INSTITUTIONEN FÖR DATAVETENSKAP, FYSIK och MATEMATIK

TENTAMEN

Tentamen i: Nätverksäkerhet (1DV425)

Program: IT-tekniker

Dag och Tid: Fredag, 2012-03-23, 08.00-13.00

Antal sidor: 4 (22 uppgifter)

Tillåtna hjälpmedel: Skrivmateriel

Skrivningsansvarig lärare: Patrik Brandt

Besöker salen: Ja☐ Nej☒

LYCKA TILL!

NAMN: _____

PERSONNUMMER: _____

Betygsgränser: **3**: 32p
4: 43p
5: 52p
Max: 58p

Nätverksäkerhet, 1DV425
2012-03-23
Tentamen, 4 hp

DENNA TENTAMEN GES TILL

ITT 10

Allmänt

- Lämna in svar på separata papper.
- Uppgifterna är inte ordnade efter svårighetsgrad.
- **Skriv namn, personnummer samt sidnummer på varje blad du lämnar in.**
- **Skriv rent dina svar. Oläsliga svar rättas inte!**

1. Förklara MX-posters roll i e-postsammanhang. (1p)

2. Är det lätt eller svårt att vara anonym på Internet (motivera ditt svar)? (2p)

3. Förklara följande begrepp (4p):

a) Oavvislighet *(Non-repudiation)*
b) Autentisering *(Authentication)*
c) Auktorisation *(Authorization)*
d) Biometrisk identifiering

4. Phishing är i dagsläget ett ständigt aktuellt hot. (2p)

a) För vem utgör det ett hot och varför?
b) Beskriv ett typiskt phishing scenario.

5. Baserat på dina kunskaper om TCP/IP, beskriv hur TCP-ACK skulle kunna användas vid en portscanning och hur man skulle kunna komma fram till att en port är öppen, stängd eller blockerad med hjälp av en sådan scanning. (2p)

6. Ett program kan antingen vara statiskt eller dynamiskt länkat. Hur skiljer sig dessa åt och vilka säkerhetsproblem kan dynamiskt länkad programvara innebära? (2p)

7. Beskriv innebörden av följande begrepp. (3p)

a) Sekretess *(Confidentiality)*
b) Tillgänglighet *(Availability)*
c) Integritet *(Integrity)*

8. Inom kryptering brukar man prata om två grundläggande metoder asymmetrisk respektive symmetrisk kryptering. Beskriv utförligt de grundläggande principerna för respektive metod. (4p)

9. Hur arbetar en IDS respektive en IPS? (2p)

10. Förklara hur Greylisting i e-postsammanhang fungerar. (2p)

11. Förklara begreppen blacklist och whitelist i brandväggsammanhang och beskriv dem sedan ur ett säkerhetsperspektiv (för- och nackdelar). (4p)

12. Varför är det osäkert att låta C:\hiberfil.sys ligga kvar när man väckt datorn från hibernation? (Hiberfil.sys är filen som används vid s.k. hibernation av datorn då internminnet skrivs ner i en fil vid nedstängning av datorn och läses tillbaka när man startar datorn igen, detta för att ge en snabbare uppstart.) (2p)

13. Vilka handlingar kan en brandvägg applicera på ett paket som vill passera igenom den? Vad kan brandväggen basera sitt beslut på? (4p)

14. När och varför bör man utföra riskanalyser? (2p)

15. PGP är en mjukvara som används för att kryptera och dekryptera e-post, texter och filer. Vid kryptering använder sig PGP av något som kallas hybridkrypto.

a) Vilka krypteringsmetoder använder PGP? (3p)
b) Beskriv utförligt hur PGP använder respektive krypteringsmetod. Rita gärna. (3p)

16. Beskriv tre saker som bör tas i beaktande när man utvärderar säkerhet i trådlösa nätverket som skiljer sig mot säkerhet i trådbundna. (3p)

17. Vad krävs för att en DNS cache poisoning ska lyckas? (2p)

18. Ett e-postmeddelandes header kan förfalskas. Det är då ofta Received-delen som förfalskas. Hur upptäcker mottagande e-postserver detta? (2p)

19. En e-postserver kan vara en så kallad Open Relay, vad innebär detta? Vad innebär det för legitima användare av e-postservern? (2p)

20. Förklara och beskriv följande fenomen i förhållande till Ipsec: (4p)

a) transport mode
b) tunnel mode
c) authentication header (AH)
d) encapsulating security payload (ESP)

21. Varför är ”chain of custody” så viktig inom computer forensics? (1p)

22. Vilken typ av information kan man inte samla in efter en attack om systemet varit avstängt? (2p)