RWANDA POLYTECHNIC

MUSANZE COLLEGE

DEPARTMENT: ICT

PROGRAM: INFORMATION TECHNOLOGY

RQF LEVEL: 8

MODULE: CYBERSECURITY

Academic: 2024-2025

ASSISSGNMENT 1

Date: 15/03/2025

Name: NIYIGABA Claude

Reg No: 24RP14647

Email: niyigabaclaujesus@gmail.com

Q1. Which best practices used to detect and identify malwares?

Detecting and identifying malware requires a combination of proactive measures, tools, and best practices. Here are the **best practices** used to detect and identify malware effectively:

i.Use Antivirus and Anti-Malware Software

- Install and regularly update reputable antivirus and anti-malware tools (e.g., Windows Defender, Malwarebytes, Kaspersky, Norton).
- Enable real-time scanning to detect threats as they occur.

ii.Keep Systems and Software Updated

- Regularly update operating systems, applications, and firmware to patch vulnerabilities that malware exploits.
- Enable automatic updates where possible.

iii.Monitor Network Traffic

- Use network monitoring tools (e.g., Wireshark, Zeek, or intrusion detection systems like Snort) to identify unusual traffic patterns.
- Look for connections to known malicious IP addresses or domains.

iv.Analyze System Behavior

- Monitor system performance for unusual activity, such as:
  - High CPU, memory, or disk usage.
  - Unexpected processes or services running.
- Use tools like **Process Explorer** (Windows) or **htop** (Linux) to inspect running processes.

v.Implement Endpoint Detection and Response (EDR)

- Use EDR solutions to monitor endpoints for suspicious activity and respond to threats in real time.

- Examples: CrowdStrike, Microsoft Defender for Endpoint, SentinelOne.

vi.Enable Firewalls and Intrusion Prevention Systems (IPS)

- Configure firewalls to block unauthorized access and monitor inbound/outbound traffic.
- Use IPS to detect and block known attack patterns.

vii.Conduct Regular Scans

- Perform full system scans periodically to detect hidden malware.
- Use tools like **Malwarebytes** for additional scans.

viii.Use Sandboxing for Suspicious Files

- Execute suspicious files in a secure, isolated environment (sandbox) to analyze their behavior.
- Tools: Cuckoo Sandbox, Joe Sandbox, or cloud-based solutions like Hybrid Analysis.

ix.Check for Indicators of Compromise (IOCs)

- Look for known IOCs, such as:
  - Malicious file hashes (MD5, SHA-256).
  - Suspicious registry entries or file paths.
  - Known malicious domains or IP addresses.
- Use threat intelligence platforms like VirusTotal or AlienVault OTX to analyze IOCs.

x.Monitor User Behavior

- Educate users about phishing and social engineering attacks.
- Monitor for unusual user activity, such as:
  - Logins from unfamiliar locations or devices.
  - Unauthorized access to sensitive files.

xi.Implement Email Security Measures

- Use email filtering tools to block phishing emails and malicious attachments.
- Train users to identify suspicious emails and avoid clicking on unknown links.

xii.Backup Data Regularly

- Maintain regular backups of critical data and ensure they are stored securely.
- Test backups periodically to ensure they can be restored in case of a ransomware attack.

xiii.Use Behavioral Analysis

- Deploy tools that use machine learning and behavioral analysis to detect zero-day threats.
- Examples: Darktrace or Microsoft Defender for Endpoint.

xiv.Leverage Threat Intelligence

- Stay informed about the latest malware trends and threats by subscribing to threat intelligence feeds.
- Use platforms like VirusTotal, AlienVault OTX, or Recorded Future.

xv.Perform Regular Audits and Penetration Testing

- Conduct security audits to identify vulnerabilities in your systems.
- Perform penetration testing to simulate attacks and identify weaknesses.

xvi.Isolate and Investigate Infected Systems

- If malware is detected, isolate the infected system from the network to prevent further spread.
- Use forensic tools (e.g., FTK Imager, Autopsy) to analyze the malware and determine its impact.

xvii.Educate and Train Employees

- Train employees on cybersecurity best practices, such as:

- Avoiding suspicious downloads or links.
- Recognizing phishing attempts.
- Reporting unusual system behavior.

xviii. Use Multi-Factor Authentication (MFA)

Implement MFA to reduce the risk of unauthorized access, even if credentials are compromised.

