اونيۏرسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LAB 9: ADMINISTERING A SECURE NETWORK

NAME: FATIN NASUHA BINTI MOHAMED SABIR

MATRIC NO: B032110289

PROGRAM: 3 BITZ S1G1

1. **Using a Secure Email Feature**
   a. How valuable is this feature?
      i. This feature is valuable as it prevents unauthorized access, forwarding and download to an email messages.
   b. Is it easy to use?
      i. Yes as it is straightforward and easy to set up.
   c. What are the limitations?
      i. The receiver can still copy the messages if they have a software for the said purpose. This feature also does not help in preventing screenshot of the email messages.
2. **Viewing Logs Using the Microsoft Windows Event Viewer**
   a. What is the importance of viewing logs?
      i. It provides early threat detection as logs can reveal early signs of potential security threats before they escalate into a full-blown attack.
      ii. We can also identify patterns and spot anomalies by analysing log data.
   b. Explain what information you can get from Windows Logs?
      i. System health and stability
         - Security events by monitoring failed login attempts
         - Windows updates and service Events. Details on the installed updates, service startup and shutdown and diagnose issues related to Windows core functionality
      ii. User activity and system usage
         - Tracking login and logout events including local and remote login
         - Monitor which files were accessed or modified by different users and applications.
   c. Explain for each section: Application, Security, Setup, System and Forwarded Events.
      i. Application

- It tracks events generated by installed applications and services which could be useful for troubleshooting application crashes and understanding application activity.

ii. Security

- It provides log events related to system security and user access which is critical for monitoring access attempts and potential security breaches.

iii. Setup

- It records events related to system installations, upgrades and configuration changes which is important in troubleshooting installation and upgrade issues, tracking configuration changes and diagnosing potential compatibility issues.

iv. System

- It shows log events generated by core system components and drivers which is crucial for troubleshooting performance problems and diagnosing hardware problems.

v. Forwarded Events

- It captures events forwarded from other machines or applications within the network.

d. Explain what information you can get from Application and Services Logs?

i. Application crashes and errors by analyzing which application is crashing and the frequency of these crashes.

ii. Failed login attempts, and unauthorized access can be useful for detecting potential malware or unauthorized access.

e. Explain for each section; Hardware Events, Internet Explorer, Key Management Service, Media Center

i. Hardware Events

- Tracks event generated by the system's hardware devices and their drivers

ii. Internet Explorer

- Record events related to the activity of the Internet Explorer

iii. Key Management Service

- Log events related to managing and using cryptographic keys used for data encryption and security