CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

OSI, TCP, UDP

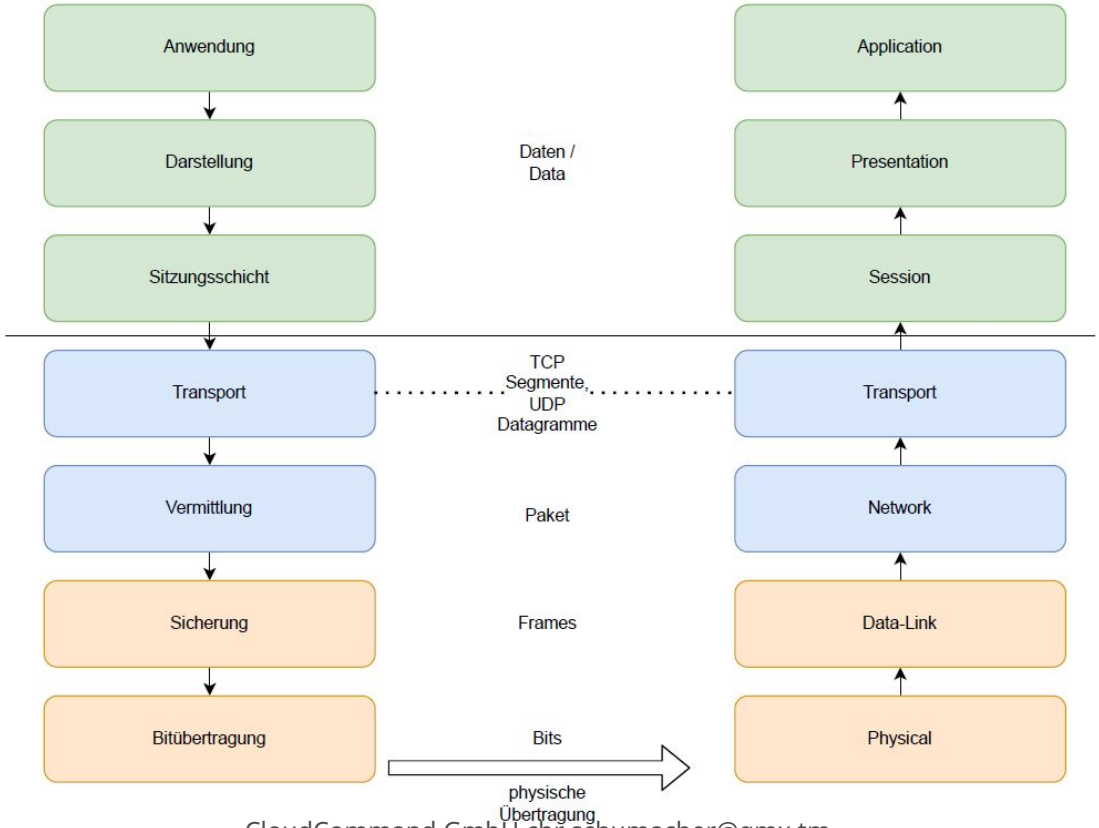
CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

