



ICTCYS407

Gather, analyse and interpret threat data

Assessment 4 of 5

Portfolio

Assessor Guide



Assessment Instructions

Task Overview

This Portfolio assessment is divided into four [4] parts. Read the simulated environment set-up and resource information in Part A and complete the associated tasks in Parts B, C and D. 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 cybersecurity threat analysis field of work.

Read the following details carefully before completing the tasks in Part B.

A1. Simulated environment access and set-up instructions

Your role

You are hired as a **Cybersecurity Analyst** by Wayne Corporation to be part of a threat investigation project. You are responsible for gathering threat data from various sources, then analyse and interpret information for threats, inconsistencies and discrepancies.

Work environment

To carry out the assigned job tasks in the cybersecurity threat analysis field of work, 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 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 'Metasploitable2 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

- Data recognition software
 - CLI tools (nmap, nikto)
 - OWASP ZAP

A3. Analytic platforms

Analytic platform for analysing threat data (SIEM) and applicable user instructions.

Note: You may use a tool/software/platform listed below or another industry-accepted SIEM platform/tool that allows you to gather, analyse and interpret threat data. You must then refer to the user instructions provided by the vendor for the specific software/tool/platform you've chosen to use.

- Splunk
- Elastic (Elk) Stack
- Manage Engine Log360

A4. Organisational procedures to prepare for gathering threat data

Note: Ensure that both the 'Kali Linux VM' and 'Metasploitable2 VM' are running. Then perform the following preparation tasks following the given organisational procedures.

Step 1: Enable firewall logging

- The 'Metasploitable2 VM' includes an operating system firewall 'iptables'. Configure this OS firewall to log all incoming traffic.
- **Procedure:** Execute the following command in the 'Metasploitable2 VM':

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

Step 2: 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 B1-4, must be saved in this folder.
- **Procedure:** Create a new folder and rename it in the following format '**Dataset-yyyymmdd**'. For example, if today is the 24th of November 2023, the folder name to be created is 'Dataset-20231124'.

Step 3: Install data recognition software

- To check for vulnerabilities in a system, the tool 'OWASP-ZAP' needs to be available in the 'Kali Linux VM'.
- **Procedure:** Follow instructions from the vendor to install 'OWASP-ZAP' tool on the 'Kali Linux VM' [ZAP – Download \[zaproxy.org\]](https://www.zaproxy.org/docs/desktop/installation/)

Part B: Collect threat data

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

- follow the given organisational procedures to prepare for gathering threat data as outlined in Part A, section A4
- use appropriate technological tools and software within the simulated environment to measure and record threat data.

Tasks:

Task B1 – Gather TCP/UDP open port data using 'nmap'

- a. Conduct a TCP port scan on the target/source machine 'Metasploitable 2', 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 1' 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 how this information is useful when detecting threats and vulnerabilities. (Word count: 75-100 words)

Evidence of performing task :

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

Assessor comments:

S NYS

Students must:

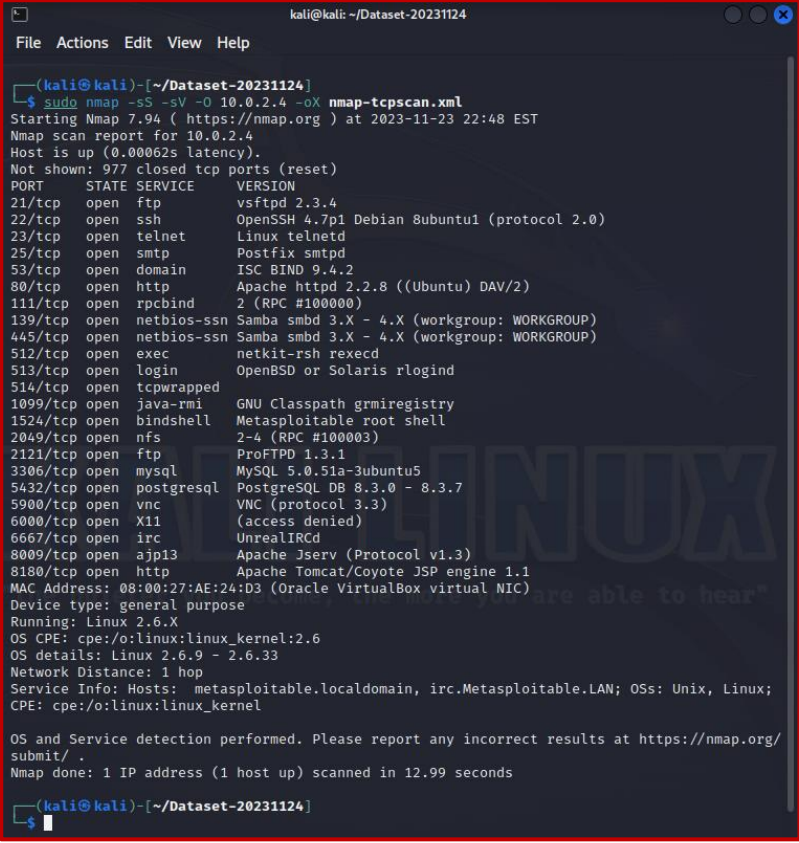
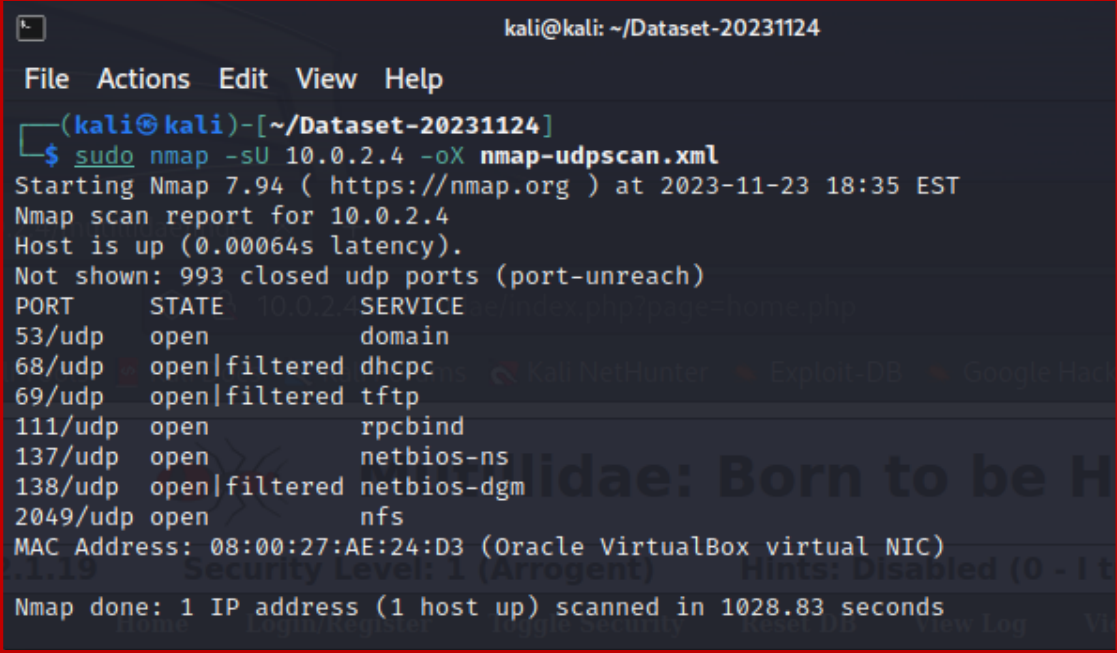
- perform the nmap scans using the correct command line options as shown in the screenshots provided.
 - `sudo nmap -sS -sV -O <target ip address> -oX nmap-tcpscan`
 - `sudo nmap -sU <Target IP Address> -oX nmap-udpscan.xml`

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. 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
<p>TCP port scan result:</p>	 <pre> kali@kali: ~/Dataset-20231124 File Actions Edit View Help (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 smbdc 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbdc 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] \$ </pre>
<p>UDP port scan result:</p>	 <pre> kali@kali: ~/Dataset-20231124 File Actions Edit View Help (kali@kali)~[~/Dataset-20231124] \$ sudo nmap -sU 10.0.2.4 -oX nmap-udpscan.xml Starting Nmap 7.94 (https://nmap.org) at 2023-11-23 18:35 EST Nmap scan report for 10.0.2.4 Host is up (0.00064s latency). Not shown: 993 closed udp ports (port-unreach) PORT STATE SERVICE 53/udp open domain 68/udp open filtered dhcp 69/udp open filtered tftp 111/udp open rpcbind 137/udp open netbios-ns 138/udp open filtered netbios-dgm 2049/udp open nfs MAC Address: 08:00:27:AE:24:D3 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 1028.83 seconds </pre>
<p>Interpretation of the obtained results:</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>

Task B2 – Gather threat data from a web server 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 2', by including:

- a. a screenshot of the web scan results
- b. 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 B2:

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

Assessor comments:

S NYS

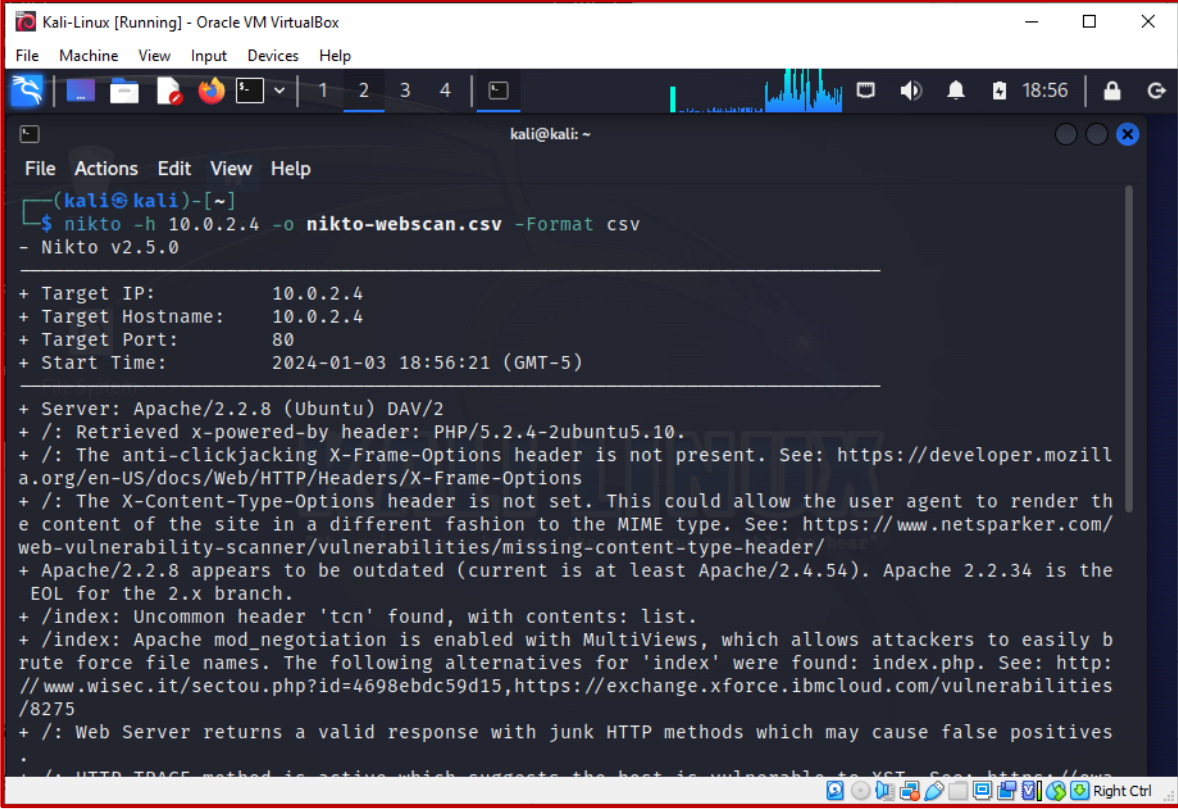
Students must:

- perform the 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. 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 B2

Criterion	Screenshot evidence
'nikto' web scan result:	
Interpretation of the obtained results:	<p>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)</p> <p>For example, according to the results obtained, this tool had identified vulnerabilities such as:</p> <ul style="list-style-type: none"> • 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. [e.g. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/]

Task B3 – 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 test such as SQL injection, Cross Site scripting, code injection etc.

Provide evidence of completing this task in 'Table 3', 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 and a brief explanation of how this information is useful when detecting threats and vulnerabilities. (Word count: 55-90 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 B3:

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

Assessor comments:

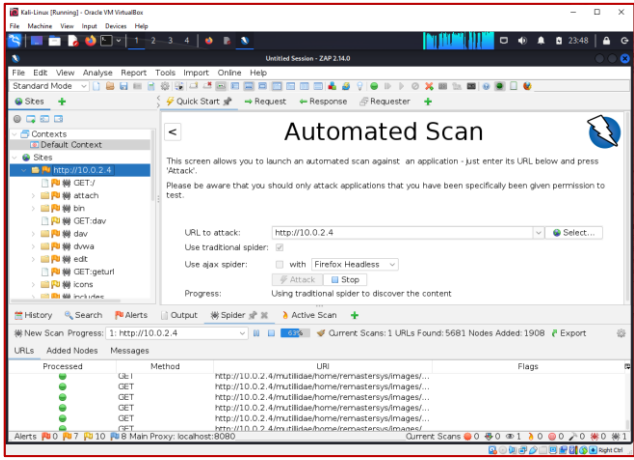
S NYS

Students must:

- perform the 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 3 - Answer table for Task B3

Criterion	Screenshot evidence
'ZAP' vulnerability scan result:	<p>Screenshot 1 - Running the scan using the web address using IP address</p>  <p>Screenshot 2 - Active scan progress</p>

http://10.0.2.4 Scan Progress						
Progress		Response Chart				
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	🔍

