Class 16

Nayem Al Hakim

Id: 2111254

Security issues related to systems and networks:

1. **Common Security Issues**: The document identifies that many exploits target a limited number of security issues, which can be effectively managed through proper strategies and frameworks.
2. **Troubleshooting Strategies**: It discusses various troubleshooting methods for common security problems and the output from different security technologies, such as host-based firewalls, application whitelisting, and removable media control.
3. **Access Violations and Data Protection**: The text emphasizes the importance of authentication, permission configurations, and the use of certificates to secure communications. It also highlights the risks of data exfiltration and suggests measures like disabling USB ports and implementing Data Loss Prevention (DLP) features.
4. **Security Technologies Output**: The document outlines how to analyze and interpret output from security devices, including Host-based Intrusion Detection Systems (HIDS), antivirus software, and file integrity checks, to identify potential threats and suspicious activities.
5. **Vulnerability Analysis**: It stresses the need to analyze vulnerability scan results, considering the criticality and likelihood of exploitation, and the potential impact on network resources. The importance of integrating data from various sources, such as firewall logs and penetration tests, is also noted.