INSTITUTIONEN FÖR DATAVETENSKAP, FYSIK och MATEMATIK

TENTAMEN

Tentamen i: Nätverkssäkerhet (1DV425)

Program: IT-tekniker

Dag och Tid: Fredag, 2012-04-20, 08.00-12.00

Antal sidor: 4 (24 uppgifter)

Tillåtna hjälpmedel: Skrivmateriel

Skrivningsansvarig lärare: Patrik Brandt

Besöker salen: Ja☐ Nej☒

LYCKA TILL!

NAMN: _____

PERSONNUMMER: _____

Betygsgränser: **3**: 35 p
4: 47 p
5: 54 p
Max: 63 p

Nätverksäkerhet, 1DV425
2012-04-20
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. Vad övervakas av en HIDS? (2p)

2. Är det lätt eller svårt att hantera autentisering av användare på Internet? (motivera ditt svar) (2p)

3. Förklara följande begrepp (3p):

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

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. Vilka problem finns för att hantera UDP i brandväggar som tillämpar ”statefull packet inspection”? (2p)

6. Förklara vilka utökade rättighetsfunktioner som erhålls vid införandet av ACLer i UNIX-miljö. Vilka för- och nackdelar medför införandet av ACLer? (3p)

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. Förklara varför man saltar lösenord. (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) Beskriv utförligt hur PGP använder respektive krypteringsmetod. Rita gärna. (2p)
b) Förklara principen ”Web of trust” och hur den tillämpas i sammanhanget. (2p)

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. Beskriv de två primära typerna av VPN. (4p)

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

19. I SMTP-protokollet är det enkelt att förfalska avsändarens e-postadress. Hur gör man detta? Hur kan det motverkas? (2p)

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

21. I vilket av TCP/IP-modellens skikt bör ”sann” integritetskontroll implementeras och varför? (2p)

22. 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)

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

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