1. Un atac local presupune:

    a. Exploatarea unei vulnerabilitati din cadrul unui proces server

    b. Accesarea unui sistem de la consola acestuia

    c. Escaladarea de privilegii

Nu este b pentru ca nu ne referim la atac fizic

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

    a. Atacurile de tip DDOS

    b. Atacuri remote

    c. Atacurile locale

3. Atacurile remote pot fi prevenite prin:

    a. Masuri de securitate impotriva atacurilor locale

    b. Instalarea de update-uri sistemului de operare

    c. Folosirea unui firewall

    d. Inchiderea porturilor si oprirea serviciilor inutile

4. Prin shell code se intelege:

    a. Codul in limbaj de ansamblare al interpretorului de comenzi Unix

    b. Un exploit descris intr-un fisier de comenzi si executat de catre shell-ul UNIX

    c. Un cod scris de obicei in limbaj de asamblare si care este injectat remote de catre atacator pentru a-i oferi un shell

5. Vulnerabilitatile de tip Social Engineering se datoreaza:

    a. Ratei de penetrare mai ridicata a noilor tehnologii comparativ cu capacitatea de absorbtie a acestora

    b. Vulnerabilitatilor descoperite periodic la nivelul WWW-ului

    c. Constrangerilor insuficiente impuse de regulile de securitate ale unui firewall

6. Care dintre urmatoarele reprezinta masuri pentru prevenirea atacurilor locale?

   a. **Limitarea numarului de programe care au bitul SUID/SGID setat**

   b. **Schimbarea sistemului de fisiere in care ruleaza un proces server (chroot)**

   c. **Rularea serviciului nu ca super-user ci cu privilegiile unui utilizator obisnuit**

7. Succesul atacurilor remote asupra proceselor server vulnerabile se datoreaza:

   a. **Modificarii pe stiva a adresei de revenire din cadrul unei functii**

   b. **Suprascrierii stivei cu codul remote care se doreste a fi executat de catre atacator**

   c. **Invalidarii insuficiente asupra deminseiunii datelor de intrare**

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

   a. **Pentru a avea o portita de accesare ulterioara a sistemului**

   b. Pentru a accesa sistemul ca root (superuser)

   c. **Pentru a-si ascunde urmele**

9. Detectarea unui virus poate fi ingreunata de:

   a. **Caracterul metamorfic al acestuia**

   b. **Suprascrierii anumitor apeluri sistem de catre virus**

   c. Lipsa rutinei de multiplicare a virusului

10. Care dintre urmatoarele afirmatii sunt adevarate depsre virusi si viermi:

    a. Un vierme este un virus care se raspandeste folosind reteaua Internet

    b. Virusii se raspandesc exclusiv offline, in timp ce viermii se raspandesc prin intermediul retelei Internet

    c. **Virusii au nevoie pentru a se raspandi de interactiunea cu utilizatorul uman, pe cand viermii se raspandesc automat**

11. Vulnerabilitatile web pot duce la:

a. Un atac remote si continuarea acestuia cu unul local

b. Modificarea regulilor de Firewall referitoare la portul 80 (HTTP) pentru a oferi atacatorului noi modalitai de access

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

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

a. Omogenitatea aplicatiilor web folosite in Internet

b. Exportarea de catre aplicatiile web a unei "semnaturi" ce insica numele si versiunea aplicatiei web

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

d. Folosirea motoarelor de cautare pentru a localiza alte sisteme vulnerabile

13. Care dintre urmatoarele reprezinta proprietati ale shell codului injectat remote de catre un atacator:

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

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

c. De obicei nu trebuie sa contina octeti cu valoarea 0

14. Epidemia datorata unui virus informatic este cu atat mai mare cu cat:

a. Diversitatea sistemelor (din punct de vedere hardware si software) atacata este mai mica

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

c. Numarul de sisteme antivirus pe sistemele atacate este mai mic

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

a. Programele SUID-ate

b. Porturile deschise

c. Utilizatorii sub care ruleaza anumite servicii

16. Pentru a-si ascunde urmele, un atacator ce a compromi securitatea unui sistem poate folosi:

a. Pachete UDP avand adresa IP sursa falsificata (spoofing)

b. Un rootkit

c. Un troian

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

a. Octetul cu valoarea 0 nu reprezinta codul unei instructiuni valide in limbaj de ansamblare

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

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

18. Care dintre urmatoarele afirmatii despre un "exploit" sunt adevarate:

a. Se bazeaza pe validari insuficiente ale datelor de intrare

b. Este folosit doar pentru atacuri remote

c. Trebuie scris in acelasi limbaj ca si cel in care este scris programul atacat

19. Vulnerabilitatile de tip Social Engineering se datoreaza:

a. Constrangerilor insuficiente impuse de regulile de securitate ale unui firewall

b. Ratei de penetrare mai ridicata a noilor tehnologii comparativ cu capacitatea de absorbtie a acestora

c. Vulnerabilitatilor descoperite periodic la nivelul WWW-ului

20. Atacurile locale se bazeaza pe:

a. Vulnerabilitati in programele care au bitul SUID setat

b. Vulnerabilitati in diverse procese server

c. Vulnerabilitati la nivelul apelurilor sistem oferite de catre sistemul de operare

d. Lipsa securitatii fizice a sistemului si a liberului access la consola acestuia

Pentru limitarea atacurilor Web se recomanda:

a) Auditul codului server side si folosirea de librarii specializate consacrate pentru efectuarea validarilor

b) Folosirea unor mecanisme de securitate complementare precum diferite module de securitate la nivelul serverului web (spre exemplu mod_security pe Apache)

c) In cazul folosirii de aplicatii web larg raspandite in Internet, actualizarea periodica a acestora si urmarirea listelor de discutii si a anunturilor dezvoltatorilor

d) Folosirea protocolului https in locul protocolului http pentru a accesa aplicatia web

Mutatii -> toate 3
Aparitie -> dialere, scareweb, ransomware