1. Care dintre urmatoarele afirmatii despre procesul de schimb de chei sunt adevarate in contextulfolosirii algoritmilor de criptare simetrici, respectiv asimetrici:
   a. In ambele situatii, schimbul de chei se poate realiza pe acelasi canal / prin acelasi mecanismprin care are loc si comunicarea
   b. Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa serealizeze doar in cazul algoritmilor de criptare asimetrici
   c. Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa serealizeze doar in cazul algoritmilor de criptare simetrici
   d. In ambele situatii, schimbul de chei trebuie sa se desfasoare pe un alt canal / printr-unmecanism de comunicare alternativ

2. Care dintre urmatoarele reprezinta proprietati care trebuie sa fie respectate de catre o semnatura electronica:
   a. nereutilizabila
   b. nerepudiabila
   c. nefalsificabila
   d. autentica
   e. nealterabila

3. Care este cel mai uzual mod de transmitere a unei chei publice catre terti:
   a. Pe un canal alternativ care nu poate fi controlat de atacator
   b. Pe un canal de comunicare criptat pentru a asigura confidentialitatea cheii
   c. Fiind vorba de o cheie publica, nu este important ca, canalul pe care este transmisa sa fie sigur
   d. In cadrul unui certificat digital

4. Care dintre urmatoarele mecanisme limiteaza succesul exploit-urilor de tip shell code?
   a. Arhivarea (compactarestivei
   b. Randomizarea stivei
   c. Data Execution Prevention
   d. Inlaturarea bitului de executie de pe programul atacat

5. Care dintre urmatoarele vulnerabilitati ar putea fi exploatata pentru a fura sesiunea unui utilizator autentificat?
   a. Cross-Site Request Forgery (CSRF)
   b. Cross-Site scripting (XSS)
   c. SQL Injection

6. Care dintre următoarele afirmații sunt adevărate în ceea ce privește certificatele digitale Web client-side?
   a. Sunt transmise clientului exclusiv pe canale de încredere (sigure)
   b. Sunt semnate cu aceeași cheie privată cu care este semnat și certificatul serverului Web
   c. Folosite împreună cu protocolul SSL și cu autentificarea pe bază de user și parolă sporesc securitatea autentificării și identificării clientului

7. Care este pericolul interceptării de către un terț (Man in the Middle) a unei chei publice din cadrul unui certificat digital semnat de către o autoritate de certificare și transmis pe un canal nesigur?
   a. Atacatorul poate înlocui cheia publică din certificat cu propria cheie publică, corespunzătoare unei chei private pe care acesta o deține
   b. Nu există niciun pericol, destinatarul la care ajunge certificatul îl poate valida pe baza semnăturii depuse de autoritatea de certificare
   c. Atacatorul poate înlocui cheia privată din certificat cu propria cheie privată, corespunzătoare unei chei publice pe care acesta o deține

8. Cum se poate „fura” un cookie de sesiune al unui alt utilizator?
   a. Prin lipsa invalidării sesiunii (logout) și navigarea în continuare pe un site malițios
   b. Prin interceptarea datelor la nivelul rețelei de transport în lipsa folosirii unei conexiuni sigure
   c. Prin intermediul unui cod JavaScript injectat de către atacator

9. Care dintre următoarele reprezintă măsuri pentru evitarea vulnerabilităților de tip XSS?
   a. Înlocuirea anumitor caractere din datele primite de la client cu entitățile HTML corespunzătoare
   b. Folosirea la nivelul browserului a unor biblioteci de funcții JavaScript consacrate și testate anterior
   c. Dezactivarea din cadrul aplicației web a posibilității rulării de cod JavaScript de către browser
   d. Verificări riguroase la nivelul browserului legate de validitatea datelor introduce

10. Cheia privată este folosită pentru:
   a. Semnarea documentelor
   b. Verificarea semnăturilor digitale
   c. Decriptarea mesajelor primite
   d. Criptarea mesajelor trimise

11. Care dintre următoarele afirmații sunt adevărate în ceea ce privește o semnătură digital?
   a. Semnătura digitală este de fapt un hash
   b. Orice document semnat digital poate fi datat în timp
   c. Pentru a aplica o semnătură digitală, mai este nevoie de cel puțin încă o parte implicată care să semneze și ea documentul (autoritate de certificare, notar electronic, partenerul cu care se semnează un contract digital, etc.)
   d. Semnătura digitală este criptată cu ajutorul unei chei private

