

# ZSL

Zentrum für Schulqualität  
und Lehrerbildung  
Baden-Württemberg

## Network Security Concepts

### 35.000

Mails mit Schadprogrammen wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

### 76 %

ist der Anteil unerwünschter SPAM-MAILS an allen in den Netzen des Bundes eingegangenen Mails

### 52.000

WEBSEITEN

wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

**+++ BSI Bericht 2020 +++**

durchschnittlich  
**322.000** Schadprogramm-  
Varianten pro Tag  
bis zu  
**20.000**  
BOT-INFektionen  
deutscher Systeme

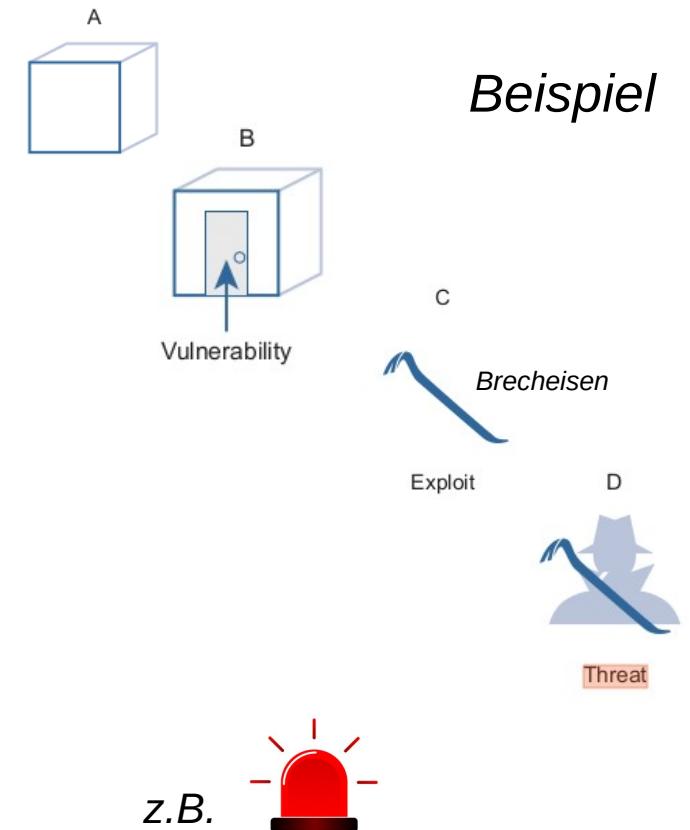
täglich  
**24,3 MIO.**  
Patientendatensätze  
waren Schätzungen zufolge international frei im Internet zugänglich

Cisco  
Networking Academy

Quelle BSI (3.12.2020):  
[https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020/pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020/pdf?__blob=publicationFile&v=2)

# Fachbegriffe der Netzwerksicherheit im Überblick

<b>Assets</b>	Alle Vermögenswerte einer Organisation: z.B. Personen, Geräte, Daten etc.
<b>Vulnerability</b>	Sicherheitslücke / Schwachstelle, die ausgenutzt werden könnte
<b>Exploit</b>	Mechanismus / Tool zur Ausnutzung einer Vulnerability / Sicherheitslücke
<b>Threat</b>	Alle Umstände oder Ereignisse, die die Assets / Vermögenswerte nachteilig beeinflussen ( <i>potentielle Gefahr</i> )
<b>Mitigation</b>	Maßnahme zur Verhinderung bzw. Verringerung eines Threats oder eines Risikos (z.B. Port Security, ACLs etc.)
<b>Risk</b>	Bewertung der Wahrscheinlichkeit, dass eine Sicherheitslücke ausgenutzt wird sowie deren Folgen



Quelle: Odom, W. (2020) CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press

# Vektoren der Netzwerk-Angriffe

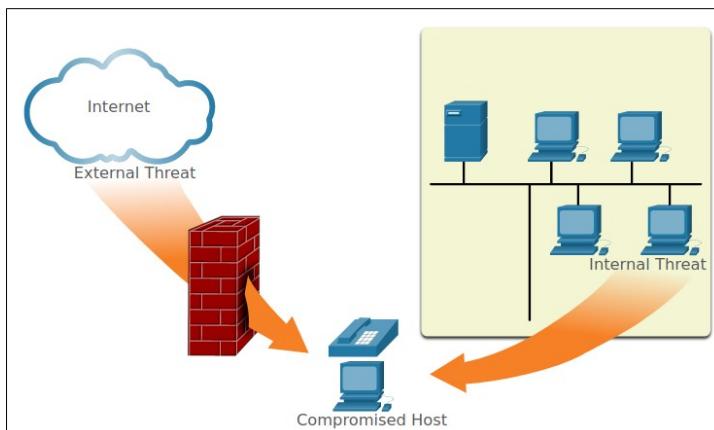
Angriffsvektor: Kombination von Weg und Technik, mit der sich Angreifer Zugang zu IT-Systemen verschaffen (z.B. Phishing)

## Bedrohung (engl. Threat)

**Externe**  
über das Internet  
z.B. DoS

**Interne**  
potentiell größere Gefahr, da direkter Zugriff auf die Infrastruktur möglich ist, u.a.

- Datendiebstahl
- Kompromittierung von Servern und Netzwerkzwischengeräten
- Netzwerkausfall
- Infizierte USB-Sticks



# Datenverlust

(Un-)beabsichtigter Datenverlust oder ein Datenleck kann für Unternehmen weitreichende Folgen haben:

- Marken- und Rufschädigung
- Verlust von Wettbewerbsvorteilen, Einnahmen und Kunden
- Rechtsstreitigkeiten, die Strafen oder Schadensersatz nach sich ziehen
- Betroffene müssen informiert werden und der Vertrauensbruch muss behoben werden

# Datenverlustvektoren - Übersicht

<b>E-Mail / Social Networking</b>	Nachrichten können abgefangen werden oder sensible Daten veröffentlicht oder missbraucht werden.
<b>Unverschlüsselte (End-)Geräte</b>	Dieb kann auf wertvolle vertrauliche Daten zugreifen.
<b>Cloudspeicher</b>	Sensible Daten können verloren gehen, wenn der Zugang durch schwache Sicherheitseinstellungen kompromittiert wurde.
<b>Wechseldatenträger</b>	Unternehmensdaten können unautorisiert auf Wechselträger wie USB-Sticks, SD-Karten, etc. übertragen werden.
<b>Hard Copy / Ausdrucke</b>	Vertrauliche Daten sollten geschreddert werden, wenn sie nicht mehr benötigt werden.
<b>Unzureichende Zugriffskontrolle</b>	Schwache Passwörter können von Bedrohungskräften leicht überwunden werden.

*Data Loss Preventionen (DLP):* Maßnahmen um den Abfluss von sensiblen Daten zu verhindern, z.B. E-Mails überwachen

# Begriff: Hacker

- 1960er manipulierten Phreaker analoge Telefonleitungen
- grundsätzliche Bezeichnung für Computerexperten
- Ein *Hack* ist eine clevere Lösung eines Computerproblems

## Grundlegende Klassifikation von Hackern:

**White Hat:** Ethische Hacker, die Ihre Fähigkeiten für legale Zwecke nutzen und Schwachstellen den Entwicklern melden.



**Gray Hat:** Führen Straftaten aus, aber nicht ausschließlich zum eigenen Vorteil. Geben manchmal die Schwachstelle bekannt, nachdem sie sie ausgenutzt haben.



**Black Hat:** Unethische und kriminelle Handlungen zur eigenen Bereicherung.



# Weitere Hacker-Einteilung

<b>Script Kiddies</b>	Teenager oder unerfahrene Hacker, die Skripte, Tools und Exploits ausführen, jedoch nicht zum eigenen Profit.
<b>Vulnerability Broker</b>	In der Regel Gray Hat Hackers, die versuchen Exploits aufzudecken u. Anbieter zu informieren - gelegentlich für Preise oder Belohnungen.
<b>Hacktivists</b>	Gray Hat Hacker, die Artikel und sensible Daten veröffentlichen sowie Angriffe ausüben, um gegen verschiedene politische und soziale Ansichten zu protestieren.
<b>Cyber Criminals</b>	Black Hat Hackers, die alleine oder für eine Organisation arbeiten. → <i>meist finanziell motiviert</i>
<b>State-Sponsored</b> Staatl. Gruppierung	White oder Black Hat Hackers, die Regierungsgeheimnisse stehlen, Informationen sammeln und Netzwerke sabotieren. Ziele sind ausländische Behörden, Terroristengruppen und Großunternehmen. Die meisten Länder üben bis zu einem gewissen Grad <i>state-sponsored</i> Hacking aus → <i>politisch motiviert</i>

Auf den folgenden Folien wird häufig die Bezeichnung **Bedrohungskteur** (*threat actor*) verwendet. Dieser umfasst Hacker sowie Personen, Geräte, Gruppen oder Staaten, die beabsichtigt oder unbeabsichtigt die Quelle eines Angriffs sind.

# Penetrationstest- / Sicherheitstest-Tools I

Angriff-Tools werden ausgefeilter und hochautomatisiert, während sie immer weniger technisches Wissen von den Benutzern erfordern. Mit den folgenden Tools kann die Sicherheit im eigenen (!) Netz getestet oder verbessert werden:

## Fuzzer / Fuzzing

*Negative oder Robustness Testing*

Eingabe von Zufallsdaten, um Schwachstellen (z.B. Bugs, Pufferüberläufe, Abstürze) aufzuspüren.