Screenshot 3 – Scan result and alert details

Cross Site Scripting (Reflected)

URL: http://10.0.2.4/mutillidae/index.php?page=%22%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E

Risk: High

Confidence: Medium

Parameter: page

Attack: "><script>alert(1);</script>

Evidence: "><script>alert(1);</script>

CWE ID: 79

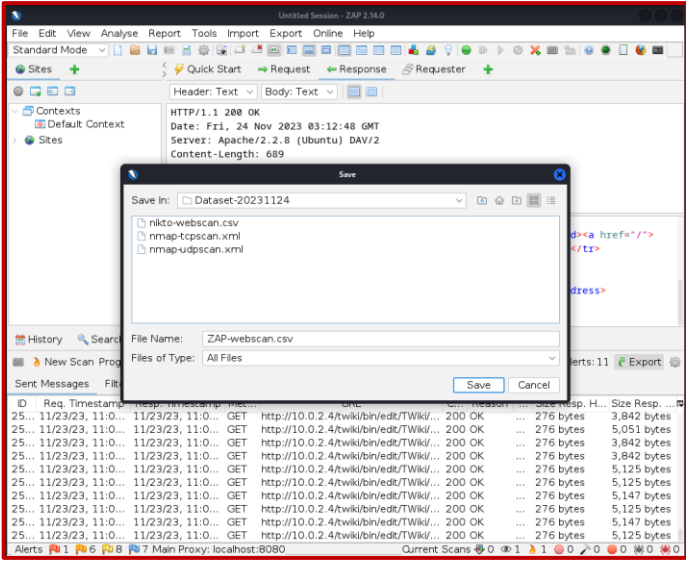
WASC ID: 8

Source: Active (40012 - Cross Site Scripting (Reflected))

Input Vector: URL Query String

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS

Other Info:

Criterion	Screenshot evidence
	<p>Exporting results to a file called 'ZAP-webscan.csv'.</p> 
<p>Interpretation of the obtained results:</p>	<p>The output of the scan provide detailed information on the alerts captured. These alerts are classified into risk level priority.</p> <p>For example, the highest priority resulted:</p> <p>The scan captured a total of 31 alerts, out of which 10 are high risk, 6 medium risks and 8 low low risk. The high risks include vulnerabilities for:</p> <ul style="list-style-type: none"> • Cross-site scripting (706 alerts) • External Redirect (208 alerts) • Hash disclosure MD5 crypt • Path traversal • SQL injection • Remote code execution • Remote file inclusion

Task B4 – 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.

- a. 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).
- b. 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'
- c. Verify that the 'firewall-logs.txt' contains the log events from iptables firewall.
- d. Provide evidence of completing this task in 'Table 4', by including:
 - o 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 B4:

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

Assessor comments:

S NYS

Students must:

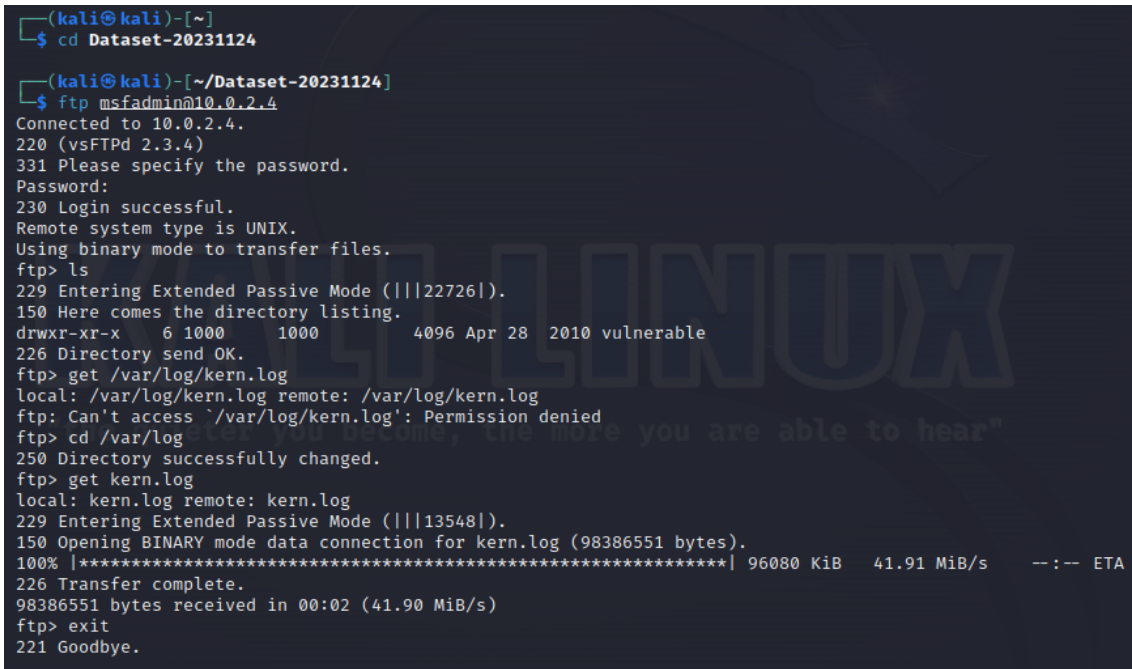
- perform the task using appropriate tools to filter and collect the required log events as shown in the screenshots provided.

