Q1. Care dintre urmatoarele afirmatii despre procesul de schimb de chei sunt adevarate in contextul folosirii de algoritmii de criptare simetrici, respectiv asimetrici:

a) In ambele situatii, schimbul de chei se poate realiza pe acelasi canal / prin acelasi mecanism prin care are loc si comunicarea
b) Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare asimetrici
c) Schimbul de chei pe un alt canal / mecanism diferit de comunicare alternativ trebuie sa se realizeze doar in cazul algoritmilor de criptare simetrici
d) In ambele situatii, schimbul de chei trebuie sa se desfasoare pe un alt canal / printr-un mecanism de comunicare alternativ

Ans: d)

Reason: pt criptare simetrica - cheia o interschimbi ori f2f spre exemplu ca pe vremuri. La criptare asimetrica, cheia publica se distribuie printr-un certificat digital spre ex https://en.wikipedia.org/wiki/Key_distribution

Q2. 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

Ans: all

Reason: vezi slide-ul cu lista asta

Q3. 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 e important ca, canalul pe care este transmisa sa fie sigur
d. In cadrul unui certificat digital

Ans: d

Q4. Care dintre urmatoarele mecanisme limiteaza succesul exploit-urilor de tip shell code?

a. Arhivarea (compactarea) stivei
b. Randomizarea stivei
c. Data Execturion Prevention
d. Inlaturarea bitului de executie de pe programul atacat

Ans: b, c

Q5. Care dintre urmatoarele vulnerabilitati ar putea fi exploatata pentru a fura sesiunea unui utilizator autentificat?

a. Cross-Site Request Forgery (CRSF)
b. Cross-Site scripting (XSS)
c. SQL Injection

Ans: b.

Q6. Care dintre urmatoarele afirmatii sunt adevarate in ceea ce priveste certificatele digitale Web client-side:

a. Sunt transmise clientului exclusiv pe canale de incredere (sigure)
b. Sunt semnate cu aceeasi cheie privata cu care este semna si certificatul serverului Web
c. Folosite impreuna cu protocolul SSL si cu autentificarea de paza de user si parola sporesc securitatea autentificarii si identificarii clientului

Ans: a, c

Q7. Care este pericolul interceptarii de catre un tert (Man in the Middle) a unei chei publice din cadrul unui certificat digital semnat de catre o autoritate de certificare si transmis pe un canal nesigur ?

a. Atacatorul poate inlocui cheia publica din certificat cu propria cheie publica, corespunzatoare unei chei private pe care acesta o detine
b. Nu exista niciun pericol, destinatarul la care ajunge certificatul il poate valida pe baza semnaturii depuse de autoritatea de certificare
c. Atacatorul poate inlocui cheia privata din certificat cu propria cheie privata, corespunzatoare unei chei publice pe care acesta o detine

Ans: b) Reason: certificatul digital e public, si el contine cheia publica, oricine are acces.

Q8. Cum se poate fura un cookie de sesiune al unui alt utilizator ?

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

Ans: b, c

Reason: Raspunsul “A” nu este pentru ca poti ramane conectat pe site-uri si sa parasesti pagina (nu te mai deloghezi, ramai conectat), cum e teams-ul (cu conditia sa fie construite bine)

Q9. Care dintre urmatoarele reprezinta masuri pentru evitarea vulnerabilitatilor de tip XSS:

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

Ans: a

Q10. Cheia privata este folosita pentru:

a. Semnarea documentelor
b. Verificarea semnaturilor digitale
c. Decriptarea mesajelor primite
d. Criptarea mesajelor trimise

Ans: a,c

Q11. Care dintre urmatoarele afirmatii sunt adevarate in ceea ce priveste o semnatura digitala:

a. **Semnatura digitala este de fapt un hash**
b. Orice document semnatdigital poate fi datat in timp
c. 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)
d. **Semnatura digitala este criptata cu ajutorul unei chei private**

Ans: a, d

Reason: Slide 15: It is a hash of a document encrypted with the author's private key

Q12. Ce memoreaza autoritatile de marca temporala?

a. cererile si raspunsurile venite spre si dinspre acestea

b. nu memoreaza nimic, doar semneaza, validitatea semnaturii putand fi usor dovedita cu ajutorul cheii publice a autoritatii de marca temporala

c. documente semnate

Ans: a)

Reason: Slide 54 (Functiile cerute unui ceas de increde Timestamp Authority: sa arhiveze durabil cererile si raspunsurile)

Q13. Apelurile sistem Linux pot fi apelate ca functii de la intreruperea:

a. 21h
b. Apelurile sistem Linux sunt implementate in C nu ca functii de la o anumita intrerupere
c. **80h**
d. 80
e. 21

Ans: c

Q14. Care dintre urmatoarele protocoale folosesc criptografia cu cheie publica:

a. **Https**
b. Smtp
c. Nslookup
d. **Ssh**

Ans: a, d

Q15. Ce se trimite unei autoritati de marca temporala pentru a dovedi ca un anumit document exista la un anumit moment de timp ?

a. **Un hash al documentului si o semnatura**
b. Documentul, semnatura si momentul de timp
c. Documentul semnat

Ans: a

Q16. Caracterul NULL (‘\0’) nu apare deobicei in string-ul ce reprezinta shell code-ul deoarece:

a. **Majoritatea programelor exploatate sunt scrise in limbajul C, acest caracter ar marca terminarea prematura a datelor de intrare**
b. 00h nu este o adresa de revenire valida in cadrul stivei
c. Octetul cu valoarea 0 nu reprezinta codul unei instructiunii valide in limbaj de ansamblare