Tools: *Skipfish, Wapiti etc.*

```
$ sudo skipfish -S /usr/share/skipfish/dictionaries/minimal.wl -W new dic.t.wl -o /home/skipfish3 http://192.168.178.41
```

● XSS vector in document body (1)

1. <http://192.168.178.41/phpMyAdmin/index.php?db=&table=.htaccess.aspx-->>>  
+ ]  
Memo: injected '<sf...>' tag seen in HTML

● Incorrect caching directives (lower risk) (3)

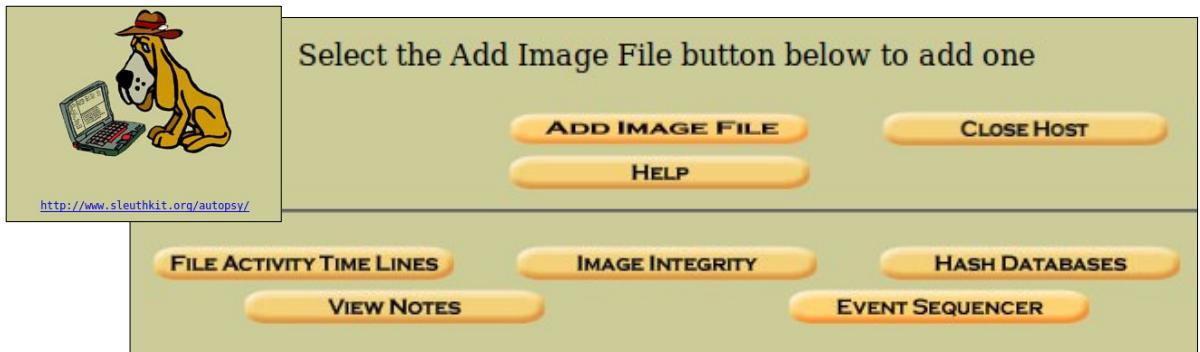
● Signature match (informational) (1)



## Forensic Tools

Digitale Beweisaufnahme sowie Spuren der Angreifer zu sichern (z.B. Logs, gelöschte Dateien)

Tools: *Sleuth Kit, Helix etc.*



Select the Add Image File button below to add one

**ADD IMAGE FILE**   **CLOSE HOST**

**FILE ACTIVITY TIME LINES**   **IMAGE INTEGRITY**   **HASH DATABASES**

**VIEW NOTES**   **EVENT SEQUENCER**

<http://www.sleuthkit.org/autopsy/>

# Penetrationtest- / Sicherheitstest-Tools II

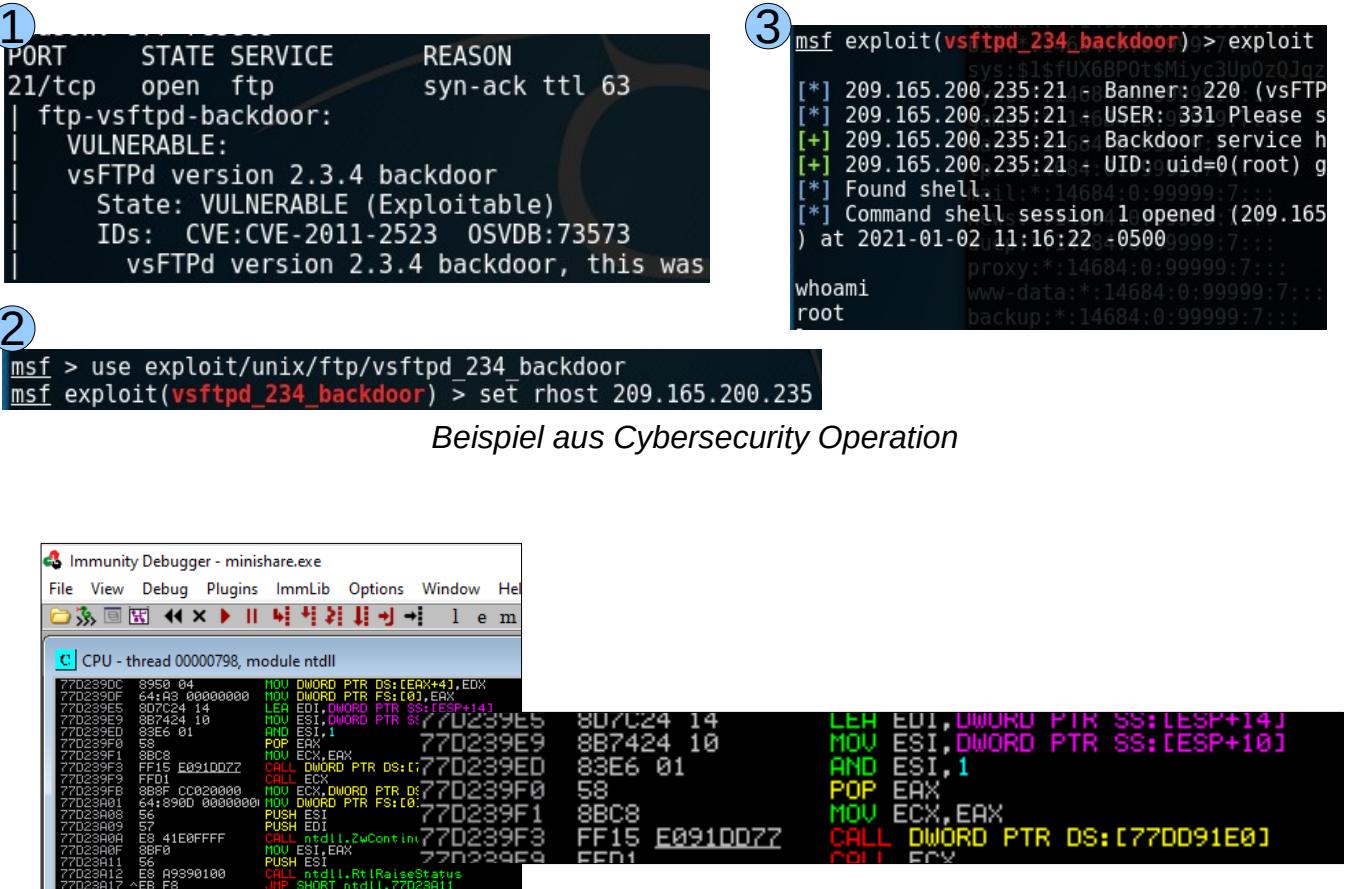
# Vulnerability Exploitation Tools

Sucht nach Schwachstellen und wendet Exploits an, um das System zu testen  
(Penetrationstest)

**Tools: Metasploit, Social Engineer Toolkit**

# Debuggers

Programmabläufe in Laufzeit  
mitverfolgen und Binärkode  
analysieren *Tools: Immunity  
Debugger, GDB etc.*



# Penetrationstest- / Sicherheitstest-Tools III

<b>Encryption Tools</b>	Schützt vor unautorisiertem Zugriff, indem es Daten verschlüsselt <i>Tools: VeraCrypt, OpenSSL etc.</i>
<b>Rootkit Detectors</b>	Versteckte Malware mit Admin-Rechten suchen, z.B. mit Integritätsprüfung von Dateien (Prüfsummen) <i>Tools: AIDE, Netfilter etc.</i>
<b>Packet Crafting</b>	Erstellen von angepassten PDUs (IP/ICMP/TCP/UDP) z.B. um die Firewall zu testen. <i>Tools: Hping, Yersinia etc.</i>
<b>Packet Sniffer</b>	LAN und WLAN Traffic aufzeichnen und analysieren <i>Tools: Wireshark, Tcpdump etc.</i>

Weitere Tools sind ...

<b>Password Crackers</b>	Passwörter knacken u.a. mittels <i>Brute-Force</i> oder <i>Dictionary Tools</i> : John the Ripper, Hydra etc.	<pre>\$ sudo john shadow2.txt ... Proceeding with wordlist:/usr/sha secret          (muster)</pre>
<b>Wireless Hacking</b>	Schwachstellen von WLAN ausnutzen (Geräte vom WLAN trennen, PSK knacken, Captive Portal umgehen, Rogue AP) <i>Tools: Aircrack-ng etc.</i>	
<b>Network Scanning</b>	Offene TCP / UDP Ports oder aktive Systeme / Hosts ( <i>Ping-Scan</i> ) finden <i>Tools: nmap, SuperScan etc.</i>	

# Angriffsarten

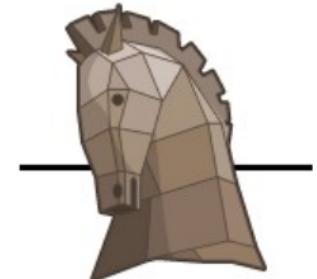
<b>Eavesdropping</b> <i>(dt. Abhören)</i>	Netzwerk Traffic anhören und aufzeichnen.
<b>Data Modification</b>	Daten werden bei der Übertragung oder im Speicher geändert ohne Wissen des Senders oder Empfängers.
<b>Password-Based</b>	Übernahme eines gültigen User-Accounts, der zur Sammlung von weiteren Informationen (z.B. Netzwerkeinstellungen) und zur Manipulation (z.B. Löschen von Dateien) dient.
<b>Man-in-the-Middle</b>	Kommunikation zwischen Sender und Empfänger überwachen, aufzeichnen und manipulieren.
<b>Compromised-Key</b>	Sichere Kommunikation mit Hilfe des Schlüssels unerkannt entschlüsseln.
<b>Sniffer</b>	Programm oder Gerät, das Netzwerkpakete liest und aufzeichnet. Unverschlüsselter Traffic ist komplett sichtbar.

Weitere sind: **IP Address Spoofing** (→ CCNA\_SRWE\_Modul 10) und **Denial of Service** (später)

# Malware – Rückblick: CCNA ItN Modul 16

## Was ist Malware?

- **Malware:** Malicious Software = Bösartige Software
- **Ziel:** Hosts/Netzwerk beschädigen oder stören, Daten beschädigen oder stehlen, Dienste beeinträchtigen, etc.



## Typen von Malware

- **Viren:** verbreiten sich selbstständig über andere Software (ausführbare Dateien).
- **Würmer:** ähnlich der Viren, benötigen aber keinen Wirt für die Reproduktion. Es werden Systemdienste genutzt.
- **Trojaner:** gibt sich als legitimes Programm aus und verleitet Anwender zur Installation. Sind vor allem für die Einrichtung von Backdoors bekannt, die einem Angreifer Zutritt verschaffen.

# Viren

- Erfordert meist Interaktion des Endnutzers (z.B. Datei öffnen oder herunterladen)
- Legt seinen Programmcode u.a. in Dateien, anderen Programmen oder Speicherbereiche ab (sog. Wirtsdateien). Werden diese aufgerufen, wird auch der Programmcode des Virus ausgeführt und in vielen Fällen auch direkt der Schadcode, andernfalls wurde ein Trigger bzw. eine Bedingung bestimmt (z.B. Datum)
- Viren können ...
  - ... Dateien ändern, beschädigen oder löschen sowie gesamte Partitionen löschen
  - ... Probleme beim Booten verursachen und Anwendungen beschädigen
  - ... vertrauliche Informationen aufzeichnen und an Angreifer senden
  - ... auf E-Mail Accounts zugreifen und E-Mails zur Verbreitung nutzen
  - ... ruhen bis Angreifer ihn aktiviert



- Übliche Infektionswege von Viren:
  - Downloads aus dem Internet
  - E-Mail-Anhänge
  - Datei auf Wechselmedien z.B. USB-Stick

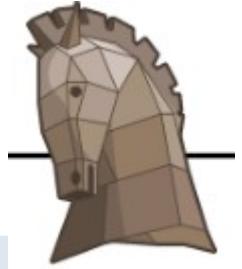


<b>Boot sector virus</b>	Bei Systemstart wird zunächst der Virus im Bootsektor (z.B. im Master Boot Record) gestartet - heutzutage selten
<b>Firmware virus</b>	Firmware / Betriebsssoftware (z.B. UEFI)
<b>Macro virus</b>	MS Office (i.d.R. in VBA geschrieben) oder andere Anwendungen mit Makro-Features
<b>Program virus</b>	Virus fügt sich in ein ausführbares Programm ein (z.B. .exe)
<b>Script virus</b>	Verbreitung über Interpreter, der Skripte wie z.B. Java-Script, PHP oder Bashscript ausführt

# Trojanisches Pferd

Getarnt als harmloses / nützliches Programm, das Schadcode enthält und weitere Malware nachladen kann.