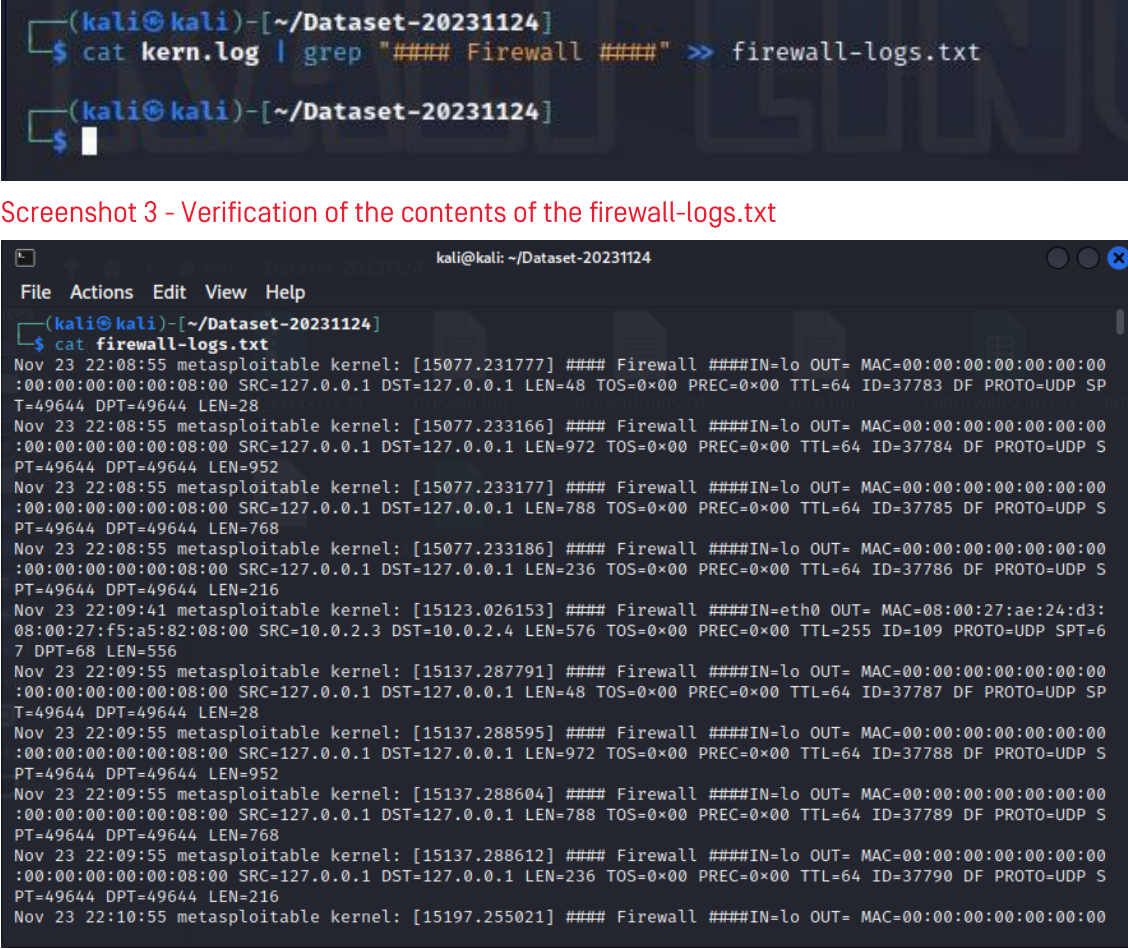
Note: The students should use the 'Metasploitable2 VM' IP address to specify the target web server, according to the configuration of their simulated virtual environment.

