Câu 1. Mạng Extranet VPN thường được sử dụng để

**(A) Kết nối các khách hàng và đối tác tới mạng Intranet trung tâm.**

(B) Kết nối các văn phòng chi nhánh với nhau

(C) Kết nối các văn phòng chi nhánh với mạng Inttranet trung tâm

(D) Kết nối chỉ trong một chi nhánh

Câu 2. Cho sơ đồ giao thức Needham-Schroeder như sau.

1. Alice → Sandy: Alice, Bob

2. Sandy → Alice: {TS, L, K, Bob, {TS, L, K, Alice}KBS}KAS

3. Alice → Bob: {TS, L, K, Alice}KBS, {Alice, TA}K

4. Bob → Alice: {TA+1}K

Hãy chọn phát biểu đúng.

(A) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Alice có thể sử dụng vé này bao nhiêu lần tùy ý (bước 3 và 4); giá trị KBS trong vé là để Alice biết vé này chỉ để liên lạc với Bob.

**(B) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Vé này có thời hạn sử dụng được xác định bởi TS và L. Trong thời hạn đó, Alice có thể liên lạc với Bob (bước 3 và 4) số lần tùy ý.**

(C) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Thời hạn bắt đầu có hiệu lực của vé được xác định bởi TS, Alice có thể liên lạc với Bob (bước 3 và 4) L lần, sau đó thì phải xin cấp vé mới.

(D) Có thể coi bước 1 và 2 là pha cấp vé {TS, L, K, Alice}KBS cho Alice. Alice có thể sử dụng vé này bao nhiêu lần tùy ý (bước 3 và 4); giá trị TS trong vé là để Alice biết vé này được cấp bởi Sandy.

Câu 3. Chọn phát biểu đúng về giao thức an toàn mạng.

(A) Giao thức an toàn mạng là giao thức được thiết kế để đảm bảo an toàn cho các giao thức mạng không có tính năng an toàn.

(B) Giao thức an toàn mạng có thể nằm ở bất kỳ tầng nào của chồng giao thức TCP/IP.

**(C) Một giao thức an toàn mạng sẽ đảm bảo tính bí mật và toàn vẹn cho thông tin được truyền qua nó.**

(D) Một giao thức an toàn mạng sẽ đảm bảo cả ba tính chất bí mật, toàn vẹn và khả dụng cho thông tin được truyền qua nó.

Câu 4. Cho biết cấu trúc của gói tin ESP IPsec như sau:

Untitled\_202141910629\_0.png

Giả sử kết nối IPsec được thiết lập ở chế độ Tunnel Mode, sử dụng giao thức ESP. Xét gói tin IPsec chứa dữ liệu trao đổi giữa trình duyệt và web server. Hãy cho biết giá trị của trường Next Header trong ESP Trl.   
**Next Header = 6**

Câu 5. Hãy cho biết số hiệu của giao thức AH: **RFC 1826**

Câu 6. Trong các thành phần sau, thành phần nào có thể đóng vai trò Authenticator?

(A) Supplicant

(B) User

(C) Gateway

**(D) NAS (Network Access Server)**

Câu 7. Sau khi kết thúc giao thức SSH-TRANS, giữa SSH Server và SSH Client

(A) thỏa thuận được 2 khóa phiên đối xứng. Trong đó 1 khóa được sử dụng để mã hóa thông điệp, 1 khóa được sử dụng để xác thực thông điệp giữa Server và Client.

**(B) thỏa thuận được 2 khóa phiên đối xứng. Trong đó 1 khóa được sử dụng để mã hóa và xác thực thông điệp từ Server tới Client, 1 khóa được sử dụng để mã hóa và xác thực thông điệp từ Client tới Server.**

(C) thỏa thuận được 4 khóa phiên đối xứng. Trong đó 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Server tới Client, 2 khóa được sử dụng để mã hóa và xác thực thông điệp từ Client đến Server.

(D) thỏa thuận được 1 khóa phiên đối xứng để mã hóa và xác thực thông điệp trao đổi sau đó giữa Server và Client.

Câu 8. Giao thức WEP là viết tắt của cụm từ nào sau đây?

(A) Wired Equivalent Private

(B) Wired Equivalence Private

(C) Wired Equivalence Privacy

**(D) Wired Equivalent Privacy**

Câu 9. Mỗi đầu mối IPsec phải duy trì một cơ sở dữ liệu thông tin để khi có một gói tin cần được xử lý bằng IPsec thì biết được cần xử lý như thế nào. Hãy cho biết tên viết tắt của cơ sở dữ liệu đó.

Câu 10. Vào năm 2003, khi chuẩn IEEE 802.11i còn chưa được chính thức ban hành, Wi-Fi Alliance đã đưa ra một giao thức an toàn dựa trên một phần của IEEE 802.11i để áp dụng trong các thiết bị Wi-Fi. Tên viết tắt của giao thức an toàn đó là: **WPA**

Câu 11. Chọn phát biểu SAI về WPA2.

(A) WPA2 hỗ trợ xác thực thông điệp bằng AES-CBC-MAC.

(B) WPA2 hỗ trợ xác thực bằng giao thức EAP.

**(C) WPA2 quy định mọi thiết bị Wi-Fi chỉ hỗ trợ mã hóa bằng AES.**

(D) WPA2 hỗ trợ thỏa thuận khóa giữa AP và các Station để khóa giữa AP với các Station khác nhau là khác nhau.

Câu 12. Xét mô hình mạng sau đây.

Untitled\_2021419102723\_0.png

Giả sử Firewall không cho kết nối từ Internet đi vào WORK NET nhưng một kỹ sư lại muốn truy cập từ HOME NET tới Web Server để hoàn thành sớm các công việc của mình. Anh ta thiết lập một SSH Server tại HOME NET với một địa chỉ Internet và một địa chỉ cục bộ. Cách làm nào sau đây giúp anh kỹ sư đạt được mục đích?

(A) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển kết nối tới 192.168.1.2:80 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://192.168.1.2.

(B) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển kết nối tới 192.168.1.2:80 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://192.168.1.2.

**(C) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Local Port Forwarding để chuyển kết nối tới 42.112.11.2:22 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.112.11.2:22.**

(D) Từ máy CompW thực hiện kết nối tới SSH Server, sử dụng Remote Port Forwarding để chuyển kết nối tới 42.112.11.2:22 sang 10.0.0.11:80. Sau đó, từ máy CompH truy cập tới Web Server bằng cách nhập vào trình duyệt địa chỉ http://42.112.11.2:22.

Câu 13. Bạn được yêu cầu chọn một thuật toán mật mã khóa công khai để sử dụng trong một giao thức mạng, bạn sẽ chọn thuật toán nào sau đây?

(A) Triple-DES

(B) **RSA**

(C) ECB

(D) SHA

Câu 14. Chọn phát biểu đúng về hoạt động của giao thức SSL Handshake?

(A) Trong SSL Handshake, Client bắt buộc gửi Certificate sang cho Server

(B) Trong SSL Handshake, Server không bắt buộc phải Certificate của mình sang Client, Client bắt buộc gửi Certificate sang cho Server

(C) Trong SSL Handshake, Server không bắt buộc phải Certificate của mình sang Client

**(D) Trong SSL Handshake, Server bắt buộc phải gửi Certificate của mình sang Client, Client không bắt buộc gửi Certificate sang cho Server**

Câu 15. Xét mô hình kết nối sau.

Untitled\_2021419101437\_0.png

Biết rằng trình duyệt trên Web Client truy cập tới Web Server qua giao thức HTTPS. Hãy chọn phát biểu ĐÚNG NHẤT.

**(A) Cả trình duyệt trên Web Client và phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ SSL/TLS.**

(B) Trình duyệt trên Web Client phải được lập trình đễ hỗ trợ SSL/TLS

(C) Phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ SSL/TLS.

(D) SSL/TLS là trong suốt đối với tầng ứng dụng (Application) trong chồng giao thức TCP/IP nên trình duyệt và phần mềm máy chủ web không cần phải biết về sự tồn tại của SSL/TLS.

Câu 16. Một giao thức liên lạc giữa mail client và mail server, hoạt động trên cổng TCP mặc định là 143. Hãy cho biết tên viết tắt của giao thức. **IMAP**

Câu 17. Trong sơ đồ sau: Alice và Bob phải chia sẻ trước với nhau tham số nào?

1. Alice → Bob: "Alice"

2. Bob → Alice: NB;

3. Alice → Bob: {NB}K

4. Bob: …

**Key**

Câu 18. Mô tả nào sau đây KHÔNG đúng về giao thức WEP?

