



**ICTSAS530**

# Use network tools

Assessment 2 of 6

Short Answer Questions

**Assessor Guide**



# Assessment Instructions

## Task Overview

This assessment task includes 12 short answer questions. Read each question carefully before typing your response in the space provided.

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

## 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.

Read the following scenario and access the resources provided to answer Questions 1 to 3.

**Scenario:** ABC Corporation, a leading financial institution, is planning to enhance the security of its network infrastructure due to increasing cybersecurity threats. The organisation deals with sensitive financial data and wants to ensure the confidentiality, integrity, and availability of its information. As the network administrator, you are tasked with proposing a comprehensive solution that includes both hardware and software components to strengthen the security posture of ABC Corporation's network.

### Question 1

Outline the features and functions of a high-security network.

[Word count: 65 – 100 words]

**Assessor instructions:** Students must demonstrate their understanding of the functions and features of a high-security network.

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 exemplar answer.

A sample answer is provided below.

A high-security network incorporates robust features and functions to safeguard sensitive data.

- It deploys advanced firewalls, intrusion detection/prevention systems, and encryption mechanisms for secure communication.
- Access controls, stringent authentication, and regular audits ensure authorised access.
- Hardware, like dedicated security appliances, and software, such as SIEM systems, collaboratively monitor and respond to potential threats.
- Network segmentation limits lateral movement, and redundancy mechanisms ensure continuous availability.
- Regular updates, vulnerability assessments, and employee training contribute to a proactive security posture.
- The holistic approach, combining both technical and procedural elements, establishes a resilient and reliable high-security network infrastructure.

### Question 2

Identify three (3) specific computing hardware and components that can be used to reinforce an organisation's network security. Outline the features and functions of each that contribute to the overall security of the network.

[Word count: 40-65 words per hardware/component]

**Assessor instructions:** Students must demonstrate their ability to identify organisational hardware and components and understand their functions and features.

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 exemplar answer.

A sample answer is provided below.

**Firewall Appliance:** Implementing a dedicated firewall appliance is crucial for controlling and monitoring network traffic. By defining and enforcing security policies, the firewall restricts unauthorised access and protects against various cyber threats. Additionally, features such as intrusion prevention and VPN support contribute to a robust defence mechanism.

**Intrusion Detection and Prevention System (IDPS):** Deploying an IDPS hardware device is essential for real-time monitoring of network activities. The IDPS identifies and responds to suspicious behaviour, providing an additional layer of defence against potential security breaches. Its ability to analyse patterns and detect anomalies enhances the overall threat detection capability.

**Hardware Security Module (HSM):** Utilising an HSM is crucial for managing cryptographic keys and performing secure cryptographic operations. The HSM ensures the integrity and confidentiality of sensitive data by safeguarding encryption keys, making it significantly challenging for malicious actors to compromise cryptographic operations.

### Question 3

Distinguish the functions and features between the following types of industry-recognised network tools for maintaining a high-security network.

- a) Command-line tools
- b) Hardware tools
- c) Software tools

For each type [a-c] of tool your answers in 'Table 1' must be within the specified word limit for the following criterion:

- d) Functions
- e) Features
- f) Example tool name, functionality and features:

**Assessor instructions:** Students must demonstrate their understanding of:

- different types of industry-recognised network tools to maintain high-security networks
- features and functions of command-line, software and hardware tools.

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 exemplar answer.

A sample answer is provided below.

Table 1 - Question 1: Answer table

Criterion:	Command-line tools	Hardware tools	Software tools
<b>Functions:</b> (Word count: 35-55)	Command-line tools are typically used for direct, text-based interaction with a system or application.  They are often employed for tasks such as network configuration,	Hardware tools in network security are physical devices designed to perform specific security functions.  They often handle tasks such as traffic filtering, encryption, and secure access control.	Software tools in network security are applications or programs that run on general-purpose computing devices.  They encompass a wide range of security functions,

