20.1 Trainer – Grundlagen und OSI-Modell

Diese Trainer-Seite wiederholt die Grundlagen der Netzwerktechnik, das OSI-Modell, das TCP/IP-Modell und die wichtigsten Begriffe zur Kommunikation im Netzwerk.

Ziel ist nicht nur Auswendiglernen, sondern sicheres Zuordnen in typischen IHK-Aufgaben.

Merksatz:

> OSI ist das Denkmodell.
> TCP/IP ist das Praxismodell.
> Die Fehlersuche erfolgt systematisch nach Schichten.

Lernziele

Nach dieser Seite solltest du sicher können:

- die sieben OSI-Schichten nennen
- OSI und TCP/IP unterscheiden
- Protokolle passenden Schichten zuordnen
- MAC-Adresse,
  IP-Adresse
  und Port unterscheiden
- Kapselung erklären
- typische Fehlerbilder einer Schicht zuordnen
- Prüfungsfragen kurz und fachlich beantworten

Kurzüberblick: OSI-Modell

Schicht	Name	Hauptaufgabe
7	Anwendungsschicht	Dienste für Anwendungen
6	Darstellungsschicht	Datenformat, Codierung, Verschlüsselung
5	Sitzungsschicht	Sitzungen verwalten
4	Transportschicht	Ende-zu-Ende-Kommunikation, Ports
3	Vermittlungsschicht	IP-Adressierung und Routing
2	Sicherungsschicht	lokale Kommunikation über MAC-Adressen

Schicht	Name	Hauptaufgabe
1	Bitübertragungsschicht	Bits als Signale übertragen

Merksatz:

> Von unten nach oben:
> Signal,
> Frame,
> Paket,
> Segment,
> Sitzung,
> Darstellung,
> Anwendung.

Kurzüberblick: TCP/IP-Modell

TCP/IP-Schicht	Entspricht grob OSI	Beispiele
Anwendung	OSI 5 bis 7	HTTP, DNS, DHCP, SMTP
Transport	OSI 4	TCP, UDP
Internet	OSI 3	IP, ICMP
Netzzugang	OSI 1 bis 2	Ethernet, WLAN, MAC

Merksatz:

> TCP/IP fasst OSI-Schichten zusammen.

Aufgabe 1

Ordne die Begriffe der passenden OSI-Schicht zu:

Begriff	OSI-Schicht
MAC-Adresse	?
IP-Adresse	?
Portnummer	?
DNS	?
Kabel	?

Antwort anzeigen

Begriff	OSI-Schicht
MAC-Adresse	Schicht 2
IP-Adresse	Schicht 3
Portnummer	Schicht 4
DNS	Schicht 7
Kabel	Schicht 1

Merksatz:

MAC = lokal.
IP = logisch.
Port = Dienst.
DNS = Anwendung.
Kabel = Signal.

Aufgabe 2

Welche Aussage ist richtig?

A: Ein Switch arbeitet hauptsächlich mit IP-Adressen.

B: Ein Router arbeitet hauptsächlich mit MAC-Adressen.

C: Ein Switch arbeitet hauptsächlich mit MAC-Adressen.

D: DNS gehört zur Bitübertragungsschicht.

Antwort anzeigen

Richtig ist:

C: Ein Switch arbeitet hauptsächlich mit MAC-Adressen.

Begründung:

Ein Switch arbeitet hauptsächlich auf OSI-Schicht 2
und leitet Ethernet-Frames anhand von MAC-Adressen weiter.

Aufgabe 3

Welche Aussage beschreibt das TCP/IP-Modell am besten?

A: Es hat immer genau sieben Schichten.

B: Es ist ein praxisnahes Modell für reale Netzwerkkommunikation.

C: Es ersetzt IP-Adressen durch MAC-Adressen.

D: Es wird nur für WLAN verwendet.

Antwort anzeigen

Richtig ist:

B: Es ist ein praxisnahes Modell für reale Netzwerkkommunikation.

Begründung:

Das OSI-Modell ist ein theoretisches Referenzmodell mit sieben Schichten.
Das TCP/IP-Modell ist praxisnäher und wird zur Beschreibung realer Internetkommunikation genutzt.

Aufgabe 4

Ordne die TCP/IP-Schichten den OSI-Schichten zu.

TCP/IP-Schicht	OSI-Schichten
Anwendung	?
Transport	?

TCP/IP-Schicht	OSI-Schichten
Internet	?
Netzzugang	?

