12.7 Merksätze und Prüfungswissen zu Sniffing, Analyse und Fehlersuche

Diese Seite fasst die wichtigsten Inhalte zu Sniffing, Paketmitschnitt, Wireshark, tcpdump, systematischer Fehlersuche, Logs, Monitoring und Dokumentation zusammen.

Diese Themen sind besonders wichtig, weil sie in der Praxis und in Prüfungsaufgaben häufig miteinander verbunden werden.

Merksatz:

```
Netzwerkanalyse bedeutet:
messen,
prüfen,
vergleichen
und fachlich einordnen.
```

Grundidee der Netzwerkanalyse

Netzwerkanalyse soll klären, was wirklich passiert.

Dabei nutzt man:

```
- Fehlerbeschreibung
- OSI-Modell
- Paketmitschnitt
- Logs
- Monitoring
- Konfigurationsprüfung
- Vergleich mit funktionierenden Systemen
```

Ziel ist nicht, blind etwas zu ändern.

Ziel ist:

```
Ursache finden
Ursache nachweisen
Ursache beheben
```

Ergebnis dokumentieren

Merksatz:

Nicht raten,
sondern prüfen.

Sniffing

Sniffing bedeutet:

Netzwerkverkehr mitschneiden und analysieren.

Dabei werden Pakete sichtbar gemacht.

Man erkennt zum Beispiel:

- Quell- und Ziel-MAC
- Quell- und Ziel-IP
- Protokoll
- Port
- DNS-Anfragen
- TCP-Handshake
- TLS-Handshake
- DHCP-Ablauf
- ICMP-Meldungen
- Wiederholungen
- Resets
- Timeouts

Merksatz:

Sniffing zeigt den tatsächlichen Netzwerkverkehr.

Paketmitschnitt

Ein Paketmitschnitt ist eine Aufzeichnung von Netzwerkpaketen.

Er hilft bei Fragen wie:

```
Kommt das Paket an?
Antwortet das Ziel?
Wird DNS richtig gefragt?
Findet ein TCP-Handshake statt?
Gibt es Retransmissions?
Gibt es Resets?
Gibt es TLS-Fehler?
Gibt es ICMP-Fehler?
Kommt DHCP-DORA zustande?
```

Merksatz:

```
Paketmitschnitt ersetzt Vermutungen durch Messdaten.
```

PCAP-Datei

Paketmitschnitte werden häufig als PCAP oder PCAPNG gespeichert.

Vorteile:

```
- spätere Analyse möglich
- Analyse mit Wireshark möglich
- Weitergabe an Fachabteilung möglich
- Beweissicherung bei Störungen
- Vergleich mit Logs möglich
```

Achtung:

```
PCAP-Dateien können sensible Daten enthalten.
```

Merksatz:

```
PCAP-Dateien wie vertrauliche Daten behandeln.
```

Datenschutz bei Paketmitschnitten

Paketmitschnitte können enthalten:

- IP-Adressen
- MAC-Adressen
- Hostnamen
- Benutzernamen
- Cookies
- Tokens
- unverschlüsselte Passwörter
- E-Mail-Inhalte
- personenbezogene Daten
- interne Strukturen

Deshalb:

nur mit berechtigtem Zweck
nur so lange wie nötig
nur relevanten Verkehr
sicher speichern
Zugriff begrenzen
nach Zweck löschen

Merksatz:

Sniffing ist technisch nützlich,
aber datenschutzrelevant.

Wireshark

Wireshark ist ein grafisches Werkzeug zur Paketanalyse.

Es zeigt:

- Paketliste
- Paketdetails
- Paketbytes
- Protokolle
- Filtermöglichkeiten

- Conversations
- Endpoints
- Expert Information

Wireshark eignet sich besonders gut, um Protokollabläufe sichtbar zu machen.

Merksatz:

Wireshark macht Netzwerkverkehr lesbar.

---

tcpdump

tcpdump ist ein Kommandozeilenwerkzeug für Paketmitschnitte.

Typische Nutzung:

auf Servern
auf Firewalls
auf Routern
per SSH
in minimalen Linux-Umgebungen

tcpdump kann Mitschnitte live anzeigen oder als PCAP-Datei speichern.

