12.1 Sniffing, Paketmitschnitt und Netzwerkanalyse

Sniffing bedeutet:

```
Netzwerkverkehr mitschneiden und analysieren.
```

Dabei werden Datenpakete sichtbar gemacht, damit man verstehen kann, was im Netzwerk wirklich passiert.

Typische Werkzeuge sind:

```
- Wireshark
- tcpdump
- tshark
- Packet Capture auf Firewalls
- Switch-Port-Mirroring
- Browser-Entwicklertools
- Logdateien als Ergänzung
```

Merksatz:

```
Sniffing zeigt den tatsächlichen Netzwerkverkehr.
```

Warum nutzt man Paketmitschnitte?

Ein Paketmitschnitt hilft, wenn normale Fehlermeldungen nicht ausreichen.

Man kann damit prüfen:

```
Kommt ein Paket überhaupt an?
Antwortet das Zielsystem?
Wird DNS korrekt gefragt?
Findet ein TCP-Handshake statt?
Gibt es Wiederholungen?
Gibt es Timeouts?
Wird die Verbindung aktiv abgelehnt?
```

Wird TLS aufgebaut?
Werden DHCP-Pakete gesendet?
Gibt es ARP-Probleme?

Merksatz:

Paketmitschnitt hilft,
Vermutungen durch echte Daten zu ersetzen.

Sniffing ist nicht immer erlaubt

Netzwerkverkehr kann sensible Informationen enthalten.

Beispiele:

- Benutzernamen
- Passwörter
- Cookies
- Tokens
- E-Mail-Inhalte
- interne IP-Adressen
- Kundendaten
- personenbezogene Daten
- vertrauliche Kommunikation

Deshalb gilt:

Paketmitschnitte nur mit Erlaubnis,
Zweckbindung
und möglichst begrenztem Umfang durchführen.

Merksatz:

Sniffing ist technisch hilfreich,
aber datenschutz- und sicherheitsrelevant.

Was sieht man in einem Paketmitschnitt?

In einem Paketmitschnitt sieht man je nach Protokoll:

- Quell-MAC-Adresse
- Ziel-MAC-Adresse
- Quell-IP-Adresse
- Ziel-IP-Adresse
- Protokoll
- Quellport
- Zielport
- Flags
- Paketgröße
- Zeitstempel
- DNS-Anfragen
- TCP-Handshake
- TLS-Handshake
- unverschlüsselte Nutzdaten

Bei verschlüsselten Verbindungen sieht man den Inhalt nicht einfach im Klartext.

Merksatz:

Metadaten sind oft sichtbar,
Inhalte bei TLS meist nicht.

OSI-Schichten im Paketmitschnitt

Ein Paketmitschnitt zeigt mehrere OSI-Schichten gleichzeitig.

Sichtbarer Bereich	OSI-Schicht
MAC-Adressen	2
VLAN-Tags	2
IP-Adressen	3
ICMP	3
TCP / UDP	4
Ports	4
TLS-Handshake	6 / 7-Bezug
DNS, HTTP, DHCP, SMTP	7

Merksatz:

```
Paketmitschnitt verbindet die Schichten sichtbar miteinander.
```

Wireshark

Wireshark ist ein grafisches Werkzeug zur Analyse von Netzwerkpaketen.

Es zeigt Pakete übersichtlich mit:

```
- Paketliste
- Paketdetails
- Rohdaten
- Protokollauswertung
- Filtern
- Zeitinformationen
- Verbindungsübersichten
```

Wireshark eignet sich besonders gut, um Protokolle Schritt für Schritt zu verstehen.

Merksatz:

```
Wireshark macht Netzwerkverkehr sichtbar und lesbar.
```

---

tcpdump

tcpdump ist ein Kommandozeilenwerkzeug für Paketmitschnitte.

Es wird häufig auf Linux, Unix, Firewalls, Servern oder Netzwerkgeräten verwendet.

Vorteile:

```
- schnell
- leicht auf Servern nutzbar
- gut für SSH-Sitzungen
- kann Mitschnitte als Datei speichern
- gut für gezielte Filter
```

Merksatz:

tcpdump ist Paketmitschnitt auf der Kommandozeile.

---

tshark

tshark ist die Kommandozeilenversion von Wireshark.