Antwort anzeigen

TCP/IP-Schicht	OSI-Schichten
Anwendung	OSI 5 bis 7
Transport	OSI 4
Internet	OSI 3
Netzzugang	OSI 1 bis 2

Merksatz:

TCP/IP-Anwendung umfasst OSI-Sitzung,
Darstellung
und Anwendung.

Aufgabe 5

Ein Benutzer kann einen Server per IP-Adresse erreichen, aber nicht per Namen.

Welches Thema ist am wahrscheinlichsten betroffen?

Antwort anzeigen

Wahrscheinlich betroffen:

DNS

Begründung:

Wenn die IP-Adresse erreichbar ist,
aber der Name nicht funktioniert,
ist die Grundverbindung wahrscheinlich vorhanden.
Das Problem liegt wahrscheinlich bei der Namensauflösung.

IHK-sichere Antwort:

```
Da die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird,
sollte DNS geprüft werden.
```

Aufgabe 6

Ein Client hat die Adresse:

```
169.254.12.34
```

Was bedeutet das typischerweise?

Antwort anzeigen

Das ist eine APIPA-Adresse.

Bedeutung:

```
Der Client hat wahrscheinlich keine gültige IP-Adresse von einem DHCP-Server erhalten.
```

Typische Ursachen:

```
DHCP-Server nicht erreichbar
falsches VLAN
DHCP-Scope erschöpft
DHCP-Relay fehlt
Netzwerkverbindung fehlerhaft
```

Merksatz:

```
169.254.x.x deutet auf DHCP-Problem hin.
```

Aufgabe 7

Ein Client erreicht Geräte im eigenen Netz, aber keine Ziele im Internet.

Was sollte zuerst geprüft werden?

Antwort anzeigen

Zuerst prüfen:

```
Standardgateway
```

Weitere mögliche Ursachen:

```
Routing
NAT
Firewall
DNS bei Zugriff über Namen
```

Begründung:

```
Wenn lokale Kommunikation funktioniert,
aber externe Netze nicht erreichbar sind,
fehlt häufig der Weg aus dem eigenen Netz.
```

Merksatz:

```
Lokal ja,
extern nein:
Gateway prüfen.
```

Aufgabe 8

Was bedeutet Kapselung?

Antwort anzeigen

Kapselung bedeutet:

Beim Senden werden Daten von Schicht zu Schicht weitergegeben
und jede Schicht ergänzt eigene Steuerinformationen.

Beispiel:

Anwendungsdaten
werden zu TCP-Segmenten,
IP-Paketen,
Ethernet-Frames
und schließlich Bits.

IHK-sichere Kurzformulierung:

Kapselung beschreibt das Verpacken von Daten durch die einzelnen Netzwerkschichten.
Jede Schicht ergänzt eigene Informationen,
die für die Kommunikation auf dieser Schicht benötigt werden.

Aufgabe 9

Bringe die PDU-Begriffe in die richtige Reihenfolge von oben nach unten.

Bits

Paket

Daten

Frame

Segment

Antwort anzeigen

Richtige Reihenfolge von oben nach unten:

Daten

Segment

Paket

Frame

Bits

Zuordnung:

Schicht	PDU
Anwendung	Daten
Transport	Segment oder Datagramm
Vermittlung	Paket
Sicherung	Frame
Bitübertragung	Bits

Aufgabe 10

Welche OSI-Schicht ist betroffen, wenn ein Netzwerkkabel defekt ist?

Antwort anzeigen

Betroffen ist:

OSI-Schicht 1

Begründung:

Ein defektes Kabel betrifft die physische Signalübertragung.

Merksatz:

Kabel,
Stecker,
Funk
und Signal gehören zu Schicht 1.

Aufgabe 11

Welche OSI-Schicht ist betroffen, wenn ein Gerät im falschen VLAN ist?

Antwort anzeigen

Betroffen ist hauptsächlich:

OSI-Schicht 2

Begründung:

VLANs trennen Netzbereiche auf Layer 2.
Ein falsches VLAN kann dazu führen,
dass ein Gerät im falschen Broadcast-Bereich landet
oder eine falsche IP-Konfiguration erhält.

Aufgabe 12

Welche OSI-Schicht ist betroffen, wenn die Subnetzmaske falsch ist?

Antwort anzeigen

Betroffen ist:

OSI-Schicht 3

Begründung:

IP-Adresse,
Subnetzmaske,
Gateway
und Routing gehören zur Vermittlungsschicht.