Merksatz:

tcpdump ist Paketmitschnitt auf der Kommandozeile.

---

tshark

tshark ist die Kommandozeilenversion von Wireshark.

Es eignet sich für:

- PCAP-Auswertung ohne GUI
- automatisierte Analyse
- Protokollauswertung
- Filterung
- Ausgabe bestimmter Felder

Merksatz:

> tshark bringt Wireshark-Funktionen auf die Kommandozeile.

Capture Filter und Display Filter

Capture Filter:

> bestimmen,
> was überhaupt aufgezeichnet wird.

Display Filter:

> bestimmen,
> was nachträglich angezeigt wird.

Filterart	Zeitpunkt	Wirkung
Capture Filter	vor oder während Aufnahme	begrenzt Aufzeichnung
Display Filter	nach Aufnahme	begrenzt Anzeige

Merksatz:

> Capture Filter spart Daten.
> Display Filter hilft bei Analyse.

Wichtige Wireshark-Filter

Fragestellung	Filteridee
bestimmte IP	ip.addr == 192.168.10.20
Quell-IP	ip.src == 192.168.10.20
Ziel-IP	ip.dst == 192.168.10.20
TCP-Port	tcp.port == 443
UDP-Port	udp.port == 53
DNS	dns
ARP	arp

Fragestellung	Filteridee
ICMP	icmp
HTTP	http
TLS	tls
TCP Reset	tcp.flags.reset == 1
Retransmission	tcp.analysis.retransmission

Merksatz:

> Filter müssen zur Frage passen.

Wichtige tcpdump-Filter

Ziel	Beispiel
Interface mitschneiden	tcpdump -i eth0
keine Namensauflösung	tcpdump -nn -i eth0
Host filtern	tcpdump -nn -i eth0 host 192.168.10.20
Quelle filtern	tcpdump -nn -i eth0 src host 192.168.10.20
Ziel filtern	tcpdump -nn -i eth0 dst host 192.168.10.20
Port filtern	tcpdump -nn -i eth0 port 443
TCP-Port	tcpdump -nn -i eth0 tcp port 443
UDP-Port	tcpdump -nn -i eth0 udp port 53
ICMP	tcpdump -nn -i eth0 icmp
ARP	tcpdump -nn -i eth0 arp
Datei schreiben	tcpdump -nn -i eth0 -w capture.pcap
Datei lesen	tcpdump -nn -r capture.pcap

Merksatz:

> tcpdump-Filter möglichst gezielt setzen.

Mitschnittort

Der Ort des Mitschnitts ist entscheidend.

Mögliche Stellen:

```
- Client
- Server
- Firewall
- Router
- Switch Mirror Port
- Reverse Proxy
- VPN-Gateway
- Container-Host
```

Je nach Ort sieht man andere Pakete.

Merksatz:

```
Der Mitschnittort entscheidet,
was sichtbar ist.
```

Port Mirroring

In geswitchten Netzwerken sieht ein Client nicht automatisch den gesamten Verkehr.

Port Mirroring kopiert Verkehr von einem oder mehreren Switchports auf einen Analyseport.

Auch genannt:

```
SPAN
```

Merksatz:

```
Port Mirroring macht fremden Switch-Verkehr für Analyse sichtbar.
```

Promiscuous Mode

Promiscuous Mode bedeutet:

```
Die Netzwerkkarte nimmt auch Frames an,
die nicht direkt an ihre eigene MAC-Adresse gerichtet sind.
```

Wichtig:

```
In geswitchten Netzen reicht das allein oft nicht,
weil der Switch fremden Verkehr gar nicht an diesen Port sendet.
```

Merksatz:

```
Promiscuous Mode ersetzt kein Port Mirroring.
```

TCP-Handshake

TCP baut eine Verbindung mit drei Schritten auf:

```
SYN
SYN-ACK
ACK
```

Bedeutung:

```
SYN:
Client möchte Verbindung starten.

SYN-ACK:
Server antwortet und akzeptiert grundsätzlich.

ACK:
Client bestätigt.
```

