## C1

**1. Care sunt pierderile posibile datorate unui sistem compromis?**
- pierderi de informatii
- pierderi financiare datorate alterarii anumitor valorii(bug-ul EMAG :)) )
- pierderea integritatii sitemului

**2. Care sunt cei cinci pasi principali in ciclul de management al securitatii?**
- definirea politicilor de securitate
- implementarea politicilor
- administrarea
- auditul
- manag. riscului

**3. Ce se foloseste pentru a permite unui utilizator de incredere sa realizeze anumite operatii regulate de mentenanta a sistemului fara a furniza parola utilizatorului root?**
- delegarea autoritatii(sudo)

**4. Enumerati cateva amenintari posibile la securitatea sistemului?**
- personal imbecil
- dezastre(incendii, cutremure) -> afecteaza partea fizica
- maware, virusi,etc. ->afecteaza partea software

**5. Odata ce atacatorii s-au infiltrat intr-un sistem, pot instala un program ce le permite sa obtina privilegii de root intr-un sistem. Cum se numeste acest tip de program?**
- rootkit

## C2

**1. Identificati trei probleme sau facilitati potentiale de securitate fizica in camera in care va aflati.**
- laptopuri neandocate
- usi neincuiate de la camera serverelor
- lipsa restrictiilor accesului persoanelor in anumite camere

**2. Cum se ocupa organizatia in care va aflati de securitatea fizica?**
- restrictionarea accesului fizic
- controlarea personalului ce pot porni/configura masinile folosind BIOS-ul
- oferirea unui lant de autoritate
- polite de asigurre in caz de dezastre
- sisteme anti-incendiu

**3. Explicati cateva din beneficiile utilizarii unor cozi de audit clare si bine definite.**
- se pot identifica mai usor responsabilii pt o actiune nedorita
- se poate monitoriza mai usor sistemul
- se poate determina cazua unui defect

## C3

**1. De ce este important sa existe un plan bun de securitate inainte de a incepe instalarea unui sistem?**
- pentru a avea bine definit rolul sistemului
- pentru ca sisemul poate fi atacat/compromis si imediat dupa instalare

**2. Adevarat sau Fals: Scopul pentru care un server este partitionat in functie de destinatia sa este**

**pentru a fi mai scalabil in viitor.**
- A

**3. Numiti trei grupuri de pachete ce nu sunt necesare pe un server.**
- games
- X
- GNOME
- KDE

**4. Numiti doua subsisteme sau aspecte ale unui sistem ce necesita hardening.**
- identificare si autentificare
- controlul acc si autorizare
- disponibilitatea si intergritaea sistemului
- auditul si detectia intr.
- kernel

**5. Adevarat sau fals: Capturarea configuratiei trebuie facuta doar o singura data, dupa ce sistemul a fost instalat.**
- F

## C4

**1. Adevarat sau Fals: Linux identifica un utilizator dupa numele de utilizato.**
- F(identifica dupa UID(user ID))

**2. Unde stocheaza Linux parolele utilizatorilor?**
- in shadow

**3. Ce contine fisierul /etc/default/useradd?**
- contine setarile predefinite pentru crearea IDurilor utilizator in sistem.

**4. Ce permit modulele PAM?**
- verificarea autentificicarii folosindu-se de diferite module(pt parole, pt login, etc.)
- crearea unei scheme complexe de autentificare

**5. Care sunt modulele pe care le poate utiliza pam_pwdb?**
- auth, account, password(NU-S SIGUR!!!)

**6. Adevarat sau Fals: Scopul lui pam_securetty este de a verifica /etc/securetty cu dispozitivul de pe care s-a incercat login-ul.**
- A

**7. Ce sunt parolele puternice?**
- parole de epste 8 caractere utlizand combinatii alfa numerice care nu pot fi ghicite si pot fi memorate

## C6

**1. Ce reprezinta un atac denial of service?**
-Denial of service este un atac impotriva disponibilitatii unui sistem.

**2. Care este diferenta dintre utilizarea ulimit si /etc/security/limits.conf?**

-/etc/security/limits.conf e mai usor de configurat si controlat decat folosind comanda ulimit.

