Abschlussprüfung Winter 2004/05

Lösungshinweise

Fachinformatiker/Fachinformatikerin Systemintegration 1197

1 Ganzheitliche Aufgabe I Fachqualifikationen

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen - erklären - beschreiben - erläutern usw.). Wird eine bestimmte Anzahl verlangt (z. B. „Nennen Sie fünf Merkmale ..."), so ist bei Aufzählung von fünf richtigen Merkmalen die volle vorgesehene Punktzahl zu geben, auch wenn im Lösungshinweis mehr als fünf Merkmale genannt sind. Bei Angabe von Teilpunkten in den Lösungshinweisen sind diese auch für richtig erbrachte Teilleistungen zu geben.

In den Fällen, in denen vom Prüfungsteilnehmer

- keiner der sechs Handlungsschritte ausdrücklich als „nicht bearbeitet" gekennzeichnet wurde,
- der 6. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 5 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 6. Handlungsschritt soll in diesen Fällen allein wegen des Verstoßes gegen die Formvorschrift nicht erfolgen!

1. Handlungsschritt (20 Punkte)

a) 12 Punkte

Koppelelement	Einsatz	Anforderungen	Anzahl Geräte
A	EV	1. Einrichtung von VLANs (A1) 2. Erhöhung der Übertragungsrate durch „link aggregation" und Nutzung der Ersatzkabel (Einleitung) 3. Zusammenschaltung von mehreren Koppelelementen im Stack „stack-wide trunking" (Einleitung, A4)	48 Geräte 3 (48 Ports) x 16
B	GV	1. Einrichtung von VLANs (B5) 2. Erhöhung der Übertragungsrate durch „link aggregation" und Nutzung der Ersatzkabel (B3) 4. Routing zwischen VLANs/Subnetzen durch Layer 3 switching und Routing Protokoll (B1, B2, Einleitung)	1 (bis 2) Geräte

b) 8 Punkte

172.18.0.1/16 als Zugangsadresse, für 350 Hostadressen werden 9 Bit benötigt; bleiben 7 Bit für die Einrichtung von Subnetzen, $2^7 - 2 = 126$ mögliche Subnetze

2. Handlungsschritt (20 Punkte)

a) 5 Punkte

TCP ist ein verbindungsorientiertes Protokoll.
Mit dem ersten TCP-Paket wird der Verbindungsaufbau eingeleitet. Es reicht meistens aus, das erste TCP-Paket abzublocken, um eine unerwünschte TCP-Verbindung abzuweisen.
Das erste TCP-Paket ist anhand des „nicht gesetzten" Ack-Flag's immer eindeutig identifizierbar. Mit dem „nicht gesetzten" Ack-Flag lässt sich zudem die Richtung feststellen, aus der eine Verbindung aufgebaut werden soll.

UDP ist ein verbindungsloses (zustandsloses) Protokoll.
Im Gegensatz zu TCP verfügt der UDP-Header über keine Status-Flag's und damit über keinen entsprechenden Steuermechanismus.

b) 5 Punkte, 5 x 1 Punkt

Zugriff	Dienst	Portnummer
Aufrufen von Webseiten	WWW	80
Downloads von Daten	FTP Data Channel	20
	FTP Control Channel	21
Senden von E-Mails	SMTP	25
Abrufen von E-Mails	POP3	110
Domain-Name-Service	DNS	53

c) 10 Punkte

Interface: ETH0								
Regel	**Richtung**	**Quell-IP**	**Ziel-IP**	**Protokoll**	**Quell-Port**	**Ziel-Port**	**Ack-Flag**	**Aktion**
1	raus	LAN	Mail-Server	TCP	>1023	25	egal	weiterleiten
2	rein	Mail-Server	LAN	TCP	25	>1023	ja	weiterleiten
3	raus	LAN	Mail-Server	TCP	>1023	110	egal	weiterleiten
4	rein	Mail-Server	LAN	TCP	110	>1023	ja	weiterleiten
5	egal	jede	jede	jedes	jeder	jeder	egal	blockieren