Es kann Pakete aufzeichnen, filtern und Protokolldaten ausgeben.

Typische Nutzung:

- Analyse auf Servern
- automatisierte Auswertung
- schnelle Suche in Mitschnitten
- Export bestimmter Felder

Merksatz:

tshark bringt Wireshark-Funktionen auf die Kommandozeile.

Packet Capture auf Firewalls

Viele Firewalls bieten eine eingebaute Paketmitschnittfunktion.

Vorteil:

Man sieht,
ob Pakete an der Firewall ankommen
und auf welchem Interface sie erscheinen.

Das ist hilfreich bei:

- NAT-Problemen
- Routingproblemen
- DMZ-Verkehr
- VPN-Problemen
- Firewall-Regelprüfung
- asymmetrischem Routing

Merksatz:

```
Mitschnitt auf der Firewall zeigt,
was die Firewall wirklich sieht.
```

Switch-Port-Mirroring

Ein Switch leitet normalerweise nur relevante Frames an den passenden Port weiter.

Damit ein Analysegerät trotzdem Verkehr anderer Ports sehen kann, nutzt man:

```
Port Mirroring
```

oder:

```
SPAN-Port
```

Dabei wird Verkehr von einem oder mehreren Ports auf einen Analyseport kopiert.

Merksatz:

```
Port Mirroring kopiert Verkehr zu einem Analyseport.
```

Warum sieht man nicht automatisch alles?

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

Er sieht hauptsächlich:

```
- eigenen Verkehr
- Broadcasts
- Multicasts
- bestimmte lokale Pakete
```

Er sieht normalerweise nicht:

```
den gesamten Verkehr anderer Clients
```

Dafür braucht man Port Mirroring, Mitschnitt am Zielsystem oder Mitschnitt an einer Firewall.

Merksatz:

> In geswitchten Netzen sieht man ohne Mirror nicht alles.

Promiscuous Mode

Promiscuous Mode bedeutet:

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

Das ist für Sniffing hilfreich.

Aber:

> In geswitchten Netzwerken reicht Promiscuous Mode allein nicht,
> um fremden Verkehr zu sehen.

Merksatz:

> Promiscuous Mode hilft,
> ersetzt aber kein Port Mirroring.

Capture Filter und Display Filter

Bei Wireshark und tcpdump gibt es unterschiedliche Filterarten.

Capture Filter:

> bestimmen,
> was überhaupt aufgezeichnet wird.

Display Filter:

> bestimmen,
> was nachträglich angezeigt wird.

Beispiel:

```
Capture Filter:
nur Verkehr zu Host 192.168.10.20 mitschneiden

Display Filter:
im vorhandenen Mitschnitt nur DNS anzeigen
```

Merksatz:

```
Capture Filter begrenzt Aufnahme.
Display Filter begrenzt Anzeige.
```

Capture Filter

Capture Filter werden vor oder während der Aufnahme angewendet.

Vorteil:

```
kleinere Dateien
weniger Daten
bessere Übersicht
weniger sensible Daten
```

Nachteil:

```
was nicht aufgezeichnet wurde,
kann man später nicht analysieren.
```

Merksatz:

```
Capture Filter nur setzen,
wenn klar ist,
was benötigt wird.
```

Display Filter

Display Filter werden nach der Aufnahme angewendet.

Vorteil:

```
alle Daten bleiben erhalten
Ansicht kann beliebig eingegrenzt werden
ideal für Analyse
```

Beispiele für Filterideen:

```
nur eine IP-Adresse
nur DNS
nur TCP-Fehler
nur HTTP
nur Pakete mit Reset
```

Merksatz:

```
Display Filter sind sicherer für Analyse,
weil die Rohdaten erhalten bleiben.
```

Wichtige Filtergedanken

Typische Fragen:

```
Welche IP-Adresse interessiert mich?
Welcher Port interessiert mich?
Welches Protokoll interessiert mich?
Welche Richtung interessiert mich?
Welche Fehlermeldung sehe ich?
Welche Zeitspanne ist relevant?
```

Beispiele:

```
Verkehr eines bestimmten Hosts
DNS-Anfragen
TCP-Verbindungen zu Port 443
ICMP-Pakete
DHCP-DORA
ARP-Anfragen
```

Merksatz:

```
Gute Filter entstehen aus einer klaren Fragestellung.
```

MAC-Adressen im Mitschnitt

MAC-Adressen gehören zu OSI-Schicht 2.

