20.17 Spezialtrainer – Standardports und Dienste

Dieser Spezialtrainer ist eine zusätzliche Übungsseite.

Der allgemeine Netzwerktechnik-Trainer ist bereits abgeschlossen. Diese Seite dient nur als vertiefender Trainer für Standardports, Dienste, TCP, UDP und typische Port-Fehlerbilder.

Ziel ist, Portnummern nicht nur auswendig zu lernen, sondern in Prüfungsaufgaben richtig anzuwenden.

Merksatz:

```
IP findet den Host.
Port findet den Dienst.
Protokoll sagt,
ob TCP oder UDP gemeint ist.
```

Lernziele

Nach dieser Seite solltest du sicher können:

```
- wichtige Standardports nennen
- TCP und UDP bei Ports unterscheiden
- typische Dienste zuordnen
- Firewall-Regeln genauer formulieren
- Port-Fehlerbilder erkennen
- erklären,
  warum ping keinen Porttest ersetzt
- unsichere Dienste erkennen
- sichere Alternativen nennen
```

Kurzüberblick: wichtigste Ports

Dienst	Protokoll und Port	Zweck
FTP	TCP 21	Dateiübertragung, unverschlüsselt
SSH	TCP 22	sichere Fernadministration
SFTP	TCP 22	Dateiübertragung über SSH
SMTP	TCP 25	E-Mail-Übertragung

Dienst	Protokoll und Port	Zweck
DNS	UDP/TCP 53	Namensauflösung
DHCP Server	UDP 67	DHCP-Server
DHCP Client	UDP 68	DHCP-Client
HTTP	TCP 80	Web unverschlüsselt
POP3	TCP 110	E-Mail-Abruf
NTP	UDP 123	Zeitsynchronisation
IMAP	TCP 143	E-Mail-Abruf und Synchronisation
SNMP	UDP 161	Netzwerkmanagement
HTTPS	TCP 443	Web verschlüsselt
SMB	TCP 445	Datei- und Druckfreigaben
SMTPS	TCP 465	SMTP über TLS
IMAPS	TCP 993	IMAP über TLS
POP3S	TCP 995	POP3 über TLS
RDP	TCP 3389	Remote Desktop

Merksatz:

```
Portnummer immer zusammen mit TCP oder UDP lernen.
```

Aufgabe 1

Welchen Port nutzt SSH typischerweise?

Antwort anzeigen

SSH nutzt typischerweise:

```
TCP 22
```

SSH steht für:

```
Secure Shell
```

Nutzung:

```
sichere Fernadministration
```

```
verschlüsselte Kommandozeile
```

```
SFTP
```

Merksatz:

```
SSH = TCP 22.
```

Aufgabe 2

Welchen Port nutzt HTTPS typischerweise?

Antwort anzeigen

HTTPS nutzt typischerweise:

```
TCP 443
```

HTTPS bedeutet:

```
HTTP über TLS
```

Nutzung:

```
verschlüsselte Webkommunikation
```

Merksatz:

```
HTTPS = TCP 443.
```

Aufgabe 3

Welchen Port nutzt HTTP typischerweise?

Antwort anzeigen

HTTP nutzt typischerweise:

```
TCP 80
```

Wichtig:

```
HTTP ist unverschlüsselt.
```

Besser für sensible Daten:

```
HTTPS über TCP 443
```

Merksatz:

```
HTTP = TCP 80.
HTTPS = TCP 443.
```

Aufgabe 4

Welchen Port nutzt DNS?

Antwort anzeigen

DNS nutzt:

```
UDP 53
```

und bei Bedarf auch:

```
TCP 53
```

Typisch:

```
normale DNS-Abfragen häufig UDP 53

größere Antworten,
Zonentransfers
oder bestimmte Fälle TCP 53
```

Merksatz:

```
DNS = UDP/TCP 53.
```

Aufgabe 5

Welche Ports nutzt DHCP?