3. Handlungsschritt (20 Punkte)

a) 8 Punkte

Frame 1 bis 2: Address-Resolution-Protokoll zur Ermittlung der Ziel-MAC-Adresse von 172.18.2.50

Frame 3 bis 5: Aufbau der TCP-Verbindung durch Anforderung des Netzanwendungsprotokolls telnet (Zielport 23) im 3-Wege-Handshake

Frame 6 bis 17: Aushandeln der Übertragungsparameter für das Telnet-Protokoll

Frame 18 bis 85: Datenaustausch über Netzanwendungsprotokoll Telnet

Frame 86 bis 89: Abbau der Telnet- und TCP-Verbindung (Abbau muss bereits durch ein „FIN" Flag im Frame 86 eingeleitet worden sein.)

b) 4 Punkte

Die Angabe Win steht für „Window" und dient der Flusssteuerung nach dem Fenstermechanismus. Das Feld gibt an, wie viele Bytes (hier 1024 Byte) – beginnend ab der Quittungsnummer – der Zielrechner in seinem Aufnahme-Puffer noch aufnehmen kann.

c) 2 Punkte

MAC-Adresse: 00:04:76:1c:ca:af

d) 6 Punkte

Dst-Port:
1033: Der Telnet-Client (172.18.2.115) benutzt als Quellport einen frei belegbaren Port und fordert bei der Zielinstanz die gewünschte Standardanwendung Telnet mit der Port-Angabe 23 an. Für den „Telnet-Server" ist der Port 1033 deshalb der Zielport (Dst Port).

Len: 9: Länge des TCP-Datenfeldes, hier 9 Byte (Telnet-Daten). Daten sind: „Zeilen-Anfang" - „Neue Zeile" – „Login:"

Flags: 0x0018 (PSH, ACK): Das Push-Flag bewirkt, dass die Daten sofort an die nächsthöhere Schicht weitergegeben werden. In diesem Fall wird „Login:" in einer neuen Zeile am Zeilenanfang sofort dargestellt. Das ACK-Flag zeigt eine gültige Quittungsnummer an, hier „15".

4. Handlungsschritt (20 Punkte)

aa) 2 Punkte

Level 1 und Level 5

ab) 6 Punkte

RAID Level 1 und RAID Level 5 sind fehlertolerante Festplattensysteme, die aus mehreren physikalischen Einzelfestplattenlaufwerken bestehen.

Vorteil:
Fällt ein physikalisches Festplattenlaufwerk aus, stehen alle Daten weiterhin Online zur Verfügung.

RAID-Level 1
Die Datensicherung erfolgt durch Festplattenspiegelung. Jeder Schreibvorgang erfolgt stets gleichzeitig auf zwei Festplatten.

Vorteil:
Fällt eine Festplatte aus, steht auf der zweiten Festplatte sofort eine Kopie der verlorenen Daten zur Verfügung.

Nachteile:
Durch das gleichzeitige Schreiben auf 2 Festplatten verringert sich die Schreibgeschwindigkeit.
Der Kapazitätsverlust beträgt 50 %.

RAID-Level 5
Die Datensicherung erfolgt durch „Stripe Set mit verteilter Parität". Es sind mindestens drei Festplatten erforderlich. Vom Controller werden die Daten in Blöcke zerlegt und gleichmäßig auf die physikalischen Festplatten verteilt, wobei eine physikalische Festplatte immer einen Block mit den Paritätsinformationen erhält.
Fällt eine physikalische Festplatte aus, kann der Controller anhand der Paritätsinformationen die verlorenen Daten wiederherstellen und den kompletten Daten Online zur Verfügung stellen.

