Examen SSI

Ex1

Criptologie - Știința care se ocupa de criptanaliza si criptografie.

Criptografie - Disciplina care studiază principiile, mijloacele si metodele de transformare a datelor pentru a ascunde conținutul lor semantic, a preveni utilizarea lor neautorizata sau a preveni modificarea lor nedetectata.

Criptanaliza - Încercare de a înfrânge protecția criptografica fără o cunoaștere inițiala a cheii utilizate in furnizarea protecției

! Confidențialitate - Asigurarea ca informațiile nu sunt dezvăluite entităților neautorizate

! Integritate - Protejarea împotriva modificării sau distrugerii necorespunzătoare a informatiilor

! Disponibilitate - Asigurarea accesului si utilizării informațiilor in timp util si fiabil

Adversar - O entitate (inclusiv un insider) care acționează rău intenționat pentru a compormite un sistem.

Securitate - O condiție care rezulta din stabilirea si menținerea masurilor de protectie care permit unei organizații/sistem sa își îndeplinească misiunea sau functiile critice, in ciuda riscurilor reprezentate de amenințări.

Risc - O măsură a gradului in care o entitate este amenințată de o eventuala circumstanta sau eveniment.

Vulnerabilitate - Slăbiciune intr-un sistem informațional, proceduri de securitate ale sistemului, controale interne sau implementare care ar putea fi exploatate sau declansate de o sursa de amenințare.

Securitate cibernetica - Capacitatea de a proteja/apăra spațiul cibernetic de atacuri cibernetice.

malware = Hardware, firmware sau software rău intenționate care sunt introduse intentionat intr-un sistem pentru a deteriora funcționarea normala a acestuia.

virus = Un program care se poate răspândi pentru a infecta sisteme fără permisiunea utilizatorului si fără ca acesta sa știe.

dropper = Un software care ascunde un malware de anti-virus pentru a facilita infectarea sistemelor.

downloader = Un software ce are ca scop instalarea unui malware pe un sistem fara sa declanșeze alarme de securitate.

trojan = Un tip de malware deghizat intr-un software normal care odată ajuns in sistem oferă atacatorului toate permisiunile user-ului.

spyware = Un tip de malware care acumulează informațiile unui sistem si al utilizatorului si le trimite mai departe fără cunoștința sau permisiunea acestuia.

riskware = Orice program legitim care prezintă riscuri potențiale din cauza vulnerabilității de securitate, incompatibilității software-ului sau încălcărilor legale.

ransomware = Un tip de malware care amenință să publice sau blochează accesul la date sau la un sistem, de obicei prin criptarea acestora, până când victima plătește o taxă de răscumpărare atacatorului.

adware = Un tip de malware sau software nedorit conceput pentru a furniza reclame direcționate pe computerele infectate

worm = Un subset al malware-ului trojan care se poate răspândi singur de la un computer la altul de obicei prin LAN.

obfuscare = A face ceva greu de înțeles. Un cod greu de înțeles este mai greu de atacat.

Inginerie sociala - O încercare de a păcăli pe cineva sa dezvăluie informații (de exemplu, o parola) care pot fi folosite pentru a ataca sisteme sau rețele

Phishing - O tehnica pentru încercarea de a achiziționa date sensibile, cum ar fi numerele de cont bancar, printr-o solicitare frauduloasa prin e-mail sau pe un site web, in care făptuitorul se maschează ca o afacere legitima sau o persoana de incredere.

Whaling - Un tip specific de phishing care vizează membrii de rang înalt ai organizatiilor.

Pharming - Utilizarea mijloacelor tehnice pentru a redirecționa utilizatorii către accesarea unui site Web fals, mascat drept unul legitim si divulgarea informatiilor personale.

Spear phishing - Un termen colocvial care poate fi folosit pentru a descrie orice atac de phishing foarte vizat

Spoofing - Falsificarea adresei de trimitere a unei transmisii pentru a obține intrarea ilegala intr-un sistem securizat.

Ex2

- ex adevărat/fals destul de basic; ce ti rămâne după ce răsfoiești pdf-ul

Ex3

RSA

- Algoritm de criptare cu cheie publica
- Utilizeaza doua chei diferite pentru criptare si decriptare: cheie publica si cheie privata
- Generarea cheilor
    - Pentru a cripta/decripta date, RSA trebuie sa genereze o cheie privata si una publica
    - Pentru modulul de criptare/decriptare n se aleg doua numere prime mari diferite p si q care se inmultesc (n = p*q)
    - Cheia publica: exponentul e care este un numar intreg mai mic decat (p-1)(q-1) si este coprim (p-1)(q-1)
    - Cheia privata: d este inversul modular al lui e mod (p-1)(q-1)

! e*d mod (p-1)(q-1) = 1

Ex4

Sisteme de criptare afine

$E(x) = (a * x + b) \bmod m$

$D(y) = (a^{-1}(y-b)) \bmod m$

- x – textul clar
- y – textul criptat
- a, b – constante (a si m coprime, b orice numar intreg)
- m este dimensiunea alfabetului

Ex5

ElGamal

- Se bazeaza pe DLP (dificultatea problemei DDH)
    - Fie G un grup finit si m <- R G. Daca g <- R g atunci g' = mg ramane aleator in G: P(mg=g') = 1/|G|, unde probabilitatea este data de alegerea aleatoare a lui g.
- Se genereaza (G, q, g) si se alege x aleator din Zq si se calculeaza $h=g^x$
    - Cheia publica este G, q, g, h
    - Cheia privata este G, q, g, x

- Enc: data o cheie publica G, q, g, h si un mesaj m se alege y aleator din Zq si intoarce $c = (c1, c2) = (g^y, m * h^y)$
- Dec: data o cheie privata G, q, g, x si un mesaj criptate c=(c1, c2) intoarce $m = c2*c1^{-x}$

Ex6

Meet-in-the-middle

- Daca se cunoaște o pereche de text clar / text criptat (x, y) cu y = F k2(F k1(x)):

1. Pentru fiecare k1 din $\{0,1\}^n$ calculează z = F k1(x) si păstrează (z, k1)
2. Pentru fiecare k2 din $\{0,1\}^n$ calculează $z = (F\ k2)^{-1}$ si păstrează (z, k2)
3. Verifica daca exista perechi (z, k1) si (z, k2) care coincid pe prima componenta
4. Atunci valorile k1 si k2 satisfac F k1(x) = F $k2^{)-}$1(y) adică y = F'k1, k2 (x)

- Complexitatea acestui atac este 2^n.

Man-in-the-middle

- Schimbul Diffie Hellman e total nesigur pentru un adversar activ
- Scenariu:
    - Alice ii trimite lui Bob mesajul
    - Oscar intercepteaza mesajul si raspunde lui Alice in locul lui Bob
    - Oscar si Alice detin acum cehia comuna
    - Oscar initiaza, in locul lui Alice, o noua sesiune cu Bob
    - Oscar si Bob detin acum cheia comuna
- atacul este posibil deoarece poate impersona pe Alice sau pe Bob,
- Oscar îl decriptează folosind k_A, apoi îl recripteaza folosind k_B și îl transmite către Bob
- Alice și Bob comunica fără sa fie conștienți de existența lui Oscar
- deci Alice trimite h1 către B dar este interceptat de Oscar și transformat în h1' (la fel și pentru h2), iar Oscar are acces la mesaje, cheile de decriptare fiind calculate în funcție de h1' si h2'