**Høgskolen i Telemark**
**Avdeling for allmenne fag**

## Sluttprøve – Vår 2009

Kurskode: **5623 Informasjonssikkerhet;**

**Kandidatnummer: ................**

Eksamensdato: **11.05.2009 (mandag)** Tid: **4 timer** Tid: **9 - 13** Eksamenssted: **Bø Idrh; Antall sider: 9**

## Merknader:

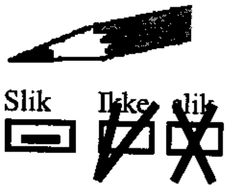
**Sluttprøve teller 100 % av totalkarakteren.**

**Hjelpemiddel: ingen**

**Eksamensresultata blir offentliggjort på Arena høgskole – da trenger du heller ikke/ikkje kandidatnummeret**

**Veiledning: Oppgavesettet består av 40 spørsmål. Alle spørsmål har 4 svaralternativer. Kun ett alternativ er riktig.** Du får **3 poeng** for riktig svar, **-1 poeng** for galt svar og **0 poeng** for spørsmål som ikke er besvart. **I tillegg kommer 3 spørsmål** som dere må skrive svar på selv. Resultatene konverteres til bokstav karakterskala.

Spørsmålene besvares ved å sette en strek i ruten for riktig svaralternativ.
Ved strek i mer enn én rute (svaralternativ), regnes spørsmålet som ubesvart.
Bruk blyant slik at du kan korrigere svarene dine!



| | A | B | C | D |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |

| | A | B | C | D |
|---|---|---|---|---|
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |
| 21 | | | | |
| 22 | | | | |
| 23 | | | | |
| 24 | | | | |

| | A | B | C | D |
|---|---|---|---|---|
| 25 | | | | |
| 26 | | | | |
| 27 | | | | |
| 28 | | | | |
| 29 | | | | |
| 30 | | | | |
| 31 | | | | |
| 32 | | | | |
| 33 | | | | |
| 34 | | | | |
| 35 | | | | |
| 36 | | | | |

| | A | B | C | D |
|---|---|---|---|---|
| 37 | | | | |
| 38 | | | | |
| 39 | | | | |
| 40 | | | | |

## Oppgavesett

### Oppgave 1

Before you can formulate a defence for a network, you will need:

A. appropriate security certifications
B. a clear picture of the dangers to be defended against
C. to read a security textbook
D. the help of an outside consulate

### Oppgave 2

When a hacking technique uses persuasion and deception to get a person to provide information to help them compromise security, this is referred to as:

A. social engineering
B. conning
C. human intelligence
D. soft hacking

### Oppgave 3

What is a sneaker?

A. a person who hacks a system without being caught
B. a person who hacks a system by faking a legitimate password
C. a person who hacks a system to test its vulnerability
D. a person who is an amateur hacker

### Oppgave 4

Which of the following is the most basic security activity?

A. authentication
B. firewalls
C. password protection
D. auditing

### Oppgave 5

The utility that gives you information about your machine's network configuration is:

A. ping
B. IPConfig
C. tracert
D. MyConfig

### Oppgave 6

When a hacker reviews a network's potential vulnerabilities, this assessment is referred to as:

A. scanning
B. assessing
C. checking
D. footprinting

**Oppgave 7**

What feature of NetCop makes it particularly useful?

- **A.** you can scan a single IP or multiple IPs.
- **B.** you can find out what ports are open.
- **C.** you can find out what operating system is running.
- **D.** you can scan multiple domains.

**Oppgave 8**

What should a system administrator do about vulnerabilities that are found on his system?

- **A.** immediately correct them
- **B.** document them.
- **C.** discuss the corrections with upper management
- **D.** change software to avoid them

**Oppgave 9**

What do you call a DoS launched from several machines simultaneously?

- **A.** Wide-area attack
- **B.** Smurf attack
- **C.** SYN flood
- **D.** DDoS attack

**Oppgave 10**

What is the most significant weakness in a DoS attack from the attacker's viewpoint?

- **A.** The attack is often unsuccessful
- **B.** The attack is difficult to execute.
- **C.** The attack is easy to stop.
- **D.** The attack must be sustained.

**Oppgave 11**

How can securing internal routers help protect against DoS attacks?

- **A.** Attacks can not occur if your internal router is secured
- **B.** Because attacks originate outside your network, securing internal routers cannot help protect you against DoS
- **C.** Securing the router will only stop router-based DoS attacks
- **D.** It will prevent an attack from propagating across network segments.

**Oppgave 12**

What can you do with your firewall to defend against DoS attacks?

- **A.** Block all incoming traffic.
- **B.** Block all incoming TCP packets.
- **C.** Block all incoming traffic on port 80.
- **D.** Block all incoming ICMP packets.

**Oppgave 13**

What is the most common way for a virus to spread?

- **A.** By copying to shared folders
- **B.** By e-mail attachments

- **C.** By FTP
- **D.** By downloading from a WEB site

**Oppgave 14**
What was the most interesting to security experts about the Mimail virus?

- **A.** It spread more rapidly than other virus attacks
- **B.** It spread in a multiple ways
- **C.** It grabbed e-mail addresses from documents on the hard drive
- **D.** It deleted critical system files.

**Oppgave 15**
A key logger is what type of malware?

- **A.** Virus.
- **B.** Buffer overflow.
- **C.** Trojan horse.
- **D.** Spyware.

**Oppgave 16**
Before shutting a service on an individual machine, which of the following would you always check?

- **A.** To determine whether you will need to shut down other services as well
- **B.** To determine whether shutting down this service will affect other services.
- **C.** To find out what this service does.
- **D.** To find out whether this service is critical to system operations.