**3. Numiti trei categorii principale de atacuri denial of service.**
- Distrugerea resurselor sistemului
- Alterarea configuratiei
- Epuizarea resurselor

**4. Cum se seteaza dimensiunea maxima a fisierelor create de un utilizator?**
- folosind ocmanda ulimit

**5. Adevarat sau Fals: Facilitatea de blocare a conturilor este activa in mod predefinit?**
- A

**6. Care sunt principalii pasi pentru setarea cotelor?**
- utilizand Quota :

- Mount your filesystems with quota support
- Install the quota software
- Configure your limits

**7. Numiti patru mecanisme ce permit unui sistem sa reziste la atacurile DoS.**
- hw tolerant la defect si cu resurse mai mari decat cele necesare
- personal care sa respecte anumite proceduri
- configurarea software
- securitate fizica

## C7

**1. Descrieti conceptul de integritate a sistemului.**
- este o stare a sistemului in care isi indeplineste functiile fara sa fie perturbat de diferiti factori interni/externi

**2. Care este diferenta dintre TCB si TP?**
- TCB reprezinta totalitatea componentelor hw, software si firmware ce sunt critice pt secruitatea sistemului
- TP este o componenta a OS de a permite comunicarea securizata intre useri si TCB

**3. Adevarat sau Fals: Integritatea kernelului nu trebuie protejata?**
- F

**4. Care sunt metodele ce pot fi folosite pentru a distruge integritatea sistemului?**
- Stepping stones
- Slabirea configuratiei
- Instalarea de binare modificate
- Modificarea kernelului

**5. Cum utilizam securitatea nativa Linux pentru a proteja calea de executie a utilizatorului root?**
- toate directoarele si programele in calea (PATH) definita pentru root sunt detinute de root si au permisiuni de scriere doar pentru root

**6. Care este sintaxa comenzii rpm pentru a verifica integritatea si autenticitatea unui pachet rpm?**
- rpm -ivh(nu-s sigur!!!!)

**7. Ce reprezinta verificarea urmelor?**
- verificarea comportamentului programelor(contextul proceselor, durata, etc.)

**8. Ce reprezinta aplicarea unui backdoor asupra /bin/login si de ce ar face acest lucru un atacator?**
- la logarea oricarui utlizator ruleaza progr /bin/login, cel care iti cere si iti verifica userul si parola
- un atacator ce foloseste un rootkit, poate inlocui login-ul original cu unul modificat astfel incat sa poata accesa sistemul cu o parola "back-door"

**9. Care sunt cele trei moduri de modificare a unui kernel?**
- instalare patchuri kerenel
- instalarea unui nou modul de kernel
- redirectarea executiei

## C8

**1. De ce majoritatea distributiilor Linux au politica predefinita de audit nula?**
- din motive de sescuritate(nu-s sigur!!!!)

**2. Cine este indicat sa configuraze fisierele de log? De ce?**
- sysadminul pt ca e responsabilitatea lui

**3. Care sunt nivelurile syslog?**
0 Emergency: system is unusable
1 Alert: action must be taken immediately
2 Critical: critical conditions
3 Error: error conditions
4 Warning: warning conditions
5 Notice: normal but significant condition
6 Informational: informational messages
7 Debug: debug-level messages

**4. Ce comanda este utilizata pentru a vedea inregistrarile din /var/log/wtmp?**
- last

**5. Adevarat sau Fals: Comenzile ac, sa, si lastcomm commands fac parte din suita de contabilizare a proceselor.**
- A

**6. Adevarat sau Fals: Police, Retention, Rotation, si Archive sunt parte din managementul fisierelor de log.**
- A

## C9

**1. What is host-based of intrusion management?**
- este un intrusion detection system ce analizeaza componentele interne ale sistemului (folosindu-se de loguri)

**2. What are the two basic types of intrusion detection systems?**

- rule-based
- adaptive

**3. TRUE or FALSE: Rootkits are used by intruders to hide and secure their presence on your system.**
- T

**4. Which are the warning signs that you know? (Write down at least two of them.)**
- lipsa fisiere
- schimbari neasteptate
- loginuri la ore ciudate

**5. What are the phases of a Incident Management Process?**
- Preparation->Detection->Containment->Eradication->Rotation->Follow Up

**6. TRUE or FALSE: Due to the dynamic kernel module of the SNARE tool, you should recompile your kernel.**
- F

## C10

**1. Care este metoda prin care putem permite/interzice accesul la o masina cu X?**
- xhost
- xAuthority

**2. Numiti trei amenintati potentiale pentru un sistem cu imprimanta?**
- pot fi interceptate informatiile ce urmeaza a fi pritnate
- furarea documentelor
- schimbari neautorizate de setari
- folosirea lor de atacatori pt a se conecta la sistem din spatele firewall-ului

**3. Numiti doua functii pe care GnuPG le poate realiza.**
- Fiecare utilizator poate sa isi controleze setarile de criptare.
- Poate fi folosit pentru semnarea e-mail-ului si a fisierelor cat si pentru criptarea datelor.
- Realizeaza transferul securizat al e-mail-ului si al fisierelor.
- Previne obtinerea datelor de interes prin interceptari.

**4. Care sunt cele mai importante doua variabile de mediu de care trebuie tinut cont in scripturile shell?**
- PATH
- IFS