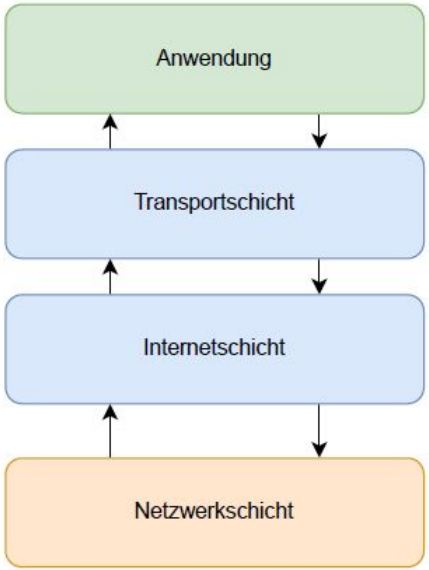
01 OSI
02 TCP/UDP
03 Sockets
04 DNS

01 OSI

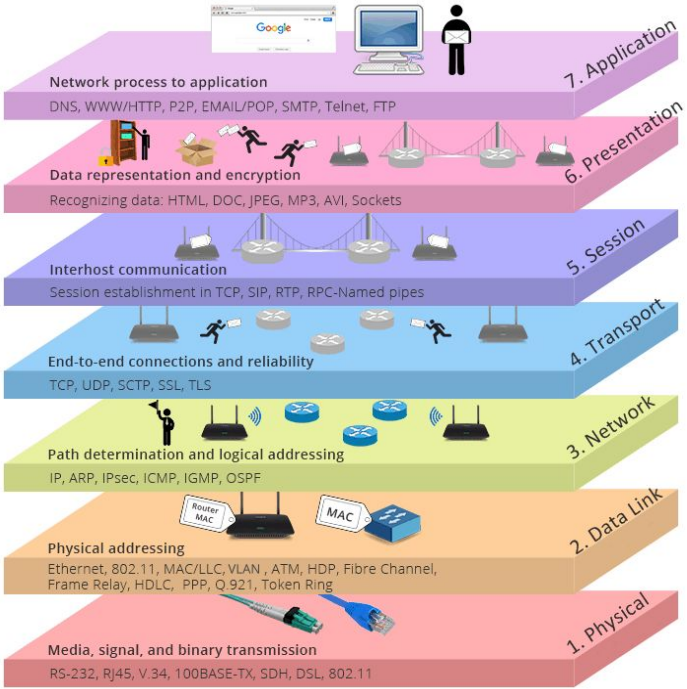
OSI


Anwendung
Darstellung
Sitzungsschicht
Transport
Vermittlung
Sicherung
Bitübertragung
Daten / Data
TCP Segmente, UDP Datagramme
Paket
Frames
Bits
physische Übertragung
Application
Presentation
Session
Transport
Network
Data-Link
Physical

TCP/IP


Anwendung
Transportschicht
Internetschicht
Netzwerkschicht

OSI



OSI

Schicht	Nr.	Exploit / Angriff	Maßnahme
Anwendung	7	SQL-Injection, Cross-site Scripting, Remote Code Execution, Phishing, Buffer Overflows, File Upload, Fehlkonfiguration durch Updates	Blacklisting, Validierung, Compliance
Darstellung	6	Injection, Manipulation des Datenformats, Reverse Engineering von Serialisierung	Validierung von Eingaben, Blacklisting/Whitelisting
Sitzung	5	Network-Scan, Session-Hijacking, Token-Spoofing, Token Brute-Force, RPC, Session Flooding	Session Limit,Token-Invalidierung, TLS/SSL, Random Session-IDs, Secure Logout

OSI

Schicht	Nr.	Exploit / Angriff	Maßnahme
Transport	4	SYN-Flood, UDP-Packet-Flood, ACK-Loop, TCP-Session-Hijacking	SQR (Sequenznummer Randomisierung), Limitierung der Anfragen
Vermittlung	3	MITM (Smurfing, Flooding) Onlinestatus abfragen	IPSec, Segmentierung (Content Delivery Networks), ACL
Sicherung	2	MAC Spoofing, Flooding	Anzahl zulässiger MACs pro Port, Segmentierung
Bitübertragung	1	(Signalstörung), Sniffing	isolierte Kabel, Zugriffskontrolle

02 TCP/UDP

TCP/UDP

TCP (Transmission Control Protocol)

- Verbindungsorientiert
- Sequenzierung
- 3-Way-Handshake
- ACK-Pakete

UDP (User Datagram Protocol)

- Verbindungslos
- Effizient
- Kein erzwungener Handshake
- Paketverlust wird in kauf genommen

Ports

- Well-Known Ports (0-1023)
- Registered Ports (1024 – 49151)
- Dynamische/Private Ports (49152-65535)

Ports

Port	Service	Funktion
20	FTP	Datenübertragung
21	FTP	Verbindung
22	SSH	Fernzugriff per Secure Shell
23	Telnet	Remote-Anmeldung (unverschlüsselt
25	SMTP	Versenden von E-Mails an Server
53	DNS	Übersetzen von Web-Adressen
67/68	DHCP	Host-Konfiguration
80	HTTP	Website (unverschlüsselt)

Ports

Port	Service	Funktion
88	Kerberos	Authentifizierungssystem von Microsoft
110	POP3	Synchronisieren von E-Mails
143	IMAP	Zugriff auf E-Mails ohne lokale Synchro
194	IRC	Textbasiertes Chatsystem
443	HTTPS	Website mit TLS/SSL
445	SMB	Teilen von Netzwerkressourcen
587	S-SMTP	Verschlüsseltes SMTP
993	S-IMAP	Verschlüsseltes IMAP

Ports

Port	Service	Funktion
995	S-POP3	Verschlüsseltes POP3
3306	MySQL	Datenbanken auf MySQL-Basis
3389	RDP	Fernsteuerung von Computern mit geteilten Ressourcen
5900	VNC	Fernsteuerung von Computern

03 Sockets

Sockets

Sockets sind die Kommunikationsendpunkte von Programmen.
Die Adresse eines Sockets ergibt sich aus:

- Anwendung (ausführender Prozess)
- IP-Adresse
- Port + Protokoll
    - Datagram-Sockets (Verbindungslos)
    - Stream-Sockets (Verbindungsorientiert)

