CloudCommand

Übung: DNS-Hierarchie

Voraussetzungen & nötige Tools

Technische Voraussetzungen:

- Ein Rechner mit Internetzugang
- Möglichst ein UNIX-ähnliches Betriebssystem (Linux/Mac) oder Windows mit installiertem dig-Tool

Alternativen:

- Online-Tools wie DNSDumpster.com oder MXToolbox.com, falls lokale Installation nicht möglich ist.

Dokumentation und Auswertung

Was dokumentieren?

- Ergebnisse aller Abfragen (Screenshots oder Kopien der Terminalausgabe)
- Auffälligkeiten in Wireshark
- Eventuelle Fehler und deren Behebung

Diskussionspunkte:

- Was hat überrascht?
- Wo bestanden Schwierigkeiten bei der Auflösung oder in der Konfiguration?
- Was konntet ihr Neues über die DNS-Hierarchie lernen?

1. Abfragen mit nslookup und dig

Anleitung:

1. Wählt 3 Domains aus (z. B. example.com, heise.de, wikipedia.org).
2. Führt mit nslookup und dig jeweils A-Record-Abfragen durch.
3. Versucht, den Mail-Exchange (MX)-Record zu finden (z. B. dig MX example.com).
4. Analysiert die Ausgaben: Welche Nameserver wurden kontaktiert? Wie sehen die Antworten aus?

Tipp: *Notiert die Reihenfolge und vergleicht die Ergebnisse beider Tools, um Unterschiede und Gemeinsamkeiten zu erkennen.*

2. Protokollanalyse mit Wireshark

Technische Voraussetzungen:

1. Startet Wireshark und wählt das entsprechende Netzwerkinterface aus.
2. Filtert den Traffic mit dns (z. B. im Filterfeld „dns“ eingeben).
3. Führt erneut Abfragen aus (z. B. mit dig example.com). Beobachtet in Echtzeit, wie die DNS-Pakete aussehen.
4. Untersucht, welche Flags gesetzt sind (z. B. Recursion Desired, Recursion Available).
5. Notiert, welche Nameserver (IP-Adressen) in den einzelnen Paketen auftauchen.

2. Protokollanalyse mit Wireshark

Zusatzaufgabe:

Vergleicht den Traffic bei einer erfolgreichen Abfrage (Antwortcode NOERROR) mit einer unbekannten Domain (z. B. dig nonexistentdomain.abc) und analysiert, wie sich die DNS-Antwort unterscheidet.

3. Eigene DNS-Zone aufsetzen

Anleitung:

1. Richtet auf einer VM oder einem lokalen System einen kleinen Bind9-Server (oder alternativen DNS-Server) ein.
2. Legt eine Zonendatei für eine fiktive Domain an (z. B. meinedomain.local).
3. Konfiguriert A-Records, CNAME-Records und MX-Records nach eigenem Belieben.
4. Testet die Auflösung eurer fiktiven Domain lokal mit dig @localhost meinedomain.local.

Hinweis: *Dieser Teil ist optional und kann je nach Vorkenntnis etwas Zeit in Anspruch nehmen, macht aber Spaß und fördert das Verständnis für DNS-Konfigurationen.*

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm