Ochiq kodli OT xavfsizligi (eng)

1. Analyze in detail the main differences in licensing, transparency, and security philosophy between open source operating systems (OS) and proprietary OSes (e.g., Windows/macOS). (Explain the concept of "Security by Transparency".)

2. In-depth justify the impact of the open source operating system development model (community, foundation, consortium) on security, in particular, how it positively and negatively affects the speed of vulnerability detection and patching.

3. MAC used in Linux OS

4. How do (Enforced Access Control) mechanisms (SELinux, AppArmor) work? Explain their advantages and limitations over discretionary access control (DAC) with examples.

5. What is the "Attack Surface" in open source systems and how open source operating systems (e.g., minimal Linux distributions) allow it to be drastically reduced compared to closed OSes?

6. What is the role of licensing and audit capabilities (SBOM, reproducible builds) of open source operating systems in meeting corporate compliance (e.g. ISO 27001 or CIS Benchmarks) requirements?

7. What functions do package managers (apt, dnf) used in Linux distributions perform from a security perspective (repo signatures, centralized updates) and how does this mechanism differ from the update process in closed systems?

8. Explain the main functions of namespaces, cgroups and seccomp, which are security mechanisms at the kernel level of the operating system, and highlight their importance in ensuring container (Docker, Kubernetes) security.

9. Explain with examples the importance of LTS (Long Term Support) distributions in Linux security standards in ensuring stability and long-term protection.

10. How does Kernel Live Patching (kpatch, Ksplice) technology work in Linux systems and justify its importance in improving security while ensuring continuous operation of the system.

11. Analyze how the flexible architecture of open source OSes allows them to create optimal security configurations for different industries (server, cloud, IoT, mobile - Android).

12. What serious threats does misconfiguration of file system permissions (rwx) pose to Linux security? What combination of permissions is optimal for protecting sensitive files?

13. What is the risk of Privilege Escalation? What mechanisms can this attack be carried out on Linux systems (for example, incorrect sudo configuration)? What are the defenses against it?

14. How does the Buffer Overflow vulnerability occur in the Linux environment? How can an attacker exploit this vulnerability to execute his code, and what defense mechanisms do modern Linux kernels use to protect against this attack?

15. Prove that the human factor is the biggest vulnerability in the security of Linux systems. How do errors such as weak passwords, phishing, and negligence affect system security, and what training policies should be implemented to eliminate them?

16. List common vulnerabilities that arise as a result of incorrect configuration settings (for example, unnecessary services, default passwords). What hardening actions should an administrator regularly perform to minimize these risks?

17. What threats do vulnerabilities in network services (for example, SSH, Web server) pose? Explain the mechanism of remote exploitation through them.

18. Distinguish the types of malware (virus, trojan, rootkit) common against Linux systems and analyze their features of entry into the system, hiding and operation.

19. How is a Rootkit attack detected in Linux systems and what mechanisms for its hiding in the system (kernel or user space) are there? What are the difficulties in removing rootkits?

20. Explain with examples the importance of the principle of minimizing user rights (Least Privilege Principle) in ensuring Linux security. How can this principle be applied in practice?

21. Analyze the complementary function of iptables/nftables and SELinux/AppArmor mechanisms in increasing the security of a Linux system. What level of protection does each provide?

22. What is the main role of scripting technologies (Python, Bash) in cybersecurity? Analyze the advantages and limitations of automating the process of detecting vulnerabilities using them.

23. Analyze the advantages of Python in cybersecurity (flexibility, libraries). What are the basic principles of a port scanner or web vulnerability scanner script using modules such as socket and requests?

24. Justify the role of Bash scripts in checking the security of a Linux system. Explain how you can quickly detect incorrect file permissions or open ports using a simple Bash script.

25. Explain in detail the capabilities of the Nmap tool. In particular, how do NSE (Nmap Scripting Engine) scripts work and what deep information (service version, security vulnerabilities) do they serve to collect when scanning a network?

26. Analyze the role of the Metasploit Framework in the process of vulnerability detection and exploitation. Explain when Metasploit is used and how its payload mechanism works.

27. Compare the main tasks and areas of application of tools such as Nikto and OpenVAS. Differentiate their methods of detecting vulnerabilities in web servers and network infrastructure.

28. Analyze the differences (flexibility, cost, upgradability) between a script-based approach and commercial vulnerability scanners. Why might the former be preferable for specific needs?

29. Analyze the risks (system damage, false results) that can arise when automating the vulnerability search process using scripts and what measures should be taken to minimize them?

30. What types of analysis (open ports, misconfigured services, weak protocols) are performed using scripts when checking network security? How do these analyses contribute to improving security?

31. Explain in theory the mechanism for automatic detection of attack anomalies using Machine Learning (ML) technologies in Python. What are the advantages and limitations of such an approach?