Sockets können Daten senden als auch empfangen und werden von der jeweiligen Anwendung bei Bedarf geöffnet und wieder geschlossen. Ähnlich wie bei IP-Adressen und Ports unterscheidet man zwischen lokalen und remote Sockets

Sockets

Code Beispiel:

```
Socket mysocket = getSocket(type = "TCP")
connect(mysocket, address = "203.0.113.0", port = "80")
send(mysocket, "Hello, world!")
close(mysocket)
```

04 DNS

DNS

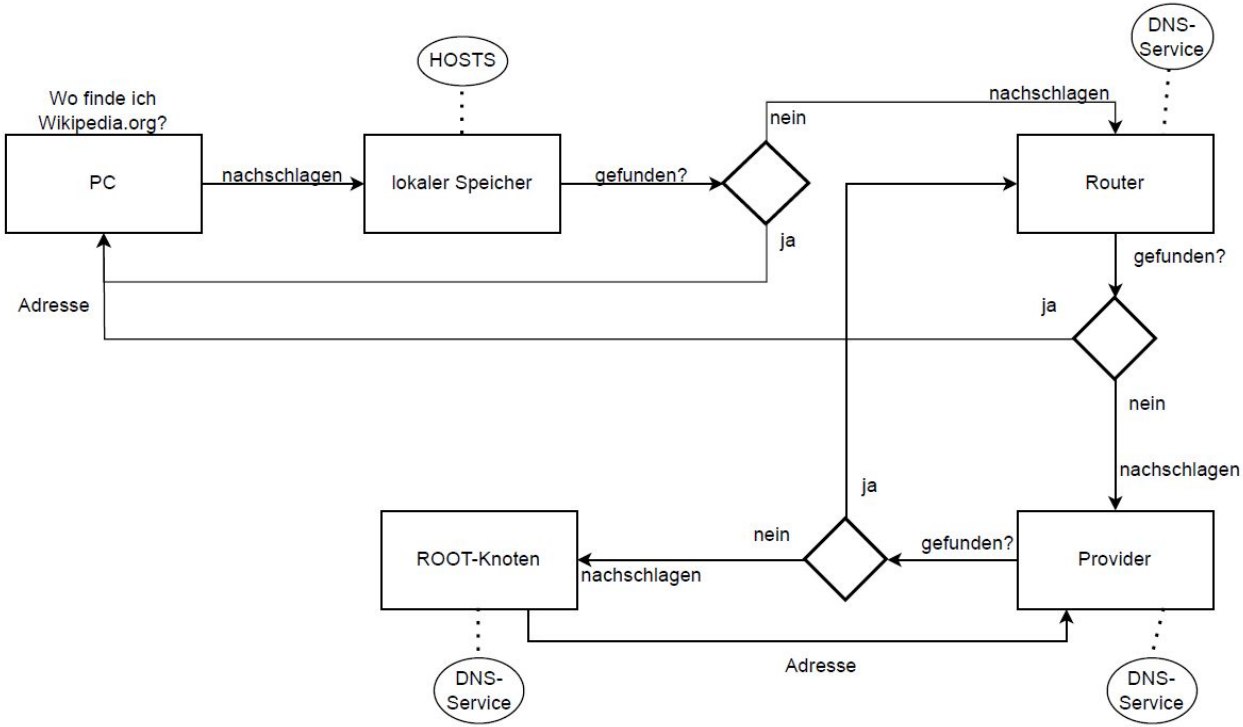
DNS (Domain Name System) ist das Nachschlagewerk für Domains. Einem Namen wird eine IP-Adresse zugeordnet, die im Anschluss kontaktiert werden kann.

Die verknüpften Einträge werden nach je nach Zweck im Cache gespeichert oder dauerhaft angelegt, wenn sich das Gerät in der zugewiesenen Zone befindet.

DNS

Eintrag / Record	Funktion
SOA-Record	Autoritätsursprung, Seriennummern, TTL
NS-Record	Verknüpfte Nameserver
A-Record	Verweis auf IPv4-Adresse
AAAA-Record	Verweis auf IPv6-Adresse
CNAME-Record	Alias für eine Domain
MX-Record	Mail Austausch
PTR-Record	Zuweisung eines Namens für IP (Reverse DNS)
TXT-Record	Frei wählbarer Text (Alle anderen Zwecke)

DNS


Wo finde ich
Wikipedia.org?
PC
nachschlagen
HOSTS
lokaler Speicher
gefunden?
nein
ja
nachschlagen
DNS-
Service
Router
gefunden?
ja
Adresse
nein
nachschlagen
ja
ROOT-Knoten
nachschlagen
nein
gefunden?
Provider
Adresse
DNS-
Service
DNS-
Service

DANKE!

Gibt es noch Fragen?

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm