**ÔN TẬP**

**TUẦN 9 - ANDROID SECURITY**

**Câu 1: Ghép các cấp độ bảo mật mạng của ứng dụng Android với đặc điểm tương ứng:**

**a. Pinning → Xác minh chứng chỉ máy chủ, HTTPS → Dữ liệu gửi qua mạng được mã hóa, Cleartext Traffic → Dữ liệu gửi qua mạng không được mã hóa**

b. Pinning → Xác minh chứng chỉ máy chủ, HTTP → Dữ liệu gửi qua mạng được mã hóa, Cleartext Traffic → Dữ liệu gửi qua mạng không được mã hóa

c. Pinning → Xác minh chứng chỉ máy chủ, HTTPS → Dữ liệu gửi qua mạng không được mã hóa, Cleartext Traffic → Dữ liệu gửi qua mạng không được mã hóa

**Câu 2: App Signing đảm bảo điều gì trong bảo mật ứng dụng Android?**

**a. Ứng dụng được xác thực nguồn gốc và tính toàn vẹn**

b. Mã hóa dữ liệu người dùng

c. Tăng hiệu suất ứng dụng

d. Giảm kích thước APK

**Câu 3: Ghép các cơ chế bảo mật trong Android với mô tả tương ứng:**

**a. Mandatory Access Control (MAC) → Chỉ chỉnh sửa được bởi quản trị viên, SEAndroid → Phiên bản MAC cho Linux kernel, Discretionary Access Control (DAC) → Người dùng có thể chuyển quyền truy cập**

b. Mandatory Access Control (MAC) → Chỉ chỉnh sửa được bởi quản trị viên, SEAndroid → Phiên bản MAC cho Linux kernel, Discretionary Access Control (DAC) → Người dùng không thể chuyển quyền truy cập

c. Mandatory Access Control (MAC) → Chỉnh sửa được bởi quản trị viên và người dùng, SEAndroid → Phiên bản MAC cho Linux kernel, Discretionary Access Control (DAC) → Người dùng có thể chuyển quyền truy cập

**Câu 4: Code Signing trong Android giúp đảm bảo điều gì?**

**a. Ứng dụng không bị thay đổi bởi bên thứ ba**

b. Mã hóa toàn bộ dữ liệu ứng dụng

c. Đẩy nhanh quá trình cài đặt

d. Hạn chế truy cập vào tài nguyên hệ thống

**Câu 5: Ghép các kỹ thuật ngăn chặn dịch ngược ứng dụng Android với chức năng tương ứng:**

**a. Encrypt Resources → Mã hóa tài nguyên để tránh bị phân tích, ProGuard → Làm rối mã nguồn để gây khó khăn cho việc dịch ngược, Obfuscation → Ẩn danh các biến, class và phương thức**

b. Encode Resources → Mã hóa tài nguyên để tránh bị phân tích, ProGuard → Làm rối mã nguồn để gây khó khăn cho việc dịch ngược, Obfuscation → Ẩn danh các biến, class và phương thức

c. Encrypt Resources → Mã hóa tài nguyên để tránh bị phân tích, ProGuard → Encode mã nguồn về Base64 để gây khó khăn cho việc dịch ngược, Obfuscation → Ẩn danh các biến, class và phương thức

