Korrekturrand

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiter/-in in der IT-Abteilung der MITTIG GmbH. Im Rahmen der Weiterentwicklung der IT-Infrastruktur sind Sie an verschiedenen Maßnahmen beteiligt.

Bearbeiten Sie vier der folgenden fünf Handlungsschritte:
1. Beschaffung und Konfiguration eines Servers
2. Einrichtung eines E-Mail Servers und des DHCP-Dienstes
3. Einrichtung und Dokumentation einer Firewall
4. Rechtevergabe an Benutzer
5. Einführung von IPv6

1. Handlungsschritt (25 Punkte)

In der MITTIG GmbH soll ein weiterer Server als Virtualisierungsplattform angeschafft werden.

Folgendes Angebot liegt vor (Ausschnitt):

Position	Anzahl	Beschreibung
1	1	Dual-Socket-Rack-Server Intel® Xeon® Prozessor E5-2600v3 128 GiByte, DDR4 ECC registered PCI-Express 3.0
2	1	LTO, 160 Mbit/s, 2,500 GiByte, SAS 6 Gbit/s
3	2	SSD SATA, 6 Gbit/s, 450 GiByte, hot-plug-fähig, 2,5 Zoll
4	6	HDD SAS, 12 Gbit/s, 800 GiByte, hot-plug-fähig, 2,5 Zoll
5	1	PRAID EP400i, RAID 5/6-Ctrl., SAS/SATA 12 Gbit/s RAID-Level: 0, 1, 10, 5, 50, 6, 60
6	2	hot-plug-Netzteil

a) Im Angebot werden die folgenden Speicher genannt.

Erläutern Sie die vier genannten Speicher in folgender Tabelle, indem Sie die Langform der Bezeichnung nennen und die Speichertechnik beschreiben. 8 Punkte

Speicher	Erläuterung
LTO	
SSD	
HDD	
DDR4	

b) Das Speichersystem des Servers soll aus zwei RAID-Verbünden bestehen.
Es stehen die Festplatten aus dem Angebot zur Verfügung.

Anforderungen:
- Der RAID-Verbund für das Betriebssystem soll Ausfallsicherheit gewährleisten.
- Der RAID-Verbund für die Datenspeicherung soll Ausfallsicherheit gewährleisten und zusätzlich größtmögliche Speicherkapazität bieten.

Geben Sie zu jedem RAID-Verbund den entsprechenden RAID-Level und die dazugehörige Netto-Speicherkapazität an.

8 Punkte

Der Rechenweg ist anzugeben.

c) Ein ECC-fähiger RAM kann Speicherfehler erkennen und korrigieren.

Nennen Sie die Speicherfehler, die erkannt werden können und die Speicherfehler, die erkannt und korrigiert werden können.

3 Punkte

d) Der Server dient als Virtualisierungsplattform für verschiedene Anwendungsserver.

Erläutern Sie drei Vorteile von virtuellen Servern gegenüber physischen Servern. 6 Punkte

Korrekturrand

Korrekturrand

2. Handlungsschritt (25 Punkte)

Der E-Mailserver der MITTIG GmbH wird virtualisiert. Im Zuge dieser Konsolidierung sollen Dienste neu konfiguriert werden.