**(A) Không có khóa phiên nào được thiết lập trong suốt quá trình xác thực**

(B) Không có bảo vệ chống tấn công phát lại

(C) Hỗ trợ xác thực hai chiều

(D) Cùng một khóa chia sẻ giống nhau được dùng cho cả mã hóa và xác thực

Câu 19. Chọn phát biểu đúng về giao thức PAP (Password Authentication Protocol).

(A) PAP là giao thức bắt tay 3 bước

(B) Trong giao thức PAP, mật khẩu được mã hóa trước khi truyền đi

(C) PAP là giao thức xác thực 2 chiều

**(D) PAP là giao thức bắt tay 2 bước**

Câu 20. Đâu không phải khả năng mà giao thức SSH đem lại?

(A) Mã hóa dữ liệu tầng Network

(B) Mã hóa dữ liệu tầng ứng dụng

(C) Xác thực dữ liệu

**(D) Nén dữ liệu**

Câu 21. Trong một giao thức an toàn mạng ở tầng Liên mạng (Internet) của chồng giao thức TCP/IP

(A) có thể sử dụng kết hợp, nhưng không nên sử dụng kết hợp ký số và mã hóa vì sẽ làm giảm đáng kể hiệu năng của hệ thống.

(B) cần phải sử dụng kết hợp mã hóa và ký số nếu muốn đảm bảo đồng thời tính bí mật và tính xác thực cho thông tin.

**(C) có thể sử dụng kết hợp mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.**

(D) luôn phải có sự kết hợp mã hóa và ký số để đảm bảo tính bí mật và xác thực cho thông tin.

Câu 22. Trong một giao thức an toàn mạng, chứng thư số khóa công khai được sử dụng để

(A) kiểm tra chữ ký số của chủ thể được nêu danh trong chứng thư.

(B) trao đổi khóa phiên với chủ thể được nêu danh trong chứng thư.

**(C) xác nhận một khóa công khai thuộc về chủ thể được nêu danh trong chứng thư.**

(D) mã hóa thông tin gửi cho chủ thể được nêu danh trong chứng thư.

Câu 23. Chọn phát biểu ĐÚNG NHẤT về mã hóa dữ liệu tầng ứng dụng trong giao thức SSL/TLS.

(A) Việc mã hóa dữ liệu luôn là bắt buộc.

(B) Việc mã hóa dữ liệu luôn được thực hiện bằng mật mã đối xứng.

(C) Việc mã hóa dữ liệu bằng mật mã đối xứng hay mật mã khóa công khai là do CipherSuite quyết định.

**(D) Việc mã hóa dữ liệu luôn được thực hiện bằng mật mã khóa công khai, sử dụng chứng thư số X.509.**

Câu 24. Chọn phát biểu ĐÚNG NHẤT về Security Association (SA) trong IPsec.

(A) Một SA được xác định duy nhất bởi SPI kết hợp với giao thức con IPsec.

**(B) Một SA được xác định duy nhất bởi SPI.**

(C) Một SA được xác định duy nhất bởi một trong 2 cách: bởi địa chỉ máy đích, hoặc bởi SPI kết hợp với giao thức con IPsec.

(D) Một SA được xác định duy nhất bởi địa chỉ của máy đích.

Câu 25. Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng “nonce” được sử dụng trong các giao thức xác thực.

**(A) Nonce luôn được sinh ra bởi bên yêu cầu xác thực (Claimant)**

(B) Nonce có thể được sinh bởi bên xác thực (Verifier) hoặc bên yêu cầu xác thực (Claimant) thùy thuộc vào sự thỏa thuận giữa hai bên trong pha đầu tiên của giao thức xác thực.

(C) Nonce được sinh bởi bên xác thực (Verifier) nếu bên xác thực khởi xướng phiên liên lạc, được sinh bởi bên yêu cầu xác thực (Claimant) nếu bên yêu cầu xác thực khởi xướng phiên liên lạc.