Merksatz:

```
SYN,
SYN-ACK,
ACK
= TCP-Verbindung aufgebaut.
```

TCP-Fehlerbilder

Beobachtung	mögliche Bedeutung
nur SYN-Wiederholungen	keine Antwort, Firewall, Routing oder Rückweg
SYN und RST	Port geschlossen oder Verbindung aktiv abgelehnt
viele Retransmissions	Paketverlust oder fehlende Bestätigung
Zero Window	Empfänger kann keine Daten aufnehmen
SYN, SYN-ACK, kein ACK	Rückweg oder Clientproblem
Handshake klappt, Anwendung fehlerhaft	höhere Schicht prüfen

Merksatz:

```
TCP-Analyse beginnt beim Handshake.
```

UDP-Analyse

UDP hat keinen Verbindungsaufbau.

Es gibt keinen TCP-Handshake.

Bei UDP prüft man:

```
Anfrage gesendet?
Antwort zurück?
richtiger Port?
ICMP-Fehler?
Firewall blockiert?
Dienst antwortet?
```

Beispiele für UDP:

```
DNS
DHCP
NTP
SNMP
VoIP
```

Merksatz:

UDP hat keinen Handshake,
deshalb Anfrage und Antwort direkt prüfen.

DNS-Analyse

DNS ist häufig der erste Schritt vor einer Verbindung.

Prüfen:

Welcher DNS-Server wird gefragt?
Welcher Name wird gefragt?
Welche Antwort kommt zurück?
A oder AAAA?
NXDOMAIN?
falscher DNS-Server?
Split DNS?
Cache?
TTL?

Merksatz:

DNS-Probleme sieht man oft vor dem eigentlichen Verbindungsversuch.

DHCP-Analyse

Der klassische DHCP-Ablauf lautet:

Discover
Offer
Request
Acknowledge

Kurz:

DORA

Fehlerbilder:

Discover ohne Offer:
DHCP-Server oder Relay antwortet nicht.

Offer ohne Request:
Client akzeptiert Angebot nicht.

Request ohne Acknowledge:
Server bestätigt nicht.

Merksatz:

DHCP mit DORA prüfen.

ARP-Analyse

ARP löst im lokalen IPv4-Netz auf:

IPv4-Adresse zu MAC-Adresse

Typische ARP-Fehler:

viele ARP-Anfragen ohne Antwort
falsche MAC-Adresse
doppelte IP-Adresse
Gateway antwortet nicht
VLAN falsch
falsche Netzmaske

Merksatz:

ARP-Probleme sind lokale Schicht-2- oder Schicht-3-Probleme.

ICMP-Analyse

ICMP liefert Diagnose- und Fehlermeldungen.

Beispiele:

```
Echo Request
Echo Reply
Destination Unreachable
Time Exceeded
Fragmentation Needed
```

Wichtig:

```
ICMP ist mehr als Ping.
```

Merksatz:

```
ICMP-Meldungen können Ursachen sichtbar machen.
```

TLS-Analyse

Bei TLS sieht man normalerweise nicht den verschlüsselten Inhalt.

Man sieht aber häufig:

```
Client Hello
Server Hello
SNI
Zertifikatsinformationen
TLS-Version
Cipher-Auswahl
TLS Alert
```

Typische Probleme:

```
falscher Hostname
abgelaufenes Zertifikat
nicht vertrauenswürdige CA
inkompatible TLS-Version
unvollständige Zertifikatskette
```

Merksatz:

TLS schützt Inhalte,
aber der Handshake liefert Hinweise.

SNI

SNI steht für:

Server Name Indication

SNI zeigt beim TLS-Aufbau, welchen Hostnamen der Client erreichen möchte.

Wichtig bei:

mehreren HTTPS-Diensten auf einer IP-Adresse

Merksatz:

SNI zeigt den gewünschten HTTPS-Hostnamen.

HTTP-Analyse

Bei HTTP prüft man:

Methode
Host-Header
Pfad
Statuscode
Header
Weiterleitung
Antwortzeit
Anwendungsmeldung

Wichtige Statuscodes:

Code	Bedeutung
200	OK
301 / 302	Weiterleitung

Code	Bedeutung
400	Bad Request
401	nicht authentifiziert
403	nicht berechtigt
404	nicht gefunden
500	interner Serverfehler
502	Bad Gateway
503	Dienst nicht verfügbar
504	Gateway Timeout

Merksatz:

> HTTP-Statuscodes helfen bei Schicht-7-Fehlern.