Antwort anzeigen

DHCP nutzt:

```
UDP 67 für den DHCP-Server

UDP 68 für den DHCP-Client
```

Merksatz:

```
DHCP = UDP 67 und UDP 68.
```

Aufgabe 6

Welchen Port nutzt SMB typischerweise?

Antwort anzeigen

SMB nutzt typischerweise:

```
TCP 445
```

Nutzung:

```
Datei- und Druckfreigaben

Netzlaufwerke

Windows-Freigaben
```

Merksatz:

```
SMB = TCP 445.
```

Aufgabe 7

Welchen Port nutzt RDP typischerweise?

Antwort anzeigen

RDP nutzt typischerweise:

```
TCP 3389
```

RDP steht für:

```
Remote Desktop Protocol
```

Merksatz:

```
RDP = TCP 3389.
```

Aufgabe 8

Welchen Port nutzt NTP?

Antwort anzeigen

NTP nutzt typischerweise:

```
UDP 123
```

NTP steht für:

```
Network Time Protocol
```

Aufgabe:

```
Zeitsynchronisation
```

Merksatz:

```
NTP = UDP 123.
```

Aufgabe 9

Welchen Port nutzt SNMP?

Antwort anzeigen

SNMP nutzt typischerweise:

```
UDP 161
```

SNMP steht für:

```
Simple Network Management Protocol
```

Aufgabe:

```
Netzwerkgeräte überwachen und verwalten
```

Merksatz:

> SNMP = UDP 161.

Aufgabe 10

Ordne die Webports zu.

Dienst	Protokoll und Port
HTTP	?
HTTPS	?

Antwort anzeigen

Dienst	Protokoll und Port
HTTP	TCP 80
HTTPS	TCP 443

Merksatz:

> HTTP unverschlüsselt.
> HTTPS verschlüsselt mit TLS.

Aufgabe 11

Ordne die E-Mail-Protokolle zu.

Dienst	Protokoll und Port
SMTP	?
POP3	?
IMAP	?
SMTPS	?
POP3S	?
IMAPS	?

Antwort anzeigen

Dienst	Protokoll und Port
SMTP	TCP 25
POP3	TCP 110
IMAP	TCP 143
SMTPS	TCP 465
POP3S	TCP 995
IMAPS	TCP 993

Merksatz:

SMTP sendet.
POP3 und IMAP empfangen.
S am Ende bedeutet verschlüsselte Variante.

Aufgabe 12

Was macht SMTP?

Antwort anzeigen

SMTP steht für:

Simple Mail Transfer Protocol

Aufgabe:

E-Mails senden und zwischen Mailservern übertragen.

Typischer Port:

TCP 25

Merksatz:

SMTP sendet E-Mails.

Aufgabe 13

Was macht POP3?

Antwort anzeigen

POP3 steht für:

Post Office Protocol Version 3

Aufgabe:

E-Mails vom Server abrufen.

Typischer Port:

TCP 110

Verschlüsselte Variante:

POP3S über TCP 995

Merksatz:

POP3 ruft E-Mails ab.

Aufgabe 14

Was macht IMAP?

Antwort anzeigen

IMAP steht für:

Internet Message Access Protocol

Aufgabe:

E-Mails auf dem Server abrufen und synchron verwalten.

Typischer Port:

TCP 143

Verschlüsselte Variante:

IMAPS über TCP 993

Merksatz:

IMAP synchronisiert E-Mails.

Aufgabe 15

Was ist der Unterschied zwischen POP3 und IMAP?

Antwort anzeigen

POP3:

einfacher E-Mail-Abruf

traditionell eher Herunterladen vom Server

IMAP:

serverseitige Verwaltung

Synchronisation über mehrere Geräte

Ordnerstruktur bleibt serverseitig erhalten

Merksatz:

POP3 ruft ab.
IMAP synchronisiert.

Aufgabe 16

Ordne Dateiübertragungsprotokolle zu.

Dienst	Protokoll und Port	Sicherheit
FTP	?	?
SFTP	?	?
FTPS	?	?