Merksatz:

IP-Konfiguration ist Schicht 3.

Aufgabe 13

Welche OSI-Schicht ist betroffen, wenn TCP 443 durch eine Firewall blockiert wird?

Antwort anzeigen

Betroffen ist mindestens:

OSI-Schicht 4

Begründung:

TCP und Ports gehören zur Transportschicht.
TCP 443 ist der typische Port für HTTPS.

Wichtig:

Eine Firewall kann je nach Funktion auch auf mehreren Schichten arbeiten.

Aufgabe 14

Welche OSI-Schicht ist betroffen, wenn ein TLS-Zertifikat abgelaufen ist?

Antwort anzeigen

Betroffen ist hauptsächlich:

```
OSI-Schicht 6
```

Begründung:

```
TLS,
Zertifikate
Verschlüsselung
und Darstellung gehören zur Darstellungsschicht.
```

Merksatz:

```
Zertifikatsfehler:
Schicht 6.
```

Aufgabe 15

Welche OSI-Schicht ist betroffen, wenn ein Webserver HTTP 500 zurückgibt?

Antwort anzeigen

Betroffen ist hauptsächlich:

```
OSI-Schicht 7
```

Begründung:

```
HTTP ist ein Anwendungsprotokoll.
Ein HTTP-500-Fehler deutet auf einen serverseitigen Anwendungsfehler hin.
```

Merksatz:

```
HTTP-Statuscodes gehören zur Anwendungsschicht.
```

Aufgabe 16

Welche Aussage zu ping ist richtig?

A: ping prüft immer,
ob eine Webseite funktioniert.

B: ping prüft ICMP-Erreichbarkeit.

C: ping prüft,
ob TCP 443 offen ist.

D: ping ersetzt einen DNS-Test.

Antwort anzeigen

Richtig ist:

B: ping prüft ICMP-Erreichbarkeit.

Begründung:

ping nutzt ICMP.
Ein erfolgreicher ping bedeutet nicht automatisch,
dass ein bestimmter Dienst wie HTTPS,
SSH
oder SMB funktioniert.

Merksatz:

ping ist kein Diensttest.

Aufgabe 17

Was ist der Unterschied zwischen Authentifizierung und Autorisierung?

Antwort anzeigen

Authentifizierung:

```
Prüfung der Identität.
```

Beispiel:

```
Benutzer meldet sich mit Passwort und MFA an.
```

Autorisierung:

```
Prüfung der Berechtigung.
```

Beispiel:

```
Benutzer darf eine Datei lesen oder nicht.
```

Merksatz:

```
Authentifizierung:
Wer bist du?

Autorisierung:
Was darfst du?
```

Aufgabe 18

Ein Benutzer kann sich anmelden, aber nicht auf eine Datei zugreifen.

Was ist wahrscheinlicher: Authentifizierungsproblem oder Autorisierungsproblem?

Antwort anzeigen

Wahrscheinlicher ist:

Autorisierungsproblem

Begründung:

Die Anmeldung funktioniert bereits.
Das Problem liegt daher wahrscheinlich bei Berechtigungen,
Gruppen,
ACLs,
Freigaberechten
oder Dateisystemrechten.

Merksatz:

Login ja,
Zugriff nein:
Rechte prüfen.

Aufgabe 19

Was ist der Unterschied zwischen TCP und UDP?

Antwort anzeigen

TCP:

verbindungsorientiert
zuverlässig
bestätigt Daten
stellt Reihenfolge sicher
mehr Overhead

UDP:

verbindungslos
schneller

weniger Overhead

keine eingebaute Zustellgarantie

Beispiele:

TCP	UDP
HTTPS	DNS
SSH	DHCP
SMTP	VoIP
SMB	NTP

Merksatz:

TCP = zuverlässig.

UDP = schnell und schlank.

Aufgabe 20

Was macht ARP?

Antwort anzeigen

ARP steht für:

Address Resolution Protocol

Aufgabe:

ARP löst im lokalen IPv4-Netz eine IP-Adresse in eine MAC-Adresse auf.

Beispiel:

Ein Client möchte sein Gateway erreichen.

Dafür benötigt er die MAC-Adresse des Gateways.

Diese ermittelt er mit ARP.

Merksatz:

```
ARP findet MAC-Adressen im lokalen IPv4-Netz.
```

Aufgabe 21

Ein Host möchte ein Ziel außerhalb des eigenen Subnetzes erreichen.