Criterion:	Command-line tools	Hardware tools	Software tools
	troubleshooting, and security monitoring. Command-line tools allow administrators to execute specific commands to perform tasks efficiently.	Hardware tools are deployed at key points in the network infrastructure to enforce security policies.	from antivirus software to encryption utilities. Software tools are often flexible and can be updated easily to adapt to evolving security threats.
<b>Features:</b> [Word count: 25-45]	Lightweight and efficient, suitable for use in resource-constrained environments. Provide granular control over system configurations and network parameters. Often scriptable, allowing for automation of repetitive tasks.	Dedicated hardware for enhanced performance and reliability. Typically, these tools operate at the network layer, providing a proactive defense against threats. Hardware-based encryption for securing communication channels.	Can be installed on various platforms, making them adaptable to different environments. Regularly updated to address new vulnerabilities and threats. Configurable and customisable to suit specific security requirements.
<b>Example tool name, functionality and features:</b> [Word count: 35-55]	<b>Tool: nmap</b> Functionality: nmap is a powerful network scanning tool used to discover hosts, services, and vulnerabilities on a network. Features: It can perform a variety of scanning techniques, service version detection, and OS fingerprinting, providing detailed information about the network.	<b>Tool: Firewall Appliance</b> Functionality: A dedicated firewall appliance filters and monitors network traffic, enforcing security policies to protect against unauthorised access and cyber threats. Features: Stateful packet inspection, access control lists, VPN support, and intrusion prevention capabilities are common features found in firewall appliances.	<b>Tool: Wireshark</b> Functionality: Wireshark is a network protocol analyser used for troubleshooting, analysis, software and communication protocol development, and education. Features: Captures and analyses the data travelling back and forth on a network, helping security professionals identify network issues and potential security threats.

Read the following scenario and answer Questions 4, 5 and 6.

**Scenario:** Imagine you are a system administrator responsible for managing a network of computers in a large organisation. You need to perform routine tasks such as updating software, troubleshooting issues, conducting vulnerability scans and configuring network and security settings.

You are evaluating the use of command-line interface [CLI] versus graphical user interface [GUI] systems for these tasks.

#### Question 4

Differentiate the functions and features of the command-line interface [CLI] and graphical user interface [GUI] systems used for maintaining high-security networks.

[Word count: 75 – 100 words]

**Assessor instructions:** Students must demonstrate their understanding of the functions and features of CLI and GUI systems.

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 exemplar answer.

A sample answer is provided below.

The Command-Line Interface (CLI) relies on text commands, offering efficiency, resource conservation, and script automation for maintaining high-security networks. It excels in remote management and is preferred for its speed and precision.

In contrast, the Graphical User Interface (GUI) provides a user-friendly visual environment, aiding in the visualisation of network configurations. GUI is accessible to users with varying technical expertise, featuring point-and-click interactions, reducing the learning curve. GUI is advantageous for managing security policies visually.

The choice between CLI and GUI depends on factors such as task complexity, administrator expertise, and the need for automation in high-security network maintenance.

## Question 5

Analyse the use of command-line interface (CLI) and graphical user interface (GUI) systems for the tasks outlined in the given scenario by comparing their advantages and disadvantages.

[Word count: 165 – 200 words].

**Assessor instructions:** The student must analyse command-line and graphical user interface systems.

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.

In the given scenario, the choice between a command-line interface (CLI) and a graphical user interface (GUI) depends on the nature of the tasks at hand. CLI provides efficiency for experienced users due to its ability to execute commands quickly, script automation, and operate over SSH, making it suitable for remote administration. However, it has a steeper learning curve for beginners and may lack the visual feedback provided by a GUI.

On the other hand, a GUI offers an intuitive and visually-driven environment, making it accessible for users with varying technical expertise. It simplifies complex tasks through menus and buttons, reducing the likelihood of syntax errors. However, GUIs may be less efficient for repetitive tasks, lack some advanced features, and consume more system resources.

Ultimately, for routine tasks like updating software or configuring network settings, a GUI may be preferable for its user-friendly approach. Meanwhile, a CLI could be more efficient for troubleshooting and automation. The ideal choice depends on the administrator's skillset, task complexity, and the need for automation and speed.

## Question 6

Identify and discuss the specific command-line tools you would use, their functions, features and how they contribute to completing the tasks outlined in each of the analysis scenarios (a-c) in 'Table 2'.

For each analysis scenario ensure that your answer:

- identifies 2-3 examples of command-line tools and their functions (Word count: 90-130 words)
- outlines 2-3 features of the selected tools (Word count: 45-75 words)

**Assessor instructions:** Students must identify command-line tools according to the given analysis scenarios.

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 exemplar answer.

A sample answer is provided below.