Antwort anzeigen

Dienst	Protokoll und Port	Sicherheit
FTP	TCP 21	unverschlüsselt
SFTP	TCP 22	über SSH verschlüsselt
FTPS	TCP 21 oder weitere Ports je nach Modus	FTP mit TLS

Merksatz:

FTP ist unverschlüsselt.
SFTP nutzt SSH.
FTPS ist FTP mit TLS.

Aufgabe 17

Warum ist FTP unsicher?

Antwort anzeigen

FTP ist unsicher, weil es klassisch unverschlüsselt überträgt.

Risiken:

```
Zugangsdaten können mitgelesen werden

Daten können mitgelesen werden

Man-in-the-Middle möglich
```

Bessere Alternativen:

```
SFTP

FTPS

HTTPS-basierter Upload
```

Merksatz:

```
FTP nicht für sensible Daten verwenden.
```

Aufgabe 18

Was ist der Unterschied zwischen SFTP und FTPS?

Antwort anzeigen

SFTP:

```
Dateiübertragung über SSH

typischerweise TCP 22
```

FTPS:

```
FTP mit TLS-Verschlüsselung

basiert auf FTP
```

Wichtig:

```
SFTP und FTPS sind nicht dasselbe.
```

Merksatz:

```
SFTP = SSH.
FTPS = FTP mit TLS.
```

Aufgabe 19

Warum ist „Port 53 freigeben“ ungenau?

Antwort anzeigen

Die Angabe ist ungenau, weil nicht klar ist, ob TCP 53, UDP 53 oder beides gemeint ist.

Bei Firewall-Regeln müssen angegeben werden:

```
Quelle

Ziel

Protokoll

Port

Aktion
```

Merksatz:

Portnummer ohne TCP oder UDP ist unvollständig.

Aufgabe 20

Warum ist „Port 443 erlauben“ in einer Firewall-Regel noch nicht vollständig?

Antwort anzeigen

Es fehlen wichtige Angaben:

Quelle

Ziel

Protokoll

Richtung

Aktion

Zweck

Besser:

Quelle:
Internet

Ziel:
Webserver-DMZ

Protokoll:
TCP

Port:
443

Aktion:
erlauben

Zweck:
HTTPS-Zugriff

Merksatz:

Firewall-Regeln brauchen mehr als nur eine Portnummer.

Aufgabe 21

Was bedeutet LISTEN bei einem TCP-Port?

Antwort anzeigen

LISTEN bedeutet:

Ein Dienst wartet auf eingehende Verbindungen.

Beispiel:

Webserver lauscht auf TCP 443.

Merksatz:

LISTEN = Dienst wartet auf Verbindung.

Aufgabe 22

Was bedeutet ESTABLISHED bei TCP?

Antwort anzeigen

ESTABLISHED bedeutet:

Eine TCP-Verbindung besteht aktiv.

Beispiel:

Client hat eine HTTPS-Verbindung zum Server aufgebaut.

Merksatz:

ESTABLISHED = Verbindung besteht.

Aufgabe 23

Was bedeutet SYN_SENT?

Antwort anzeigen

SYN_SENT bedeutet:

Der Client hat einen TCP-Verbindungsaufbau gestartet
und wartet auf Antwort.

Wenn es hängen bleibt, sind möglich:

Ziel nicht erreichbar

Port blockiert

Dienst antwortet nicht

Firewall blockiert

Routingproblem

Merksatz:

```
SYN_SENT zeigt:
Anfrage raus,
Antwort fehlt.
```

Aufgabe 24

Was bedeutet TIME_WAIT?

Antwort anzeigen

TIME_WAIT ist ein TCP-Zustand nach dem Schließen einer Verbindung.

Er sorgt dafür, dass verspätete Pakete einer alten Verbindung nicht mit neuen Verbindungen verwechselt werden.

Merksatz:

```
TIME_WAIT nach Verbindungsende ist normal.
```

Aufgabe 25

Ein Server ist per ping erreichbar, aber TCP 22 ist nicht erreichbar.

Was ist wahrscheinlich?

Antwort anzeigen

Ping prüft ICMP. TCP 22 ist SSH.