(D) Nonce luôn được sinh ra bởi bên xác thực (Verifier)

Câu 26. Chọn phát biểu đúng về giao thức CHAP

(A) Trong giao thức CHAP, mật khẩu được truyền dưới dạng rõ

**(B) CHAP là giao thức bắt tay 3 bước**

(C) CHAP là giao thức bắt tay 2 bước

(D) Giao thức CHAP sử dụng cả nonce và timesamp

Câu 27. Cho mô hình mạng dưới đây

Giữa hai gateway G1 và G2, người ta thiết lập giao thức IPsec sử dụng giao thức AH ở chế độ tunnel. Hai gateway này kết nối hai mạng LAN 10.0.1.0/24 và 10.0.2.0/24 với nhau. Xét một gói tin UDP được gửi từ H1 đến H2. Trong IP Header của gói tin IP tại H1, các giá trị Source IP và Destination IP và Protocol là gì?

(A) 172.16.0.1, 172.16.0.2 và 6

(B) 10.0.1.2, 172.16.0.2 và 6

**(C) 10.0.1.2, 10.0.2.2 và 17**

(D) 172.16.0.1, 172.16.0.2 và 17

Câu 28. Tổ hợp an toàn (SA) trong IPsec tương ứng với cụm từ nào sau đây?

(A) Secured Association

**(B) Security Association**

(C) Security Associated

(D) Secured Associating

Câu 29. SSH là viết tắt của?

(A) Secure Server

**(B) Secure Shell**

(C) Security Shell

(D) Secure Socket

Câu 30. Tại sao mã xác thực thông báo (MAC) có thể xác thực được nguồn gốc của dữ liệu?

**(A) Vì trong MAC có chứa một giá trị bí mật được chia sẻ trước giữa người gửi và người nhận.**

(B) Vì MAC có khả năng chống tấn công phát lại (replay attack)

(C) Vì trong MAC có chứa định danh của cả người gửi và người nhận.

(D) Vì trong MAC có sử dụng hàm băm.

Câu 31. Cho sơ đồ giao thức xác thực bằng mật khẩu sau đây.

Untitled\_202141995123\_0.png

Hãy cho biết ý nghĩa của việc sử dụng “Salt” trong sơ đồ trên.

(A) Chống lại các tấn công sử dụng bảng giá trị băm

**(B) Chống lại tấn công từ điển khi thông tin về Alice trong “Password file” bị lộ.**

(C) Đóng vai trò như là một khóa mật mã để sử dụng khi băm (hash) mật khẩu của Alice.

(D) Để làm tăng tính ngẫu nhiên cho mật khẩu của người dùng, bởi người dùng có xu hướng chọn mật khẩu dễ nhớ.

Câu 32. IPsec là viết tắt của?

(A) Internal Protocol Setup

(B) Internet Protocol Seting

(C) Internal Protocol Security

**(D) Internet Protocol Security**

Câu 33. Xét mô hình kết nối sau.

Untitled\_2021419101437\_0.png

Biết rằng một kết nối IPsec ở chế độ Transport đã được thiết lập giữa hai máy Web Client và Web Server. Hãy chọn phát biểu ĐÚNG NHẤT.

(A) Phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ IPsec.

(B) IPsec là trong suốt đối với tầng ứng dụng (Application) trong chồng giao thức TCP/IP nên trình duyệt và phần mềm máy chủ web không cần phải biết về sự tồn tại của IPsec.

(C) Trình duyệt trên Web Client phải được lập trình đễ hỗ trợ IPsec.

**(D) Cả trình duyệt trên Web Client và phần mềm máy chủ web trên Web Server phải được lập trình để hỗ trợ IPsec.**

Câu 34. Đâu là một điểm khác biệt giữa WEP và TKIP?

(A) WEP sử dụng hàm kiểm tra CRC32, còn TKIP sử dụng thuật toán Michael-64.

(B) WEP sử dụng hệ mật DES, còn TKIP sử dụng hệ mật AES.

**(C) WEP không hỗ trợ giao thức xác thực EAP, còn TKIP có hỗ trợ EAP.**

(D) WEP không hỗ trợ khóa khóa nhóm, còn TKIP hỗ trợ khóa nhóm.

Câu 35. Cho biết cấu trúc của gói tin AH IPsec như sau:

Untitled\_20214191019\_0.png

Giả sử kết nối IPsec được thiết lập ở chế độ Tunnel Mode, sử dụng giao thức AH. Xét gói tin IPsec chứa dữ liệu trao đổi giữa trình duyệt và web server. Hãy cho biết giá trị của trường Next Header trong AH Header.

Câu 36. Giao thức SSL cung cấp dịch vụ nào sau đây?