12. Ce memorează autoritățile de marcă temporală?
   a. Cererile și răspunsurile venite spre și dinspre acestea
   b. Nu memorează nimic, doar semnează, validitatea semnăturii putând fi ușor dovedită cu ajutorul cheii publice a autorității de marcă temporală
   c. Documentele semnate

13. Apelurile sistem Linux pot fi apelate ca funcții de la întreruperea:
   a. 21h
   b. Apelurile sistem Linux sunt implementate în C nu ca funcții de la o anumită întrerupere
   c. 80h
   d. 80
   e. 21

14. Care dintre următoarele protocoale folosesc criptografia cu cheie publică?
   a. https
   b. smtp
   c. nslookup (name secure lookup)
   d. ssh

15. Ce se trimite unei autorități de marcă temporală pentru a dovedi că un anumit document există la un anumit moment de timp?
   a. un hash al documentului și o semnătură
   b. documentul, semnătura și momentul de timp
   c. documentul semnat

16. Caracterul NULL (“\0”) nu apare de obicei în string-ul ce reprezintă shell code-ul deoarece:
   a. Majoritatea programelor exploatate sunt scrise în limbajul C, acest caracter ar marca terminarea prematură a datelor de intrare
   b. 00h nu este o adresă de revenire validă în cadrul stivei
   c. Octetul cu valoarea 0 nu reprezintă codul unei instrucțiuni valide în limbaj de asamblare

17. Care dintre următoarele reprezintă măsuri pentru evitarea injecțiilor SQL:
    a. Folosirea la nivelul backend-ului de mecanisme de tipul ”prepared statement”
    b. Verificări riguroase la nivelul backend-ului legate de validitatea datelor introduse precum și folosirea de biblioteci specializate pentru persitarea datelor (ORM-uri)
    c. Verificări riguroase la nivelul browserului legate de validitatea datelor introduse
    d. Dezactivarea în cadrul aplicației Web a posibilității rulării de cod SQL de către browser

18. Criptarea datelor între parteneri se poate face în Internet la care dintre următoarele niveluri:
    a. Fizic și legătură de date
    b. Rețea
    c. Aplicație

19. Certificatele digitale autosemnate se folosesc:
    a. Un certificat nu poate fi autosemnat
    b. De către autoritățile de certificare
    c. Doar dacă aparțin/sunt emise de către un utilizator pentru el însuși și nu sunt semnate și de către autoritățile de certificare

20. Diseminarea în siguranță către terți a cheii publice a unei entități se poate face:
    a. Prin intermediul unui certificat digital semnat
    b. Fiind vorba de cheia publică, nu trebuie luate măsuri suplimentare de siguranță, toată lumea putând cunoaște această cheie
    c. Odată cu diseminarea spre terți a cheii private
    d. Pe un canal alternativ securizat, diferit de cel pe care urmează să se facă comunicarea

21. Care este pericolul compromiterii unui certificat digital emis unui site Web în scopul autentificării acestuia de către clienți (compromitere în sensul aducerii acestui certificat la cunoștință publică)?
    a. Se poate extrage cheia publică din acel certificat, dar acest fapt nu reprezintă un pericol
    b. Se poate extrage cheia privată din acel certificat
    c. Se pot semna documente în numele site-ului web respectiv
    d. Nu există niciun pericol

22. Autoritățile de marcă temporală care dovedesc existența unui document la un anumit moment de tip:
    a. Semnează și ele documentul
    b. Stochează documentul
    c. Semnează un hash al documentului

23. Funcția aplicată pe text și pe cheia privată poate asigura:
    a. Confidențialitatea mesajului
    b. nonrepudierea mesajului
    c. autenticitatea mesajului
    d. integritatea mesajului

24. Care dintre următoarele reprezintă scheme de validare a unui 3ertificate digital:
    a. DCVP – Digital Certificate Validation Process
    b. OCSP – Online Certificate Status Protocol
    c. CRLs – Certificate Revocation Lists

25. Cheia publică este folosită pentru:
    a. Semnarea documentelor
    b. Criptarea mesajelor
    c. Decriptarea mesajelor
    d. Verificarea semnăturilor digitale