Sie zeigen, welche Geräte im lokalen Netzwerksegment miteinander kommunizieren.

Wichtig:

```
MAC-Adressen ändern sich bei jedem Routing-Hop.
```

Ein Paket zum Internet hat im LAN als Ziel-MAC nicht den Webserver im Internet, sondern die MAC-Adresse des Standard-Gateways.

Merksatz:

```
Im lokalen Netz ist die Ziel-MAC oft das Gateway.
```

IP-Adressen im Mitschnitt

IP-Adressen gehören zu OSI-Schicht 3.

Sie zeigen:

```
Quell-IP
Ziel-IP
```

Bei NAT können sich IP-Adressen ändern.

Beispiel:

```
vor NAT:
private Client-IP

nach NAT:
öffentliche Firewall-IP
```

Merksatz:

```
IP-Adressen zeigen logische Endpunkte,
können durch NAT geändert werden.
```

Ports im Mitschnitt

Ports gehören zu OSI-Schicht 4.

Sie zeigen, welcher Dienst angesprochen wird.

Beispiel:

```
Zielport TCP 443:
typischerweise HTTPS

Zielport TCP 22:
typischerweise SSH

Zielport UDP 53:
typischerweise DNS
```

Merksatz:

```
Ports helfen,
Dienste zu erkennen.
```

Quellport und Zielport

Bei Client-Server-Verbindungen nutzt der Client meist einen temporären Quellport.

Beispiel:

```
Client:
192.168.10.50:53124

Server:
203.0.113.10:443
```

Dabei ist:

```
53124 = temporärer Quellport
443 = Zielport des Dienstes
```

Merksatz:

```
Der bekannte Dienstport ist meistens der Zielport beim Server.
```

TCP-Handshake im Mitschnitt

TCP baut eine Verbindung mit drei Schritten auf:

```
SYN
SYN-ACK
ACK
```

Im Mitschnitt sieht man dadurch, ob eine TCP-Verbindung zustande kommt.

Beobachtung	mögliche Bedeutung
SYN, SYN-ACK, ACK	Verbindung aufgebaut
nur SYN-Wiederholungen	keine Antwort, Firewall oder Routingproblem
SYN, RST	Ziel lehnt aktiv ab
SYN, SYN-ACK, danach kein ACK	Rückweg oder Clientproblem
viele Retransmissions	Paketverlust oder Blockierung

Merksatz:

```
TCP-Handshake ist einer der wichtigsten Hinweise im Mitschnitt.
```

TCP SYN

SYN bedeutet:

```
Client möchte eine TCP-Verbindung starten.
```

Wenn man nur SYN-Pakete sieht, aber keine Antwort, kann das bedeuten:

```
Ziel antwortet nicht.
Firewall blockiert.
Rückweg fehlt.
Ziel-IP ist falsch.
Dienst ist nicht erreichbar.
Routing stimmt nicht.
```

Merksatz:

```
Nur SYN ohne Antwort deutet auf keine erreichbare Antwort hin.
```

TCP SYN-ACK

SYN-ACK bedeutet:

```
Server akzeptiert den Verbindungsaufbau grundsätzlich
und antwortet.
```

Wenn SYN-ACK ankommt, ist der Zielport grundsätzlich erreichbar.

Danach muss der Client mit ACK bestätigen.

Merksatz:

```
SYN-ACK zeigt:
Ziel hat auf TCP-Verbindungsversuch geantwortet.
```

TCP ACK

ACK bestätigt empfangene Daten oder Verbindungsaufbau.

ACKs sind normaler Bestandteil von TCP.

Sie zeigen, dass Pakete angekommen sind und die Verbindung fortgesetzt werden kann.

Merksatz:

```
ACK bestätigt Empfang.
```

TCP RST

RST steht für:

```
Reset
```

Ein RST beendet oder verweigert eine Verbindung aktiv.