**Câu 6: Ứng dụng phát hiện thiết bị đã root bằng cách nào?**

**a. Kiểm tra sự tồn tại của file hoặc công cụ liên quan đến root**

b. Quét toàn bộ bộ nhớ trong

c. Xóa dữ liệu người dùng

d. Khởi động lại thiết bị

**Câu 7: Multi-User Support trong Android cho phép điều gì?**

**a. Cho phép nhiều người dùng chia sẻ cùng một thiết bị**

b. Quản lý nhiều ứng dụng trong một tài khoản

c. Chia sẻ dữ liệu giữa các ứng dụng

d. Đẩy nhanh quá trình xử lý của hệ thống

**Câu 8: Vai trò chính của Device Admin API trong Android là gì?**

**a. Quản lý các chính sách bảo mật trên thiết bị**

b. Quản lý các kết nối mạng

c. Quản lý giao diện người dùng

d. Bảo vệ dữ liệu trong ứng dụng

**Câu 9: Công cụ nào dưới đây là một công cụ phân tích tĩnh trong Android?**

**a. SonarQube**

b. Burp Suite

c. Wireshark

d. Postman

**Câu 10: Binder trong Android có thể hoạt động như gì?**

**a. Token bảo mật**

b. UID giả mạo

c. Firewall nội bộ

d. Key mã hóa

**Câu 11: Cấu hình Network Security Configuration được dùng để làm gì?**

**a. Kiểm soát các kết nối mạng của ứng dụng**

b. Quản lý quyền truy cập dữ liệu người dùng

c. Bảo vệ dữ liệu trong bộ nhớ

d. Tăng tốc độ xử lý mạng

**Câu 12: Runtime Integrity Checks trong ứng dụng Android thường được dùng để làm gì?**

**a. Phát hiện các thay đổi trái phép trong runtime**

b. Tăng hiệu năng runtime

c. Quản lý quyền truy cập tài nguyên

d. Mã hóa toàn bộ dữ liệu

**Câu 13: Google Play Protect cung cấp chức năng nào?**

**a. Quét ứng dụng để phát hiện phần mềm độc hại**

b. Lưu trữ các bản sao lưu của ứng dụng

c. Đảm bảo dữ liệu không bị mã hóa

d. Cho phép các ứng dụng chia sẻ dữ liệu

**Câu 14: Package Manager trong Android có vai trò gì?**

**a. Quản lý việc cài đặt, gỡ bỏ và truy cập thông tin ứng dụng**

b. Quản lý giao tiếp giữa các tiến trình

c. Bảo vệ dữ liệu người dùng

d. Quản lý quyền truy cập của ứng dụng

**Câu 15: Permission cấp "normal" được cấp khi nào?**

**a. Khi rủi ro thấp, không yêu cầu xác nhận từ người dùng**

b. Khi truy cập tài nguyên nhạy cảm

c. Khi truy cập dữ liệu người dùng

d. Khi yêu cầu quyền nâng cao

**Câu 16: Ghép các cấp Permission trong Android với đặc điểm của chúng:**

**a. Signature → Chỉ cấp nếu ứng dụng có cùng chữ ký số, Dangerous → Yêu cầu xác nhận từ người dùng, Normal → Không yêu cầu xác nhận từ người dùng**

b. Signature → Chỉ cấp nếu ứng dụng có cùng chữ ký số, Dangerous → Yêu cầu xác nhận từ máy chủ, Normal → Không yêu cầu xác nhận từ người dùng

c. Signature → Chỉ cấp nếu ứng dụng có cùng chữ ký số, Dangerous → Yêu cầu xác nhận từ người dùng, Normal → Không yêu cầu xác nhận từ máy chủ

**Câu 17: Kỹ thuật nào thường được sử dụng để ngăn chặn phân tích động ứng dụng Android?**

**a. Phát hiện trình giả lập**

b. Quản lý bộ nhớ trong

c. Làm rối mã nguồn

d. Mã hóa giao diện người dùng

**Câu 18: Secure Startup trong Android được dùng để làm gì?**

**a. Yêu cầu xác thực trước khi hoàn tất khởi động**

b. Khởi động ứng dụng ngay lập tức

c. Giảm thiểu thời gian khởi động

d. Quản lý việc cài đặt ứng dụng

**Câu 19: Full-Disk Encryption (FDE) trong Android đảm bảo điều gì?**

**a. Mã hóa toàn bộ dữ liệu lưu trữ trên thiết bị**

b. Bảo vệ dữ liệu chỉ trong các ứng dụng cụ thể

c. Tăng tốc độ xử lý của thiết bị

d. Mã hóa dữ liệu trên mạng

**Câu 20: Ghép các thuật ngữ mã hóa trong Android với mô tả tương ứng:**

**a. File-Based Encryption (FBE) → Mã hóa ở mức file thay vì toàn bộ đĩa, FDE → Mã hóa toàn bộ đĩa, Keymaster → Bảo vệ các khóa mã hóa trong Android**

b. File-Based Encryption (FBE) → Mã hóa ở mức file thay vì toàn bộ đĩa, FDE → Mã hóa toàn bộ đĩa, Keymaster → Bảo vệ các ciphertext được mã hóa trong Android

c. File-Based Encryption (FBE) → Mã hóa ở mức file và toàn bộ đĩa, FDE → Mã hóa toàn bộ đĩa, Keymaster → Bảo vệ các khóa mã hóa trong Android