26. Un certificat digital ajută la:
    a. Verificarea integrității și autenticității unui mesaj semnat de către persoana căreia îi este emis certificatul digital
    b. Decriptarea unui mesaj criptat de persoana căreia îi este emis certificatul
    c. Criptarea unui mesaj destinat persoanei căreia îi este emis certificatul

27. Pentru a asigura securitatea unei aplicații web, unde este locul in care trebuie plasate validările asupra datelor introduse de utilizatori?
    a. validările privind autorizarea utilizatorilor de a efectua o acțiune trebuie să fie făcute client-side, iar cele ce privesc integritatea datelor trebuie făcute server-side
    b. server-side
    c. client-side

28. Încrederea unui utilizator într-o autoritate de certificare:
    a. presupune emiterea de către autoritatea de certificare a unui certificat digital utilizatorului
    b. presupune cunoașterea de către utilizator a cheii publice a autorității de certificare
    c. presupune cunoașterea de către utilizator a cheii private a autorității de certificare

29. Un certificat digital autosemnat:
    a. Conține cheia privată corespunzătoare cheii publice cu care se face semnarea certificatului
    b. Conține cheia publică corespunzătoare cheii private cu care se face semnarea certificatului
    c. Fiind autosemnat conține atât cheia publică cât și cheia privată corespunzătoare

30. Semnarea unui document asigură:
    a. Datarea în timp a documentului
    b. Confidențialitatea datelor conținute în document
    c. Autenticitatea documentului
    d. Nemodificarea ulterioară a documentului

31. Cum se poate preveni o vulnerabilitate de tip SQL Injection?
    a. prin limitarea lungimii pentru fiecare dintre parametrii folosiți în interogări
    b. prin utilizarea de Prepared Statements
    c. prin adăugarea de apostroafe în jurul parametrilor folosiți în interogări

32. Pentru crearea unei infrastructuri bazate pe chei publice și private este necesar:
    a. Generarea perechii (cheie publică, cheie privată) implicate în procesul de semnare și verificare a certificatelor digitale emise
    b. Obținerea unui certificat digital semnat de către o autoritate de certificare recunoscută
    c. Obținerea unei perechi (cheie publică, cheie privată) de la o autoritate de certificare recunoscută

33. Care dintre următoarele afirmații despre un „exploit” sunt adevărate?
    a. Se bazează pe validări insuficiente ale datelor de intrare
    b. Este folosit doar pentru atacuri remote
    c. Trebuie scris în același limbaj ca și cel în care este scris programul atacat

34. Vulnerabilitățile de tip Social Engineering se datorează:
    a. Constrângerilor insuficiente impuse de regulile de securitate ale unui firewall
    b. Ratei de penetrare mai ridicată a noilor tehnologii comparativ cu capacitatea de absorbție a acestora
    c. Vulnerabilităților descoperite periodic la nivelul World Wide Web-ului

35. Pentru limitarea atacurilor Web se recomandă:
    a. Auditul codului server side și folosirea de librării specializate consacrate pentru efectuarea validărilor
    b. Folosirea unor mecanisme de securitate complementare precum diferite module de securitate la nivelul serverului web (spre exemplu mod_security pe Apache)
    c. În cazul folosirii de aplicații web larg răspândite în Internet, actualizarea periodică a acestora și urmărirea listelor de discuții și a anunțurilor dezvoltatorilor
    d. Folosirea protocolului https în locul protocolului http pentru a accesa aplicația web

36. Care dintre următoarele reprezintă măsuri pentru prevenirea atacurilor locale?
    a. Schimbarea sistemului de fișiere în care rulează un proces server (chroot)
    b. Limitarea numărului de programe care au bitul SUID/SGID setat
    c. Rularea serviciului nu ca super-user ci cu privilegiile unui utilizator obișnuit

37. Un atac local presupune:
    a. Exploatarea unei vulnerabilități din cadrul unui proces server
    b. Accesarea unui sistem de la consola acestuia
    c. Escaladarea de privilegii

38. Care dintre următoarele tipuri de atacuri este asociat cu escaladarea de privilegii?
    a. Atacurile de tip DDOS
    b. Atacurile remote
    c. Atacurile locale

39. Atacurile remote pot fi prevenite prin:
    a. Măsuri de securitate împotriva atacurilor locale
    b. Instalarea de update-uri pentru sistemul de operare
    c. Folosirea unui firewall
    d. Închiderea porturilor și oprirea serviciilor inutile