Table 2 - Question 2: Answer table

Analysis scenario:	Command-line tools and their functions and features <i>[Word count: 110-145 per scenario]</i>	Features of the selected tools
<p>a) You need an efficient way to remotely update the software on multiple computers (both Windows and Linux) in your organisation.</p>	<p>One prominent command-line tool for software updates on Linux systems is 'apt-get' or 'yum,' depending on the distribution. For example, on Debian-based systems, 'sudo apt-get update' refreshes the package list, and 'sudo apt-get upgrade' installs the latest versions.</p> <p>PowerShell emerges as a robust command-line tool for remotely managing software updates on Windows computers. To initiate this process, one can leverage the 'Update-Help' command to ensure the PowerShell help system is up-to-date, gaining access to the latest cmdlets and modules related to software management.</p> <p>These command-line tools can be executed remotely over SSH or through other remote access methods, facilitating efficient administration and reducing the need for manual intervention.</p>	<p>Common features include the ability to:</p> <ul style="list-style-type: none"> <li>• install, update and remove packages</li> <li>• ensure that all required dependencies for a package are installed</li> <li>• manage software repositories to access and download packages</li> <li>• update the system with the latest available software packages</li> <li>• allow automation of package management tasks via scripts or commands</li> <li>• provide information about installed packages, repositories and dependencies</li> <li>• adjust package manager settings and preferences.</li> </ul>
<p>b) You need to analyse network connectivity issues on a Linux server, which requires an</p>	<p>To diagnose network connectivity issues on a Linux server, the following command-line tools can be utilised:</p> <ul style="list-style-type: none"> <li>• Ping: Use the ping command to check the reachability of a host and measure round-trip times. For example, ping google.com</li> </ul>	<p>Common features include:</p> <ul style="list-style-type: none"> <li>• Cross-platform compatibility – as these tools can be run on various Unix-like operating systems and it provides consistent functionality across</li> </ul>

Analysis scenario:	Command-line tools and their functions and features	Features of the selected tools
<p>efficient way to diagnose and troubleshoot any problems encountered.</p>	<p><i>[Word count: 110-145 per scenario]</i></p> <p>can help determine if the server can communicate with external hosts.</p> <ul style="list-style-type: none"> <li>• Traceroute: Employ the traceroute command to trace the route that packets take to reach a destination. This helps identify the specific network hop where connectivity issues may arise. For instance, traceroute example.com provides a detailed path analysis.</li> <li>• Netstat: Utilise Netstat to display network connections, routing tables, interface statistics, masquerade connections, and more. The command netstat -rn shows the routing table, aiding in identifying routing-related issues.</li> </ul> <p>These tools collectively offer insights into network connectivity problems, helping pinpoint and resolve issues efficiently.</p>	<p>these different platforms for network monitoring and troubleshooting.</p> <ul style="list-style-type: none"> <li>• Support for various options – options can be used to customise output, filter results and specify intervals for continuous monitoring. Options also allow users to tailor the output their specific requirements.</li> </ul>
<p>c) You need to monitor system resource usage on a Windows server to gather information on CPU, memory, and disk utilisation.</p>	<p>To monitor system resource usage on a Windows server, the following command-line tools can be employed:</p> <ul style="list-style-type: none"> <li>• Performance Monitor (PerfMon): Access the command-line version of PerfMon with perfmon. This tool allows you to collect and analyse performance data over time. You can use scripts or commands to automate data collection.</li> <li>• Resource Monitor: This tool can monitor the usage and performance of key Windows resources such as CPU, disk, network and memory in real time and allows for the identification of which processes are using which resources in the system</li> </ul> <p>These tools offer real-time and historical insights into CPU, memory, and disk usage, aiding in proactive monitoring and issue resolution.</p>	<p><b>Common features include:</b></p> <ul style="list-style-type: none"> <li>• <b>Customisable Counters:</b> Users can configure and customise performance counters to monitor specific aspects of system performance based on their requirements.</li> <li>• <b>Graphical Representation:</b> Both tools offer graphical representation of performance data, facilitating visualisation and analysis through charts, graphs, and reports.</li> <li>• <b>Logging and Data Storage:</b> PerfMon support logging and data storage capabilities, allowing users to log performance data to files for later analysis and reporting.</li> </ul>
<p>d) You are responsible for securing a web server and need to identify</p>	<p>To identify potential vulnerabilities on a web server, the following command-line tools can be utilised:</p> <ul style="list-style-type: none"> <li>• Nmap (Network Mapper): Use nmap to perform network scans, identify open</li> </ul>	<p><b>Common features include:</b></p> <p>Network scanning capabilities to discover hosts, services, and open ports.</p>