Ping richtig einordnen

Ping prüft ICMP-Erreichbarkeit.

Ping zeigt nicht:

> ob TCP 443 offen ist
> ob HTTPS funktioniert
> ob DNS korrekt ist
> ob Anmeldung klappt
> ob Berechtigung besteht
> ob Anwendung gesund ist

Merksatz:

> Ping ist kein vollständiger Diensttest.

Porttest richtig einordnen

Ein Porttest zeigt:

> Verbindung zum Port möglich oder nicht.

Er zeigt nicht automatisch:

> Anwendung funktioniert
> Login funktioniert
> Zertifikat passt
> Berechtigung stimmt
> Datenbank erreichbar
> API antwortet fachlich korrekt

Merksatz:

> Offener Port heißt nicht:
> Anwendung funktioniert.

Wichtige Analysewerkzeuge

Werkzeug	Zweck
ping	ICMP-Erreichbarkeit
traceroute / tracert	Weg zum Ziel
nslookup	einfache DNS-Prüfung
dig	detaillierte DNS-Prüfung
curl	HTTP/HTTPS/API-Test
nc	Port- und Verbindungstest
Test-NetConnection	Windows-Porttest
ss	lokale Ports und Verbindungen
netstat	Netzwerkstatus, älter
openssl s_client	TLS- und Zertifikatsprüfung
tcpdump	Paketmitschnitt CLI
tshark	PCAP-Analyse CLI
Wireshark	grafische Paketanalyse
journalctl	Linux-Logs
Ereignisanzeige	Windows-Logs

Merksatz:

Kein Werkzeug beantwortet alles.

Systematische Fehlersuche nach OSI

Schicht	Prüfung
1	Kabel, Link, Signal, WLAN
2	MAC, VLAN, Switch, ARP
3	IP, Subnetz, Gateway, Routing
4	TCP, UDP, Ports, Firewall
5	Sitzung, Session, Timeout
6	TLS, Zertifikat, Codierung
7	Anwendung, DNS, DHCP, HTTP, Authentifizierung

Merksatz:

OSI-Modell hilft,
den Fehlerbereich einzugrenzen.

Bottom-Up

Bottom-Up bedeutet:

von Schicht 1 nach oben prüfen.

Beispiel:

Kabel
Link
VLAN
IP
Gateway
Port
Dienst
Anwendung

Merksatz:

Bottom-Up beginnt beim Fundament.

Top-Down

Top-Down bedeutet:

bei der Anwendung beginnen
und nach unten prüfen.

Beispiel:

Webseite
HTTP-Status
TLS
Port
DNS
Routing
Link

Merksatz:

Top-Down beginnt beim sichtbaren Dienst.

Divide and Conquer

Divide and Conquer bedeutet:

Man prüft eine mittlere Ebene,
um den Suchbereich zu verkleinern.

Beispiel:

Ping geht,
aber Webdienst nicht.

Dann ist grob klar:

IP-Erreichbarkeit ist wahrscheinlich vorhanden,
aber Port,
Firewall,
TLS
oder Anwendung müssen weiter geprüft werden.

Merksatz:

Divide and Conquer halbiert den Suchbereich.

Fehlerbild sauber aufnehmen

Wichtige Fragen:

Wer ist betroffen?
Was funktioniert nicht?
Was funktioniert noch?
Seit wann?
Wo tritt der Fehler auf?
Intern oder extern?
LAN oder WLAN?
VPN oder lokal?
Nur ein Benutzer oder alle?
Welche Fehlermeldung?
Was wurde zuletzt geändert?

Merksatz:

Gute Fehlerbeschreibung ist Diagnosearbeit.