40. Prin shell code se înțelege:
    a. Codul în limbaj de asamblare al interpretorului de comenzi Unix
    b. Un exploit descris într-un fișier de comenzi și executat de către shell-ul UNIX
    c. Un cod scris de obicei în limbaj de asamblare și care este injectat remote de către atacator pentru a-i oferi un shell

41. Succesul atacurilor remote asupra proceselor server vulnerabile se datorează:
    a. Modificării pe stivă a adresei de revenire din cadrul unei funcții
    b. Suprascrierii stivei cu codul remote care se dorește a fi executat de către atacator
    c. Invalidării insuficiente asupra dimensiunii datelor de intrare

42. Din ce motive un atacator instalează pe un sistem compromis un rootkit?
    a. Pentru a avea o portiță de acces pentru accesarea ulterioară a sistemului
    b. Pentru a accesa sistemul ca root (superuser)
    c. Pentru a-și ascunde urmele

43. Detectarea unui virus poate fi îngreunată de:
    a. Caracterul metamorfic al acestuia
    b. Suprascrierii anumitor apeluri de sistem de către virus
    c. Lipsa rutinei de multiplicare a virusului

44. Care dintre următoarele afirmații sunt adevărate despre viruși și viermi?
    a. Un vierme este un **virus** care se răspândește folosind rețeaua Internet
    b. Virușii se răspândesc exclusiv offline, în timp ce viermii se răspândesc prin intermediul rețelei Internet
    c. Virușii au nevoie pentru a se răspândi de interacțiunea cu utilizatorul uman, **pe când viermii** se răspândesc automat

45. Vulnerabilitățile web pot duce la:
    a. Un atac remote și continuarea acestuia cu unul local
    b. Modificarea regulilor de firewall referitoare la portul 80 (HTTP) pentru a oferi atacatorului noi modalități de acces
    c. Compromiterea conținutului site-ului web ce conține o aplicație web vulnerabilă

46. Care dintre următorii factori conduc la răspândirea mai agresivă a webworm-urilor?
    a. Omogenitatea aplicațiilor web folosite în Internet
    b. Exportarea de către aplicațiile web a unei "semnături" ce indică numele și versiunea aplicației web
    c. Numărul relativ mic de servere web folosite în Internet (Apache și IIS)
    d. Folosirea motoarelor de căutare pentru a localiza alte sisteme vulnerabile

47. Care dintre următoarele reprezintă proprietăți ale shell codului injectat remote de către un atacator?
    a. Este scris pe același număr de biți ca și nucleul sistemului de operare ce se dorește a fi atacat
    b. Adresele în cadrul shell code-ului trebuie să fie absolute, nu relative
    c. De obicei nu trebuie să conțină octeți cu valoarea 0

48. Epidemia datorată unui virus informatic este cu atât mai mare cu cât:
    a. Diversitatea sistemelor (din punct de vedere hardware și software) atacate este mai mică
    b. Factorul uman în particular și societatea în general nu absorb suficient de rapid noile tehnologii pe care virusul le exploatează
    c. Numărul de sisteme antivirus instalate pe sistemele atacate este mai mic

49. Care dintre următorii factori fac ca un sistem de calcul să fie mai susceptibil la atacuri:
    a. Programele SUID-ate
    b. Porturile deschise
    c. Utilizatorii sub care rulează anumite servicii

50. Pentru a-și ascunde urmele, un atacator care a compromis securitatea unui sistem poate folosi:
    a. Pachete UDP având adresa IP sursă falsificată (spoofing)
    b. Un rootkit
    c. Un troian

51. Atacurile locale se bazează pe:
    a. Vulnerabilități în programele care au bitul SUID setat
    b. Vulnerabilități în diverse procese server
    c. Vulnerabilități la nivelul apelurilor de sistem oferite de către sistemul de operare
    d. Lipsa securității fizice a sistemului și a liberului access la consola acestuia

52. Exploiturile pot fi folosite pentru a ataca:
    a. Aplicații web
    b. Aplicații client
    c. Procese server
    d. Orice proces care citește date de intrare