Vorteile:
- Höhere Schreibgeschwindigkeit als bei RAID Level 1
- Geringerer Kapazitätsverlust als bei RAID Level 1:
  maximal 33 % bei 3 physikalischen Einzellaufwerken, bei 4 Laufwerken nur noch 25 % usw.,
  Kapazitätsverlust = 100 % / Anzahl der physikalischen Einzellaufwerke

Nachteile:
- Es sind mindesten 3 physikalische Festplattenlaufwerke erforderlich.
- Bei Ausfall einer Festplatte müssen die verlorenen Daten aufwendig rekonstruiert werden.

ba) 3 Punkte

Für das Einrichten bzw. den Aufbau einer gesicherten Verbindung zum Webserver

bb) 3 Punkte

Es ist die Zeitspanne, nach deren Ablauf der Webserver einen inaktiven Benutzer automatisch trennt.

bc) 3 Punkte

Normalerweise wird für jede http-Client-Anforderung eine neue TCP-Verbindung auf- und wieder abgebaut. Die HTTP-Keep-Alive-Funktion ermöglicht es, dass die TCP-Verbindung zum Webserver zwischen den einzelnen http-Client-Anforderungen geöffnet bleibt.

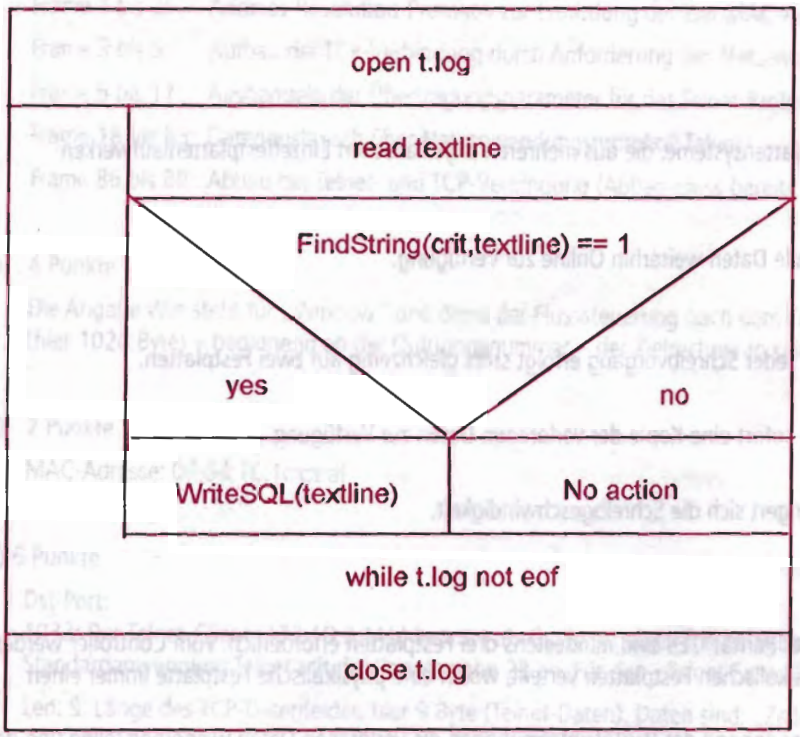
bd) 3 Punkte

Vorteil:
Bei einem stark ausgelasteten Webserver werden die Antwortzeiten für die verbundenen Nutzer verbessert.