Typische Fehlerbilder

Fehlerbild	erste Richtung
kein Link	Schicht 1
169.254.x.x	DHCP
Gateway nicht erreichbar	Schicht 2 / 3

Fehlerbild	erste Richtung
IP geht, Name nicht	DNS
Ping geht, Port nicht	Schicht 4 / Firewall / Dienst
Port offen, Anwendung fehlerhaft	Schicht 7
Timeout	keine passende Antwort
Connection Refused	Dienst lehnt aktiv ab
401	Authentifizierung
403	Autorisierung
404	Pfad oder Ressource fehlt
500	Anwendung oder Server
502	Proxy zu Backend
Zertifikatswarnung	TLS, DNS, Zeit oder CA

Merksatz:

```
Fehlerbild gibt Richtung,
aber noch keinen Beweis.
```

Authentifizierung und Autorisierung

Authentifizierung bedeutet:

```
Wer bist du?
```

Beispiele:

```
Benutzername
Passwort
MFA
Zertifikat
Token
```

Autorisierung bedeutet:

```
Was darfst du?
```

Beispiele:

```
Rolle
Gruppe
Rechte
Freigabe
API-Scope
```

Merksatz:

```
401 ist oft Authentifizierung.
403 ist oft Autorisierung.
```

Timeout und Connection Refused

Timeout:

```
Keine Antwort kommt zurück.
```

Mögliche Ursachen:

```
Firewall droppt
Routing fehlt
Rückweg fehlt
Ziel antwortet nicht
```

Connection Refused:

```
Ziel lehnt aktiv ab.
```

Mögliche Ursachen:

```
Dienst läuft nicht
falscher Port
Dienst lauscht nicht
Host lehnt ab
```

Merksatz:

```
Timeout = keine Antwort.
Refused = aktive Ablehnung.
```

MTU-Probleme

MTU steht für:

```
Maximum Transmission Unit
```

Typische Hinweise:

```
kleine Pakete funktionieren
große Übertragungen hängen
VPN instabil
Webseiten laden teilweise
Downloads brechen ab
viele Retransmissions
Fragmentation Needed fehlt oder wird blockiert
```

Merksatz:

```
Kleine Daten gehen,
große nicht:
MTU prüfen.
```

Logs

Logs zeigen Ereignisse und Entscheidungen.

Wichtige Logquellen:

```
- Firewall-Logs
- DNS-Logs
- DHCP-Logs
- VPN-Logs
- Webserver-Logs
```

- Reverse-Proxy-Logs
- Authentifizierungslogs
- Systemlogs
- Anwendungslogs
- Mailserver-Logs
- Datenbank-Logs

Merksatz:

Logs zeigen,
was Systeme entschieden oder gemeldet haben.

Monitoring

Monitoring überwacht Systeme und Dienste dauerhaft.

Es prüft zum Beispiel:

Erreichbarkeit
Antwortzeiten
CPU
RAM
Speicherplatz
Bandbreite
Paketverlust
Zertifikate
Dienste
Logs
Verbindungen

Merksatz:

Monitoring erkennt Probleme über Zeit.

Dokumentation

Gute Dokumentation enthält:

- Netzplan
- IP-Adressplan
- VLAN-Plan
- Firewall-Regeln
- NAT-Regeln
- DNS-Einträge
- DHCP-Scopes
- Serverrollen
- Dienste
- Ansprechpartner
- Änderungen
- Notfallverfahren

Merksatz:

> Dokumentation ist ein Werkzeug für Fehlersuche.

Root Cause Analysis

Root Cause Analysis bedeutet:

> die eigentliche Ursache finden.

Nicht nur:

> Dienst neu starten

Sondern:

> Warum ist der Dienst abgestürzt?
> Warum war Speicher voll?
> Warum gab es keinen Alarm?
> Warum wurde die Änderung nicht getestet?

Merksatz:

Ursache beheben,
nicht nur Symptom beseitigen.

Workaround und Lösung

Workaround:

vorübergehende Umgehung

Lösung:

eigentliche Ursache wird beseitigt

Beispiel:

Workaround:
IP-Adresse statt DNS-Namen verwenden.

Ursache:
DNS-Eintrag falsch.

Lösung:
DNS-Eintrag korrigieren.

Merksatz:

Workaround ist nicht automatisch Lösung.

Eine Änderung pro Test

Bei Fehlersuche sollte man nicht viele Dinge gleichzeitig ändern.