xix. Monitor for Ransomware Indicators

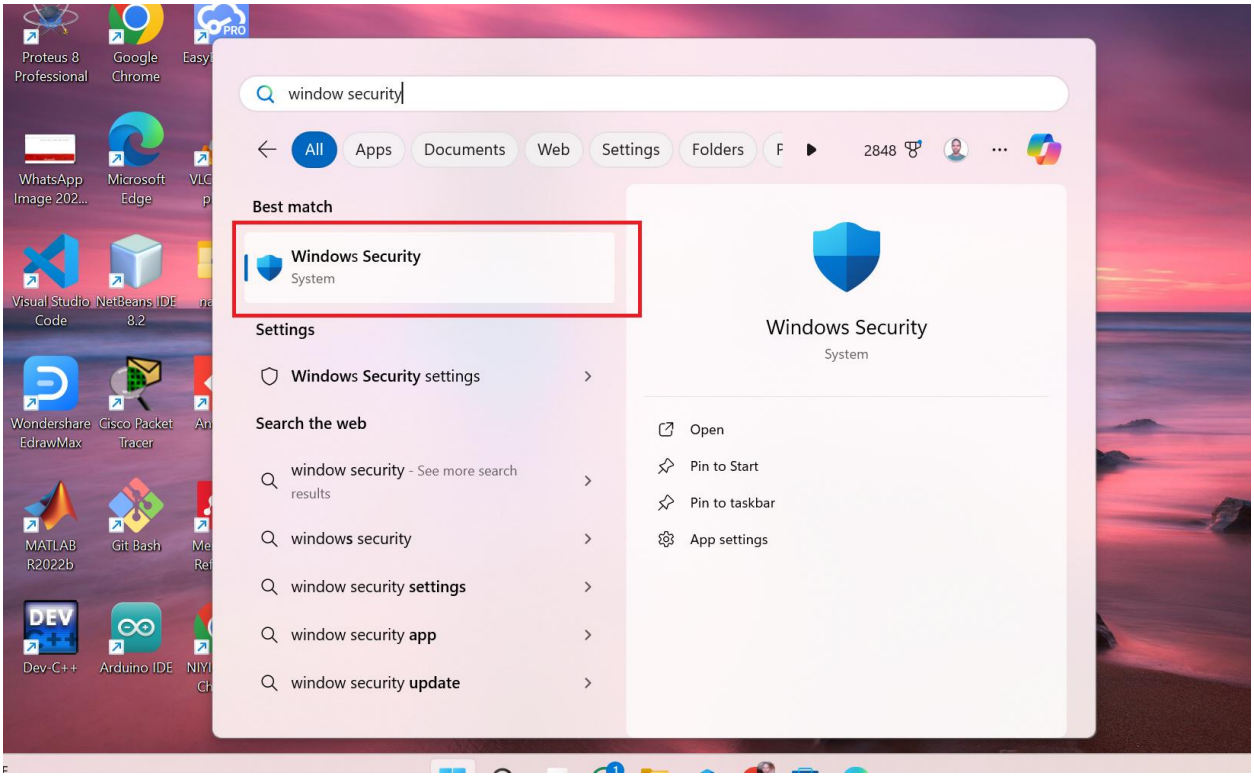
- Look for signs of ransomware, such as:
  - Encrypted files with unusual extensions.
  - Ransom notes or messages demanding payment.
- Use ransomware-specific detection tools like **RansomWhere?** or **CryptoPrevent**.