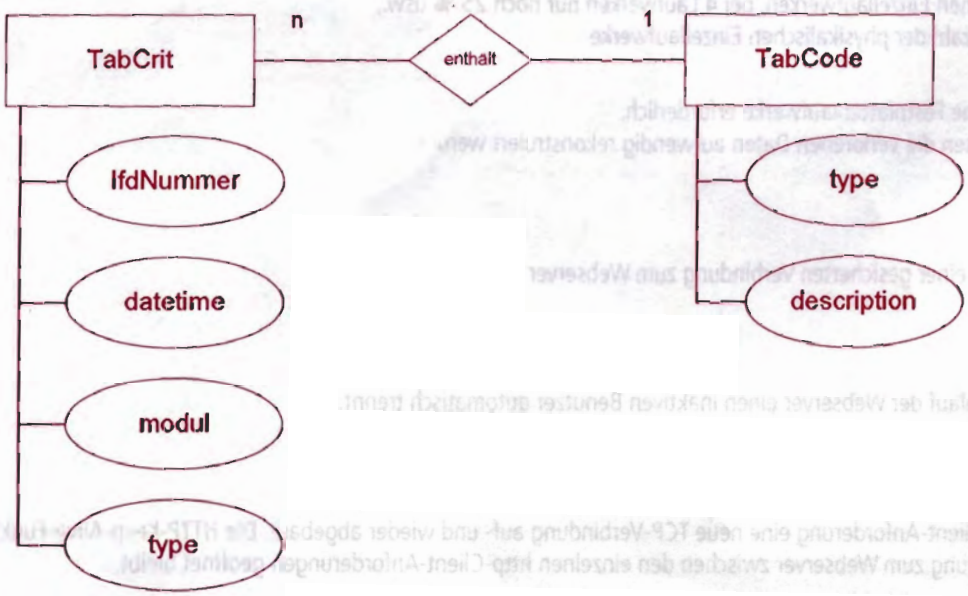
Nachteil:
Es können weniger Nutzer gleichzeitig auf die Webseite zugreifen.

5. Handlungsschritt (20 Punkte)

a) 16 Punkte



b) 4 Punkte



(Andere Darstellungsform möglich)

6. Handlungsschritt (20 Punkte)

a) 4 Punkte, 2 x 2 Punkte

Virus

Parasitäres Programmelement, das sich mit Hilfe eines Wirtsprogramms vervielfältigt

- Vermehrt sich über ein Kopierteil.
- Hat einen Auslöser und einen Schadensteil.
- Wird durch ein Ereignis (z. B. Datum) aktiviert.

Wurm

- Nistet sich in einem System ein, von dem er sich über Netzwerkverbindungen (z. B. e-Mail) verbreitet.
- Kann einen Auslöser und einen Schadensteil enthalten.

Trojanisches Pferd

- Verbreitet sich nicht aktiv, sondern wird vom Benutzer unbemerkt auf das System geholt.
- Hat keine Kopierfunktion.
- Hat keinen Auslöser; Schadensfunktion wird sofort gestartet (z. B. 0190 Dialer).

b) 6 Punkte, 3 x 2 Punkte

- Mitarbeiterschulung:
  regelmäßige Schulung der Mitarbeiter, damit sie bei Virenbefall nicht in Panik geraten; ein Mitarbeiter, der z. B. aus Panik bei einem Virenbefall die Festplatte formatiert, richtet ein größeren Schaden an als der Virus selbst.
- Pförtner-PC:
  PC ohne Netzwerk mit aktuellen Virensuchprogrammen, mit denen alle von außen kommenden Programme, Dateien, CDs u. a. auf Viren untersucht und freigegeben werden müssen
- Verwendung aktueller Virenscanner:
  regelmäßig die aktuellste Version der Virensoftware verwenden, Update-Möglichkeiten aus dem Internet nutzen
- Verwendung von Antiviren-Software verschiedener Hersteller:
  Virensuchprogramme verschiedener Hersteller unabhängig voneinander benutzen

c) 4 Punkte, 4 x 1 Punkt

- Unterstützte Plattformen
- Häufigkeit der Updates
- Handhabung der Updates
- Telefonischer Support
- Vorortsupport
- Hotlinezeiten
- Kosten
- Erkennungsrate

d) 6 Punkte, 4 x 1,5 Punkte

- Absendererkennung
- Blockierung per IP-Adresse
- Reverse DNS
- Authentifikation vor dem Versand
- Einsatz Blackhole List (Internet)
- Einsatz Whitelist (Liste mit legitimen Sendern)
- Teergrube
- Bayes-Filter