Grundläggande Operativsystem 1DV415 - Seminarie 4

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

5 november 2013

Introduktion

Detta seminarie behandlar följande:

1. Säkerhet

Alla svar måste motiveras.

Läshänvisningar:

- Föreläsning 8
- Operating Systems - Internals and design principles
  - Kap. 14–15
- Operativsystem - Teori och praktiskt handhavande
  - -
- Internet

Frågor

1. Varför är säkerhet och skydd viktigt även för datorer som inte innehåller hemlig eller känslig information?
2. Vad är skillnaden mellan säkerhet och skydd?
3. Tänk dig en krypteringsalgoritm som slumpmässigt ändrar ordningen på bokstäverna i ett ord. Varför skulle denna typ av algoritm vara olämplig för kryptering?
4. Vad utgör begränsningen i hur stark kryptering man kan använda?
5. Förklara skillnaden i kryptering mellan en hemlig och delad nyckel samt kryptering med publik och privat nyckel.
6. Längre och mer komplicerade lösenord innebär automatiskt bättre säkerhet. Sant eller falskt?
7. Hur fungerar saltning och hur kan det höja säkerheten när man använder lösenord?

8. Varför är det svårt för en ej behörig användare att få tillgång till ett system som använder biometrisk säkerhet?

9. Förklara en nackdel med att lagra okrypterad användarinformation på smard cards.

10. Varför är det lämpligt att låta *tickets* gå ut (bara kunna användas under en viss tid) när du använder Kerberos?

11. På vilket sätt kan arbetsstationsloginscript vara mer säkert än serverautentisieringsscript när man använder dem för single sign on?

12. Termen *subjekt* refererar alltid till en användare i systemet. Sant eller falskt?

13. Hur kan *bäst före-datum* (nycklarna går ut och blir oanvändbara efter en viss tid) på nycklar försvåra knäckandet av en kryptering?

14. Hur skiljer sig maskar från andra typer av virus?

15. Varför är det svårt att upptäcka och stoppa DoS-attacker?

16. Varför är buffer overflow-attacker farliga? Hur kan man motverka dem?

17. Nämn två sätt en attackerare kan använda för att försöka penetrera ett datorsystem.

18. Kommer en brandvägg i hemmamiljö troligen blockera all data trafik som inte uttryckligen tillåts eller tillåta all trafik som inte uttryckligen blockeras?

19. Nämn en stor nackdel med att använda och förlita sig på IDS-system (Intrusion Detection System).

20. Förklara skillnaden mellan host/dator-baserad IDS och nätverksbaserad IDS.

21. Vilken typ av scanning ger bäst skydd i ett antivirusprogram, heuristisk eller signaturbaserad?

22. Varför räcker det inte med bara åtkomstkontroll av rättigheter när man verkligen vill skydda filer och data?

23. När du ska skicka stora mängder data är det inte effektivt att bygga överföringen på privat/publik nyckel, utan man vill istället använda en delad nyckel. Hur kan man överföra denna nyckel på ett säkert sätt?

24. Varför är det viktigt att man använder en stor nyckellängd?