- 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 4 - Answer table for Task B4

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>

Criterion	Screenshot evidence
	 <p>Screenshot 3 - Verification of the contents of the firewall-logs.txt</p>
<p>Interpretation of the obtained results:</p>	<p>The firewall log captures the following information:</p> <ul style="list-style-type: none"> • source and destination IP and MAC addresses • DPT=80 traffic (that is destination port 80 web traffic) • Timestamp of in/out traffic • The connection interface # (e.g. eth0) • Protocol type weather TCP/UDP • Len - size of the packet transferred <p>This information is useful when identifying the specificst of any malicious device access attempts to the web server.</p>

Part C: Create dataset

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

- acces the 'Kali Linux VM' machine to create the threat dataset as a compressed archive file
- refer to the industry standard procedures on how to create compressed archives at [Linux Archive Files: How to Create & Manage Archive Files in Linux \(linuxfoundation.org\)](https://www.linuxarchive.com/2017/02/how-to-create-and-manage-archive-files-in-linux/)
- follow relevant procedures when performing the tasks.

Task:

Create a compressed archive file to contain the following five(5) log files collected in Part B of this assessment:

1. nmap-tcpscan.xml
2. nmap-udpscan.xml
3. nikto-webscan.csv
4. ZAP-webscan.csv
5. firewall-logs.txt

Dataset file naming convention: The name of the archive file should be according to the following naming convention: 'Dataset-<Student ID>.tar.gz'.

Note: For example, if the student ID is '12345678' the file name should be 'Dataset-12345678.tar.gz'

As evidence of completing this task, provide the 3-5 screenshots to demonstrate:

- that the 'Dataset-yyyyymmdd' folder contains the above-mentioned five (5) log files
- the process used to create the compressed archive file of the dataset
- confirm that the compressed archive file is created according to the naming convention.

Also, submit a copy of the dataset file: 'Dataset-<Student ID>.tar.gz' with this assessment submission.

Evidence of completing the task:

Assessor instructions: Students must:

- create the dataset folder following the given naming convention and ensure the required log files are included in the dataset
- create the compressed archive file of the dataset using command-line tools, following industry standard procedures.

A sample answer is provided below.

Screenshot of the contents in the 'Dataset-12345678' folder.

```
(kali@kali)-[~/Dataset-20231124]
└─$ ls
firewall-logs.txt  kern.log  nikto-webscan.csv  nmap-tcpscan.xml  nmap-udpscan.xml  ZAP-webscan.csv
```

Screenshot of the command used to create the dataset compressed archive file

```
(kali@kali)-[~/Dataset-20231124]
└─$ tar -czvf Dataset-XXXXXXXX.tar.gz nmap-tcpscan.xml nmap-udpscan.xml nikto-webscan.csv ZAP-webscan.csv firewall-logs.txt
nmap-tcpscan.xml
nmap-udpscan.xml
nikto-webscan.csv
ZAP-webscan.csv
firewall-logs.txt
```

The following screenshot shows the compressed archive file created having the specified naming convention.

```
(kali@kali)-[~/Dataset-20231124]
└─$ ls
Dataset-XXXXXXXX.tar.gz  kern.log  nmap-tcpscan.xml  ZAP-webscan.csv
firewall-logs.txt      nikto-webscan.csv  nmap-udpscan.xml
```

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

Assessor comments:

S NYS

Part D: Ingest data logs to analytic platform

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

- access the threat dataset folder created previously in Part C of this assessment
- use the required technological tools and software in gathering, analysing and interpreting threat data
- use the required analytical platform and applicable user instructions as outlined in Part A, Section A3 of this assessment.
 - Sign-up for a free trial version of an industry-standard cloud-hosted SIEM platform of your choice.

Tasks:

D1. Create a new index in the analytical platform called 'dataset_XXXXXXX', where 'XXXXXXX' is your unique Student ID.

D2. Ingest the data logs into the analytical platform according to user instructions provided by the platform vendor. Note: Ensure that the data in the threat dataset are searchable using the index name created in the previous task.

D3. Verify the consistency and reliability of the ingested threat dataset in the analytic platform by performing a search using the specified index. Ensure that the following five (5) log files are available as a source for analysis.

1. Firewall-logs.txt
2. Nikto-webscan.csv
3. Nmap-tcpscan.xml
4. Nmap-udpscan.xml
5. ZAP-webscan.csv

Provide 3-5 screenshots of the process used when performing this task with brief explanations and comments on the process used in 'Table 5'. [Word count: 25-50 words]

Evidence of performing the task(s):