Mögliche Ursachen:

```
SSH-Dienst läuft nicht

SSH lauscht auf anderem Port

lokale Firewall blockiert
```

Netzwerkfirewall blockiert

Zugriff nur aus bestimmten Netzen erlaubt

Dienst lauscht nur auf localhost

Merksatz:

Host erreichbar heißt nicht:
Dienst erreichbar.

Aufgabe 26

Ein Webserver ist intern auf TCP 443 erreichbar, aber nicht von außen.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

öffentliche IP

DNS

Portweiterleitung

Router-Firewall

lokale Firewall

Dienststatus

doppeltes NAT

CGNAT

```
Provider blockiert Port
```

Merksatz:

```
Intern ja,
extern nein:
NAT,
Firewall,
DNS
und öffentliche IP prüfen.
```

Aufgabe 27

Ein Dienst läuft, lauscht aber nur auf 127.0.0.1.

Was bedeutet das?

Antwort anzeigen

127.0.0.1 ist localhost.

Wenn ein Dienst nur auf 127.0.0.1 lauscht, ist er nur lokal auf dem Server erreichbar.

Andere Geräte können ihn nicht direkt erreichen.

Prüfen:

```
Bind-Adresse

Dienstkonfiguration

Firewall
```

Merksatz:

```
127.0.0.1 = nur lokal.
```

Aufgabe 28

Ein Dienst lauscht auf 0.0.0.0.

Was bedeutet das?

Antwort anzeigen

0.0.0.0 bedeutet bei einem lauschenden Dienst:

```
Der Dienst lauscht auf allen IPv4-Schnittstellen des Systems.
```

Wichtig:

```
Ob der Dienst erreichbar ist,
hängt zusätzlich von Firewall,
Routing,
NAT
und Berechtigungen ab.
```

Merksatz:

```
0.0.0.0 = alle IPv4-Interfaces.
```

Aufgabe 29

Warum ersetzt ping keinen Porttest?

Antwort anzeigen

ping prüft ICMP-Erreichbarkeit.

ping prüft nicht:

```
TCP-Port

UDP-Port
```

```
Dienststatus

Anwendung

Anmeldung

Berechtigungen
```

Beispiel:

```
Ein Server kann auf ping antworten,
obwohl TCP 443 blockiert ist.
```

Merksatz:

```
ping prüft den Host,
nicht den Dienst.
```

Aufgabe 30

Welche Werkzeuge oder Methoden eignen sich zur Portprüfung?

Antwort anzeigen

Mögliche Prüfungen:

```
Dienststatus prüfen

Firewall-Logs prüfen

Porttest vom Client aus

ss oder netstat auf dem Server

curl für HTTP/HTTPS
```

Verbindungsprüfung mit geeigneten Tools

Logs des Dienstes prüfen

Wichtig:

Immer TCP oder UDP beachten.

Merksatz:

Portprüfung braucht Richtung,
Ziel,
Protokoll
und Dienststatus.

Aufgabe 31

Warum sollte RDP nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

RDP ist ein häufiges Angriffsziel.

Risiken:

Brute Force

Credential Stuffing

Exploits

unberechtigter Fernzugriff

Besser:

```
VPN

RDP-Gateway

MFA

Zugriff nur von bekannten Quellnetzen

Logging
```

Merksatz:

```
RDP nicht offen ins Internet stellen.
```

Aufgabe 32

Warum sollte SMB nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

SMB ist für Datei- und Druckfreigaben gedacht und sollte nicht öffentlich erreichbar sein.

Risiken:

```
Datenabfluss

Malware-Ausbreitung

Brute Force

Ausnutzung von Schwachstellen

Zugriff auf interne Freigaben
```

Merksatz:

SMB gehört nicht offen ins Internet.

Aufgabe 33

Warum sollte Telnet nicht verwendet werden?

Antwort anzeigen

Telnet überträgt unverschlüsselt.

Risiken:

Zugangsdaten können mitgelesen werden

Sitzungen können mitgelesen werden

Man-in-the-Middle-Angriffe möglich

Sichere Alternative:

SSH

Merksatz:

Telnet unsicher,
SSH sicherer.