*Folgende Bedrohungen gibt es ...*



<b>Remote-access (RAT)</b>	Ermöglicht unautorisierter (Admin-)Zugriff
<b>Data-sending</b>	Übertragung von sensiblen Daten wie Passwörtern
<b>Destructive</b>	Beschädigt oder löscht Dateien
<b>Proxy</b>	Opfer-System wird als Quelle für Angriffe verwendet, damit bleibt der Angreifer anonym
<b>FTP</b>	Ermöglicht unautorisierte Dateiübertragung, indem bspw. ein FTP-Server beim Opfer installiert wird
<b>Security software disabler</b>	Deaktiviert Firewall und Antiviren-Programme
<b>Keylogger</b>	Zeichnet Tastatureingaben auf und stiehlt damit vertrauliche Daten wie Passwörter, Kreditkartendaten

... sowie **Denial of Service (DoS)**

# Weitere Malware-Arten

## Adware

- Software, die zusätzlich mit anderer (erwünschter) Software runtergeladen wird
- Pop-up Fenster, neue Toolbars im Browser, Weiterleitung auf ungewollte Webseiten etc.
- Spioniert Nutzerverhalten aus



Urheber: Wikimedia/Pujjee8312, CC-BY-SA 4.0



## Spyware

- Nutzerdaten werden unbemerkt gesammelt und an Dritte übermittelt (ähnlich wie Adware)
- persönliche Daten, Internetnutzung, Logindaten, Screenshots etc.

# Weitere Malware-Arten II

## Ransomeware

- Bedrohungskteur verschlüsselt Dateien und fordert anschließend Lösegeld (engl. *Ransom*)
- Bei ausbleibender Zahlung werden Daten teils gelöscht oder veröffentlicht – hohe kriminelle Energie
- Anonyme Zahlungsmethode z.B. über die Kryptowährung Bitcoin
- Keine Garantie, dass nach Zahlung die gelieferte Entschlüsselungs-Software alle Daten wieder freigibt
- Verbreitung erfolgt über Krypto-Trojanern (E-Mail Anhänge, Software-Downloads und über den Browser → *Drive-by-Download*)



Urheber: Wikimedia/So5146, CC-BY-SA 4.0

## Rootkit (Administratoren-Bausatz)

- Nutzt Schwachstellen, um Admin-Rechte zu erlangen und eine Backdoor (Hintertür) zu platzieren.
- Über Backdoors können Bedrohungssakteure jegliche Malware einschleusen.
- Schadprogramm wird häufig von der Firewall und Antiviren-Programmen nicht entdeckt.
- Manipuliert u.a. Systemprogramme (z.B. netstat) oder Logdateien, um seine Existenz zu verbergen.
- Spezielle Rootkit-Entferner werden benötigt, um das System wieder zu desinfizieren.  
Besser eine Neuinstallation durchführen.

```
[*] Command shell session
) at 2021-01-02 11:16:22
whoami
root
█
```

**Beispiel:  
Sony-Rootkit**

```
L$ sudo chkrootkit
ROOTDIR is '/'
Checking `amd' ...          not found
Checking `basename' ...      not infected
Checking `biff' ...          not found
Checking `chfn' ...          not infected
```

# Reconnaissance Angriffe

## Reconnaissance (dt. Auskundschaften)

Informationen sammeln, um Kenntnisse über das Netzwerk zu erlangen und Schwachstellen zu finden.

- Recherche: Suchmaschinen, Whois, Websites des Opfers
- Ping Sweep: IP-Range nach aktive IP-Adressen scannen
- Portscan: Offene Ports und Dienste z.B. mit Nmap aufspüren
- Vulnerability Scanner: IT-Systeme werden auf bekannte Schwachstellen geprüft
- Exploitation Tools: Programme wie Metasploit versuchen die Schwachstellen auszunutzen

```
-$ whois lidl.com
Domain Name: LIDL.COM
Registry Domain ID: 20229768_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2020-02-14T04:22:53Z
Creation Date: 2000-02-20T00:40:04Z
Registry Expiry Date: 2021-02-20T00:40:04Z
Registrant Organization: Lidl Stiftung & Co.
Registrant Street: Stiftsbergstr. 1
Registrant City: Neckarsulm
Registrant State/Province:
Registrant Postal Code: 74167
Registrant Country: DE
Registrant Phone: +49.713294295354
Registrant Fax: +49.713294295439
Registrant Email: domains@lidl.com
```

```
root@kali:~# nmap -n -vv -sn 192.168.178.0/24 -oG - | grep -i 'up'
Host: 192.168.178.1 () Status: Up
Host: 192.168.178.21 () Status: Up
```

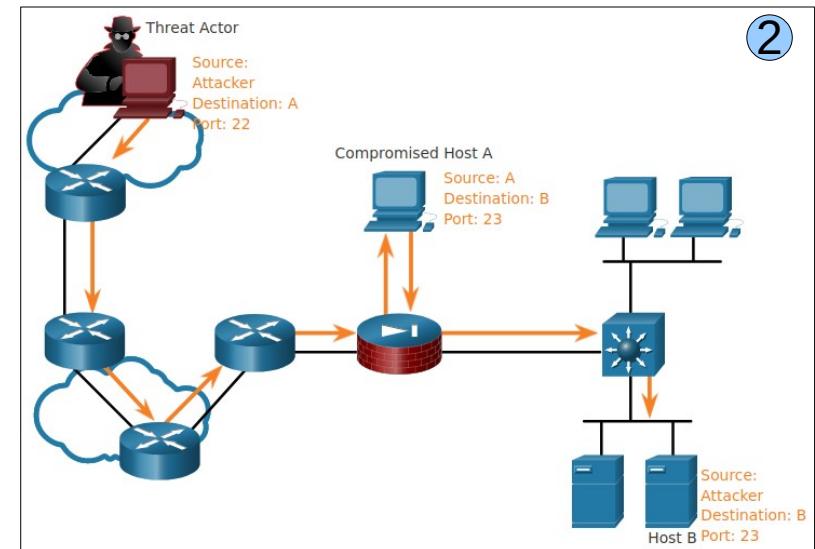
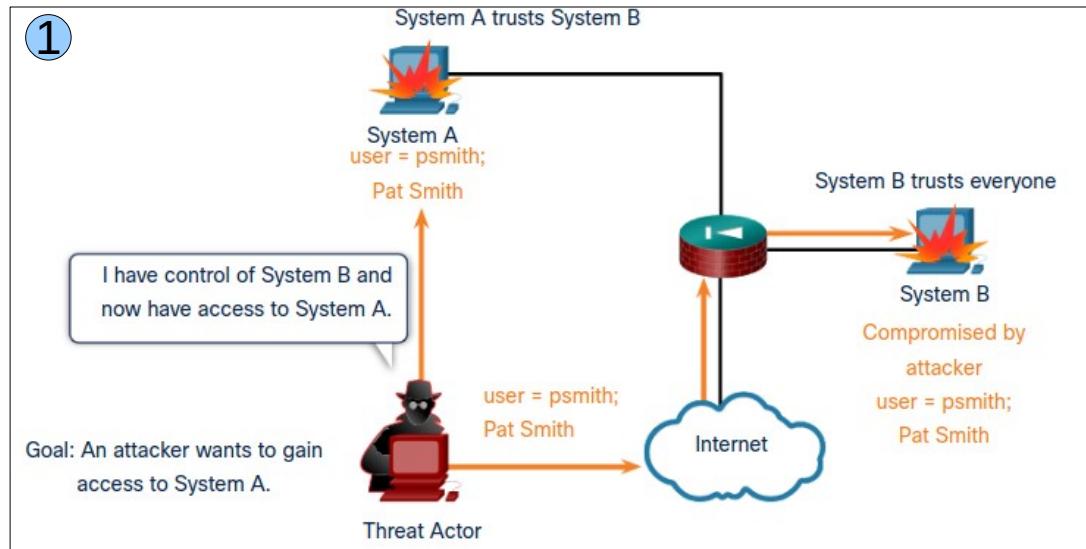
```
Nmap scan report for 209.165.200.235
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
```

# Netzwerk: Zugriff-/Access-Angriffe

**Passwort:** Verschiedene Methoden einsetzen, um Passwörter zu knacken

**Spoofing:** Angreifer täuschen andere Geräte, indem sie Adressen fälschen

**Trust Exploitation:** Über andere „vertrauenswürdige“ Geräte des Netzwerks wird das Ziel angegriffen ①. *Port Redirection* ist davon eine Art, indem z.B. Zugriffe nur vom „inside“ Host erlaubt sind ②.



Weitere sind: **Man-in-the-Middle** und **Buffer Overflow** (Überlauf eines reservierten Speicherbereichs)

# Social Engineering

Beeinflussung / Manipulation von Personen, um bestimmte Verhaltensweisen hervorzurufen oder damit sie vertrauliche Informationen preisgeben.

<b>Pretexting</b>	Unter einem Vorwand ( <i>engl. pretext</i> ) sensible Daten entlocken. Häufig i.V.m. <i>Impersonation</i> – vorgeben jemand anderes zu sein z.B. Mitglied der IT-Abteilung benötigt Anmeldeinformationen
<b>Tailgating dt. drängeln</b>	Physisches Eindringen eines Angreifers in einen für Dritte nicht zugänglichen Raum eines Unternehmens
<b>Spear phishing</b>	Gezielter Phishing Angriff mit einer persönlich wirkenden Nachricht an Mitarbeiter:innen oder Führungskräfte
<b>Something for Something / Quid pro Quo</b>	Informationen im Austausch gegen eine Zahlung oder einer (möglichen) Belohnung, z.B. Gewinnspiel, Support

# Social Engineering II

## Baiting *dt. Ködern*

Neugierde von Opfern ausnutzen, indem Speichermedien (z.B. USB-Sticks) verteilt oder im öffentlichen Raum zurückgelassen werden, die Schadcode enthalten

## Shoulder surfing

Jemanden bei der Eingabe von Zugangsdaten (Passwörter, PINs etc.) über die Schulter sehen

## Dumpster diving

Müll wird nach ausnutzbaren Daten durchsucht

Hallo, hier ist Amy vom Kundendienst. Wir müssen außerhalb Ihrer Bürozeiten die Software auf Ihrem Rechner aktualisieren. Wie lauten Ihre Benutzer-ID und Ihr Kennwort? Sie können das Passwort morgen wieder ändern, wenn Sie sich eingeloggt haben.