Analysis scenario:	Command-line tools and their functions and features	Features of the selected tools
potential vulnerabilities.	<p data-bbox="419 181 807 210"><i>[Word count: 110-145 per scenario]</i></p> <p data-bbox="509 217 1007 405">ports, and gather information about the services running on those ports. For example, <code>nmap -p 1-1000 example.com</code> scans the first 1000 ports on the specified host.</p> <ul data-bbox="461 432 1007 913" style="list-style-type: none"> <li data-bbox="461 432 1007 620">• Nikto: Employ nikto for web server scanning, detecting outdated software, and potential vulnerabilities. The command <code>nikto -h http://example.com</code> scans a web server for common issues.</li> <li data-bbox="461 647 1007 913">• OpenVAS (Open Vulnerability Assessment System): Utilise the <code>openvas-cli</code> command to interact with OpenVAS for vulnerability scanning. This tool checks for known vulnerabilities in the system and provides detailed reports.</li> </ul> <p data-bbox="411 936 1007 1084">These tools assist in identifying and addressing security vulnerabilities, ensuring the web server's integrity and safeguarding against potential threats.</p>	<p data-bbox="1038 217 1437 365">Vulnerability detection and assessment to identify security weaknesses and misconfigurations.</p> <p data-bbox="1038 387 1401 495">Reporting functionalities to generate detailed reports on discovered vulnerabilities.</p> <p data-bbox="1038 517 1453 624">Customisation options to tailor scans according to specific requirements and environments.</p> <p data-bbox="1038 647 1422 795">Integration with other security tools and frameworks for enhanced analysis and remediation.</p>

Read the following scenario and answer Questions 7 and 8.

Scenario: ABC Corporation, a leading financial institution, is planning to enhance the security of its network infrastructure due to increasing cybersecurity threats. The organisation deals with sensitive financial data.

As a system administrator, you need to perform routine work tasks such as vulnerability assessments and running diagnostic tests on a high-security server using command-line text.

### Question 7

Outline the functions and features of command-line text for carrying out work tasks in the scenario.

[Word count: 75-100 words]

**Assessor instructions:** Students must demonstrate their understanding of the functions and features of command-line text.

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 exemplar answer.

A sample answer is provided below.

#### Features of command-line text:

- Text-Based Interaction: Enables users to interact with a computer system using text commands.

- **Efficiency:** Streamlines tasks through direct command execution, minimising graphical interface navigation.
- **Scripting:** Supports automation through scriptable commands, allowing users to create and execute scripts.

#### Functions of command-line text:

- **System Configuration:** Adjusts system settings, network configurations, and user permissions.
- **File Management:** Creates, deletes, copies, and moves files and directories.
- **Process Control:** Manages running processes, monitors system performance, and troubleshoots issues.

#### Other answers may include:

##### Features:

- **Resource Efficiency:** Consumes fewer system resources compared to graphical interfaces.
- **Granular Control:** Offers precise control over system configurations and operations.

##### Functions

- **Network Operations:** Performs tasks like network diagnostics, protocol analysis, and connectivity testing.
- **Security Operations:** Implements security measures, such as access controls and encryption, for enhanced system security.

## Question 8

Outline three (3) key organisational processes and requirements for writing command-line text to conduct work tasks in the scenario.

[Word count: 75-100 words]

**Assessor instructions:** Students must outline organisational processes and requirements for writing command-line text.

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 exemplar answer.

A sample answer is provided below.

- **Scripting Standards:**  
Define scripting standards specifying coding practices, documentation requirements, and version control (allowing for easy tracking of changes, rollbacks, and collaboration among multiple administrators) to maintain consistency and facilitate collaboration.
- **Code Review Processes:**  
Institute code review processes to assess the security implications of command-line scripts, ensuring adherence to best practices and identifying potential vulnerabilities.
- **Documentation Requirements:**

Mandate thorough documentation for command-line scripts, including their purpose, usage instructions, and potential security implications, promoting transparency and knowledge sharing.