Aufgabe 34

Ordne sichere und unsichere Varianten zu.

Unsicherer Dienst	Sicherere Alternative
Telnet	?
FTP	?
HTTP	?

Unsicherer Dienst	Sicherere Alternative
POP3	?
IMAP	?

Antwort anzeigen

Unsicherer Dienst	Sicherere Alternative
Telnet	SSH
FTP	SFTP oder FTPS
HTTP	HTTPS
POP3	POP3S
IMAP	IMAPS

Merksatz:

> Unverschlüsselte Dienste vermeiden,
> wenn sensible Daten übertragen werden.

Aufgabe 35

Welcher Port passt zu welchem Dienst?

Port	Dienst
22	?
53	?
67/68	?
80	?
123	?
443	?
445	?
3389	?

Antwort anzeigen

Port	Dienst
22	SSH / SFTP
53	DNS
67/68	DHCP
80	HTTP
123	NTP
443	HTTPS
445	SMB
3389	RDP

Aufgabe 36

Welcher Dienst passt zu welchem Port?

Dienst	Port
SSH	?
DNS	?
DHCP	?
HTTP	?
HTTPS	?
SMB	?
RDP	?
NTP	?

Antwort anzeigen

Dienst	Port
SSH	TCP 22
DNS	UDP/TCP 53
DHCP	UDP 67/68
HTTP	TCP 80
HTTPS	TCP 443
SMB	TCP 445

Dienst	Port
RDP	TCP 3389
NTP	UDP 123

Aufgabe 37

Ein DNS-Server ist nicht erreichbar. Welche Firewall-Regel könnte fehlen?

Antwort anzeigen

Möglicherweise fehlt:

```
UDP 53
```

und je nach Fall auch:

```
TCP 53
```

Saubere Regel:

```
Quelle:
Clientnetz

Ziel:
DNS-Server

Protokoll:
UDP und TCP

Port:
53

Aktion:
erlauben
```

Merksatz:

```
DNS braucht meistens UDP 53,
TCP 53 mitdenken.
```

Aufgabe 38

Ein Client erhält keine DHCP-Adresse. Welche Ports sind relevant?

Antwort anzeigen

Relevant sind:

```
UDP 67

UDP 68
```

Zusätzlich prüfen:

```
DHCP-Server

VLAN

DHCP-Relay

DHCP-Scope

Firewall-Regeln
```

Merksatz:

```
DHCP = UDP 67 und 68.
```

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Ein Server ist pingbar,
aber die Webseite funktioniert nicht.
Was prüfen Sie?

Antwort A:

Der Server ist erreichbar,
also ist alles gut.

Antwort B:

ping prüft nur ICMP.
Für die Webseite müssen TCP 80 oder TCP 443,
Webdienst,
Firewall,
TLS
und Anwendung geprüft werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort unterscheidet Host-Erreichbarkeit
und Dienst-Erreichbarkeit.

Merksatz:

ping ist kein Diensttest.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Warum ist eine Firewall-Regel mit „Port 443 erlauben“ unvollständig?

Antwort A:

Weil man noch mehr schreiben kann.

Antwort B:

Für eine saubere Firewall-Regel fehlen Quelle,
Ziel,
Protokoll,
Richtung,
Aktion
und Zweck.
Außerdem muss TCP 443 genannt werden,
weil Portnummern ohne Transportprotokoll ungenau sind.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt fachlich,
welche Angaben in einer Regel fehlen.

Merksatz:

Firewall-Regel vollständig formulieren.