Social Engineer

## Beispiel Pretexting & Impersonation

# Schutzmaßnahmen gegen Social Engineering

Immer  
vertrauliche  
Informationen  
*sicher ent-  
sorgen*

Niemals  
jemandem  
Benutzer-  
name und  
Passwort  
mitteilen

Logindaten  
nicht an leicht  
zugänglichen  
Orten auf-  
bewahren

Niemals  
E-Mails von  
unsicheren  
Sendern  
öffnen

Niemals arbeits-  
bezogene  
Informationen in  
den Sozialen  
Medien posten

Niemals  
Passwörter  
von der  
Arbeit wieder  
verwenden

Offene  
Accounts nie  
unbeobachtet  
lassen

Immer  
verdächtige  
Personen  
melden

*... Mitarbeiter Schulungen und Unternehmensrichtlinien sind wichtig!*

# Denial of Service ... Angriff auf die Verfügbarkeit!

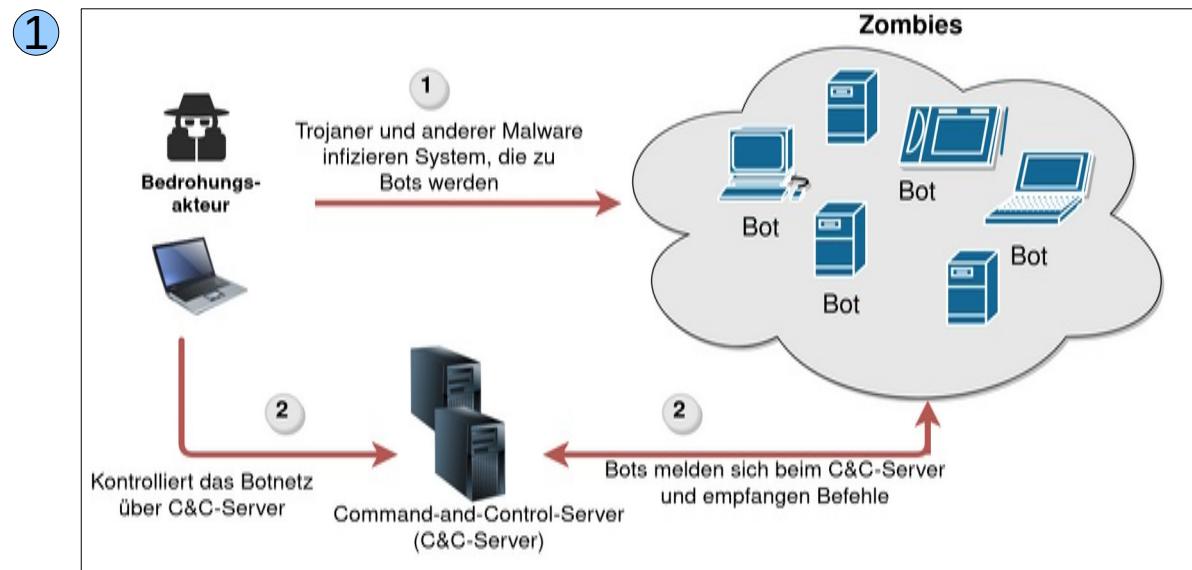
Legitimen Usern wird der Zugriff auf ein Netzwerk-Dienst verweigert aufgrund ...

**einer Überflutung von Dienstanfragen oder -paketen**

Der Ziel-Host oder das Netzwerk ist überlastet

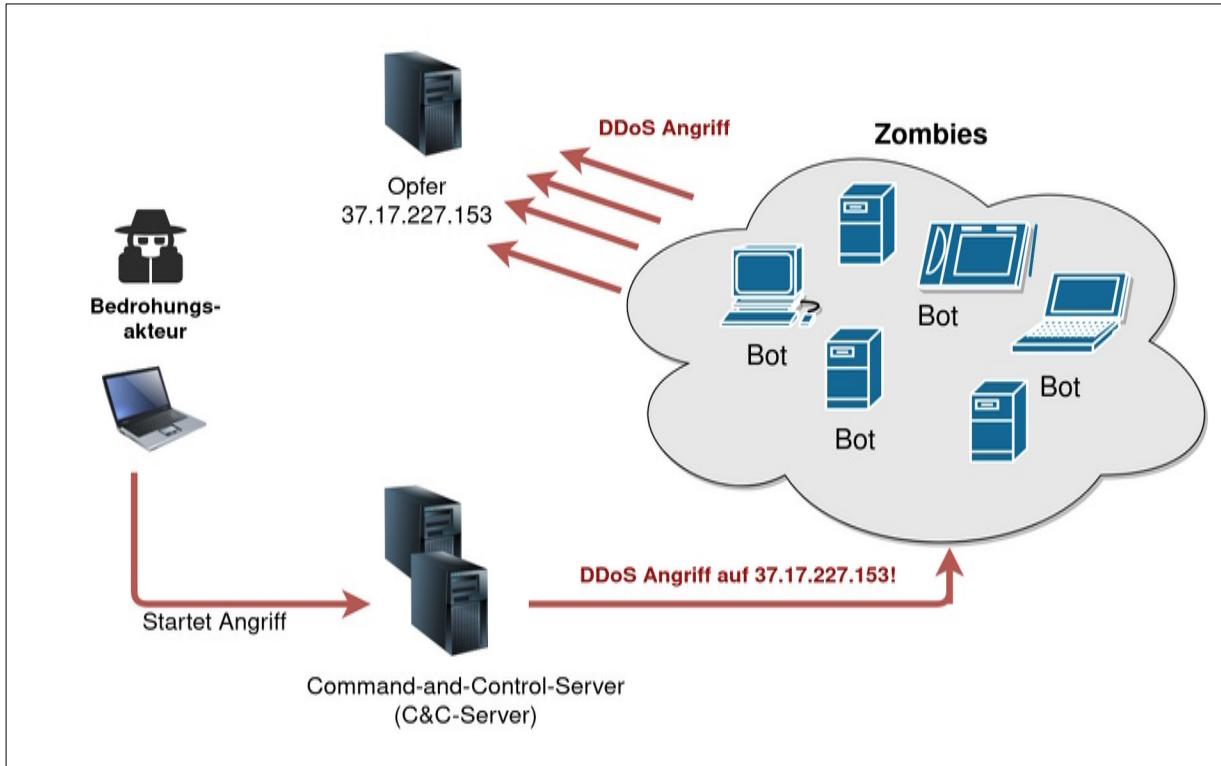
**Zusendung von schadhaften Paketen**  
Bekannte Schwachstellen werden ausgenutzt (z.B. Überforderung von Firewall Sensoren, viele Fragmente)

Distributed Denial of Service (DDoS) → viele Zombies in einem Botnet



# Distributed Denial of Service (DDoS)

②



Wenn die Bandbreite durch viele gefälschte Anfragen aufgebraucht ist, müssen Maßnahmen in Abstimmung mit dem Provider erfolgen (z.B. DDoS-Pakete filtern)

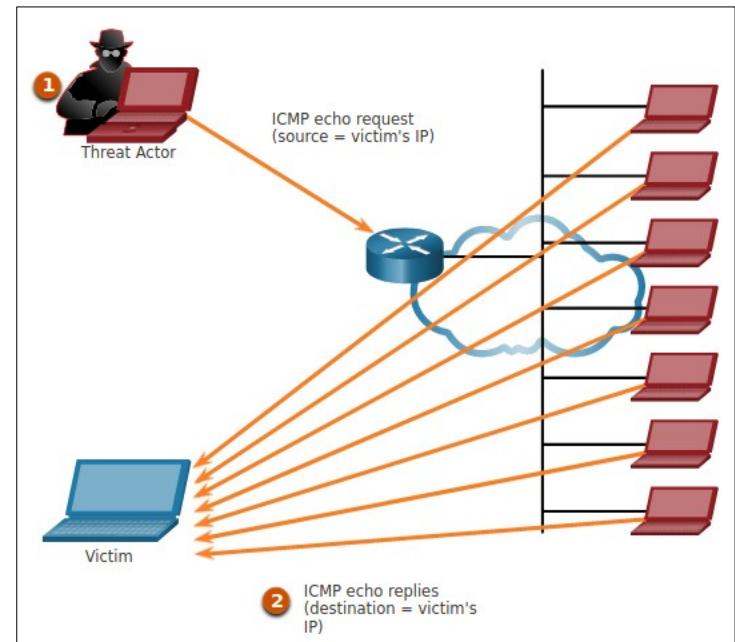
# IP Schwachstellen und Bedrohungen

## ICMP Angriff

- Echo Request & Reply-Pakete (Ping) können für Spionage und DoS-Angriffe verwendet werden
- Weiterer ICMP-Typ u.a.: „*redirect*“ / Umleitungsmeldung vom Gateway → Man-in-the-Middle Angriff
- ICMP mit ACLs einschränken!

## Amplification & Reflection Angriff (Smurf)

- ① Bedrohungskteur sendet ICMP Echo Requests mit der Quell-IP-Adresse des Opfers
- ② Hosts überfluten das Opfer aufgrund der gespooften Quell-IP-Adresse



## Address Spoofing Angriffe → siehe CCNA SRWE Modul 3

- *Bsp.: MAC-Address-Spoofing Angriff*
- Non-blind-spoofing: Angreifer kann Daten zwischen Sender und Empfänger überwachen, aufzeichnen und manipulieren → *MitM-Angriff*
- Blind-spoofing: Angreifer kann Traffic nicht einsehen → *DoS Angriff*

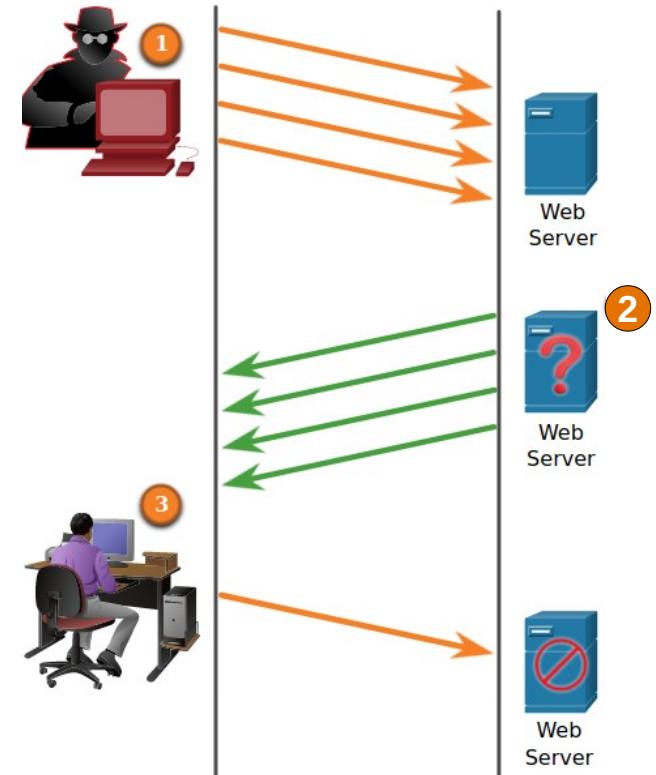
## Session hijacking

- Ein Man-in-the-Middle Angriff indem eine Sitzung übernommen wird
- Für *TCP-Sessions* muss IP-Adresse gefälscht sein, die nächste Sequenznummer vorhergesagt sowie ACK-Flags gesendet werden
- *Http-Sitzungen* können mittels einer abgefangenen Session-ID (häufig über Cookies) identifiziert und gekapert werden

## DHCP Angriffe → siehe CCNA SRWE Modul 3

# (TCP) SYN Flood Angriff

- Bekanntester DoS Angriff
  - Nutzt den *Three-Way-Handshake* aus
- ① Massenhafte Verbindungsauflöserungen (SYN-Flags) werden versendet
  - ② Server antwortet mit einem SYN-ACK-Flag (*Server hält den Socket offen und weist dem Prozess einen Speicherbereich zu*)
  - Antwort des Clients (ACK-Flag) bleibt aus  
(*nach ca. 75 Sekunden werden die Ressourcen wieder freigegeben*)
  - ③ Legitime User können den Webserver nicht mehr erreichen, da er überlastet ist



# TCP Reset Angriff

- Angreifer sendet ein gefälschtes TCP-Segment mit einem RST-Flag
- Verbindung zwischen Client und Server wird getrennt
- Voraussetzung: IP-Adressen, Portnummern und Sequenznummer müssen korrekt sein.