xx. Collaborate with Cybersecurity Experts

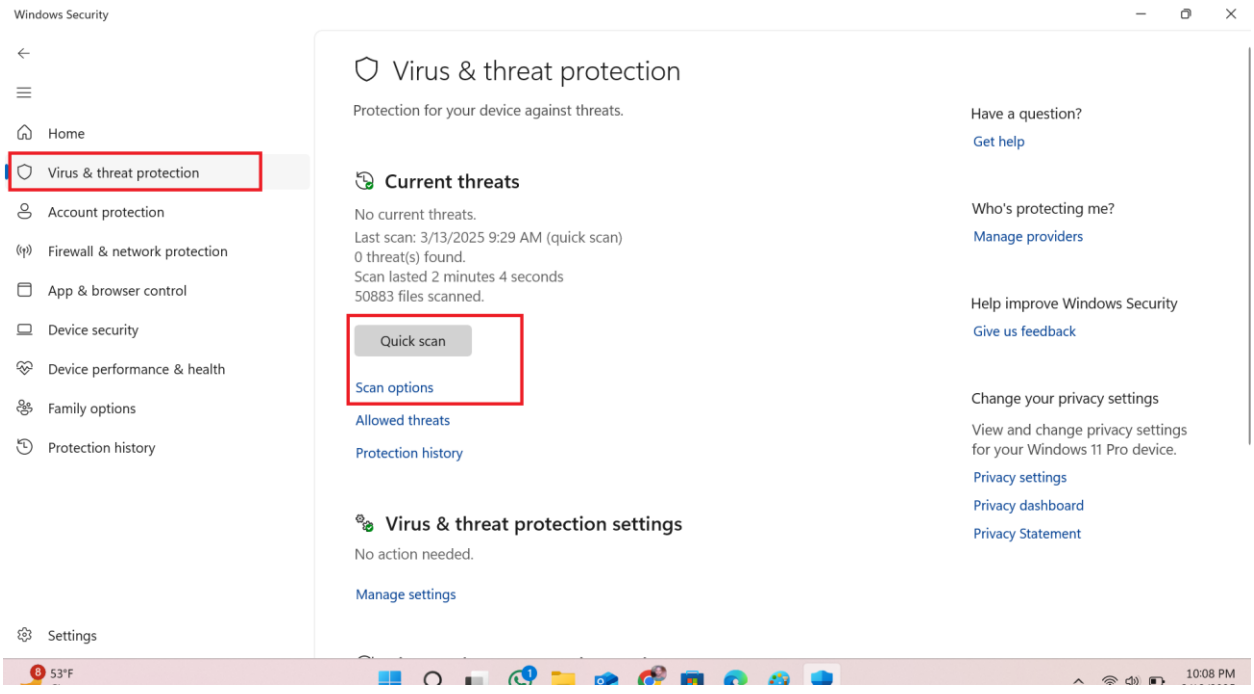
If malware is detected, consult with cybersecurity professionals or incident response teams to mitigate the threat effectively.

Q2. From one practice, screenshot ho to identify a malware.

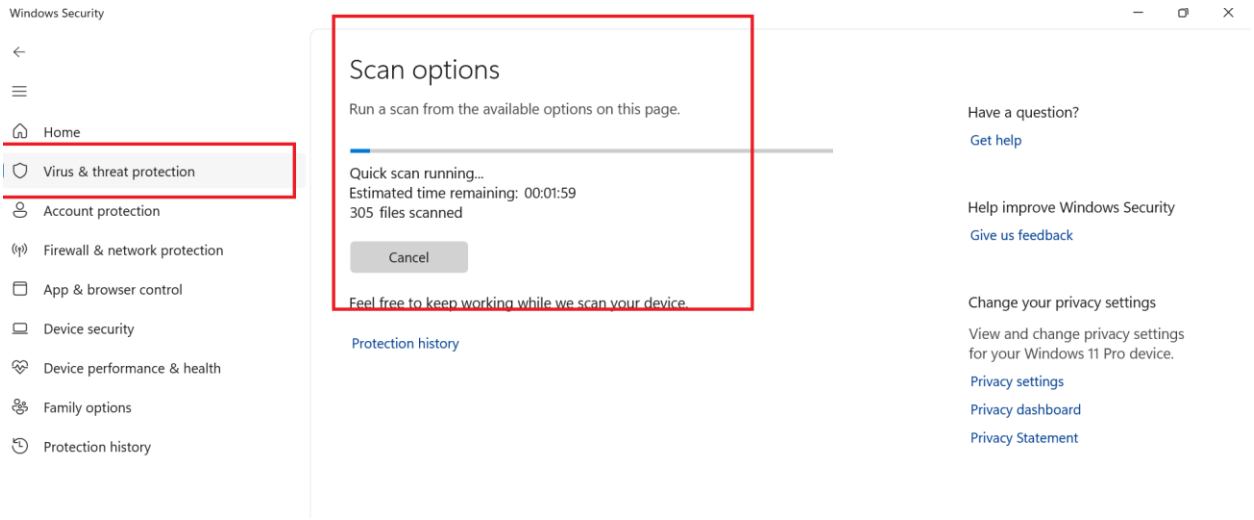
Step 1


window security
All
Apps
Documents
Web
Settings
Folders
2848
Best match
Windows Security
System
Settings
Windows Security settings
Search the web
window security - See more search results
windows security
window security settings
window security app
window security update
Windows Security
System
Open
Pin to Start
Pin to taskbar
App settings
Proteus 8 Professional
Google Chrome
WhatsApp Image 202...
Microsoft Edge
Visual Studio Code
NetBeans IDE 8.2
Wondershare EdrawMax
Cisco Packet Tracer
MATLAB R2022b
Git Bash
Dev-C++
Arduino IDE