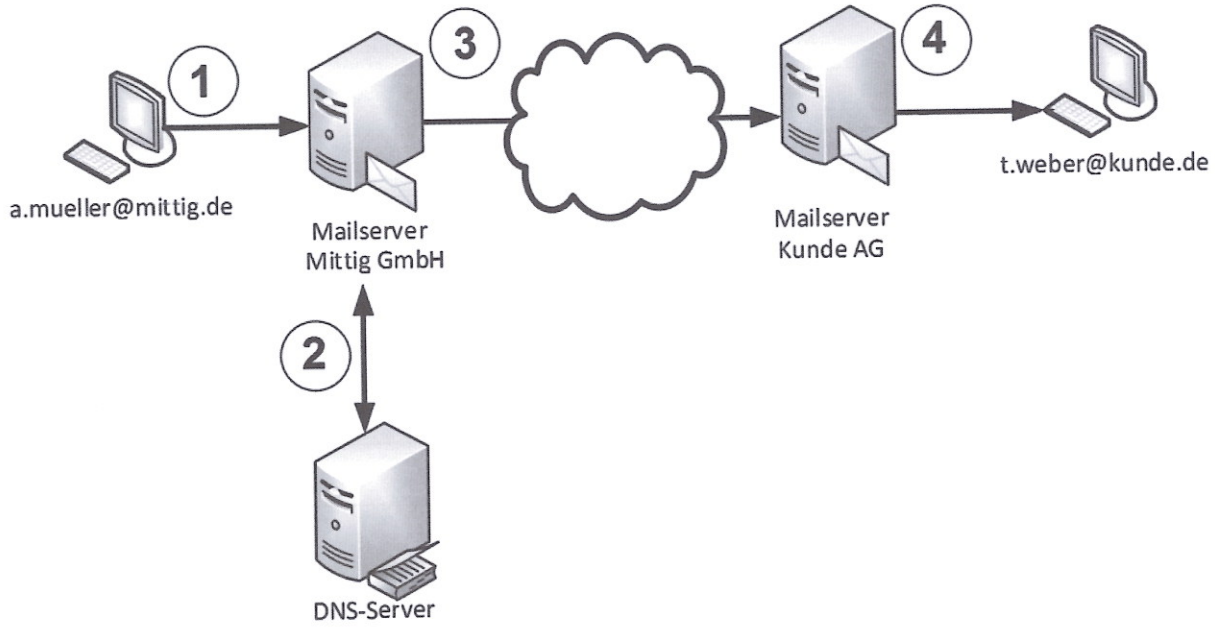
a) Der E-Mailserver soll von POP3 auf IMAP umgestellt werden.

Erläutern Sie zwei wesentliche Vorteile, die IMAP gegenüber POP3 bietet. 4 Punkte

b) Es soll sichergestellt werden, dass Benutzername und Passwort nicht im Klartext übertragen werden.

Erläutern Sie eine entsprechende Möglichkeit unter Angabe des zu verwendenden Protokolls. 4 Punkte

c) Die folgende Grafik zeigt den Versand einer E-Mail von einem Mitarbeiter der MITTIG GmbH an einen Mitarbeiter der Kunde AG.



Beschreiben Sie in folgender Tabelle die Schritte 1 bis 3 des E-Mail-Versands. 6 Punkte

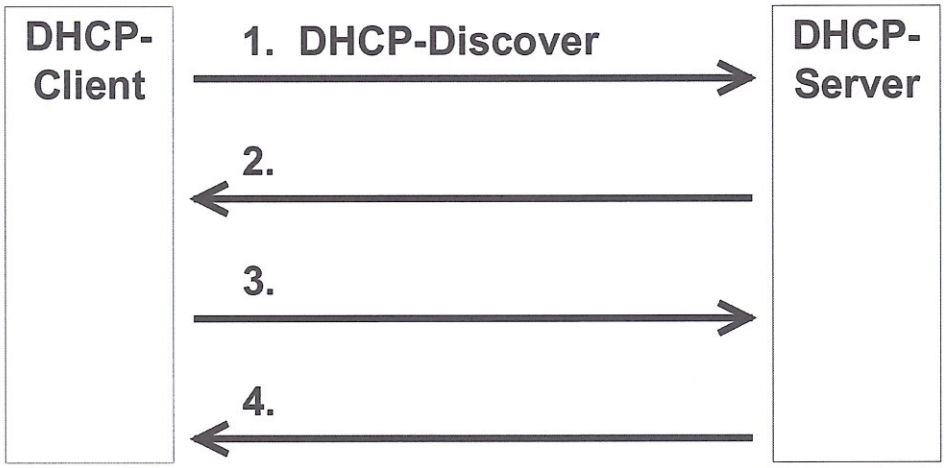
Korrekturrand

Schritt	Beschreibung
1	
2	
3	
4	Push-Nachricht wird mit MAPI vom E-Mailserver der Kunde AG an den Client des Empfängers t.weber@kunde.de übertragen

d) Im Netz der MITTIG GmbH ist ein DHCP-Server installiert.

da) Sie sollen anhand folgender Grafik den Ablauf einer Anfrage eines DHCP-Clients an den DHCP-Server darstellen.