No.	Time	Source	Destination	Protocol	Length	Info
16	18.255777164	127.0.0.1	127.0.0.1	TCP	74	45900 → 8000 [SYN] Seq=2029627772 Win=65495
17	18.255801578	127.0.0.1	127.0.0.1	TCP	74	8000 → 45900 [SYN, ACK] Seq=549924517 Ack=20
18	18.255835281	127.0.0.1	127.0.0.1	TCP	66	45900 → 8000 [ACK] Seq=2029627773 Ack=549924
19	18.298765097	127.0.0.1	127.0.0.1	TCP	54	8000 → 45900 [RST] Seq=549924518 Win=262656
20	18.362858737	127.0.0.1	127.0.0.1	TCP	54	8000 → 45900 [RST] Seq=549924518 Win=262656
21	20.131184883	127.0.0.1	127.0.0.1	TCP	74	45902 → 8000 [SYN] Seq=3289996542 Win=65495
22	20.131209744	127.0.0.1	127.0.0.1	TCP	74	8000 → 45902 [SYN, ACK] Seq=4127464748 Ack=3
23	20.131233161	127.0.0.1	127.0.0.1	TCP	66	45902 → 8000 [ACK] Seq=3289996543 Ack=412746
24	20.149976013	127.0.0.1	127.0.0.1	TCP	54	8000 → 45902 [RST] Seq=4127464749 Win=262656
25	20.186798634	127.0.0.1	127.0.0.1	TCP	54	8000 → 45902 [RST] Seq=4127464749 Win=262656
26	23.761663676	127.0.0.1	127.0.0.1	TCP	68	8000 → 45896 [PSH, ACK] Seq=2086062461 Ack=2
27	23.761692291	127.0.0.1	127.0.0.1	TCP	54	45896 → 8000 [RST] Seq=298341777 Win=0 Len=0
28	23.761771395	127.0.0.1	127.0.0.1	TCP	66	8000 → 45900 [RST, ACK] Seq=549924518 Ack=20
29	23.761796002	127.0.0.1	127.0.0.1	TCP	66	8000 → 45902 [RST, ACK] Seq=4127464749 Ack=3
30	23.806873070	127.0.0.1	127.0.0.1	TCP	54	8000 → 45896 [RST] Seq=0 Win=262656 Len=0
31	23.867319289	127.0.0.1	127.0.0.1	TCP	54	8000 → 45896 [RST] Seq=0 Win=262656 Len=0

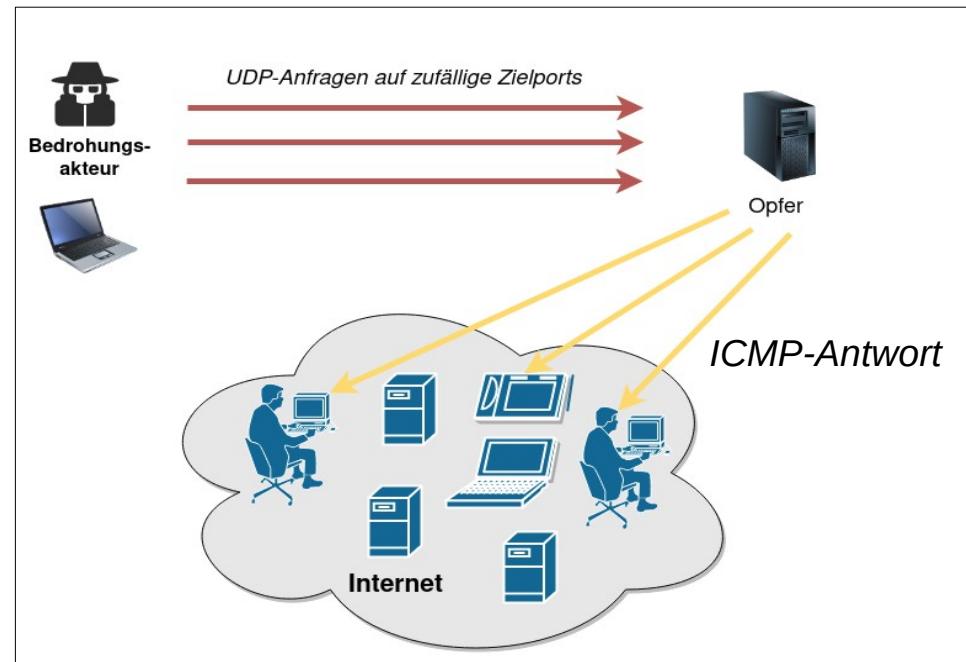
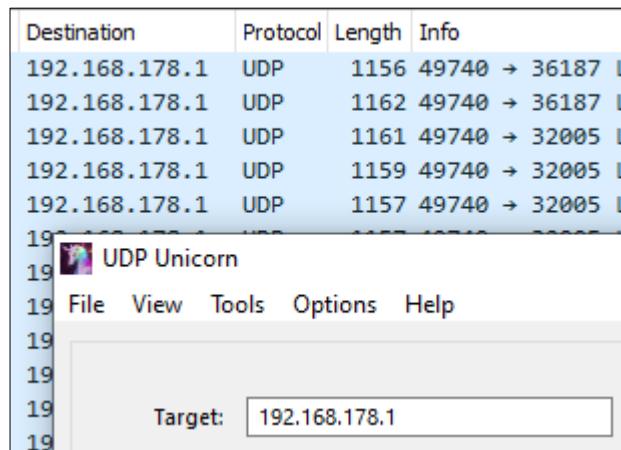
Wireshark-Auszug: RST-Segmente führen kontinuierlich zu Verbindungsabbrüchen

Anleitung: <https://robertheaton.com/2020/04/27/how-does-a-tcp-reset-attack-work/>

[Zugriff: 02.01.2021]

# UDP Flooding Angriff

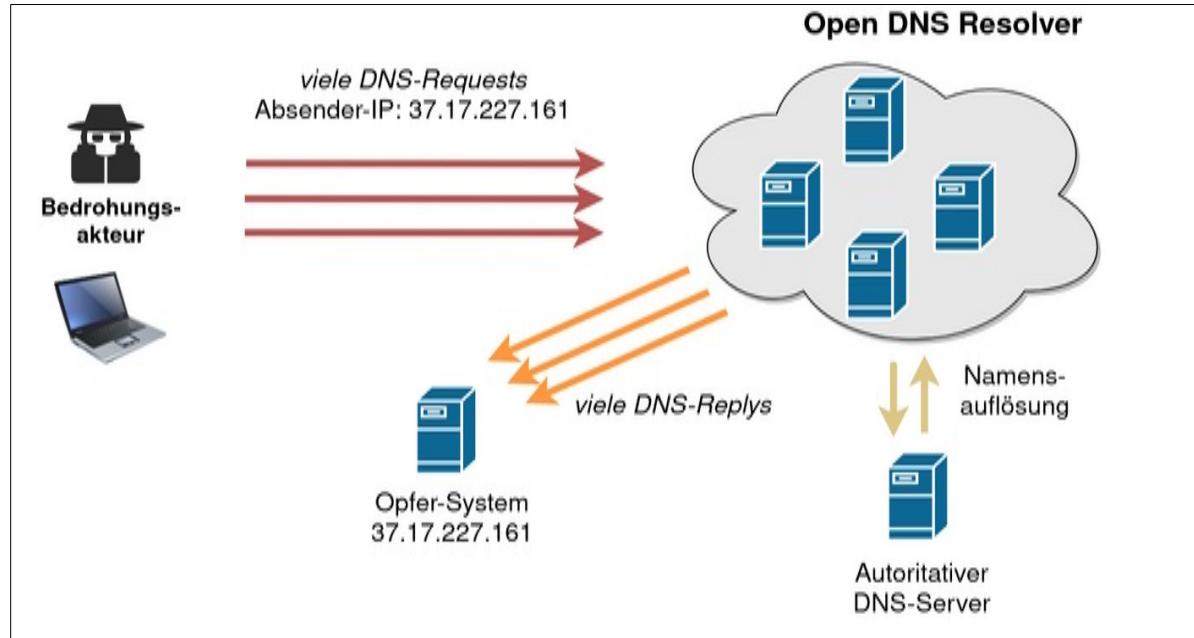
- Gefälschte UDP-Pakete fluten beliebig *geschl.* Ports (kein Dienst ist aktiv!)
- Server antwortet auf die Anfrage mit einer ICMP Nachricht: *port unreachable*
- Reguläre Anfragen können vom Server nicht mehr beantwortet werden
- Zur Verschleierung des Angriffs wird häufig die Absender-Adresse gefälscht
- *Tools: Unicorn, Low Orbit etc.*



# DNS Resolver Attacks

Offene DNS Resolver können für Angriffe missbraucht werden  
(z.B. Google 8.8.8.8, Quad9 9.9.9.9 oder OpenDNS 208.67.222.222)

- **DNS Amplification und Reflection Angriff:** Bedrohungskteur sendet DNS Anfragen mit der IP-Adresse des Opfers