**Câu 21: Mỗi ứng dụng Android được gán gì để cô lập dữ liệu và tiến trình của nó?**

**a. Một UID riêng**

b. Một GID riêng

c. Một PID riêng

d. Một sandbox riêng

**Câu 22: Verify Boot trong Android có tác dụng gì?**

**a. Đảm bảo hệ thống khởi động không bị sửa đổi trái phép**

b. Đẩy nhanh quá trình khởi động

c. Tăng hiệu năng của ứng dụng

d. Hạn chế truy cập vào dữ liệu người dùng

**Câu 23: Encrypted Shared Preferences trong Android đảm bảo điều gì?**

**a. Mã hóa dữ liệu lưu trữ trong Shared Preferences**

b. Quản lý tài nguyên mạng

c. Chia sẻ dữ liệu giữa các ứng dụng

d. Phân tích dữ liệu người dùng

**Câu 24: Ghép các cơ chế bảo vệ runtime của Android với chức năng tương ứng:**

**a. Address Space Layout Randomization (ASLR) → Bố trí ngẫu nhiên bộ nhớ để làm khó khai thác, ProGuard → Làm rối mã để tránh dịch ngược, Hardened Runtime → Giảm thiểu khả năng khai thác lỗ hổng trong runtime**

b. Address Space Layout Randomization (ASLR) → Bố trí ngẫu nhiên bộ nhớ để làm khó khai thác, ProGuard → Mã hoá bằng AES 256 để tránh dịch ngược, Hardened Runtime → Giảm thiểu khả năng khai thác lỗ hổng trong runtime

c. Address Space Layout Randomization (ASLR) → Bố trí ngẫu nhiên bộ nhớ để làm khó khai thác, ProGuard → Làm rối mã để tránh dịch ngược, Hardened Runtime → Giảm thiểu khả năng khai thác lỗ hổng ngoài runtime

**Câu 25: Ghép các công cụ bảo mật Android với chức năng tương ứng:**

**a. ProGuard → Làm rối mã nguồn và tối ưu hóa ứng dụng, Network Security Config → Kiểm soát lưu lượng mạng của ứng dụng, Android Keystore → Lưu trữ và quản lý khóa mã hóa**

b. ProGuard → Làm rối mã nguồn và tối ưu hóa ứng dụng, Network Security Config → Kiểm soát lưu lượng mạng của ứng dụng, Android Keystore → Lưu trữ và quản lý khóa công khai RSA, ECC,…

c. ProGuard → Làm rối mã nguồn và tối ưu hóa ứng dụng, Network Security Config → Kiểm soát lưu lượng mạng của máy chủ, Android Keystore → Lưu trữ và quản lý khóa mã hóa

**Câu 26: Permission cấp "dangerous" yêu cầu điều kiện gì?**

**a. Yêu cầu xác nhận từ người dùng**

b. Tự động cấp quyền

c. Chỉ cấp khi ứng dụng được ký

d. Không yêu cầu điều kiện đặc biệt

**Câu 27: SELinux trong Android đóng vai trò gì?**

**a. Thực thi Mandatory Access Control (MAC) để tăng cường bảo mật**

b. Quản lý dữ liệu cá nhân của người dùng

c. Kiểm soát giao tiếp giữa các tiến trình

d. Tăng tốc độ xử lý của hệ thống

**Câu 28: Certificate Pinning trong bảo mật Android giúp đảm bảo điều gì?**

**a. Kết nối chỉ được thực hiện với các máy chủ có chứng chỉ đáng tin cậy**

b. Mã hóa dữ liệu người dùng

c. Quản lý tài nguyên ứng dụng

d. Chia sẻ dữ liệu giữa các ứng dụng

**Câu 29: Android Keystore được sử dụng để làm gì?**

**a. Lưu trữ và quản lý khóa mã hóa**

b. Quản lý quyền truy cập tài nguyên

c. Bảo vệ dữ liệu người dùng

d. Chạy các tác vụ nền

**Câu 30: Play Integrity API trong Android được sử dụng để làm gì?**

**a. Xác minh tính toàn vẹn của ứng dụng**

b. Mã hóa toàn bộ dữ liệu trong ứng dụng

c. Quản lý các tài nguyên mạng

d. Tăng cường hiệu suất runtime