53. Care este scopul unui „honeypot"?
    a. Atragerea atacatorilor pentru a le monitoriza și înțelege tacticile
    b. Protejarea datelor mai sensibile prin criptarea acestora într-un „honeypot"
    c. Identificarea și eliminarea software-ului malițios prin rularea acestuia într-o mașină virtuală „honeypot"

54. Ce înseamnă un exploit de tip "zero-day"?
    a. Un atac care exploatează o vulnerabilitate de securitate care nu este încă cunoscută de către dezvoltatorii software
    b. tactică de securitate folosită pentru a preveni accesul neautorizat la o rețea
    c. Un tip de criptare folosit pentru a proteja date sensibile
    d. Un exploit folosit în prima zi ("ziua zero") după lansarea unui patch pentru o anumită vulnerabilitate

55. Ce presupune un atac de tip „phishing”?
    a. Spargerea sistemelor server (site web, server de date) aparținând unei instituții bancare
    b. Clonarea unui site web legitim
    c. Trimiterea de e-mailuri în masă prin care destinatarii sunt invitați să își divulge datele personale

56. Ordonați următoarele forme de malware în ordine cronologică crescătoare a apariției:
    a. dialer, ransomware, scareware
    b. dialer, scareware, ransomware
    c. dialer, ransomware, scareware
    d. ransomware, dialer, scareware

57. Ce este ingineria socială (social engineering)?
    a. Utilizarea manipulării psihologice pentru a obține informații confidențiale de la diverse personae
    b. metodă de gestionare a proceselor existente la nivelul societății umane
    c. Modul în care societatea își definește propriile procese de (auto) protecție în fața pericolelor

58. Ce este un „ransomware”?
    a. Un tip de software malițios care blochează accesul utilizatorului la sistemele sau datele sale și solicită o răscumpărare pentru deblocare
    b. Un instrument de criptare folosit pentru a proteja date sensibile
    c. Un tip de atac care vizează ștergerea datelor critice

59. Care dintre următoarele sunt vulnerabilități/exploaturi celebre apărute recent?
    a. Basshole
    b. Shellshock
    c. Heartbleed

60. Ce este un atac de tip phishing?
    a. Un atac care încearcă să obțină informații sensibile prin inducerea în eroare a utilizatorilor
    b. Un atac care are ca scop supravegherea rețelelor sociale
    c. Un atac care folosește software malițios pentru a compromite un system

61. Un rootkit este folosit pentru:
    a. Ascunderea urmelor lăsate de un atacator
    b. Oferirea unei portițe de acces (backdoor) atacatorului
    c. Atacarea de la distanță a unui system

62. “Vulnerability window” înseamnă:
    a. Intervalul de timp dintre prima exploatare a unei vulnerabilități și dezvoltarea unui patch pentru acea vulnerabilitate
    b. Intervalul de timp dintre descoperirea unei vulnerabilități într-o aplicație software și dezvoltarea unui patch pentru această vulnerabilitate
    c. Intervalul de timp dintre infectarea sistemului și dezinfectarea acestuia

63. Rețelele „BotNet” sunt folosite, în general, pentru:
    a. Atacuri de tip DDoS
    b. Utilizarea distribuită a puterii de procesare a computerelor pentru sarcini care necesită resurse mari, cum ar fi: spargerea parolelor, decriptarea, minarea de criptomonede
    c. Trimiterea de e-mailuri nesolicitate (spam)

64. Ce este un atac de tip „Man-in-the-Middle” (MitM)?
    a. Un atac în care atacatorul interceptează și modifică comunicațiile dintre două entități
    b. Un tip de autentificare folosit pentru a accesa rețele securizate
    c. O metodă de atac folosită împotriva terților de încredere

65. Macroviruşii au următoarele avantaje faţă de un virus clasic scris în limbaj de asamblare:
    a. Găsesc în reţelele Enterprise, unde există un flux mare de documente, un mediu perfect pentru răspândire
    b. Sunt independenţi de platformă, fiind scrişi în limbaje de tip scripting
    c. Sarcina malițioasă (payload) adăugată de virus în fișierul infectat ocupă mai puțin spațiu
    d. Prin infectarea fişierelor Office, cum ar fi documente Word sau Excel, nu pot fi detectaţi de antiviruşii bazaţi pe semnături

66. Ce tip de malware se replică ataşându-se fişierelor executabile sau zonelor de sistem?
    a. Vierme
    b. Trojan
    c. Rootkit
    d. Virus