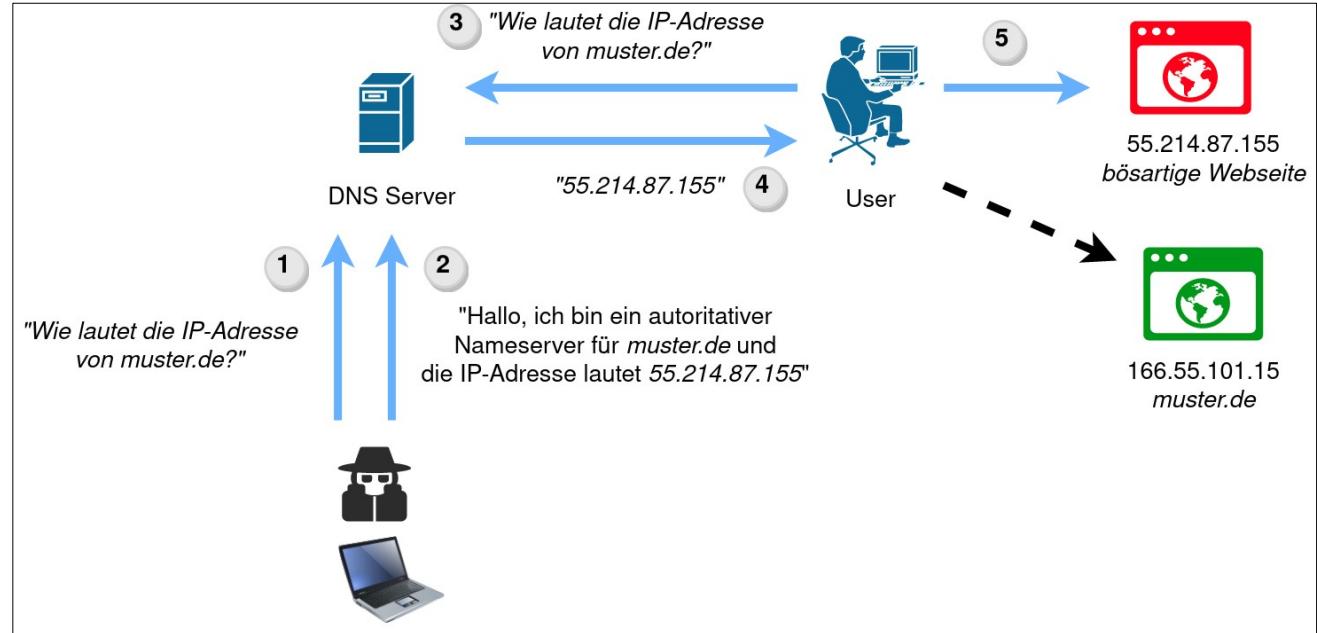


- **DNS Server überlasten:** DoS Angriff auf einen offenen DNS-Resolver

# DNS Resolver Attacks II

- **DNS Cache Poisoning (stark vereinfacht):**

- Jeder DNS Resolver speichert DNS Antworten von anderen (autoritativen) Nameserver im Cache bis TTL abgelaufen ist.
- Angreifer gibt sich als Nameserver aus und sendet eine manipulierte Antwort an den DNS Resolver
- DNS Resolver speichert die empfangene Resource Record im Cache
- Clients werden bei Anfragen auf eine bösartige Webseite weitergeleitet



# Weitere DNS Angriffe und Techniken

## DNS Domain Shadowing Angriff

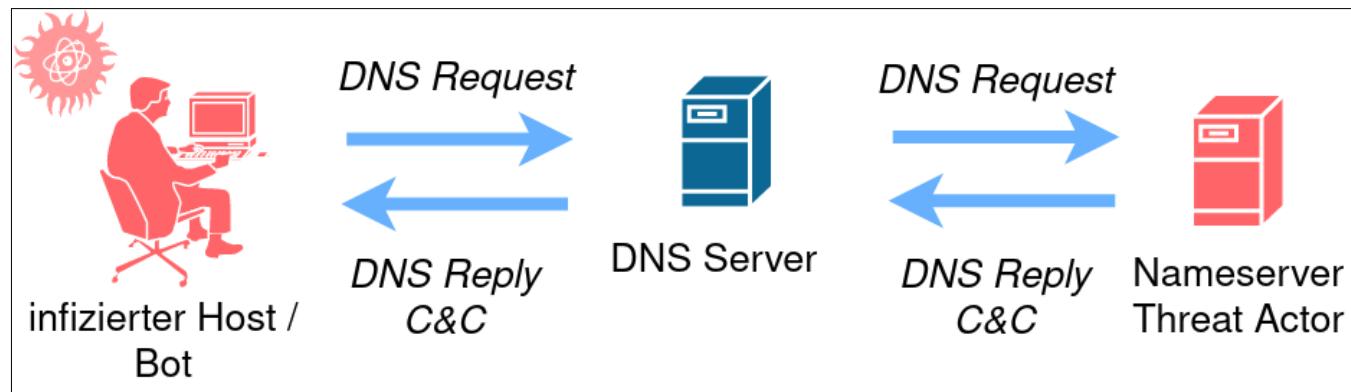
Bedrohungskteur verschafft sich Zugriff zu einem Domain-Account und generiert heimlich Sub-Domains, die bspw. auf bösartige Server weiterleiten.

## DNS Stealth Techniques / DNS Tarntechniken

- *Fast Flux:*  
Bedrohungskteur verschleiert Standort des Webservers mit bösartigen Webseiten, indem er in kurzen Zeitabständen (ca. 5 Minuten) die IP-Adresse der Domain wechselt (A / AAAA Resource Record). *Double IP Flux = Fast Flux + Wechsel des zuständigen autoritativen Nameservers*
- *Domain Generation Algorithms (DGA)*  
Schnell wechselnde Domainnamen, die für „Rendezvous“ / Treffpunkte zwischen Botnets und C&C-Server verwendet werden

# DNS Tunneling

- Bedrohungskteur verwendet DNS Tunnel, um „eigenen“ Traffic zu verstecken
- Daten werden als DNS Anfrage gekennzeichnet und an den DNS Server / ISP weitergeleitet (rekursive Anfrage)
- DNS Server leitet die Anfrage an einen verantwortlichen Nameserver weiter, der dem Bedrohungskteur gehört
- Angreifer antwortet auf die DNS Anfrage und versteckt Anweisungen in der DNS Antwort
- Symptome: verdächtige Domainnamen und auffällig viel Traffic in kurzer Zeit
- Geht auch mit  
ICMP, VPN,  
SSH
- ...



# CIA-Triade /-Schutzziele

Bewährte Strategien zur Verteidigung von IT-Systemen werden in drei Bereiche eingeteilt, sog. CIA-Triade bzw. CIA-Schutzziele:

- **Vertraulichkeit (engl. Confidentiality)**

Nur autorisierte Personen oder Geräte dürfen auf sensible Daten zugreifen → Verschlüsselung von Daten, z.B. mit AES

- **Integrität (engl. Integrity)**

Schutz vor unbefugten Änderungen von Daten  
→ Hashing, z.B. mit SHA

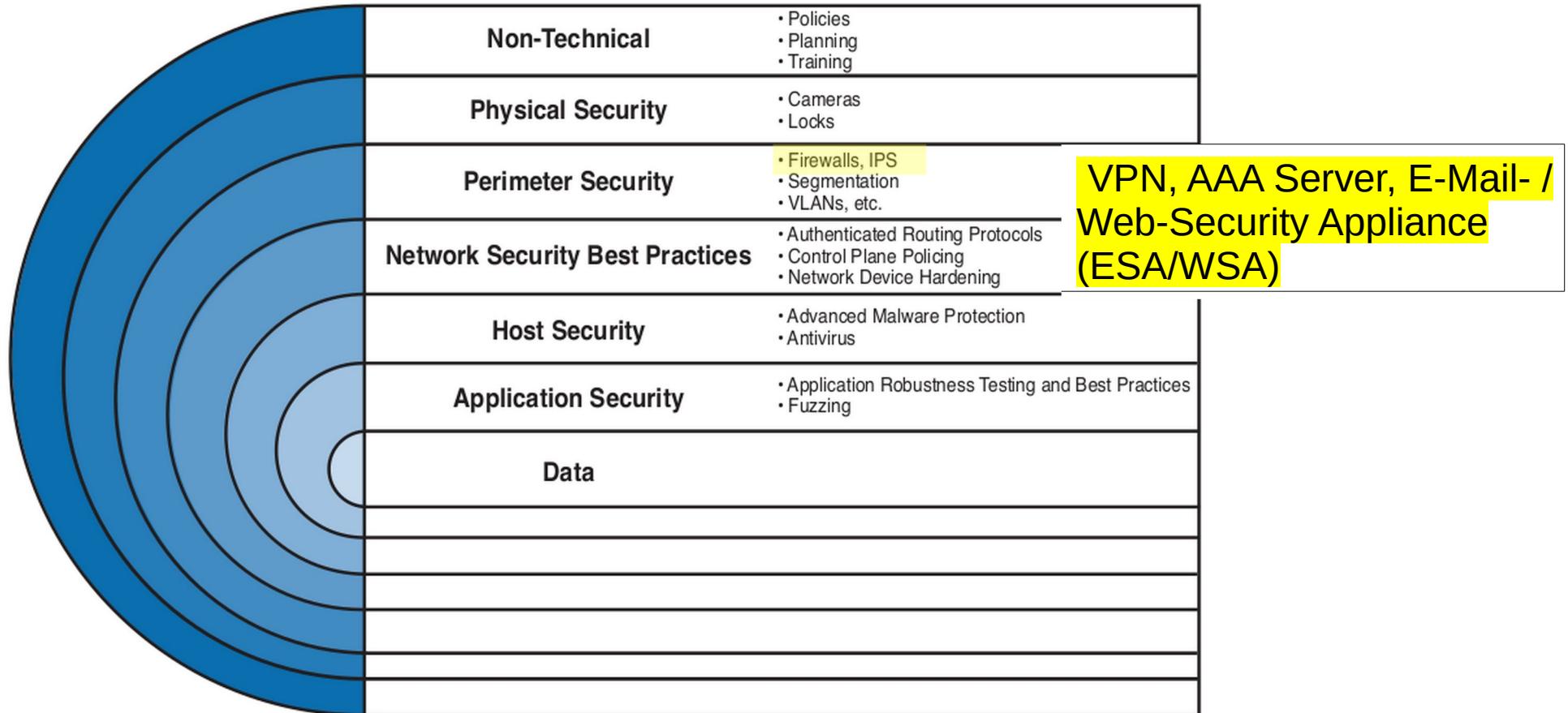
- **Verfügbarkeit (engl. Availability)**

Ununterbrochener Zugriff auf wichtige Daten  
→ Redundante Dienste, Gateways, Links etc.



# Defense-in-Depth Approach („Tiefenverteidigungs-Methode“)

Ziel ist der Einsatz von mehreren Schutz-Schichten bzw. -Systemen

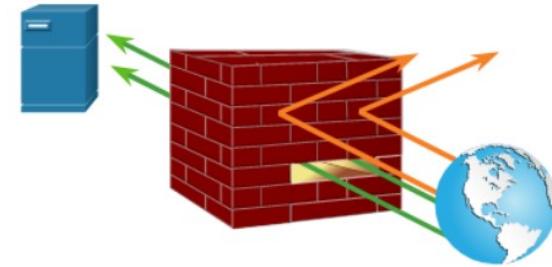


Bildquelle: Santos, O. (2017) CCNA Cyber Ops SECFND 210-250 Official Cert Guide

# (Netzwerk-)Firewall

- Bestehen aus einem oder mehreren Systemen
- Kontrollieren Zugriffe zwischen unterschiedlichen Netzwerken bzw. Netzwerk-Segmenten anhand von Richtlinien (*Policies*)

-  Blockiert bösartige Pakete
-  Schützt sensible Daten (z.B. Zugriffskontrolle, AAA Dienste, DMZ)
-  Steuert den Einsatz von Protokollen (z.B. nur eine bestimmte Anzahl von DNS Anfragen zulassen)



## ABER

-  Fehlkonfiguration kann verheerende Auswirkungen haben
-  Schädliche Daten bleiben unentdeckt, indem sie getunnelt bzw. versteckt werden
-  Netzwerkverkehr kann sich stark verlangsamen
-  User versuchen Firewalls zu umgehen, damit sie geblockte Webseiten aufrufen können

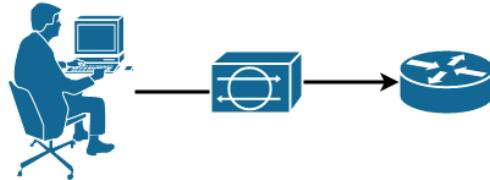
# (Netzwerk-) Intrusion-Prevention-System

- Sensoren analysieren und zeichnen Daten im Netzwerk auf
- Bösartige Pakete können anhand von Angriffsmustern erkannt und geblockt werden
- Angriffsmuster können bekannte Signaturen oder Anomalien sein, d.h. das Netzwerk verhält sich nicht „normal“



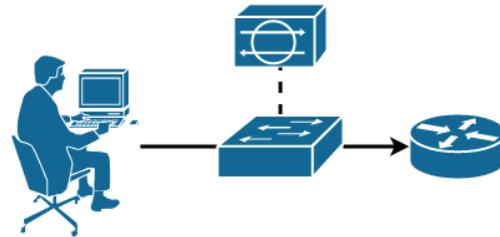
```
01/02-14:31:22.431686 [**] [1:1000003:0] Malicious Server Hit! [**]
[Priority: 0] {TCP} 209.165.200.235:37028 -> 209.165.202.133:6666
```

## Intrusion-Prevention-System (IPS) vs. Intrusion-Detection-System (IDS)



„inline“

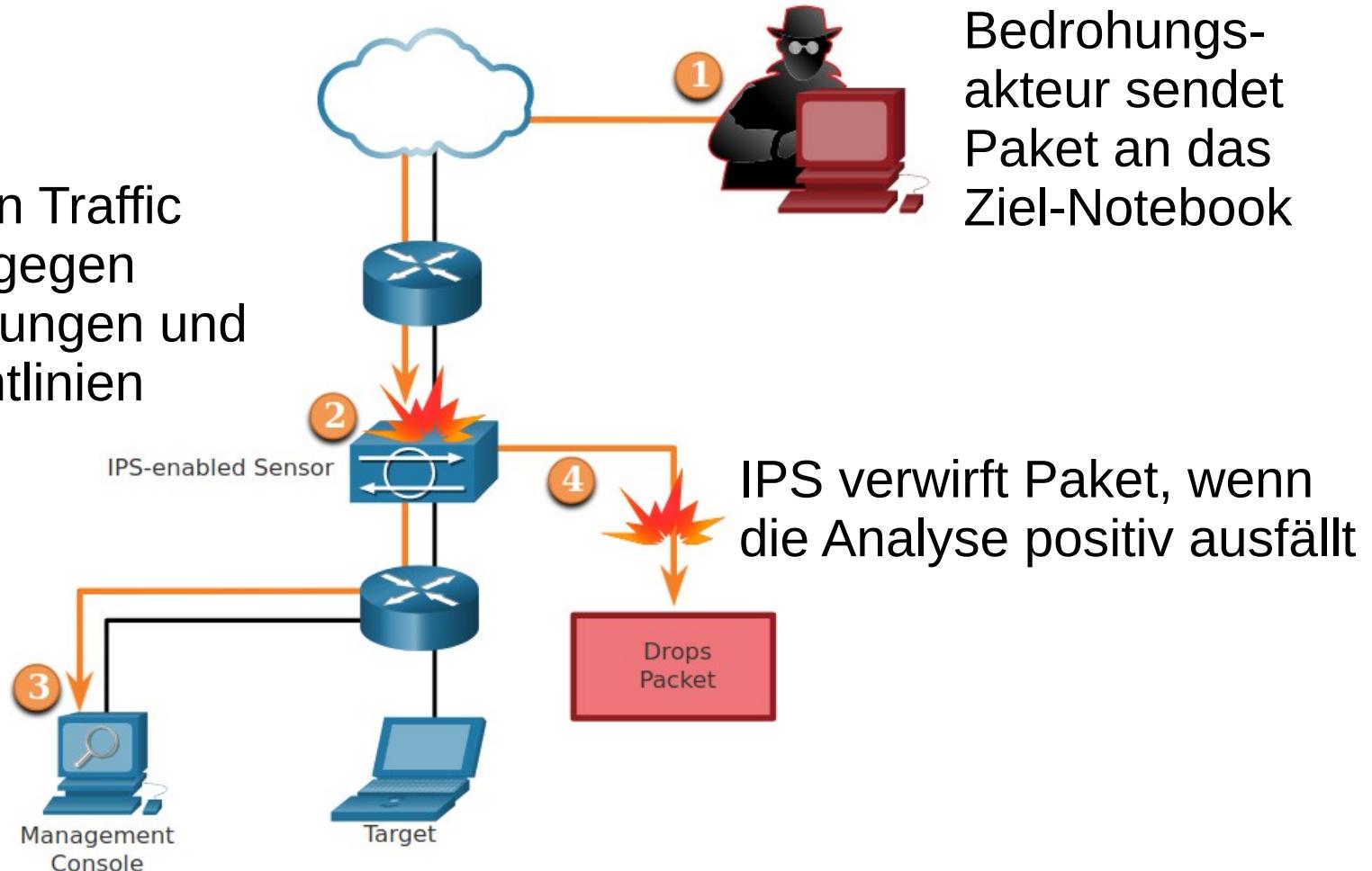
... kann Traffic direkt blockieren



... überprüft Kopie des Datenstroms

# IPS Operationen: Deny Traffic

IPS analysiert den Traffic und prüft diesen gegen bekannte Bedrohungen und konfigurierte Richtlinien



# Sichere Datenübertragung - Überblick

## Datenintegrität

- Daten wurden nicht verändert
- *Hashing: MD5 und SHA*

## Authentizität

- Nachricht wurde nicht gefälscht und stammt vom Kommunikationspartner
- *Hash Message Authentication Code (HMAC)*

## Vertraulichkeit

- Nur autorisierte Benutzer können die Nachricht lesen
- *Symmetrische (AES) und asymmetrische (RSA) Verschlüsselung*

## Verbindlichkeit / Nichtbestreitbarkeit

- Sender kann die Gültigkeit der Nachricht nicht abstreiten
- *Digitale Signaturen*

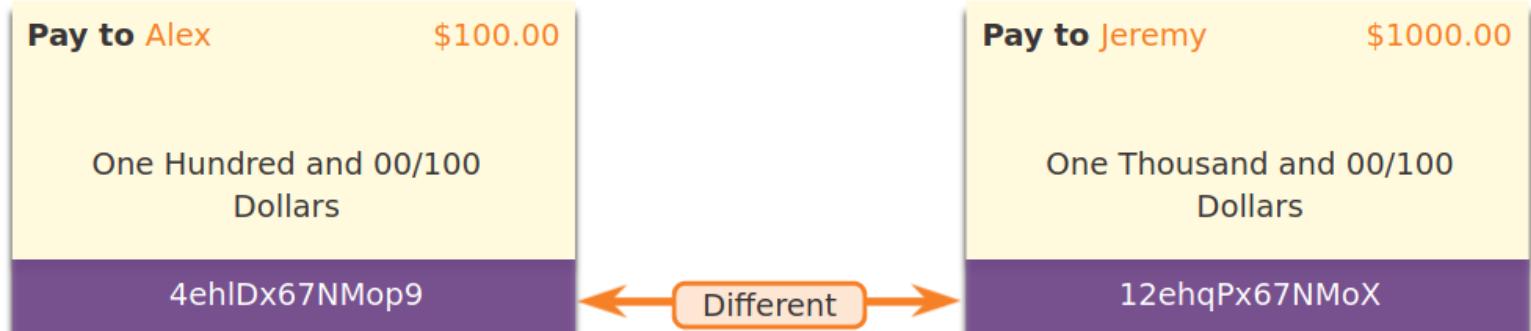
# Datenintegrität - Hashing

Mit Hashing (*dt. zerhacken*) kann überprüft werden, ob Daten verändert wurden (absichtlich oder versehentlich).

## Hash Algorithmus

- Aus einem beliebig langem Eingabewert (Nachricht) wird immer ein gleich langer Ausgabewert (Hashwert z.B. `4ehIDx67NMop9`) erstellt.
- Nachricht und Hashwert werden in Klartext übermittelt.
- Empfänger lässt erneut einen Hashwert aus der Nachricht berechnen:  
Neu berechneter Hashw. = übermittelter Hashw. → Nachricht unverändert  
Neu berechneter Hashw. ≠ übermittelter Hashw. → Nachricht verändert

### *Beispiel:*



# Bekannte kryptographische Hash-Algorithmen

## Message Digest Version 5 (MD5) - Klassiker

- Generiert aus einem Eingabewert einen 128-Bit-Hash
- Gilt seit 2012 als nicht sicher, dennoch ist es weit verbreitet (z.B. Dateidownload etc.)

## Secure Hashing Algorithm (SHA)

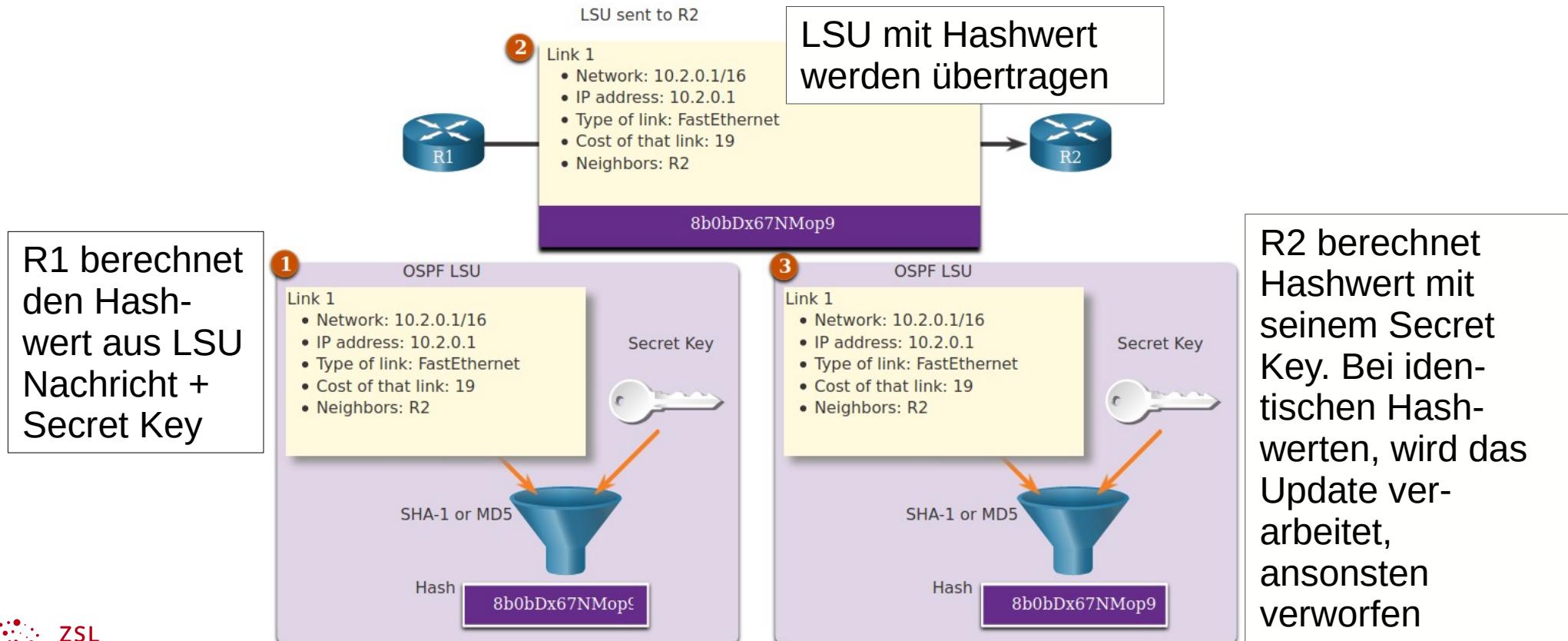
- SHA-1 gilt als nicht sicher
- SHA-2 stellt verschieden lange Hashwerte bereit:  
SHA-224, SHA-256, SHA-384 & SHA-512  
→ *neuester Stand*
- SHA-3 ist noch nicht weit verbreitet