32. What is the main purpose of a Privilege Escalation attack? Explain with examples the vertical and horizontal types of this attack and what are the most effective defenses against it?

33. How does a Buffer Overflow attack affect OS security? What techniques does an attacker use to change the working order of memory and how do mechanisms such as Data Execution Prevention (DEP) resist this?

34. Analyze the main characteristics of a rootkit attack. Explain in detail its methods of entry, concealment and operation (for example, kernel-level rootkits).

35. What is the importance of a strong password policy in protecting a system from attacks? List the main requirements for a strong password and explain the role of Password Managers in this regard.

36. How does the Two-Factor Authentication (2FA) mechanism work and what additional layer of security does it create in protecting user accounts? Justify the practical advantages of its implementation.

37. Explain the main tasks of a firewall in protecting the OS from attacks. How does it filter incoming and outgoing traffic through the network (packet filtering, state control)?

38. Analyze the principles of operation of antivirus and antimalware programs (signature-based, heuristic analysis). What important role do they play in protecting the system from malicious programs and what is the importance of regularly updating them?

39. What are the risks of improper use of "root" rights in Linux systems? Give practical recommendations for limiting and managing root rights based on the principle of "Least Privilege".

40. What is the main role of regular monitoring and analysis of log files in detecting attacks on the system at an early stage? What types of events can be considered suspicious activity in the logs?

41. Explain the difference between Remote Exploit and Local Exploit with examples. What specific measures should be taken to protect against both types of attacks?

42. Explain the main role of Antivirus and Antimalware programs in ensuring OS security. Describe the open source antivirus programs that are common in the Linux environment (for example, ClamAV).

43. What role do firewalls and packet filtering tools (iptables, nftables) play in network security? What security policies can be implemented with their help (closing ports, restricting traffic)?

44. What is the main difference between IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems? What mechanisms do they use to detect and prevent attacks (signature-based, anomaly-based)?

45. How do vulnerability scanners (e.g., Nessus, OpenVAS) help administrators? Analyze their operating principles (system scanning, vulnerability database usage).

46. What is the role of Authentication and Authorization (AAA) tools (Kerberos, PAM) in centralizing OS security? How do these systems manage user identities and rights?

47. What aspects of OS security (confidentiality, integrity, authenticity) do cryptographic tools (GnuPG, OpenSSL) provide? Give practical examples of data encryption (storing passwords, email).

48. What is the main function of Audit and Monitoring tools (auditd, syslog, Logwatch)? What information base do they create in the process of detecting attacks and responding quickly (Incident Response)?

49. Justify the crucial importance of Backup and Recovery programs in ensuring information security. What is the role of backups in protecting against ransomware attacks?

50. How does any OS security software increase the reliability and uninterrupted operation of the system? Compare the role of IDS/IPS and backup systems in this regard.

51. Why is the integration of several software programs important for ensuring OS security in a corporate environment? For example, what is the effectiveness of the joint work of Firewall, IDS and SIEM systems?

52. Why are insider threats considered more dangerous than external attacks? Analyze their main types (unauthorized access, data theft, misuse of services).

53. What methods can be used to attempt unauthorized access to a network (weak passwords, credential harvesting, brute force)? What measures are taken to detect these attacks?

54. Analyze the threats carried out by internal attackers (employees). Evaluate the motivation of these threats (intention, carelessness) and the level of damage they cause to the organization.

55. Explain the role of network monitoring (NetFlow, Wireshark) in detecting threats within a network. What anomalies (abnormal traffic, large data transfers) can be observed with these tools?

56. Compare Signature-based and Anomaly-based threat detection methods. Analyze the advantages, disadvantages, and effectiveness of each method in detecting new (zero-day) threats.

57. How do UBA (User Behavior Analytics) systems work? How do they detect insider attackers by studying normal user behavior, and what are the drawbacks of this method?

58. Analyze the possibilities of using Machine Learning (ML) and AI technologies to detect threats within the network. Assess the risk of these algorithms being "black-box" and the possibility of making wrong decisions.

59. What important role does network segmentation play in protecting against threats within the network? How does creating a separate subnet for each department limit the spread of a threat to the entire network?

60. What is the main function of RBAC (Role Based Access Control) policies in reducing unauthorized access attempts within the network? Explain the importance of clearly defining rights according to roles.

61. Explain the crucial importance of developing a network security policy and regular employee awareness measures in ensuring information security

65. What are the risks of not having enough or no backups? How should a backup policy be developed based on the 3-2-1 rule in the event of ransomware attacks or data theft?

66. Analyze the security problems caused by insufficient monitoring and control. How can this problem be solved by regularly monitoring system logs and implementing SIEM systems?

67. Explain the negative impact of delaying updates (Patch) on cybersecurity. Justify the practical importance of implementing an automatic update installation and testing (staging) phase.

68. Explain the main purpose of the continuous security audit and scanning process. How do these activities help identify vulnerabilities and configuration errors at an early stage?