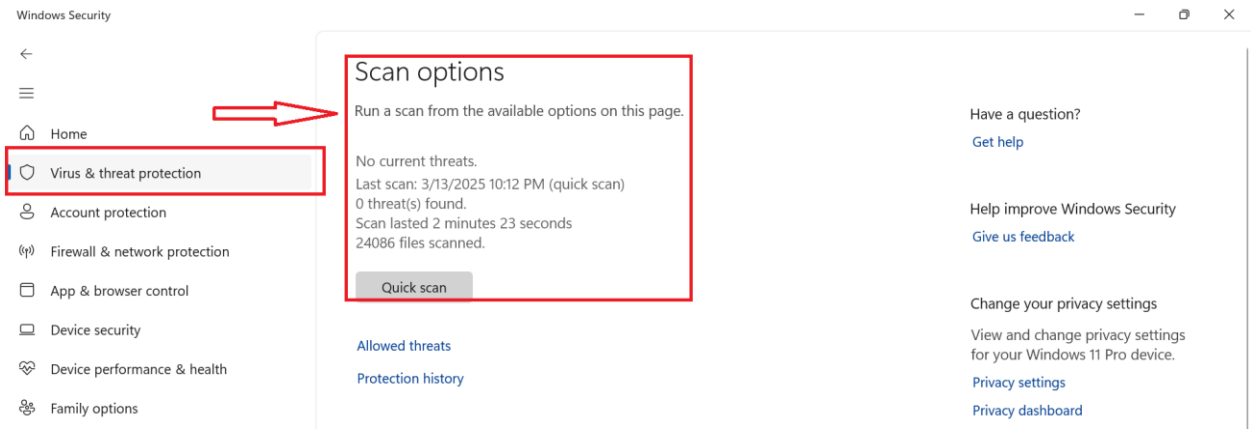
Step 2

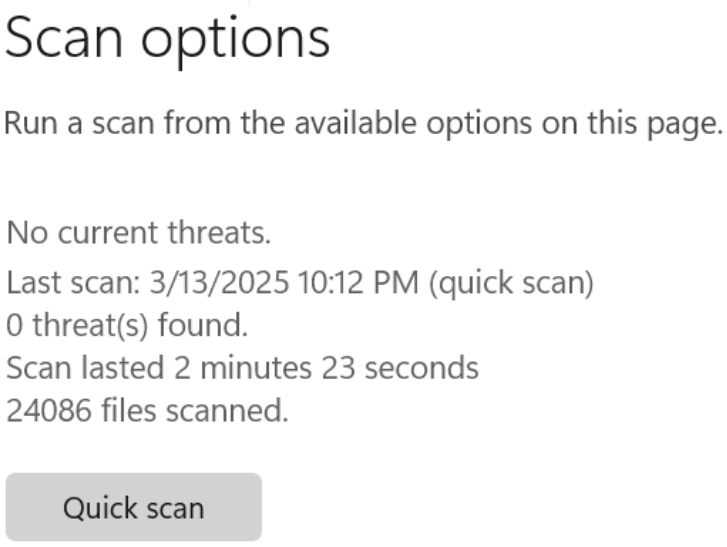

Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Settings
Virus & threat protection
Protection for your device against threats.
Current threats
No current threats.
Last scan: 3/13/2025 9:29 AM (quick scan)
0 threat(s) found.
Scan lasted 2 minutes 4 seconds
50883 files scanned.
Quick scan
Scan options
Allowed threats
Protection history
Virus & threat protection settings
No action needed.
Manage settings
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard
Privacy Statement
53°F
10:08 PM

Step 3


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Scan options
Run a scan from the available options on this page.
Quick scan running...
Estimated time remaining: 00:01:59
305 files scanned
Cancel
Feel free to keep working while we scan your device.
Protection history
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard
Privacy Statement

Step 4


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Scan options
Run a scan from the available options on this page.
No current threats.
Last scan: 3/13/2025 10:12 PM (quick scan)
0 threat(s) found.
Scan lasted 2 minutes 23 seconds
24086 files scanned.
Quick scan
Allowed threats
Protection history
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard


Scan options
Run a scan from the available options on this page.
No current threats.
Last scan: 3/13/2025 10:12 PM (quick scan)
0 threat(s) found.
Scan lasted 2 minutes 23 seconds
24086 files scanned.
Quick scan