Mögliche Ursachen:

```
- Dienst läuft nicht
- Port geschlossen
- Anwendung lehnt ab
- Firewall sendet Reset
- falsches Protokoll auf Port
- Verbindung wird abgebrochen
```

Merksatz:

```
RST = aktive Ablehnung oder Abbruch.
```

TCP Retransmission

Retransmission bedeutet:

```
TCP sendet ein Paket erneut.
```

Grund:

```
keine Bestätigung erhalten
```

Mögliche Ursachen:

```
- Paketverlust
- Firewall blockiert Pakete
- Überlastung
- schlechter Link
- Rückwegproblem
```

- Ziel antwortet nicht

Merksatz:

Retransmissions deuten auf verlorene oder unbeantwortete Pakete hin.

TCP Window

TCP Window beschreibt, wie viele Daten empfangen werden können, bevor eine Bestätigung nötig ist.

Wenn das Fenster sehr klein oder null wird, kann das auf Leistungsprobleme hindeuten.

Beispiel:

Empfänger kann nicht schnell genug verarbeiten.

Merksatz:

TCP Window betrifft Flusskontrolle und Leistung.

UDP im Mitschnitt

UDP hat keinen Verbindungsaufbau wie TCP.

Es gibt keinen SYN, kein SYN-ACK und kein ACK für den Verbindungsaufbau.

Bei UDP prüft man:

Wird Anfrage gesendet?
Kommt Antwort zurück?
Gibt es ICMP-Fehler?
Wird der richtige Port genutzt?

Merksatz:

UDP ist verbindungslos,
deshalb sieht man keinen Handshake.

ICMP im Mitschnitt

ICMP gehört zu Schicht 3.

Es wird genutzt für:

```
- Ping
- Ziel nicht erreichbar
- Time Exceeded
- Fragmentierung nötig
- Diagnosemeldungen
```

ICMP-Meldungen können wichtige Hinweise geben.

Beispiel:

```
Destination Unreachable
```

Merksatz:

```
ICMP liefert oft Hinweise auf Netzwerkprobleme.
```

ARP im Mitschnitt

ARP gehört zur lokalen IPv4-Kommunikation.

ARP fragt:

```
Welche MAC-Adresse gehört zu dieser IPv4-Adresse?
```

Beispiel:

```
Wer hat 192.168.10.1?
```

Antwort:

```
192.168.10.1 ist bei MAC-Adresse xx:xx:xx:xx:xx:xx
```

Merksatz:

ARP löst IPv4-Adresse zu MAC-Adresse im lokalen Netz auf.

ARP-Probleme erkennen

Typische Hinweise:

viele ARP-Anfragen ohne Antwort
falsche MAC-Adresse
doppelte IP-Adresse
Gateway antwortet nicht
Client fragt falsches Ziel direkt

Mögliche Ursachen:

- Ziel nicht im lokalen Netz
- falsche Netzmaske
- falsches Gateway
- VLAN falsch
- IP-Konflikt
- Gerät offline

Merksatz:

ARP-Probleme zeigen oft lokale Layer-2- oder Layer-3-Fehler.

DNS im Mitschnitt

DNS ist häufig sehr gut im Mitschnitt erkennbar.

Man sieht:

welche Namen gefragt werden
welcher DNS-Server gefragt wird
welche Antwort zurückkommt
ob A- oder AAAA-Records angefragt werden
ob NXDOMAIN zurückkommt
ob Antwort verzögert ist

Merksatz:

```
DNS-Mitschnitt zeigt,
welcher Name wirklich wohin aufgelöst wird.
```

DHCP im Mitschnitt

DHCP kann man im Mitschnitt gut erkennen.

Der klassische Ablauf:

```
Discover
Offer
Request
Acknowledge
```

Fehlerbilder:

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

Offer kommt,
aber kein Ack:
Anfrage oder Serverbestätigung gestört.

falsche Optionen:
Gateway oder DNS falsch verteilt.
```

Merksatz:

```
DHCP-DORA ist im Mitschnitt gut nachvollziehbar.
```

TLS im Mitschnitt

Bei TLS sieht man normalerweise nicht den verschlüsselten Inhalt.

Man sieht aber oft:

```
TLS-Version
Server Name Indication
Zertifikatsinformationen
Cipher-Aushandlung
Handshake-Fehler
Verbindungsabbrüche
```

Wichtig:

```
Der Inhalt von HTTPS bleibt ohne Entschlüsselung geschützt.
```

Merksatz:

```
TLS versteckt Inhalte,
aber der Handshake liefert Hinweise.
```

SNI im Mitschnitt

SNI steht für:

```
Server Name Indication
```

Der Client teilt beim TLS-Aufbau mit, welchen Hostnamen er erreichen möchte.

Das ist wichtig, wenn mehrere HTTPS-Dienste auf derselben IP laufen.

Beispiel:

```
wiki.firma.de
cloud.firma.de
git.firma.de
```

alle über:

```
dieselbe IP und TCP 443
```

Merksatz:

SNI zeigt den gewünschten TLS-Hostnamen.

HTTP im Mitschnitt

Unverschlüsseltes HTTP kann im Mitschnitt direkt gelesen werden.

Man sieht zum Beispiel:

Methode
Pfad
Host-Header
Statuscode
Header
teilweise Inhalte

Bei HTTPS sieht man diese Inhalte normalerweise nicht, weil sie verschlüsselt sind.

Merksatz:

HTTP ist lesbar,
HTTPS schützt den Inhalt.

FTP und Telnet im Mitschnitt

FTP und Telnet können unverschlüsselte Inhalte übertragen.

Bei klassischem FTP können sichtbar sein:

Benutzername
Passwort
Befehle
Dateiinhalte

Bei Telnet können sichtbar sein:

Login
Passwort
Befehle

Merksatz:

> Unverschlüsselte Protokolle sind im Mitschnitt gefährlich sichtbar.

SMB im Mitschnitt

SMB-Verkehr kann Hinweise liefern bei:

- Zugriff verweigert
- Verbindungsproblemen
- Namensproblemen
- Protokollversionsproblemen
- Dateioperationen
- Authentifizierungsproblemen

Wichtig:

> Moderne SMB-Kommunikation kann teilweise signiert oder verschlüsselt sein.

Merksatz:

> SMB-Mitschnitte helfen bei Freigabe- und Rechteproblemen.

Zeitstempel im Mitschnitt

Zeitstempel zeigen, wann Pakete gesendet oder empfangen wurden.

Sie helfen bei:

- Timeouts
- Verzögerungen
- Wiederholungen
- langsamen Antworten
- Reihenfolge von Ereignissen

Wichtig:

Systemzeit des Analysegeräts sollte korrekt sein.

Merksatz:

Ohne korrekte Zeit sind Mitschnitte schwerer auszuwerten.

Paketgröße

Die Paketgröße kann Hinweise geben.

Beispiele:

sehr kleine Pakete:
Steuerinformationen, ACKs, Handshake

große Pakete:
Datenübertragung

fragmentierte Pakete:
MTU- oder Fragmentierungsthemen möglich

Merksatz:

Paketgrößen können Leistungs- oder MTU-Probleme sichtbar machen.

MTU-Probleme im Mitschnitt

MTU steht für:

Maximum Transmission Unit

MTU-Probleme können auftreten, wenn Pakete zu groß sind und Fragmentierung nicht richtig funktioniert.

Typische Hinweise:

Verbindungen bauen auf,
aber größere Datenübertragungen hängen.

Webseiten laden teilweise.

VPN-Verbindungen haben Probleme.

ICMP Fragmentation Needed fehlt oder wird blockiert.

Merksatz:

MTU-Probleme zeigen sich oft erst bei größeren Paketen.

Wo sollte man mitschneiden?

Der Ort des Mitschnitts ist entscheidend.

Mögliche Stellen:

Client
Server
Firewall WAN
Firewall LAN
Firewall DMZ
Switch Mirror Port
Router
VPN-Gateway
Reverse Proxy

Je nach Stelle sieht man unterschiedliche Informationen.

Merksatz:

Der Mitschnittort entscheidet,
was man sehen kann.

Clientseitiger Mitschnitt

Ein Mitschnitt am Client zeigt:

```
was der Client wirklich sendet
welche DNS-Anfragen gestellt werden
welche IP erreicht wird
ob Antwort zurückkommt
welche Fehlversuche entstehen
```

Gut bei:

```
Einzelclient-Problemen
DNS-Problemen
Browserproblemen
VPN-Clientproblemen
```

Merksatz:

```
Client-Mitschnitt zeigt die Sicht des Clients.
```

Serverseitiger Mitschnitt

Ein Mitschnitt am Server zeigt:

```
ob Anfragen beim Server ankommen
von welcher IP sie ankommen
auf welchem Port sie ankommen
ob der Server antwortet
ob die Host-Firewall beteiligt sein könnte
```

Gut bei:

```
Dienstproblemen
Firewallverdacht
NAT-Fragen
Rückwegproblemen
```

Merksatz:

```
Server-Mitschnitt zeigt,
ob der Dienst wirklich erreicht wird.
```

Firewall-Mitschnitt

Ein Mitschnitt auf der Firewall zeigt:

```
kommt Verkehr auf WAN an?
wird Verkehr nach NAT weitergeleitet?
kommt Antwort zurück?
auf welchem Interface erscheint Verkehr?
wird Rückverkehr sichtbar?
```

Gut bei:

```
NAT
DMZ
VPN
Routing
Portweiterleitung
asymmetrischem Routing
```

Merksatz:

```
Firewall-Mitschnitt zeigt den Übergang zwischen Zonen.
```

Mehrere Mitschnitte vergleichen

Manchmal braucht man Mitschnitte an mehreren Stellen.

Beispiel:

```
Client sendet SYN.
Firewall WAN sieht SYN.
Firewall DMZ sieht weitergeleitetes SYN.
Server sieht kein SYN.
```

Dann liegt das Problem zwischen Firewall und Server.

Oder:

```
Server antwortet.
Firewall sieht Antwort.
Client sieht Antwort nicht.
```

Dann Rückweg oder Filter prüfen.

Merksatz:

```
Mehrere Mitschnitte zeigen,
wo Pakete verschwinden.
```

Paketmitschnitt und Logs kombinieren

Paketmitschnitte zeigen Verkehr.

Logs zeigen Entscheidungen und Anwendungszustände.

Beispiele:

```
Firewall-Log:
Paket wurde blockiert.

Webserver-Log:
Anfrage kam an und erzeugte 500.

Auth-Log:
Anmeldung wurde abgelehnt.

Paketmitschnitt:
TCP-Verbindung wurde aufgebaut.
```

Merksatz:

```
Mitschnitt und Logs ergänzen sich.
```

Typische Analysefragen

Bei einem Paketmitschnitt fragt man:

Sehe ich überhaupt Pakete?
Sehe ich die richtige Quelle?
Sehe ich das richtige Ziel?
Sehe ich den richtigen Port?
Sehe ich DNS vorher?
Sehe ich einen TCP-Handshake?
Sehe ich Reset oder Timeout?
Sehe ich TLS-Handshake?
Sehe ich Antwortpakete?
Sehe ich Wiederholungen?
Sehe ich ICMP-Fehler?
Passt die Richtung?

Merksatz:

Mitschnitt immer mit konkreter Frage auswerten.

Typisches Fehlerbild: Nur SYN-Wiederholungen

Wenn man nur SYN-Pakete sieht, aber keine SYN-ACK-Antwort, kann das bedeuten:

Ziel nicht erreichbar
Firewall droppt
falsche Ziel-IP
Routingproblem
Rückweg fehlt
Dienst oder Host antwortet nicht
NAT falsch

Merksatz:

Nur SYN-Wiederholungen deuten auf fehlende Antwort hin.

Typisches Fehlerbild: RST nach SYN

Wenn auf ein SYN direkt ein RST kommt, kann das bedeuten:

```
Port geschlossen
Dienst läuft nicht
Host lehnt Verbindung ab
Firewall lehnt aktiv ab
falscher Zielport
```

Merksatz:

```
RST nach SYN heißt:
Verbindung wird aktiv abgelehnt.
```

Typisches Fehlerbild: DNS NXDOMAIN

NXDOMAIN bedeutet:

```
Name existiert nicht.
```

Mögliche Ursachen:

```
falscher Name
DNS-Zone fehlt
Tippfehler
interner DNS nicht genutzt
falscher Suchsuffix
Split DNS falsch
```

Merksatz:

```
NXDOMAIN heißt:
DNS kennt diesen Namen nicht.
```

Typisches Fehlerbild: DHCP Discover ohne Offer

Wenn ein Client DHCP Discover sendet, aber kein Offer erhält, kann das bedeuten:

```
DHCP-Server nicht erreichbar
DHCP-Relay fehlt
VLAN falsch
DHCP-Server down
Firewall blockiert
Scope voll
falsches Netzwerk
```

Merksatz:

```
Discover ohne Offer:
Client findet keinen antwortenden DHCP-Server.
```

Typisches Fehlerbild: TLS Alert

Ein TLS Alert zeigt, dass der TLS-Aufbau ein Problem hat.

Mögliche Ursachen:

```
Zertifikatproblem
falscher Hostname
inkompatible TLS-Version
inkompatible Cipher Suite
Client oder Server bricht ab
mTLS-Zertifikat fehlt
```

Merksatz:

```
TLS Alert deutet auf Problem im TLS-Handshake hin.
```

Typisches Fehlerbild: Viele Retransmissions

Viele Retransmissions können bedeuten:

```
Paketverlust
Überlastung
Firewall blockiert einzelne Pakete
```

Rückwegproblem
WLAN-Probleme
MTU-Probleme
schlechte Verbindung

Merksatz:

Viele Wiederholungen zeigen,
dass Bestätigungen fehlen.

Typisches Fehlerbild: ARP ohne Antwort

ARP-Anfragen ohne Antwort können bedeuten:

Ziel ist nicht im lokalen Netz
Ziel ist offline
VLAN falsch
falsche IP-Adresse
falsche Netzmaske
Gateway nicht erreichbar
IP-Konflikt

Merksatz:

ARP ohne Antwort zeigt lokale Erreichbarkeitsprobleme.

Sicherheit beim Speichern von Mitschnitten

Paketmitschnitte können sensible Daten enthalten.

Deshalb:

nur notwendige Dauer mitschneiden
Filter nutzen
Dateien sicher speichern
Zugriff beschränken
Mitschnitte nach Zweck löschen
keine Mitschnitte unnötig weitergeben

personenbezogene Daten beachten

Merksatz:

Mitschnittdateien wie sensible Daten behandeln.

PCAP-Dateien

Paketmitschnitte werden häufig als PCAP oder PCAPNG gespeichert.

Diese Dateien können später geöffnet und analysiert werden.

Vorteile:

- spätere Analyse möglich
- Weitergabe an Fachabteilung möglich
- Vergleich mit Logs möglich
- Dokumentation eines Fehlerfalls

Achtung:

PCAP-Dateien können vertrauliche Informationen enthalten.

Merksatz:

PCAP ist praktisch,
aber sensibel.

Was ein Paketmitschnitt nicht automatisch liefert

Ein Paketmitschnitt zeigt nicht automatisch:

warum ein Benutzer keine Berechtigung hat
warum eine Anwendung intern Fehler wirft
warum ein Passwort falsch ist
warum ein Serverprozess abgestürzt ist
welche Firewall-Regel intern entschieden hat
ob ein Zertifikat fachlich richtig beantragt wurde

Dafür braucht man zusätzlich:

```
Logs
Konfiguration
Berechtigungsprüfung
Dienststatus
Fachwissen
```

Merksatz:

```
Paketmitschnitt zeigt Verkehr,
aber nicht jede Ursache.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was versteht man unter Sniffing?
- Wofür nutzt man einen Paketmitschnitt?
- Was ist Wireshark?
- Was ist tcpdump?
- Was ist Port Mirroring?
- Warum sieht man in einem geswitchten Netzwerk nicht automatisch allen Verkehr?
- Was ist der Unterschied zwischen Capture Filter und Display Filter?
- Was sieht man bei einem TCP-Handshake?
- Was bedeuten SYN, SYN-ACK und ACK?
- Was bedeutet TCP Reset?
- Was bedeuten Retransmissions?
- Warum sieht man bei HTTPS den Inhalt nicht einfach im Klartext?
- Was kann man bei DNS im Mitschnitt erkennen?
- Was zeigt DHCP-DORA im Mitschnitt?
- Warum sind Paketmitschnitte sensibel?
```

Typische Prüfungsfallen