Other answers may include:

- **Policy Development:**  
Establish organisational policies that dictate the use of command-line tools, defining acceptable commands and scripting practices in alignment with security objectives.
- **Logging and Auditing:**  
Enable logging and auditing mechanisms for command-line activities, ensuring that all script executions are recorded for accountability and forensic purposes.
- **Secure Credential Management:**  
Establish secure practices for storing and managing credentials within scripts, such as using encryption or secure key management systems to prevent unauthorised access.
- **Security Testing:**  
Integrate security testing into the development lifecycle, conducting regular assessments of command-line scripts for vulnerabilities and potential exploits.

## Question 9

Discuss two (2) different strategies to undertake risk analysis in a high-security network.

[Approximate word count: 95 - 120 words]

**Assessor instructions:** Students must demonstrate their understanding of strategies to undertake risk analysis.

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 exemplar answer.

A sample answer is provided below.

**Business Impact Analysis:**

- Identify critical business processes and assets.
- Assess potential impacts of disruptions or security breaches on these processes.
- Determine recovery time objectives (RTO) and recovery point objectives (RPO) for each process.
- Evaluate dependencies between processes and prioritise them based on their criticality to the organisation.
- Develop strategies to mitigate risks and ensure continuity of operations.

**Data Analysis:**

- Analyse the organisation's data assets, including sensitive information and intellectual property.
- Assess data access controls, encryption methods, and data integrity mechanisms.
- Identify potential threats to data confidentiality, integrity, and availability.
- Evaluate data storage, transmission, and backup mechanisms for vulnerabilities.
- Develop data protection strategies, such as encryption, access controls, and data loss prevention (DLP) measures.

Other answers may include:

### Monte Carlo Simulation:

- Model various scenarios and their associated probabilities based on historical data and expert judgment.
- Simulate the impact of these scenarios on the network's security posture.
- Analyse the results to identify potential vulnerabilities and their likelihood of occurrence.
- Incorporate feedback from stakeholders to refine the simulation model.
- Use the insights gained to prioritise risk mitigation efforts and allocate resources effectively.

### Tree Assessment:

- Construct a hierarchical tree structure representing different elements of the network, including assets, threats, vulnerabilities, and controls.
- Assess the likelihood and impact of various threats and vulnerabilities on each node of the tree.
- Analyse the effectiveness of existing security controls in mitigating identified risks.
- Identify potential gaps in the security posture and prioritise remediation efforts based on their criticality.
- Continuously update the tree assessment to reflect changes in the network environment and emerging threats.

### Quantitative Analysis:

- Assign numerical values to risks, such as potential financial losses or the likelihood of a security breach.
- Calculate risk exposure by multiplying the impact and likelihood of each risk.
- Use mathematical models and statistical techniques to quantify uncertainties and assess the overall risk level.
- Determine the return on investment (ROI) of security measures by comparing the cost of mitigation to the expected loss reduction.
- Enable informed decision-making by providing stakeholders with quantifiable metrics for risk management.

### Qualitative Analysis:

- Evaluate risks based on subjective criteria, such as expert judgment, experience, and intuition.
- Use risk matrices or heat maps to categorise risks according to their severity and likelihood.
- Conduct workshops or interviews with stakeholders to gather qualitative insights into potential threats and vulnerabilities.
- Identify emerging risks and trends in the threat landscape through open-ended discussions and brainstorming sessions.
- Supplement quantitative data with qualitative analysis to gain a comprehensive understanding of the network's risk profile.

## Question 10

List and describe five (5) techniques for categorising system vulnerability alerts.

[Approximate word count: 95 - 120 words for technique]

**Assessor instructions:** Students must demonstrate their understanding of techniques to categorise system vulnerability alerts.

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 exemplar answer.

A sample answer is provided below.

<ol style="list-style-type: none"> <li><b>Severity level</b> – Assign severity levels (e.g., critical, high, medium, low) based on the potential impact of the vulnerability on system integrity, confidentiality, and availability.</li> <li><b>Common Vulnerability Scoring System (CVSS):</b> Utilise the CVSS to quantify and rank vulnerabilities, considering factors like exploitability, impact, and complexity.</li> <li><b>Categorisation by Exploitation Vector:</b> Classify alerts based on the vectors through which vulnerabilities can be exploited, such as network-based, local, or physical access.</li> <li><b>Asset Criticality:</b> Prioritise vulnerabilities affecting critical assets, categorising them based on the importance of the compromised asset to overall business functions.</li> <li><b>User Access Level:</b> Consider the access level required for exploiting vulnerabilities, categorising them based on whether they require local access, network access, or privileged credentials.</li> </ol>
---

### Question 11

List three (3) common types of security threats on devices and networks and outline their features.