Ans: a

Q17. Care dintre urmatoarele reprezinta masuri pentru evitarea injectiilor SQL:

a. **Folosirea la nivelul backend-ului de mecanisme de tipul prepared statement**
b. **Verificari riguroase la nivelul backend-ului legate de validitatea datelor introduse precum si folosirea de biblioteci specializate pentru persistarea datelor (ORM-uri)**
c. Verificari reguroase la nivelul browserului legate de valididatea datelor introduse

d. Dezactivarea in cadrul aplicatiei Web a posibilitatii rularii de cod SQL de catre browser

Ans: a, b

Q18. Criptarea datelor intre parteneri se poate face in Internet la care dintre urmatoarele nivele:

a) Fizic si legatura de date
b) Retea
c) Aplicatie

Ans: a), b), c)

Q19. Certificatele digitale autosemnate se folosesc:

a) Un certificat nu poate fi autosemnat
b) De catre autoritatile de certificare
c) Doar daca apartin/sunt emise de catre un utilizator pentru el insusi si sunt semnate si de catre autoritatile de certificare

Ans: b)

Q20. Diseminarea in siguranta catre terti a cheii publice a unei entitati se poate face:

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

Ans: a), d)

Q21. Care este pericolul compromiterii unui certificat digital emis unui site Web in scopul autentificarii acestuia de catre clienti (compromitere in sensul aducerii acestui certificat la cunostinta publica) ?

a) **Se poate extrage cheia publica din acel certificat, dar acest fapt nu reprezinta un pericol**
b) Se poate extrage cheia privata din acel certificat
c) Se pot semna documentele in numele site-ului web respectiv
d) **Nu exista niciun pericol**

Ans: a), d)

Reason: certificatul digital al oricarui site e public, orice are acces la el...iar el detine cheia publica.

Q22. Autoritatile de marca temporala care dovedesc existenta nui document la un anumit moment de tip:

a) Semneaza si ele documentul
b) Stocheaza documentul
c) **Semneaza un hash al documentului**

Ans: c)

Q23. Functia aplicata pe text si pe cheia privata poate asigura:

a) **Confidentialitatea mesajului**
b) Nonrepudierea mesajului
c) Autenticitatea mesajului
d) Integristatea mesajulu

Ans: a)

Reason: il criptezi => confidentialitate. Daca mai era si un al treilea element (adica identitatea utilizatorului) atunci erau si b si c.

Q24. Care dintre urmatoarele reprezinta scheme de validare a unui certificat digital:

a) DCVP – Digital Certificate Validation Process
b) **OCSP – Online Certificate Status Protocol**
c) **CRLs – Certificate Revocation Lists**

Ans: b), c) (verifica daca un certificat nu mai e valid)

Reason: Certificate authorities are also responsible for maintaining up-to-date revocation information about certificates they have issued, indicating whether certificates are still

valid. They provide this information through Online Certificate Status Protocol (OCSP) and/or Certificate Revocation Lists (CRLs).

Q25. Cheia publica este folosita pentru:

A) Semnarea documentelor
B) Criptarea mesajelor
C) Decriptarea mesajelor
D) Verificarea semnaturilor digitale

Ans: b), d)

Injectiile JavaScript se datoreaza:

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

Cum se poate preveni o vulnerabilitate de tip SQL Injection?

a) Prin limitarea lungimii pentru fiecare dintre parametrii folositi in interogari

b) Prin utilizarea de Prepared Statements

c) Prin adaugarea de apostroafe in jurul parametrilor folositi in interogari

Pentru evitarea injectiilor SQL in PHP 7 se recomanda:

a) Eliminarea ghilimelelor si apostrofelor din datele primite de la client

b) Evitarea acestora folosind functia mysql_real_escape_string

c) Folosirea de "prepared statement"-uri

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

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

b) Server-side

c) Client-side

Increderea unui utilizator intr-o autoritate de certificare:

a) Presupune emiterea de catre autoritatea de certificare a unui certificat digital utilizatorului

b) Presupune cunoasterea de catre utilizator a cheii publice a autoritatii de certificare

c) Presupune cunoasterea de catre utilizator a cheii private a autoritatii de certificare

Semnarea unui document asigura:

a) Datarea in timp a documentului

b) Confidentialitatea datelor continute in document

c) Autenticitatea documentului

d) Nemodificarea ulterioara a documentului

Since the fake www.bank.example does not know the corresponding private key, it cannot create the signature needed to verify its authenticity. Daca se modifica documentul se modifica si semnaruta.

Un certificat digital autosemnat:

a) Contine cheia privata corespunzatore cheii publice cu care se face semnarea certificatului

b) Contine cheia publica corespunzatore cheii private cu care se face semnarea certificatului

c) Fiind autosemnat contine atat cheia publica cat si cheia privata corespunzatoare

Reason: In cryptography and computer security, **self-signed certificates** are public key certificates that are not issued by a certificate authority (CA)

Un certificat digital ajuta la:

a) Verificarea integritatii si autenticitatii unui mesaj semnat de catre persoana careia ii este emis certificatul digital

b) Decriptarea unui mesaj criptat de persoana careia ii este emis certificatul

c) Criptarea unui mesaj destinat persoanei careia ii este emis certificatul

Reason: The certificate includes the public key and information about it, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer)

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

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

b) Obtinerea unui certificat digital semnat de catre o autoritate de certificare recunoscuta

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