Welche MAC-Adresse wird im lokalen Ethernet-Frame verwendet?

Antwort anzeigen

Verwendet wird:

```
die MAC-Adresse des Standardgateways
```

Begründung:

```
Das IP-Ziel bleibt der entfernte Zielhost.
Aber lokal wird das Frame an den nächsten Hop gesendet,
also an das Gateway.
```

Merksatz:

```
IP zeigt zum Endziel.
MAC zeigt zum nächsten lokalen Hop.
```

Aufgabe 22

Was ist der Unterschied zwischen Switch und Router?

Antwort anzeigen

Switch:

arbeitet hauptsächlich auf Schicht 2
leitet Frames anhand von MAC-Adressen weiter
verbindet Geräte im lokalen Netz

Router:

arbeitet auf Schicht 3
leitet Pakete anhand von IP-Adressen weiter
verbindet unterschiedliche IP-Netze

Merksatz:

Switch verbindet lokal.
Router verbindet Netze.

Aufgabe 23

Was ist der Unterschied zwischen VLAN und Subnetz?

Antwort anzeigen

VLAN:

logische Trennung auf Schicht 2

Subnetz:

logische IP-Aufteilung auf Schicht 3

Wichtig:

In der Praxis wird einem VLAN häufig ein eigenes IP-Subnetz zugeordnet.
Fachlich sind VLAN und Subnetz aber nicht dasselbe.

Merksatz:

```
VLAN = Layer 2.
Subnetz = Layer 3.
```

Aufgabe 24

Warum braucht man Inter-VLAN-Routing?

Antwort anzeigen

VLANs sind voneinander getrennte Layer-2-Bereiche.

Damit Geräte aus unterschiedlichen VLANs miteinander kommunizieren können, braucht man Routing zwischen diesen Netzen.

Das nennt man:

```
Inter-VLAN-Routing
```

Möglich über:

```
Router
Layer-3-Switch
Firewall
```

Merksatz:

```
VLANs trennen.
Routing verbindet gezielt.
```

Aufgabe 25

Was ist der Unterschied zwischen NAT und Firewall?

Antwort anzeigen

NAT:

übersetzt IP-Adressen

Firewall:

erlaubt oder blockiert Verkehr anhand von Regeln

Wichtig:

Viele Geräte kombinieren NAT und Firewall.
Fachlich bleiben es unterschiedliche Funktionen.

Merksatz:

NAT übersetzt.
Firewall filtert.

Aufgabe 26

Was ist PAT?

Antwort anzeigen

PAT steht für:

Port Address Translation

PAT ist eine Form von NAT, bei der zusätzlich Ports genutzt werden, um viele interne Verbindungen über eine öffentliche IP-Adresse zu unterscheiden.

Merksatz:

PAT nutzt Ports zur Zuordnung mehrerer Verbindungen.

Aufgabe 27

Warum ist eine Any-to-Any-Firewall-Regel kritisch?

Antwort anzeigen

Any-to-Any ist kritisch, weil dadurch jede Quelle zu jedem Ziel kommunizieren darf.

Risiken:

```
große Angriffsfläche
schlechte Nachvollziehbarkeit
Umgehung von Sicherheitszonen
unnötige Freigaben
```

Besser:

```
genaue Regeln mit Quelle,
Ziel,
Port,
Protokoll
und Zweck.
```

Merksatz:

```
Firewall-Regeln so genau wie möglich formulieren.
```

Aufgabe 28

Was bedeutet Default Deny?

Antwort anzeigen

Default Deny bedeutet:

```
Standardmäßig ist Verkehr verboten.
```

Nur ausdrücklich erlaubter Verkehr wird zugelassen.

Vorteil:

bessere Kontrolle
kleinere Angriffsfläche
weniger ungewollte Freigaben

Merksatz:

Erst blockieren,
dann gezielt erlauben.

Aufgabe 29

Was ist der Unterschied zwischen RPO und RTO?

Antwort anzeigen

RPO:

Recovery Point Objective

maximal akzeptabler Datenverlust

RTO:

Recovery Time Objective

maximal akzeptable Wiederherstellungszeit

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Aufgabe 30

Warum ersetzt ein Snapshot kein Backup?

Antwort anzeigen

Ein Snapshot ersetzt kein Backup, weil er oft auf demselben Speicher oder System liegt wie die Produktivdaten.