[Approximate word count: 60-95 words]

**Assessor instructions:** Students must demonstrate their understanding of strategies to undertake risk analysis.

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 exemplar answer.

A sample answer is provided below.

Table 3 – Question 10: Answer table

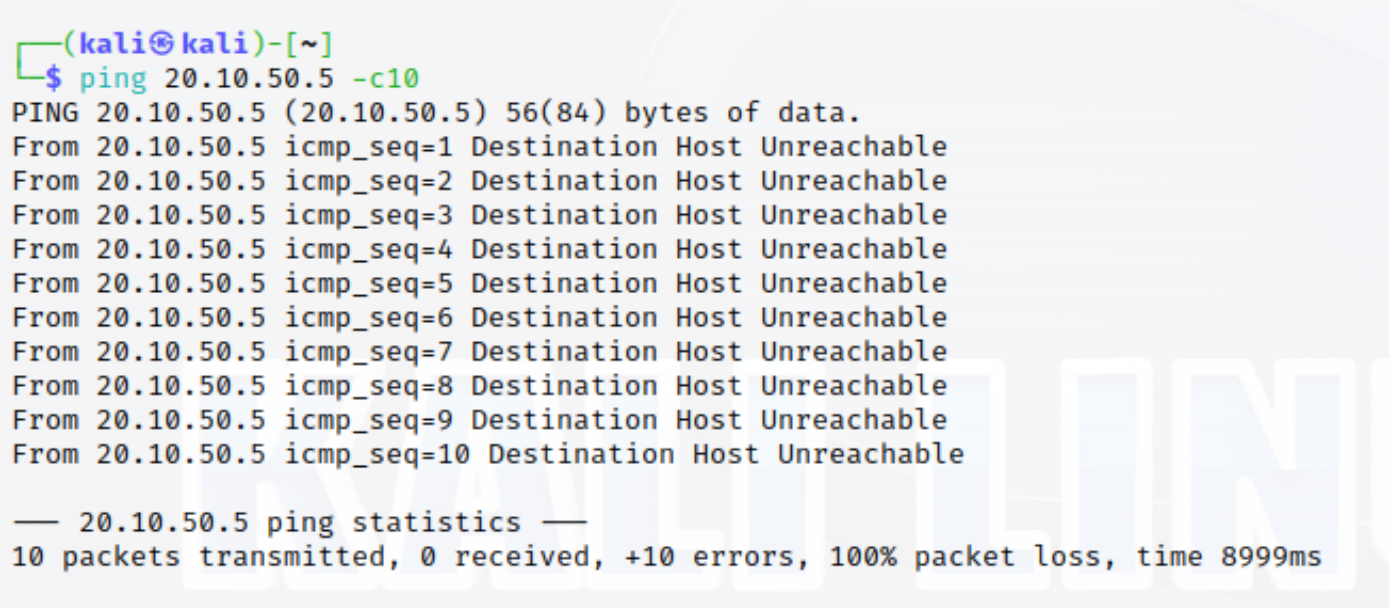
Security threat types	Features
<i>[Word count: 45-75 words per tool]</i>	
A. Malware	<p><b>Infection:</b> Malware, including viruses, worms, and Trojans, can infect devices through various means, such as malicious downloads, email attachments, or compromised websites.</p> <p><b>Payload:</b> Malware often carries a payload that can disrupt normal device functions, steal sensitive information, or provide unauthorised access to a system.</p> <p><b>Self-Replication:</b> Worms and certain viruses have the ability to self-replicate and spread across networks, increasing the scope and impact of the infection.</p> <p><b>Concealment:</b> Malware may employ tactics to evade detection by antivirus software, making it challenging to identify and remove.</p>
B. Phishing	<p><b>Deceptive Communication:</b> Phishing attacks typically involve fraudulent emails, messages, or websites that mimic legitimate sources to trick users into revealing sensitive information.</p>