Ergänzen Sie dazu in der Grafik die noch fehlende Beschriftung zu 2. bis 4. 3 Punkte



db) Nennen Sie drei Konfigurationsparameter, die der DHCP-Server den Clients anbietet. 3 Punkte

e) Die IT-Sicherheit im Netzwerk der MITTIG GmbH soll überwacht werden. Dies kann mit einem Honeypot realisiert werden.

Zu diesem Verfahren finden Sie folgenden Artikel.

A honeypot is a computer system that is set up to act as a decoy to lure cyberattackers, and to detect, deflect or study attempts to gain unauthorized access to information systems. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value.

Erläutern Sie die Funktionsweise eines Honeypot. 5 Punkte

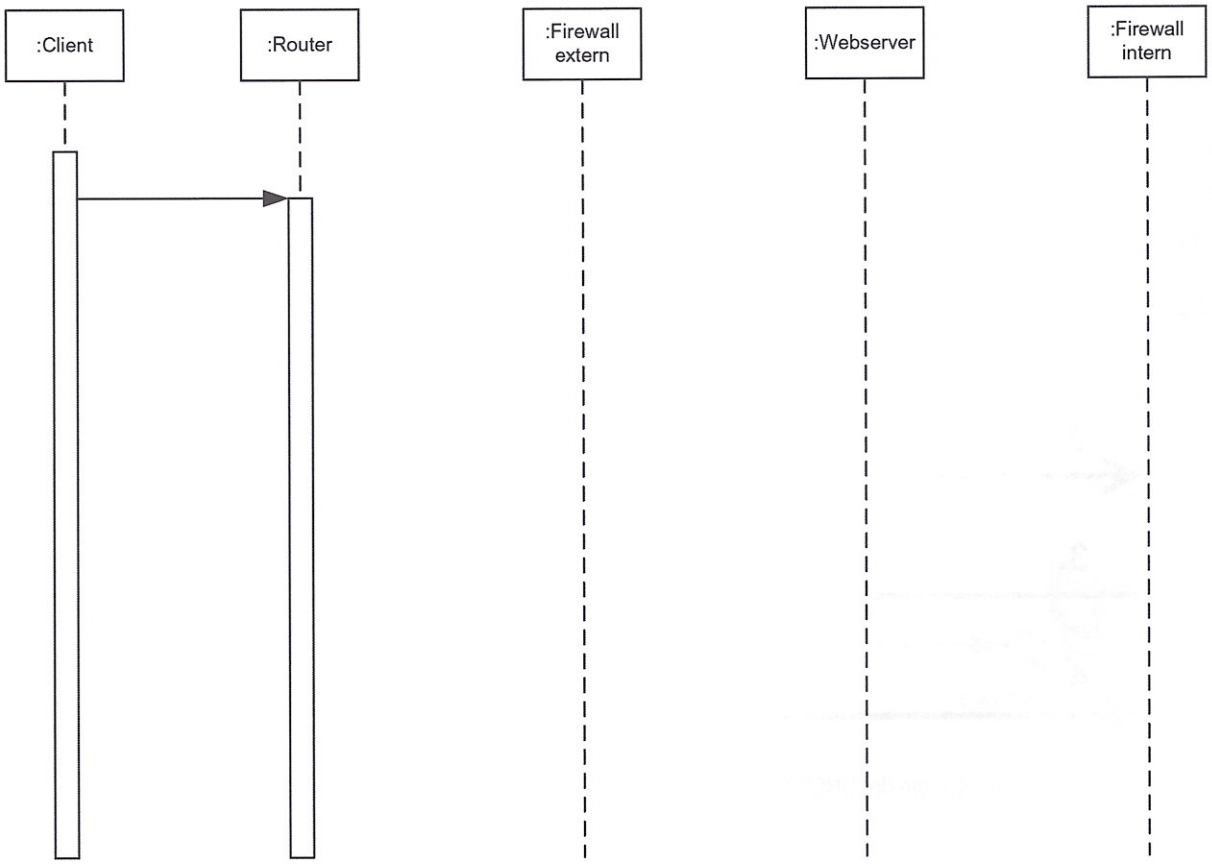
3. Handlungsschritt (25 Punkte)