Risiken:

Speicherdefekt betrifft Snapshot ebenfalls
Ransomware kann Snapshot erreichen
Snapshot kann gelöscht werden
Speicherplatz kann volllaufen

Merksatz:

Snapshot ist Momentaufnahme,
aber kein vollständiges Backup-Konzept.

Aufgabe 31

Ordne die Angriffe dem passenden Schutzziel zu.

Angriff	Schutzziel
DDoS	?
Datenabfluss	?
Manipulation einer Konfigurationsdatei	?
Ransomware	?

Antwort anzeigen

Angriff	Schutzziel
DDoS	Verfügbarkeit
Datenabfluss	Vertraulichkeit
Manipulation einer Konfigurationsdatei	Integrität
Ransomware	Verfügbarkeit, bei Datenabfluss auch Vertraulichkeit

Merksatz:

```
Erst Schutzziel erkennen,
dann Maßnahme auswählen.
```

Aufgabe 32

Was ist der Unterschied zwischen IDS und IPS?

Antwort anzeigen

IDS:

```
Intrusion Detection System

erkennt und meldet Angriffe
```

IPS:

```
Intrusion Prevention System

erkennt und blockiert Angriffe zusätzlich
```

Merksatz:

```
IDS meldet.
IPS blockiert.
```

Aufgabe 33

Was bedeutet Least Privilege?

Antwort anzeigen

Least Privilege bedeutet:

```
Benutzer,
Dienste
und Prozesse erhalten nur die Rechte,
die sie für ihre Aufgabe wirklich benötigen.
```

Ziel:

```
Schaden bei Fehlern oder Angriffen begrenzen.
```

Merksatz:

```
So wenig Rechte wie möglich,
so viele wie nötig.
```

Aufgabe 34

Was bedeutet MFA?

Antwort anzeigen

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

Dabei werden mehrere Faktoren kombiniert.

Beispiele:

```
Wissen:
Passwort

Besitz:
Smartphone,
Token,
Smartcard
```

Sein:
biometrisches Merkmal

Merksatz:

MFA sorgt dafür,
dass ein Passwort allein nicht reicht.

Aufgabe 35

Was ist der Unterschied zwischen Brute Force, Password Spraying und Credential Stuffing?

Antwort anzeigen

Brute Force:

viele Passwortversuche gegen ein Konto oder Ziel

Password Spraying:

ein häufiges Passwort gegen viele Konten

Credential Stuffing:

bereits geleakte Zugangsdaten werden bei anderen Diensten getestet

Merksatz:

Brute Force:
viele Versuche.

Password Spraying:
ein Passwort,
viele Konten.

Credential Stuffing:
geleakte Zugangsdaten.

Aufgabe 36

Was bedeutet Hardening?

Antwort anzeigen

Hardening bedeutet:

ein System sicherer zu konfigurieren,
indem unnötige Funktionen deaktiviert
und Angriffsflächen reduziert werden.

Beispiele:

unnötige Dienste deaktivieren
Standardpasswörter ändern
unsichere Protokolle abschalten
Rechte begrenzen
Logging aktivieren
Updates einspielen

Merksatz:

Hardening verringert die Angriffsfläche.

Aufgabe 37

Was ist der Unterschied zwischen IaaS, PaaS und SaaS?

Antwort anzeigen

IaaS:

Infrastructure as a Service

virtuelle Infrastruktur,
zum Beispiel virtuelle Maschinen,
Netzwerk
und Speicher

PaaS:

Platform as a Service

verwaltete Plattform für Anwendungen

SaaS:

Software as a Service

fertige Anwendung aus der Cloud

Merksatz:

IaaS = Infrastruktur.
PaaS = Plattform.
SaaS = Software.

Aufgabe 38

Was bedeutet Shared Responsibility in der Cloud?

Antwort anzeigen

Shared Responsibility bedeutet:

Cloud-Anbieter und Kunde teilen sich die Verantwortung.

Typisch:

Anbieter schützt die Cloud-Infrastruktur.

Kunde schützt Daten,
Identitäten,
Zugriffsrechte,
Konfigurationen
und Anwendungen je nach Modell.

Merksatz:

Cloud bedeutet geteilte Verantwortung.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Ein Client erreicht die Webseite per IP-Adresse,
aber nicht per Namen.
Nennen Sie eine wahrscheinliche Ursache.

Antwort A:

Internet kaputt.

