Sisteme de operare avansate

10 februarie 2010

Timp de lucru: 60 de minute

Notă: Toate răspunsurile trebuie justificate

1. În ce condiții începe procesul de tainting din DSA, și când se termină?

2. Explicați ce se întâmplă în cazul apelării instrucțiunii de mai jos în contextul unui proces rulat în UML, în toate cele 4 cazuri (clasificare după pointer valid/nu, pagină în memorie/nu).

```
open(0x12345678, O_CREAT);
```

3. Care sunt avantajele folosirii unui TLB cu taguri pentru virtualizare? Explicați de ce.

4. Dați exemple concrete de tipuri de workload-uri care pot beneficia de NIC offloading, și de workload-uri care nu pot beneficia.

5. Dați un exemplu de workload în care futexurile se comportă mai bine decât mutexurile clasice și un exemplu în care se comportă similar. Este posibil ca futexurile să fie mai ineficiente decât mutexurile? În ce caz?

6. Explicați cum pot fi exploatate următoarele apeluri de sistem protejate de syscall wrappers, și ce informații ar putea să afle atacatorul:

a. `open("/path/to/some/file", ..)`

b. `rename("/path/to/source", "/path/to/destination")`

7. De ce este RCU mai eficient decât o abordare cu read/write locking?

8. Dați un exemplu de bug care poate fi prins de algoritmul MUVI (altul decât cele din paper/slide-uri).

9. Descrieți pașii prin care procesorul (x86) determină adresa unei rutine de tratare a întreruperii în mod protejat.