Besser:

eine Hypothese bilden
einen Test durchführen
Ergebnis prüfen

```
dokumentieren
nächste Hypothese testen
```

Merksatz:

```
Mehrere Änderungen gleichzeitig verschleiern die Ursache.
```

Nach Änderung zuerst Änderung prüfen

Wenn ein Fehler nach einer Änderung auftritt, prüft man zuerst diese Änderung.

Beispiele:

```
Firewall-Regel geändert
DNS geändert
Zertifikat erneuert
VLAN geändert
Update installiert
Passwort geändert
Reverse Proxy angepasst
VPN geändert
```

Merksatz:

```
Die letzte Änderung ist oft der wichtigste Hinweis.
```

Sicherheitsbewusstsein bei Analyse

Analysewerkzeuge können sensible Informationen offenlegen.

Beispiele:

```
unverschlüsselte Passwörter
Tokens
Cookies
interne Hostnamen
IP-Adressbereiche
Benutzerinformationen
```

Fehlermeldungen
Konfigurationsdetails

Deshalb:

Zugriff beschränken
Dateien schützen
keine unnötigen Mitschnitte
Logs nicht ungeschützt teilen
Datenschutz beachten

Merksatz:

Diagnose darf keine neue Sicherheitslücke erzeugen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was versteht man unter Sniffing?
- Wofür nutzt man Wireshark?
- Wofür nutzt man tcpdump?
- Was ist eine PCAP-Datei?
- Was ist Port Mirroring?
- Warum sieht man im Switch-Netz nicht automatisch allen Verkehr?
- Was ist der Unterschied zwischen Capture Filter und Display Filter?
- Wie erkennt man einen TCP-Handshake?
- Was bedeuten SYN, SYN-ACK und ACK?
- Was bedeutet RST?
- Was bedeutet Retransmission?
- Warum sieht man HTTPS-Inhalte nicht im Klartext?
- Was kann man bei DNS im Mitschnitt erkennen?
- Wie analysiert man DHCP?
- Warum reicht Ping nicht aus?
- Warum reicht ein Porttest nicht aus?
- Wie hilft das OSI-Modell bei der Fehlersuche?
- Was ist Bottom-Up?
- Was ist Top-Down?

- Was ist Divide and Conquer?
- Warum sind Logs wichtig?
- Warum ist Monitoring wichtig?
- Warum ist Dokumentation wichtig?

Typische Prüfungsfallen

Sniffing zeigt echten Verkehr.

Sniffing ist datenschutzrelevant.

Wireshark ist grafisch.

tcpdump ist Kommandozeile.

tshark ist Wireshark auf Kommandozeile.

PCAP-Dateien können sensible Daten enthalten.

In geswitchten Netzen sieht man nicht automatisch alles.

Port Mirroring kopiert Verkehr.

Promiscuous Mode reicht allein oft nicht.

Capture Filter begrenzen Aufnahme.

Display Filter begrenzen Anzeige.

TCP hat Handshake.

UDP hat keinen Handshake.

SYN startet TCP-Verbindung.

SYN-ACK ist Serverantwort.

ACK bestätigt.

RST lehnt ab oder beendet.

Retransmission bedeutet erneutes Senden.

DNS früh prüfen.

DHCP-DORA kennen.

ICMP ist mehr als Ping.

HTTPS-Inhalte sind verschlüsselt.

TLS-Handshake kann trotzdem Hinweise liefern.

SNI zeigt gewünschten Hostnamen.

Ping prüft nicht den Dienst.

Port offen heißt nicht Anwendung funktioniert.

Timeout und Connection Refused unterscheiden.

401 ist Authentifizierung.

403 ist Autorisierung.

OSI-Modell hilft beim Eingrenzen.

Logs und Mitschnitt ergänzen sich.

Monitoring zeigt Zustand über Zeit.