(A) Tính bí mật

(B) Tính toàn vẹn

(C) Nén dữ liệu

**(D) Cả ba đáp án trên**

Câu 37. Giao thức xác thực nào sau đây sử dụng trung tâm phân phối khóa (KDC- Key Distribution Center)

(A) CHAP.

(B) EAP

(C) PAP

**(D) Kerberos**

Câu 38. Hãy chọn phát biểu ĐÚNG NHẤT về đại lượng “timestamp” được sử dụng trong các giao thức xác thực.

(A) Giá trị của timestamp do bên xác thực (Verifier) quyết định.

(B) Giá trị của timestamp được các bên (bên xác thực và bên yêu cầu xác thực) thống nhất trước khi tiến hành xác thực.

(C) Giá trị của timestamp do bên yêu cầu xác thực (Claimant) quyết định.

**(D) Giá trị của timestamp được mỗi bên (bên xác thực và bên yêu cầu xác thực) tự xác định khi cần.**

Câu 39. Cho sơ đồ giao thức Kerberos như sau

Untitled\_202141995438\_0.png

1. C→AS: IDC, IDTGS

2. AS→C: {{IDC, IDTGS, T1, L1, KC\_TGS}KAS\_TGS, KC\_TGS, T1, L1}KC

3. C→TGS: {IDC, IDTGS, T1, L1, KC\_TGS}KAS\_TGS, {IDC, T2}KC\_TGS, IDSS

4. TGS→C: {{IDC, IDSS, T3, L2, KC\_SS}KTGS\_SS, KC\_SS, T3}KC\_TGS

5. C→SS: {IDC, IDSS, T3, L2, KC\_SS}KTGS\_SS, { IDC, T4}KC\_SS

6. SS→C: {T4+1}KC\_SS

Hãy chọn phát biểu ĐÚNG NHẤT về lý do để giao thức Kerberos được coi là có tính chất Single Sign-On.

(A) Vì Client có thể yêu cầu AS cấp đồng thời nhiều vé để xin truy cập tới nhiều Service Server khác nhau.

**(B) Vì khi AS cấp cho Client một vé thì Client có thể dùng vé đó để liên hệ với TGS nhiều lần để xin truy cập tới nhiều Service Server khác nhau.**

(C) Vì khi TGS cấp cho Client một vé thì Client có thể sử dụng vé đó để truy cập tới nhiều Service Server khác nhau.

(D) Vì Client có thể yêu cầu TGS cấp đồng thời nhiều vé để truy cập tới nhiều Service Server khác nhau.

Câu 40. Trong các giao thức an toàn mạng, mật mã đối xứng có thể được sử dụng để đảm bảo tính chất an toàn nào của thông tin?

(A) Tính bí mật.

(B) Tính toàn vẹn.

(C) Tính xác thực.

**(D) Cả 3 tính chất trên.**

Câu 41. Tấn công hủy xác thực (deauthentication attack) vào mạng không dây là loại tấn công nào sau đây?

(A) Tấn công hạ cấp

**(B) Tấn công từ chối dịch vụ**

(C) Tấn công mật mã

(D) Tấn công Brute-force

Câu 42. Phương án nào sau đây không phải là phương pháp xác thực được sử dụng trong WLAN?

(A) Xác thực dựa trên địa chỉ MAC

(B) Xác thực dựa trên khóa chia sẻ trước

**(C) Xác thực dựa trên địa chỉ IP**

(D) Xác thực mở rộng EAP

Câu 43. Chọn phát biểu SAI về giao thức EAP

(A) Trong giao thức EAP mật khẩu được truyền đi dưới dạng rõ.

(B) EAP là giao thức xác thực khả mở rộng.

**(C) EAP là giao thức xác thực 1 chiều.**

(D) EAP là giao thức sử dụng nhiều phương thức xác thực khác nhau.

Câu 44. Phát biểu nào dưới đây là đúng?

(A) Các giao thức SSL, TLS, SSH là những giao thức hoạt động ở cả tầng giao vận và tầng mạng.

**(B) POP, IMAP, DHCP, SNMP là những giao thức hoạt động ở tầng ứng dụng.**

(C) TCP, ICMP, SSL và HTTP là những giao thức hoạt động ở tầng giao vận.

(D) ARP, PPP, IP là giao thức hoạt động ở tầng liên kết dữ liệu.