69. How does improper access rights management manifest itself as a common security problem? Explain the role of IAM (Identity and Access Management) systems and SSO (Single Sign-On) technologies in solving this problem.

70. Analyze the problem of improper storage of confidential data (unencrypted storage, storage in unauthorized locations). Justify the importance of data encryption and secure storage policies.

71. What should be the interaction between technical measures (Hardening, Firewall, Patching) and administrative measures (policies, awareness) in eliminating security problems? Explain the mechanism of complementarity of these two approaches.

72. Compare the main features of the security architecture of mobile operating systems (Android, iOS). Explain how Sandboxing and App Store/Play Market control mechanisms work and their role in ensuring mobile security.

73. Distinguish between the types of Malware (virus, trojan, spyware, ransomware) that threaten mobile devices. How do they penetrate the device and what damage can they cause?

74. Justify the importance of the Encryption mechanism in mobile security. What protection do Full Disk Encryption and TLS/SSL provide?

75. Analyze the importance of Two-Factor Authentication (2FA) and Biometric Authentication mechanisms in mobile OSs in protecting accounts from compromise.

76. What threats does Insecure Application Usage pose to mobile devices? Highlight the importance of controlling applications based on permission and installing only from trusted sources.

77. Explain the role of MDM (Mobile Device Management) systems in ensuring mobile OS security in a corporate environment. What security policies (password requirements, remote wipe) can be enforced using MDM?

78. How are phishing attacks carried out on mobile devices? What awareness measures should be taken to protect user personal information?

79. How do Wi-Fi and Bluetooth connections in public places pose a threat to mobile security? Justify the importance of using a VPN (Virtual Private Network) to minimize these risks.

80. Explain the role of the regular update process of mobile operating systems in security. What vulnerabilities can delaying updates lead to?

81. Compare the security mechanisms of Android and iOS. How does the fact that one is open source (Android) and the other has a closed ecosystem (iOS) affect security outcomes?

82. Explain the relationship between the main requirements for operating system security (Identification, Authorization, Data Protection, Audit, Integrity, Privacy, Availability) based on the CIA (Confidentiality, Integrity, Availability) triad.

83. What is the main essence of the identification and authentication requirement? What level of security does each of the password, biometric data and two-factor authentication tools provide?

84. Analyze the authorization (distribution of access rights) requirement in detail. Substantiate the crucial importance of the "Least Privilege" principle in ensuring OS security with examples.

85. Through what mechanisms is the data protection requirement met in the OS? Explain the role of encryption, access rights and audit mechanisms in ensuring data security.

86. Explain the role of the Audit and Accountability requirement in OS security. How is the process of logging and reporting each action in the system implemented and what results does it give?

87. What risks does a violation of the system and data integrity requirement lead to? How is integrity ensured through mechanisms such as Hashing and Digital Signatures?

88. Analyze the importance of security-certified OSs (e.g., Common Criteria EAL). How do the security extensions of SELinux (Security-Enhanced Linux) and its Mandatory Access Control (MAC) policy work?

89. Explain the security architecture of Qubes OS (Virtualization-based application isolation). What unique approach does this operating system take to ensure high confidentiality and security?

90. How is the system availability requirement met? Explain the role of OS protection against DoS (Denial of Service) attacks, load balancing, and backup mechanisms in this regard.

91. Analyze the practical benefits of using standardized policies (CIS Benchmarks) in meeting OS security requirements

92. Justify the crucial importance of security logs in monitoring the security of information systems. Explain the main function of each of the system, access, and application logs and the type of information they store.

93. Explain in detail the Main Steps of Security Log Analysis (collection, normalization, analysis, visualization). Why is log centralization (SIEM, ELK) important?

94. Analyze the main functions of SIEM (Security Information and Event Management) systems (log collection, correlation, real-time monitoring). How does a SIEM system detect suspicious events and send alerts to the administrator?

95. Compare the advantages, disadvantages, and areas of application in a corporate environment of log analysis tools such as Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), and Graylog.

96. Why are audit reports created? What role do they play in monitoring compliance with system security policies and meeting regulatory requirements?

97. Explain the concept of log correlation. How does this process help identify hidden or sophisticated attack chains (Kill Chains) from individual log entries?

98. What specialized functions do network monitoring tools (IDS/IPS) such as Snort perform in collecting and analyzing network logs? What are the limitations of relying solely on network logs?

99. Analyze the capabilities of the Wazuh tool. How does it perform log collection, security monitoring, and threat detection (SIEM integration) tasks, and assess its complexity in configuration.

100. Explain a practical mechanism for early detection of unauthorized access and attacks through log analysis. What types of log entries (e.g., multiple failed login attempts) require immediate alerting?

101. What is the importance of security logs in ensuring confidentiality and assisting in the forensic process? Why is it necessary to keep logs in an immutable state and have a retention policy?