Fișă de lucru 2

Securitatea rețelelor de calculatoare

Nume și prenume _____ Clasa _____ Data _____

Timp de lucru: 50 de minute

90 de puncte + 10 puncte din oficiu

Vei identifica obiectivele securității, vei recunoaște tipurile de atacuri și vei propune măsuri de protecție.

1. Recunoaște obiectivul de securitate 12 puncte

Completează cu: confidențialitate, integritate, disponibilitate. Folosește fiecare termen o singură dată. Câte 4 puncte pentru fiecare răspuns.

a) Informațiile pot fi accesate doar de persoane autorizate: _____.
b) Datele sunt corecte și nu au fost modificate neautorizat: _____.
c) Serviciile pot fi utilizate și răspund cererilor utilizatorilor: _____.

2. Clasifică atacurile 18 puncte

Notează C pentru confidențialitate, I pentru integritate sau D pentru disponibilitate. Urmează clasificarea din material. Câte 3 puncte pe rând.

Atac sau situație	**C / I / D**
Interceptarea informațiilor în timpul transmiterii	
Furtul unei sesiuni deja autentificate	
Inundarea serverului cu cereri până nu mai răspunde	
Abuzul de privilegii	
Divulgarea accidentală a unor informații private	
Furnizarea de date neașteptate care blochează sistemul	

3. Asociază noțiunea cu descrierea 12 puncte

Scrie litera corectă. Fiecare literă se utilizează o singură dată. Câte 2 puncte pentru fiecare asociere.

1. Manipulare socială ___ 2. Backdoor ___ 3. Furtul sesiunii ___
4. Acumularea informațiilor ___ 5. Atac la autentificare ___
6. Supresia jurnalizării ___

A. Preluarea unei sesiuni a unui utilizator deja autentificat.
B. Combinarea informațiilor din surse diferite pentru a deduce date private.
C. Păcălirea unei persoane pentru a obține informații sau acces.
D. Ascunderea evenimentelor sau îngreunarea analizei jurnalelor.
E. Identificarea nelegitimă drept alt utilizator sau altă aplicație.
F. Folosirea unei căi ascunse de acces la sistem.

4. Adevărat sau fals 16 puncte

Notează A sau F (2 puncte pe enunț). Corectează cele două afirmații false (4 puncte pentru fiecare reformulare).

a) Un sistem este sigur dacă folosește doar cele mai noi tehnologii. ___
b) Principiul „least privilege” cere acordarea doar a drepturilor necesare. ___
c) Jurnalizarea și monitorizarea ajută la detectarea incidentelor. ___
d) Setările de securitate pot elimina complet orice risc. ___

Reformularea primei afirmații false:

Reformularea celei de-a doua afirmații false:

5. Explică și exemplifică 12 puncte

Câte 6 puncte pentru fiecare cerință: 3 puncte pentru explicație și 3 puncte pentru exemplu.

a) Explică principiul „defense in depth” și oferă un exemplu care combină cel puțin două măsuri de protecție a unei rețele.

b) Explică de ce informațiile sensibile trebuie criptate când sunt transmise printr-o rețea nesigură. Oferă un exemplu de informație care necesită protecție.

Indiciu: gândește-te ce ar putea vedea o persoană care interceptează traficul.

6. Rezolvă un studiu de caz 20 de puncte

Citește situația și răspunde la cerințe.

În rețeaua unei școli, toți elevii folosesc același cont cu drepturi de administrator. Firewallul a fost dezactivat pentru a nu mai afișa notificări. Aplicațiile nu sunt actualizate, iar jurnalele de activitate nu sunt verificate. În plus, nu se realizează copii de siguranță ale documentelor importante.

a) Alege patru probleme distincte. Pentru fiecare, propune o măsură concretă și adecvată. (16 puncte: 2 puncte pentru problemă și 2 puncte pentru măsură.)

Problema identificată	**Măsura de protecție propusă**

b) Explică de ce instalarea unui antivirus nu rezolvă singură toate problemele din situația descrisă. Menționează o măsură tehnică și o măsură care ține de oameni sau de proceduri. (4 puncte)