.txt' contains the log events from iptables firewall.
- Provide evidence of completing this task in 'Table 5', by including:
  - 1-3 screenshots of the process used when performing this task
  - an interpretation of the obtained results and a brief explanation of how this information is useful when detecting threats and vulnerabilities. [Word count: 55-90 words]

### Evidence of performing task E4:

**Assessor instructions:** Assessors are to indicate the task result as Satisfactory [S] or Not Yet Satisfactory [NYS].

**Assessor comments:**

S  NYS

**Students must:**

- perform the task using appropriate tools to filter and collect the required log events as shown in the screenshots provided.

Note: The students should use the 'Metasploitable2 VM' IP address to specify the target web server, according to the configuration of their simulated virtual environment.

- correctly interpret information from the scan results obtained. The interpretation is likely to include different wording than the sample answer provided. 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.

Table 5 - Answer table for Task E4

Criterion	Screenshot evidence
'OS Firewall' logs:	<p>Screenshot 1 – Accessing the /var/log/kern.log from the 'Metasploitable2 VM' using the ftp protocol.</p>  <p>Screenshot 2 – Using command-line to filter the log records that only contain the log-prefix '#### Firewall ####' and saving to firewall-logs.txt.</p>  <p>Screenshot 3 - Verification of the contents of the firewall-logs.txt</p> 



Congratulations, you have reached the Assessment 5!



© UP Education Online Pty Ltd 2023

Except as permitted by the copyright law applicable to you, you may not reproduce or communicate any of the content on this website, including files downloadable from this website, without the permission of the copyright owner.

**WARNING**

This material has been reproduced and communicated to you by or on behalf of UP Education in accordance with section 113P of the *Copyright Act 1968* [the Act].

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.