Korrekturrand

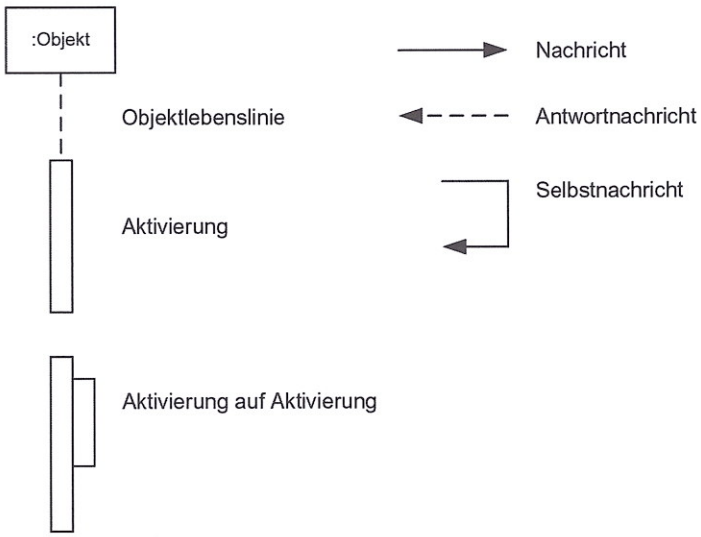
In der MITTIG GmbH wird der Webserver durch eine Firewall in einer Demilitarisierten Zone (DMZ) geschützt.

a) Ergänzen Sie das Sequenzdiagramm für eine positiv gefilterte Anfrage an den Webserver von einem externen Client. 10 Punkte

Client	Stellt Anfragen an Webserver
Router des Providers	Leitet die Anfragen an die Firewall weiter, wenn er einen Eintrag für die Zieladresse in seiner Routingtabelle findet
Firewall	Untersucht den Datenverkehr und verhindert nicht erwünschten Datenverkehr
Webserver	Nimmt Anfragen an



Notation UML-Sequenzdiagram (Auszug)



Korrekturrand

b) Durch die DMZ ist das lokale Netzwerk der MITTIG GmbH gegenüber Angriffen aus dem Internet besser geschützt.

Beschreiben Sie die organisatorische Maßnahme, die diesen Schutz bewirkt. 3 Punkte

c) Für die externe Firewall der MITTIG GmbH wurden folgende Regeln aufgestellt:

Regel-Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Interface	Richtung
1	Permit	TCP	ANY	Webserver der MITTIG GmbH	>1023	80	Internet	IN
2	Permit	TCP	ANY	Webserver der MITTIG GmbH	>1023	443	Internet	IN
...								
99	Deny	IP	ANY	ANY	-	-	Internet	IN

Erläutern Sie die Regeln 1, 2 und 99. 6 Punkte

Regel-Nr.	Erläuterung
1	
2	
99	

d) Eine Stateful Packet Inspection Firewall (SPI-Firewall) hat gegenüber einem reinen Paketfilter weitere Sicherheitsmerkmale.

Nennen Sie die Bezeichnung eines Feldes im TCP-Header, welches nur von der SPI-Firewall analysiert wird. 2 Punkte

e) In der MITTIG GmbH wird diskutiert, einen HTTP Proxy einzusetzen.

Erläutern Sie eine grundsätzliche Funktion eines HTTP Proxy. 4 Punkte

4. Handlungsschritt (25 Punkte)

Korrekturrand

Sie sollen für das lokale Netzwerk der MITTIG GmbH folgende Aufgaben erledigen:
- Zugriffsrechte für den Ordner *Intern* ermitteln und festlegen
- Eine neue Passwortrichtlinie implementieren

a) Die Beschäftigten der Mittig GmbH sind sechs Benutzergruppen zugeordnet. Die folgende Tabelle zeigt die Benutzergruppen und deren Mitglieder:

Benutzergruppen

	Bezeichnung	Personal-Nummern der Mitglieder	Beschreibung
1.	Angestellte	FM1 bis FM99	Festangestellte Mitarbeiter
2.	Azubis	A1 bis A19	Mitarbeiter, die eine Ausbildung absolvieren
3.	Praktikanten	P1 bis P19	Mitarbeiter, die ein Praktikum absolvieren
4.	OrdnerAdmins	FM15, FM25, FM35	Administratoren, welche die Ordnerberechtigungen verwalten
5.	ITAdmins	FM10, FM19, FM29	IT-Administratoren
6.	Befristete	A1 bis A19, P1 bis P19	Befristete Mitarbeiter = alle Mitarbeiter die eine Ausbildung oder ein Praktikum absolvieren

Das Betriebssystem unterstützt die folgenden Datei- und Ordnerberechtigungen:

Permission	Action
Read	Read the file and view its attributes, ownership, and permissions set.
Write	Overwrite the file, change its attributes, view its ownership, and view the permissions set.
Read & Execute	Run and execute the application. In addition, the user can perform all duties allowed by the Read permission.
Modify	Modify and delete a file including perform all of the actions permitted by the Read, Write, and Read and Execute file permissions.
Full Control	Change the permission set on a file, take ownership of the file, and perform actions permitted by all of the other file permissions.

Für den Ordner *Intern* wurden die folgenden Berechtigungen vergeben, die auch für die darin gespeicherten Dateien gelten.

Benutzergruppe	Vollzugriff	Ändern	Schreiben	Lesen
Angestellte			X	X
Befristete				X
OrdnerAdmins		X		
ITAdmins	X			

Die folgenden Aufgaben beziehen sich auf den Ordner *Intern*, in dem Textdateien, aber auch ausführbare Programmdateien gespeichert sind.

aa) Nennen Sie die Benutzergruppen, die berechtigt sind, Dateien zu löschen. 4 Punkte

ab) Ermitteln Sie die Aktionen, zu der Mitarbeiter FA44 berechtigt ist. 5 Punkte

ac) Ermitteln Sie die Aktionen, zu denen der Praktikant P10 berechtigt ist. 5 Punkte

Korrekturrand

ad) Einem Benutzer können mit dem Kommandozeilenbefehl *adacl* Berechtigungen gewährt oder entzogen werden. Syntax:

adacl [/Pfad] [/Aktion] [/Benutzer oder Benutzergruppe] [/Berechtigung]

adacl	Befehlsname
Pfad	Dateiname oder Ordnername
Aktion	grant = Gewähren von Berechtigungen revoke = Entziehen von Berechtigungen
Benutzer	Name des Benutzers oder der Benutzergruppe
Berechtigung	F = Vollzugriff M = Ändern W = Schreiben RX = Lesen und Ausführen R = Lesen N = Kein Zugriff

Mitarbeiter FM25 soll die Berechtigung zum Lesen und Ausführen von Dateien im Ordner „d:\Intern" erhalten.

Erstellen Sie die entsprechende Anweisung. 3 Punkte

b) Sie arbeiten an der Umsetzung einer neuen Passwort-Richtlinie mit.

Demnach muss jedes Passwort drei der folgenden vier Bedingungen erfüllen:
- Enthält mindestens vier Großbuchstaben (GrBu)
- Enthält mindestens drei Kleinbuchstaben (KlBu)
- Enthält mindestens zwei Sonderzeichen (SoZe)
- Enthält mindestens eine Ziffer (Ziff)

Erstellen Sie eine if-Anweisung, mit der überprüft werden kann, ob ein Passwort der Richtlinie entspricht. 8 Punkte

Hinweis:

Verwenden Sie dazu
- die logischen Variablen GrBu, KlBu, SoZe und Ziff, (true, wenn Bedingung erfüllt ist),
- die logischen Operatoren,
- die Syntax der if-Anweisung.