Mini-Prüfung: Ports auswendig

Dienst	Protokoll und Port
FTP	TCP 21
SSH	TCP 22
SFTP	TCP 22

Dienst	Protokoll und Port
SMTP	TCP 25
DNS	UDP/TCP 53
DHCP Server	UDP 67
DHCP Client	UDP 68
HTTP	TCP 80
POP3	TCP 110
NTP	UDP 123
IMAP	TCP 143
SNMP	UDP 161
HTTPS	TCP 443
SMB	TCP 445
SMTPS	TCP 465
IMAPS	TCP 993
POP3S	TCP 995
RDP	TCP 3389

Mini-Prüfung: Fehlerbilder

Fehlerbild	Wahrscheinlichstes Thema
ping geht, SSH nicht	TCP 22, SSH-Dienst, Firewall
ping geht, HTTPS nicht	TCP 443, Webdienst, Firewall, TLS
DNS antwortet nicht	UDP/TCP 53
DHCP funktioniert nicht	UDP 67/68, DHCP, VLAN, Relay
SMB-Freigabe nicht erreichbar	TCP 445, Firewall, SMB-Dienst
RDP geht nicht	TCP 3389, RDP-Dienst, Firewall
Dienst nur lokal erreichbar	bindet nur an 127.0.0.1
Port offen, Login scheitert	Authentifizierung
Port offen, Zugriff verweigert	Autorisierung
SYN_SENT bleibt stehen	Antwort fehlt, Firewall, Routing oder Dienst

Typische Prüfungsfallen

Falle	Richtig denken

Portnummer ohne TCP/UDP	unvollständig
ping ersetzt Porttest	falsch
DNS nur UDP	meistens UDP, aber TCP mitdenken
SFTP und FTPS gleichsetzen	falsch
HTTP und HTTPS gleichsetzen	falsch
RDP ins Internet öffnen	Sicherheitsrisiko
SMB ins Internet öffnen	Sicherheitsrisiko
Dienst läuft = Dienst erreichbar	nicht automatisch
127.0.0.1 als Bind-Adresse übersehen	nur lokal erreichbar
Firewall-Regel ohne Quelle und Ziel	unvollständig

IHK-sichere Kurzformulierung

Ports gehören zur OSI-Schicht 4 und werden von TCP oder UDP genutzt, um Daten dem richtigen Dienst oder Prozess zuzuordnen. Eine IP-Adresse identifiziert den Host, der Port den Dienst. Standardports sollten immer zusammen mit dem Transportprotokoll gelernt werden, zum Beispiel SSH TCP 22, DNS UDP/TCP 53, HTTP TCP 80, HTTPS TCP 443, SMB TCP 445 und RDP TCP 3389. ping prüft nur ICMP-Erreichbarkeit und ersetzt keinen Port- oder Diensttest. Für Firewall-Regeln reicht eine Portnummer allein nicht aus; benötigt werden Quelle, Ziel, Protokoll, Port, Richtung, Aktion und Zweck.

Merksätze

```
IP findet den Host.

Port findet den Dienst.

Ports gehören zu Schicht 4.

TCP und UDP unterscheiden.

Portnummer ohne TCP oder UDP ist unvollständig.

SSH = TCP 22.

SFTP = TCP 22.

DNS = UDP/TCP 53.
```

DHCP = UDP 67 und 68.

HTTP = TCP 80.

HTTPS = TCP 443.

SMB = TCP 445.

RDP = TCP 3389.

NTP = UDP 123.

SMTP sendet E-Mails.

IMAP synchronisiert E-Mails.

POP3 ruft E-Mails ab.

FTP ist unverschlüsselt.

SFTP nutzt SSH.

FTPS ist FTP mit TLS.

Telnet vermeiden,
SSH nutzen.

HTTP vermeiden,
HTTPS nutzen.

ping ist kein Porttest.

Host erreichbar heißt nicht:
Dienst erreichbar.

LISTEN heißt:
Dienst wartet.

ESTABLISHED heißt:

Verbindung besteht.

SYN_SENT heißt:
Anfrage raus,
Antwort fehlt.

127.0.0.1 heißt:
nur lokal.

0.0.0.0 heißt:
alle IPv4-Interfaces.

RDP nicht offen ins Internet stellen.

SMB nicht offen ins Internet stellen.

Firewall-Regeln brauchen Quelle,
Ziel,
Protokoll,
Port,
Richtung,
Aktion
und Zweck.