Security threat types	Features
<i>[Word count: 45-75 words per tool]</i>	
	<p><b>Social Engineering:</b> Phishers use psychological manipulation to exploit human trust, often posing as trustworthy entities such as banks, government agencies, or well-known companies.</p> <p><b>Credential Theft:</b> The primary goal is to steal usernames, passwords, or financial information, which can be used for unauthorized access or identity theft.</p> <p><b>Spoofing:</b> Phishing attempts may involve email or website spoofing to appear genuine, adding to the deception.</p>
C. DOS Attacks	<p><b>Network Overload:</b> DoS attacks flood a network, system, or service with excessive traffic, overwhelming its capacity and causing disruptions.</p> <p><b>Distributed Denial of Service (DDoS):</b> DDoS attacks involve multiple compromised devices, forming a botnet that collaboratively floods the target, making mitigation more challenging.</p> <p><b>Service Unavailability:</b> The primary goal is to make a service or network resource temporarily or indefinitely unavailable to legitimate users.</p> <p><b>Amplification:</b> Some DoS attacks use amplification techniques, such as DNS or NTP reflection, to magnify the volume of attack traffic.</p>

Refer to the following scenario and answer Question 12.

**Scenario:** A network administrator had setup a 'Kali Linux' machine to conduct security tests and wants to run a vulnerability test on a web server with an IP address of 20.10.50.5.

Before conducting the vulnerability tests, the network administrator wants to check network connectivity between the test 'Kali Linux' machine and the web server. Following is a screenshot of the results obtained from the network connectivity test.



```

(kali@kali)-[~]
└─$ ping 20.10.50.5 -c10
PING 20.10.50.5 (20.10.50.5) 56(84) bytes of data:
From 20.10.50.5 icmp_seq=1 Destination Host Unreachable
From 20.10.50.5 icmp_seq=2 Destination Host Unreachable
From 20.10.50.5 icmp_seq=3 Destination Host Unreachable
From 20.10.50.5 icmp_seq=4 Destination Host Unreachable
From 20.10.50.5 icmp_seq=5 Destination Host Unreachable
From 20.10.50.5 icmp_seq=6 Destination Host Unreachable
From 20.10.50.5 icmp_seq=7 Destination Host Unreachable
From 20.10.50.5 icmp_seq=8 Destination Host Unreachable
From 20.10.50.5 icmp_seq=9 Destination Host Unreachable
From 20.10.50.5 icmp_seq=10 Destination Host Unreachable

— 20.10.50.5 ping statistics —
10 packets transmitted, 0 received, +10 errors, 100% packet loss, time 8999ms

```

## Question 12

Analyse the outcome of the network connectivity test and outline:

- two (2) possible root causes of the issue
- the use of problem-solving techniques to resolve the issue.

[Approximate word count: 90–120 words]

**Assessor instructions:** Students must demonstrate their understanding of using problem-solving techniques to analyse outcomes and manage networks.

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 exemplar answer.

A sample answer is provided below.

1. **Incorrect IP Address or Gateway Configuration:** If the IP address of the destination host or the default gateway is configured incorrectly on either the source or destination device, the ping test will fail to reach the intended destination.
2. **Cable Faults:** Physical network cables connecting the source and destination devices may be damaged, disconnected, or improperly connected. This could result in a failure to establish a connection and transmit ICMP packets between the devices.

By systematically investigating these potential root causes through troubleshooting steps such as checking configurations, examining network hardware, and testing physical connections, network administrators can pinpoint the source of the ping test failure and take appropriate corrective actions to restore connectivity and ensure network reliability.

Other root causes may include:

- **Misconfigured Firewall:** If the firewall settings are too restrictive, they may block ICMP (Internet Control Message Protocol) packets used by ping tests. This can prevent successful communication between the source and destination.
- **Hardware Failure:** Network interface cards (NICs), switches, routers, or other network hardware may malfunction or fail, preventing successful transmission and reception of ICMP packets necessary for the ping test.

# Assessment submission checklist

Students must have completed all questions within this assessment before submitting. This includes:

1	12 short answer questions completed in the spaces provided.	<input type="checkbox"/>
---	---	--------------------------

## Assessment feedback

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

<b>Assessor comments:</b>	<input type="checkbox"/> S	<input type="checkbox"/> NYS

  
**Congratulations, you have reached the end of Assessment 2!**

© 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.