Variablen, Typ *bool*

GrBu
KlBu
SoZe
Ziff

Logische Operatoren

||	für logisch ODER
&&	für logisch UND

Syntax der if-Anweisung

if (logische Bedingung) { … } else { ….} ;

5. Handlungsschritt (25 Punkte)

Korrekturrand

Die MITTIG GmbH möchte ihr Netzwerk für IPv6 vorbereiten. Sie sollen bei der Vorbereitung mitwirken.

a) In einem Handbuch zu IPv6 werden folgende Fachbegriffe erläutert.

Geben Sie die Erläuterungen jeweils sinngemäß in Deutsch wieder.

aa) *Link Local Address (FE80::/10)* This address is found on each IPv6 interface after stateless auto-configuration. Packets using link-local addressing will never pass a router. 2 Punkte

ab) *Unique Local Unicast (FC00::/7)* An identifier for a network or host. Can be used to build a private network, like the private network address space (10.x.x.x) in IPv4. 2 Punkte

ac) *Global Unicast Address (2000::/3)* This address is the analogue of the normal IPv4 Addresses. Identifies a unique interface. 2 Punkte

ad) *IPv6 Neighbor Discovery* replaces the address resolution protocol (ARP) in IPv4. For example the Neighbor Discovery Protocol is responsible for stateless auto-configuration, duplicate address detection and finds the link layer address of another node. Using multicast, Neighbor Discovery Protocol avoids broadcasts. 3 Punkte

b) Ermitteln Sie die letzte /64 Netzwerk-ID des Adressbereiches der Unique Local Unicast Adressen. 4 Punkte

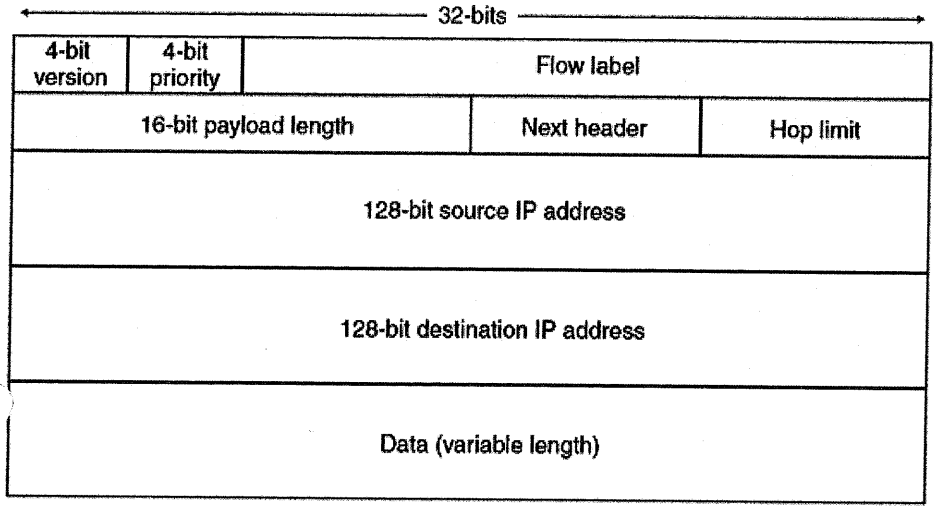
c) In einem IPv6-Testnetzwerk mit dem Präfix /32 wurde der Datenverkehr mithilfe eines Protokollanalysators aufgezeichnet.

Korrekturrand

Trace

```
60 00 00 00 00 40 3A 40 FC 00 01 01 00 00 00 00
00 00 AF C1 00 B8 00 51 FC 00 00 03 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

IPv6-Header



ca) Ermitteln Sie die IPv6-Senderadresse. 3 Punkte

cb) Ermitteln Sie die IPv6-Empfängeradresse. 3 Punkte

d) Sie sollen einen weiteren Rechner manuell konfigurieren. Dieser soll mit dem Rechner im Testnetzwerk (siehe Trace) kommunizieren können. Der Standardgateway hat die erste mögliche Adresse im Netzwerk.

da) Ermitteln Sie eine mögliche IPv6-Adresse für den Rechner. 3 Punkte

db) Ermitteln Sie die IPv6-Adresse für den Standardgateway. 3 Punkte

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

[1] Sie hätte kürzer sein können. [2] Sie war angemessen. [3] Sie hätte länger sein müssen. ☐