67. Ce tip de malware se răspândeşte automat prin reţele, fără interacţiunea utilizatorului?
    a. Vierme
    b. Trojan
    c. Virus
    d. Botnet

68. Ce deosebeşte un troian de alte tipuri de malware?
    a. Se autoreplică între sisteme
    b. Dezactivează sistemul de operare
    c. Se deghizează ca un software legitim
    d. Necesită un rootkit pentru a funcţiona

69. Care este funcţia unui rootkit într-un sistem compromis?
    a. Criptează fişierele utilizatorului
    b. Ascunde prezenţa atacatorului şi permite accesul viitor
    c. Afişează reclame pop-up
    d. Şterge software-ul antivirus

70. Ce componentă este folosită de un virus pentru a se multiplica?
    a. Modul de încărcare (payload)
    b. Interfaţa cu utilizatorul
    c. Codul de replicare
    d. Strat de ofuscare

71. Ce tip de malware preia controlul modemului pentru a apela numere cu taxă specială?
    a. Adware
    b. Spyware
    c. Dialer
    d. Rootkit

72. Ce este un botnet?
    a. O tehnică de inginerie social
    b. O reţea de calculatoare infectate controlate de la distanţă
    c. O reţea peer-to-peer
    d. Un grup de troieni

73. Cum funcţionează, de obicei, scareware-ul?
    a. Criptează datele şi cere o răscumpărare
    b. Fură datele de autentificare
    c. Imită un antivirus pentru a speria utilizatorii să instaleze malware real
    d. Creează actualizări false de system

74. Care este rolul unui „botmaster”?
    a. Inginer antivirus
    b. Administrator de rețea
    c. Controlorul unui botnet
    d. Replicator de viermi

75. Ce face ca APT-urile (Advanced Persistent Threats) să fie deosebit de periculoase?
    a. Abilitatea lor de a șterge toate fișierele
    b. Comportamentul lor discret și de spionaj pe termen lung
    c. Utilizarea rețelelor sociale
    d. Viteza mare de infecție

76. Ce tip de software colectează date despre utilizator fără consimțământ explicit, dar poate părea legitim?
    a. Software invaziv asupra confidențialității
    b. Adware
    c. Keylogger
    d. Exploit zero-day

77. Ce este malware-ul polimorf?
    a. Folosește polimorfismul din programarea orientată pe obiecte
    b. Își modifică structura codului păstrând același comportament
    c. Șterge fișiere la întâmplare
    d. Atacă simultan mai multe sisteme de operare

78. Ce vulnerabilitate este exploatată printr-un atac de tip buffer overflow?
    a. Neconcordanțe în permisiunile fișierelor
    b. Lipsa verificărilor de limită la alocarea memoriei
    c. Configurări greșite ale firewall-ului
    d. Autentificare compromise

79. Ce protejează DEP (Data Execution Prevention)?
    a. Împotriva ransomware-ului
    b. Împotriva execuției de cod malițios în regiuni de memorie rezervate datelor
    c. Împotriva autentificării neautorizate
    d. Împotriva keyloggerelor

80. Ce înseamnă „fereastra de vulnerabilitate” (vulnerability window)?
    a. Intervalul dintre infecție și curățare
    b. Intervalul dintre descoperirea unei vulnerabilități și disponibilitatea unui patch
    c. Intervalul dintre logare și delogare
    d. Intervalul dintre scanare și detecție

81. Ce tehnică cheie este folosită în atacurile buffer overflow pentru a deturna fluxul de execuție?
    a. Interceptarea apelurilor de system
    b. Suprascrierea adresei de revenire în stivă
    c. Supraîncărcarea memoriei
    d. Schimbarea permisiunilor fișierelor

82. Care funcție din C este considerată periculoasă în contextul buffer overflow?
    a. scanf
    b. gets
    c. fopen
    d. fread

83. Ce exploatează un exploit de tip „zero-day”?
    a. Semnăturile antivirus
    b. Vulnerabilități necunoscute și nepatch-uite
    c. Porturi deschise
    d. API-uri ale rețelelor sociale

84. Care este scopul instrucțiunii ret în limbaj de asamblare?
    a. Încarcă memorie
    b. Execută o funcție
    c. Returnează controlul funcției apelante
    d. Alocă spațiu în stivă