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

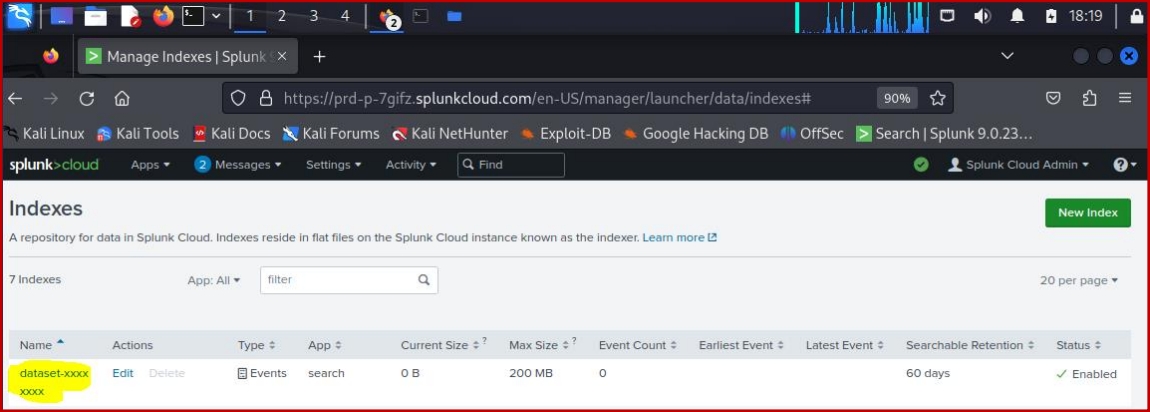
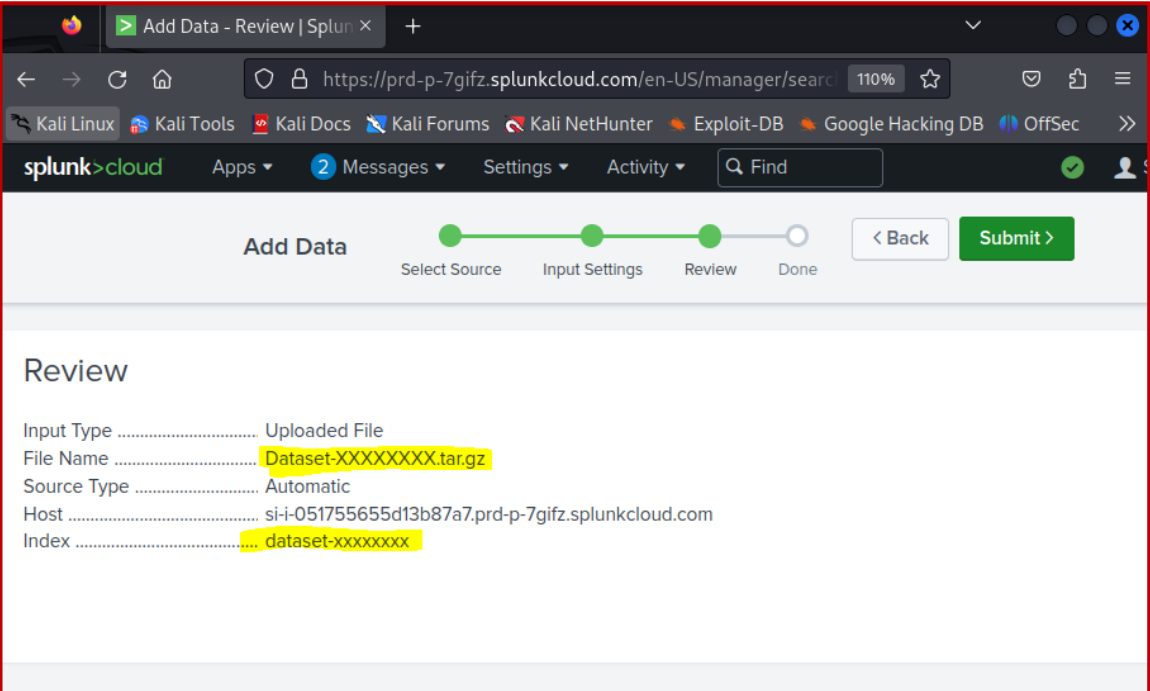
Assessor comments:

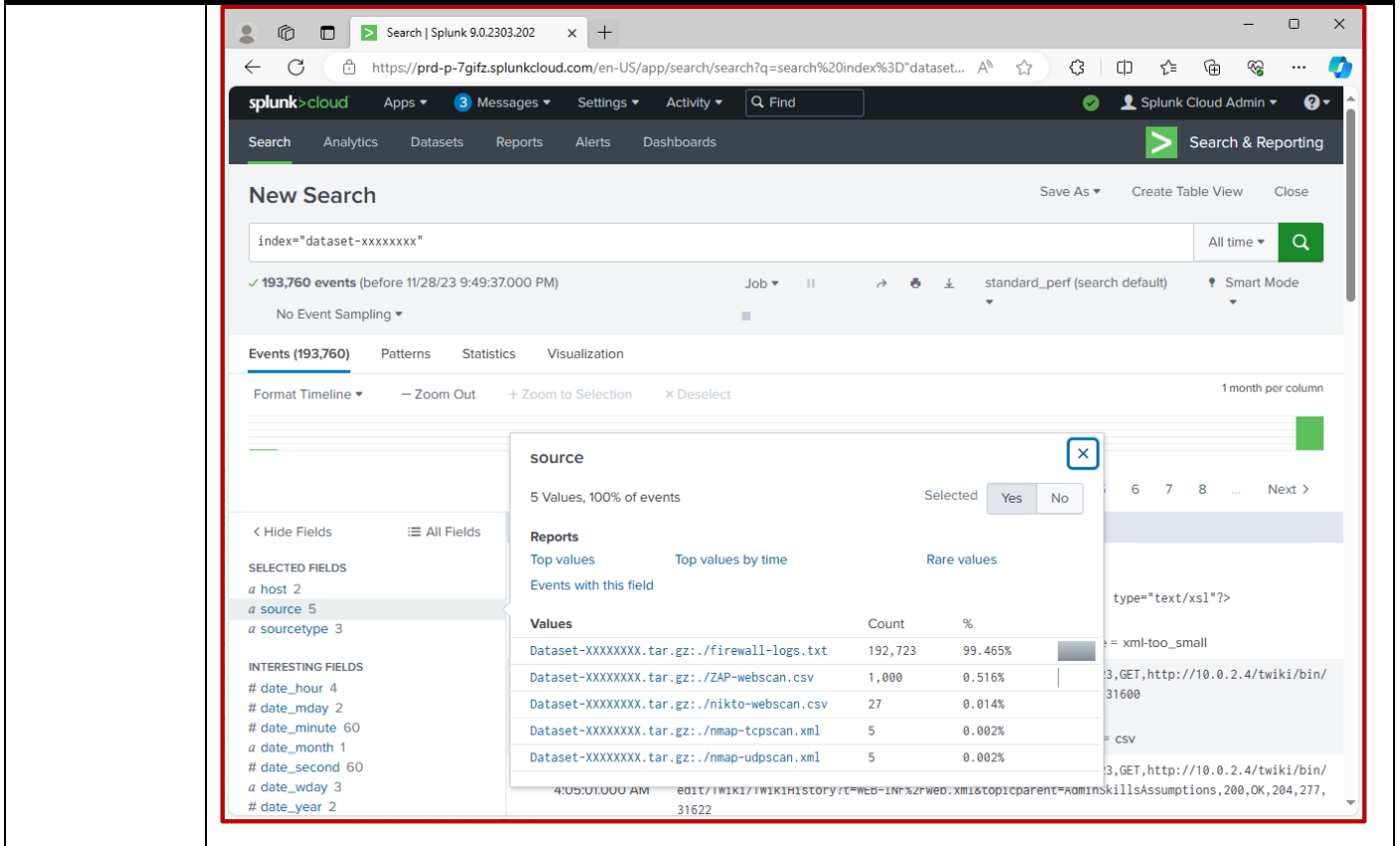
S NYS

The screenshots provided by the student should clearly indicate that they have successfully ingested the data into the analytical platform of their choice and have verified that the dataset is searchable using the specified index using the compressed archive file.

The following example shows the interface of the Splunk Cloud Platform and how an index is created first, and then the data is ingested and verified.

Table 5 - Answer table for Part D tasks

Criterion	Screenshot evidence
<p><i>Index creation</i></p>	 <p>Steps to create an index: Settings > Indexes > New index > dataset_XXXXXXXX</p> <p>Students will need to provide approximate values for max raw data size and searchable retention [days], if this is done in Splunk.</p>
<p><i>Dataset ingested to the analytical platform</i></p>	 <p>Selected the source file, which is the compressed archive file 'Dataset-XXXXXXXX'.tar.gz</p>
<p><i>Verified the ingested threat dataset in the analytical platform</i></p>	<p>Started a search using the specified index and ensured that the five log files in the dataset appear under the 'source' option.</p>



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: Collect threat data		
B1	Two [2] screenshots and interpretation	<input type="checkbox"/>
B2	One [1] screenshot and interpretation	<input type="checkbox"/>
B3	Three to five [3-5] screenshots and interpretation	<input type="checkbox"/>
B4	One to three [1-3] screenshots and interpretation	<input type="checkbox"/>
Part C: Create dataset		
C1	Three to five [3-5] screenshots Submitted dataset file: 'Dataset-<Student ID>.tar.gz'.	<input type="checkbox"/>
Part D: Ingest data logs to analytic platform		
D1-3	Three to five [3-5] screenshots	<input type="checkbox"/>

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 4!

© 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.