**Oppgave 17**
Which would be most important to block end users from doing on their own machine?

- **A.** Running programs other than those installed by the IT staff.
- **B.** Surfing the Web and using chat rooms
- **C.** Changing their screen saver and using chat rooms
- **D.** Installing software or changing systems settings

**Oppgave 18**
Which of the following is a step you might take for large networks, but not for smaller networks?

- **A.** Use an IDS.
- **B.** Segment the network with firewalls between the segments.
- **C.** Use antivirus software on all machines on the network
- **D.** Do criminal background checks for network administrators.

**Oppgave 19**
Which of the following is a common way to establish security between a Web server and a network?

- **A.** Block all traffic between the Web server and the network
- **B.** Place virus scanning between the network and the Web server.
- **C.** Put a firewall between the Web server and the network.
- **D.** Do not connect your network to the Web server.

**Oppgave 20**

Which of the following methods uses a variable-length symmetric key?

- **A.** Blowfish
- **B.** Caesar
- **C.** DES.
- **D.** RSA

**Oppgave 21**

Which of the following is most likely to be true of an encryption method that sis advertised as unbreakable?

- **A.** It is probably suitable for military use
- **B.** It may be too expensive for your organization
- **C.** It is likely to be exaggerated
- **D.** It is probably one you want to use.

**Oppgave 22**

Which of the following is most true regarding new encryption methods?

- **A.** Never use them until they have been proven.
- **B.** You can use them but you must be cautious.
- **C.** Only use them if they are certified
- **D.** Only use them if they are rated unbreakable.

**Oppgave 23**

What is the greatest security risk to any company?

- **A.** Disgruntled employees.
- **B.** Hackers.
- **C.** Industrial spies.
- **D.** Faulty network security

**Oppgave 24**

What is information warfare?

- **A.** Only spreading disinformation.
- **B.** Spreading disinformation or gathering information
- **C.** Only gathering information
- **D.** Spreading disinformation or secure communications.

**Oppgave 25**

What is a major weakness with a network host-based firewall?

- **A.** Its security is dependent on the underlying operating system
- **B.** It is difficult to configure.
- **C.** It can be easily hacked.
- **D.** It is very expensive

**Oppgave 26**
Which of the following is the correct term for simply making your system less attractive to intruders?

- **A.** Intrusion deterrence.
- **B.** Intrusion deflection
- **C.** Intrusion camouflage
- **D.** Intrusion avoidance

**Oppgave 27**
In order for a DoS/DDoS attack to be effective, which of the following elements needs to be used?

- **A.** Flood of packets.
- **B.** TCP hijacking
- **C.** Deny authentication between servers
- **D.** IP spoofing

**Oppgave 28**
A Smurf IP attack is considered one of the more creative forms of DoS because:

- **A.** it acts as a virus.
- **B.** it makes the network attack itself.
- **C.** it spoofs IP addresses.
- **D.** it uses hashing.

**Oppgave 29**
Which of the following is the most common function of spyware?

- **A.** Obtain system IP addresses
- **B.** Obtain cookies
- **C.** Check for open ports
- **D.** Obtain usernames and passwords

**Oppgave 30**
Attacks on your system may be prevented or trapped through the use of:

- **A.** an intrusion-detection system.
- **B.** antivirus software.
- **C.** a network prevention system.
- **D.** a proxy filtering system.

**Oppgave 31**
Which of the following are examples of single-key encryption?

- **A.** Blowfish and PGP
- **B.** DES and RSA
- **C.** Blowfish and DES
- **D.** PGP and RSA.

**Oppgave 32**
The pump and dump scheme is:

- **A.** buying risk-free investments.

**B.** investing in offshore property.
**C.** buying worthless stock at inflated prices.
**D.** allowing someone to transfer money from his country into your bank account.

**Oppgave 33**
Defense in depth is needed to assure that which three mandatory activities are present in a security system?

**A.** Prevention, response, and prosecution
**B.** Response, collection of evidence and prosecution
**C.** Prevention, detection, and response
**D.** Prevention, response, and management

**Oppgave 34**
The three types of security controls are:

**A.** people, functions and technology.
**B.** people, process and technology.
**C.** technology, roles and separation of duties.
**D.** separation of duties, processes, and people.

**Oppgave 35**
Intrusion response is a:

**A.** preventive control.
**B.** detective control.
**C.** monitoring control.
**D.** reactive control.

**Oppgave 36**
What is the number one priority of disaster response?

**A.** Protecting hardware.
**B.** Protecting software.
**C.** Transaction processing.
**D.** Personnel safety.

**Oppgave 37**
The most extensive type of disaster recovery testing is:

**A.** checklists
**B.** full interruption
**C.** simulation
**D.** parallel testing

**Oppgave 38**
What is an audit trail?

**A.** A fitness path for quality inspectors
**B.** A sound recording of conversations taped through perimeter devices
**C.** A history of transactions indicating data that has been changed or modified.
**D.** All of the above

**Oppgave 39**
Which is the most effective means of determining how controls are functioning within an operating system?

- **A.** Interview with computer operator.
- **B.** Review of software control features and/or parameters.
- **C.** Review of operating system manual.
- **D.** Interview with product vendor

**Oppgave 40**
Which of the following is most affected by DoS?

- **A.** Confidentiality
- **B.** Integrity.
- **C.** Accountability.
- **D.** Availability.

**Oppgave 41**
Name some most important steps you will make to secure your computer (shortly in points)

**Oppgave 42**

If you have downloaded a virus or Trojan

Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames and passwords, personal numbers, etc.

In this case, what you should do (write short in points).

**Oppgave 43**
How to Identify a Scam or Fraud. Write in points (it is possible to mention at least 12 indications, but 5 points are enough).

Answers to questions 41, 42 and 43 can be written in Norwegian or English. You can choose.