Antwort B:

Wahrscheinlich liegt ein DNS-Problem vor,
weil die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt eine wahrscheinliche Ursache
und begründet sie mit dem Fehlerbild.

Merksatz:

Ursache,
Begründung,
Prüfung.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Warum sollte RDP nicht direkt aus dem Internet erreichbar sein?

Antwort A:

Weil das nicht gut ist.

Antwort B:

RDP ist ein häufiges Angriffsziel für Brute-Force-Angriffe und Exploits.
Sicherer ist der Zugriff über VPN oder RDP-Gateway mit MFA und Firewall-Beschränkung.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt ein konkretes Risiko
und passende Schutzmaßnahmen.

Merksatz:

> Sicherheitsantwort:
> Risiko,
> Maßnahme,
> Wirkung.

Mini-Prüfung: 10 schnelle Zuordnungen

Frage	Antwort
DNS gehört zu welcher OSI-Schicht?	Schicht 7
TCP gehört zu welcher OSI-Schicht?	Schicht 4
IP gehört zu welcher OSI-Schicht?	Schicht 3
MAC gehört zu welcher OSI-Schicht?	Schicht 2
Kabel gehört zu welcher OSI-Schicht?	Schicht 1
HTTPS nutzt typischerweise welchen Port?	TCP 443
SSH nutzt typischerweise welchen Port?	TCP 22
SMB nutzt typischerweise welchen Port?	TCP 445
DHCP nutzt welche Ports?	UDP 67 und 68
DNS nutzt welchen Port?	UDP/TCP 53

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinlichstes Thema
IP geht, Name nicht	DNS
169.254.x.x	DHCP
lokal geht, extern nicht	Gateway, Routing, NAT oder Firewall
Host erreichbar, Dienst nicht	Port, Dienst oder Firewall
Login geht, Zugriff nicht	Autorisierung / Rechte
Anmeldung scheitert	Authentifizierung
Zertifikatswarnung	TLS/Zertifikat
nach Update defekt	Change prüfen
Daten verschlüsselt und Lösegeldforderung	Ransomware

Fehlerbild	Wahrscheinlichstes Thema
sehr viele Loginversuche	Brute Force

IHK-sichere Kurzformulierung

Das OSI-Modell hilft, Netzwerkkommunikation und Fehler systematisch einzuordnen. Schicht 1 betrifft Signale und Medien, Schicht 2 lokale Kommunikation mit MAC-Adressen, Schicht 3 IP-Adressierung und Routing, Schicht 4 Transport mit TCP, UDP und Ports und Schicht 7 Anwendungsprotokolle wie DNS, DHCP und HTTP. Das TCP/IP-Modell ist praxisnäher und fasst mehrere OSI-Schichten zusammen. Bei der Fehlersuche sollte man Fehlerbilder auswerten: IP erreichbar, Name nicht deutet auf DNS hin; 169.254.x.x deutet auf DHCP hin; lokal erreichbar, extern nicht deutet auf Gateway, Routing, NAT oder Firewall hin. Gute Prüfungsantworten nennen Ursache, Begründung und passende Prüfung oder Maßnahme.

Merksätze

OSI ist das Denkmodell.

TCP/IP ist das Praxismodell.

Schicht 1:
Signal.

Schicht 2:
MAC und VLAN.

Schicht 3:
IP und Routing.

Schicht 4:
TCP,
UDP
und Ports.

Schicht 7:
Dienste und Anwendungen.

MAC ist lokal.

IP ist logisch.

Port ist Dienstzuordnung.

DNS löst Namen auf.

DHCP verteilt IP-Konfiguration.

Gateway führt in andere Netze.

NAT übersetzt Adressen.

Firewall filtert Verkehr.

ping prüft ICMP,
nicht den Dienst.

IP ja,
Name nein:
DNS.

169.254.x.x:
DHCP.

Lokal ja,
extern nein:
Gateway prüfen.

Host ja,
Dienst nein:
Port prüfen.

Login ja,
Zugriff nein:
Rechte prüfen.

TCP ist zuverlässig.

UDP ist schnell und verbindungslos.

ARP löst IPv4 zu MAC auf.

VLAN trennt logisch.

Routing verbindet Netze.

Backup ohne Restore-Test ist unsicher.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

IDS meldet.

IPS blockiert.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Rechte.

Hardening reduziert Angriffsfläche.

Gute Prüfungsantwort:
Ursache,
Begründung,
Prüfung.