```
Sniffing zeigt echten Netzwerkverkehr.
```

Sniffing ist datenschutzrelevant.

Wireshark ist grafisch.

tcpdump ist Kommandozeile.

In geswitchten Netzen sieht man nicht automatisch alles.

Port Mirroring kopiert Verkehr auf Analyseport.

Promiscuous Mode allein reicht im Switch-Netz oft nicht.

Capture Filter begrenzt Aufnahme.

Display Filter begrenzt Anzeige.

Was nicht aufgezeichnet wurde,
kann später nicht analysiert werden.

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.

TLS schützt Inhalte.

HTTP ist lesbar,
HTTPS normalerweise nicht.

FTP und Telnet sind im Mitschnitt gefährlich sichtbar.

Mitschnittort ist entscheidend.

Logs und Mitschnitt ergänzen sich.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Sniffing	Mitschneiden von Netzwerkverkehr
Paketmitschnitt	Aufzeichnung von Paketen
Wireshark	grafisches Analysewerkzeug
tcpdump	Kommandozeilenwerkzeug für Mitschnitte
tshark	Wireshark auf Kommandozeile
PCAP	Datei mit Paketmitschnitt
Port Mirroring	Kopieren von Switch-Verkehr auf Analyseport
SPAN	Port-Mirroring-Begriff bei Switches
Promiscuous Mode	Netzwerkkarte nimmt fremde Frames an
Capture Filter	Filter vor der Aufnahme
Display Filter	Filter für Anzeige nach Aufnahme
SYN	TCP-Verbindungsstart
SYN-ACK	TCP-Antwort des Servers
ACK	Bestätigung
RST	Reset, aktive Ablehnung oder Abbruch
Retransmission	erneutes Senden eines Pakets
ARP	IPv4-Adresse zu MAC-Adresse
ICMP	Diagnose- und Fehlermeldungsprotokoll
SNI	Hostname im TLS-Handshake
TLS Alert	Fehlermeldung im TLS-Handshake
NXDOMAIN	DNS-Name existiert nicht
DORA	DHCP Discover, Offer, Request, Acknowledge

IHK-sichere Kurzformulierung

Sniffing bezeichnet das Mitschneiden und Analysieren von Netzwerkverkehr. Mit Werkzeugen wie Wireshark, tcpdump oder Paketmitschnitten auf Firewalls kann geprüft werden, welche Pakete tatsächlich gesendet und empfangen werden. Dabei lassen sich unter anderem MAC-Adressen, IP-

Adressen, Ports, Protokolle, TCP-Handshakes, DNS-Anfragen, DHCP-Abläufe, ICMP-Meldungen, TLS-Handshakes und Wiederholungen erkennen. In geswitchten Netzwerken sieht ein Client nicht automatisch den gesamten Verkehr; dafür ist häufig Port Mirroring oder ein Mitschnitt an der richtigen Stelle nötig. Paketmitschnitte können sensible Daten enthalten und müssen deshalb sorgfältig und nur mit berechtigtem Zweck eingesetzt werden.

Merksätze

Sniffing = Netzwerkverkehr mitschneiden.

Paketmitschnitt zeigt echten Verkehr.

Wireshark ist grafisch.

tcpdump ist Kommandozeile.

tshark ist Wireshark für die Kommandozeile.

PCAP-Dateien enthalten Mitschnitte.

Mitschnitte können sensible Daten enthalten.

In geswitchten Netzen sieht man nicht automatisch alles.

Port Mirroring kopiert Verkehr.

Promiscuous Mode reicht allein oft nicht.

Capture Filter begrenzt Aufnahme.

Display Filter begrenzt Anzeige.

Mitschnittort ist entscheidend.

MAC-Adressen gehören zu Schicht 2.

IP-Adressen gehören zu Schicht 3.

Ports gehören zu Schicht 4.

DNS gehört zu Schicht 7.

TCP hat Handshake.

UDP hat keinen Handshake.

SYN startet TCP-Verbindung.

SYN-ACK antwortet.

ACK bestätigt.

RST lehnt ab oder beendet.

Retransmission bedeutet erneutes Senden.

ARP löst IPv4 zu MAC auf.

ICMP liefert Diagnosehinweise.

DHCP-DORA ist im Mitschnitt sichtbar.

TLS schützt Inhalte.

HTTP ist lesbar.

HTTPS ist normalerweise nicht lesbar.

FTP und Telnet sind unsicher,
weil Inhalte sichtbar sein können.

Logs und Paketmitschnitt zusammen auswerten.