Dokumentation beschleunigt Fehlersuche.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Sniffing	Mitschneiden von Netzwerkverkehr
Paketmitschnitt	Aufzeichnung von Paketen

Begriff	Kurze Erklärung
PCAP	Datei mit Paketmitschnitt
Wireshark	grafisches Analysewerkzeug
tcpdump	Kommandozeilenwerkzeug für Mitschnitt
tshark	Wireshark auf Kommandozeile
Port Mirroring	Verkehr auf Analyseport kopieren
Promiscuous Mode	Netzwerkkarte nimmt fremde Frames an
Capture Filter	Filter vor der Aufnahme
Display Filter	Filter nach der Aufnahme
SYN	TCP-Verbindungsstart
SYN-ACK	TCP-Antwort des Servers
ACK	Bestätigung
RST	Reset, aktive Ablehnung oder Abbruch
Retransmission	erneutes Senden
ARP	IPv4-Adresse zu MAC-Adresse
ICMP	Diagnose- und Fehlermeldungsprotokoll
DNS	Namensauflösung
DHCP-DORA	Discover, Offer, Request, Acknowledge
SNI	Hostname im TLS-Handshake
TLS Alert	TLS-Fehlermeldung
Bottom-Up	von Schicht 1 nach oben prüfen
Top-Down	von Anwendung nach unten prüfen
Divide and Conquer	Suchbereich in der Mitte eingrenzen
Timeout	keine Antwort
Connection Refused	aktive Ablehnung
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
Log	Ereignisprotokoll
Monitoring	dauerhafte Überwachung
Root Cause	eigentliche Ursache
Workaround	vorübergehende Umgehung
Runbook	Schritt-für-Schritt-Anleitung

IHK-sichere Gesamtformulierung

Sniffing bezeichnet das Mitschneiden und Analysieren von Netzwerkverkehr. Mit Werkzeugen wie Wireshark, tcpdump oder tshark können Pakete untersucht werden, um DNS-Anfragen, ARP, ICMP, TCP-Handshakes, UDP-Kommunikation, DHCP-DORA, TLS-Handshakes, Resets, Retransmissions und Timeouts zu erkennen. In geswitchten Netzwerken sieht ein Client nicht automatisch den gesamten Verkehr; dafür wird häufig Port Mirroring benötigt. Das OSI-Modell hilft bei der Fehlersuche, indem Fehler schichtweise eingegrenzt werden. Ping und Porttests liefern nur Teilinformationen und ersetzen keine vollständige Prüfung von DNS, Routing, Firewall, NAT, Dienst, TLS, Anwendung, Logs und Berechtigungen. Logs, Monitoring und Dokumentation ergänzen Paketmitschnitte und sind wichtig, um Ursachen nachzuweisen und dauerhaft zu beheben.

Wichtigste Merksätze

Nicht raten,
sondern messen.

Sniffing zeigt echten Verkehr.

Paketmitschnitt zeigt Pakete.

Logs zeigen Ereignisse.

Monitoring zeigt Zustand über Zeit.

Dokumentation zeigt Aufbau und Änderungen.

Wireshark ist grafisch.

tcpdump ist Kommandozeile.

tshark ist Wireshark auf Kommandozeile.

PCAP-Dateien sind sensibel.

Mitschnittort ist entscheidend.

Port Mirroring kopiert Switch-Verkehr.

Capture Filter vor Aufnahme.

Display Filter nach Aufnahme.

TCP hat Handshake.

UDP hat keinen Handshake.

SYN,
SYN-ACK,
ACK
= TCP-Verbindung aufgebaut.

RST bedeutet aktive Ablehnung oder Abbruch.

Retransmission bedeutet erneutes Senden.

DNS immer früh prüfen.

DHCP mit DORA prüfen.

ARP ist lokal wichtig.

ICMP ist mehr als Ping.

TLS schützt Inhalte.

SNI zeigt Hostnamen.

HTTP-Statuscodes helfen bei Schicht 7.

Ping reicht nicht aus.

Port offen reicht nicht aus.

Timeout ist keine Antwort.

Connection Refused ist aktive Ablehnung.

401 ist Authentifizierung.

403 ist Autorisierung.

OSI-Modell grenzt Fehler ein.

Bottom-Up beginnt unten.

Top-Down beginnt oben.

Divide and Conquer grenzt mittig ein.

Eine Änderung pro Test.

Letzte Änderung zuerst prüfen.

Workaround ist nicht automatisch Lösung.

Root Cause suchen.

Ergebnisse dokumentieren.