Description :	UNIVERSAL
Release :	15.2.E3k
Release Date :	08-Dec-2020
FileName :	c1000-universalk9-tar.152-7.E3k.tar
Min Memory :	DRAM 512 Flash 256
Size :	36.71 MB ( 38492160 bytes)
MD5 Checksum :	9154ec0a337636d85270424d2535f4bb 
SHA512	95a9856a7269b9bedf568bee5961d484 ... 
Checksum :	

Hashing alleine kann keine Sicherheit bei der Übertragung der Daten bieten  
*(Bspw. kann die Nachricht und der Hashwert manipuliert werden → MitM)*

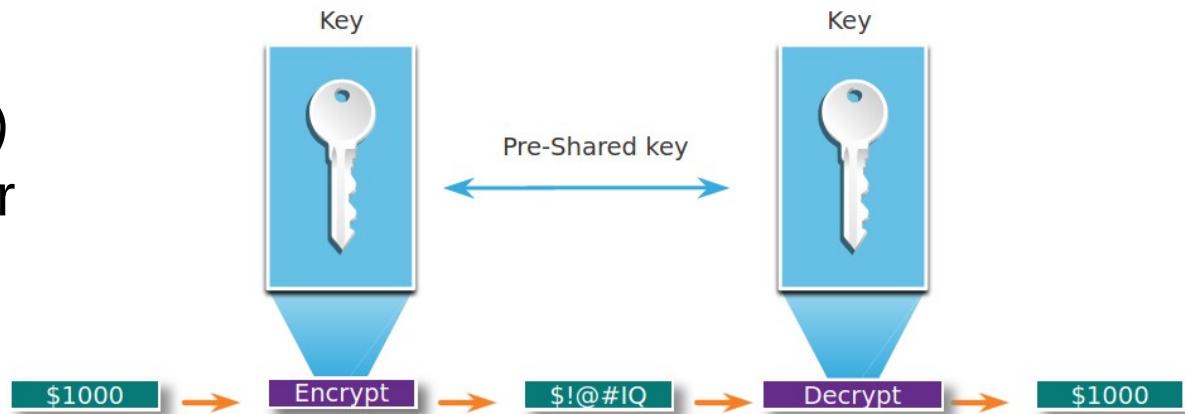
# (Keyed-) Hash Message Authentication Code (HMAC)

- Kombiniert Hashing-Funktion mit einem geheimen Schlüssel
- Nur mit Schlüssel kann der Hashwert erzeugt und überprüft werden
- Beispiel Authentifizierung von OSPF-Nachrichten:



# Symmetrische Verschlüsselung

- Sender und Empfänger verschlüsseln Daten mit dem gleichen Schlüssel
- Gängige Schlüssellängen sind zwischen 128 und 512 Bits, z.B. VPN
- **Vorteil:** (CPU-)ressourcenschonend bzw. schneller im Vergleich zur asymmetrischen Verschlüsselung
- **Nachteile:** Vor der Datenübertragung muss der Schlüsselaustausch erfolgen und für jeden Kommunikationspartner muss ein eigener Schlüssel verwaltet werden
- Wird häufig zur Verschlüsselung von großen Datenmengen (*Nutzdaten*) und in Kombination mit der asymmetrischen Verschlüsselung verwendet



# Block- und Stromchiffren

## Blockchiffren

- Zeichen werden blockweise verschlüsselt: 64 oder 128 Bit
- Bei weniger Zeichen werden Daten aufgefüllt (z.B. Leerzeichen)
- Blockchiffren generieren mehr Ausgabedaten als Eingabedaten vorlagen



## Stromchiffren

- Klartext wird zeichenweise bzw. Bit für Bit verschlüsselt
- Verwendung bei Echtzeitübertragungen z.B. Mobilfunk, WLAN



# Symmetrische Verschlüsselungsalgorithmen

<b>3DES</b>  (Triple Digital Encryption Standard)	<ul style="list-style-type: none"><li>• Nachfolger von DES</li><li>• Ein fester Block von Zeichen (<i>64 Bit</i>) wird verschlüsselt und drei Mal wiederholt (<i>effektiv nur 112 Bit Schlüssellänge</i>)</li><li>• Wird häufig verwendet, dennoch langsam und nicht sehr sicher</li><li>• Empfohlen wird eine kurze Schlüssel-Lebensdauer</li></ul>
<b>AES</b>  (Advanced Encryption Standard)	<ul style="list-style-type: none"><li>• Bietet unterschiedliche Kombinationen von Blockgrößen und Schlüssellängen an (128, 192 oder 256-Bit)</li><li>• Alle AES-Varianten gelten als sicher</li><li>• Ein fester Block von Zeichen (<i>hier 64 Bit</i>) wird verschlüsselt</li></ul>

Weiterer symmetrischer Stromchiffre Algorithmus ist  
**Rivest Ciphers (RC4)** → von AES abgelöst

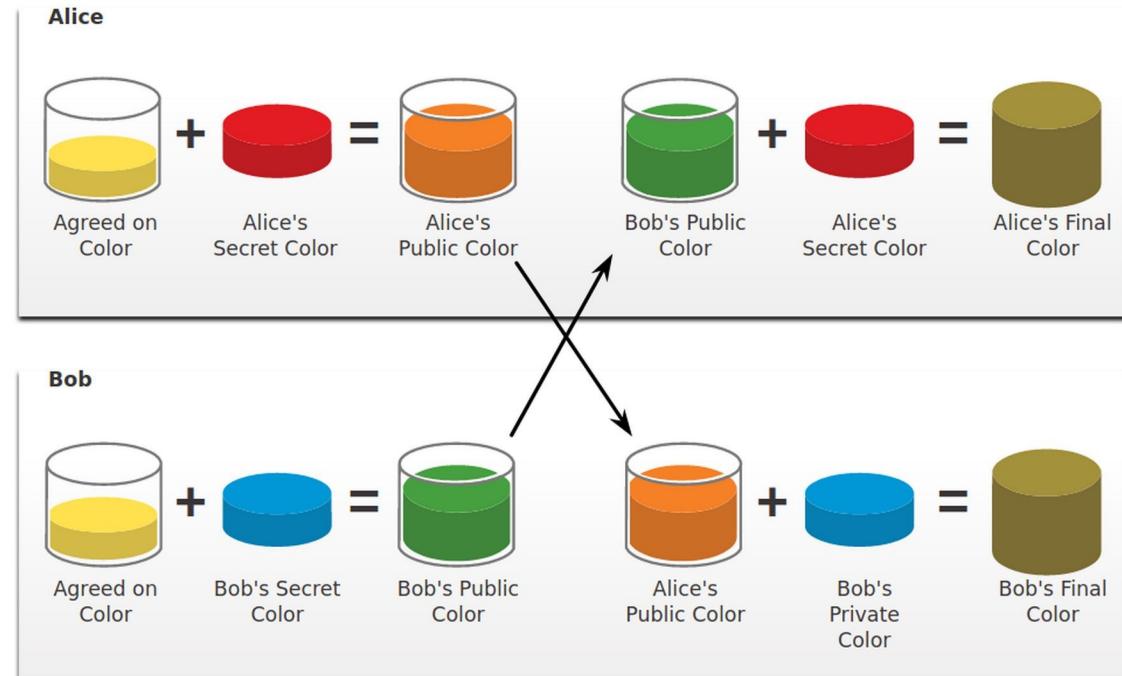
# Asymmetrische Verschlüsselung

- auch Public-Key Algorithmus genannt
- Ver- und Entschlüsselung erfolgen mit unterschiedlichen Schlüsseln
- Sender verschlüsselt Nachricht mit öffentlichem Schlüssel
- Empfänger entschlüsselt Nachricht mit (*geheimen*) privatem Schlüssel
- Nachteil: Wesentlich ressourcenaufwendiger als die symmetrische Verschlüsselung



# Asymmetrische Algorithmen: Diffie-Hellman (DH)

- Erstes asymmetrisches Verfahren (1976)
- Beide Kommunikationspartner generieren einen gemeinsamen *shared Key*, ohne dass dieser Schlüssel übertragen werden muss
- Verwendung u.a. bei SSL/TLS, SSH und IPsec
- Großteil des Datenverkehrs wird symmetrisch verschlüsselt (z.B. 3DES, AES) und DH wird zur Generierung des symmetrischen Schlüssels verwendet
- Schlüssellänge 512, 1024, 2048, 3072 oder 4096



# Weitere asymmetrische Algorithmen

## Rivest, Shamir, and Adleman (RSA) Verschlüsselungs-Algorithmus

- 1978 entwickelt und weit verbreitet
- Produkt zweier großer Primzahlen
- Primfaktorzerlegung (Faktorisierung) ist sehr aufwendig und bei großen Zahlen faktisch unmöglich
- Einsatzzweck: Verschlüsselung von kleinen Datenmengen, z.B. Schlüsselaustausch sowie digitale Signaturen
- Schlüssellänge sollte 2048 oder 4096 Bit besitzen

Weitere asymmetrische Algorithmen sind:

**EIGamal** → basiert auf DH und Standard der US-Regierung sowie

**Elliptische-Kurven-Kryptographie (ECC)** → bei gleichem Sicherheitsniveau ist eine kürzere Schlüssellänge als bei RSA möglich

# Modulabschluss

- Lab - Lab - Social Engineering – 3.5.7
- Lab - Explore DNS Traffic – 3.8.8
- Module Quiz – Network Security Concepts – 3.11

## Fragen ...

